УДК 512.5

Козачок О. Я.

DOI: https://doi.org/10.18523/2617-70803202038-47

РАНДОМІЗОВАНІ АЛГОРИТМИ ПЕРЕВІРКИ ЧИСЕЛ НА ПРОСТОТУ

Рандомізація та ймовірнісний підхід у побудові алгоритмів займають помітне місце. Через обмеженість обчислювальних ресурсів та складність багатьох задач у деяких випадках отримати точні результати є неможливим або занадто витратним, тому результати можуть містити деяку невизначеність. Також у деяких випадках недетермінованість алгоритму є його перевагою, наприклад у задачах криптографії, або корисною характеристикою, як-от у симуляціях процесів, що містять невизначені параметри.

У цій роботі ми розглядаємо основні поняття та твердження, що стосуються рандомізованих алгоритмів перевірки чисел на простоту, наводимо необхідні теореми.

Ключові слова: алгоритми, прості числа, рандомізовані алгоритми, перевірка чисел на простоту.

Вступ

Великі прості числа (порядку 10^{300}) використовують у криптографії з відкритим ключем, а також у хеш-таблицях і для генерації псевдовипадкових чисел (зокрема, в генераторі псевдовипадкових чисел Вихор Мерсенна).

Завдяки використанню двійкового представлення чисел ледь не у всіх цифрових пристоях перевірка числа на парність чи непарність є максимально можливою простою операцією. Тому в цьому тексті будемо виходити з цього факту, який має наслідком можливість звуження формулювань на множини непарних або парних чисел, вважаючи, що визначення парності або непарності має нехтувану складність. Можна також зауважити, що й у десятковому записі чисел парність чи непрарність числа є очевидною характеристикою.

Класичними роботами в цій галузі вже зараз можна назвати такі: [1–7; 9].

Загальні відомості

Наведемо загальні відомості щодо поняття алгоритму та простих чисел.

Відношення подільності у множині цілих чисел $\mathbb{Z}$ будемо позначати як $b|a$:

$$\forall a, b \in \mathbb{Z} \,:\, b|a \Longleftrightarrow \exists c \in \mathbb{Z} \,:\, a = bc.$$

Дільник числа $a \in \mathbb{Z}$ — це таке число $b \in \mathbb{Z}$, що $b|a$. Для будь-якого числа 1 та саме число є його дільниками:

$$\forall a \in \mathbb{Z} \,:\, 1|a \ \wedge \ a|a.$$

Просте число — це більше за одиницю натуральне число, яке має рівно два різні натуральні дільники. Множину простих чисел зазвичай позначають через $\mathbb{P}$.

$\forall a \in \mathbb{Z} \,:\, a \in \mathbb{P} \Longleftrightarrow a \in \mathbb{N} \ \wedge \ 1 < a \ \wedge \ \nexists b \in \in \mathbb{N} \backslash \{1, a\} \,:\, b|a.$

Складене — це більше за одиницю натуральне число, яке не є простим.

Існує деяка неусталеність термінів «ймовірно просте число» та «псевдопросте число». В деяких текстах вони збігаються, а в деяких розділені. Раціонально припустити, що це залежить від проблематики, яка розглядається. В нашому випадку вважатимемо їх взаємозамінними і такими, що відповідають визначенню ймовірно простого числа нижче.

Ймовірно просте число — ціле число, яке задовільняє деяким властивостям простих чисел. Ймовірно просте число може бути простим або складеним числом. Раціонально розглядати ті властивості простих чисел, які не притаманні більшості складених чисел та для яких існують ефективні алгоритми.

Факторизація (натурального) числа — представлення числа у вигляді добутку простих чисел:

$$\forall n \in \mathbb{N} \,:\, n = \prod_{p \in \mathbb{P}} p^{\alpha_p}, \quad \forall p \in \mathbb{P} \,:\, \alpha_p \in \mathbb{N}_0.$$

Надзвичайно важливу роль відіграють такі теореми.

Теорема 1 (Мала теорема Ферма)**.** $\forall a, p \in \mathbb{N}$, $\gcd(a, p) = 1$,

$$p \in \mathbb{P} \Longrightarrow a^{p-1} \equiv 1 \ (\mod p),$$

або, в іншій формі,

$$\forall a \in \mathbb{N} : \forall p \in \mathbb{P} : a^p \equiv a \pmod{p}.$$

Доведення. $\{ k \cdot a \pmod{p} \mid k \in \{1, \ldots, (p-1)\} \} = \{ k \mid k \in \{1, \ldots, (p-1)\} \}$

$$\prod_{k=1}^{p-1} (k \cdot a) \equiv \left[\prod_{k=1}^{p-1} (k \cdot a \mod p) \right] \pmod{p} \equiv \left[\prod_{k=1}^{p-1} k \right] \pmod{p} \equiv (p-1)! \pmod{p}$$

$$(p-1)!\, a^{p-1} \pmod{p} \equiv (p-1)! \pmod{p} \Longrightarrow a^{p-1} \pmod{p} \equiv 1 \pmod{p}$$

$$\begin{cases} (p-1)!\, a^{p-1} \pmod{p} \equiv (p-1)! \pmod{p} \\ p \nmid (p-1)! \end{cases} \Longrightarrow a^{p-1} \pmod{p} \equiv 1 \pmod{p}$$

У випадку іншої форми теореми маємо два випадки:

- $\gcd(a, p) = 1$:
  $\left(p \in \mathbb{P} \Longrightarrow a^{p-1} \equiv 1 \pmod{p}\right) \Longrightarrow (p \in \mathbb{P} \Longrightarrow a^p \equiv a \pmod{p})$
- $\gcd(a, p) > 1$:
  $\begin{cases} p \mid a \\ a \equiv p \cdot \dfrac{a}{p} \equiv 0 \pmod{p} \end{cases} :\Longrightarrow (p \in \mathbb{P} \Longrightarrow a^p \equiv a \pmod{p})$

Зауваження до Малої теореми Ферма:
$\neg \left(\forall a \in \mathbb{N}_{2 \le (\cdot)} : \forall n \in \mathbb{N}_{2 \nmid (\cdot)} : \gcd(a, n) = 1 : a^{n-1} \equiv 1 \pmod{n} \Longrightarrow n \in \mathbb{P}\right)$.
Доведення. Контрприклад: $4^{15-1} = 268435456 \equiv 1 \pmod{15}$. $2 \le 4,\ 2 \nmid 15,\ \gcd(2, 15) = 1$.

Наслідок з Малої теореми Ферма. $\forall a \in \mathbb{N}_{2 \le (\cdot)} : \forall n \in \mathbb{N}_{2 \nmid (\cdot)} : \gcd(a, n) = 1$:

$$a^{n-1} \not\equiv 1 \pmod{n} \Longrightarrow n \notin \mathbb{P}.$$

Теорема 2. *$\forall p \in \mathbb{P}$, $\forall a \in \mathbb{N}_{1 < (\cdot) < p}$, $\exists s \in \mathbb{N}_1$: $\exists d \in \mathbb{N}_{2 \nmid (\cdot)} : p - 1 = 2^s \cdot d$, $p \nmid a$:*

$$\left[\begin{array}{l} a^d \equiv 1 \pmod{p} \\ a^{d \cdot 2^k} \equiv -1 \pmod{p},\ 0 \le k < s \end{array} \right.$$

Доведення. Розкладемо вираз $a^{p-1} - 1$. Згідно з Малою теоремою Ферма (Теоремою 1) $p \in \mathbb{P} \Longrightarrow a^{p-1} \equiv 1 \pmod{p}$, тоді $a^{p-1} - 1 \equiv 0 \pmod{p} \Longrightarrow p \mid \left(a^{p-1} - 1\right)$ та, розкладаючи в добуток при $p - 1 = 2^s \cdot d$,

$$\begin{aligned} a^{p-1} - 1 &= a^{2^s d} - 1 \\ &= \left(a^{2^{s-1} d} - 1\right)\left(a^{2^{s-1} d} + 1\right) \\ &= \left(a^{2^{s-2} d} - 1\right)\left(a^{2^{s-2} d} + 1\right) \left(a^{2^{s-1} d} + 1\right) \\ &= \left(a^{2d} - 1\right)\left(a^{2d} + 1\right) \cdot \ldots \\ &\quad \cdot \left(a^{2^{s-2} d} + 1\right)\left(a^{2^{s-1} d} + 1\right) \\ &= \left(a^{d} - 1\right)\left(a^{d} + 1\right)\left(a^{2d} + 1\right) \cdot \ldots \\ &\quad \cdot \left(a^{2^{s-2} d} + 1\right)\left(a^{2^{s-1} d} + 1\right). \end{aligned}$$

Відповідно

$$\left[\begin{array}{l} \gcd\left(\left(a^d - 1\right), p\right) > 1 \\ \exists k \in \mathbb{N}_{1 \le (\cdot) < s} : \gcd\left(\left(a^{d \cdot 2^k} + 1\right), p\right) > 1 \end{array} \right.$$

або, в іншому записі,

$$\left[\begin{array}{l} a^d \equiv 1 \pmod{p} \\ a^{d \cdot 2^k} \equiv -1 \pmod{p},\ 0 \le k < s \end{array} \right. .$$

Тест простоти, або **перевірка числа на простоту** — алгоритм визначення, чи є число простим. Для визначення того, що натуральне число є складеним, достатньо знайти його будь-який простий дільник, який менший за задане число. Тому загалом факторизація є складнішою задачею, ніж тест простоти.

Мультиплікативна група кільця лишків за модулем n — множина класів рівності чисел за модулем n, які є взаємно простими до n та утворюють групу з операцією множення за модулем n. Також може бути визначена як група оборотних елементів кільця лишків за модулем n.

В цьому тексті будемо її позначати як $\mathbb{Z}_n^*$. Елементами $\mathbb{Z}_n^*$ є множини $\mathbb{Z}_{k \not\equiv (\cdot) \pmod{n}}$, де $k \in \{ k \in \mathbb{Z} \mid 0 < k < n : \gcd(k, n) = 1 \}$. Для однозначного представлення кожного елемента $\mathbb{Z}_n^*$ достатньо лише одного його числа. $\#\mathbb{Z}_n^* = \varphi(n)$. Тоді множина з $\varphi(n)$ елементів попарно нерівних між собою за модулем n та взаємно простих з n однозначно визначають $\mathbb{Z}_n^*$.

Теорема 3 (Китайська теорема про лишки)**.** *$\forall \{a_1, \ldots, a_k\} \in \mathbb{Z}^k$, $\forall \{n_1, \ldots, n_k\} \in \mathbb{N}^k$, $\forall i \ne j : \gcd(n_i, n_j) = 1$:*

$\forall x_1, x_2 \in \mathbb{Z}$:

$$\left(\forall i \in \{1, 2\} : \begin{cases} x_i \equiv a_1 \pmod{n_1} \\ \vdots \\ x_i \equiv a_k \pmod{n_k} \end{cases} \right. \Longrightarrow x_1 \equiv x_2 \left(\mod \prod_{i=1}^{k} n_i \right) \Bigg).$$

Теорема 4 (Про існування генеруючого елемента в $\mathbb{Z}_p^*$)**.** *$\forall p \in \mathbb{P}$: $\mathbb{Z}_p^*$ є циклічною групою.*

Алгоритми

У загальному випадку, алгоритм — це визначений порядок дій для досягнення деякого результату.

Рандомізований алгоритм — алгоритм, поведінка якого визначається не лише вхідними значеннями, а також значеннями, які надходять від генератора випадкових чисел [7].

У [8] подано дещо ширше визначення:

Рандомізований алгоритм — алгоритм, що приймає випадкові рішення під час свого виконання.

Використовують такі дві категорії рандомізованих алгоритмів:

1. Алгоритми типу Лас-Вегас — алгоритми, що дають завжди правильний результат, але час їх виконання є випадковою величиною.
2. Алгоритми типу Монте-Карло — алгоритми, виконання яких детерміновано, але результат є правильним лише з певною ймовірністю.

Рандомізовані алгоритми перевірки числа на простоту

Тест Ферма

На основі **зауваження** та **наслідку з Малої теореми Ферма** можемо дати таке визначення:

Псевдопросте число Ферма [Fermat pseudoprime] n **в базі** a — число, яке задовільняє властивості

$$\gcd(a,n)=1 \ \wedge \ a^{n-1}\equiv 1 \ (\mod n).$$

Розглянемо множину класів рівності чисел за модулем n:

$$\mathrm{Fe}[n]=\left\{ a\in\mathbb{Z}_n^* \,|\, a^{n-1}\equiv 1 \ (\mod n)\right\}.$$

Маємо:

$$n\in\mathbb{P}\Longrightarrow \#\mathrm{Fe}[n]=\#\mathbb{Z}_n^*=n-1,$$

в іншому випадку таку теорему

Теорема 5. $\forall n\in\mathbb{N}_2\backslash\mathbb{P}$:

$$\left[\begin{array}{l}\#Fe[n]=\#\mathbb{Z}_n^*,\\ \#Fe[n]\le\dfrac{1}{2}\cdot\#\mathbb{Z}_n^*.\end{array}\right.$$

Доведення.

$$\forall n\in\mathbb{N}:\ \left\{\begin{array}{l} a^{n-1}=1\Longrightarrow 1\in\mathrm{Fe}[n]\\ \forall a_1,a_2\in\mathrm{Fe}[n]:\left(\left\{\begin{array}{l}a_1^{n-1}\equiv 1 \ (\mod n)\\ a_2^{n-1}\equiv 1 \ (\mod n)\end{array}\right.\right.\\ \left.\Longrightarrow (a_1a_2)^{n-1}\equiv 1 \ (\mod n)\right)\\ \Longrightarrow (a_1a_2)\in\mathrm{Fe}[n]\\ \forall a\in\mathrm{Fe}[n]:\left(a^{n-1}\equiv 1 \ (\mod n)\right.\\ \left.\Longrightarrow \left(a^{-1}\right)^{n-1}\equiv 1 \ (\mod n)\right)\\ \Longrightarrow (a)^{-1}\in\mathrm{Fe}[n]\end{array}\right.$$

$\Longrightarrow \mathrm{Fe}[n]$ – (під)група.

А за теоремою Лагранжа у скінченній групі порядок кожної підгрупи ділить порядок групи. Звідки випливає твердження теореми.

Теорема 6. $\forall n\in\mathbb{N}_2 : n=\prod\limits_{i=1}^{k}p_i^{\alpha_i}, \qquad \forall i : p_i\in\in\mathbb{P}\wedge\alpha_i\in\mathbb{N}_1.$

$$\#Fe[n]=\prod_{i=1}^{k}\gcd(n-1,p_i-1).$$

Число Кармайкла — це таке складене число, що

$$\#\mathrm{Fe}[n]=\#\mathbb{Z}_n^*.$$

Теорема 7 (Теорема Кармайкла)**.** $\forall n\in\in\mathbb{N}_{odd}\backslash\mathbb{P}$:

$$\#Fe[n]=\#\mathbb{Z}_n^*\iff \left\{\begin{array}{l} n=\prod\limits_{i=1}^{k}p_i, k\ge 3\wedge\forall i : p_i\in\mathbb{P}\\ \wedge\forall i,j : i\ne j\Longrightarrow p_i\ne p_j.\\ \forall i : (p_i-1)\,|\,(n-1)\end{array}\right.$$

Доведення. $n:=\prod\limits_{i=1}^{k}p_i^{\alpha_i}, \qquad \forall i : p_i\in\mathbb{P}\wedge\alpha_i\in\in\mathbb{N}_1$. За теоремою про розклад мультиплікативної групи кільця лишків за модулем n:

$$\mathbb{Z}_n^*\backsimeq\mathbb{Z}_{p1_i^{\alpha_1}}^*\times\ldots\times\mathbb{Z}_{p_i^{\alpha_i}}^*\times\ldots\times\mathbb{Z}_{p_k^{\alpha_k}}^*.$$

$\forall a\in\mathbb{Z}_n^* : a^{n-1}\equiv 1 \ (\mod n)\Longrightarrow\forall i : 1\le\le i\le k : \forall a\in\mathbb{Z}_{p_i^{\alpha_i}}^* : a^{n-1}\equiv 1 \ (\mod p_i^{\alpha_i})$.

$\forall i : 1\le i\le k : \exists a_i\in\mathbb{Z}_{p_i^{\alpha_i}}^* :$ $\mathrm{ord}(a_i)=\#\mathbb{Z}_{p_i^{\alpha_i}}^*=\varphi(p_i^{\alpha_i})=(p_i-1)\,p_i^{\alpha_i-1}\Longrightarrow$ $(p_i-1)\,p_i^{\alpha_i-1}|\,(n-1)$.

$$\left\{\begin{array}{l}\forall i : (p_i-1)\,p_i^{\alpha_i-1}|\,(n-1)\\ n=\prod\limits_{i=1}^{k}p_i^{\alpha_i}\end{array}\right.\Longrightarrow \forall i : \left\{\begin{array}{l}0=\alpha_i-1\\ (p_i-1)\,|\,(n-1)\end{array}\right..$$

В результаті вищевикладеного маємо:

$$\left\{\begin{array}{l} n=\prod\limits_{i=1}^{k}p_i, \qquad i\ne j\Longrightarrow p_i\ne p_j,\\ \forall i : (p_i-1)\,|\,(n-1).\end{array}\right.$$

$$\Longleftrightarrow\forall a\in\mathbb{Z}_n^* : a^{n-1}\equiv 1 \ (\mod n).$$

Доведемо, що дійсно $k\ge 3$.

Нехай $k=2$:

$$\left\{\begin{array}{l} n:=p_1\cdot p_2, \qquad p_1\ne p_2,\\ n-1=p_1\cdot(p_2-1)+(p_1-1),\\ \forall i : (p_i-1)\,|\,(n-1).\end{array}\right.\Longrightarrow$$

$$\left(\left\{\begin{array}{l}(p_2-1)\,|\,(p_1-1)\\ (p_1-1)\,|\,(p_2-1)\end{array}\right.\Longrightarrow p_1=p_2\right).$$

Маємо суперечність.

Наслідок з теореми Кармайкла. $\#\text{Carmichael} = \#\mathbb{N}$.

У 1912 р. американський математик Роберт Кармайкл висунув гіпотезу, що чисел, названих його ім'ям, є нескінченно багато. У 1994 р. гіпотеза була доведена В. Альфордом, Г. Гранвілем та К. Померансом.

Користуючись асимптотичним наближенням функції розподілу простих чисел $\pi(n) \sim \frac{n}{\log n}$ та верхньою межею оцінки кількості чисел Кармайкла

$$\#\text{Carmichael}_{(\cdot)\leq n} = n \cdot \exp\left(-k \cdot \frac{(\log n)\log(\log(\log n))}{\log(\log n)}\right), k \in \mathbb{R}_{0<(\cdot)},$$

маємо

$$\lim_{n\to\infty} \frac{\#\text{Carmichael}_{(\cdot)\leq n}}{\pi(n)} = \lim_{n\to\infty} \frac{n \cdot \exp\left(-k \cdot \frac{(\log n)\log(\log(\log n))}{\log(\log n)}\right)}{\frac{n}{\log n}} = \lim_{n\to\infty} \log n \cdot (\log n)^{\left(-k \cdot \frac{(\log n)\log(\log(\log n))}{\log^2(\log n)}\right)} = 0$$

$$\lim_{n\to\infty} \frac{\#\text{Carmichael}_{(\cdot)\leq n}}{\#(\mathbb{N}\backslash\mathbb{P})} = \lim_{n\to\infty} \frac{\#\text{Carmichael}_{(\cdot)\leq n}}{n - \pi(n)} = 0.$$

Тоді при достатньо великих числах можна вважати

$$\forall n \in (\mathbb{N}\backslash\mathbb{P}) : \Pr(n \in \text{Carmichael}) \approx 0 \wedge \Pr(n \in (\mathbb{N}\backslash(\text{Carmichael} \cup \mathbb{P}))) \approx 1.$$

З попереднього випливає

$$n \in (\mathbb{N}\backslash\mathbb{P}) : \Pr(\#\text{Fe}[n] = \#\mathbb{Z}_n^*) \to 0 \wedge \Pr\left(\#\text{Fe}[n] \leq \frac{1}{2} \cdot \#\mathbb{Z}_n^*\right) \to 1, \qquad n \to \infty.$$

Тепер можемо запропонувати алгоритм тесту на простоту, що спирається на Малу теорему Ферма.

Algorithm 1: Randomized Fermat's Primality Test algorithm 1

```
Data: n ∈ N_odd
Result: n ∈ P with Pr > 1/2 or n ∉ P with Pr = 1
begin
    a ⟵ RandomChoice[{ a ∈ N_2 | gcd(a, n) = 1 }]
    if a^{n-1} ≡ 1 ( mod n) then
        return ( Pr[n ∈ P] > 1/2 )
    else
        return ( Pr[n ∉ P] = 1 )
    end
end
```

Тест Соловея–Штрассена

Символ Лежандра — функція $\left(\frac{(\cdot)}{(\cdot\cdot)}\right)_L : \mathbb{N} \times \mathbb{P} \to \{0, -1, +1\}$, яка визначається так:

$$\left(\frac{a}{p}\right)_L \mapsto \begin{cases} 0, & a \equiv 0 \pmod p; \\ 1, & \exists x \in \mathbb{N} : x^2 \equiv a \pmod p \\ & \wedge\ a \not\equiv 0 \pmod p; \\ -1, & \nexists x \in \mathbb{N} : x^2 \equiv a \pmod p. \end{cases}$$

Символ Якобі — функція $\left(\frac{(\cdot)}{(\cdot\cdot)}\right)_J : \mathbb{N} \times \times \mathbb{N}_{\text{odd}} \to \{0, -1, +1\}$, яка визначається так:

$$n := \prod_{i=1}^{k} p_i^{\alpha_i}, \qquad \forall i : p_i \in (\mathbb{P}\backslash\{2\}) \wedge \alpha_i \in \mathbb{N}_1$$

$$\left(\frac{a}{n}\right)_J \mapsto \begin{cases} 0, & \gcd(a,n) > 1; \\ \prod\limits_{i=1}^{k} \left(\left(\frac{a}{p_i}\right)_L\right)^{\alpha_i}, & \gcd(a,n) = 1. \end{cases}$$

Далі для простоти будемо використовувати одне позначення: $\left(\frac{(\cdot)}{(\cdot\cdot)}\right)$. Бо символ Якобі продовжує символ Лежандра на $\mathbb{N}_{\text{odd}}$.

Теорема 8. $\forall n \in \mathbb{N}_{odd} : n \in \mathbb{P}$

$$\iff \qquad \forall a \in \mathbb{Z}_n^* : a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n.$$

Доведення.

- $n \in \mathbb{P} \Longrightarrow \forall a \in \mathbb{Z}_n^* : a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n$. Імплікація випливає з критерію Ойлера: $\forall p \in \mathbb{P}\backslash\{2\} : a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.
- $n \in \mathbb{P} \Longleftarrow \forall a \in \mathbb{Z}_n^* : a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n$. Припустимо хибність зворотної імлікації:

  $$\exists n \in \mathbb{N}\backslash\mathbb{P} : \forall a \in \mathbb{Z}_n^* : a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n.$$

  Тоді $a^{n-1} \equiv \left(a^{\frac{n-1}{2}}\right)^2 \equiv \left(\frac{a}{n}\right)^2 \equiv 1 \pmod n$.
  Якщо $a^{n-1} \equiv 1 \pmod n \Longrightarrow n \in$ $\in$ Carmichael. $n := \prod\limits_{i=1}^{k} p_i$, $\exists b \in \mathbb{N} : \left(\frac{b}{p_1}\right) \equiv -1 \pmod n$.
  Згідно з **Китайською теоремою про лишки**:

$$\exists \alpha \in \mathbb{Z}_n^* : \left\{ \begin{array}{l} \alpha \equiv b \pmod{p_1}, \\ \forall i \in \{2, \ldots, k\} : \alpha \equiv 1 \pmod{p_i} \end{array} \right.$$
$$\Longrightarrow \left(\frac{\alpha}{n}\right) = \prod_{i=1}^{k} \left(\frac{\alpha}{p_i}\right) = \left(\frac{\alpha}{p_1}\right) = -1.$$
$$\left(\left\{ \begin{array}{l} \forall a \in \mathbb{Z}_n^* : a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}, \\ \exists \alpha \in \mathbb{Z}_n^* : \left(\frac{\alpha}{n}\right) = -1 \end{array} \right. \right.$$
$$\left. \Longrightarrow \alpha^{\frac{n-1}{2}} \equiv -1 \pmod{n} \right)$$
$$\Longrightarrow$$
$$\forall i \in \{2, \ldots, k\} : \alpha^{\frac{n-1}{2}} \equiv -1 \pmod{p_i}.$$

Отримали суперечність, бо $\forall i \in \{2, \ldots, k\} : \alpha \equiv 1 \pmod{p_i}$.

Псевдопросте число Ойлера n **у базі** a — число, яке задовільняє властивості

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

Розглянемо множину класів рівності чисел за модулем n:

$$\mathrm{Eu}[n] := \left\{ a \in \mathbb{Z}_n^* \,|\, a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n} \right\}.$$

Теорема 9. $\forall n \in \mathbb{N}_2 \backslash \mathbb{P}$

$$\#Eu[n] \leq \frac{1}{2} \cdot \#\mathbb{Z}_n^*.$$

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

$$\left\{ \begin{array}{l} \forall a \in \mathbb{Z}_n^* : a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n} \\ \forall b \in \mathbb{Z}_n^* : b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n} \\ \forall m \in \mathbb{N}_{\mathrm{odd}} : \forall \{x, y\} \subset \mathbb{Z} : \\ \left(\frac{x \cdot y}{m}\right) = \left(\frac{x}{m}\right) \cdot \left(\frac{y}{m}\right) \end{array} \right.$$
$$\Longrightarrow$$
$$(a \cdot b)^{\frac{n-1}{2}} \equiv (a)^{\frac{n-1}{2}} \cdot (b)^{\frac{n-1}{2}}$$
$$\equiv \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right) \equiv \left(\frac{a \cdot b}{n}\right) \pmod{n}.$$

Маємо: $\mathrm{Eu}[n]$ — підгрупа в $\mathbb{Z}_n^*$.
На основі теореми:

$$n \in \mathbb{N}_{\mathrm{odd}} \backslash \mathbb{P} :$$
$$\forall m \in \mathbb{N}_{\mathrm{odd}} : m \in \mathbb{P} \iff$$
$$\forall x \in \mathbb{Z}_m^* : x^{\frac{m-1}{2}} \equiv \left(\frac{x}{m}\right) \pmod{m} \Longrightarrow$$
$$\exists c \in \mathbb{Z}_n^* : c^{\frac{n-1}{2}} \not\equiv \left(\frac{c}{n}\right) \pmod{n}.$$

Маємо: $\#\mathrm{Eu}[n] \neq \#\mathbb{Z}_n^*$.
А за теоремою Лагранжа у скінченній групі порядок кожної підгрупи ділить порядок групи. Звідки випливає твердження теореми.

Наведемо деякі властивості :

- $n \in (\mathbb{N}_{\mathrm{odd}} \backslash \mathbb{P}) : \forall a \in \mathbb{Z}_n^* \; \forall b \in \mathbb{Z}_n^* : \{a, b\} \subseteq \mathrm{Eu}[n] \Longrightarrow \{a \cdot b, \; a \cdot b^{-1}, \; a^{-1} \cdot b\} \subseteq \mathrm{Eu}[n]$
- $n \in (\mathbb{N}_{\mathrm{odd}} \backslash \mathbb{P}) : \forall a \in \mathbb{Z}_n^* : a \in \mathrm{Fe}[n] \Longrightarrow a \in \mathrm{Eu}[n]$
- $n \in (\mathbb{N}_{\mathrm{odd}} \backslash \mathbb{P}) : \mathrm{Eu}[n] \overset{\mathrm{group}}{\leq} \mathbb{Z}_n^*$

Тепер можемо запропонувати алгоритм тесту на простоту, що використовує поняття псевдопростого числа Ойлера та в літературі часто згадується як алгоритм Соловея–Штрассена. На відміну від тесту, що спирається на Малу теорему Ферма, цей алгоритм розпізнає числа Кармайкла.

Algorithm 2: Randomized Solovay–Strassen Primality Test algorithm 1

```
Data: n ∈ N_odd
Result: n ∈ P with Pr > 1/2 or n ∉ P with Pr = 1
begin
    a ⟵ RandomChoice[N_{2≤(·)<n}]
    if gcd(a, n) > 1 :
        return ( Pr[n ∉ P] = 1 )
    elif a^{(n-1)/2} ≡ (a/n) ( mod n) :
        return ( Pr[n ∈ P] > 1/2 )
    else:
        return ( Pr[n ∉ P] = 1 )
end
```

Тест Мілера–Рабіна

Цей тест за часом походження та широтою використання можна назвати класичним, його запропонував у 1980 році Міхаель Рабін у статті [2].

Строго псевдопросте число n у базі a, $1 < a < n-1$, $a \in \mathbb{N}$ — число $n > 3$, для якого

$$\gcd(a, n) = 1 \; \wedge \; \left(a^d \equiv 1 \pmod{n} \right.$$
$$\left. \vee \; a^{d \cdot 2^r} \equiv -1 \pmod{n} \right),$$

де $n - 1 = 2^s \cdot d$, $0 \leq r < s$.

Свідок простоти числа n — число $a \in \mathbb{N}$, $1 < a < n-1$, таке, що n є сильно псевдопростим числом у базі a.

Лжесвідок простоти числа n — число $a \in \mathbb{Z}_n^*$, таке, що

$$\left[\begin{array}{l} a^{n-1} \not\equiv 1 \pmod{n}; \\ \left[\begin{array}{l} \left(\forall k \in \mathbb{N} : a^k \not\equiv -1 \pmod{n}\right); \\ (\exists p \in \mathbb{P} : p | n : \forall k \in \mathbb{N}_{\leq p-2} : \\ a^k \not\equiv 1 \pmod{p} \; \wedge \; a^{p-1} \equiv 1 \pmod{p}) \end{array} \right. \end{array} \right.$$

Теорема Рабіна, яка є основою рандомізованого алгоритму, спирається на ряд таких тверджень.

Теорема 10. *Добуток свідка та лжесвідка простоти числа* $n \in \mathbb{N}_{>1}$ *не є свідком простоти того самого числа, тобто*

$$\forall w \in WP(n)\,,\ \forall f \in FWP(n)\ :$$

$$wf\ (\mod n) \notin WP(n)\,,$$

або, в іншій формі, $WP(n) \bigcap f \cdot WP(n) = \emptyset$.

Доведення. $\left[\begin{array}{l} f^{n-1} \not\equiv 1\ (\mod n)\,, \\ f^{n-1} \equiv 1\ (\mod n)\,. \end{array}\right.$

- $f^{n-1} \not\equiv 1\ (\mod n) \Longrightarrow (wf)^{n-1} \not\equiv w^{n-1}\ (\mod n)$. $w \in \mathrm{WP}(n) \overset{\text{def}}{\Longrightarrow} w^{n-1} \equiv 1\ (\mod n)$, тоді $(wf)^{n-1} \not\equiv 1\ (\mod n)$ та відповідно $wf\ (\mod n) \notin \mathrm{WP}(n)$.
- $\left\{\begin{array}{l} f^{n-1} \equiv 1\ (\mod n) \\ \forall k \in \mathbb{N} : a^k \not\equiv -1\ (\mod n) \\ \forall k \in \mathbb{N} : a^k \not\equiv -1\ (\mod n) \\ \wedge\ \exists p \in \mathbb{P} : p|n : a^{p-1} \equiv 1\ (\mod p) \end{array}\right.$
  $n - 1 = 2^s \cdot d : k \in \mathbb{N}_{\leq s-1} :$
  $\left\{\begin{array}{l} f^{2^k \cdot d} \equiv 1\ (\mod n) \\ \mathbb{P} \ni p|n \end{array}\right. \Longrightarrow f^{2^k \cdot d} \equiv 1\ (\mod p) \equiv f^{p-1} \equiv 1\ (\mod p)$
  $\left\{\begin{array}{l} f^{2^k \cdot d} \equiv 1\ (\mod p) \\ f^{p-1} \equiv 1\ (\mod p) \end{array}\right. \Longrightarrow (p-1) \,|\, \left(2^k \cdot d\right)$
  $\left\{\begin{array}{l} (p-1) \in \{\, k \in \mathbb{N} \,|\, 2|k \,\} \\ d \in \{\, k \in \mathbb{N} \,|\, \neg 2|k \,\} \\ (p-1) \,|\, \left(2^k \cdot d\right) \end{array}\right. \Longrightarrow k \geq 1$
  $f^d \equiv 1\ (\mod p) \Longrightarrow f^d \equiv 1\ (\mod n)$
  $\left\{\begin{array}{l} \gcd(w,n) = 1 \\ \mathbb{P} \ni p|n \end{array}\right. \Longrightarrow \gcd(w,p) = 1$
  $\forall q \in \mathbb{N}_{k \leq (\cdot) \leq s}\ :\ w^{2^q d} \equiv 1\ (\mod p) \Longrightarrow w^{2^q d} \equiv -1\ (\mod p)$
  $w \in \mathrm{WP}(n) \overset{\text{def}}{\Longrightarrow} w^{2^q d} \equiv 1\ (\mod n)$, тоді $w^{2^{k-1} d} \equiv \pm 1\ (\mod n)$
  $(wf)^{2^q d} \equiv 1\ (\mod p)$
  $(wf)^{2^q d} \equiv \pm f^{2^{k-1} d} \not\equiv \pm 1\ (\mod p)$
  та відповідно $wf\ (\mod n) \notin \mathrm{WP}(n)$.

Теорема 11. *Нехай* $p \in \mathbb{P}$, $n \in \mathbb{N}_{\neg 2|(\cdot)} \bigcap \mathbb{N}_{p^2|(\cdot)}$*:*

$$\mathcal{H} = \left\{ 1 + \frac{k \cdot n}{p} \,|\, k \in \mathbb{N}_{0 \leq (\cdot) \leq p-1} \right\}$$

$\mathcal{H} \subseteq \mathbb{Z}_m^*$, $\forall h \in \mathcal{H} \backslash \{1\} : \deg(h) = p$.

Доведення. $\forall h_1, h_2 \in \mathcal{H}\ :\ \exists k_1, k_2 \in \mathbb{N}_{0 \leq (\cdot) \leq p-1}\ :$

$$h_1 = 1 + \frac{k_1 \cdot n}{p}\ \wedge\ h_2 = 1 + \frac{k_2 \cdot n}{p}$$

$$\left(1 + \frac{k_1 \cdot n}{p}\right)\left(1 + \frac{k_2 \cdot n}{p}\right) =$$

$$1 + (k_1 + k_2)\frac{n}{p} + (k_1 k_2)\frac{n^2}{p^2} =$$

$$1 + (k_1 + k_2)\frac{n}{p} + (k_1 k_2)\left(\frac{n}{p^2}\right) \times n \equiv \ldots$$

$$\equiv 1 + (k_1 + k_2)\frac{n}{p}\ (\mod n)$$

$$\equiv 1 + (k_1 + k_2) \cdot \frac{n}{p} + \alpha \cdot n\ (\mod n) \equiv \ldots$$

$$\equiv 1 + (k_1 + k_2 + \alpha \cdot p) \cdot \frac{n}{p}\ (\mod n)$$

$$\equiv 1 + (k_1 + k_2\ (\mod p)) \cdot \frac{n}{p}\ (\mod n)\,,$$

де $\alpha \in \mathbb{Z}$ виконала лише технічну роль у доведенні.

Теорема 12. *Нехай* $a, b \subseteq \mathbb{Z}_n^*$, $a \neq b$, *тоді*

$$a\,WP(n) \bigcap b\,WP(n) = \emptyset$$

$$\Longleftrightarrow ab^{-1}\,WP(n) \bigcap WP(n) = \emptyset.$$

Доведення. Тут всі операції і перетворення в групі $\mathbb{Z}_n^*$.

$x \in a\mathrm{WP}(n) \bigcap b\mathrm{WP}(n)$
$\Longleftrightarrow \exists w_a, w_b \in \mathrm{WP}(n)\ :\ x = a \cdot w_a = b \cdot w_b,$
$\Longleftrightarrow \exists w_a, w_b \in \mathrm{WP}(n)\ :\ xb^{-1} = ab^{-1} \cdot w_a = w_b$
$\Longleftrightarrow xb^{-1} \in ab^{-1}\mathrm{WP}(n) \bigcap \mathrm{WP}(n)$

Очевидно, $\nexists x\ :\ x \in a\mathrm{WP}(n) \bigcap b\mathrm{WP}(n) \Longleftrightarrow \nexists y\ :\ y \in ab^{-1}\mathrm{WP}(n) \bigcap \mathrm{WP}(n)$.

Теорема 13. *Нехай* $n \in \mathbb{N}$, $p \in \mathbb{P}\ :\ n|p^2$, *тоді*

$$\#\,WP(n) \leq \frac{\varphi(n)}{p}.$$

Доведення. Нехай: $\mathcal{H} = \left\{ 1 + \frac{k \cdot n}{p} \,|\, k \in \mathbb{N}_{0 \leq (\cdot) \leq p-1} \right\}$, $p \in \mathbb{P}$, $n \in \mathbb{N}_{\neg 2|(\cdot)} \bigcap \mathbb{N}_{p^2|(\cdot)}$, $\mathcal{H} \subseteq \mathbb{Z}_m^*$, $\forall h \in \in \mathcal{H} \backslash \{1\} : \deg(h) = p$.

$p|n \Longrightarrow p \nmid (n-1)$

$\forall h \in \mathcal{H} \backslash \{1\}\ :\ h^{n-1} \not\equiv 1\ (\mod n) \Longrightarrow h \in \in \mathrm{FWP}(n)$.

Згідно з лемою, яка стверджує, що $\mathrm{WP}(n) \bigcap f \cdot \mathrm{WP}(n) = \emptyset$:

$$\forall h_1, h_2 \in \mathcal{H}\ :\ h_1 \neq h_2\ :$$

$$h_1 h_2^{-1}\mathrm{WP}(n) \bigcap \mathrm{WP}(n) = \emptyset$$

$$\Longrightarrow h_1\mathrm{WP}(n) \bigcap h_2^{-1}\mathrm{WP}(n) = \emptyset.$$

$\forall h \in \mathcal{H}\ :\ h\mathrm{WP}(n) \in \mathbb{Z}_n^*\ :$

$$\left\{\begin{array}{l} \#\bigcup\limits_{h \in \mathcal{H}} h\mathrm{WP}(n) \leq \#\mathbb{Z}_n^* = \varphi(n) \\ h_1\mathrm{WP}(n) \bigcap h_2^{-1}\mathrm{WP}(n) = \emptyset \end{array}\right.$$

$$\Longrightarrow \#\bigcup_{h \in \mathcal{H}} h\mathrm{WP}(n) = p \cdot \#\mathrm{WP}(n) \leq \varphi(n)$$

Отримали те, що необхідно було довести: $\#\mathrm{WP}(n) \leq \dfrac{\varphi(n)}{p}$.

$\forall x \in \mathbb{Z}_n^* : x\mathrm{WP}(n) = \{(x \cdot w) \in \mathbb{Z}_n^* \mid \exists w \in \mathrm{WP}(n)\} \Longrightarrow \#x\mathrm{WP}(n) = \#\mathrm{WP}(n)$

Теорема 14. *$\forall n \in \mathbb{N}_{(9<(\cdot))\wedge(2\nmid(\cdot))}$, $n := \prod_{i=1}^{k} p_i$, $\forall i : p_i \in \mathbb{P}$, $\forall i < j : p_i > p_j$ (тобто n, вільне від квадратів):*

$$k > 1 \Longrightarrow \#WP(n) \leq \frac{\varphi(n)}{4}.$$

($k = 1 \Longrightarrow \#WP(n) = \varphi(n)$.)

Доведення. Згідно з **Китайською теоремою про лишки** та **теоремою про існування генеруючого елемента в $\mathbb{Z}_p^*$** існують $a_1, a_2 \in \mathbb{Z}_n^*$:

$\forall i \in \{1,\dots,n\} \setminus \{2\} : a_1 \equiv 1 \pmod{p_i} \vee \mathrm{ord}\left[\mathbb{Z}_{p_1}^*\right](a_1) = p_1 - 1,$

$\forall i \in \{1,\dots,n\} \setminus \{1\} : a_2 \equiv 1 \pmod{p_i} \vee \mathrm{ord}\left[\mathbb{Z}_{p_2}^*\right](a_2) = p_2 - 1.$

Далі, $\forall i \in \{1,2\}$:

$$\begin{aligned} & a_i \equiv 1 \pmod{\frac{n}{p_i}} \\ & \Longrightarrow \forall j \in \mathbb{N} : (a_i)^j \equiv 1 \pmod{\frac{n}{p_i}}, \\ & \Longrightarrow \forall j \in \mathbb{N} : (a_i)^j \not\equiv -1 \pmod{n}. \end{aligned}$$

Тоді $\{a_1, a_2\} \subseteq \mathrm{FWP}(n)$.

- $k = 2$: $\exists j \in \mathbb{N} : \Longrightarrow$

$$\begin{aligned} & (a_1 a_2)^j \equiv 1 \pmod{n} \\ & \Longrightarrow (a_1 a_2)^j \equiv 1 \pmod{p_1}, \\ & \Longrightarrow (a_1 a_2)^j \equiv 1 \pmod{p_1}, \\ & \Longrightarrow (p_1 - 1) \mid j. \end{aligned}$$

$$\left\{ \begin{array}{l} n - 1 = p_2 p_1 - 1 = p_2(p_1 - 1) + p_2 - 1 \\ p_2 < p_1 \end{array} \right. \Longrightarrow n - 1 < p_1.$$

Маємо $(a_1 a_2)^{n-1} \not\equiv 1 \pmod{n}$ та відповідно $(a_1 a_2) \in \mathrm{FWP}(n)$.

- $k > 2$: $(a_1 a_2) \equiv 1 \pmod{\frac{n}{p_1 p_2}} \Longrightarrow \exists j \in \mathbb{N} : (a_1 a_2)^j \equiv 1 \pmod{\frac{n}{p_1 p_2}}$

$$\begin{aligned} & (a_1 a_2) \equiv 1 \pmod{\frac{n}{p_1 p_2}} \\ & \Longrightarrow \exists j \in \mathbb{N} : (a_1 a_2)^j \equiv 1 \pmod{\frac{n}{p_1 p_2}}, \\ & \Longrightarrow \exists j \in \mathbb{N} : (a_1 a_2)^j \not\equiv -1 \pmod{n}, \\ & \Longrightarrow (a_1 a_2) \in \mathrm{FWP}(n). \end{aligned}$$

Згідно з лемою: $\forall \{\alpha, \beta\} \{\alpha, \beta\} \subseteq \{\mathrm{WP}(n), a_1\mathrm{WP}(n), a_2\mathrm{WP}(n), (a_1 a_2)\mathrm{WP}(n)\}$:

$$\alpha \neq \beta \Longrightarrow \left\{ \begin{array}{l} \alpha \cap \beta = \emptyset, \\ \#\alpha = \#\beta, \\ \alpha \cup \beta \subseteq \mathbb{Z}_n^*. \end{array} \right.$$

Маємо,

$$\#\left(\mathrm{WP}(n) \cup a_1\mathrm{WP}(n) \cup a_2\mathrm{WP}(n) \cup (a_1 a_2)\mathrm{WP}(n)\right)$$

$$= 4 \cdot \#\mathrm{WP}(n) \leq \#\mathbb{Z}_n^* = \varphi(n) \Longrightarrow \#\mathrm{WP}(n) \leq \frac{\varphi(n)}{4}.$$

Для $\forall p \in \mathbb{P} : \#\mathrm{WP}(p) = \varphi(p) = p - 1$. Тоді для $\forall n \in \mathbb{N}_{(9<(\cdot))\wedge(2\nmid(\cdot))} : \#\mathrm{WP}(n) \leq \dfrac{\varphi(n)}{4} \leq \dfrac{n-1}{4}$.

Наслідок теореми Рабіна.

$$\forall n \in \mathbb{N}_{(9<(\cdot))\wedge(2\nmid(\cdot))}, \ \forall b \in \mathbb{N}_{(\cdot)<n} :$$

$$\left\{ \begin{array}{l} n \in \mathbb{P} : \Pr(b \in \mathrm{WP}(n)) = 1, \\ n \notin \mathbb{P} : \Pr(b \in \mathrm{WP}(n)) \leq \dfrac{\left(\frac{\varphi(n)}{4}\right)}{n-2} \\ \leq \dfrac{\left(\frac{n-2}{4}\right)}{n-2} = \dfrac{1}{4}. \end{array} \right.$$

Маємо , що $\Pr(n \in \mathbb{P} \wedge b \in \mathrm{WP}(n)) = 1 - \dfrac{1}{4} = \dfrac{3}{4}$.

Рандомізований алгоритм Рабіна перевірки числа на простоту полягає у випадковому виборі числа $1 < b < n$ і класифікації його як елемента однієї з множин $\mathrm{WP}(n)$ або $\mathrm{FWP}(n)$.

Algorithm 3: Miller-Rabin algorithm 1

```
Data: n ∈ ℕ: (9 < n) ∧ (2 ∤ n)
Result: n ∈ ℙ with Pr = 3/4 or n ∉ ℙ with Pr = 1
begin
    b ⟵ RandomInteger[2, n − 1]
    {(j, d)} ⟵ {(j, d) ∈ ℕ0 × ℕ1 | 2^j · d = n − 1 : 2 ∤ d}
    i ⟵ 0
    y ⟵ b^d ( mod n)
    if (1 = y) :
        return ( Pr[n ∈ ℙ] = 3/4 )
    else:
        while TRUE do
            if (n − 1 = y) :
                return ( Pr[n ∈ ℙ] = 3/4 )
            else:
                i ⟵ 1 + i
                if (i < j) :
                    y ⟵ y^2 ( mod n)
                    if (1 = y) :
                        return ( Pr[n ∉ ℙ] = 1 )
                else:
                    return ( Pr[n ∉ ℙ] = 1 )
        end
end
```

Тест Люка

Числа Фібоначчі $F_n,\ n \in \mathbb{N}_0$ — це рекурентна послідовність:

$$F_0 = 0,\ F_1 = 1, \quad \forall n \in \mathbb{N}_2 \,:\, F_{n+2} = F_n + F_{n+1}.$$

$\{F_n\}_0^\infty =$
$\{0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,$
$21,\ 34,\ 55,\ 89,\ 144,\ \dots\}.$
Числа Люка $L_n,\ n \in \mathbb{N}_0$ -

$$L_0 = 2,\ L_1 = 1, \quad \forall n \in \mathbb{N}_2 \,:\, L_n = L_{n-1} + L_{n-2}.$$

$\{L_n\}_0^\infty = \{2,\ 1,\ 3,\ 4,\ 7,\ 11,\ 18,$
$29,\ 47,\ 76,\ 123,\ \dots\}.$
Зв'язок між числами Люка та Фібоначчі:

$$L_n = F_{n-1} + F_{n+1} = F_n + 2F_{n-1} = F_{n+2} - F_{n-2};$$
$$L_{m+n} = L_{m+1}F_n + L_m F_{n-1};$$
$$F_{2n} = L_n F_n;$$
$$F_n = \frac{L_{n-1} + L_{n+1}}{5}.$$

Розглянемо множину рекурентних послідовностей, що мають характеристичне рівняння вигляду

$$x^2 - ax + b = 0,$$

яке визначає рекурентну послідовність вигляду: $y_{n+2} = a \cdot y_{n+1} - b \cdot y_n$.

Дискримінант цього рівняння $D = a^2 - 4b$, а його корені позначимо через α та β:

$$\begin{cases} \alpha = \dfrac{a + \sqrt{D}}{2}; \\ \beta = \dfrac{a - \sqrt{D}}{2}. \end{cases} \Longrightarrow \begin{cases} \alpha + \beta = a; \\ \alpha - \beta = \sqrt{D}; \\ \alpha \cdot \beta = b. \end{cases} .$$

Визначимо дві послідовності

$$U_n(a,b) := \frac{\alpha^n - \beta^n}{\alpha - \beta} = \sum_{k=0}^{n-1} \alpha^k \beta^{n-k-1};$$
$$V_n(a,b) := \alpha^n + \beta^n;$$

$U_n(a,b)$ та $V_n(a,b)$ будуть рекурентними послідовностями вигляду $y_{n+2} = a \cdot y_{n+1} - b \cdot y_n$, а α та β — коренями характеристичного многочлена, якщо

$$\begin{cases} U_0(a,b) := 0 \\ U_1(a,b) := 1 \end{cases}; \qquad \begin{cases} V_0(a,b) := 2 \\ V_1(a,b) := a \end{cases}.$$

Тоді відповідно $\forall n \in \mathbb{N}_2 \,:\, U_k(a,b) := aU_{k-1}(a,b) - bU_{k-2}(a,b)$; $V_k(a,b) := aV_{k-1}(a,b) - bV_{k-2}(a,b)$.

Послідовності Люка — пара полідовностей $U(a,b) := \{U_k(a,b)\}_{k\in\mathbb{N}_0}$, $V(a,b) := \{V_k(a,b)\}_{k\in\mathbb{N}_0}$, які залежать від двох параметрів a та b. Окремими реалізаціями таких є наступні послідовності:

- числа Фібоначчі, $\{F_n\}_0^\infty = U(1,-1)$;
- числа Люка, $\{L_n\}_0^\infty = V(1,-1)$;
- числа Пелля, як $U(2,-1) = \left\{ \dfrac{\left(1+\sqrt{2}\right)^k - \left(1-\sqrt{2}\right)^k}{2\sqrt{2}} \right\}_{k\in\mathbb{N}_0}$
$= \{0,\ 1,\ 2,\ 5,\ 12,\ 29,\ 70,\ 169,$
$408,\ 985,\ 2378,\ \dots\}.$
- числа Пелля-Люка, як $V(2,-1) = \left\{ \left(1+\sqrt{2}\right)^k + \left(1-\sqrt{2}\right)^k \right\}_{k\in\mathbb{N}_0}$
$= \{2,\ 2,\ 6,\ 14,\ 34,\ 82,\ 198,\ 478,\ 1154,\ \dots\}.$
- числа Мерсена, як $U(3,2) = \left\{2^k - 1\right\}_{k\in\mathbb{N}_0}$
$= \{0,\ 1,\ 3,\ 7,\ 15,\ 31,\ 63,\ 127,\ 255,\ 511,\ \dots\}.$
- послідовність чисел $V(3,2) = \left\{2^k + 1\right\}_{k\in\mathbb{N}_0}$
$= \{2,\ 3,\ 5,\ 9,\ 17,\ 33,\ 65,\ 129,\ 257,\ 513,\ \dots\}.$

Однією з найвідоміших робіт із послідовностей Люка з точки зору проблеми простих числе є [10].

Теорема 15 (Теорема Люка)**.** $\forall \{a,b\} \subset \mathbb{N} \,:\, D = a^2 - 4b \neq 0 \,:$

$$\forall p \in \mathbb{P}\backslash\{2\} \,:\, \begin{cases} p \nmid b \\ \left(\dfrac{D}{p}\right) = -1 \end{cases} \Longrightarrow p | U_{p+1}(a,b)\,.$$

Наслідок з теореми 15. $\forall n \in \mathbb{N}_{\text{odd}} \,:$

$$\begin{cases} n \nmid b \\ \left(\dfrac{D_{a,b}}{n}\right) = -1 \\ n \nmid U_{n+1}(a,b) \end{cases} \Longrightarrow n \in \mathbb{N}\backslash\mathbb{P}.$$

Псевдопросте число Люка n із параметрами $(D_{a,b}, a, b)$ — число, яке задовільняє властивості

$$\begin{cases} n \nmid b, \\ \left(\dfrac{D_{a,b}}{n}\right) = -1, \\ n | U_{n+1}(a,b)\,. \end{cases} =: lprp_{a,\,b}(n)\,.$$

Визначимо множину псевдопростих чисел Люка:

$$\mathrm{Lu}_{a,b}[n] := \left\{\, n \in \mathbb{N} \,|\, lprp_{a,\,b}(n) \,\right\}.$$

Наступну теорему іноді називають «Малою теоремою Ферма» для послідовностей Люка.

Теорема 16. $\forall n \in \mathbb{N}_{odd} \,:\, \varepsilon(n) := \left(\dfrac{D_{a,b}}{n}\right)$, $\delta(n) := n - \varepsilon(n)$

$$\begin{cases} n \in \mathbb{P} \\ \gcd(n,b) = 1 \end{cases} \Longrightarrow U_{\delta(n)}(a,b) \equiv 0 \ (\mod n)\,.$$

Зауваження до Теореми 16. При виконанні умов цієї теореми та $\exists n \in \mathbb{N}_{\text{odd}} \backslash \mathbb{P} : U_{\delta(n)} \equiv 0 \pmod{n}$.

У статті [10] рекомендується уникати ситуації, коли $\left(\frac{D_{a,b}}{n}\right) = 1$, та обирати такі параметри, щоб $\left(\frac{D_{a,b}}{n}\right) = -1$. Що випливає з практики обчислень, яка дає підстави висувати гіпотезу про таке: щільність множини баз, за якими складені числа є псевдопростими, є більшою для випадків $\left(\frac{D}{n}\right) = 1$, ніж при $\left(\frac{D}{n}\right) = -1$.

Також у тій самій роботі рекомендуються такі два шляхи зробити це:

- Нехай D — перший елемент послідовності 5, -7, 9, -11, 13,... $5+2k\cdot(-1)^k$,... такий, що $\left(\frac{D}{n}\right) = -1$.

  Тоді покладемо: $a = 1$, $b = \frac{1-D}{4}$.
- Нехай D — перший елемент послідовності 5, 9, 13, 17, 21,... $5+4k$,... такий, що $\left(\frac{D}{n}\right) = -1$.

  Тоді покладемо:

$$a = \min\left\{ k \in \mathbb{N}_{\text{odd}} \,|\, k > \sqrt{D} \right\},$$

$$b = \frac{a^2 - D}{4}.$$

На основі викладеного можна запропонувати два тести. Треба мати на увазі, що

- у випадку $\left(\frac{D}{n}\right) = 0$ число n є складене;
- у випадку, якщо $\sqrt{n} \in \mathbb{N}$, то $\left(\frac{D}{n}\right) > -1$, тому при деяковому пороговому повторенні $\left(\frac{D}{n}\right) = 1$ для перших значень D із запропонованих вище послідовностей необхідно перевірити цю можливість, бо у разі її реалізації алгоритм може досить довго перебирати значення, допоки не настане ситуація $\left(\frac{D}{n}\right) = 0$.

Цей спосіб тестування чисел має надзвичайно важливе значення, однак як окремий алгоритм майже ніколи не використовується, а є складовою частиною комбінованих алгоритмів перевірки на простоту. Про це буде сказано далі.

Комбіновані тести

Цілком очевидно, що будь-які тести можна комбінувати один з одним, очікуючи отримати з певної точки зору кращі результати.

Найпоширенішими та найважливішими у цьому контексті є комбіновані тести з використанням послідовностей Люка. При невеликій алгоритмічній складності вони дають результати з надзвичайно високою ймовірністю, а до певних досить великих чисел дають точно правильний результат. Тому при обмеженнях на величину числа, яка в багатьох практичних випадках не є фактором, що обмежує застосування, можуть розглядатися як детерміновані в сенсі точності результату. Однак можуть зберігати пробабалістичний характер в сенсі часу виконання.

Найпростішим випадком і найочевиднішим буде поєднати тест Ферма з використанням послідовностей Люка типу A або B. Найпростішим випадком тут буде зафіксувати основу в тесті Ферма, тобто зробити його детермінованим, і покласти $a = 2$. Це дасть найкращі можливості з використання швидких алгоритмів піднесення числа в степінь за модулем. При цьому сам тест у цілому буде рандомізованим, бо частина його, де використовуються послідовності Люка, буде пробабалістичною.

Algorithm 4: Randomized Lucas Primality Test algorithm 1

Data: $n \in \mathbb{N}_{\text{odd}}$, maxIterations $\in \mathbb{N} \bigcup \{\infty\}$
Result: probably $n \in \mathbb{P}$ (Lucas pseudoprime) or $n \notin \mathbb{P}$ with $\Pr = 1$
begin
  if $(\sqrt{n} \in \mathbb{N}) \vee \left(2^{n-1} \equiv 1 \pmod{n}\right)$ **:**
    return ($\Pr[n \notin \mathbb{P}] = 1$)
  else:
    $k \longleftarrow 0$
    while *maxIterations* $> k$ **do**
      $D \longleftarrow 5 + 2k \cdot (-1)^k$
      if $\left(\frac{D_{a,b}}{n}\right) = -1$ **:**
        $a \longleftarrow 1$
        $b \longleftarrow \frac{1-D}{4}$
        if $\begin{cases} n \nmid b, \\ n | U_{n+1}(a,b). \end{cases}$ **:**
          return *probably* $n \in \mathbb{P}$ *(Lucas pseudoprime)*
        else:
          return ($\Pr[n \notin \mathbb{P}] = 1$)
        $k \longleftarrow k + 1$
      end
      return *encountered maxIterations threshold*
  end

Дуже важливим та цікавим прикладом є поєднання тестів Мілера–Рабіна та Люка. Існує така гіпотеза [3]:

Гіпотеза. $\forall n \in \mathbb{N}_{\text{odd}}$:

$$\begin{cases} \exists a \in \mathbb{N}_{1<(\cdot)<n-1} : \text{Strong pseudoprime}\,(n,a) \\ \exists\,\{a,b\} \in \mathbb{N} : \\ \text{Lucas pseudoprime of type A}\,(n) \\ \vee \text{Lucas pseudoprime of type B}\,(n) \end{cases}$$

$$\Longrightarrow n \in \mathbb{P}.$$

Доведення досі ніким не знайдено.

На практиці відомо, що жодне складене число, менше за 2^{64}, не пройде цей тест.

Список літератури

1. Pomerance Jr. Carl, Selfridge John L., Wagstaff Samuel S. The pseudoprimes to $25 \cdot 10^9$. *Mathematics of Computation.* 1980. Vol. 151. https://dx.doi.org/10.1090%2FS0025-5718- 1980-0572872-7
2. Rabin Michael O. Probabilistic algorithm for testing primality. *Journal of Number Theory.* 1980. Vol. 12. https://doi.org/10.1016%2F0022-314X%2880%2990084-0.
3. Song Y. Yan. Primality Testing and Integer Factorization in Public-Key Cryptography. Springer, 2009.
4. Calude Cristian S. Information and Randomness: An Algorithmic Perspective. Springer, 2002.
5. Prabhakar Raghavan Rajeev Motwani. Randomized Algorithms. Cambridge University Press, 1995.
6. Hromkovic Juraj. Design and Analysis of Randomized Algorithms. Springer, 2005.
7. Rivest Ronald L., Cormen Thomas H., Leiserson Charles E., Stein Clifford. Introduction to Algorithms. The MIT Press, 2009.
8. Upfal Eli, Mitzenmacher Michael. Probability and Computing: Randomization and Probabilistic Techniques in Algorithms and Data Analysis. Cambridge University Press, 2017.
9. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. МЦНМО, 2006.
10. Baillie Robert, Wagstaff Samuel. Lucas Pseudoprimes. Mathematics of Computation. 1980. Vol. 151. https://dx.doi.org/10.1090%2FS0025-5718-1980-0583518-6.

References

1. Jr. Carl Pomerance, John L. Selfridge and Samuel S. Wagstaff, "The pseudoprimes to $25 \cdot 10^9$", Mathematics of Computation. **151** (1980). https://dx.doi.org/10.1090%2FS0025-5718- 1980-0572872-7.
2. Michael O. Rabin, "Probabilistic algorithm for testing primality", Journal of Number Theory. **12** (1980). https://doi.org/10.1016%2F0022-314X%2880%2990084-0.
3. Song Y. Yan, *Primality Testing and Integer Factorization in Public-Key Cryptography* (Springer, 2009).
4. Cristian S. Calude, *Information and Randomness: An Algorithmic Perspective* (Springer, 2002).
5. Prabhakar Raghavan Rajeev Motwani, *Randomized Algorithms* (Cambridge University Press, 1995).
6. Juraj Hromkovic, *Design and Analysis of Randomized Algorithms* (Springer, 2005).
7. Ronald L. Rivest, Thomas H. Cormen, Charles E. Leiserson and Clifford Stein, *Introduction to Algorithms* (The MIT Press, 2009).
8. Eli Upfal and Michael Mitzenmacher, *Probability and Computing: Randomization and Probabilistic Techniques in Algorithms and Data Analysis* (Cambridge University Press, 2017).
9. О. Н. Василенко, *Теоретико-числовые алгоритмы в криптографии* (МЦНМО, 2006).
10. Robert Baillie and Samuel Wagstaff, "Lucas Pseudoprimes", Mathematics of Computation. 151 (1980). https://dx.doi.org/10.1090%2FS0025-5718-1980-0583518-6.

O. Kozachok

RANDOMIZED PRIMALITY TESTS

Randomization and probabilistic approach in the algorithms development occupy prominent place. Due to limited computing resources and complexity many tasks in some cases it's impossible to obtain accurate results or it's too costly, so the results may contain some uncertainty. There are also cases when the indeterminacy of the algorithm is its advantage, for example in cryptography problems, or a useful characteristic: in simulations of processes containing undefined parameters.

In this paper, we consider the basic concepts and statements concerning randomized algorithms for checking numbers for simplicity, we present the necessary theorems.

Keywords: algorithms, prime numbers, randomized algorithms, primality tests.

Матеріал надійшов 23.09.2020