

Testování prvočíslnosti

Fermatův test

Malá Fermatova věta: Nechť p je prvočíslo, $a \in \{1, 2, \dots, p-1\}$. Pak $a^p \bmod p = a$ nebo ekvivalentně $a^{p-1} \bmod p = 1$.

Algoritmus Fermatova testu

- testujeme, zda n je prvočíslo
- bereme libovolné $a < n$ a počítáme $a^{n-1} \bmod n$
- pokud nevyjde 1 $\Rightarrow n$ je složené
- pokud vyjde 1 \Rightarrow nic s jistotou nevíme

Carmichaelova čísla

Definice: Složená čísla n taková, že pro každé $a < n$ a $NSD(a, n) = 1$ platí $a^{n-1} \bmod n = 1$, nazýváme *Carmichaelova*.

- nejmenší $561 = 3 \times 11 \times 17$
- Chernik 1939: $(6k+1)(12k+1)(18k+1)$ je Carmichaelovo číslo, pokud je každý faktor prvočíslem
- Alford, Ganville, Pomerance 1994: existuje ∞ -mnoho Carmichaelových čísel
- Důsledek: Fermatův test nedostatečný k testování prvočíslnosti!

Solovayův-Strassenův test

Kvadratické reziduum

- **Definice:** Nechť p je liché prvočíslo. Pak $a \in \mathbb{N} \setminus p\mathbb{N}$ nazveme *kvadratické reziduum*, pokud $a = x^2 \bmod p$ pro nějaké $x \in \{1, 2, \dots, p-1\}$. V opačném případě nazveme a *kvadratické nereziduum*.
- např. $p = 7$, pak

$$\begin{aligned} 1 &= 1^2 \bmod 7 \quad (= 6^2 \bmod 7) \\ 2 &= 3^2 \bmod 7 \quad (= 4^2 \bmod 7) \\ 4 &= 2^2 \bmod 7 \quad (= 5^2 \bmod 7) \end{aligned}$$

Legendrův symbol

- **Definice:** Nechť p je liché prvočíslo a $a \in \mathbb{N}$. Pak definujeme

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{je-li } a \text{ násobkem } p, \\ 1 & \text{je-li } a \text{ kvadratické reziduum mod } p, \\ -1 & \text{je-li } a \text{ kvadratické nereziduum mod } p. \end{cases}$$

- **Eulerova věta:** Nechť p je liché prvočíslo a $a \in \mathbb{N}$. Pak $\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$.

Vlastnosti Legendrova symbolu

- $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$
(speciálně když b není násobek p , pak $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$)

- $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
- **Zákon kvadratické reciprocity:** Necht p, q jsou lichá prvočísla, pak $\left(\frac{q}{p}\right) = (-1)^{\frac{(q-1)(p-1)}{4}} \left(\frac{p}{q}\right)$.

Jacobiho symbol

- **Definice:** Necht $n > 1$ je liché přirozené číslo a jeho prvočíselný rozklad má tvar $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Pak definujeme

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \dots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

Vlastnosti Jacobiho symbolu

- $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$, speciálně $\left(\frac{a}{p}\right) = 0 \Leftrightarrow NSD(a, p) > 1$,
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$
(speciálně když b není násobek p , pak $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$)
- $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
- **Zákon kvadratické reciprocity:** Necht p, q jsou lichá přirozená čísla, pak $\left(\frac{q}{p}\right) = (-1)^{\frac{(q-1)(p-1)}{4}} \left(\frac{p}{q}\right)$.
- Jak spočítat Jacobiho symbol $\left(\frac{a}{p}\right)$ bez faktorizace p ?

Výpočet Jacobiho (Legendrova) symbolu $\left(\frac{a}{b}\right)$

- necht $a, b \in \mathbb{Z}$, b liché
- polož $(X, Y, Z) := (a, b, 1)$
- while $X \neq 0$ and $X \neq 1$ do (kontroluj v každém kroku)
 1. if $X < 0$, $(X, Y, Z) := (-X, Y, Z \cdot (-1)^{\frac{Y-1}{2}})$
 2. if $X \geq Y$, $(X, Y, Z) := (X \bmod Y, Y, Z)$
 3. if X sudé, $(X, Y, Z) := \left(\frac{X}{2}, Y, Z \cdot (-1)^{\frac{Y^2-1}{8}}\right)$
 4. if X liché, $(X, Y, Z) := (Y \bmod X, X, Z \cdot (-1)^{\frac{(X-1)(Y-1)}{4}})$
- výstup: $\left(\frac{a}{b}\right) = X \cdot Z$

Princip Solovayova-Strassenova testu

- n je liché prvočísló \Rightarrow pro každé $a < n$ platí $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \bmod n$
- n je složené číslo \Rightarrow existuje $a < n$, pro které $\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \bmod n$
(takových a je aspoň $1/2$, tj. $\frac{n-1}{2}$)

Algoritmus Solovayova-Strassenova testu

- testujeme, zda n je prvočísló
- bereme libovolná $a_1, a_2, \dots, a_r \in \{1, 2, \dots, n-1\}$

- kontrolujeme $NSD(a_i, n) = 1$
- spočteme $\left(\frac{a_i}{n}\right)$ a $a_i^{\frac{n-1}{2}} \pmod n$
- pro nějaké a_i neplatí $\left(\frac{a_i}{n}\right) = a_i^{\frac{n-1}{2}} \pmod n \Rightarrow n$ složené
- pro všechna a_i platí $\left(\frac{a_i}{n}\right) = a_i^{\frac{n-1}{2}} \pmod n \Rightarrow n$ prvočíslo s pravděpodobností $1 - \frac{1}{2^r}$

Rabinův-Millerův test

Princip Rabinova-Millerova testu

- n liché prvočíslo a $n - 1 = 2^k t$
- Malá Fermatova věta \Rightarrow pro každé $a < n$ platí

$$0 = (a^{n-1} - 1) \pmod n = (a^{2^k t} - 1) \pmod n$$

- n nutně dělí aspoň jednu ze závorek:

$$\begin{aligned} (a^{2^{k-1}t} - 1)(a^{2^{k-1}t} + 1) &= (a^{2^{k-2}t} - 1)(a^{2^{k-2}t} + 1)(a^{2^{k-1}t} + 1) = \\ &= \underline{\underline{(a^t - 1)(a^t + 1) \dots (a^{2^{k-2}t} + 1)(a^{2^{k-1}t} + 1)}} \end{aligned}$$

- n složené číslo, pak existuje $a < n$, pro které n nedělí žádnou ze závorek (takových a jsou aspoň $3/4$, tj. $\frac{3(n-1)}{4}$)

Algoritmus Rabinova-Millerova testu

- testujeme, zda n je prvočíslo
- rozložíme $n - 1 = 2^k t$
- bereme libovolná $a_1, a_2, \dots, a_r \in \{1, 2, \dots, n - 1\}$
- kontrolujeme $NSD(a_i, n) = 1$
- klademe $b_i = a_i^t$
- pokud pro některé b_i platí:
 - $b_i \pmod n \neq \pm 1$,
 - $b_i^{2^j} \pmod n \neq -1$ pro každé $j \in \{1, \dots, k - 1\}$, $\Rightarrow n$ je složené
- jinak je n prvočíslo s pravděpodobností $1 - \frac{1}{4^r}$