Kongruence – je relace ekvivalence, která zachovává na algebře všechny její n-ární operace: $\forall a,b,c,d \in G$ platí:

$$\boxed{a \equiv b \wedge c \equiv d \iff \begin{array}{l} a+c \equiv b+d \\ a \cdot c \equiv b \cdot d \\ a^{-1} \equiv b^{-1} \\ -a \equiv -b \end{array}}$$

Eulerova funkce – udává počet čísel k, která jsou menší než číslo $\underline{m}$ a zároveň jsou s číslem $\underline{m}$ nesoudělná, tj. $NSD(m,k)=1$

Eulerova fce má tvar: $\boxed{\varphi(m) = \varphi(p_1^{n_1} \cdots p_r^{n_r}) = p_1^{n_1-1} \cdot (p_1-1) \cdots p_r^{n_r-1} \cdot (p_r-1)}$

kde $p_1^{n_1} \cdots p_r^{n_r}$ je rozklad čísla m na ~~p~~ součin prvočísel

$\underline{Př1}$ Máme číslo $m=60$. Spočítejte jeho Eulerovu fci.

$$\varphi(60) = \varphi(2 \cdot 2 \cdot 5 \cdot 3) = \varphi(2^2 \cdot 5 \cdot 3) = 2^{2-1} \cdot (2-1) \cdot 5^{1-1} \cdot (5-1) \cdot 3^{1-1} \cdot (3-1) =$$

$$= 2^1 \cdot (1) \cdot \underbrace{5^0}_{=1} \cdot (4) \cdot \underbrace{3^0}_{=1} \cdot (2) = \underline{\underline{16}}$$

$\underline{\text{Eulerova věta}}$: Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ a $NSD(m,a)=1$. Pak $\boxed{a^{\varphi(m)} \equiv 1 \pmod m}$

$\underline{Př2}$ Zjistěte zbytek čísla $2^{50}+3^{50}$ po dělení číslem 17.

– platí $NSD(17,2)=1$ a $NSD(17,3)=1$, $\varphi(17) = 17^0 \cdot (17-1) = \underline{16}$

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

- $2^{50} = 2^{3\cdot 16} \cdot 2^2 \equiv 1 \cdot 2^2 \pmod{17} = 4$
- $3^{50} = 3^{3\cdot 16} \cdot 3^2 \equiv 1 \cdot 3^2 \pmod{17} = 9$

– kongruence zachovává operace a proto můžeme napsat

$$2^{50} + 3^{50} \equiv 4 + 9 \pmod{17} = 13$$

Zbytek po dělení čísla $2^{50} + 3^{50}$ číslem 17 je $\underline{\underline{13}}$.

- Využití Eulerovy fce v šifře RSA – je to asymetrický šifrovací systém, protože k zašifrování a dešifrování se používají dva odlišné klíče → → veřejný klíč a soukromý klíč

Postup tvorby klíčů:

1) zvolme si dvě velká náhodná prvočísla $\underline{p}$ a $\underline{q}$
2) spočítáme jejich součin $\underline{n} = p \cdot q$
3) Spočítáme Eulerovu fci $\underline{\varphi(n)} = p^0 \cdot (p-1) \cdot q^0 \cdot (q-1)$
4) Zvolíme si celé číslo $\underline{e} < \varphi(n)$ a $NSD(e, \varphi(n)) = 1$
5) nalezneme číslo $\underline{d}$ tak, aby platilo $d \cdot e \equiv 1 \pmod{\varphi(n)}$
6) pokud e je prvočíslo, pak $d = (1 + r \cdot \varphi(n))/e$, kde $r = [(e-1) \cdot \varphi(n)^{(e-2)}]$

Př 3 Zvolili jsme si dvě prvočísla $p=5$ a $q=3$. Sestavíme klíče pro RSA.

- $n = p \cdot q = 5 \cdot 3 = 15$
- $\varphi(15) = 3^0 \cdot (3-\cancel{1}) \cdot 5^0 (5-1) = 2 \cdot 4 = 8$
- zvolíme si $e = 3 \Rightarrow e < \varphi(n) = 8 \wedge NSD(3,8) = 1$ a $\underline{e}$ je prvočíslo
- vypočítáme $\underline{r}$ a $\underline{d}$:

$$r = \{(3-1) \cdot \varphi(n)^{(3-2)}\} = 2 \cdot 8^1 = \underline{\underline{16}}$$

$$d = (1 + 16 \cdot 8)/3 = \frac{129}{3} = \underline{\underline{43}}$$

Tedy $d \cdot e \equiv 1 \pmod{\varphi(n)} \Rightarrow 43 \cdot 3 \equiv 1 \pmod 8$

- dvojice (n,e) tvoří veřejný klíč, kde $\underline{n}$ je modulo a $\underline{e}$ je šifrovací či veřejný exponent
- dvojice (n,d) tvoří soukromý klíč, kde $\underline{n}$ je modulo a $\underline{d}$ je dešifrovací či soukromý exponent.

- Chceme zašifrovat zprávu, kterou jsme převedli na číslo $\underline{8}$.

šifrování: $8^e \pmod n \Rightarrow 8^3 \equiv 2 \pmod{15}$, tj. 2 je šifra

dešifrování: $2^d \pmod n \Rightarrow 2^{43} = 8796093022208 \equiv 8 \pmod{15}$,

tj. získali jsme opět původní zprávu $\underline{8}$.

Normální podgrupa: N je normální podgrupa grupy G, tj. $N \lhd G \Leftrightarrow$
$\Leftrightarrow$ 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 normální!
- V komutativních grupách jsou všechny jejich podgrupy normální, protože platí: $g \cdot n \cdot g^{-1} \underset{\text{komutativita}}{=} g \cdot g^{-1} \cdot n = 1 \cdot n = n \in N$

Př 4/ Máme grupu $G = \{(a,b) \mid a,b \in \mathbb{Z}\}$ s operací sčítání, která má tvar: $(a,b) + (c,d) = (a+c, b+d)$. Zjistěte zda podgrupa $H = \{(a,b) ; 15 / 3a+5b\}$ (kde 15 dělí kombinaci čísel $3a+5b$) je normální podgrupa.

- spočteme inverzní prvek k prvku $g \in G$:

$(a,b) + (c,d) = (0,0)$ kde $(0,0)$ je neutrální prvek

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

$\Leftrightarrow a+c = 0 \;\wedge\; b+d = 0$

$c = -a \qquad d = -b$

Tedy $g^{-1} = (-a,-b)$.

- máme dokázat $g+h+g^{-1} \in H$, kde $h=(e,f) \in H$ a platí $15 / 3e+5f$

$$(a,b)+(e,f)+(-a,-b) = (\cancel{a}+e+(\cancel{-a}), \cancel{b}+f+(\cancel{-b})) = \underline{\underline{(e,f)}} \in H \checkmark$$

Tedy podgrupa H je normální podgrupou.

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

Př 5. Máme grupu všech zobrazení z $\mathbb{R}$ do $\mathbb{R}$, tj. $G=\{f: \mathbb{R} \to \mathbb{R};\ f(x)=ax+b;\ a,b \in \mathbb{R};\ a \neq 0\}$. Zjistěte zda podgrupa $T=\{g: \mathbb{R} \to \mathbb{R},\ g(x)=x+b;\ b \in \mathbb{R}\}$ je normální. Na této grupě je definovaná operace skládání funkcí.

- zjistíme inverzní prvek k $f \in G$:

$$f(x)=ax+b$$
$$y=ax+b \Rightarrow x=\frac{y-b}{a} \qquad \text{tj. } \underline{\underline{f^{-1}(x)=\frac{x-b}{a}}}$$

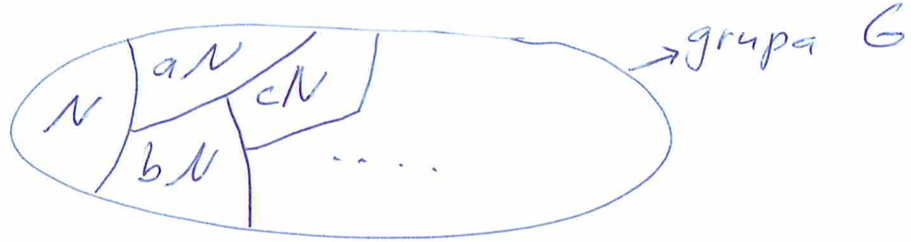
- dokážeme $f \circ g \circ f^{-1} \in T$, kde $g(x)=x+b' \in T$:

$$f \circ g \circ f^{-1}(x) = f(g(f^{-1}(x))) = f\left(g\left(\frac{x-b}{a}\right)\right) = f\left(\frac{x-b}{a}+b'\right) =$$
$$= a \cdot \left(\frac{x-b}{a}+b'\right)+b = \cancel{a}\,\frac{x-b}{\cancel{a}}+ab'+b = x-\cancel{b}+ab'+\cancel{b} =$$
$$= x+\underbrace{ab'}_{=c} = \underline{\underline{x+c \in T}}$$

Tedy T je normální podgrupa.

Rozklad grupy G podle podgrupy N:

- levý rozklad je $\boxed{G/_N = \{x \cdot N, x \in G\}}$, kde levá třída grupy G podle podgrupy N určená prvkem $a \in G$ je $\boxed{a \cdot N = \{a \cdot n, n \in N\}}$.
- pravý rozklad je $\boxed{G/_N = \{N \cdot x, x \in G\}}$, kde pravá třída grupy G podle podgrupy N určená prvkem $a \in G$ je $\boxed{N \cdot a = \{n \cdot a, n \in N\}}$.



- sjednocením všech tříd rozkladu dostaneme celou grupu G.
- každé dvě třídy jsou disjunktní, tj. nemají žádný společný prvek.

Pozn. Podgrupa N je normální $\iff$ $aN = Na$

Př 6 Máme grupu čtvercových matic nad racionálními čísly, tj. $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a,b,c,d \in \mathbb{Q} \right\}$. Zjistěte zda levá třída rozkladu a pravá třída ~~p~~ rozkladu podle podgrupy $H = \left\{ \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}, e \in \mathbb{Q} \right\}$ se rovnají. Je zde definovaná operace násobení matic.

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

násobení čísel je komutativní

Tedy pravá a levá třída rozkladu se rovnají a tedy H je normální podgrupa.

- Důležitost normálních podgrup – jsou důležité pro zavedení operace na faktorgrupě. Pro třídy rozkladu platí:

(1) $$\boxed{\begin{aligned} aN = bN &\iff a^{-1}b \in N \\ cN = dN &\iff c^{-1}d \in N \end{aligned} \quad \text{pro } \forall a,b,c,d \in G}$$

kde G je grupa a N je její podgrupa.

- Zavedeme zde operaci $\cdot$, pro kterou platí $aN = bN \land cN = dN \Rightarrow a \cdot cN = b \cdot dN$
- Podle rovnic z (1) můžeme přepsat $acN = bdN$ na $(ac)^{-1}bd \in N$ a máme zjistit zda opravdu $(ac)^{-1}bd$ je z N.

Tedy $(ac)^{-1}bd = c^{-1} \cdot a^{-1} \cdot b \cdot d = \underbrace{c^{-1} \cdot \underbrace{a^{-1} \cdot b}_{\in N} \cdot c}_{\overset{?}{\in} N} \cdot \underbrace{c^{-1} \cdot d}_{\in N} \in N$

zde vložíme $c \cdot c^{-1}$

$\overset{?}{\in} N$ – pokud N je normální, tak to platí!

Tedy zavedená operace $\circ$ na faktorgrupách je korektní!

Faktorizace grup

- důležitá je tzv. Hlavní věta o faktorgrupách (ve skriptech je to věta 2.22 či pozn. 2.23).

Postup jak najít faktorgrupu:

1) určit, kdy jsou dva prvky ze stejné třídy rozkladu, tj. dva prvky $a, b \in G$ jsou ve stejné třídě $\iff a^{-1}b \in N$.
2) Zavedeme fci $f: G \to K$, kde K je izomorfní s G/N tj. platí

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[dr] & K \\ & G/N \arrow[u, "\cong"'] \end{tikzcd}$$

$K \cong G/N$ neboli jsou izomorfní $\iff$ f je surjektivní homomorfismus jehož jádro tvoří podgrupa N.

3) Ověření, že f je homomorfismus
4) Ověření, že f je surjektivní
5) ověření, že jádro homomorfismu je podgrupa N, podle které rozkládáme grupu G.

Př 7) Faktorizujte grupu $(\mathbb{Z}, +)$ podle podgrupy $k\cdot\mathbb{Z} = \{k\cdot n,\ n\in\mathbb{Z}\}$.

1) Dva prvky $a, b \in \mathbb{Z}$ patří ~~do~~ stejné třídy $\Leftrightarrow$ $-a+b \in k\cdot\mathbb{Z}$

$\Leftrightarrow k \mid b-a \Leftrightarrow a \equiv b \pmod{k}$

tj. dva prvky leží ve stejné třídě, pokud po dělení číslem k mají stejný zbytek.

2) Zavedeme fci $f: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_k, \oplus)$

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

3) ověříme homomorfismus:

$$f(x) \oplus f(y) = [x]_k \oplus [y]_k = [x+y]_k = f(x+y)$$

$\hookrightarrow$ je to homomorfismus

4) Surjekce:
musí platit, že pro $\forall\ [x]_k \in \mathbb{Z}_k$ existuje $\exists\ y \in \mathbb{Z}$:

$$f(y) = [x]_k$$
$$[y]_k = [x]_k \Leftrightarrow y \equiv x \pmod{k} \rightarrow \text{takové } y \text{ určitě existuje}$$

$\hookrightarrow$ je to surjekce.

5) Jádro homomorfismu: $\ker f = \{x,\ f(x) = [0]_k\} = \{x,\ [x]_k = [0]_k\} =$
$= \{x,\ k \mid x\} = k\cdot\mathbb{Z}$ $\rightarrow$ platí, že jádro homomor. je $k\cdot\mathbb{Z}$.

Tedy faktorgrupa pro grupu $(\mathbb{Z}, +)$ podle podgrupy $(k \cdot \mathbb{Z}, +)$ je $(\mathbb{Z}_k, +)$.

Př 8, Máme grupu všech zobrazení $G = \{f : \mathbb{R} \to \mathbb{R} ;\ f(x) = ax + b,\ a, b \in \mathbb{R},\ a \neq 0\}$ s operací skládání fcí. Faktorizujte grupu podle její normální podgrupy $T = \{g : \mathbb{R} \to \mathbb{R},\ g(x) = x + b,\ b \in \mathbb{R}\}$.

1) Prvky jsou ve stejné třídě : $h(x) = ax + b$, $t(x) = cx + d \in G \iff h^{-1} \circ t(x) \overset{?}{\in} T$

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

$$h^{-1} \circ t(x) = h^{-1}(t(x)) = h^{-1}(cx + d) = \frac{(cx + d) - b}{a} = \frac{c}{a} x + \underbrace{\frac{d - b}{a}}_{= t} = \frac{c}{a} x + t \in T \iff$$

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

2) pro zavedení zobrazení φ je pro nás důležitý pouze lineární koeficient funkce f, tj. $f(x) = ax + b$ je důležité $\underline{a}$.

Takže $\varphi(f(x)) = \varphi(ax + b) \longmapsto a$

a tedy zobrazení je $\varphi : (G, \circ) \longrightarrow (\mathbb{R} \setminus \{0\}, \cdot)$

3) homomorfismus:

$$\varphi(h \circ t(x)) = \varphi(h(t(x))) = \varphi(h(cx+d)) = \varphi(a(cx+d)+b) =$$
$$= \varphi(acx + ad+b) = \underline{\underline{ac}}$$

rovnají se

$$\varphi(h(x)) \cdot \varphi(t(x)) = \varphi(ax+b) \cdot \varphi(cx+d) = \underline{\underline{a \cdot c}}$$

– je to homomorfismus ✓

4) surjekce:
pro $\forall a$ $\mathbb{R} \setminus \{0\}$ existuje fce $f(x) = cx+d \in G$:

$$\varphi(f(x)) = a$$
$$\varphi(cx+d) = a$$
$$\underline{\underline{c = a}}$$

– taková funkce lze určitě najít. ✓

5) Jádro homomorfismu:

$$\ker \varphi = \{f(x),\ \varphi(f(x)) = 1\} = \{f(x), \varphi(ax+b) = 1\} = \{f(x),\ a = 1\} =$$
$$= \{f(x);\ f(x) = x+b\} = \underline{\underline{T}} \checkmark$$

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

Pozn. Paralela faktoralgeber ~~v~~ informatice:
Redukce DKA automatu, kdy dva stavy patří do jedné třídy $\Leftrightarrow$ jsou tyto stavy nerozlišitelné. Tedy redukovaný DKA je faktoralgebrou pro DKA automat.

<u>Ideál</u>: Podokruh I okruhu R je ideálem, $I \triangleleft R \Leftrightarrow$ platí:

1) I je neprázdná množina, tj. $I \neq \emptyset$.
2) pro $\forall a,b \in I$ platí: $(a+b) \in I$, tj. $(I,+)$ tvoří aditivní podgrupu grupy $(R,+)$.
3) pro $\forall r \in R$, $\forall a \in I$ platí: $ra \in I \wedge a \cdot r \in I$.

Levý ideál je podokruh I, pro který platí $r \cdot I = \{r \cdot i, i \in I\} \subseteq I$, tj. $r \cdot i \in I$.
Pravý ideál je podokruh I, pro který platí $I \cdot r = \{i \cdot r, i \in I\} \subseteq I$, tj. $i \cdot r \in I$.
Ideál je takový, který je levým i pravým ideálem.

<u>Př 9</u> Máme nekomutativní okruh matic $(M_{2x2}(\mathbb{Q}), +, \cdot)$. Je množina matic $H = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, a,b \in \mathbb{Q}\right\}$ pravým, resp. levým ideálem?

Levý ideál: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & 0 \\ f & 0 \end{pmatrix} = \begin{pmatrix} ae+bf & 0 \\ ee+df & 0 \end{pmatrix} \in H$ ✓ $\rightarrow$ je to levý ideál

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

Tedy množina H není ideálem okruhu, je pouze levým ideálem.

Př 10/ Máme okruh $(\mathbb{Z},+,\cdot)$. Je množina generovaná jedním prvkem $\underline{n}$ ideálem okruhu?

- množina generovaná jedním prvkem $\underline{n}$ má tvar:

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

1) $n\mathbb{Z}\neq\emptyset$ tj. je to neprázdná množina.

2) pro $\forall\, a,b \in n\mathbb{Z}$, kde $a=nx$, $x\in\mathbb{Z}$; $b=ny$, $y\in\mathbb{Z}$ má platit $a+b\overset{?}{\in} n\mathbb{Z}$

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

3) pro $\forall\, r\in\mathbb{Z}$, $\forall\, a\in\mathbb{Z}$, kde $a=nx$, $x\in\mathbb{Z}$ platí:

$$r\cdot a = r\cdot n\cdot x \underset{\substack{\text{komutativita}\\ \text{násobení čísel}}}{=} n\cdot \underbrace{r\cdot x}_{=t\in\mathbb{Z}} = n\cdot t \in n\mathbb{Z} \checkmark$$

$$a\cdot r = n\cdot \underbrace{x\cdot r}_{s\in\mathbb{Z}} = \cancel{n\cdot x\cdot r}\ n\cdot s \in n\mathbb{Z} \checkmark$$

$\hookrightarrow$ Tedy množina generovaná jedním prvkem $\underline{n}$ je ideálem okruhu celých čísel $(\mathbb{Z},+,\cdot)$.

Př 11/ Příklad ideálů tohoto okruhu celých čísel $(\mathbb{Z},+,\cdot)$:

$\langle 2\rangle = \{\dots,-4,-2,0,2,4,\dots\}$, $\langle 3\rangle = \{\dots,-6,-3,0,3,6,\dots\}$

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

- Hlavním ideálem je ideál generovaný jedním prvkem, tj. $\langle 2\rangle, \langle 3\rangle, \langle 4\rangle$ jsou hlavní ideály.
- Maximální ideál je takový, že platí:
  - ideál I je maximální $\Leftrightarrow I \subseteq J \wedge J = I$ nebo $J = R$ - celý okruh

tedy z př. 11, jsou maximální ideály pouze $\langle 2\rangle, \langle 3\rangle$.
Ideál $\langle 4\rangle$ není maximální protože je podmnožinou ideálu $\langle 2\rangle$, tj. $\langle 4\rangle \subseteq \langle 2\rangle$.

Faktorizace okruhu

- R je okruh, I je ideál okruhu. $R/_I = \{a+I, a\in R\}$ je faktorokruh.
- platí, že $(I,+)$ je normální podgrupou aditivní grupy $(R,+)$ okruhu.
- pro faktorokruh musí platit, že pro aditivní operaci se jedná o faktorgrupu a pro multiplikativní operaci se jedná o monoid.
- Operace zavedené na faktorokruhu:

$$(a+I)+(b+I) = (a+b)+I$$
$$(a+I)\cdot(b+I) = a\cdot b + I$$

Př. 12) Faktorizujme okruh $(\mathbb{Z},+,\cdot)$ podle množiny sudých čísel, tj. podle $2\mathbb{Z} = \{2k, k\in\mathbb{Z}\}$. Z předchozího příkladu př. 10, víme, že obecně $n\mathbb{Z}$ je ideálem okruhu, ~~tj~~ i $2\mathbb{Z}$ je ideálem okruhu $(\mathbb{Z},+,\cdot)$.

- nejdříve zjistíme zda pro aditivní operaci se jedná o faktorgrupu,
tj. 1) dva prvky leží ve stejné třídě $\Leftrightarrow -a+b \in 2\mathbb{Z} \Leftrightarrow 2 \mid b-a \Leftrightarrow$
$\Leftrightarrow a \equiv b \pmod 2$

2) Zavedeme ~~oper~~ fci $f: \mathbb{Z} \to \mathbb{Z}_2$, tj. funkce zobrazuje prvky do jedné ze dvou tříd.

3,-5) homomorfismus, surjekce a zda jádro homomorfismu tvoří obecně $k\mathbb{Z}$ bylo řešeno v příkladě Př 71 tj. platí to i pro $2\mathbb{Z}$.

$\Rightarrow$ Tedy Faktorokruh má zápis $\mathbb{Z}/_{2\mathbb{Z}} = \{a+2\mathbb{Z},\ a \in \mathbb{Z}\}$, jsou zde dvě třídy $0+2\mathbb{Z}$ pro sudá čísla a $1+2\mathbb{Z}$ pro lichá čísla.

- Musí se ověřit, zda zde platí operace zavedené na faktorokruzích

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

$\cdot: (a+2\mathbb{Z})\cdot(b+2\mathbb{Z}) = a\cdot b + \underbrace{a\cdot 2\mathbb{Z}}_{\in 2\mathbb{Z}} + \underbrace{b\cdot 2\mathbb{Z}}_{\in 2\mathbb{Z}} + \underbrace{2\mathbb{Z}\cdot 2\mathbb{Z}}_{\in 2\mathbb{Z}} = a\cdot b + 2\mathbb{Z} \in 2\mathbb{Z}$ ✓

Tedy Faktorokruh okruhu $(\mathbb{Z},+,\cdot)$ podle ideálu $(2\mathbb{Z},+,\cdot)$ je $(\mathbb{Z}_2,+,\cdot)$.