

Uděláme první odhad:  $|L_n| \leq \frac{1}{n} |Z_n^*| = \frac{3840}{4} = 960$

Zkoumáme lepsí odhad:  $|L_n| \leq \frac{1}{2^{r-1}} \cdot |K_n| = \frac{1}{23} \cdot 256 = \frac{256}{8} = 32$ , to je lepsí odhad

Ukáme ještě lepsí odhad:  $|L_n| \leq \frac{1}{2^{r-1}} \cdot |\text{Ker } \mu_g|$

$$\begin{aligned} n-1 &= 6544 = 2^4 \cdot 409 \\ |Z_5^*| &= 4 = 2^2 \cdot 1 \\ |Z_7^*| &= 6 = 2^1 \cdot 3 \\ |Z_{11}^*| &= 10 = 2^1 \cdot 5 \\ |Z_{17}^*| &= 16 = 2^4 \cdot 1 \end{aligned} \quad \left. \begin{array}{l} h=4 \\ h_1=2 \\ h_2=1 \\ h_3=1 \\ h_4=4 \end{array} \right\} g = \min \{h_i : h_i \geq 1\} \Rightarrow \mu_g = \rho_{409 \cdot 2}$$

Najdeme  $\rho_{409 \cdot 2}$ : řešíme  $x^{409 \cdot 2^1} = x^{818} = 1 \vee Z_n$

$\gcd(409 \cdot 2, |Z_5^*|) = 2$ , redukuje se to na  $x^2 = 1$

(protože 409 je prvočíslo, a všechny velikosti  $Z_p^*$  jsou sude, bude vždy  $\gcd(n, \varphi(n)) = 2$ , když  $n$  je liché)

Řešení je  $x \in \{-1, 1, \pm i, \pm 1\}$ , celkem je 16 různých řešení, tj.  $|\text{Ker } \rho_{409 \cdot 2}| = 16$

$|L_n| \leq \frac{|\text{Ker } \mu_g|}{2^{r-1}} = \frac{16}{8} = 2$ , ve skutečnosti jsou falešně vzdělky pouze dva, a jsou to 1 a -1, které lichom stejně nekontrolují.

Přednáška  
2.5.2019

Tvrzení: Problem faktorisace  $n$  je ekvivalentní problemu znalosti  $\varphi(n)$ , aneb se znalostí jednoho lze spočítat druhé v polynomickém čase.

- z faktorisace  $\prod p_i^e$  snadno spočítáme  $\varphi(n)$
- pro  $n = p \cdot q$  se znalostí  $\varphi(n)$  spočítáme  $p$  a  $q$  (kvadratickou rovnici)
- pro libovolné  $n$  můžeme polynomickým alg. když udělá faktorisaci ke znalosti násobku exponentu grupy  $Z_n^*$ .

Exponent grupy: Exponent grupy  $Z_n^*$  je nejmenší  $m > 0$  takové, že  $a^m = 1$  pro všechna  $a \in Z_n^*$ . Každá se  $\lambda(n)$ , tiská se Hornu Carmichaelova fce.

- $\lambda(\prod p_i^e) = \text{lcm}(\lambda(p_1^{e_1}), \dots, \lambda(p_r^{e_r}))$
- $\lambda(p^e) = \varphi(p^e) = p^{e-1} \cdot (p-1)$  pro prvočísla  $p > 2$
- $\lambda(2^e) = \frac{\varphi(2^e)}{2} = 2^{e-2}$  pro  $e \geq 3$ ,  $\lambda(4) = 2$ ,  $\lambda(2) = 1$

1) Pro  $\forall n$  platí:  $\lambda(n) / \varphi(n)$ , aneb  $\varphi(n)$  je násobek exponantu grupy  $Z_n^*$

Dk: Když je  $n$  liché  $p^e$ , pak se  $\lambda(n)$  sčítá podle pravidel 2 a 3 níže, a pak máme  $\lambda(n) / \varphi(n)$ .

Pro obecné  $n$ :  $\varphi(n) = \varphi(\prod p_i^{e_i}) = \prod \varphi(p_i^{e_i})$   
 $\lambda(n) = \text{lcm}(\varphi(p_1^{e_1}), \dots, \varphi(p_r^{e_r}))$  bude liché mít vždy delitelné vždy níže

2) Pro  $\forall n > 2$  je  $\lambda(n)$  sude.

Dk: V každémse lichém vypočítá je dvojka, proto jsou všechny  $\lambda(n)$  sude.

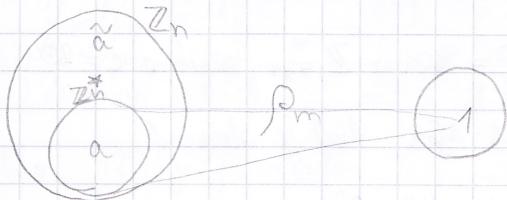
3) Pokud  $d/n$ , pak  $\lambda(d)/\lambda(n)$ .

Dk:  $\frac{2^f}{2^e}$ , když  $f < e$ :  $\lambda(2^f) = 2^{f-2}$ ,  $\lambda(2^e) = 2^{e-2}$ , a zímní  $2^{f-2}/2^{e-2} = p^f/p^e$ , když  $f < e$ :  $\lambda(p^f) = p^{f-1}(p-1)$ ,  $\lambda(p^e) = p^{e-1}(p-1)$ , taky se to dělí.  
Obecný případ:  $n = \prod p_i^{e_i}$ ,  $m = \prod p_i^{e_i} \cdot \prod q_j^{f_j}$ , když  $n/m$

Lemmatum: Když  $a/b$  a  $c/d$ , pak  $\text{lcm}(a, c) / \text{lcm}(b, d)$

Dk:  $a/b / \text{lcm}(b, d)$ ,  $c/d / \text{lcm}(b, d)$ . Proto  $\text{lcm}(b, d)$  jde zapsat jako násobek čísel  $a, c$ . Proto musí být i násobkem jejich lcm.

Najvětší exponent:  $\exp(G) = e$ ,  $e$  je sudé, když  $e = 1 \cdot 2^n$ . Nejdříve m. faktorizací, než  $e/m$ , když  $\exp(G) \neq m$ .



pro  $a \in Z_n^* \Rightarrow a^{\lambda(n)} = 1$

pro  $\tilde{a} \in Z_n^+ \setminus Z_n^* \Rightarrow \tilde{a}^{\lambda(n)} \neq 1$

Algoritmus na faktorizaci se analozi možnosti  $\lambda(n)$

$$a = \text{RAND}(Z_n)$$

$$d = \text{gcd}(a, n)$$

if  $d > 1$ :

return  $d$

$b = a^t \pmod{Z_n}$  (tedy určíme jinou  $a$ , která jsou  $\sim Z_n^*$ , když nesoučítíme  $n$ )

for  $j$  in range( $0, n$ ):

$$d = \text{gcd}(b - 1, n)$$

if  $1 < d < n$ :

return  $d$

$$b = b^2 \pmod{Z_n}$$

return False

Umožníme na  $b$  a  $a$  opakovat faktorizaci množinou na 2, když se máme faktorizovat, jak se to obvykle provedlo v MR.

Turzni: Pravděpodobnost, že algoritmus najde faktor, je apon  $\frac{1}{2}$ .

- pokud vybereme  $a \in Z_n^*$ , tak faktorizujeme rovnou

- pokud  $a \in Z_n^+ \setminus Z_n^*$ , tak faktorizujeme vidy, když  $a \notin L$ , když když poleze pěs nebo výjimky  $\exists i$ .

$\Rightarrow$  jedinečná čísla, která nefaktorizují, jsou čísla  $\sim L$ :

$$\frac{|L|}{|Z_n^+|} < \frac{|L|}{|Z_n^*|} < \frac{1}{2} \quad \checkmark$$

Algoritmus na výpočet celočíselné druhé odmocniny

Př: Vypočítejte  $\sqrt{30}$  celočíselně:  $n=30$ ,  $30 \leq 2^5 \Rightarrow \sqrt[2]{30} < 2^{2.5} \approx 2^3$ ,  $\sqrt[2]{30} = m$

- výsledek zábere mezijs 3 čísla, připravíme si je:  $m \leftrightarrow (\underline{?}, \underline{?}, \underline{?})_2$

$m=0$ , poskupně budeme počítat od čísla na výšejišších polohách

$$i=2) \quad m = (m + 2^i) = 0 + 2^2 = 4$$

$m^2 = 4^2 = 16$ , ale  $16 < 30$ , proto musí být hodnota 1:  $(1, \underline{?}, \underline{?})_2$

$$i=1) \quad m = (m + 2^i) = 4 + 2^1 = 6$$

$m^2 = 6^2 = 36$ ,  $36 > 30$ , protože je hodnota čísla 0:  $(1, 0, \underline{?})_2$

pokrač.  $m^2$  bylo moc velké, vrátíme  $m$  na původní hodnotu  $m=4$

$$i=0) \quad m = (m + 2^i) = 4 + 2^0 = 5$$

$m^2 = 25$ ,  $25 < 30$  ✓, hodnota čísla je 1

$(1, 0, 1)_2$

Máme výsledek,  $\sqrt[2]{30} = 101_{\text{bin}} = 5 \text{ dec}$ , což znamená,  $\sqrt[2]{30} \approx 5.4$

Algoritmus na výpočet celočíselné e-tej odmocniny

Př: Vypočítejte  $\sqrt[3]{30}$  celočíselně:  $n=30$ ,  $30 \leq 2^5 \Rightarrow \sqrt[3]{30} < 2^{\frac{5}{3}} \approx 2^2$ ,  $m \leftrightarrow (\underline{?}, \underline{?})_2$

$$i=1) \quad m = (0 + 2^i) = 2$$

$$m^3 = 2^3 = 8$$

$8 < 30$  ✓

$$i=2) \quad m = (2 + 2^i) = 3$$

$$m^3 = 3^3 = 27$$

✓

$\sqrt[3]{30} \approx 3.107$ , celočíselné výslo 3

Algoritmus na pomocné perfektní množiny: zkusíme brát i od 2 do  $\text{len}(n)$  a uvidíme, jestli pro nějaké i platí  $\lfloor \sqrt[n]{n} \rfloor^e = n$ .

**Pr:** Faktorizujte  $n = 1771$ , znáte-li  $\varphi(n) = 1320$ .  $\varphi(n) = 1320 = 165 \cdot 2^3$

Víme, že pro každé  $a \in \mathbb{Z}_n^*$  je  $a^{\varphi(n)} = 1$ .

Kvůli  $a=5$ ,  $\gcd(1771, 5) = 1$   
 $5 \xrightarrow{165} (804) \xrightarrow{20} 1 \xrightarrow{2} 1 \xrightarrow{2} 1$ , našli jsme  $\sqrt[1]{1} = 804 \in \mathbb{Z}_{1771}^*$ , máme  $c = 804$

$$\gcd(c-1, n) = \gcd(803, 1771) = 11 \Rightarrow n = 11 \cdot 161, 161 \text{ je složné}$$

Kvůli  $a=69$  v  $\mathbb{Z}_{161}$ .  $\varphi(161) = \frac{\varphi(n)}{\varphi(11)} = \frac{1320}{10} = 132 = 33 \cdot 2^2$

$69 \xrightarrow{33} 69 \xrightarrow{2} 92 \xrightarrow{2} 92$ , nebyla nám 1, tj. 69 je soudělá se 161  
 Majdeme  $\gcd(161, 69) = 23$ ,  $161 = 23 \cdot 7$

$$\Rightarrow 1771 = 7 \cdot 11 \cdot 23$$

Cvičení Pr: Fermatovým testem ověřte, zda  $n=85$  je prvočíslo. Za svědky volíme  
 2.5.2019  $a=4, a=2$ .

$$1) a=4, 4^{84} = \dots = 1 \pmod{85} \quad \checkmark$$

$$2) a=2, 2^{84} = \dots = 16 \pmod{85} \quad \times \quad \text{není to prvočíslo}$$

**Pr:** Pro dané ověřte MR testem.  $\varphi(n) = 84 = 2 \cdot 42 = 2 \cdot 21$

$$1) a=4 \quad 4 \xrightarrow{21} 4 \xrightarrow{2} 16 \xrightarrow{2} 1$$

Nášli jsme  $\sqrt[1]{1} = 16$ , takže není prvočíslo. Naše možnosti faktorizovat:

$$\gcd(15, 85) = 5, \gcd(17, 85) = 17 \Rightarrow 85 = 17 \cdot 5$$

$$2) a=2 \quad 2 \xrightarrow{21} 32 \xrightarrow{2} 4 \xrightarrow{2} 16 \neq 1 \quad \text{není to prvočíslo}$$

**Pr:** Popište množiny falošních svědků  $K_n$  a  $L_n$  pro  $n=85$ . ( $= 17 \cdot 5$ )

-  $K_n$  (Fermatov test)

Hledáme  $a$ , že  $a^{85} = 1$ , tedy rovnici  $x^{85} = 1$ , vyřešíme to residuálně v  $\mathbb{Z}_{17}^*$  a  $\mathbb{Z}_5^*$ .

$$\sim \mathbb{Z}_5^*: \gcd(84, \varphi(5)) = \gcd(84, 4) = 4, \text{ takže jsou } 4 \text{ řešení, a to je celá } \mathbb{Z}_5^*.$$

$$\sim \mathbb{Z}_{17}^*: \gcd(84, \varphi(17)) = \gcd(84, 16) = 4, \text{ tj. najdu } P_4. \text{ Výsledek bude, že } \mathbb{Z}_{17}^* = \langle 3 \rangle, \text{ pak bude } P_4 = \langle 3^{16} \rangle = \langle 3 \rangle = \langle 13 \rangle = \{ \pm 1, \pm 4 \}$$

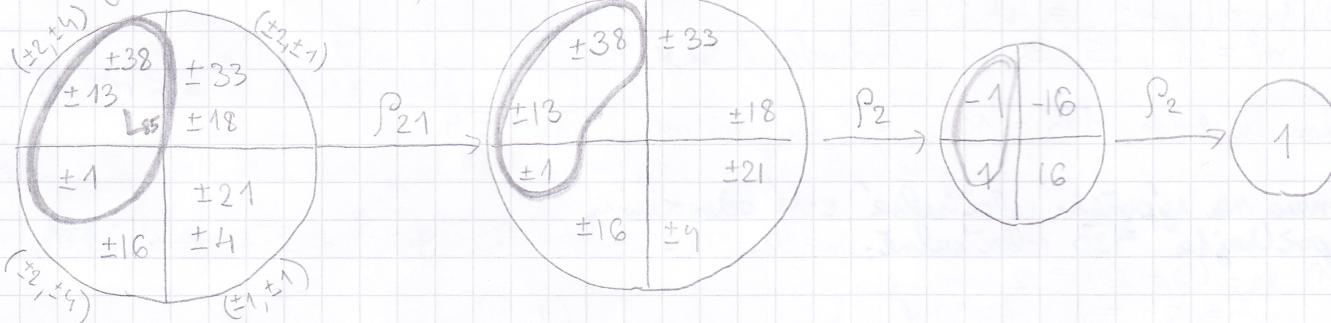
$$K_{85} = \{ \pm 1, \pm 2 \} \cdot q_5 + \{ \pm 1, \pm 4 \} \cdot q_7, \text{ máme ale k } 4 \cdot 4 = 16 \text{ svědků.}$$

$$\text{Hrubý odhad na počet svědků byl přitom } |K_{85}| \leq \frac{1}{2} |\mathbb{Z}_{85}^*| = \frac{1}{2} \cdot 64 = 32$$

-  $L_n$  (Miller-Rabinov test)

$$L_{85} = \{ a \in K_{85} \mid a^{21 \cdot 2^i} = 1, \text{ pak } a^{21 \cdot 2^{i-1}} = -1, 1 \leq i \leq 2 \}$$

$K_{85}$  je residuálně  $\{ \pm 1, \pm 2 \} \times \{ \pm 1, \pm 4 \}$



Falošní svědkové jsou všechny množny pro  $-1$  a množny pro  $1$ , které předtím byly  $\pm 1$ .

$$L_{85} = \{ \pm 1, \pm 13, \pm 38 \}, \text{ celkem je svědků 6.}$$

$$\text{Hrubý odhad byl } \frac{1}{4} \cdot |\mathbb{Z}_n^*| = \frac{1}{4} \cdot 64 = 16$$

$$\text{Položebný odhad: } |L_n| = \frac{2}{2^r} |K_n| = \frac{2}{2^2} \cdot |K_n| = \frac{2}{4} \cdot 16 = 8$$

Príklad: Uveďte MR testem, ada  $n=929$  je prvočíslo, s pravděpodobností výsledku nejvýš 2%.

Při 3 pokusech mám pravděpodobnost výsledku  $\frac{1}{n^3} = \frac{1}{929^3} = 0,015625 < 0,02$ , tedy budou mi stačit 3 pokusy.

$$\begin{array}{ll} 1) \text{ Zvolím } a = 123 & 123 \xrightarrow{29} 18 \xrightarrow{2} 324 \xrightarrow{2} 928 = (-1) \xrightarrow{2} 1 \dots \checkmark \\ 2) \text{ Zvolím } a = 2 & 2 \xrightarrow{29} 883 \xrightarrow{2} 258 \xrightarrow{2} 605 \xrightarrow{2} 928 = (-1) \xrightarrow{2} 1 \dots \checkmark \\ 3) \text{ Zvolím } a = 58 & 58 \xrightarrow{29} 605 \xrightarrow{2} 928 = -1 \xrightarrow{2} 1 \dots \end{array}$$

ANO, 929 je prvočíslo.

Príklad: Při generování prvočísla p spolu s faktorizací  $p-1$  byla vygenerovaná posloupnost  $621, 221, 73, 73, 49, 22, 3, 2, 2$ . Ověřte, ada bylo generování náspevné a k tomu použito MR test s množinou  $S$ ,  $k=2$ ,  $s=10$ . (Tj. zkoušme všechna prvočísla do  $s=10$ , a vybereme  $k=2$  svědků.)

Ugenerujeme si množinu  $S$  malých prvočísel,  $p < s = 10$ ,  $S = \{2, 3, 5, 7\}$ .

A posloupnost náspevně všechna složená čísla testem MRS(., 2)

~~621, 221, 73, 49, 22, 3, 2, 2~~ (3, 2, 2)

$$n-1 = 73 \cdot 3 \cdot 2 \cdot 2 = 876, \text{ když } n = 877.$$

$$\text{MRS}(877, 2), \quad n-1 = 876 = 2^2 \cdot 219$$

Zkouším dělitelnost prvočísla  $n$  v  $S$

Zkouším  $a = 5: 5 \xrightarrow{219} 159 \xrightarrow{2} 876 = -1 \xrightarrow{2} 1 \quad \checkmark$

Zkouším  $a = 102: 102 \xrightarrow{219} 1 \quad \checkmark$

Nášli jsme prvočíslo  $n = 877$  a máme rozklad  $n-1$ .