

Příklad: Najděte křížkový algoritmus pro $\frac{73}{15}$ a spočtejte všechny konvergenty.

$$\frac{73}{15} = 4 + \frac{13}{15} = 4 + \frac{1}{\frac{15}{13}} = 4 + \frac{1}{1 + \frac{2}{13}} = 4 + \frac{1}{1 + \frac{1}{\frac{13}{2}}} = 4 + \frac{1}{1 + \frac{1}{6 + \frac{1}{2}}}$$

$$0: (4) = 4$$

$$1: (4, 1) = 4 + \frac{1}{1} = 5$$

$$2: (4, 1, 6) = 4 + \frac{1}{1+1/6} = 4 + \frac{1}{7/6} = 4 + \frac{6}{7} = \frac{34}{7} \approx 4.86$$

$$3: (4, 1, 6, 2) = \frac{73}{15}$$

Příklad: Proveďte Wienerův algoritmus na RSA s nezájímým klíčem (55751, 22109)

Kdyby se p a q lásily o jeden bit, tak $q < p < 2q$, $d < \frac{1}{3}\sqrt{n}$, pak by měl $\frac{e}{n}$ byl jenom s konvergencí algoritmu $\frac{k}{d}$

$$\text{Euklid: } 22109 = 0 \cdot 55751 + 22109$$

$$55751 = 2 \cdot 22109 + 11533$$

$$22109 = 1 \cdot 11533 + 10576$$

$$11533 = 1 \cdot 10576 + 957$$

$$10576 = 11 \cdot 957 + 49$$

$$957 = 19 \cdot 49 + 28$$

$$49 = 2 \cdot 26 + 23$$

$$26 = 1 \cdot 23 + 3$$

$$23 = 7 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$= \frac{1}{\frac{1}{5/2}} = \frac{2}{5}$$

$$k=2, d=5, \varphi(n) = \frac{22109 \cdot 5 - 1}{2} = 55272, \text{ to by mělo řešit}$$

$$\varphi(n) = (p-1)(q-1) = p \cdot q - (p+q) + 1 = 55751 + 1 - (p+q) = 55752 - (p+q)$$

$$p+q = 55752 - 55272 = 480$$

$$p \cdot q = 55751$$

$$x^2 - 480x + 55751 = 0 \quad D = b^2 - 4ac = 7396 = 86^2$$

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a} = \frac{480 \pm 86}{2} \leftarrow 283 \quad \leftarrow 197$$

Nášli jsme poučísla $p = 197, q = 283$ původní klíč (55751, 22109).

Přednáška
20.3.2019

Tvrzení: Nechť G je Abelova grupa a H je podgrupa v G .

- předpisem $aH \cdot bH = abH$ je abH již korektně definována operace na množině bH

- množina všech těch grup G podle podgrupy H spojuje tento operaci opět korektně grupu. Nazývá se faktorová grupa grupy G podle H a značí se G/H .

- nekomutativní grupy G lze faktorizovat jen podle normálních podgrup H , tj. jen když platí $aH = Ha$ pro všechny $a \in G$

Příklad: $(\mathbb{Z}/n\mathbb{Z}, +) = (\mathbb{Z}_n, +)$

Definice: Nechť G je Abelova grupa, H je podgrupa v G , $a, b \in G$. Řekneme, že a je kongruentní s b podle podgrupy H , $a \equiv b \pmod H$, pokud $ab^{-1} \in H$

Tvrzení: Následující tvrzení jsou ekvivalentní:

$a \equiv b \pmod H$ iff $Ha = Hb$ iff $a = hb$ pro nějaké $h \in H$.

Kongruence podle podgrupy

- Kongruence podle podgrupy je relace ekvivalence na množině G , kdy vlastní G na bázi a to jsou právě bády a H , kde $a \in G$.
- Pro Abelovu grupu máte platí, že kongruence je eachována při binární operaci, tedy binární operaci lze definovat přes reprezentanty.
- Takhle tak faktorová grupa grupy G podle kongruence modulo H , nějž je značka G/H .

Def: Nechť $(R, +, \cdot)$ je komutativní okruh. Podmnožina $I \subseteq R$ se nazývá ideál okruhu R iif:

- $(I, +)$ je podgrupa grupy $(R, +)$
- pro všechny $i \in I$ a $r \in R$ je $i \cdot r \in I$

Chceme-li vyvodit faktorský komutativní okruh, musíme povést ideál, pokud jde přes reprezentanta, korektně definovat sítání i násobení na bádách.

Když ideál $n\mathbb{Z}$ v \mathbb{Z} je kwaru $m\mathbb{Z}$ pro nějaké $m \in \mathbb{Z}$. Faktorský okruh je $(\mathbb{Z}/m\mathbb{Z}, +, \cdot) = (\mathbb{Z}_m, +, \cdot)$ struktuře slyškaných čísel modulo m .

Připomínání Lagrangeovy věty: Takhle podgrupy je dělitelom velikosti grupy

Def: Nechť (G_1, \cdot) , (G_2, \circ) jsou grupy. Zobrazení $f: G_1 \rightarrow G_2$ nazývá grupový homomorfismus, pokud pro všechna $a, b \in G_1$ platí:

$$f(a \cdot b) = f(a) \circ f(b)$$

$$f(1) = 1$$

$$f(a^{-1}) = f(a)^{-1}$$

Tracení: Nechť (G_1, \cdot) , (G_2, \circ) jsou grupy. Zobrazení $f: G_1 \rightarrow G_2$ je grupový homomorfismus, právě když $f(a \cdot b) = f(a) \circ f(b)$

Dk: 1) f respektuje neutralitu

\forall grupě je neutralní jediný idempotentní prvek, tedy jediný, kde $e^2 = e$. To plyne a toto, že když je rovnice $g^2 = g$ a my násobíme ji sprava g^{-1} , dostaneme $g^1 = g \cdot g^{-1} = e$.

Ukážeme, že $f(1)$ je idempotent v G_2 :

$$f(1)^2 = f(1) \circ f(1) = f(1 \cdot 1) = f(1), \text{ my násobíme sprava inverzí } \Rightarrow f(1) = f(1) \cdot f(1)^{-1} = 1$$

2) f respektuje inverse - pokud ano, jejich binární operace bude 1

$$f(a) \circ f(a^{-1}) = f(a \cdot a^{-1}) = f(1) = 1$$

3) Kladny homomorfismus: Pro grupy G_1, G_2 , Abelianu grupu G a podgrupu H

- Minimální homomorfismus: $f: G_1 \rightarrow G_2 : g \mapsto 1$

- projekce na bádu: $\pi: G \rightarrow G/H : a \mapsto aH$

- inverzí: $i: H \rightarrow G$

- exponenciální zobrazení: $f: (\mathbb{Z}, +) \rightarrow G : z \mapsto a^z$ pro $a \in G$

$$f(z_1 + z_2) = a^{z_1 + z_2} = a^{z_1} \cdot a^{z_2} = f(z_1) \cdot f(z_2) \quad \checkmark$$

- m-krátká mocnina: $f: G \rightarrow G : a \mapsto a^m$, G je Abelova grupa

$$f(a_1 \cdot a_2) = (a_1 \cdot a_2)^m = \underbrace{a_1 \cdot a_2 \cdot a_1 \cdot a_2 \cdots a_1 \cdot a_2}_{m-\text{krať}} = \underbrace{a_1 \cdot a_1 \cdots a_1 \cdot a_2 \cdot a_2 \cdots a_2}_{m-\text{krať}} =$$

$$= a_1^m \cdot a_2^m = f(a_1) \cdot f(a_2) \quad \text{Toto platí jen pro Abelovu grupu, potéže je komutativní.}$$

- Číselský algebraický homomorfismus: Ten je očekáváno obecnou izomorfismus

Def: Nechť $(G_1, \cdot), (G_2, \circ)$ jsou grupy. Grupouj homomorfismus, který je zároveň
zájemně jednoznačným odkazem, se nazývá grupouj izomorfismus.

Tvrzení: Nechť $n = \prod_{i=1}^k p_i^{e_i}$, kde prvočísla p_i jsou navzájem kóma. \leftarrow Číslo slyšitelné
Zobrazení $\theta: \mathbb{Z}_n \rightarrow \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \dots \times \mathbb{Z}_{p_k^{e_k}} : a \mapsto (a_1, \dots, a_k)$, kde $0 \leq a_i < p_i^{e_i}$,
splňují $a_i \equiv a \pmod{p_i^{e_i}}$, je grupouj isomorfismus adičních grup $\mathbb{Z}_n \cong \prod_{i=1}^k \mathbb{Z}_{p_i^{e_i}}$. \leftarrow homomorfismus

Resstrukce zobrazení θ na množinu \mathbb{Z}_n^* je grupouj izomorfismus multiplicativních
grup: $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \mathbb{Z}_{p_2^{e_2}}^* \times \dots \times \mathbb{Z}_{p_k^{e_k}}^*$.

Nechť $(R_1, +, \cdot), (R_2, +, \cdot)$ jsou komutativní obryhy a jednotky. Zobrazení $f: R_1 \rightarrow R_2$
je nazývá obrysovou homomorfismus, pokud je to grupouj homomorfismus adičních
grup a respektuje násobení a jednotkový prvek.

- $f(a+b) = f(a) + f(b)$
- $f(a \cdot b) = f(a) \cdot f(b)$
- $f(1) = 1$

Tvrzení: Nechť G je Abelova grupa, H_1, H_2 jsou její podgrupy. Potom $H_1 \cap H_2 = \{1\}$,
tak $H_1 \times H_2 \cong H_1 \cdot H_2$, a zobrazení $f: H_1 \times H_2 \rightarrow H_1 \cdot H_2 : (h_1, h_2) \mapsto h_1 \cdot h_2$ je grupouj
izomorfismus.

Dk: 1) Je to homomorfismus?

$$f((h_1, h_2), (h'_1, h'_2)) = f(h_1 \cdot h'_1, h_2 \cdot h'_2) = h_1 \cdot h'_1 \cdot h_2 \cdot h'_2$$

$$f(h_1, h_2) \cdot f(h'_1, h'_2) = (h_1 \cdot h_2)(h'_1 \cdot h'_2) = h_1 \cdot h_2 \cdot h'_1 \cdot h'_2$$

Chceme, aby se výrazy výše shodovaly. Můžeme říct, že se opravdu shodují, protože platíme
v Abelových grupách a kdy platí komutativita.

2) Je majemně jednoznačný?

- na: f je zjednodušená, protože pro každé $h_1, h_2 \in H_1 \cdot H_2$ máme moc (h_1, h_2) ,
který vždy existuje
- prosté použijeme koreni: f je prosté \iff je jádro triviale (je v něm jen jednotka e)

$$\text{Ker } f = \{(h_1, h_2) \in H_1 \times H_2 \mid f(h_1, h_2) = 1\}$$

$$f(h_1, h_2) = h_1 \cdot h_2 = 1$$

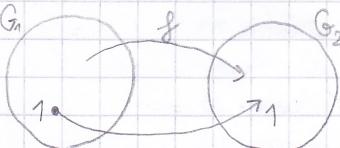
$$h_1 = h_2^{-1}$$

V jádru by mohly být jiné funkce, které jsou navzájem invertibilní. My ale máme,
že $H_1 \cap H_2 = \{1\}$, proto jediná možná dvojice v jádru je $(1, 1)$. Jádro je triviale,

když zobrazení je prosté a lze i izomorfismus.

Tvrzení: Homomorfismus je prostý, právě když je jádro triviale.

Dk: $G_1 \xrightarrow{f} G_2$ " \Rightarrow " f je homomorfismus, když $f(1) = 1$, když $1 \in \text{Ker } f$.



Když pro $a \neq b$ platilo $f(a) = f(b) = 1$, pak je to
ve sporu s tím, že f je prosté.

" \Leftarrow " Dokážu obrněně: Když by prosté' nebylo, tj. $\exists a, b, c \neq b, a \neq c$ takže $f(b) = f(c)$, takže:
 $f(b \cdot c^{-1}) = f(b) \circ f(c^{-1}) = 1$, protože $b \cdot c^{-1}$ leží v jádru spolu s 1 , proto jádro nemá triviale.

Důsledek: $H_1 \times H_2 \cong H_1 \cdot H_2$, pak $|H_1 \times H_2| = |H_1| \cdot |H_2|$, kde $H_1 \cdot H_2$ je nazývá
mitinou direktní součin. (když existuje izomorfismus, pak jsou stejně velké), $H_1 \cap H_2 = \{1\}$

Příklad: Když je $g \in G$ je jednoznačně napořádatý jako $g = h_1 \cdot h_2$, $h_1 \in H_1$, $h_2 \in H_2$

Definice: Nechť $f: G_1 \rightarrow G_2$ je grupouj homomorfismus.

- Obraz f je množina $\text{Im } f = \{b \in G_2; b = f(a) \text{ pro nějaké } a \in G_1\}$
- Jádro f je množina $\text{Ker } f = \{a \in G_1; f(a) = 1\}$

$$\text{Príklad: } \mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

$$H_1 = \{\pm 1\} = \{1, 14\}$$

$$H_2 = \langle 2 \rangle = \{2, 4, 8, 16\} = \{1, 2, 4, 8\}$$

$$H_1 \cap H_2 = \{1\} \quad \checkmark$$

$$H_1 \cdot H_2 = \{1, 2, 4, 8, 14, 28, 56, 112\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

$$|H_1| = 2, |H_2| = 4, |H_1 \cdot H_2| = |H_1| \cdot |H_2| = 2 \cdot 4 = 8 \quad \checkmark$$

	1	14
1	1	14
2	2	13
4	4	11
8	8	7

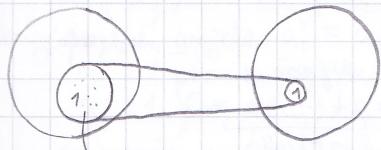
Tvrzení: Nechť $f: G_1 \rightarrow G_2$ je grupový homomorfismus.

- $\text{Ker } f$ je podgrupa grupy G_1 (dokonce normální podgrupa). Až $a \in \text{Ker } f = \text{Ker } f \cdot a$, tedy G)
- $\text{Im } f$ je podgrupa grupy G_2
- Obraz podgrupy je podgrupa
- Uzor podgrupy je podgrupa
- f je prostý homomorfismus iff $\text{Ker } f = \{1\}$

→ větu dokážeme pouze pro Abeliané grupy

1. věta o isomorfismu: Nechť $f: G \rightarrow G'$ je grupový homomorfismus. Pak $G/\text{Ker } f \cong \text{Im } f$. Speciálně zobrazení $\varphi: G/\text{Ker } f \rightarrow G': a \cdot \text{Ker } f \mapsto f(a)$ je prostý grupový homomorfismus, jehož obrazem je $\text{Im } f$.

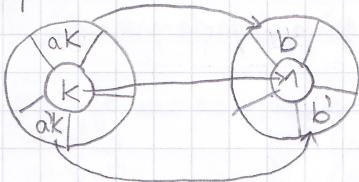
Dk:



$$(3) a, b \in K \Rightarrow ab \in K ?$$

Předpokládejme, že $a, b \in K$. Z vlastnosti homomorfismu plyne, že $f(a \cdot b) = f(a) \cdot f(b)$:
 $1 = f(a) \cdot f(b) = f(a \cdot b)$, tedy $f(a \cdot b) = 1$, což znamená, že $a \cdot b$ patří k K .

Grupa G se rozdělí na několik částí, které homomorfismus zachová.



$$\begin{aligned} f(a) &= b \\ f(x) &= b \text{ pro } x \in aK \end{aligned}$$

Všechny prvky $x \in aK$ se odváží na stejný prvek $b \in G'$

Chci ukázat, že $f(a) \neq f(a')$, když v tom, že $aK \cap a'K = \emptyset$.

Když $f(a) = f(a')$, tak $f(a) \cdot f(a')^{-1} = 1$, a toto díky vlastnostem homomorfismu znamená, že $f(a \cdot a'^{-1}) = 1$, tedy $f(a \cdot a'^{-1}) \in K$.

Označme $a \cdot a'^{-1} = k$. Pak $a = k \cdot a' = a'k$, ale toto znamená, že $a \in a'K$, což je spor.

Zobrazení $\varphi: G/K \rightarrow G': aK \mapsto f(a)$ je bijekce na $\text{Im } \varphi$ a laky homomorfismus, tedy to je isomorfismus.

Není $|aK| = |K| = |\alpha K|$, tedy $\forall b \in \text{Im } f$ mají stejně rozměr.

Uloha $f(x) = b$ (nejít všechny možné b) má řešení ve formě $x = a \cdot c$, kde a je partikulární řešení a $c \in K$ je homogenní řešení $f(x) = 1$.

To je stejně jako řešení soustavy lin. rovníc $x = a + c$

Nechť G je Abelova grupa, pak $\rho: G \rightarrow G: a \mapsto a^m$ je grupový homomorfismus.

- $\text{Ker } \rho = \{a \in G \mid a^m = 1\} = \overline{G^1}^m$, což je množina všech m-lých odmocin, kouč podgrupy grupy G .

- $\text{Im } \rho = \{a^m, a \in G\} = G^m$, množina všech m-lých mocien, kouč podgrupy G .

- $G/\text{ker } \rho \cong \text{Im } \rho$ a příslušný izomorfismus je $\varphi: a\text{ker } \rho \mapsto a^m$

- Tedy každý prvek v G^m má stejně moc m-lých odmocin. Najdeme-li jedno řešení rovnice $x^m = b$, označme je a , pak každá řešení má tvar $x = a \cdot c$, kde c je nějaké řešení rovnice $x^m = 1$, $b \in G^m$.

Počle Eulerový věty v grupě platí, že $a^n = 1$, kde n je velikost grupy, pro všechny $a \in G$. Pro konkrétní a ale nemusí platit, že n je nejméně exponent, kdežto dle 1.

Definice: Nechť (G, \cdot) je grupa s neutrálním 1, $a \in G$. Nejménší $n \in \mathbb{N}$ takový, že $a^n = 1$ v grupě G , se nazývá říd protok a v G , označme $r(a) = n$. Pokud takové n neexistuje, má a nekonečné říd.

Příklad: $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ $|\mathbb{Z}_9^*| = \varphi(9) = \varphi(3^2) = 6$
 $r(8) = 2, r(4) = 3, r(2) = 6, r(-1) = 2$
 $r(-1 \cdot h) = r(-h) = r(5) = r(-1) \cdot r(4) = 2 \cdot 3 = 6$

Poznámky:

- Každý větme, že $a^{r(a)} = 1$, můžeme při výpočtu a^k sjednodušit exponent $a^{k \bmod r(a)}$
- Je-li grupa abelián, pak $r(a)$ je nejménší r. takové, že $a \cdot a = \underbrace{a + \dots + a}_{k \text{ krát}} = 0$
- Říd protoku a v grupě G je roven řadu cyklické grupy $\langle a \rangle$

Důsledek: $r(a)/|G|$, je Lagrangeova věta

Obecná Eukleiova věta: Nechť G je konečná grupa. $\forall a \in G$ platí: $a^{|G|} = 1$

Dk: Vím, že $r(a)/|G|$.
Potom $a^{|G|} = a^{k \cdot r(a)} = (a^{r(a)})^k = 1^k = 1$

Využili jsme Lagrangeovu větu, a ta platí i pro nekomutativní grupy, proto pro ně platí i Eukleiova věta.

Tvrzení: Nechť G je konečná grupa, $a, b \in G$.

1) $a^k = 1$ v grupě G iff $r(a) | k$

2) $r(a^{-1}) = r(a)$

3) Nechť máme $a \cdot b = b \cdot a$. Pokud jsou $r(a), r(b)$ nesoudělné, pak $r(a \cdot b) = r(a) \cdot r(b)$

Dk: 1) " \Leftarrow " $r(a)/k$

$$k = r(a) \cdot l$$

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

" \Rightarrow " sporem, stiskněme $k = r(a) \cdot l + z$, kde $0 < z < r(a)$

$$1 = a^k = a^{r(a) \cdot l + z} = (a^{r(a)})^l \cdot a^z = 1^l \cdot a^z = a^z, \text{ tedy } a^z = 1$$

ale máli jsme $z < r(a)$, $a^z = 1$, a přitom by mělo být $r(a)$ nejménší takové číslo, proto máme spor, $r(a)$ musí delít k .

2) Označme $r(a) = r$

$$(a^{-1})^r = a^{-r} = (a^r)^{-1} = 1^{-1} = 1, \text{ takže vidíme, že } (a^{-1})^{r(a)} = 1$$

Jde o nejménší takové r^2 .

Amo, neboť $a = (a^{-1})^{-1}$

Když $(a^{-1})^s = 1$ pro $s < r$, tak by $a^s = ((a^{-1})^{-1})^s = ((a^{-1})^s)^{-1} = 1^{-1} = 1$

Což je spor s větou, že $r(a) = r$, $s < r$.

$$3) (a \cdot b)^{r(a) \cdot r(b)} = \underbrace{(ab \cdot ab \cdot ab \cdots ab)}_{r(a) \cdot r(b) \text{ kрат}} = (a \cdots a \cdot b \cdots b) = a^{r(a) \cdot r(b)} \cdot b^{r(a) \cdot r(b)} = \\ = (a^{r(a)})^{r(b)} \cdot (b^{r(b)})^{r(a)} = 1^{r(b)} \cdot 1^{r(a)} = 1 \cdot 1 = 1$$

Takže jste chtěli, ale je $r(a) \cdot r(b)$ nejmenší takový exponens?

Když $(a \cdot b)^s = 1$, $s < r(a) \cdot r(b)$
 $(a \cdot b)^s = 1$ množinou na $r(a)$
 $(a \cdot b)^{r(a) \cdot s} = 1^{r(a)}$

$$1 = (a \cdot b)^{r(a) \cdot s} = a^{r(a) \cdot s} \cdot b^{r(a) \cdot s} = 1 \cdot b^{r(a) \cdot s} = b^{r(a) \cdot s}$$

Odešroumí 1) platí $r(b)/r(a) \cdot s$. A protože $\gcd(r(a), r(b)) = 1$, musí mít $r(b)/s$, obdobně dostaneme $r(a)/s$.

s je společný násobek $r(a)$, $r(b)$ a chceme, aby byl nejmenší. Z neoddelitelnosti $r(a), r(b)$: $\text{lcm}(r(a), r(b)) = r(a) \cdot r(b)$.

Takže když $r(a) \cdot r(b)/s$, můžeme mít $r(a) \cdot r(b) \leq s$, tedy $r(a) \cdot r(b)$ je nejmenší možný exponens.

TVRZENÍ: Nechť G_1, G_2 jsou konečné grupy, $(a_1, a_2) \in G_1 \times G_2$. Pak $r(a_1, a_2) = \text{lcm}(r(a_1), r(a_2))$

Dk: $(a_1, a_2)^r = (a_1^r, a_2^r)$, když můžeme díky operacím na $G_1 \times G_2$ se výpočítat

Když poprvé vypadne $a_1^r = a_2^r = 1$?

$$a_1^r = 1 \text{ pro } r(a_1)/r$$

$$a_2^r = 1 \text{ pro } r(a_2)/r$$

Chci nejmenší r , když splní vlastnosti výše, a to je $\text{lcm}(r(a_1), r(a_2))$.

TVRZENÍ: Nechť G je konečná群, $a \in G$. Pak $r(a^k) = \frac{r(a)}{\gcd(k, r(a))}$

Dk: Předpokládám nejmenší bladnou s , kde $(a^k)^s = 1$, t.j. $a^{ks} = 1$, proto $r(a)/k \cdot s$

Máme zadání $k, r(a)$. $k \cdot s = l \cdot r(a)$, kde $l \cdot r(a)$ je společný násobek $k, r(a)$.

Chci, aby bylo $k \cdot s$ co nejmenší, proto $k \cdot s = \text{lcm}(k, r(a))$.

Použijeme morec: $\text{lcm}(A, B) = \frac{A \cdot B}{\gcd(A, B)}$; $\text{lcm}(k, r(a)) = \frac{k \cdot r(a)}{\gcd(k, r(a))} = k \cdot s$, t.j. $s = \frac{r(a)}{\gcd(k, r(a))}$

Pr: proč je morec výše správný?

$$A = 2 \cdot 3^2 \cdot 5$$

$$\gcd(A, B) = 2 \cdot 3$$

$$B = 2^3 \cdot 3 \cdot 7$$

$$\text{lcm}(A, B) = 2^3 \cdot 3^2 \cdot 5 \cdot 7$$

$$\text{lcm}(A, B) = \frac{A \cdot B}{\gcd(A, B)} = \frac{2^4 \cdot 3^3 \cdot 5 \cdot 7}{2 \cdot 3} = 2^3 \cdot 3^2 \cdot 5 \cdot 7$$

Multiminoing: můžou obsahovat jeden prvek na více řádcích.

$$A = \{2, 3_1, 3_2, 5\}$$

$$B = \{2_1, 2_2, 2_3, 3, 7\}$$

lcm a \gcd se chovají jako \cup a \cap na multiminoích

$$\text{lcm}(A, B) = A \cup B$$

$$\gcd(A, B) = A \cap B$$

$A \cdot B$ přidá prvek do nových řádců multimino, A/B odstraní prvek $B \in A$.

TVRZENÍ: Když $d/r(a)$, pak $r(ad) = \frac{r(a)}{d}$

Pr: Pracujeme s $\mathbb{Z}_8^* = \{1, 2, 4, 5, 7, 8\}$

$$r(2) = 6, \text{ t.j. } 2^6 \equiv 1 \text{ poprvé}$$

$$r(4) = r(2^2) = \frac{r(2)}{2} = \frac{6}{2} = 3$$

$$(2^2)^s = 1 \text{ poprvé}, \text{ můžeme } 2 \cdot s = 6 \Rightarrow s = 3$$

$$\langle 2 \rangle = \{2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16 = 7, 2^5 = 2^4 \cdot 2 = 7 \cdot 2 = 14 = 5, 2^6 = 5 \cdot 2 = 10 = 1\} = \\ = \{2, 4, 8, 7, 5, 1\} = \mathbb{Z}_8^*, |\langle 2 \rangle| = 6$$

Důsledek: $n(a^k) = n(a)$ právě když $\gcd(k, n(a)) = 1$
 cyklická podgrupa $\langle a \rangle$ má celkem $\varphi(n(a))$ generátorů.

Def: Grupa G se nazývá cyklická grupa, pokud pro nějaký prvek $a \in G$ je $G = \langle a \rangle$.
 Prvek a je generátor grupy.

Príklad: Našli jsme, že v grupě \mathbb{Z}_q^* je generátor 2. Je tam i jiné a, aby $|Ka| = 6$?

$a = 2^k$, protože všechny prvky v \mathbb{Z}_q^* můžeme vyjádřit jako mocniny dvojkdy

$$n(2^k) = \frac{n(2)}{\gcd(k, n(2))} = \frac{6}{\gcd(k, 6)} \quad \text{Chceme, aby } n(2^k) = 6, \text{ proto musí platit } \gcd(k, 6) = 1.$$

To lude platit pro $k \in \{1, 5\}$, takže generátory \mathbb{Z}_q^* jsou $2^1 = 2$ (vžimne) a $2^5 = 5$.

\Rightarrow cyklická grupa \mathbb{Z}_q^* má dvě možnosti, jak zvolit generátor.

Obecně: Pokud je \mathbb{Z}_n^* cyklická, tak má kolik generátorů, kolik je rozdílných prvků $\varphi(|G|)$, což je $\varphi(\varphi(n)) = \varphi(\varphi(n))$. Pozor, n je základ grupy, ne počet prvků v ní.

Tvrzení: 1) Cyklické grupy jsou Abeliány.

2) konečná grupa řádu n je cyklická \Leftrightarrow obsahuje prvek řádu $n(a) = n$.

3) cyklická grupa řádu n má $\varphi(n)$ generátorů. Důvod: podle výše, že při náhodné volbě prveku $a \in G$ nejdeme generátor, je $\frac{\varphi(n)}{n}$.

Tvrzení: Prvek $a \in G$ je generátor, konečné grupy G řádu n právě když je obsahena následující

2 podmínky: 1) $a^r \neq 1$ pro $\forall r < n$, r/n

2) $a^r \neq 1$ pro $\forall r = \frac{n}{p}$, kde p je prvočíslo a $p \mid n$

Príklad: Grupy $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$ jsou cyklické s generátorem 1.

$$\mathbb{Z}_5^* = \{1, 2, 4, 5, 7, 8\}, (\mathbb{Z}_5^*, \cdot) \text{ je cyklická s generátorem 2.}$$

$$\mathbb{Z}_3^* = \{1, -3\}, (\mathbb{Z}_3^*, \cdot) \text{ není cyklická, protože } \forall a: a^2 = 1, \text{ ale } |G|=4.$$

Príklad: Je daná grupa $\mathbb{Z}_{19}^* = \mathbb{Z}_{19} - \{19\}$

Najděte generátor

$$\begin{aligned} \text{pro řád generátoru musí platit } n(a) = |G| = 18 \\ \text{pravděpodobnost, že trefíme generátor, je: } p = \frac{\varphi(|G|)}{|G|} = \frac{\varphi(18)}{18} = \frac{\varphi(2) \cdot \varphi(9)}{18} = \\ = \frac{1 \cdot (3^2 - 3)}{18} = \frac{6}{18} = \frac{1}{3} \end{aligned}$$

O řádu víme, že dělí velikost grupy. Možné řády jsou: 1, 2, 3, 6, 9, 18. Zvolíme nějaké a a budeme ho umocňovat na tyto řády. Chceme, aby vyslo $a^k = 1$ jen pro $k = 18$.

Ukánujme $a=2$

$$2^1 = 2 \quad \checkmark$$

$$2^2 = 4 \quad \checkmark$$

$$2^3 = 4 \cdot 2 = 8 \quad \checkmark$$

$$2^6 = (2^3)^2 = 8^2 = 64 = 7 \quad \checkmark$$

$$2^9 = 2^{6+3} = 8 \cdot 7 = 56 = -1 \quad \checkmark$$

} první k , pro které $a^k = 1$, lude skutečně $k=18$,
 tj. $a=2$ je generátor.

Jak si mohou počítat? Když $a^6 \neq 1$, mohlo by $a^3 = 1$?

$$\text{Ne, protože } a^6 = (a^3)^2 = 1^2 = 1.$$

Když ověřujeme mocniny a, nemusíme ukončit vše, stačí vyskočit nevětší delitele.



Ukálu vyskočit, že $a^6 \neq 1$ a $a^9 \neq 1$, a pak už ně lude
 a generátor.

Náležíte $n(8)$ nebo \mathbb{Z}_{19}^* .

$n(8) = n(2^3)$, $n(2) = 18$, $d = 3$. Prostředí $n(a)$ je dělitelné d, takže $n(a^d) = \frac{n(a)}{d}$

$$n(2^3) = \frac{n(2)}{3} = \frac{18}{3} = 6$$

Spočtěte 8^{195} nebo \mathbb{Z}_{19}^*

Využijeme volej, že $n(8) = 6$, a že $8^{n(8)} = 1$

$$8^{195} = 8^{180+12+3} = 8^{6 \cdot 30 + 8^2 + 3} = 8^{0+0+3} = 8^3 = 64 \cdot 8 = 7 \cdot 8 = 56 = 18$$

Najděte 9-ti prvních prvků podgrupy nebo \mathbb{Z}_{19}^*

$$P_9 = \langle b \rangle, \text{ kde } n(b) = 9.$$

Prostředí 2 je generátorem, $b = 2^k$ pro nějaké k , aby $(2^k)^9 = 1$ poprvé.

$$(2^k)^9 = 2^{k \cdot 9} = 2^{18} \approx k=2$$

$$b = 2^2 = 4$$

$$\begin{aligned} P_9 = \langle b \rangle &= \{4\}, 4^2 = 16, 4^3 = 16 \cdot 4 = 64 = 7, 4^4 = 4^3 \cdot 4 = 7 \cdot 4 = 28 = 9, 4^5 = 9 \cdot 4 = 36 = 17, \\ 4^6 &= 17 \cdot 4 = 68 = 11, 4^7 = 11 \cdot 4 = 44 = 6, 4^8 = 6 \cdot 4 = 24 = 5, 4^9 = 5 \cdot 4 = 20 = 1 \} = \\ &= \{1, 4, 5, 6, 7, 9, 11, 16, 17\} \end{aligned}$$

Grupy, podgrupy, grupové homomorfismy

Cvičení
21.3.2019

Příklad: $G = \{a, b, c, d\}$, $(G, *)$ je Abelova grupa, s operací $*$ zadánou v tabulkách. Doplňte chybějící hodnoty do tabulky, aby $(G, *)$ měla Abelovou grupu.

	a	b	c	d
a	a ¹	b ²	c ³	d ⁴
b	b ²	a ⁵	d ³	c ¹
c	c ³	d ⁵	a ²	b ⁴
d	d ⁴	c ⁵	b ³	a ²

$$1: a \cdot b = b \cdot a = b$$

2: v každém řádku a sloupci je každý prvek jen jednou. Poch a tedy může mít význam $d \cdot d = a$

$$3: obdobně c \cdot d = b \quad c \cdot d \cdot c = b$$

4: v G musí být neutralní, kterým může být jidině a

5: doplníme d a c do tabulky, aby byl každý prvek v každém řádku / sloupci

Zobrazení $G \rightarrow G: x \mapsto a \cdot x$ musí být bijemce, když má každý prvek v sloupcích mít význam

Máme kompletní tabulku. Jednotkový je prvek a, inverse jsou $b^{-1} = b$, $c^{-1} = c$, $d^{-1} = d$.

Příklad: (G') je Abelova grupa. Zkážete, že máloždíří množina tvorí podgrupu:

a) $G^m = \{a = g^m; g \in G\}$

test 3x1

$a, b \in G^m \Rightarrow a = g_1^m, b = g_2^m$. Pokud $ab^{-1} \in G^m$, tak G^m je podgrupa

$$b^{-1} = (g_2^m)^{-1} = \overline{g_2^{-m}} = (g_2^{-1})^m$$

přitom g_2^{-1} leží v G' , $g_1 \cdot g_2^{-1}$ taky leží v G'

$$a \cdot b^{-1} = g_1^m \cdot (g_2^{-1})^m = \underbrace{g_1 \cdot g_1 \cdot \dots \cdot g_1}_{m \text{ krát}} \cdot \underbrace{g_2^{-1} \cdot g_2^{-1} \cdot \dots \cdot g_2^{-1}}_{m \text{ krát}} = \underbrace{g_1 g_2^{-1} \cdot \dots \cdot g_1 g_2^{-1}}_{m \text{ krát}} = (g_1 g_2^{-1})^m \in G^m$$

b) $\sqrt[m]{1} = \{a \in G; a^m = 1\} = G'$

test násobení: $a, b \in G' \Rightarrow ab \in G'$?

$$a, b \in G' \Rightarrow a^m = 1, b^m = 1. \text{ Pak } a^m \cdot b^m = 1 \cdot 1 = 1$$

$(a \cdot b)^m = ab \cdot \dots \cdot ab \cdot \dots \cdot b = a^m \cdot b^m = 1$ takže $a \cdot b \in G'$

test neutralní: $1 \in G'$?

$$1^m = 1 \cdot 1 \cdot \dots \cdot 1 = 1 \Rightarrow 1 = \sqrt[m]{1}, \text{ takže } 1 \in G'$$

test inverze: $a \in G' \Rightarrow a^{-1} \in G'$?

$$a^m = 1, \text{ protože } a \in G'. \text{ Pak } (a^{-1})^m = (a^m)^{-1} = 1^{-1} = 1, \text{ takže } a^{-1} \in G'$$

Příklad: Najděte G^m pro $G = \mathbb{Z}_5^*$ nebo $G = \mathbb{Z}_{15}^*$.

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

$$G^1 = G = \mathbb{Z}_5^*$$

$$G^2 = \{1^2 = 1, 2^2 = 4, 3^2 = 9 = 4, 4^2 = 16 = 1\} = \{1, 4\}$$

$$G^3 = \{1^3 = 1, 2^3 = 8 = 3, 3^3 = 27 = 12 = 2, 4^3 = 64 = 1\} = \{1, 2, 3, 4\}$$

$$G^4 = \{1^4 = 1, 2^4 = 16 = 1, 3^4 = 81 = 1, 4^4 = 256 = 1\} = \{1\}$$

$$\hookrightarrow 1 \cdot 1 = 1, \text{ takže je Euler-Fermatovy věty } a^4 = 1 \forall a \in \mathbb{Z}_5^*$$

$$G^5 = G^1 = \mathbb{Z}_5^*$$

G má podgrupy $\{1\}, \{1, 4\}, \{1, 2, 3, 4\}$. Najít všechny podgrupy je neknižicí nárok, ale v tomto malém případě je všechno řešitelné, řešíme načálo vše, protože:

- 1 lam můžete být všechny
- pokud 1 lam je 2, množina lam být i $2 \cdot 2 = 4$, a tím i $2 \cdot 4 = 8 = 3$
- pokud 1 lam je 3, množina lam být i $3 \cdot 3 = 9 = 4$, a tím i $4 \cdot 3 = 12 = 2$.

$$-\mathbb{Z}_5^* = \{1, 2, 4, 7, 8, 11, 13, 14\} = | \mathbb{Z}_{15}^* | = \varphi(15) = 2 \cdot 4 = 8$$

\hookrightarrow v tomto množině lze lepej počítat.

$$G^1 = G = \mathbb{Z}_{15}^*$$

$$G^2 = \{1, 2^2 = 4, 4^2 = 16 = 1, 7^2 = 49 = 4, (-7)^2 = 49 = 4, (-4)^2 = 1, (-2)^2 = 4, (-1)^2 = 1\} = \{1, 4\}$$

$$G^3 = \{1, 4 \cdot 2 = 8 = -7, 1 \cdot 4 = 4, 4 \cdot 7 = 28 = -2, 4 \cdot (-7) = -28 = 2, 1 \cdot (-4) = -4, 4 \cdot (-2) = 7, 1 \cdot (-1) = -1\} = \{1, -7, 4, -2, 2, -4, 7, -1\}$$

$$G^4 = \{1 \cdot 1 = 1, -7 \cdot 2 = 1, \dots\} = \{1\}, \text{ příští } G^m \text{ už se bude cyklotis.}$$

5 je neoddělné $\Rightarrow \varphi(15) = 8$, proto platí $|G^5| = \varphi(15) = 8$.

Perioda cyklosu se dá spočítat číslem větou o slystech, říká se tomu společný exponent grupy.
Vynáleza se Carmichaelova funkce $\lambda(15)$.

Jen v \mathbb{Z}_{15}^* i jiné podgrupy? Ano, např. $\{1, -1\} = \{1, 14\}$ a množina další.

Zobrazení m-láč možnosti $\rho_m: G \rightarrow G: x \mapsto x^m$ se bude chovat jako homomorfismus pro Abelianou grupu G (viz přednáška).

Jeho obraz je $\text{Im } \rho_m = G^m$, kernel $\text{Ker } \rho_m = \sqrt[m]{G}$

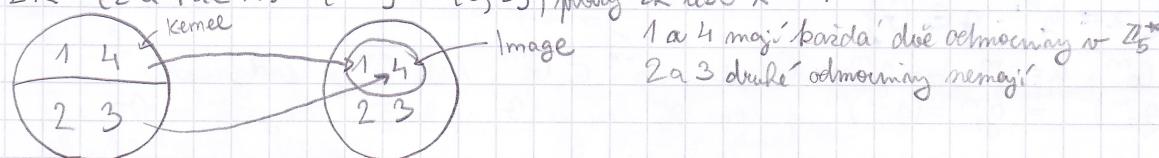
Díky první věti o izomorfismu $G/\text{Ker } \rho_m \cong \text{Im } \rho_m$, a $\text{Ker } \rho_m \rightarrow \rho(a) = a^m$

Každý $b \in G^m$ má stejnou moc m-lých odmocnin, $a^m = b$, a c , $c \in \sqrt[m]{G}$

Cílem dala pro $\rho_2: \mathbb{Z}_5^* \rightarrow \mathbb{Z}_5^*: x \mapsto x^2$

$K = \text{Ker } \rho_2 = \{a \mid a^2 = 1\} = \{1, 4\} = \{\pm 1\}$, který K řeší $x^2 = 1$

$2K = \{2 \cdot a \mid a \in K\} = \{\pm 2\} = \{2, 3\}$, prody $2K$ řeší $x^2 = 4$



1 a 4 mají každá dvě odmocniny v \mathbb{Z}_5^*

2 a 3 druhé odmocniny nemají

Faktorová grupa $\mathbb{Z}_5^*/K = \{1, 2K\}$ a množení má množinu $(ab)K = a(K)bK$

$$\begin{array}{c|cc} & 1K & 2K \\ \hline 1K & 1K & 2K \\ 2K & 2K & 4K=1K \end{array} \quad 4K = 4 \cdot \{1, 4\} = \{4, 4^2 = 16 = 1\} = \{1, 4\} = K$$

Ověření borekmosti definice nasobení

$$\begin{array}{c|cc} & 1K & 2K \\ \hline 1K & 00 & 00 \\ 2K & 00 & 00 \end{array} \quad \text{v každém čtvrti spočítané hodnoty, všechny 4 se musí shodovat}$$

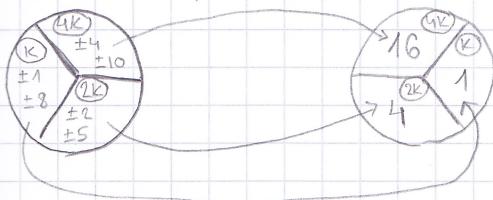
$$\begin{array}{c|cc} & 1K & 2K \\ \hline 1K & 00 & 00 \\ 2K & 00 & 00 \end{array} \quad 1. \text{ věta o izomorfismu: } \mathbb{Z}_5^*/K \cong (\mathbb{Z}_5^*)^2 = \{1, 4\}$$

$$\begin{array}{c|cc} & 1K & 2K \\ \hline 1K & 00 & 00 \\ 2K & 00 & 00 \end{array} \quad 1K = 1^2 = 1$$

$$2K = 2^2 = 4$$

Př: Máme operaci ρ_2 na \mathbb{Z}_{21}^* = {1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20}, $21=3 \cdot 7$, $\varphi(21)=12$
 $\text{Ker } \rho_2 = \{\pm 1, \pm 8\}$, možnáme dostat hrubou silou, ale mohli bychom ho dostat pomocí $\mathbb{Z}_{21} \cong \mathbb{Z}_7 \times \mathbb{Z}_3$

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



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

Je na grupě \mathbb{Z}_{21}^* grupa $K = \{\pm 1, \pm 3\}$ vnitřní direktní součinitel? (Dá se zapsat \mathbb{Z}_{21}^* jako

$$\mathbb{Z}_{21}^* = K \times H, \text{ kde } K \cap H = \{1\}, K \cdot H = \mathbb{Z}_{21}^*, \text{ tj. } |\mathbb{Z}_{21}^*| = |K| \cdot |H|.$$

$$|\mathbb{Z}_{21}^*| = |\text{Ker}| \cdot |H| \quad \Rightarrow \text{ sledujeme kryptykovou } H = \{1, 4, 16\}$$

$$12 = 4 \cdot |H|$$

$$\Rightarrow |H| = 3$$

Ano, hledaná H existuje, je to $\langle 4 \rangle$. $H = \langle 4 \rangle = \{1, 4, 16, 64=1\} = \{1, 4, 16\}$.

$$\begin{array}{c} \bullet \quad 1 \quad 4 \quad -5 \\ \begin{array}{r} 1 \quad 1 \quad 4 \quad -5 \\ -1 \quad -1 \quad -4 \quad 5 \\ \hline 8 \quad 8 \quad -10 \quad 2 \\ -8 \quad -8 \quad 10 \quad -2 \end{array} \end{array} \quad H$$

or tabulce mám celkem $12 = |\mathbb{Z}_{21}^*|$ řadmot, kdyžda je jiná, to sedí!