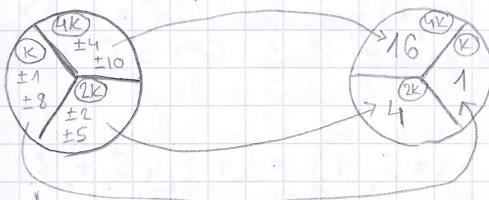


$\text{PF: Máme operaci } \rho_2 \text{ na } \mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}, 21=3 \cdot 7, \varphi(21)=12$
 $\text{Ker } \rho_2 = \{\pm 1, \pm 8\}$, božme dostali hruškovou silou, ale mohli bychom to dostat pomocí $\mathbb{Z}_{21} \cong \mathbb{Z}_7 \times \mathbb{Z}_3$

$$|\text{Im } \rho_2| = \frac{|\mathbb{Z}_{21}^*|}{|\text{Ker } \rho_2|} = \frac{12}{4} = 3$$



$$\begin{aligned} K: x^2 &= 1 \\ 2K: x^2 &= 4 \\ 4K: x^2 &= 16 \end{aligned}$$

K v grupe \mathbb{Z}_{21}^* grupa $K = \{\pm 1, \pm 3\}$ máloň direktní osvětlení? (Dá se zapsat \mathbb{Z}_{21}^* jako $\mathbb{Z}_{21}^* = K \times H$, kde $K \cap H = \{1\}$, $K \cdot H = \mathbb{Z}_{21}^*$, t.j. $|H| = |\text{Ker } \rho_2| = |K| \cdot |H|$).

$$\begin{aligned} |\mathbb{Z}_{21}^*| &= |\text{Ker } \rho_2| \cdot |H| \\ 12 &= 4 \cdot |H| \\ \Rightarrow |H| &= 3 \end{aligned}$$

Ano, nalezená H existuje, je to $\langle 4 \rangle$. $H = \langle 4 \rangle = \{1, 4, 16 = 1\} = \{1, 4, 16\}$.

$$\begin{array}{c} \bullet 1 \ 4 \ -5 \\ 1 \ 1 \ 4 \ -5 \\ -1 \ -1 \ -4 \ 5 \\ 3 \ 8 \ -10 \ 2 \\ -8 \ -8 \ 10 \ -2 \end{array} \quad \text{or tabulce mimo celkem } 12 = |\mathbb{Z}_{21}^*| \text{ hodnot, každá je jiná, to sedí!} \quad (G, \cdot)$$

Definice: Nechť G je grupa s neutrálním prvkem 1. Nejmenší přirozené číslo $m > 0$ takové, že pro $\forall a \in G$ je $a^m = 1$, se nazývá exponent grupy, množina $\exp(G)$. Pokud takové m neexistuje, je $\exp(G) = 0$.

Předměstka
27.3.2019

$$\begin{aligned} \text{Např: } \exp(\mathbb{Z}_n) &= n \\ \exp(\mathbb{Z}) &= 0 \\ \exp(\mathbb{Z}_q^*) &= q = \varphi(q) \\ \exp(\mathbb{Z}_2^*) &= 2 = \varphi(3) \end{aligned}$$

$$\prod_{i=1}^{|\text{G}|} r(a)^{\exp(G)}$$

Exponent je to samé, co $n(a)$ a platí pro něj stejně věty, jenže to, co se předtím týkalo a , musí platit $\forall a \in G$.

- Tvrzení:** Je-li G konečná grupa, pak má kládají exponent a platí $\exp(G) / |\text{G}|$
- Má-li grupa G kládají exponent, pak $\forall a \in G: n(a) / \exp(G)$
 - Je-li grupa G cyklická, pak $\exp(G) = 0$ pro nekonečnou G
 $\exp(G) = |\text{G}|$ pro konečnou G
 - Použili G_1, G_2 grupy, pak $\exp(G_1 \times G_2) = \text{lcm}(\exp(G_1), \exp(G_2))$

Věta: Má-li Abelova grupa G exponent $\exp(G) = m, m > 0$, pak obsahuje prvek rádu m . (doházení pořejí).

Věta: Když je n nekonečná cyklická grupa, je izomorfická s grupou $(\mathbb{Z}, +)$. Každá cyklická grupa rádu n je izomorfická s grupou $(\mathbb{Z}_n, +)$.

Prostřední izomorfismus je $f: k \mapsto a^k$, kde a je generátor grupy.

$f: (\mathbb{Z}, +) \rightarrow (G, \cdot)$: $k \mapsto a^k$ je izomorfismus. Je to zároveň grupou homomorfismus, neboť $f(k+l) = a^{k+l} = a^k \cdot a^l = f(k) \cdot f(l)$.

Dk: 1) je f na?

Ano, protože pro všechny $x \in G$ platí, že $x = a^k$, kde a je generátor.

2) je f funkce?

$$\text{Ker } f = \{k \in \mathbb{Z} : f(k) = a^k = 1, 1 \in G\}$$

- pro nekonečnou G : pouze $a^0 = 1$, tedy $\text{Ker } f = \{0\}$, jadro je buď prázdno, protože f je funkce
- pro konečnou G : $|\text{G}| = m$, tedy $n(a) = m$, a toho $a^m = a^{n \cdot k} = a^0 = 1$. V jadru lze dělit násobky rádu a , $n(a) = n \cdot k$: $\text{Ker } f = \{m \cdot k, k \in \mathbb{Z}\} = m\mathbb{Z}$.

Z první věty o izomorfismu $\mathbb{Z}/\text{Ker } f \cong \text{Im } f$, $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$. Tyto věti souborem $\psi: \mathbb{Z}/\mathbb{Z}_n \rightarrow a^k$, kde býdy $x + n\mathbb{Z} = \{x + nk : k \in \mathbb{Z}\} = [x]_n$ jsou slyšitelné měny mod n . Takže $(G) \cong (\mathbb{Z}_n, +)$ a prostřední izomorfismus je ψ .

Podgrupy konečných cyklických grup:

(Podgrupy $n \cdot (\mathbb{Z}_n, +)$) jsou kroužky $d\mathbb{Z}_n = \langle d \rangle$, kde d/n . Průběhem podgrupas $d\mathbb{Z}_n$, $d\mathbb{Z}_n = \{di, 1 \leq i \leq \frac{n}{d}\}$ má $\frac{n}{d}$ prvků. Našíme $d_1\mathbb{Z}_n \subseteq d_2\mathbb{Z}_n$ iff $\frac{n}{d_1} \mid \frac{n}{d_2}$.

Nechť $G = \langle a \rangle$ je cyklická grupa řádu n . Podgrupy $n \cdot (G, \cdot)$ jsou kroužky $G^d = \langle a^d \rangle$, kde d/n . Průběhem podgrupa $G^d = \{a^{id}, 1 \leq i \leq \frac{n}{d}\}$ má $\frac{n}{d}$ prvků. Našíme $G_{d_1} \subseteq G_{d_2}$ protože budež d_2/d_1 , právě když $\frac{d_1}{d_2}$.

Příklad: $\mathbb{Z}_9^* = \langle 2 \rangle$, $\varphi(9) = 6$, $\mathbb{Z}_9^* = \{1, 2, 4, 8, -1, -2 = 7, -4 = 5, 1\} = \{1, 2, 4, 5, 7, 8\}$

$\mathbb{Z}_n^* \cong (\mathbb{Z}_{\varphi(n)}, +)$, $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$2+4=6=0 \text{ v } \mathbb{Z}_6$; $2^2 \cdot 2^4 = 2^6 = 2^0 = 1 \text{ v } \mathbb{Z}_9^*$, násobí 10, že to je jednotka

Podgrupy: $6 \cdot \mathbb{Z}_6 = 0\mathbb{Z}_6 = \{0\}$
 $2 \cdot \mathbb{Z}_6 = \{0, 2, 4, 6, 8, 10\} = \{0, 2, 4\}$
 $3 \cdot \mathbb{Z}_6 = \{0, 3, 6, 9, 12, 15\} = \{0, 3\}$
 $1 \cdot \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
t. dělitelé $\varphi(n)$, t. dělitelé řádky

$\mathbb{Z}_6 \quad 3\mathbb{Z}_6 \quad 6\mathbb{Z}_6$

$P_1 = \{1\} = \langle 1 \rangle$
 $P_3 = \{1, 4, 7\} = \langle 4 \rangle$
 $P_2 = \{1, -1\} = \langle -1 \rangle$
 $P_6 = \mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\} = \langle 2 \rangle$

Pokud je grupa cyklická, našíme všechny velikosti podgrup.

Twrzení: Nechť $G = \langle a \rangle$ je cyklická grupa řádu n .

- každá podgrupa cyklické podgrupy je cyklická
- pro každé r/n je $r \cdot G$ jediná podgrupa řádu r . Je to podgrupa $H_r = \langle a^r \rangle$, $b = a^{\frac{n}{r}}$ je prvek řádu r .
- nechť H_r je podgrupa řádu r : a . Hr je podgrupa řádu s v G . Pak $H_r \subseteq H_s$, právě když $r \mid s$.

Důsledek: Nechť $G = \langle a \rangle$ je cyklická grupa řádu n . Pokud je r/n , pak je v grupě G právě $\varphi(r)$ prvků řádu r .

Oto Eulerova funkce platí vorec $\sum_{r|n} \varphi(r) = n$.

Dk: $(\mathbb{Z}_n, +)$ je cyklická, pro každý r/n je $\varphi(n)$ prvek řádu n a jiné řády nejsou možné.

$$m = |\mathbb{Z}_n| = \sum_{r|n} |\text{počet prvků řádu } r| = \sum_{r|n} \varphi(r) = n.$$

Rешení rovnice $x^k = 1$. Nechť $G = \langle a \rangle$ je cyklická grupa řádu n .

- pokud r/n , pak má rovnice $x^r = 1$ právě r řešení v G . Nejmenší jsou všechny prvky a jediné r -prvkové podgrupy v G , jsou tedy prvky $x = b^i$, kde $b = a^{\frac{n}{r}}$ je prvek řádu r , $1 \leq i \leq r$.
- pro libovolné $k \in \mathbb{N}$ má rovnice $x^k = 1$ v G právě $d = \gcd(k, n)$ řešení a redukuje se na rovnici $x^d = 1$.

Dk: 1) Když r/n , pak je $r \cdot G$ podgrupa P_r řádu r . Dle Eulerovy věty má P_r právě pro $\forall x \in P_r$, že $x^r = 1$, tedy prvky z P_r řeší rovnici.

- ještě díky akci, že mimo P_r řádky řešení nenajdeš.

Máme nějaký prvek b , pro který platí $b^r = 1$. Pak $r(b)/r$ je řádek pro řádky. Vnačme $r(b) = s$, pak b generuje podgrupu $P_s = \langle b \rangle$, $|P_s| = s$. Ale tím s/r , a protože je G cyklická, musíme $P_s \subseteq P_r$, a když $b \in P_s$, tak nutně $b \in P_r$.

2) Když $a \in G$ bylo řešením, tak by $a^k = 1$, tj. $a(a)/k$.

Ale protože $a \in G$, tak $a(a)/|G|$, neboli $a(a)/n$. To znamená, že $a(a)$ je společný dělitel k a n, proto $a(a)/\gcd(k, n)$. Vnačme $\gcd(k, n) = d$, tedy $ad = 1$.

Důsledek: Pokud je grupa (\mathbb{Z}_n^*, \cdot) cyklická a $n > 2$, pak má rovnice $x^2 = 1$ právě dvě řešení v \mathbb{Z}_n , a to ± 1 . V \mathbb{Z}_2 má rovnice $x^2 = 1$ jediné řešení $x = 1 = -1$.

Pr: Řešte rovnici $x^{21} = 1$ v \mathbb{Z}_{19}^* . Od minula víme, že $|\mathbb{Z}_{19}^*| = 18$ a $\mathbb{Z}_{19}^* = \langle 2 \rangle$, proto $2^{18} = 1$, $\varphi(2) = 18$, $|\mathbb{Z}_{19}^*| = \varphi(n) = \varphi(19) = 18$.

Hledáme a , aby $\varphi(a)/21$ a rávnož $\varphi(a)/18$. Tím, že $\gcd(21, 18) = 3$, hromadí proto musíme redukovat na $x^3 = 1$.

Najdeme prvek x řádu 3: $b = 2^{\frac{18}{3}} = 2^6 = 7$, tento prvek generuje $P_3 = \langle 7 \rangle = \{1, 7, 11\}$, a všechny prveky v P_3 jsou řešením rovnice.

$x^2 = 1$ v \mathbb{Z}_{19}^* ? Má jen dvě řešení, a to +1 a -1.

Věta: Kladá grupa prvočíselného řádu je cyklická.

Dz: Uvohnejme libovolný prvek a , $a \in G$. Tento prvek generuje grupu $P = \langle a \rangle$, přitom o podgrupech víme, že $|P|/|G|$. Když $|G|$ je prvočíslo, tak buď $|P|=1$ nebo $|P|=|G|$, tj. $G = \langle a \rangle$.

Pozn: Předchozí tvrzení ale nesírá o cyklickost \mathbb{Z}_n^* , protože my mají prvočíselný řád jen pro $n=2$ (\mathbb{Z}_p^* , $\varphi(p)=p-1$, což je sudé).

Tvrzení: Nechť $G = \langle a \rangle$ je cyklická grupa řádu n a nechť $m \in \mathbb{N}$. Zobrazení

$\rho_m: G \rightarrow G: x \mapsto x^m$ je grupový homomorfismus. Nechť d/n , tzn: $n = r \cdot d$.

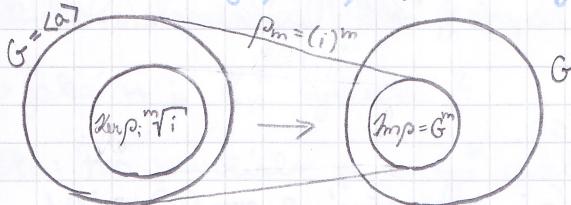
- $\text{Ker } \rho_d := \{g \in G; g^d = 1\} = \langle a^d \rangle = \langle a^r \rangle$ a má $\frac{n}{d}$ prvků.

- $\text{Im } \rho_d = \{g^d; g \in G\} = \langle a^d \rangle$ a má $\frac{n}{d}$ = r prvků.

Oba podgrupy mají stejnou strukturu, alespoň pro $n = |G| = r \cdot d$ je

$\text{Ker } \rho_n = \text{Ker } \rho_d$ a $\text{Im } \rho_n = \text{Im } \rho_d$.

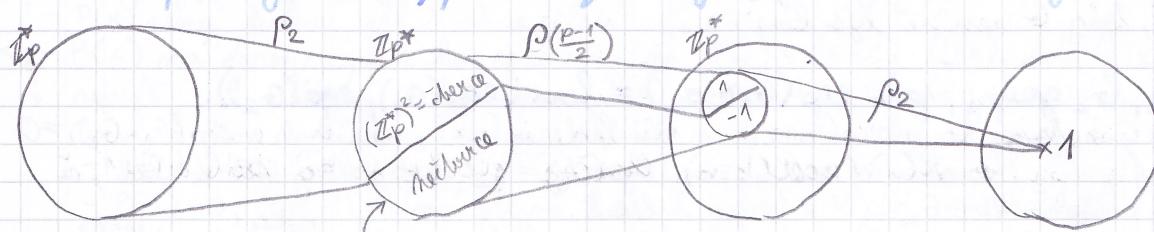
Pro obecné $m \in \mathbb{N}$ je $\rho_m = \rho_d$, kde $d = \gcd(m, |G|)$.



Důsledek: Nechť G je cyklická grupa řádu n a nechť d/n . Prvek $b \in G$ je d -tak možnivý ($b = c^d$ pro nějaké $c \in G$), právě když $b^{\frac{n}{d}} = 1$.

Eulerovo kritérium pro \mathbb{Z}_p^* : Nechť p je liché prvočíslo.

- prvek $b \in \mathbb{Z}_p^*$ je čtvrtce ($b = c^2$), právě když $b^{\frac{p-1}{2}} = 1$. V tomto případě má b dva druhé akomunity, a to $\pm c$.
- prvek $b \in \mathbb{Z}_p^*$ je nečtvrtce ($b \neq c^2$), právě když $b^{\frac{p-1}{2}} = -1$.
- součin dvou prvků je čtvrtce, právě když oba jsou čtvrtce nebo oba jsou nečtvrtce.



- $\forall b \in \mathbb{Z}_p^*$ je čtvrtce iff $p \equiv 1 \pmod{4}$
- $\forall b \in \mathbb{Z}_p^*$ je nečtvrtce iff $p \equiv 3 \pmod{4}$

Příklad: Grupa \mathbb{Z}_{19}^* má řád 18 a generátorem je $a=2$.

- racioni $x^3 = 1$ řešit $x \in \{2^{6i}, 1 \leq i \leq 3\} = \{1, 7, 13\}$, což je $(\mathbb{Z}_{19}^*)^6$

- prvek $b = 3$ je nečlenec

$$3^{\frac{19-1}{2}} = 3^{\frac{18}{2}} = 3^9 = \dots = -1 \in \mathbb{Z}_{19}^*$$

- prvek $b = 5$ je členec

$$5^{\frac{18-1}{2}} = 5^9 = \dots = 1 \in \mathbb{Z}_{19}^*$$

- platí: $c = a^{\frac{p+1}{2}}$ když $\frac{p+1}{2}$ je liché. $\approx c^2 = a^{\frac{p+1}{2}}, 5 = (\pm c)^2$

$$c = a^{\frac{p+1}{4}} = 5^{\frac{19+1}{4}} = 5^{\frac{20}{4}} = 5^5 = 9 < +c = 9 \\ -c = -9 = 19 - 9 = 10$$

Přednáška Věta: Je-li G konečná grupa, pak má kladný exponent a platí $\exp(G) / |G|$
28.3.2019

Dоказat: Z Eulerovy věty: když G je konečná, pak $\forall a: a^{|G|} = 1$. Máme tedy kandidátku na exponent, exp tedy nemůže být méně a méně je kladný.

Předpokládejme, že neplatí $\exp(G) / |G|$. Zvolime nějaké a , pro které $\exp(G) = r(a)$.

Protože neplatí $r(a) / |G|$, takže $|G| = k \cdot r(a) + l$, kde $k \geq 1, 0 < l < r(a)$.

$$1 = a^{|G|} = a^{k \cdot r(a) + l} = a^{k \cdot r(a)} \cdot a^l = 1 \cdot a^l = 1$$

Aby platila poslední rovnost, muselo by $l = 0$, ale to srovnává, že méně $r(a) = \exp(G) / |G|$.

Ted když je díky celý napsaný, vidím, že jsem mohla volbu $r(a)$ úplně vynechat a pracovat jenom s $\exp(G)$.

- Má-li grupa G kladný exponent, pak každý prvek má konečný řád a $r(a)/\exp(G)$

Dоказat: Z definice je exponent takové nejméní m , aby $\forall a \in G: a^m = 1$. Kladný exponent znamená, že takové m existuje, tj. řády prvků jsou konečné (nejvýš m).

Předpokládejme, že máme a , pro které neplatí $r(a)/\exp(G)$. Pak: $\exp(G) = k \cdot r(a) + l \Rightarrow$

$$1 = a^{\exp(G)} = a^{k \cdot r(a) + l} = a^{k \cdot r(a)} \cdot a^l = 1 \cdot a^l$$

Nuhě by muselo $l = 0$, pak ale platí $r(a) / \exp(G)$.

- Je-li grupa G cyklická, pak $\exp(G) = 0$ iff G je nekonečná, a $\exp(G) = |G|$ iff G je konečná.

Dоказat: G je konečná $\Rightarrow \exp(G) = |G|$

G je konečná a cyklická, tj. G má generátor g , $G = \langle g \rangle$, $r(g) = |G|$. Exponent l je z definice nejméní m , aby $a^m = 1 \forall a \in G$, tedy $\exp(G) \geq r(g) = |G|$. A nyní, že v G existuje neněkolik řád než $|G|$, proto $\exp(G) = |G|$

$$\exp(G) = |G| \Rightarrow G \text{ je konečná}$$

Cyklická grupa musí mít generátor, a $r(g) \leq \exp(G)$. Exponent je $|G|$, tedy konečný, tím řád g je konečný, a proto s ním nedokážeme vygenerovat nekonečnou grupu.

$$G \text{ je nekonečná} \Rightarrow \exp(G) = 0$$

Když je G nekonečná, bude generátor nekonečného řádu. Nedokážeme tedy najít nejméní m jako exponent, a tedy z definice $\exp(G) = 0$.

$$\exp(G) = 0 \Rightarrow G \text{ je nekonečná}$$

Když $\exp(G) = 0$, stanová to, že je to nejdříji minimální m , aby $a^m = 1 \forall a \in G$. Potom by ale byla grupa konečná, z Eulerovy věty je $a^{|G|} = 1$ pro $\forall a \in G$, tedy by bylo $\exp(G) = |G|$. To ale neplatí, tedy G nemůže být konečná.

- Jsou-li G_1, G_2 grupy, pak $\exp(G_1 \times G_2) = \text{lcm}(\exp(G_1), \exp(G_2))$.

Pro nekonečnou grupu G_1 je $\exp(G_1) = 0$, a pak bude i $G_1 \times G_2$ nekonečná, a $\exp(G_1 \times G_2) = 0$

Pro konečné grupy: Konečné $\exp(G_1) = e_1, \exp(G_2) = e_2$. Pro prvek $a \in G_1$ platí, že

$$a^{k \cdot e_1} = 1, \text{ odkud } \#b \in G_2 : b^{l \cdot e_2} = 1 \text{ pro } k, l \in \mathbb{Z}$$

Když chceme $\exp(G_1 \times G_2)$, hledáme nejméní takové číslo m , aby $a^{m \cdot e_1} = 1 = b^{m \cdot e_2}$, a m byl společný násobek e_1 a e_2 . To je právě $m = \text{lcm}(e_1, e_2)$.

Věta: Má-li Abelova grupa G exponent $\exp(G) = m > 0$, pak obsahuje prvek řádu m .

\Leftrightarrow existuje $a \in G$, $\exp(G) = r(a)$.

Dk: Neníře se stát, že $r(G) = b$, $r(b) = 2$, a c , $r(c) = 3$, ale nemůže prvek řádu 6.

Tvrdíme, že když $\gcd(r(b), r(c)) = 1$, pak $r(b \cdot c) = r(b) \cdot r(c)$.
K tomuto tvrzení je potřeba Abelova grupa.



Obecně: $\exp(G) = m$, m lze rozložit na násobek prvočísla: $m = \prod_{i=1}^k p_i^{e_i}$

Chceme pro $i = 1 \dots k$ mít prvek a_i řádu $r(a_i) = p_i^{e_i}$

Pak díky nezávislosti řádu lze platit pro $a = \prod_{i=1}^k a_i$, že $r(a) = \prod_{i=1}^k r(a_i)$

Pro každé $1 \leq i \leq k$ majdu $b_i \in G$ tak, že $b_i^{\frac{m}{p_i}} \neq 1$. Takouž bi existuje proto, že m je nejmenší číslo, že $a^m = 1 \forall a \in G$.

Pak: $a_i = b_i^{\frac{m}{p_i}}$ je prvek řádu $r(a_i) = p_i^{e_i}$.

1) Vídám, plati $r(a_i) = 1$?

$$a_i^{(p_i^{e_i})} = b_i^{\frac{(m/p_i)}{p_i^{e_i}}} = b_i^{\frac{m}{p_i}} = b_i^m; \text{ a protože } m \text{ je exponent, musí } b_i^m = 1.$$

2) Vídám, nenajde se menší exponent?

Využijeme uváděnou: když $a^6 \neq 1$, pak nebo $a^2 = 1$ nebo $a^3 = 1$.

$$\begin{aligned} \text{Když } a_i^{(p_i^{f_i})} = 1 \text{ pro nějaké } f_i < e_i, \text{ tak lze } a_i^{(p_i^{f_i})} = b_i^{\frac{(m/p_i)}{p_i^{f_i}}} = \\ = b_i^{\frac{m}{p_i^{e_i-f_i}}}, \text{ když vypočítáme } e_i - f_i = h_i \end{aligned}$$

$$\text{Ale pak: } b_i^{\frac{m}{p_i}} = b_i^{\frac{m}{(p_i^{e_i-h_i})}} \cdot p_i^{h_i-1} = 1^{p_i^{h_i-1}} = 1, \text{ což je spor s výběrem } b_i$$

Důsledek: Konečná Abelova grupa G je cyklická, právě když $\exp(G) = |G|$.

Pro jaká n je \mathbb{Z}_n^* cyklická?

Věta: Pro prvočíslo p je \mathbb{Z}_p^* cyklická.

Dk: $\exp(\mathbb{Z}_p^*) = m$. Z Eulerovy věty: $\forall a \in \mathbb{Z}_p^*: a^{|G|} = a^{\varphi(p)} = a^{p-1} = 1$, proto musí platit $m \leq p-1$.

Z vlastnosti exponenci: $\forall a \in \mathbb{Z}_p^*: a^m = 1 \Rightarrow a^{m-1} = 0$, tj. všechna a z \mathbb{Z}_p^* jsou kořeny polynomu stupni m : $x^m - 1 = 0$. Díky následujícímu lemma platí $p-1 \leq m$, dostáváme tedy $m = p-1$.

Ze předešlého tvrzení musí existovat $a \in \mathbb{Z}_p^*$, kde $r(a) = m = p-1 = |\mathbb{Z}_p^*|$, a to je generátor, proto $\mathbb{Z}_p^* = \langle a \rangle$ je cyklická.

Lemma: Nelinejný polynom má v lese nejsou všech kořenů, kolik je jeho stupně.

Dk: Důkaz provedeme indukcí podle stupně

1) $n=0$, máme polynom $P(x) = c$, kde c je konstanta. Jevně $c=0$ má nula kořenů

2) Předpokládejme, že to platí pro všechny polynomy stupně $n-1$.

Všem polynom $P(x)$ stupně n , můžou nastat dvě varianty:

- $P(x)$ nemá kořen, pak lemma platí

- $P(x)$ má kořen c , pak ho vypíšeme na $P(x) = (x-c) \cdot Q(x)$, kde $Q(x)$ má stupně nejsouší $n-1$. Když d byl kořen $P(x)$, tj. $P(d) = 0 = (d-c) \cdot Q(d)$, tak díky lomu, že jsme v lese a nemáme dělitelné nuly, máme dvě varianty:

- $(d-c) = 0$ Pak $d=c$ a $P(x)$ má $(n-1) \neq 1 = n$ kořenů

- $P(d) = 0$, Pak $P(x)$ má stejně kořenů jako $Q(x)$, tj. $n-1$ kořenů. } je nejsouší n .

Pozn: Pro polynomy nad okruhem \mathbb{Z} neplatí, např: $x^2 - 1 = 0 \Leftrightarrow \mathbb{Z}_8$.
 $x^2 - 1 = (x+1)(x-1)$, ale nemůžeme říct $x_1 = 1, x_2 = -1$. V \mathbb{Z}_8 jsou totiž děliteli nuly,
 $2 \times 4 = 8 = 0$, proto by bylo řešením i $x = \pm 3$.

Můžeme ho řešit tak, že $x^2 - 1 = 0$ převédeme na $x^2 = 1$, tj. vlastně hledáme invese k x ,
 Taže inverse myslíme lze v \mathbb{Z}_8^* , řešení jsou $\{\pm 1, \pm 3\}$.

Věta: Grupa \mathbb{Z}_n^* není cyklická pro každé složené číslo $n = n_1 \cdot n_2$, kde $2 < n_1 < n_2$,
 a $\gcd(n_1, n_2) = 1$. V tomto případě je $\exp(\mathbb{Z}_n^*) = \text{lcm}(\exp(\mathbb{Z}_{n_1}^*), \exp(\mathbb{Z}_{n_2}^*)) < \frac{n+1}{2}$.

Dk: Dle slyškového isomorfismu $\mathbb{Z}_n^* \cong \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$ platí $a \leftrightarrow (a_1, a_2)$.
 $\chi(a) = \text{lcm}(\chi(a_1), \chi(a_2))$, $\exp(\mathbb{Z}_n^*) = \text{lcm}(\exp(\mathbb{Z}_{n_1}^*), \exp(\mathbb{Z}_{n_2}^*))$.

Plati $\exp(\mathbb{Z}_n^*) = |\mathbb{Z}_n^*| = \varphi(n)$?

$\exp(\mathbb{Z}_n^*) \leq \text{lcm}(|\mathbb{Z}_{n_1}^*|, |\mathbb{Z}_{n_2}^*|)$. Jelikož $\exp(\mathbb{Z}_{n_1}^*) / \exp(\mathbb{Z}_{n_2}^*)$ a obrácení lamy, tak
 $\text{lcm}(\exp(\mathbb{Z}_{n_1}^*), \exp(\mathbb{Z}_{n_2}^*)) / \text{lcm}(|\mathbb{Z}_{n_1}^*|, |\mathbb{Z}_{n_2}^*|)$.

Proto $\exp(\mathbb{Z}_n^*) \leq \text{lcm}(|\mathbb{Z}_{n_1}^*|, |\mathbb{Z}_{n_2}^*|) = \text{lcm}(\varphi(n_1), \varphi(n_2))$

Z toho $\exp(\mathbb{Z}_n^*) = |\mathbb{Z}_n^*| = \varphi(n) = \varphi(n_1) \cdot \varphi(n_2)$

Pro $2 < n_1 < n_2$ jsou $\varphi(n_1), \varphi(n_2)$ sudá, tedy soudělná

Kromě $n = 2 \cdot n_1$, kde n_1 je liché, $\exp(\mathbb{Z}_n^*) = \text{lcm}(1, \exp(\mathbb{Z}_{n_1}^*)) = \exp(\mathbb{Z}_{n_1}^*)$

Důsledek: $\mathbb{Z}_{2p^e}^*$, kde p je liché prvočíslo, je cyklická.

$\exp(\mathbb{Z}_{2p^e}^*) = \exp(\mathbb{Z}_{p^e}) = |\mathbb{Z}_{p^e}| = \varphi(p^e) = \varphi(2) \cdot \varphi(p^e) = \varphi(2p^e)$
 ↓ dokážeme to protě.

Shrnutí: Grupa \mathbb{Z}_n^* je cyklická iff $n = 1, 2, 4, p^e, 2 \cdot p^e$, kde p je prvočíslo a $e \in \mathbb{N}^+$.

Cvičení Grupy \mathbb{Z}_n^* - řády prvků, podgrupy, rovnice $x^k = 1$

Pr: Mějme grupu $(\mathbb{Z}_{25}^*, \cdot)$

a) Určete velikost, najděte všechny prvky

$$|\mathbb{Z}_{25}^*| = \varphi(25) = \varphi(5) = 5^2 - 5^1 = 25 - 5 = 20$$

$$\mathbb{Z}_{25}^* = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$$

b) Určete řád $b = 6$, spočtěte $b^{57} \text{ v } \mathbb{Z}_{25}$

Řád dělí velikost grupy, kandidáti jsou: $1, 2, 4, 5, 10, 20$

$$1? \quad 6^1 = 6 \quad \times$$

$$2? \quad 6^2 = 36 = 11 \quad \times$$

$$4? \quad 6^4 = (6^2)^2 = 11^2 = 121 = 21 \quad \times$$

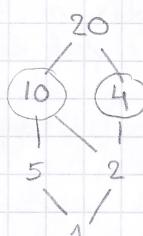
$$5? \quad 6^5 = 6^4 \cdot 6 = 21 \cdot 6 = 126 = 1 \quad \checkmark$$

$$6^{57} = 6^{11 \cdot 5 + 2} = 6^2 = \underline{\underline{11}}$$

$$\left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \chi(6) = 1$$

c) Najděte generátor \mathbb{Z}_{25}^*

Hledám a , aby $a^{20} = 1$



Hačkujte ověřit, že $a^{10} \neq 1$
 $a^{4} \neq 1$, pak je nutné
 $a^{20} = 1$ a $a^5 \neq 1, a^2 \neq 1$.

Ukusím $a = 2^2$

$$2^{10} = (2^2)^2 = (32)^2 = 7^2 = 49 = 24 \neq 1 \quad \checkmark$$

$$2^4 = 16 \neq 1 \quad \checkmark$$

$\chi(2) = 20$, t.j. 2 je generátor, $\mathbb{Z}_{25}^* = \langle 2 \rangle$

d) Kolik různých generátorů má řada? Jaká byla číslo, že ho najdeme?

$a = 2^k$, protože nás v \mathbb{Z}_{25}^* má výjdeť jeho mocnina druhé.

$$\mu(2^k) = \frac{\mu(2)}{\gcd(k, \mu(2))} = \frac{20}{\gcd(k, 20)} \quad \text{Hledáme generátor, chceme } \mu(2^k) = 20, \text{ takže } \gcd = 1.$$

$$\Rightarrow k \in \{1, 3, 7, 9, 11, 13, 17, 19\} = K$$

$$\text{Generátoru můžeme říct spolehlivý, protože počet čísel nesoudobných s } |\mathbb{Z}_{25}^*|, \text{ tj. } |K| = \varphi(|\mathbb{Z}_{25}^*|) = \varphi(\varphi(25)) = \varphi(20) = \varphi(4) \cdot \varphi(5) = (2^2 - 2^1) \cdot 4 = 2 \cdot 4 = 8$$

$$\text{Pravděpodobnost být do generátoru je } p = \frac{\varphi(\varphi(n))}{\varphi(n)} = \frac{8}{20} = 0.4$$

e) Najděte všechny pravky řádu 5.

Všechny lakové pravky budou ležet v 5-li prukové podgrupě, která bude mít nějaký generátor.

$$\text{Chceme: } \mu(2^k) = \frac{\mu(2)}{\gcd(\mu(2), k)} = 5, \text{ tj. } \gcd(20, k) = 4$$

$$\Rightarrow k \in \{4, 8, 12, 16\} \leftarrow 2^k \text{ možnosti 5, ale moždu jen generátor a ne generátory, kde je to hodit v (f)}$$

$$P_5 = \langle 2^4 \rangle = \langle -4 \rangle = \{-4 = 21, -4^2 = 16, -4^3 = 16 \cdot (-1) = -64 = 11, -4^4 = 11 \cdot (-1) = -44 = 6, -4^5 = 6 \cdot (-1) = -24 = 17\} = \{1, 6, 11, 16, 21\} \leftarrow \text{máme tu dležku, protože } 2^4 \neq -1, \text{ ale rádi si ji říkáme generátor,}\text{ když je to nějaký generátor.}$$

Všechny pravky v P_5 o výšce 1 jsou řádu 5 ($|K|=5$, ale $|P_5|=5$)

f) Vyřešte $x^5=1$ a $x^8=1$

$x^5=1$ lze řešit dle EulEROVY věty řešit všechny pravky v P_5 větve 1, tj. $\{1, 6, 11, 16, 21\}$.

$x^8=1$ lze řešit, protože 8 nedělí 20, proto najdeme 8-mi prukovou podgrupu.

ypočítáme $\gcd(20, 8) = 4$, redukujeme normu na $x^4=1$ a hledáme 4-prukovou podgrupu.

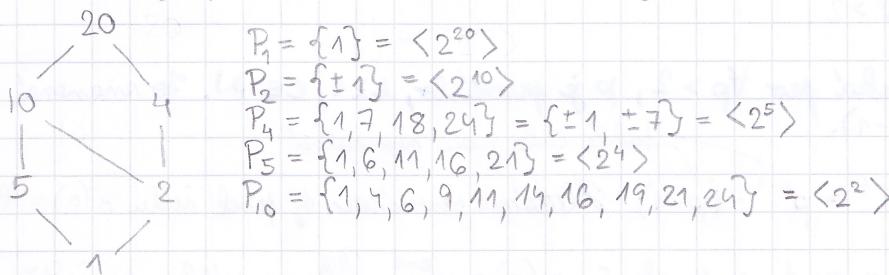
$$\mu(2^k) = \frac{20}{\gcd(20, k)} = 4 \Rightarrow \gcd(20, k) = 5 \Rightarrow k = \text{nebo 5}$$

$$P_4 = \langle 2^5 \rangle = \langle 7 \rangle = \{7, 7^2 = 49 = -1, 7^3 = (-1) \cdot 7 = -7, 7^4 = (-7) \cdot 7 = -49 = 1\} = \{1, 7, 18, 24\}$$

$x^8=1$ má řešení v P_4 .

g) Jak vypadají podgrupy?

Velikost podgrup musí musí dělit velikost grupy



Najděte podgrupy v \mathbb{Z}_{26}^* , když $x^6=1$. $|\mathbb{Z}_{26}^*| = \varphi(26) = \varphi(2) \cdot \varphi(13) = 1 \cdot 12 = 12$

Dopustné velikosti podgrup: 1, 2, 3, 4, 6, 12, nejdříve najdeme generátory \mathbb{Z}_{26}^* .

$$a = 2 ? \quad 2^6 = 64 = 12 \leftarrow \text{takže je dívá, mělo by } (a^6)^2 = 1, \text{ čekali jsme } -1.$$

$$2^4 = 16 \quad \rightarrow \text{To je dívá, mělo by } a^{16} = 1. \text{ Oba tohle } 2 \notin \mathbb{Z}_{26}^*, \text{ protože } 2 \text{ je zádečně } \leq 26. \text{ Druhý jenom nesplňuje shovávání.}$$

$$2^{12} = 144 = 1 \quad \text{protože } 2 \text{ je zádečně } \leq 26.$$

$$3^4 = 9^2 = 81 = 3$$

$$3^6 = 3^4 \cdot 3^2 = 3 \cdot 9 = 27 = 1, \text{ takže 3 nemá generátor}$$

$$a = 5 ? \quad 5^4 = 25 \equiv 25 \equiv (-1)^2 = 1 \quad \text{---} \quad 5 \quad \text{---} \quad 11 \quad \text{---}$$

$$a = 7 ? \quad 7^4 = 49^2 = (-3)^2 = 9$$

$$7^6 = 9 \cdot 7^2 = 9 \cdot (-3) = -27 = -1$$

$$7^{12} = (-1)^2 = 1$$

$$= -3$$

Rешení x^6 lze řešit v P_6 , $P_6 = \langle 7^2 \rangle = \{ \dots \} = \{1, 3, 9, 17, 23, 25\}$