

Věta: Necht' $a, b \in \mathbb{Z}$ a p je prvočíslo. Potom platí:

$$a \cdot b \equiv 0 \pmod{p} \Rightarrow (a \equiv 0 \pmod{p} \vee b \equiv 0 \pmod{p})$$

Důkaz: a) $a \equiv 0 \pmod{p} \Rightarrow$ věta platí.

b) $a \not\equiv 0 \pmod{p} \Rightarrow$

$$a \neq k \cdot p \Rightarrow \gcd(a, p) = 1$$

jestliže $a \cdot b \equiv 0 \pmod{p} \Rightarrow \exists k \in \mathbb{Z}:$

$$a \cdot b = k \cdot p$$

$$\underbrace{p \mid a \cdot b \quad \wedge \quad \gcd(a, p) = 1}_{\Downarrow}$$

$$p \mid b$$

$$\Downarrow$$
$$b = k_1 \cdot p$$

$$\Downarrow$$

$$b \equiv 0 \pmod{p}$$

Poznámka: Jinak řečeno, v $\mathbb{Z}_p$ neexistují netriviální dělitele nuly (pro $p \dots$ prvočíslo! v $\mathbb{Z}$ ano! např. $2 \cdot 3 = 6 = 0$)

Miller - Rabinův test prvočíslnosti

Poznámka: Z výše uvedeného plyne, že Fermatův test prvočíslnosti funguje dobře, pokud se snažíme prokázat složenost čísla n , které není "squarefree" (asymptotická hustota squarefree čísel je rovna $\frac{6}{\pi^2} \approx 0,6079$). U ostatních, zejména u Carmichaelových čísel Fermatův test narazí na problém - není příliš použitelný. Tyto nedostatky odstraňuje jeho upravená verze, tzv. Miller-Rabinův test prvočíslnosti:

Číslo $561 = 3 \cdot 11 \cdot 17$ je Carmichaelovo číslo, $\text{gcd}(2, 561) = 1 \Rightarrow$ není Fermatův svědek prvočíslnosti čísla $n = 561$

Ale u Miller-Rabinova testu svědkem složenosti bude! Předpokládejme, že

$n = 561$ je prvočíslo $\Rightarrow$

$$2^{560} \equiv 1 \pmod{561}$$

$$2^{560} - 1 \equiv 0 \pmod{561}$$

$$(2^{280} + 1)(2^{280} - 1) \equiv 0 \pmod{561}$$

$$(2^{280} + 1)(2^{140} + 1)(2^{140} - 1) \equiv 0 \pmod{561}$$

$$(2^{280} + 1)(2^{140} + 1)(2^{70} + 1)(2^{70} - 1) \equiv 0 \pmod{561}$$

$$(2^{280} + 1)(2^{140} + 1)(2^{70} + 1)(2^{35} + 1)(2^{35} - 1) \equiv 0 \pmod{561}$$

podle předp.: $\underbrace{\text{násobek prvočísla } n = 561}$

$\Rightarrow$ alespoň jeden z činitelů je násobek prvočísla n



Musi platit alespoň jedna z kongruencí:

/ V $\mathbb{Z}_p$, kde p je prvočíslo
neexistují netriviální
dělitelé nuly $\Rightarrow$

$$2^{280} \equiv -1 \pmod{561}$$

$$2^{140} \equiv -1 \pmod{561}$$

$$2^{70} \equiv -1 \pmod{561}$$

$$2^{35} \equiv -1 \pmod{561}$$

$$2^{35} \equiv 1 \pmod{561}$$

(pokud je 561 prvočíslo)

Alé : $2^{280} \equiv 1 \pmod{561}$

$$2^{140} \equiv 67 \pmod{561}$$

$$2^{70} \equiv 166 \pmod{561}$$

$$2^{35} \equiv 263 \pmod{561}$$

} $\Rightarrow$ Nemí splněna ani jedna z výše uvedených kongruencí. Spor! $\Rightarrow$

$m=561$ není prvočíslo

$\Rightarrow$ Miller Rabinův test: Testujeme, zda n je prvočíslo. (n je liché)

1.) Náhodně zvolíme $a \in \mathbb{N}$, $1 < a < n$

2.) $n-1 = 2^k \cdot q$, kde $k, q \in \mathbb{N}$, q je liché. Zjišťujeme, zda jsou splněny kongruence:

$$a^{2^{k-1}q} \equiv -1 \pmod{n}$$

$$a^{2^{k-2}q} \equiv -1 \pmod{n}$$

$\vdots$

$$a^{2q} \equiv -1 \pmod{n}$$

$$a^q \equiv -1 \pmod{n}$$

$$a^q \equiv 1 \pmod{n}$$

3.)

Ani jedna neplatí

$\Downarrow$

n není prvočíslo

Alespoň jedna platí

$\Downarrow$

n může (ale nemusí) být prvočíslo

Př.: Otestujte, zda n je prvočíslo. Použijte Miller-Rabinův test. (Nemá smysl testovat sudá čísla - kromě 2 jsou složená!)

a) $n = 27$

Zvolme $a = 4$. Pokud $n = 27$ je prvočíslo $\Rightarrow$

$$4^{26} \equiv 1 \pmod{27}$$

$$4^{26} - 1 \equiv 0 \pmod{27}$$

$$(4^{13} - 1)(4^{13} + 1) \equiv 0 \pmod{27} \Rightarrow$$

$$4^{13} - 1 \equiv 0 \pmod{27} \quad , \quad \text{nebo} \quad 4^{13} + 1 \equiv 0 \pmod{27}$$

Platí: $4 \equiv 4 \pmod{27}$

$$4^2 \equiv 16 \pmod{27}$$

$$4^4 \equiv 16 \cdot 16 \equiv 32 \cdot 8 = 5 \cdot 8 = 13 \pmod{27}$$

$$4^8 \equiv 13 \cdot 13 \equiv (-14) \cdot (-14) = 14 \cdot 14 = 7 \cdot 28 \equiv 7 \pmod{27}$$

$$4^{13} \equiv 4^8 \cdot 4^4 \cdot 4 \equiv 7 \cdot 13 \cdot 4 = 28 \cdot 13 \equiv 13 \pmod{27}$$

$$\Rightarrow 4^{13} - 1 \equiv 12 \pmod{27} \quad \text{a} \quad 4^{13} + 1 \equiv 14 \pmod{27} \Rightarrow \text{spor!} \Rightarrow n = 27 \text{ není prvočíslo!}$$

b) $m = 33$

Zvolme $a = 6$. Pokud $m=33$ je prvočíslo, pak $6^{32} \equiv 1 \pmod{33} \Rightarrow$

$$(6^{16}+1)(6^8+1)(6^4+1)(6^2+1)(6+1)(6-1) \equiv 0 \pmod{33}$$

$$6 \equiv 6 \pmod{33}$$

$$6^2 \equiv 36 \equiv 3 \pmod{33}$$

$$6^4 \equiv 3^2 \equiv 9 \pmod{33}$$

$$6^8 \equiv 9^2 \equiv 81 \equiv 15 \pmod{33}$$

$$6^{16} \equiv 15^2 \equiv 225 \equiv 198 + 27 \equiv 27 \pmod{33}$$

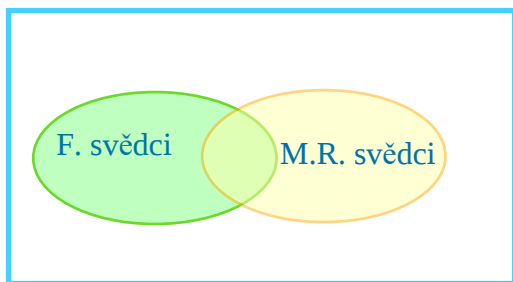
$$6^{32} \equiv 27^2 \equiv (-6)^2 \equiv 6^2 \equiv 3 \pmod{33}$$

$$\left. \begin{array}{l} 6^{16}+1 \equiv 28 \\ 6^8+1 \equiv 16 \\ 6^4+1 \equiv 10 \\ 6^2+1 \equiv 4 \\ 6+1 \equiv 7 \\ 6-1 \equiv 5 \end{array} \right\} \Rightarrow$$

$m=33$ není prvočíslo!

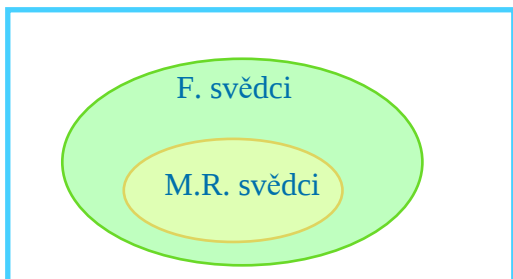
$\Rightarrow$ byl by to i Fermatův svědek složenosti!

$\Rightarrow$ Jaký je vztah mezi F. svědky a M.R. svědky?



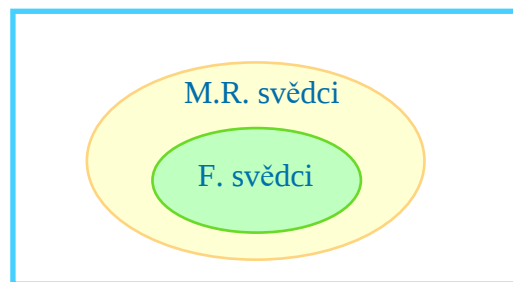
$$A = \{1, \dots, n-1\}$$

$\Rightarrow$ mělo by smysl provádět oba testy



$$A = \{1, \dots, n-1\}$$

$\Rightarrow$ mělo by smysl provádět jen Fermatův test



$$A = \{1, \dots, n-1\}$$

$\Rightarrow$ mělo by smysl provádět jen Miller Rabinův test

Lema: Necht' $a, m \in \mathbb{N}$, kde m je liché složené číslo. Jestliže a je Fermatův svědek složenosti čísla m , pak je také Miller-Rabinův svědek složenosti čísla m .

Důkaz: a je F.s.s. číslo $m \Rightarrow a^{m-1} \not\equiv 1 \pmod{m}$

$$a^{m-1} - 1 \not\equiv 0 \pmod{m} \quad / m-1 = 2^q \cdot q$$

$$(a^{2^{q-1}q} + 1)(a^{2^{q-2}q} + 1) \dots (a^{2q} + 1)(a^q + 1)(a^q - 1) \not\equiv 0 \pmod{m}$$

$\Rightarrow$ ani jedna z kongruencí ověřovaných v Miller-Rabinově testu nemůže platit.

Důsledek: Použitím Miller-Rabinova testu získáme nestatistické informace o složenosti m , kterou bychom získali při použití Fermatova testu.

Věta: Necht' $m \in \mathbb{N}$ je liché složené číslo. Počet Miller-Rabinových svědků složenosti čísla m je nejméně $\frac{3}{4}(m-1)$. (v intervalu $\langle 1, m \rangle$.)

Důsledek: Předpokládejme, že testujeme liché složené číslo m . Pravděpodobnost, že náhodně zvolené a je svědkem složenosti je alespoň $\frac{3}{4}$. Pravděpodobnost, že a není svědkem složenosti je nejvýše $\frac{1}{4}$. $\Rightarrow$

např.: Pravděpodobnost, že ani jedno ze 100 zvolených čísel a není svědkem složenosti čísla m je menší než $\left(\frac{1}{4}\right)^{100}$

Poznámka: Předpokládejme, že jsme pomocí Miller-Rabinova testu testovali náhodně vybrané ^{liché} číslo x z intervalu $\langle 1, n \rangle$ a ani jedno ze 100 náhodně vybraných čísel $a \in \langle 1, x-1 \rangle$ není svědkem složenosti čísla x . Odhadneme pravděpodobnost, že x je prvočíslo. (pro "velké" n).

Označme je vy : P... náhodně vybrané číslo $x \in \langle 1, n \rangle$ je prvočíslo. $\Rightarrow$

$$P(P) = \frac{\pi(n)}{n} \doteq \frac{\frac{n}{\ln n}}{n} = \frac{1}{\ln n}$$

LP... náhodně vybrané liché číslo $x \in \langle 1, n \rangle$ je prvočíslo. $\Rightarrow$

$$P(LP) \doteq \frac{\pi(n)}{\frac{n}{2}} \doteq \frac{2}{\ln n} \quad \Rightarrow$$

$$P(\overline{LP}) \doteq 1 - \frac{2}{\ln n}$$

M... ani jedno ze 100 náhodně vybraných čísel $a \in \langle 1, x-1 \rangle$ není svědkem složenosti čísla x . $\Rightarrow$

$$P(M|LP) = 1 \quad \wedge \quad P(M|\overline{LP}) \leq \left(\frac{1}{4}\right)^{100}$$

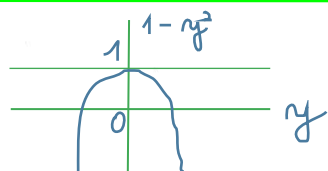
2 Bayesovy věty pak plyne:

$$P(LP|M) = \frac{P(M|LP) \cdot P(LP)}{P(M|LP) \cdot P(LP) + P(M|\overline{LP}) \cdot P(\overline{LP})} \geq \frac{1 \cdot \frac{2}{\ln n}}{1 \cdot \frac{2}{\ln n} + \left(\frac{1}{4}\right)^{100} \left(1 - \frac{2}{\ln n}\right)} \geq$$

$$\frac{1 \cdot \frac{2}{\ln n}}{1 \cdot \frac{2}{\ln n} + \left(\frac{1}{4}\right)^{100}} = \frac{1}{1 + \underbrace{\left(\frac{1}{4}\right)^{100} \frac{\ln n}{2}}_{\in \mathbb{R}^+}} \stackrel{*}{\geq} 1 - \left(\frac{1}{4}\right)^{\frac{100 \ln n}{2}} \quad \Rightarrow$$

$$\text{při } n=10^{20} : P(LP|M) \geq 1 - \left(\frac{1}{4}\right)^{\frac{100 \ln 10^{20}}{2}} = 1 - \left(\frac{1}{4}\right)^{\frac{100 \cdot 20 \ln 10}{2}} \stackrel{32=2^5}{\geq} 1 - 30 \left(\frac{1}{4}\right)^{100} \stackrel{200}{\geq} 1 - 2^5 \left(\frac{1}{2}\right)^{200} = 1 - \left(\frac{1}{2}\right)^{195} > 1 - \left(\frac{1}{10}\right)^{48}$$

* Uvažme, že $\forall y \in \mathbb{R}^+$: $1 \geq 1 - y^2 \Rightarrow 1 \geq (1-y)(1+y) \Rightarrow \frac{1}{1+y} \geq 1-y$



Poznámka: Jestliže platí obecněná Riemannova hypotéza (nemí dokázána, ale také se nedáří vyvrátit), pak má každé složené číslo n Miller-Rabinova svědka složenosti menšího než $2 \cdot (\log_2 n)^2$

⇒ stačilo by projít všechna přirozená

$$a \in \langle 1, 2 \cdot (\log n)^2 \rangle$$

pokud by žádné a z tohoto intervalu nebylo svědkem složenosti, znamenalo by to, že n je prvočíslo.

⇒ Byl by to deterministický test.

Pr. min: Otestujte, zda n je prvočíslo. Použijte Miller-Rabinův test. (Nemá smysl testovat sudá čísla - kromě 2 jsou složená!)

a) $n = 27$

Zvolme $a = 4$. Pokud $n = 27$ je prvočíslo $\Rightarrow$

$$4^{26} \equiv 1 \pmod{27}$$

$$4^{26} - 1 \equiv 0 \pmod{27}$$

$$(4^{13} - 1)(4^{13} + 1) \equiv 0 \pmod{27} \Rightarrow$$

$$4^{13} - 1 \equiv 0 \pmod{27} \quad \text{nebo} \quad 4^{13} + 1 \equiv 0 \pmod{27}$$

Platí: $4 \equiv 4 \pmod{27}$

$$4^2 \equiv 16 \pmod{27}$$

$$4^4 \equiv 16 \cdot 16 \equiv 32 \cdot 8 \equiv 5 \cdot 8 \equiv 13 \pmod{27}$$

$$4^8 \equiv 13 \cdot 13 \equiv (-14) \cdot (-14) \equiv 14 \cdot 14 \equiv 7 \cdot 28 \equiv 7 \pmod{27}$$

$$4^{13} \equiv 4^8 \cdot 4^4 \cdot 4 \equiv 7 \cdot 13 \cdot 4 \equiv 28 \cdot 13 \equiv 13 \pmod{27}$$

$$\Rightarrow 4^{13} - 1 \equiv 12 \pmod{27} \quad \text{a} \quad 4^{13} + 1 \equiv 14 \pmod{27} \Rightarrow \text{spor!} \Rightarrow n = 27 \text{ není prvočíslo!}$$

b) $n = 33$

Zvolme $a = 6$. Pokud $n = 33$ je prvočíslo, pak $6^{32} \equiv 1 \pmod{33} \Rightarrow$

$$(6^{16} + 1)(6^8 + 1)(6^4 + 1)(6^2 + 1)(6 + 1)(6 - 1) \equiv 0 \pmod{33}$$

$$6 \equiv 6 \pmod{33}$$

$$6^2 \equiv 36 \equiv 3 \pmod{33}$$

$$6^4 \equiv 3^2 \equiv 9 \pmod{33}$$

$$6^8 \equiv 9^2 \equiv 81 \equiv 15 \pmod{33}$$

$$6^{16} \equiv 15^2 \equiv 225 \equiv 198 + 27 \equiv 27 \pmod{33}$$

$$6^{32} \equiv 27^2 \equiv (-6)^2 \equiv 6^2 \equiv 3 \pmod{33}$$

$$6^{16} + 1 \equiv 28$$

$$6^8 + 1 \equiv 16$$

$$6^4 + 1 \equiv 10$$

$$6^2 + 1 \equiv 4$$

$$6 + 1 \equiv 7$$

$$6 - 1 \equiv 5$$

$n = 33$ není prvočíslo!

c) $n = 91$

Pokud je $n=91$ prvočíslo, pak $\forall a \in \{1, \dots, n-1\} : a^{90} \equiv 1 \pmod{91} \Rightarrow$

$$a^{90} - 1 = (a^{45} + 1)(a^{45} - 1) \equiv 0 \pmod{91}$$

Zvolme $a = 9$

$$9 \equiv 9 \pmod{91}$$

$$9^2 \equiv 81 \pmod{91}$$

$$9^4 \equiv 81^2 \equiv (-10)^2 \equiv 9 \pmod{91}$$

$$9^8 \equiv 81 \pmod{91}$$

$$9^{16} \equiv 9 \pmod{91}$$

$$9^{32} \equiv 81 \pmod{91}$$

$$\Rightarrow 9^{45} \equiv 9^{32} \cdot 9^8 \cdot 9^4 \cdot 9 \equiv$$

$$\equiv \underbrace{81 \cdot 81} \cdot 9 \cdot 9 \equiv$$

$$\equiv 9 \cdot 9 \cdot 9 \equiv$$

$$\equiv 81 \cdot 9 \equiv$$

$$\equiv (-10) \cdot 9 \equiv$$

$$\equiv -90 \equiv 1 \pmod{91}$$

$$\Rightarrow 9^{45} - 1 \equiv 0 \pmod{91} \Rightarrow$$

$\Rightarrow a=9$ není svědkem složenosti

Zvolme $a = 10$

$$10 \equiv 10 \pmod{91}$$

$$10^2 \equiv 9 \pmod{91}$$

$$10^4 \equiv 81 \equiv -10 \pmod{91}$$

$$10^8 \equiv 100 \equiv 9 \pmod{91}$$

$$10^{16} \equiv 81 \equiv -10 \pmod{91}$$

$$10^{32} \equiv 9 \pmod{91}$$

$$10^{45} \equiv 10^{32} \cdot 10^8 \cdot 10^4 \cdot 10 \equiv$$

$$\equiv \underbrace{9 \cdot 9} \cdot (-10) \cdot 10 \equiv$$

$$\equiv (-10) \cdot (-10) \cdot 10 \equiv$$

$$\equiv 100 \cdot 10 \equiv$$

$$\equiv 90 \cdot 10 \equiv -1$$

$$\Rightarrow 10^{45} + 1 \equiv 0 \pmod{91} \Rightarrow$$

$\Rightarrow a=10$ není svědkem složenosti

zvolme $a = 5$

$$5 \equiv 5 \pmod{91}$$

$$5^2 \equiv 25 \pmod{91}$$

$$5^4 \equiv 625 \equiv 625 - 7 \cdot 91 = 625 - 637 \equiv -12 \pmod{91}$$

$$5^8 \equiv (-12)^2 \equiv 144 \equiv 144 - 182 \equiv -38 \pmod{91}$$

$$5^{16} \equiv (-38)^2 \equiv 38 \cdot 38 \equiv 19 \cdot 76 \equiv 19 \cdot (-15) \equiv -3 \cdot 19 \cdot 5 \equiv 3 \cdot 95 \equiv 3 \cdot 4 \equiv 12 \pmod{91}$$

$$5^{32} \equiv 12 \cdot 12 \equiv 144 \equiv -38 \pmod{91}$$

$$5^{45} \equiv 5^{32} \cdot 5^8 \cdot 5^4 \cdot 5 \equiv \underbrace{(-38) \cdot (-38)}_{-12} \cdot \underbrace{(-12) \cdot 5}_{-38} \equiv (-38) \cdot 5 \equiv -2 \cdot 19 \cdot 5 \equiv -2 \cdot \underbrace{95}_4 \equiv -8$$

$$\Rightarrow 5^{45} + 1 \equiv -7 \pmod{91} \quad \text{a} \quad 5^{45} - 1 \equiv -9 \pmod{91}$$

$\Rightarrow 5$ je svědkem složenosti čísla $n = 91$