

Přednáška
3.4.2019 \mathbb{Z}_2^* minula: grupa \mathbb{Z}_2^* je cyklická, $\mathbb{Z}_{2,p}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_p^*$ taky a generátorem je $(1, g)$. Pak $r(g) = r(1, g) = 1 \cdot (p-1) = \varphi(2p) \Rightarrow$ opravdu generuje celé \mathbb{Z}_{2p}^* .

Jak ho vypočítat pro $\mathbb{Z}_{p^e}^*$?

Tvrzení: Pro každé $1 \leq k \leq p-1$ platí $p \mid \binom{p}{k}$.

Dk: $\binom{p}{k}$ je počet k -prvkových podmnožin v p -prvkové množině, označme $\binom{p}{k} = l$, $l \in \mathbb{N}$.

$$l = \binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1) \cdot (p-2) \cdots (p-k+1)}{k \cdot (k-1) \cdots 3 \cdot 2 \cdot 1}$$

Potom l musí být celé číslo, musí jít čitatel schránit jmenovatelem. Zdele nám $l = p \cdot t$ pro nějaké t , může vše, že p nemusí dělit, protože pravé číslo nám schránit nepříje, a sice $p/p + t = l$

Důsledek: $\forall \mathbb{Z}_p$ $(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k} = 1 \cdot b^p + \binom{p}{1} a b^{p-1} + \cdots + 1 a^p$, kde všechny členy s nějakými b^p a a^p jsou dělitelné p
Proto $(a+b)^p = b^p + 0 + 0 + \cdots + 0 + a^p = a^p + b^p \text{ mod } p$

Lemma 1: Nechť p je prvočíslo a $e \geq 1$, $e \in \mathbb{N}$. Když $a \equiv b \pmod{p^e}$, pak $a^p \equiv b^p \pmod{p^{e+1}}$

Př: 1) $a \equiv b \pmod{2^1} \rightsquigarrow a = b + 2l$, $l \in \mathbb{Z}$
pak $a^2 = (b+2l)^2 = b^2 + 4l^2 + 2 \cdot 2bl = b^2 + 4l^2 + 4bl \equiv b^2 \pmod{4} = b^2 \pmod{2^{1+1}=4}$
2) $a \equiv b \pmod{3^1} \rightsquigarrow a = b + 3k$, $k \in \mathbb{Z}$
 $a^3 = (b+3k)^3 = b^3 + 3b^2 \cdot 3k + 3b \cdot 3k^2 + (3k)^3 = b^3 + 9(b^2k + bk^2 + 3k^3) \equiv b^3 \pmod{3^{1+1}=9}$
↑ objevují se nám tady kombinační čísla s korespondujícími

Lemma 2: Nechť p je prvočíslo a $e \geq 1$, $e \in \mathbb{N}$. Když $a \equiv 1 + p^e \pmod{p^{e+1}}$, pak
platí $a^p \equiv 1 + p^{e+1} \pmod{p^{e+2}}$. Načež ale musí platit $p^e > 2$.

Př: 1) $p^e = 3^1$ $a = 1 + 3 \pmod{9}$, použijeme to Lemma 1:
 $a^3 = (1+3)^3 \pmod{27} = 1^3 + 3^2 \cdot 1^2 + 3^3 \cdot 1 + 3^3 \pmod{27} = 1 + 3^2 + 3^3 + 3^3 = 1 + 9 \pmod{9}$
2) $a = 1 + 2 \pmod{4} \rightarrow a^2 = 1 + 2 \cdot 2 + 2^2 \pmod{4} = 1 \pmod{8} \neq 1 + 4 \pmod{8}$
Tolle nevyplo, protože $p^e > 2$.

Tvrzení: Grupa $\mathbb{Z}_{p^e}^*$ je cyklická pro $p > 2$, p je prvočíslo, $e \geq 1$, $e \in \mathbb{N}$. To znamená, že $\exp(\mathbb{Z}_{p^e}^*) = |\mathbb{Z}_{p^e}^*| = p^{e-1} \cdot (p-1)$.

Dk: $|\mathbb{Z}_{p^e}^*| = \varphi(p^e) = p^e - p^{e-1} = p^{e-1} \cdot (p-1)$. Hledáme generátor, tj. prvek řádu $r(a) = \varphi(p^e)$.

Načálo mát prvek b , $r(b) = p-1$ a prvek c , $r(c) = p^{e-1}$. Díky nesoudělnosti řádu pak bude $r(b \cdot c) = r(b) \cdot r(c) = p^{e-1} \cdot (p-1)$.

Najdeme b : Tím, že \mathbb{Z}_p^* je cyklická, tj. má nějaký generátor g , $g^r = 1$ poprvé v \mathbb{Z}_p^* .
 $g^r = 1 \pmod{p^e} \rightsquigarrow g^r = 1 + p \cdot l$, $l \in \mathbb{Z} \rightsquigarrow g^r = 1 + p \cdot k$, $k \in \mathbb{Z}$, $\forall k \in \mathbb{Z}, g^r = 1 \pmod{p}$.
A když $g^r = 1 \pmod{p^e}$, tak $(p-1) \mid r$.

↑ $\mathbb{Z}_{p^e}^*$ nesmí být $g^{\frac{r}{p-1}}$, může vše, že $\frac{r}{p-1}$ je celočíselné. Pak $b^{\frac{r}{p-1}} = g^{\frac{r(p-1)}{p-1}} = g^r = 1$ poprvé,
akcež $r(b) = p-1$.

Najdeme c : Zvolíme $c = 1+p$, ukážeme, že $r(c) = r(1+p) = p^{e-1}$, přičtením do p -ární soustavy:

$$\begin{aligned} c^p &= 1 + p^2 \pmod{p^3} & \sim & (0, 0, \dots, 0, 1, 1)_p \\ c^{(p^2)} &= 1 + p^3 \pmod{p^4} & \sim & (1, *, *, *, 1, 0, 1)_p, * \text{ jsou některá smaky} \end{aligned}$$

$$\begin{aligned} c^{(p-1)} &= 1 + p^{e-1} \pmod{p^e} & \sim & (1, 0, 0, \dots, 0, 0, 1)_p \\ c^{(p^e)} &= 1 + p^e \pmod{p^{e+1}} & \sim & (0, 0, \dots, 0, 0, 1)_p = 1 \end{aligned}$$

Dostali jsme $c^{p^{e-1}} = 1 \text{ v } \mathbb{Z}_{p^e}^*$, takže $n(c)/p^{e-1}$. Máme také $b, n(b) = p-1$ a $c, n(c) = p^{e-1}$. $\gcd(p^{e-1}, p-1) = 1$, protož $b \cdot c$ je generátor $\mathbb{Z}_{p^e}^*$, a to je cyklická.

Příklad: $\mathbb{Z}_{27}^* = \mathbb{Z}_3^{*3}$, najděte generátor, ověřte jeho řád.

Najdeme b : $\mathbb{Z}_3^* = \{1, 2\} = \{\pm 1\}$, $\mathbb{Z}_3 = \langle -1 \rangle$, $b = -1$, $n(b) = 2 \text{ v } \mathbb{Z}_3^*$

Najdeme c : $p = 3$, $c = p+1 = 3+1 = 4$

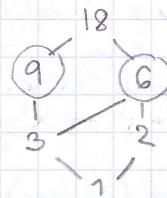
$$g = b \cdot c = -4 = 23$$

$$\mathbb{Z}_{27}^* = \varphi(3^3) = 27-9 = 18, \text{ dělitelé: } 1, 2, 3, 6, 9, 18$$

$$g^6 = 4096 = 19$$

$$g^9 = g^6 \cdot g^3 = 19 \cdot (-64) = 19 \cdot 17 = 26 = -1$$

Platí, že 23 je generátor.



Příklad: $\mathbb{Z}_{2^e}^*$, $|Z_{2^e}| = 2^{e-1} \cdot 1 \Rightarrow b=1, c=1+2$

$$c = 1+2 \pmod{2^2} \quad \checkmark$$

$$c^2 = 1+2^2 \pmod{2^3} \quad \times \quad 9 \neq 5 \pmod{8} \quad \text{Tady mám toho selhé na lemma 2.}$$

Když vychomíme skválky ráct pořádky, máme $d=5$

$$\left. \begin{array}{l} 5 = 1 + 2^2 \pmod{2^3} \quad \checkmark \\ 25 = 1 + 2^3 \pmod{2^4} \quad \checkmark \end{array} \right\} n(d) = 2^{e-2} = 2^{e-1} \cdot 2^{-1} = \frac{|Z_{2^e}|}{2}$$

$$d^{(2^{e-2})} = 1 + 2^e \pmod{2^{e+1}} \quad \left. \begin{array}{l} \text{jde o generátor jen polocíkly grupy} \end{array} \right.$$

Jenž když $d^{(2^{e-2})^2} = 1$, máme relativně $\varphi(1)$, a to v cyklické grupě byt menší, takže $Z_{2^e}^*$ není cyklická. $Z_{2^e}^* = \langle 5 \rangle \times \langle 1 \rangle$, $e > 2$

Příklad: Řešte rovnici $x^6 = 1 \text{ v } \mathbb{Z}_{304}$, $304 = 19 \cdot 2^4$

Vidíme řešení mohou mít inverzi, stačí řešit v \mathbb{Z}_{19}^* . $\mathbb{Z}_{304}^* \cong \mathbb{Z}_{19}^* \times \mathbb{Z}_{16}^*$

Řešení v \mathbb{Z}_{19}^* : v \mathbb{Z}_{19}^* máme pouze pravé řešení na přehrázce 21.3.2019, máme tedy, že generátor

$$\text{grupa je } 2 \text{ a } |Z_{19}^*| = \varphi(19) = 18.$$

Rovnici nelze redukovat proti \mathbb{Z}_{19}^* je toto pravková podgrupa, tu najdeme a tím máme řešení. $6 = \frac{1}{3} \cdot 18$, $P_6 = \langle 2^3 \rangle = \langle 8 \rangle = \{8, 8^2 = 64 = 7, 8^3 = 8 \cdot 8 = 8 \cdot 7 = 56 = 18 + 1, 8^4 = 8^3 \cdot 8 = -8 = 11, 8^5 = 8^2 \cdot 8^3 = 7 \cdot (-1) = -7 = 12, 8^6 = (8^3)^2 = (-1)^2 = 1\} = \{1, 7, 8, 11, 12, 18\}$

Řešení v \mathbb{Z}_{16}^* : Vidíme, že $\mathbb{Z}_{16}^* = \langle 5 \rangle \times \langle -1 \rangle$, bude to platit i pro $e=4$.

$$\langle 5 \rangle \quad n(5) = \frac{|Z_{16}^*|}{2} = \frac{\varphi(16)}{2} = 4$$

Rovnice $x^6 = 1 \text{ v } \mathbb{Z}_{16}^*$ se redukuje na $x^{\gcd(6, 4)} = x^2 = 1$

$P_4 = \langle 5 \rangle = \{5, 9, 13, 17\}$, chceme majet podgrupu P_2 tím, že majdeme její generátor v P_4 .

Ukazuje $13^2 = 169 = 9, 9^2 = 81 = 1 \text{ v } \mathbb{Z}_{16}^*$. Totožno $P_2 = \langle 9 \rangle = \{1, 9\}$

$$\langle -1 \rangle = P = \langle 1, -1 \rangle, \text{ obě řešení } x^6 = 1$$

$$\text{Řešení v } \mathbb{Z}_{16}^*: \{1, 9\} \times \{1, -1\} = \{1, 9, -1, -9\} = \{1, 7, 9, 15\}$$

Řešení v \mathbb{Z}_{304}^* : Dle čínské věty o slyfích: bude $6 \cdot 4 = 24$ řešení všem:

$$x \in \{1, 7, 8, 11, 12, 18\} \cdot q_{19} + \{1, 7, 9, 15\} \cdot q_{16}, \text{ a neime: } q_{19} = 96, q_{16} = -95$$

Druhé mocniny a odmocniny v \mathbb{Z}_n^*

- Nechť p je liché prvočíslo, pak rovnice $x^2 = 1$ má 2 řešení v $\mathbb{Z}_{p^e}^*$ a to $x = \pm 1$.

Máme zobrazení $\rho_2: \mathbb{Z}_{p^e}^* \rightarrow \mathbb{Z}_{p^e}^*: x \mapsto x^2$. ρ_2 je homomorfismus a dle první věty o izomorfismu $\mathbb{Z}_{p^e}^*/\text{Ker } \rho_2 \cong \text{Im } \rho_2$, když $|\text{Im } \rho_2| = |\mathbb{Z}_{p^e}^*/\text{Ker } \rho_2| = |\mathbb{Z}_{p^e}^*|/|\{\pm 1\}| = |\mathbb{Z}_{p^e}^*|/2$.

- Nechť $m = \prod_{i=1}^k p_i^{e_i}$ je liché číslo, pak rovnice $x^2 = 1$ má 2^k řešení v \mathbb{Z}_m^* .

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{e_k}}^*, \quad a \Leftrightarrow (\pm 1, \dots, \pm 1), \quad \rho_2 \text{ má } |\text{Ker } \rho_2| = 2^k, \quad |\text{Im } \rho_2| = \frac{\varphi(m)}{2^k}$$

Přednáška
4.4.2019

Réšení rovnice $x^m = x$ v \mathbb{Z}_n

$\rightsquigarrow \text{v } \mathbb{Z}_p$: když $a=0$, tak a je řešením

když $a \neq 0$, smímená to, že existuje x^{-1} v \mathbb{Z}_p , tj. řešením je $x \in \mathbb{Z}_p^*$

$$x^m = x \in \mathbb{Z}_p \quad | \cdot (x^{-1}) \text{ správce}$$

$$x^{m-1} = 1 \leftarrow \text{ludu řešit lhole v } \mathbb{Z}_p^*$$

$\rightsquigarrow \mathbb{Z}_p^*$: když a je invertibilní, tj. $a \in \mathbb{Z}_p^*$, řešme $x^{m-1} = 1$ v \mathbb{Z}_p^*

když a nemá \rightarrow , tj. $a \in \mathbb{Z}_p - \mathbb{Z}_p^*$, smímená to, že a je soudělené s p.

$$x = p \cdot l, l \in \mathbb{Z}$$

$$p \cdot l = x \rightarrow x^2 = \dots = x^l = 0, \text{ pro } x \neq 0 \text{ nevyjde } x^m = x, \text{ jediné řešení je } x=0$$

Pokud $n=n_1 \cdot n_2$, $\gcd(n_1, n_2)=1$, tak $x^m = x$ může mít v \mathbb{Z}_n i nenukládající řešení. Rovnice tedy nelze srovnat.

Carmichaelova fce: $\lambda: \mathbb{N}^+ \rightarrow \mathbb{N}^+$: $\lambda(n) = \exp(\mathbb{Z}_n^*)$. Aneb $\lambda(n)$ pro $n > 1$ je nejmenší

$m > 0$ takové, že $\forall a$, $\gcd(a, n)=1 : a^m = 1$ v \mathbb{Z}_n . $\lambda(1)=1$.

Vlastnosti: $\lambda(p^e) = \varphi(p^e) = p^{e-1}(p-1)$ pro prvočísla $p > 2$.

$$\lambda(2)=1$$

$$\lambda(4)=2$$

$$\lambda(2^e) = 2^{e-2} = \frac{\varphi(2^e)}{2} \text{ pro } e \geq 3$$

$$\lambda(n_1 \cdot n_2) = \text{lcm}(\lambda(n_1), \lambda(n_2)) \text{ pro nesoudělná } n_1, n_2$$

Diskrétní logaritmus

Definice: Nechť $G = \langle a \rangle$ je cyklická grupa řádu n s generátorem a. Každý prvek $b \in G$ lze zapsat jako $b = a^x$ pro jediné $x \in \mathbb{Z}_n$. Toto x se nazývá diskrétní logaritmus o základu a a prvkem b v grupě G. Značí se $\text{dlog}_a(b)$.

Pr.: $\mathbb{Z}_2^* = \langle 2 \rangle$, $|\mathbb{Z}_2^*| = 6$. $b \in \mathbb{Z}_2^*$ | $\begin{array}{c|cccccc} 2^{6b=0} & 1 & 2 & 4 & 5 & 7 & 8 \\ \hline 0 & 1 & 2 & 4 & 5 & 7 & 3 \end{array}$

Tvrzení: Nechť $G = \langle a \rangle$ je cyklická grupa řádu n. Exponenciální zobrazení

$\text{exp}_a: (\mathbb{Z}_n, +) \rightarrow (G, \cdot) : x \mapsto a^x$ je grupový izomorfismus.

Diskrétní logaritmus: $\text{dlog}_a: (G, \cdot) \rightarrow (\mathbb{Z}_n, +) : g = a^x \mapsto x$ je k němu inverzní, když to je také grupový izomorfismus.

2 vlastnosti homomorphismů platí v rovnici: $\forall b, c \in G, k \in \mathbb{Z}$:

$$\cdot \text{dlog}_a(b \cdot c) = \text{dlog}_a(b) + \text{dlog}_a(c)$$

$$\cdot \text{dlog}_a(1) = 0$$

$$\cdot \text{dlog}_a(b^k) = k \cdot \text{dlog}_a(b)$$

$$\cdot \text{dlog}_a(b^{-1}) = -\text{dlog}_a(b)$$

Problém: Někdy se o diskrétním logaritmu mluví obecně:

- pro nějaké $a \in G$, ne mluví generátor. Pak pokud $b \notin \langle a \rangle$, není $\text{dlog}_a(b)$ definován.

Problém diskrétního logaritmu:

Předpokládá se, že pro většinu grup je rychlý diskrétního logaritmu exponenciální problém - např. pro \mathbb{Z}_p^* a jejich podgrupy, ale pro grupy eliptických křivek.

V grupě $(\mathbb{Z}_n, +)$ není těžké dlog spočítat. Tradiční grupa je $\text{dlog}_a(b) = x \in \mathbb{Z}_n$, takové, že $b = x \cdot a$ v \mathbb{Z}_n , to je lineární rovnice a může ji řešit korověným Euklidem v $O(\text{len}(n)^2)$. $(\mathbb{Z}_n, +)$ se proto v šifrování nepoužívá.

Využití v kryptografii:

- Diffie-Hellmanův algoritmus na domluvu klíče na veřejnosti

- El-Gamal: asymetrické šifrování na stejném principu jako DH alg.

Diffie-Hellmann:

Alice svolí cyklickou grupu G rádiu n a mají generátor a . Dále svolí $x \in \mathbb{Z}_n$ a spočítá prvek $b = a^x$ v grupě G . Alice posle Bobovi prvek b a rádius o grupě (G, n, a) (druhý rádius klic).

Bob svolí $y \in \mathbb{Z}_n$ a spočítá $c = a^y$ v G . Bob posle Alice prvek c .

Tím si oba spočítají následující klic: Alice: $s_A = c^x = a^{yx}$ } $s_A = s_B = a^{xy} = s$
 (stejnou použil pro symetriku správ) Bob: $s_B = b^y = a^{xy} = a^{yx}$

El Gamal:

Alice svolí (G, n, a) jako u DH. Dále svolí $x \in \mathbb{Z}_n$ a spočítá $b = a^x$, a srovnejí grupu n prvek b .

Bob svolí jipici klic $y \in \mathbb{Z}_n$, spočítá $c = a^y$, $s = b^y$. Bob rádius správu $m \in G$: $\bar{m} = m \cdot s \sim G$. Bob posle Alice dvojici (c, \bar{m}) .

Alice si spočítá $s = c^x = a^{xy}$, najde inversi: $s^{-1} = c^{n-x} \sim G$. Alice dešifruje správu \bar{m} : $m = \bar{m} \cdot s^{-1} = (m \cdot s) \cdot s^{-1} = m \cdot 1 = m$ ✓

Př: Alice má srovný klic $b = 7$ a grupu $(\mathbb{Z}_{37}^*, n=36, a=2)$. Bob chce rádius správu $m=10$ klicem $y=8$. Alice souborový klic je $x=32$.

$$\left. \begin{array}{l} c = a^y = 2^8 = 256 = 34 \sim \mathbb{Z}_{37}^* \\ s = b^y = 7^8 = \dots = 16 \sim \mathbb{Z}_{37}^* \\ \bar{m} = m \cdot s = 10 \cdot 16 = 160 = 12 \end{array} \right\} \text{Pošle Alice: } (c, \bar{m}) = (34, 12)$$

Alice správu dešifruje:

$$s^{-1} = c^{n-x} = 34^{36-32} = 34^4 = \dots = 7$$

$$m = \bar{m} \cdot s^{-1} = 12 \cdot 7 = 10 \quad \checkmark$$

Pro šifrování a dešifrování u ElGamala potřebujeme:

- monomorfizm $\sim G$, metoda opakovacích čtvrtin k vyřešení $O(\log(n))$ násoben, kde $n = |G|$.
- pro každou správu volit nový klic y
- dvojnásobek objem des pro šifrování správ (posíláme \bar{m} a k lomu i c). To je neplatné, protože nás používá RSA.
- cyklickou grupu a její generátor, obvykle volíme \mathbb{Z}_p^* , p je prvočíslo o 1024b, a $q = |G|$ je prvočíslo o 160 bitech. Nebo můžeme použít grupu bodů na elliptické křivce, $|G| = 160$ b.

Grupy \mathbb{Z}_n^* , rádius prvků, podgrupy, $x^k = 1$, dnes spíše necyklické

Cvičení
4.4.2019

Př: $\mathbb{Z}_{15}^* = \{1, 2, 4, 8, 11, 13, 14\}$, $\varphi(15) = 2 \cdot 4 = 8$

a) Určete exponent a nejmenší aritmetický řadu prvek max. rádiu ($\alpha(a) = \exp(\mathbb{Z}_{15}^*)$)

$$\mathbb{Z}_{15}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_3^*, \mathbb{Z}_5^* \text{ a } \mathbb{Z}_3^* \text{ jsou cyklické}$$

$$\mathbb{Z}_5^* = \langle 2 \rangle, \exp(\mathbb{Z}_5^*) = 4$$

$$\mathbb{Z}_3^* = \langle -1 \rangle, \exp(\mathbb{Z}_3^*) = 2 \quad \text{toto nám sladěně říká Carmichaelova funkce.}$$

$$\exp(\mathbb{Z}_{n_1, n_2}^*) = \text{lcm}(n_1, n_2) \Rightarrow \exp(\mathbb{Z}_{15}^*) = \text{lcm}(4, 2) = \underline{\underline{4}}$$

Jak najít prvek rádiu 4?

a) $a \leftrightarrow (a_1, a_2)$, hledáme a , které má sbytek po dělení 5 = a_1 , a po dělení 3 = a_2
 $a \leftrightarrow (2, 2)$, to splňuje $a=2$ ✓

b) Zkuste si vypočítat α ověřit rádius.

$$\alpha = 2^2 \quad \langle 2 \rangle = \{2^1, 2^2 = 4, 2^3 = 8, 2^4 = 16 = 1\} \text{ ok, } \alpha(2) = 4$$

b) Počítejte se počet podgrup v \mathbb{Z}_{15}^* .

\mathbb{Z}_{15}^* není cyklická, může mít několik podgrup stejně velikosti. Zkoušme 2 případů hledání

- najdeme podgrupy v \mathbb{Z}_3^* a \mathbb{Z}_5^* a dle toho dokonad.

$$\text{v } \mathbb{Z}_3^*: P_1' = \{1\}$$

$$P_2' = \{1, 2\} = \mathbb{Z}_3^*$$

$$\text{v } \mathbb{Z}_5^*: P_1'' = \{1\}$$

$$P_2'' = \{1, 4\}$$

$$P_4'' = \{1, 2, 3, 4\} = \mathbb{Z}_5^*$$

$$P_1 = P_1' \times P_1'' = \{1\}$$

$$P_2 = P_2' \times P_1'' = \{1, 2\} \times \{1\} = \{(1, 1), (2, 1)\} = \{1, 11\}$$

$$P_3 = P_1' \times P_2'' = \{1\} \times \{1, 4\} = \{(1, 1), (1, 4)\} = \{1, 4\} \xrightarrow{(-1, -1) = -1}$$

$$P_4 = P_2' \times P_2'' = \{1, 2\} \times \{1, 4\} = \{(1, 1), (1, 4), (2, 1), (2, 4)\} = \{1, 4, 11, 14\}$$

$$P_5 = P_1' \times P_4'' = \{1\} \times \{1, 2, 3, 4\} = \{(1, 1), (1, 2), (1, 3), (1, 4)\} = \{1, 7, 13, 4\}$$

$$P_6 = P_2' \times P_4'' = \{\dots\} = \mathbb{Z}_3^* \times \mathbb{Z}_5^* = \mathbb{Z}_{15}^*$$

Najdli jsme 6 podgrup, ale nejsou jenom grupy $\{1, 14\}$.

- najdeme podgrupy generováním: $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$$\langle 1 \rangle = \{1\}$$

$$\langle 2 \rangle = \{2, 4, 8, 1\} \leftarrow \text{takto jsme předtím nenašli}$$

$$\langle 4 \rangle = \{4, 1\}$$

$$\langle 7 \rangle = \{1, 4, 7, 13\}$$

$$\langle 8 \rangle = \langle -7 \rangle = \{1, 2, 4, 8\}$$

$$\langle 11 \rangle = \langle -4 \rangle = \{11, 1\}$$

$$\langle 13 \rangle = \langle -2 \rangle = \{13, 4, 7, 1\}$$

$$\langle 14 \rangle = \langle -1 \rangle = \{14, 1\}$$

Najdli jsme 6 podgrup, ale sice neřechny

Příklad si myslíme jistě, že máme všechny podgrupy, ale budeme tomu věřit, protože to takhle má myšlení Josefa Želrollova neobecně.

c) Řešte $x^2 = 1$ a $x^3 = x$ v \mathbb{Z}_{15}

- $x^2 = 1$ x musí mít inverzi, proto $x \in \mathbb{Z}_{15}^*$

$\mathbb{Z}_{15}^* \setminus \{ \frac{\mathbb{Z}_3^*}{\mathbb{Z}_5^*} \}$ jsou cyklické, x^2 má řešení jiné než 1

$$\begin{aligned} \text{Řešení v } \mathbb{Z}_3^*: & (1, 1) \leftrightarrow 1 \\ & (2, 1) \leftrightarrow 11 \\ & (1, 4) \leftrightarrow 4 \\ & (2, 4) \leftrightarrow 14 \end{aligned}$$

$$x \in \{1, 4, 11, 14\}$$

$$- x^3 = x$$

$$\text{řešení v } \mathbb{Z}_3: \{0, 1, 2\}$$

$$\text{řešení v } \mathbb{Z}_5: \{0, 1, 4\}$$

← to jsou algoritma řešení jatoru x^2 , ale přidali jsme 0.

$$\begin{aligned} \text{řešení v } \mathbb{Z}_{15}: & (0, 0) \leftrightarrow 0 & ! \\ & (0, 1) \leftrightarrow 6 & ! \\ & (0, 4) \leftrightarrow 9 & ! \\ & (1, 0) \leftrightarrow 10 & ! \\ & (1, 1) \leftrightarrow 1 & ! \\ & (1, 4) \leftrightarrow 4 & ! \\ & (2, 0) \leftrightarrow 5 & ! \\ & (2, 1) \leftrightarrow 11 & ! \\ & (2, 4) \leftrightarrow 14 & ! \end{aligned}$$

Tablek řešení neplatí v \mathbb{Z}_{15}^* , proto nemůžeme hledat přejít do \mathbb{Z}_{15}^*



Príklad: $\exp(\mathbb{Z}_{45}^*)$. Kolik pruhů má \mathbb{Z}_{45}^* má $r(a) = \exp(\mathbb{Z}_{45}^*)^2$?

$$\mathbb{Z}_{45}^* = \mathbb{Z}_{3^2}^* \times \mathbb{Z}_5^*$$

$$\lambda(45) = \text{lcm}(\lambda(5), \lambda(9)) = \text{lcm}(r(g), r(a)) = \text{lcm}(4, 6) = 12 \Rightarrow \exp(\mathbb{Z}_{45}^*) = 12.$$

Najdené generátory $\mathbb{Z}_{3^2}^* = \langle 2 \rangle$ $(2, 2) \leftrightarrow 2$, nejvyšší rád má 2.
problém s rozdílem v rádu $\mathbb{Z}_5^* = \langle 2 \rangle$

$$\text{Druhý rád lichotě pruhů } r_{45}(2) = \text{lcm}(r_5(2), r_a(2)) = \text{lcm}(4, 6) = 12 \checkmark$$

Kolik pruhů stejného rádu bude?

$$r(ak) = \frac{r(a)}{\text{gcd}(r(a), k)} = r(a), \text{ kde } \text{gcd}(r(a), k) = 1, \text{ tj. } k \text{ nesoudělné s } r(a)$$

$$\begin{aligned} \mathbb{Z}_5^* &\text{ má 2 generátory } (\varphi(4) = 2) & \text{lcm}(4, 6) \Rightarrow 4 \text{ pruhů} \\ \mathbb{Z}_9^* &\text{ má 2 generátory } (\varphi(6) = 2) & \text{lcm}(4, 3) \Rightarrow 4 \text{ pruhů} \end{aligned} \} \text{ celkem je } 8 \text{ takových}$$

Príklad: Řešte $x^{15} = 1$ v \mathbb{Z}_{518}^* , $518 = 2 \cdot 7 \cdot 37$, $\mathbb{Z}_{518}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_7^* \times \mathbb{Z}_{37}^* \cong \langle 2 \rangle \times \mathbb{Z}_{37}^*$

$$\begin{aligned} \text{v } \mathbb{Z}_{14}^*: |\mathbb{Z}_{14}^*| = 6, \text{ rády: } 1, 2, 3, 6 & \quad \text{Naději vymeneme cyklickou } \mathbb{Z}_{14}^* \text{ až máme jen dvoujico} \\ \mathbb{Z}_{14}^* = \langle 3 \rangle, \text{ normici redukujeme na } \text{gcd}(15, 6) = 3, 1^3 \times 3^3 = 1 & \\ P_3 = \langle 3^2 \rangle = \dots = \{1, 9, 11\} & \end{aligned}$$

$$\text{v } \mathbb{Z}_{37}^*: |\mathbb{Z}_{37}^*| = 36, \text{ rády } 1, 2, 3, 4, 6, 9, 12, 18, 36, 1^3 15\text{-ti pruhůvou podgrupu nemáme.} \\ \text{Rovnice redukujeme: } \text{gcd}(15, 36) = 3, 1^3 \times 3^3 = 1.$$

Najdené generátory, vž. třeba 2?

$$\begin{aligned} 2^6 &= \dots = -10 \\ 2^{12} &= (2^6)^2 = (-10)^2 = \dots = -21 \\ 2^{18} &= \dots = -1 \end{aligned} \} \text{ano, } 2 \text{ je generátor, } \mathbb{Z}_{37}^* = \langle 2 \rangle$$

$$\text{Očekáme 3-pruhovou podgrupu: } \frac{36}{3} = 12, P_3 = \langle 2^{12} \rangle = \langle -11 \rangle = \{1, 10, 26\}$$

$$\begin{aligned} \text{Řešení v } \mathbb{Z}_{518}^*: \text{ Máme } 3 \times 3 = 9 \text{ řešení, vž. máme dva } q_{14} = 37k_1 = -111 \\ q_{37} = 14k_2 = 112 \quad \} 37k_1 + 14k_2 = 1 \\ x \in \{1, 9, 11\} \cdot q_{14} + \{1, 10, 26\} \cdot q_{37} \end{aligned}$$