

## Kongruence

- existují  $a, b$  po dělení číslem  $m$  dosadou stejný zbytek  $r$ ,  $0 \leq r < m \Rightarrow a \equiv b \pmod{m}$
- $a, b \in \mathbb{Z}, m \in \mathbb{N}$  platí:
  - $a \equiv b \pmod{m}$
  - $a = b + m \cdot t$ ,  $t$  je vhodné číslo  $\in \mathbb{Z}$ .
  - $m \mid a - b$ .

Kongruence je relace ekvivalence, kt. zachovává všechny operace na algebře:  $\forall a, b, c, d \in G$  platí:

$$a \equiv b \wedge c \equiv d \Leftrightarrow \begin{aligned} a+c &\equiv b+d \\ a \cdot c &\equiv b \cdot d \\ \bar{a}^{-1} &\equiv b^{-1} \\ -a &\equiv -b \end{aligned}$$

PF1]  $\frac{20+3}{89 \cdot 4}$  vypracujte nad  $\mathbb{Z}_5$ . ( $\approx 0,065 \notin \mathbb{Z}_5$ )

$$\begin{array}{ll} \bullet 20 \equiv 0 \pmod{5} & \bullet 3 \equiv -2 \pmod{5} \\ \bullet 89 \equiv 4 \pmod{5} & \bullet 4 \equiv -1 \pmod{5} \end{array}$$

$$\frac{20+3}{89 \cdot 3} = \frac{0-2}{-7 \cdot (-7)} = -2 \equiv 3 \pmod{5}$$

Eulerova funkce - udává' počet čísel  $\leq k$ , kt. jsou menší než číslo  $m$  a zadaneční jsou s číslem  $m$  nesoudružná, tj.  $\text{NSD}(m, k) = 1$

Eulerova funkce má' tvor:  $\varphi(m) = \varphi(p_1^{n_1} \cdots p_r^{n_r}) = p_1^{n_1-1} \cdot (p_1-1) \cdots p_r^{n_r-1} \cdot (p_r-1)$   
 kde  $p_1^{n_1} \cdots p_r^{n_r}$  je rozklad čísla  $m$  na součin prvočísel.

Pr 21  $m=60$ . Zjistěte jeho Eulerova funkci.  
 $\varphi(60) = \varphi(2^2 \cdot 5 \cdot 3) = 2^{2-1} \cdot (2-1) \cdot 5^{1-1} \cdot (5-1) \cdot 3^{1-1} \cdot (3-1)$   
 $= 2 \cdot 1 \cdot 1 \cdot 4 \cdot \underline{\underline{1}} \cdot 2 = \underline{\underline{16}}$

Eulerova věta | Nechť  $m \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ .  $\text{NSD}(m, a) = 1$ .

Pak  $a^{\varphi(m)} \equiv 1 \pmod{m}$

PF3] Zjistěte zbytek po dělení čísla  $2^{17} + 3^{50}$  číslem 17.

- platí  $\text{NSD}(2, 17) = 1$  a  $\text{NSD}(3, 17) = 1$

-  $g(17) = 17^{\phi} \cdot (17-1) = \underline{\underline{16}}$

$$2^{16} \equiv 1 \pmod{17} \quad \wedge \quad 3^{16} \equiv 1 \pmod{17}$$

-  $2^{17} = 2^{16} \cdot 2 \equiv 1 \cdot 2 = 2 \pmod{17}$

-  $3^{50} = 3^{16} \cdot 3^{16} \cdot 3^{16} \cdot 3^2 \equiv 1 \cdot 1 \cdot 1 \cdot 9 = 9 \pmod{17}$

-  $2^{17} + 3^{50} \equiv 2 + 9 = 11 \pmod{17}$

$\Rightarrow$  Zbytek po dělení čísla  $2^{17} + 3^{50}$  číslem 17 je 11.

\* Využití Eukleova nebo říčky RSA - je to asymetrický sifrování v systému, kde máme sifrovaci a dešifrovaci klíče.

Postup tvorby klíčů

1) Zvolte si dvě velká náhodná prvocísla  $p$  a  $q$

2) Sčítat jejich součin  $n = p \cdot q$

3) Spouštěte Eulerova funkce  $\varphi(n) = p^{\varphi}(p-1) \cdot q^{\varphi}(q-1)$

4) Zvolíme si cele číslo  $e < \varphi(n)$  a  $\text{NSD}(e, \varphi(n)) = 1$

5) Nakreslime číslo  $d$ , aby platilo  $d \cdot e \equiv 1 \pmod{\varphi(n)}$

6) pokud je  $e$  je pročíslo  $(e-2)^{(e-2)}$ , pak  $d = \frac{1+r \cdot \varphi(n)}{e}$ , kde  
 $r = \lceil (e-1) \cdot \varphi(n) \rceil$

Práce  $p=5$ ,  $q=3$ . Sestavte klíče pro RSA.

1) ✓  
 $n = p \cdot q = 5 \cdot 3 = 15$

2)  $\varphi(n) = \varphi(15) = 5^{\varphi}(5-1) \cdot 3^{\varphi}(3-1) = 4 \cdot 2 = 8$

3)  $e = 3 \quad e < \varphi(n) \quad \wedge \quad \text{NSD}(e, \varphi(n)) = 1$

4)  $3 < 8 \quad \wedge \quad \text{NSD}(3, 8) = 1$

5)  $r = \lceil (3-1) \cdot 8^{\varphi} \rceil = 2 \cdot 8 = 16$

$d = \frac{1+16 \cdot 8}{3} = \underline{\underline{43}}$

$\Rightarrow$  platí  $43 \cdot 3 = 129 \equiv 1 \pmod{8}$

- šifrovací klíč (veřejný): dvojice čísel  $(n, e)$ , kde  $n$  modulo a  $e$  je šifrovací či veřejný exponent.
- dešifrovací klíč (soukromý): dvojice čísel  $(n, d)$ ,  $n$  - modulo a  $d$  je dešifrovací či soukromý exponent.

• Zprávu, kterou jsme převedli na číslo 8.

$$\text{šifrování: } \boxed{8^e \pmod{n}} \Rightarrow \underline{\underline{8^3 = 512 = 2 \pmod{15}}} \quad \begin{matrix} \uparrow \\ \text{zasifrovaná zpráva} \end{matrix}$$

$$\text{dešifrování: } \underline{\underline{2^d \pmod{n}}} \Rightarrow \underline{\underline{2^{43} = 8796093022208 = 8 \pmod{15}}} \quad \begin{matrix} \downarrow \\ \text{naše původní zpráva} \end{matrix}$$

### Normalní podgrupa

$N$  je normalní podgrupa grupy  $G$ , tj.  $N \trianglelefteq G \Leftrightarrow$  pro  $\forall n \in N$

a  $\forall g \in G$  platí:  $\boxed{g \cdot n \cdot g^{-1} \in N}$

- Obecně neplatí, že každá podgrupa je normalní.

- V komutativní grupě jsou všechny její podgrupy normální.  
 $g \cdot n \cdot g^{-1} = g \cdot g^{-1} \cdot n = 1 \cdot n = \underline{\underline{n}} \in N$   
komutativita

Příklad Máme grupu  $G = \{(a, b) ; a, b \in \mathbb{Z}\}$  s operací sčítání,  
 $+ : (a, b) + (c, d) = (a+c, b+d)$

- zjistěte zda podgrupa  $H = \{(i, j) ; 13 | 3i + 5j\}$  je normální?

1) spočítatme inverzní prvek k prvku  $(a, b) \in G$ .

$$(a, b) + (c, d) = (0, 0)$$

$$(a+c, b+d) = (0, 0)$$

$$\begin{array}{lcl} a+c=0 & \wedge & b+d=0 \\ c=-a & \wedge & d=-b \end{array}$$

$\hookrightarrow$  Inverzní prvek k prvku  $(a, b)$  je  $(-a, -b)$ .

2) Máme dokázat že platí  $(a, b) + (i, j) + (-a, -b) \in H$ ,  
 $(i, j) \in H$

$$(a, b) + (i, j) + (-a, -b) = (a+i-a, b+j-b) = (\underline{\underline{i}}, \underline{\underline{j}}) \in H$$

$\Rightarrow H$  je normalní podgrupa.

Pozn] Tato grupa  $G$  je komutativní, tj. všechny její podgrupy jsou normální.

Prf] Máme grupu všech zobrazení  $\mathbb{R}$  do  $\mathbb{R}$  tj.

$$G = \{ f: \mathbb{R} \rightarrow \mathbb{R} ; f(x) = ax + b ; a, b \in \mathbb{R} ; a \neq 0 \}.$$

Zjistěte zda podgrupa  $T = \{ t: \mathbb{R} \rightarrow \mathbb{R} ; t(x) = cx, c \in \mathbb{R} \setminus \{0\} \}$  je normální. Na grupě  $G$  je definována operace "sčítání" funkcí.

1) inverzní prvek  $t \in f \in G$ :

$$f(x) = ax + b \\ y = ax + b \Rightarrow x = \frac{y-b}{a}$$

$$\text{tj. } f^{-1}(x) = \frac{x-b}{a}$$

2) dokázat  $f \circ t \circ f^{-1} \in T$ ? pro  $t(x) = cx \in T$

$$f \circ t \circ f^{-1}(x) = f(t(f^{-1}(x))) = f(t(\frac{x-b}{a})) = f(c \frac{x-b}{a}) =$$

$$= ac \frac{x-b}{a} + b = cx - cb + b = cx + b(1-c) \notin T$$

$\Rightarrow$  tj.  $T$  není normální podgrupa.

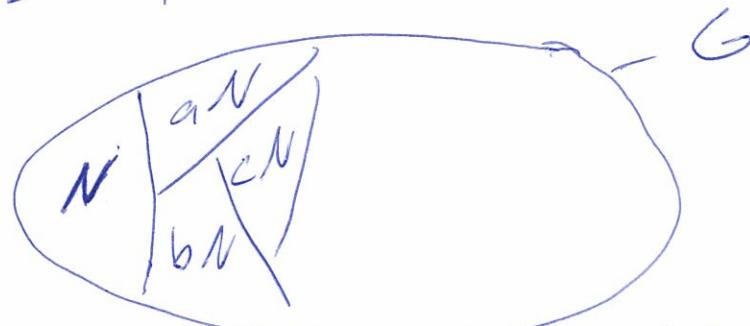
obecně neplatí  
pro libovolné  $c$

Pozn)  $T = \{t : \mathbb{R} \rightarrow \mathbb{R}; t(x) = x + b; b \in \mathbb{R}\}$   
 $\Rightarrow T$  je normální podgrupa grupy  $G$ .

Rozklad grupy  $G$  podle podgrupy  $N$ :

- levý rozklad je  $G/N = \{x \cdot N; x \in G\}$ , kde levá' řída grupy  $G$  podle podgrupy  $N$  určena' prvekem  $a \in G$  je  $a \cdot N = \{a \cdot n; n \in N\}$ .

- pravý rozklad je  $G/N = \{Nx; x \in G\}$ , kde prava' řída grupy  $G$  podle podgrupy  $N$  určená' prvekem  $a \in G$  je  $Na = \{n \cdot a; n \in N\}$ .



- sjednocením tří řídek rozkladu dostaneme celou grupu  $G$ .
- každé dve řídky jsou disjunktní, tj. nemají žádaty společný prvek.

Požadavka Podgrupa  $N$  je normální ( $\Leftrightarrow$ )  $aN = Na$

Príklad Máme grupu čtvercových matic  $2 \times 2$  nad  $\mathbb{Q}$ ,  
ej.  $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; a, b, c, d \in \mathbb{Q} \right\}$ . Zjistěte zda levá třída  
a pravá třída rozkladu podle podgrupy  $H = \left\{ \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} ; e \in \mathbb{Q} \right\}$   
se rovnají. Operace definovaná na  $G$  je násobení matic.

$$\cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} = \begin{pmatrix} ae & be \\ ce & de \end{pmatrix} \xrightarrow{\text{rovnají se}} \checkmark$$

$$\cdot \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ea & be \\ ec & de \end{pmatrix} = \begin{pmatrix} ae & be \\ ce & de \end{pmatrix}$$

$\Rightarrow$  Pravá a levá třída se rovnají a  $H$  je normální  
podgrupou.

Důležitost normálních podgrup  
- jsou důležité pro zavedení operace na faktorgrupě.

- jsou důležité pro zavedení operace na faktorgrupě.  
Pro třídy rozkladu platí:  
 $aN = bN \Leftrightarrow ab^{-1} \in N$  pro  $\forall a, b, c, d \in G$ .  
(1)  $cN = dN \Leftrightarrow c \cdot d^{-1} \in N$

Kde  $G$  je grupa a  $N$  je její podgrupa.

- zavedeme zde operaci  $\circ$  pro kterou platí  
 $aN = bN \wedge cN = dN \Rightarrow acN = bdN.$

- Podle pravidla (1) můžeme přepsat  $acN = bdN$  na  
 výraz  $ac(bd)^{-1} \in N$

Tedy  $ac(bd)^{-1} = ac \cdot d^{-1} \cdot b^{-1} = \underbrace{a \cdot c \cdot d^{-1} \cdot a^{-1}}_{\text{zde vložme}} \cdot \underbrace{b^{-1}}_{a^{-1} \cdot a \in N} \in N$   
 je 'to normální' podgrupa

$\Rightarrow$  Zavedená operace na faktorgrupách je korektní.

### Faktorizace grup

- důležitá tzn. Hlavní věta o faktorgrupách  
 (věta 2.22, pozn 2.23)

$$G \xrightarrow{f} K \xrightarrow{\cong} G/N$$

$K \cong G/N$  je izomorfni  $\Leftrightarrow$   
 $f$  surjektivní homomorfismus  
 jehož jádro je  $N$ .

### Postup

- 1) uráme  $\exists$  dva prž jso  $\in G$  ze stejné trdg rozdlena,  
tj.  $a, b \in G$  jsou ze stejné trdg  $\Leftrightarrow a^{-1}b \in N$
- 2) Zavedeme fci  $f: G \rightarrow k$ , kde  $k \cong G/N$
- 3)  $f$  je homomorfismus
- 4)  $f$  je surjektivní
- 5) jádro homomorfismu je podgrupa  $N$ .

Pr 8) Faktorizujte grupu  $(\mathbb{Z}, +)$  podle podgrupy  $k\mathbb{Z} = \{k \cdot n, n \in \mathbb{Z}\}$ .

- 1)  $a, b \in \mathbb{Z}$  patří do stejné trdg  $\Leftrightarrow -a+b \in k\mathbb{Z} \Leftrightarrow$   
 $\Leftrightarrow k | b-a \Leftrightarrow a \equiv b \pmod{k}$   
 $\Rightarrow$  dva prž jsou ve stejné trdg podle pořadí po dělení  
číslem  $k$  mají stejný zbytek.
- 2)  $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_k, \oplus)$ ,  $f(x) = [x]_k$
- 3)  $\frac{\text{homomorfismus?}}{f(x) \oplus f(y)} = [x]_k \oplus [y]_k = [x+y]_k = \underline{\underline{f(x+y)}} \quad \checkmark$

4) Surjektce?

- musí platit pro  $\forall [x]_k \in \mathbb{Z}_k$  existuje  $y \in \mathbb{Z}$ .

$$f(y) = [x]_k$$

$$[y]_k = [x]_k \Leftrightarrow y \equiv x \pmod{k} \rightarrow \text{takže } y \text{ určitě existuje}$$

5) jádro homomorfismu  $= N = k\mathbb{Z}$

$$\text{Ker } f = \{x, f(x) = [0]_k\} = \{x, [x]_k = [0]_k\} = \{x, k|x\} =$$

$$= k\mathbb{Z}$$

Plati, že jádro homomorfismu je  $k\mathbb{Z}$ .

$\Rightarrow$  Factorgraph pro grafu  $(\mathbb{Z}, +)$  podle podgrafu  $(k\mathbb{Z}, +)$   
je  $(\mathbb{Z}_k, +)$ .

Pr 91 Máme grupu  $G = \{f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = ax + b, a, b \in \mathbb{R}, a \neq 0\}$ .  
 s operací sčítání funkcií. Factorizejte grupu podle její normalní podgrupy  $T = \{t: \mathbb{R} \rightarrow \mathbb{R}, t(x) = x + b, b \in \mathbb{R}\}$

1) Dva prvek jsou stejně řidily:

$$f(x) = ax + b, g(x) = cx + d \in G$$

$$f^{-1} \circ g(x) \in T$$

$$f^{-1}(x) = \frac{x-b}{a}$$

$$f^{-1} \circ g(x) = f^{-1}(g(x)) = f^{-1}(cx+d) = \frac{cx+d-b}{a} = \frac{c}{a}x + \frac{d-b}{a} = z \in \mathbb{R}$$

$$\Leftrightarrow \frac{c}{a} = 1 \text{ neboli } \underline{c=a}$$

2) Zavedeme zobrazení  $g$  tak, že  $g(f(x)) = g(ax+b) \mapsto \underline{a}$

$\hookrightarrow$  důležitý je pro nás lineární koeficient

$$\text{tedy máme } \underline{g: (G, \circ) \rightarrow (\mathbb{R} \setminus \{0\}, \cdot)}$$

3) homomorfismus:

$$\frac{g(f \circ g(x))}{g(f(g(x)))} = g(f(g(x))) = g(f(cx+d)) = g(\underline{ax+ad+b}) =$$

rovnají se

$$g(f(x)) \cdot g(g(x)) = g(\underline{ax+b}) \cdot g(\underline{cx+d}) = \underline{(a \cdot c)}$$



4) Surjektiv  
pro  $a \in \mathbb{R} \setminus \{0\}$  musí existovat fce  $f(x) = cx + d \in G$

$$g(f(x)) = a$$

$$g(cx+d) = a$$

$$c = a$$

$\rightarrow$  takova' funkce ~~je určitá~~ je užívána

$\rightarrow$  je to surjektivní

5) jadro homomorfismu  $= T$

$$\ker g = \{f(x) \mid g(f(x)) = 1\} = \{f(x) \mid g(ax+b) = 1\} = \{f(x) \mid g(ax) = 1\} = \{f(x) \mid g(x) = 1\} = \{f(x) \mid f(x) = 1\} = T$$

$\Rightarrow$  Tedy faktorgrupa grupy  $(G, \circ)$  podle podgrupy  
 $(T, \circ)$  je  $\underline{\underline{(R \setminus \{0\}}, \circ)}$ .

Pozn 1 faktoralgebra v informatice:  
- reductie DFA je faktoralgebra pro DFA  
 $\hookrightarrow$  dva stavy patří do jedné faktory  $\Leftrightarrow$  jsou nerozlišitelné

# Ideál

Podobrazh  $I$  okruha  $R$  je ideálem  $I \triangleleft R \Leftrightarrow$  platí:

$$1) I \neq \emptyset$$

2)  $\forall a, b \in I : (a+b) \in I$  tj.  $(I, +)$  je aditívna' podgrupa  
grupy  $(R, +)$

3)  $\forall r \in R, \forall a \in I : r \cdot a \in I \wedge a \cdot r \in I$

• Levý' ideál je podobrazh  $I$ , pro lež' plati'  $r \cdot I = \{r \cdot i, i \in I\} \subseteq I$

• Pravý' ideál je podobrazh  $I$ , pro kl. plati'  $I \cdot r = \{i \cdot r, i \in I\} \subseteq I$

• Ideál je taky', pokud levý' a pravý' ideál se rovnají.

Příklad Matice nekomutativní sčítah matik  $(M_{2 \times 2}(\mathbb{Q}), +, \cdot)$

$H = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} ; a, b \in \mathbb{Q} \right\}$  je ideál sčítah? tj. zda je levým  
i pravým ideálem?

$$\text{- levý' ideál: } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & 0 \\ f & 0 \end{pmatrix} = \begin{pmatrix} ae+bf & 0 \\ ce+df & 0 \end{pmatrix} \in H \rightarrow \text{je levý'}$$

$$\text{- pravý' ideál: } \begin{pmatrix} e & 0 \\ f & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ea & eb \\ fa & fb \end{pmatrix} \notin H \rightarrow \text{není pravý'}$$

$\Rightarrow H$  není ideál.

Pr 11 | Máme okruh  $(\mathbb{Z}, +, \cdot)$ . Množina generovaná jedním prvekem  $n$  je ideálem?

- množina generovaná prvekem  $n$  má tvar:

$$\langle n \rangle = \{ \dots, -2n, -n, 0, n, 2n, \dots \} = \{ k \cdot n, k \in \mathbb{Z} \} = n \cdot \mathbb{Z}$$

1)  $n \cdot \mathbb{Z} \neq \emptyset \quad \checkmark$

2)  $\forall a, b \in n \cdot \mathbb{Z}, a+b \in n \cdot \mathbb{Z}$

$a = nx, x \in \mathbb{Z}; b = ny \quad ? \quad iy \in \mathbb{Z}$

$$\rightarrow a+b = nx+ny = \underbrace{n(x+y)}_{\text{distributivita}} = n \cdot z \in n \cdot \mathbb{Z}$$

oříknu      kde  $a = nx$  - platí'

3) pro  $\forall r \in \mathbb{Z}, \forall a \in n \cdot \mathbb{Z}$

$$\bullet r \cdot a = r \cdot n \cdot x = n \cdot \underbrace{r \cdot x}_{=t} = \underline{\underline{n \cdot t}} \in n \cdot \mathbb{Z} \quad \checkmark$$

$$\bullet a \cdot r = \cancel{n \cdot x \cdot r} = \underline{\underline{n \cdot p}} \in n \cdot \mathbb{Z} \quad \checkmark$$

$\hookrightarrow$  množina generovaná jedním prvekem  $n$  je ideálem  
celých čísel.

Příklad příklady takových idealů:

$$\langle 2 \rangle = \{ \dots, -4, -2, 0, 2, 4, \dots \}$$

$$\langle 3 \rangle = \{ \dots, -6, -3, 0, 3, 6, \dots \}$$

$$\langle 4 \rangle = \{ \dots, -8, -4, 0, 4, 8, \dots \}$$

- Hlavní ideal je ideal generovaný jedním prvkem, tj.  $\langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle$ .

- Maximální ideal je takový, že:  
I je maximální  $\Leftrightarrow I \subseteq J \wedge J=I$  nebo  $J=R$ , kde  
R je celý obor.

$\hookrightarrow \langle 2 \rangle, \langle 3 \rangle$  jsou maximální

-  $\langle 4 \rangle$  není maximální protože je to podmnožina ideálu  $\langle 2 \rangle$

$$\text{tj. } \underline{\langle 4 \rangle \subseteq \langle 2 \rangle}$$

FaktORIZACE OBORU

- R je obor, I je ideal oboru.

$$R/I = \{ a+I, a \in R \}$$

- je faktorobor.

- platí  $(I, +)$  je normální podgrupa aditivní grupy  $(R, +)$  oboru.

$\Rightarrow$  pro faktorobor musí platit, že pro aditivní operaci se  
jedná o faktorgrupu a pro množkovitelnou operaci je to  
monoid.

Operace zavedené na faktorokruhu:

$$\bullet (a+I) \oplus (b+I) = (a+b) + I$$

$$\bullet (a+I) \odot (b+I) = ab + I$$

Příklad 13 Factorizejte okruh  $(\mathbb{Z}, +)$  podle množiny sudých čísel, tj.  $2\mathbb{Z} = \{2k, k \in \mathbb{Z}\}$ . Z předchozího příkladu víme, že obecně  $n\mathbb{Z}$  je ideal a tedy  $2\mathbb{Z}$ .

1) dva průb j jsou ze stejné třídy  $\Leftrightarrow a-b \in 2\mathbb{Z} \Leftrightarrow$   
 $\Leftrightarrow 2 | a-b \Leftrightarrow a \equiv b \pmod{2}$

2) Zavedeme fci  $f: \mathbb{Z} \rightarrow \mathbb{Z}_2$ , tj. fce zobrazuje průb  
do jedné ze dvou tříd.

3-5) Dlužíme f je surjektivní homomorfismus  $\nexists$  s jádrem  
 $2\mathbb{Z}$  je dokázáno v příkladu obecně  $n\mathbb{Z}$ .

$\Rightarrow$  Tedy faktorokruh má zápis  $\mathbb{Z}/2\mathbb{Z} = \{a+2\mathbb{Z}, a \in \mathbb{Z}\}$   
jsou zde dvě třídy  $0+2\mathbb{Z}$  a  $1+2\mathbb{Z}$ .

• Hasi se ověřit platnost operací zavedených na faktorokruzích.

$$\textcircled{+} : \underline{(a+2\mathbb{Z}) + (b+2\mathbb{Z})} = a+b + \underbrace{2\mathbb{Z} + 2\mathbb{Z}}_{\in 2\mathbb{Z}} = \underline{\cancel{(a+b) + 2\mathbb{Z}}} \in 2\mathbb{Z}$$

$$\textcircled{*} : \underline{(a+2\mathbb{Z}) \cdot (b+2\mathbb{Z})} = a \cdot b + \underbrace{a \cdot 2\mathbb{Z} + b \cdot 2\mathbb{Z} + 2\mathbb{Z} \cdot 2\mathbb{Z}}_{\in 2\mathbb{Z}} = \underline{\cancel{a \cdot b + 2\mathbb{Z}}} \in 2\mathbb{Z}$$

$\Rightarrow$  Faktorordnung obrahm definiert  $(\mathbb{Z}, +, \cdot)$  posse idealen  
 $(2\mathbb{Z}, +, \cdot)$  je  $\underline{(\mathbb{Z}_2, +, \cdot)}$