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

$a \cdot b = k \cdot p$

$p \mid a \cdot b \quad \wedge \gcd(a, p) = 1$

$\Downarrow$

$p \mid b$

$\Downarrow$

$b = k_1 \cdot p \quad (k_1 \in \mathbb{Z})$

$\Downarrow$

$b \equiv 0 \pmod{p}$

Poznámka: Jinak řečeno, v $\mathbb{Z}_p$ neexistují netriviální dělitelé nuly (pro p... prvočíslo! v $\mathbb{Z}_6$ ano! např. $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$)

Miller - Rabinův test prvočíselnosti

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

Číslo $561 = 3 \cdot 11 \cdot 17$ je Carmichaelovo číslo. $\gcd(2, 561) = 1$ => Není Fermatův svědek ~~prvočíselnosti~~ složenosti čísla $n = 561$

Ale u Miller-Rabinova testu svědkem složenosti bude! Předpokládejme, že $n = 561$ je prvočíslo =>

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

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

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

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

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

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

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

podle předp.: násobek prvočísla $n = 561$

=> alespoň jeden z činitelů je násobek prvočísla n

Musí platit alespoň jedna z kongruencí:

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

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

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

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

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

(pokud je 561 prvočíslo)

Ale: $2^{280} \equiv 1 \pmod{561}$

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

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

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

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

$n = 561$ 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 $\Rightarrow$ n Není prvočíslo.

Alespoň jedna platí $\Rightarrow$ 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 $\Rightarrow$

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

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

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

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

Platí:
$4 \equiv 4 \pmod{27}$
$4^2 \equiv 16 \pmod{27}$
$4^4 \equiv 16 \cdot 16 \equiv 32 \cdot 8 = 5 \cdot 8 = 13 \pmod{27}$
$4^8 \equiv 13 \cdot 13 \equiv (-14) \cdot (-14) = 14 \cdot 14 = 7 \cdot 28 \equiv 7 \pmod{27}$
$4^{13} \equiv 4^8 \cdot 4^4 \cdot 4 \equiv 7 \cdot 13 \cdot 4 = 28 \cdot 13 \equiv 13 \pmod{27}$

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

b) $n = 33$

Zvolme $a = 10$. Pokud $n = 33$ je prvočíslo, pak $10^{32} \equiv 1 \pmod{33} \Rightarrow$

$$10^{32} - 1 = (10^{16} + 1)(10^{16} - 1) = (10^{16} + 1)(10^8 + 1)(10^8 - 1) = (10^{16} + 1)(10^8 + 1)(10^4 + 1)(10^2 + 1)(10^2 - 1) \equiv 0 \pmod{33}$$

$10 \equiv 10 \pmod{33}$
$10^2 \equiv 100 \equiv 1 \pmod{33} \Rightarrow (10^2 - 1) \equiv 0 \pmod{33} \Rightarrow 10^{32} - 1 \equiv 0 \pmod{33} \Rightarrow$ 33 může být prvočíslo

b) $n = 33$

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

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

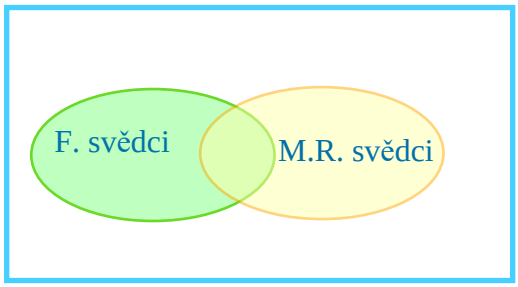
$6 \equiv 6 \pmod{33}$
$6^2 \equiv 36 \equiv 3 \pmod{33}$
$6^4 \equiv 3^2 \equiv 9 \pmod{33}$
$6^8 \equiv 9^2 \equiv 81 \equiv 15 \pmod{33}$
$6^{16} \equiv 15^2 = 225 = 198 + 27 \equiv 27 \pmod{33}$ ($198 = 6 \cdot 33$)
$6^{32} \equiv 27^2 \equiv (-6)^2 \equiv 6^2 \equiv 3 \pmod{33}$

$6^{16}+1 \equiv 28$
$6^8+1 \equiv 16$
$6^4+1 \equiv 10$
$6^2+1 \equiv 4$
$6+1 \equiv 7$
$6-1 \equiv 5$

=> $n = 33$ není prvočíslo!

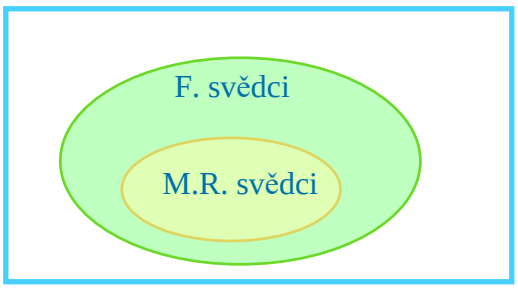
=> byl by to i Fermatův svědek složenosti!

=> Jaký je vztah mezi F. svědky a M.R. svědky?



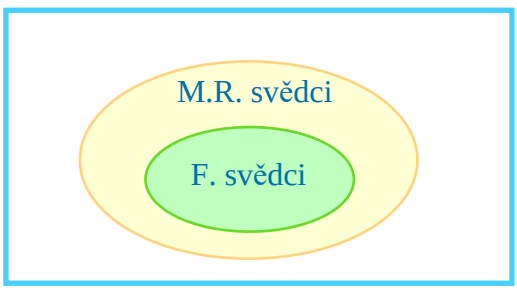
A = {1, ..., n-1}

=> mělo by smysl provádět oba testy



A = {1, ..., n-1}

=> mělo by smysl provádět jen Fermatův test



A = {1, ..., n-1}

=> mělo by smysl provádět jen Miller Rabinův test

Lemma: Nechť $a, n \in \mathbb{N}$, kde n je liché složené číslo. Jestliže a je Fermatův svědek složenosti čísla n, pak je také Miller-Rabinův svědek složenosti čísla n.

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

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

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

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

Důsledek: Použitím Miller-Rabinova testu získáme nesrovnatelně informaci o složenosti n, kterou by jsme obdrželi při použití Fermatova testu.

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

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

neboli: Pravděpodobnost, že ani jedno ze 100 zvolených čísel a není svědkem složenosti čísla n 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. Odhadněme pravděpodobnost, že x je prvočíslo. (pro „velké" n).

Označme jevy: 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. $\Rightarrow$

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

2 Bayesovy věty pak plyne:

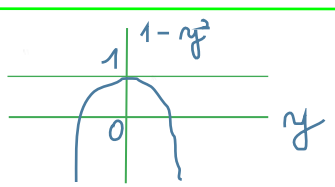
$$P(LP \mid M) = \frac{P(M \mid LP) \cdot P(LP)}{P(M \mid LP) \cdot P(LP) + P(M \mid \overline{LP})\, P(\overline{LP})} \geq \frac{1 \cdot \frac{2}{\ln n}}{1 \cdot \frac{2}{\ln n} + \left(\frac{1}{4}\right)^{100}\left(1 - \frac{2}{\ln n}\right)} \geq$$

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

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

($\ln 10 < 3$, $30 < 32 = 2^5$)

* 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 zobecněná Riemannova hypotéza (není dokázána, ale také se nedaří 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.

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 $\Rightarrow$

$$4^{26} \equiv 1 \pmod{27}$$
$$4^{26} - 1 \equiv 0 \pmod{27}$$
$$(4^{13} - 1)(4^{13} + 1) \equiv 0 \pmod{27} \Rightarrow$$

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

Platí:
$4 \equiv 4 \pmod{27}$
$4^2 \equiv 16 \pmod{27}$
$4^4 \equiv 16 \cdot 16 \equiv 32 \cdot 8 = 5 \cdot 8 = 13 \pmod{27}$
$4^8 \equiv 13 \cdot 13 \equiv (-14) \cdot (-14) = 14 \cdot 14 = 7 \cdot 28 \equiv 7 \pmod{27}$
$4^{13} \equiv 4^8 \cdot 4^4 \cdot 4 \equiv 7 \cdot 13 \cdot 4 = 28 \cdot 13 \equiv 13 \pmod{27}$

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

b) $n = 33$

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

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

$6 \equiv 6 \pmod{33}$
$6^2 \equiv 36 \equiv 3 \pmod{33}$
$6^4 \equiv 3^2 \equiv 9 \pmod{33}$
$6^8 \equiv 9^2 \equiv 81 \equiv 15 \pmod{33}$
$6^{16} \equiv 15^2 = 225 = 198 + 27 \equiv 27 \pmod{33}$ ($198 = 6 \cdot 33$)
$6^{32} \equiv 27^2 \equiv (-6)^2 \equiv 6^2 \equiv 3 \pmod{33}$

$6^{16} + 1 \equiv 28$
$6^8 + 1 \equiv 16$
$6^4 + 1 \equiv 10$
$6^2 + 1 \equiv 4$
$6 + 1 \equiv 7$
$6 - 1 \equiv 5$

$\Rightarrow$ $n = 33$ 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 $a = 9$

$9 \equiv 9 \pmod{91}$

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

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

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

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

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

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

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

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

$\equiv 81 \cdot 9 \equiv$

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

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

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

$\Rightarrow$ a = 9 není svědkem složenosti

Zvolme $a = 10$

$10 \equiv 10 \pmod{91}$

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

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

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

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

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

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

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

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

$\equiv 100 \cdot 10 \equiv$

$\equiv 9 \cdot 10 \equiv -1$

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

$\Rightarrow$ a = 10 není svědkem složenosti

Zvolme $a = 5$

$5 \equiv 5 \pmod{91}$

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

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

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

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

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

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

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

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