# Fermatův test prvočíselnosti

Malá Fermatova věta:

$$\underbrace{p \text{ je prvočíslo}}_{A} \Rightarrow \underbrace{(\forall a \in \{1,2,\dots,p-1\} : a^{p-1} \equiv 1 \pmod p)}_{B}$$

Věta obměněná:

$$\underbrace{\exists a \in \{1,2,\dots,p-1\} : a^{p-1} \not\equiv 1 \pmod p}_{B'} \Rightarrow \underbrace{p \text{ není prvočíslo}}_{A'}$$

Př. $p = 5$ je prvočíslo a platí:

$1 = 1^4 \equiv 1 \pmod 5$

$16 = 2^4 \equiv 1 \pmod 5$

$81 = 3^4 \equiv 1 \pmod 5$

$2^4 \cdot 2^4 = 4^4 \equiv 1 \pmod 5$

$n = 6$ a platí:

$1^5 \equiv 1 \pmod 6$

$2 \cdot 4 = 8 \cdot 4 = 2^5 \equiv 2 \pmod 6 \Rightarrow$ 6 není prvočíslo

$3 \cdot 3 = 27 \cdot 9 = 3^5 \equiv 3 \pmod 6 \Rightarrow$ 6 není prvočíslo

$2^5 \cdot 2^5 = 4^5 \equiv 4 \pmod 6 \Rightarrow$ 6 není prvočíslo

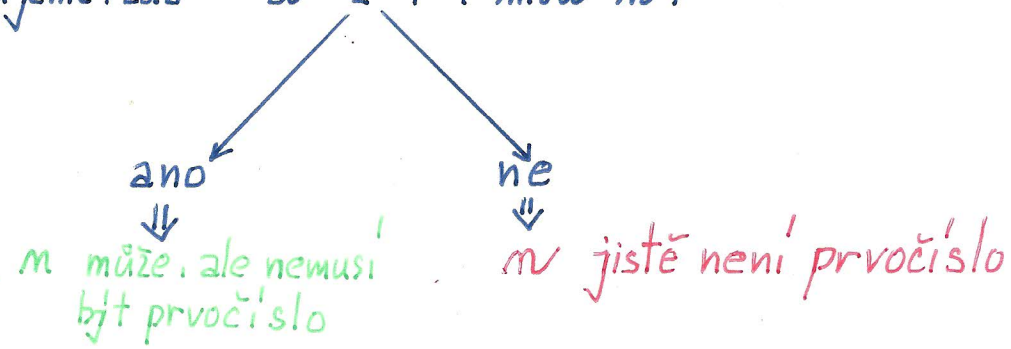
$25 \cdot 25 \cdot 5 = 5^5 \equiv 5 \pmod 6 \Rightarrow$ 6 není prvočíslo

Čísla 2, 3, 4, 5 jsou „svědky složenosti" čísla $n = 6$. $\Rightarrow$ Vidíme, že jsme měli šanci $\frac{4}{5}$ nalézt mezi čísly $a \in \{1,\dots,n-1\}$ svědka složenosti čísla $n = 6$.

## Fermatův test prvočíselnosti čísla $n$:

1.) Náhodně vybereme $a \in \{2, 3, \dots, n-1\}$

2.) Testujeme, zda $a^{n-1} \equiv 1 \pmod{n}$




**Poznámka:** Pokud bychom testovali všechna $a \in \{2, 3, \dots, n-1\}$ a všechna by splňovala $a^{n-1} \equiv 1 \pmod{n}$, znamenalo by to, že všechna $a \in \{2, 3, \dots, n-1\}$ jsou nesoudělná s $n \Rightarrow$ $n$ je jistě prvočíslo.

Pro „velká" $n$ je však časově náročné testovat všechna $a \in \{2, 3, \dots, n-1\}$.

**Př.:** Pomocí Fermatova testu prvočíselnosti otestujte, zda $n$ je prvočíslo. „Náhodně" vyberte čísla $a=8$, pak $a=13$, pak $a=3$

1.) $\boxed{n = 21}$

$a=8 \Rightarrow 8^{20} \equiv (8^2)^{10} \equiv (64)^{10} \equiv 1^{10} \equiv 1 \pmod{21} \Rightarrow$ 21 může být prvočíslo

$a=13 \Rightarrow 13^{20} \equiv (13^2)^{10} \equiv (169)^{10} \equiv 1^{10} \equiv 1 \pmod{21} \Rightarrow$ 21 může být prvočíslo

($169 = 8 \cdot 21 + 1$)

$a=3 \Rightarrow 3^{20} \equiv 9^{10} \equiv 81^5 \equiv (-3)^5 \equiv (-3) \cdot 81 \equiv 9 \pmod{21} \Rightarrow$ 21 není prvočíslo

($81 \equiv -3$, $81 \equiv -3$)

2.) $n = 17$

$a = 8 \Rightarrow 8^{16} \equiv 2^{48} \equiv (2^4)^{12} \equiv (-1)^{12} \equiv 1 \pmod{17} \Rightarrow$ 17 může být prvočíslo

$a = 13 \Rightarrow 13^{16} \equiv (13^2)^8 \equiv (169)^8 \equiv (-1)^8 \equiv 1 \pmod{17} \Rightarrow$ 17 může být prvočíslo

$a = 3 \Rightarrow 3^{16} \equiv 9^8 \equiv 81^4 \equiv 13^4 \equiv (-4)^4 \equiv 16^2 \equiv (-1)^2 \equiv 1 \pmod{17} \Rightarrow$ 17 může být prvočíslo

($81 = 4 \cdot 17 + 13$)

Př. Pomocí Fermatova testu prvočíselnosti otestujte, zda $n$ je prvočíslo. „Náhodně" vyberte $a = 7$, pak $a = 2$

a) $n = 25$

$a = 7 \Rightarrow 7^{24} \equiv (7^2)^{12} \equiv (-1)^{12} \equiv 1 \pmod{25} \Rightarrow$ 25 může být prvočíslo

$a = 2 \Rightarrow 2^{24} \equiv (2^5)^4 \cdot 2^4 \equiv (7)^4 \cdot 2^4 \equiv (49)^2 \cdot 2^4 \equiv 16 \pmod{25} \Rightarrow$ 25 není prvočíslo

b) $n = 112$

$a = 7$

$7^2 \equiv 49 \pmod{112}$

$7^3 \equiv 343 \equiv 7 \pmod{112}$

$7^4 \equiv 7 \cdot 7 \equiv 49 \pmod{112}$

$7^5 \equiv 7 \cdot 49 \equiv 7^3 \equiv 7 \pmod{112}$

$7^6 \equiv 7 \cdot 7 \equiv 49 \pmod{112}$

$\vdots$

$7^{2k-1} \equiv 7 \pmod{112}$

$7^{2k} \equiv 49 \pmod{112}$

$\Downarrow$

$7^{111} \equiv 7 \pmod{112}$

$\Downarrow$

112 není prvočíslo ($a = 2$ již není třeba testovat)

Př. Zjistěte, kolik svědků složenosti čísla $n = 15$ je mezi čísly $a \in \{1, 2, \dots, 14\}$

$1^{14} \equiv 1 \pmod{15}$ $\Rightarrow$ 1 není svědkem

$2^{14} \equiv 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^2 \equiv 1 \cdot 1 \cdot 1 \cdot 2^2 \equiv 4 \pmod{15}$

$3^{14} \equiv 3^3 \cdot 3^3 \cdot 3^3 \cdot 3^3 \cdot 3^2 \equiv (-3)(-3)(-3)(-3) \cdot 3^2 \equiv 3^3 \cdot 3^3 \equiv (-3)(-3) \equiv 9 \pmod{15}$

$4^{14} \equiv 2^{14} \cdot 2^{14} \equiv 4 \cdot 4 \equiv 1 \pmod{15}$ $\Rightarrow$ 4 není svědkem

$5^{14} \equiv (5^2)^7 \equiv 10^7 \equiv (-5)^7 \equiv (-5)(5^2)^3 \equiv 10^4 \equiv (-5)^4 \equiv (5^2)^2 \equiv 10^2 \equiv (-5)^2 \equiv 10 \pmod{15}$
($10 \equiv -5$, $10 \equiv -5$)

$6^{14} \equiv 2^{14} \cdot 3^{14} \equiv 4 \cdot 9 \equiv 6 \pmod{15}$

$7^{14} \equiv (7^2)^7 \equiv 4^7 \equiv 2^{14} \equiv 4 \pmod{15}$

$8^{14} \equiv (-7)^{14} \equiv 7^{14} \equiv 4 \pmod{15}$

$9^{14} \equiv (-6)^{14} \equiv 6^{14} \equiv 6 \pmod{15}$

$10^{14} \equiv (-5)^{14} \equiv 5^{14} \equiv 10 \pmod{15}$

$11^{14} \equiv (-4)^{14} \equiv 4^{14} \equiv 1 \pmod{15}$ $\Rightarrow$ 11 není svědkem

$12^{14} \equiv (-3)^{14} \equiv 3^{14} \equiv 9 \pmod{15}$

$13^{14} \equiv (-2)^{14} \equiv 2^{14} \equiv 4 \pmod{15}$

$14^{14} \equiv (-1)^{14} \equiv (1)^{14} \equiv 1 \pmod{15}$ $\Rightarrow$ 14 není svědkem

$\Rightarrow$ 10 ze 14 čísel $a \in \{1, 2, \dots, 14\}$ je svědkem složenosti čísla 15.

Všimněme si, že všechna čísla soudělná s $n = 15$ jsou svědky složenosti. Některá čísla nesoudělná s 15 jsou svědky (7, 8 a 13), jiná nejsou (1, 4, 11, 14).

Poznámka: Jestliže $\gcd(a, n) = d > 1$, nemůže platit $a^{n-1} \equiv 1 \pmod{n}$ (kongruence $ax \equiv 1 \pmod{n}$ nemá řešení!). $\Rightarrow$ $a$ je svědkem

Jestliže $\gcd(a, n) = 1$, může ale nemusí platit $a^{n-1} \equiv 1 \pmod{n}$ (kongruence $ax \equiv 1 \pmod{n}$ má řešení, ale nemusí platit $x = a^{n-2}$).

**Def** (Carmichaelovo číslo): Složené číslo $n \in \mathbb{N}$ nazýváme Carmichaelovým číslem právě tehdy, když

$$\forall a \in \{1, 2, \dots, n-1\},\ \gcd(a, n) = 1 \ :\ a^{n-1} \equiv 1 \pmod{n}$$

**Poznámka**: Čísla s $n$ soudělná jsou jistě svědky složenosti ($a^{n-1} \not\equiv 1 \pmod{n}$). Carmichaelovo číslo je tedy takové složené číslo, které má „minimální" počet svědků složenosti – jsou jimi pouze čísla s ním soudělná.

**Př.**: Nejmenším Carmichaelovým číslem je $n = 561 = 3 \cdot 11 \cdot 17$

a) Ověřte, že $a = 16$ ($\gcd(16, 561) = 1$) není svědkem složenosti čísla 561.

$16 \equiv 16 \pmod{561}$

$16^2 \equiv 256 \pmod{561}$

$16^3 \equiv 4096 \equiv 169 \pmod{561}$

$16^4 \equiv 16 \cdot 169 \equiv 2704 \equiv 460 \pmod{561}$

$16^5 \equiv 16 \cdot 460 \equiv 7360 \equiv 67 \pmod{561}$

$16^6 \equiv 16 \cdot 67 \equiv 1072 \equiv 511 \pmod{561}$

$16^7 \equiv 16 \cdot 511 \equiv 8176 \equiv 322 \pmod{561}$

$16^8 \equiv 16 \cdot 322 \equiv 5152 \equiv 103 \pmod{561}$

$16^9 \equiv 16 \cdot 103 \equiv 1648 \equiv 526 \pmod{561}$

$16^{10} \equiv 16 \cdot 526 \equiv 8416 \equiv 1 \pmod{561}$

$\Downarrow$

$16^{560} \equiv (16^{10})^{56} \equiv 1^{56} \equiv 1 \pmod{561} \Rightarrow$ 561 může být prvočíslo

b) Odhadněte, kolik procent z čísel $a \in \{1, 2, \dots, 560\}$ je svědkem složenosti čísla $n = 561$ při Fermatově testu.

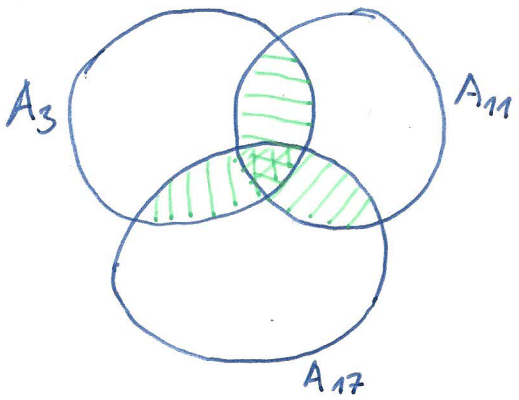
Označme $A_3 = \{3k \mid k \in \mathbb{Z},\ 1 \le 3k \le 560\}$

$A_{11} = \{11k \mid k \in \mathbb{Z},\ 1 \le 11k \le 560\}$

$A_{17} = \{17k \mid k \in \mathbb{Z},\ 1 \le 17k \le 560\}$

Protože $n = 561 = 3 \cdot 11 \cdot 17$, je Carmichaelovo číslo, jsou Fermatovými svědky složenosti čísla 561 pouze čísla soudělná s $561 = 3 \cdot 11 \cdot 17$ $\Rightarrow$ jsou to násobky čísla 3, 11, nebo 17 $\Rightarrow$ Chceme odhadnout:

$$\frac{|A_3 \cup A_{11} \cup A_{17}|}{560} = \frac{|A_3|}{560} + \frac{|A_{11}|}{560} + \frac{|A_{17}|}{560} - \left( \frac{|A_3 \cup A_{11}|}{560} + \frac{|A_3 \cup A_{17}|}{560} + \frac{|A_{11} \cup A_{17}|}{560} \right) + \frac{|A_3 \cup A_{11} \cup A_{17}|}{560}$$




$$\frac{|A_3 \cup A_{11} \cup A_{17}|}{560} \doteq \frac{1}{3} + \frac{1}{11} + \frac{1}{17} - \frac{1}{3 \cdot 11} - \frac{1}{3 \cdot 17} - \frac{1}{11 \cdot 17} + \frac{1}{3 \cdot 11 \cdot 17} =$$

$$= 1 - \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{17}\right) =$$

$$= 1 - \frac{2 \cdot 10 \cdot 16}{3 \cdot 11 \cdot 17} \doteq 1 - 0{,}57 = \underline{0{,}43}$$

$\Rightarrow$ Cca 43% čísel z $\{1, 2, \dots, 560\}$ je svědkem složenosti $n = 561$.

Pozn.: Jsnak $= \frac{n - 1 - \varphi(n)}{n - 1} \doteq \frac{n - \varphi(n)}{n} = 1 - \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$

**Př.:** Odhadněte, kolik procent čísel z množiny $\{1,2,\dots,n-1\}$ je svědkem složenosti Carmichaelova čísla $n = 252\,601 = 41 \cdot 61 \cdot 101$

Analogicky jako v předchozím příkladu:

$$\frac{|A_{41} \cup A_{61} \cup A_{101}|}{41 \cdot 61 \cdot 101} \doteq 1 - \underbrace{\left(1-\frac{1}{41}\right)}_{\to 1}\underbrace{\left(1-\frac{1}{61}\right)}_{\to 1}\underbrace{\left(1-\frac{1}{101}\right)}_{\to 1} = 1 - \underbrace{\frac{40 \cdot 60 \cdot 100}{41 \cdot 61 \cdot 101}}_{\to 1} \doteq \underbrace{1-0{,}95}_{\to 0} = 0{,}05$$

$\Rightarrow$ Cca 5% čísel z množiny $\{1,2,\dots,252\,600\}$ je svědkem složenosti čísla $n = 252\,601$.

**Poznámka:** Existence Carmichaelových čísel je zásadním nedostatkem Fermatova testu prvočíselnosti.

**Věta** (Korselt-ovo kritérium): Nechť $n$ je složené číslo. Pak $n$ je Carmichaelovo číslo, právě když platí podmínky:

1) $\forall p \in \mathbb{P}: p \mid n \;:\; p-1 \mid n-1$
2) $n$ je součinem navzájem různých prvočísel (squarefree)

$\Leftarrow$ Předpokládejme, že $n$ je složené a platí podmínky 1) a 2) $\Rightarrow$

$n = p_1 p_2 \cdots p_s$, kde $\forall j = 1,2,\dots,s: p_j - 1 \mid n-1$

Nechť $a \in \mathbb{Z}$, $\gcd(a,n) = 1 \Rightarrow \forall j = 1,2,\dots,s: p_j \nmid a \Rightarrow$

$a^{p_j - 1} \equiv 1 \pmod{p_j}$ (Malá Fermatova věta)

Protože $p_j - 1 \mid n-1$:

$a^{n-1} \equiv 1 \pmod{p_j}$ ($a^{n-1} = a^{(p_j-1)\cdot k} \equiv 1^k = 1$)

$\Rightarrow \forall j = 1,\dots,s: p_j \mid a^{n-1} - 1 \Rightarrow p_1 p_2 \cdots p_s = n \mid a^{n-1} - 1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$

**Věta:** Nechť $n \in \mathbb{N}$ a $p$ je liché prvočíslo takové, že $p^2 / n$. Potom počet přirozených čísel $a$, kde $1 \leq a \leq n-1$, které splňují kongruenci $a^{n-1} \equiv 1 \pmod n$ je nejvýše $\frac{1}{4}(n-1)$. Tj.:

$$\left| \{ a \in \mathbb{Z} \mid 1 \leq a \leq n,\ a^{n-1} \equiv 1 \pmod n \} \right| \leq \frac{1}{4}(n-1)$$

**Pozn.:** Tato věta říká, že při testování prvočíselnosti čísla $n$, které není „squarefree", máme více než 75% šanci mezi čísly $1, \dots, n-1$ náhodně vylosovat číslo $a$, které bude svědkem složenosti čísla $n$.

**Důkaz:** Nechť $n \in \mathbb{N}$ a $p \in \mathbb{P}$, $p^2 / n$, $p$ je liché.

Označme: $S = \{ a \in \{0, 1, \dots, n-1\} \mid a^{n-1} \equiv 1 \pmod n \}$

$\Rightarrow \forall a \in S:$ $a^{n-1} - 1 \equiv 0 \pmod n \Rightarrow$

$a^{n-1} - 1 = k \cdot n \quad / p^2 / n$

$a^{n-1} - 1 = k_0 \cdot p$

$a^{n-1} \equiv 1 \pmod p \Rightarrow a \not\equiv 0 \pmod p$

$\Rightarrow \forall a \in S:$ $a$ patří do některé ze zbytkových tříd $\bar{1}, \bar{2}, \dots, \overline{p-1}$ modulo $p$.

Označme: $S_b = \{ a \in S \mid a \equiv b \pmod p \}$

(všechny prvky z $S_b$ jsou čísla z $S$ kongruentní s $b \bmod p \Rightarrow$ jsou všechny navzájem kongruentní modulo $p$)

Tvrzení: $|S_b| \leq \frac{n}{p^2}$ (počet prvků $S_b$ je nejvýše $\frac{n}{p^2}$)

**Důkaz:** $\forall a_1, a_2 \in S_b:$ $a_1^{n-1} \equiv 1 \pmod n$, $a_2^{n-1} \equiv 1 \pmod n$, $p^2 / n$ a také $a_1 \equiv a_2 \pmod p$

$\Rightarrow$ Podle Lemma 2 platí: $a_1 \equiv a_2 \pmod{p^2}$

$\Rightarrow$ Všechny prvky z $S_b$ patří do stejné zbytkové třídy modulo $p^2$, označme ji $\bar{X}_{p^2}$

$n = k \cdot p^2 \Rightarrow k = \frac{n}{p^2}$

$0, 1, 2, \dots, \underbrace{qp^2+x}_{\in \bar{X}_{p^2}}, \dots, p^2 \mid p^2+1, p^2+2, \dots, \underbrace{p^2+x}_{\in \bar{X}_{p^2}}, \dots \mid 2p^2, \dots, \underbrace{2p^2+x}_{\in \bar{X}_{p^2}}, \dots \mid \dots \mid (k-1)p^2, \dots, (k-1)p^2+x, \dots \mid kp^2 = n$

$\Rightarrow$ V intervalu $\langle 0, n)$ jsou pouze čísla $0p^2+x$, $1p^2+x$, $\dots$, $(k-1)p^2+x$ ze zbytkové třídy $\bar{X}_{p^2}$ (je jich $k$)

$\Rightarrow$ Nejvýš se $k = \frac{n}{p^2}$ čísel z množiny $S$ je z množiny $S_a \subseteq S$ $\Rightarrow$

$$|S_a| \leq \frac{n}{p^2}$$

$\Rightarrow$ $S_a = \{ a \in S \mid a \equiv b \pmod p \}$ $\Rightarrow$ třídění na množiny

Víme, že $a \not\equiv 0 \pmod p \Rightarrow b \in \{1, 2, \dots, p-1\}$, navíc $S = \bigcup_{a=1}^{p-1} S_a$, $S_{b_1} \cap S_{b_2} = \emptyset$ pro $b_1 \neq b_2$

$$\Rightarrow |S| = \sum_{b=1}^{p-1} |S_b| \leq (p-1)\frac{n}{p^2}$$

$\frac{p-1}{p^2}$ jaké nalézá největší hodnoty pro liché prvočíslo $p$:

$$f(x) = \frac{x-1}{x^2} \Rightarrow f'(x) = \frac{x^2-(x-1)2x}{x^4} = \frac{-x^2+2x}{x^4} = \frac{x(2-x)}{x^4}$$


$\Rightarrow$ na $\langle 2, \infty)$ je $f$ klesající $\Rightarrow$ pro $n = 3$ dostaneme největší hodnotu

$$f(3) = \frac{3-1}{3^2} = \frac{2}{9}$$

$$\Rightarrow |S| \leq \frac{2}{9} n$$

nejmenší $n$ dělitelné druhou mocninou lichého prvočísla je $n = 9$

$\Rightarrow$

$$9 \leq n$$
$$\frac{9}{8} \leq \frac{1}{8} n$$
$$n + \frac{9}{8} \leq \frac{9}{8} n$$
$$n \leq \frac{9}{8} n - \frac{9}{8} \quad / \cdot \frac{2}{9}$$
$$\frac{2}{9} n \leq \frac{1}{4}(n-1)$$

$$\Rightarrow |S| \leq \frac{1}{4}(n-1)$$

□