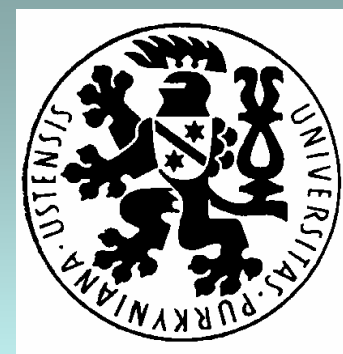




**Katedra matematiky
PF UJEP**



Aritmetika s didaktikou I.

KM1 / 0001

Přednáška 10

Dělení se zbytkem

O čem budeme hovořit:

- Binární operace „dělení se zbytkem“ v $\mathbb{N}$
- Struktury zbytkových tříd podle modulu
- Seznámíme se s homomorfizmem

Co je to „dělení se zbytkem“ ?

Základní poznatky

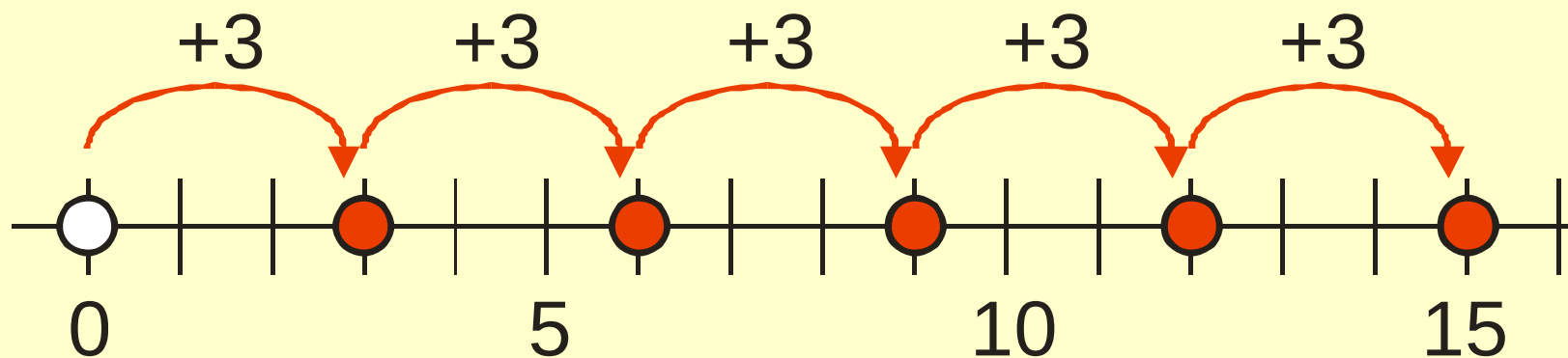
Operace **dělení** není v množině $\mathbf{N}$ úplná.

Pro libovolná dvě přirozená čísla $a, b \in \mathbf{N}$ ale můžeme vypočítat jejich „**neúplný podíl**“ a „**zbytek**“.

Příklady:

$13 : 3 = 4$ (1)	protože	$13 = 4 \cdot 3 + 1$
$13 : 5 = 2$ (3)	protože	$13 = 2 \cdot 5 + 3$
$15 : 5 = 3$ (0)	protože	$15 = 3 \cdot 5 + 0$
$15 : 7 = 2$ (1)	protože	$15 = 2 \cdot 7 + 1$
$2 : 5 = 0$ (2)	protože	$2 = 0 \cdot 5 + 2$
$9 : 9 = 1$ (0)	protože	$9 = 1 \cdot 9 + 0$

Vizuální představa



$$6 : 3 = 2 \text{ (0)}$$

protože

$$6 = 2 \cdot 3 + 0$$

$$7 : 3 = 2 \text{ (1)}$$

protože

$$7 = 2 \cdot 3 + 1$$

$$8 : 3 = 2 \text{ (2)}$$

protože

$$8 = 2 \cdot 3 + 2$$

$$9 : 3 = 3 \text{ (0)}$$

protože

$$9 = 3 \cdot 3 + 0$$

$$13 : 3 = 4 \text{ (1)}$$

protože

$$13 = 4 \cdot 3 + 1$$

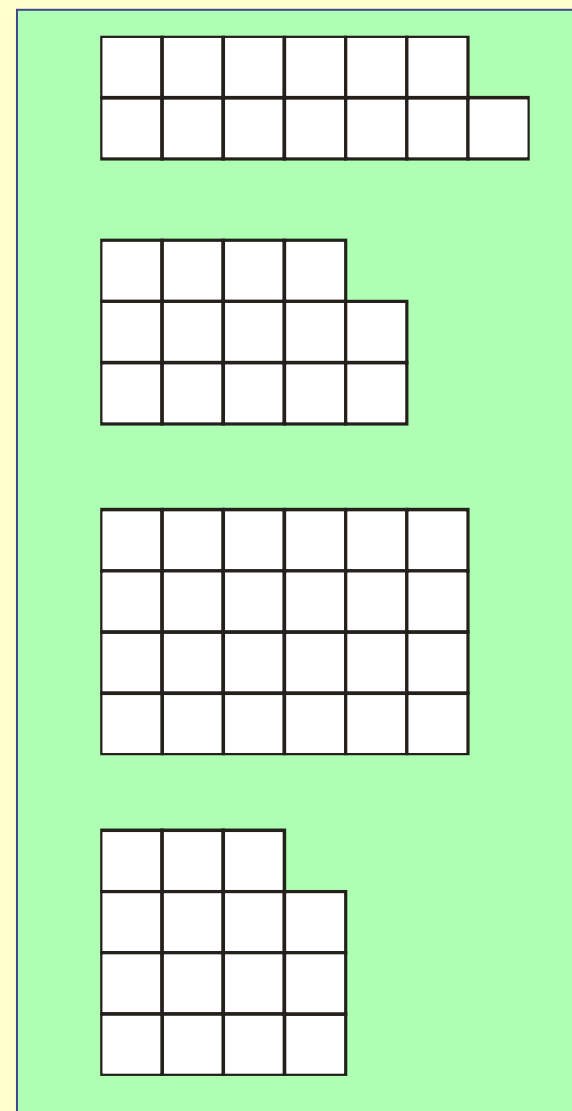
Další vizuální představa

$$13 : 2 = 6 (1) \quad \text{protože} \quad 13 = 6 \cdot 2 + 1$$

$$14 : 3 = 4 (2) \quad \text{protože} \quad 14 = 4 \cdot 3 + 2$$

$$24 : 4 = 6 (0) \quad \text{protože} \quad 24 = 6 \cdot 4 + 0$$

$$15 : 4 = 3 (3) \quad \text{protože} \quad 15 = 3 \cdot 4 + 3$$

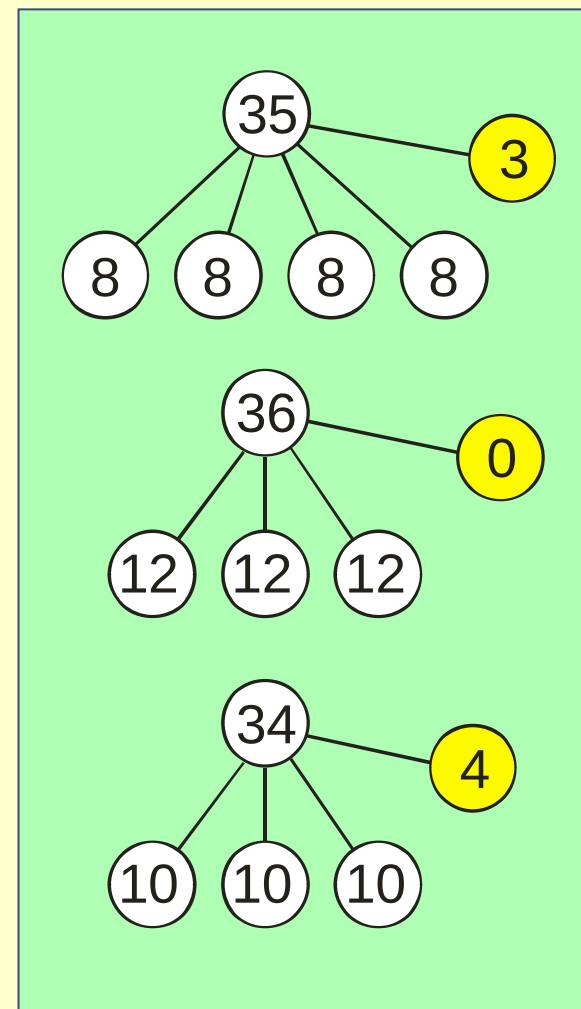


A ještě další vizuální představa

$$35 : 8 = 4 (3) \quad \text{protože} \quad 35 = 4 \cdot 8 + 3$$

$$36 : 12 = 3 (0) \quad \text{protože} \quad 36 = 3 \cdot 12 + 0$$

$$34 : 10 = 3 (4) \quad \text{protože} \quad 34 = 3 \cdot 10 + 4$$



Základní věta

Pro každá dvě čísla $a, b \in \mathbb{N}$ existuje právě jedno číslo $q \in \mathbb{N}_0$ a právě jedno číslo $r \in \mathbb{N}_0$ tak, že platí

$$a = q \cdot b + r \quad \wedge \quad 0 \leq r < b .$$

Pak zapisujeme: $a : b = q (r) .$

Při dělení se zbytkem užíváme tyto názvy:

číslu a se říká **dělenec**, číslu b se říká **dělitel**,

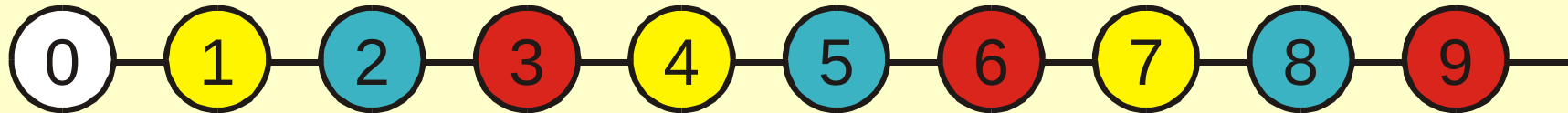
číslu q se říká **neúplný podíl** a číslu r se říká **zbytek** .

$$(\forall a, b \in \mathbb{N})(\exists! q, r \in \mathbb{N}_0) \quad a = q \cdot b + r \quad \wedge \quad 0 \leq r < b$$

Zbytek je vždy menší než dělitel !!

Hra s barevnými čísly

**Děti si periodicky obarví čísla,
například třemi barvami:**



Pak mohou řešit řadu problémů, například:

- Která další čísla budou červená (žlutá, modrá)?
 - Jakou barvu mají čísla 15, 16, 31, 32, 50 ?
- atd.

Jaké číslo vznikne, když:

- sečteme dvě červená (žlutá, modrá) čísla?
 - žluté číslo vynásobíme dvěma?
- atd.

**Výsledky „sčítání a násobení barev“
jsou v těchto tabulkách:**

+	red	yellow	blue
red	red	yellow	blue
yellow	yellow	blue	red
blue	blue	red	yellow

×	red	yellow	blue
red	red	red	red
yellow	yellow	red	blue
blue	blue	blue	yellow

**Které z těchto poznatků mohou děti odůvodnit?
Jaké představy by přitom mohly používat?**

Zbytkové třídy

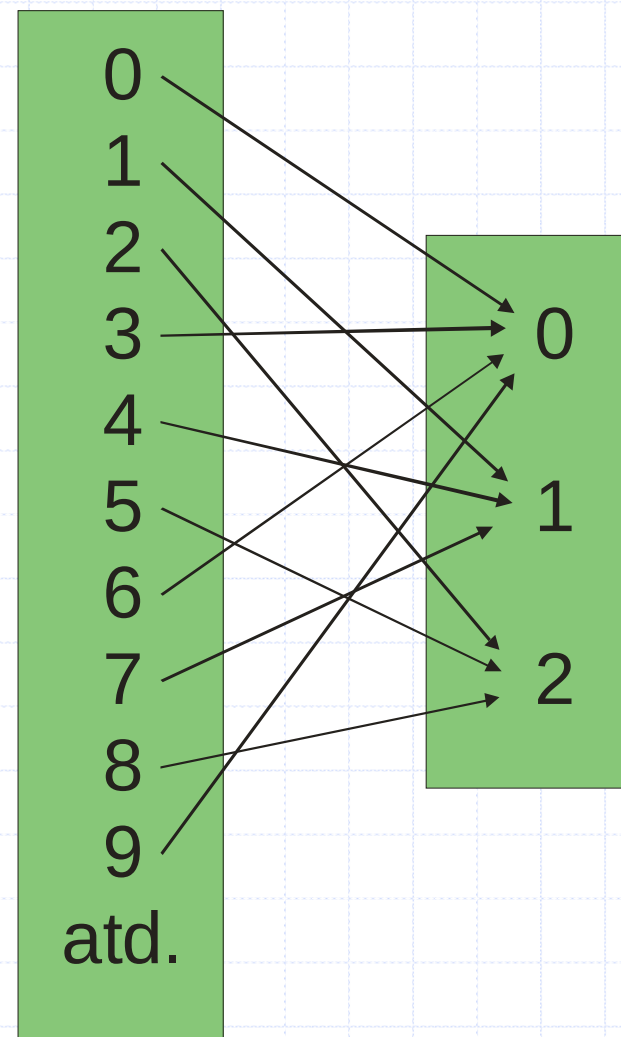
Přejdeme od barev ke zbytkům!

Množinu $\mathbf{N}_0$ můžeme rozložit podle toho, jaký mají čísla zbytek při dělení číslem 3.

Na množině zbytků můžeme definovat operace sčítání a násobení pomocí těchto formulí:

$$\mathbf{zb}(a) + \mathbf{zb}(b) =_{\mathbf{D}} \mathbf{zb}(a+b)$$

$$\mathbf{zb}(a) \cdot \mathbf{zb}(b) =_{\mathbf{D}} \mathbf{zb}(a \cdot b)$$



Barev může být i více!

Necht' je dáno libovolné přirozené číslo $m \geq 2$.
Množinu N_0 pak můžeme rozložit podle toho, jaký mají čísla zbytek při dělení číslem m .
V každé třídě rozkladu budou čísla, který mají stejný zbytek – můžeme je pokládat za ekvivalentní.
Tříd rozkladu bude právě m , protože zbytky nabývají hodnot $0, 1, 2, \dots, m-1$.
Na těchto zbytcích (resp. na těchto třídách) můžeme definovat operace sčítání a násobení uvedenými formulami a vytvořit **strukturu zbytkových tříd** $[Z_m; +; \cdot]$ podle modulu m .

Vlastnosti struktur $[\mathbb{Z}_m ; + ; \cdot]$

Vlastnosti struktur zbytkových tříd $[\mathbb{Z}_m ; + ; \cdot]$ podle modulu m jsou specifikovány touto větou:

Věta:

Je-li číslo m **prvočíslo**, je struktura $[\mathbb{Z}_m ; + ; \cdot]$ **komutativním tělesem**.

Je-li číslo m **složené**, je struktura $[\mathbb{Z}_m ; + ; \cdot]$ **komutativním okruhem s děliteli nuly**.

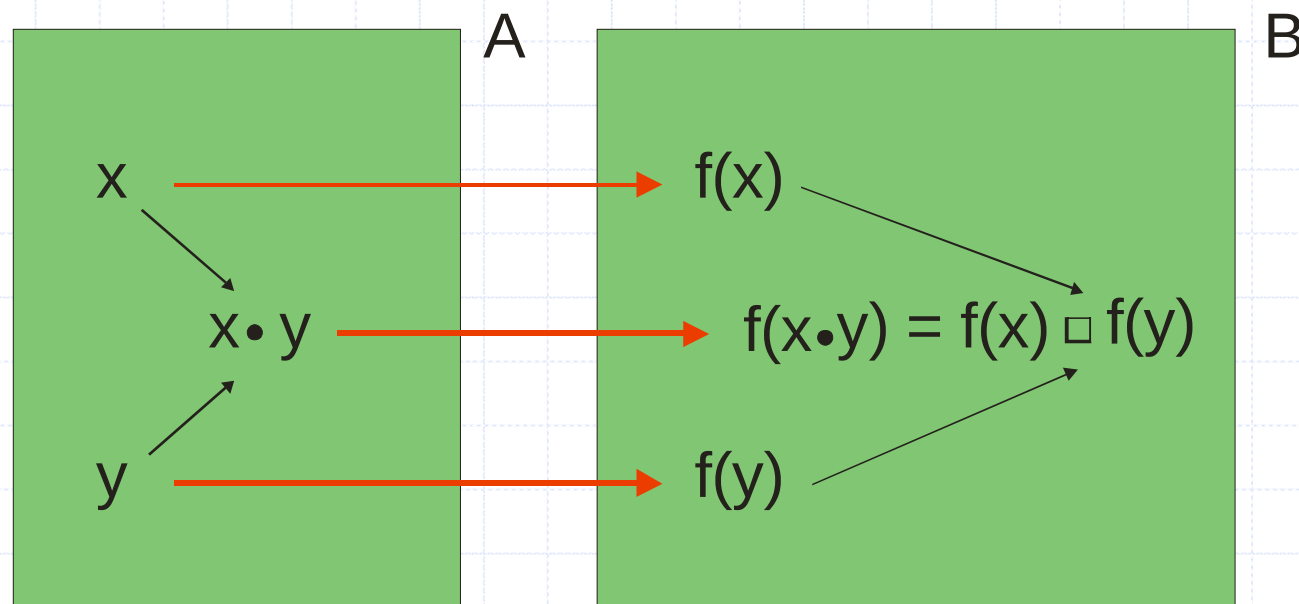
Homomorfismus

Definice homomorfizmu

Nechť jsou dány dvě struktury $[A; \bullet]$ a $[B; \square]$ s jednou binární operací. Necht' existuje zobrazení f množiny A na množinu B takové, že platí:

$$(\forall x, y \in A) \quad f(x \bullet y) = f(x) \square f(y).$$

Pak zobrazení f nazýváme **homomorfizmem**.



Homomorfizmus přenáší komutativitu!

Věta: Necht' je struktura $[\mathbf{B} ; \square]$ homomorfním obrazem komutativní struktury $[\mathbf{A} ; \bullet]$. Pak platí, že struktura $[\mathbf{B} ; \square]$ je také komutativní.

Důkaz:

Chceme dokázat, že $(\forall X, Y \in \mathbf{B}) \quad X \square Y = Y \square X$.

K libovolně zvoleným $X, Y \in \mathbf{B}$ jistě existují prvky $x, y \in \mathbf{A}$ takové, že: $f(x) = X$ a $f(y) = Y$.

Podle předpokladu platí, že $x \bullet y = y \bullet x$.

Z toho pak plyne:

$$\begin{aligned} f(x \bullet y) &= f(y \bullet x) , \\ f(x) \square f(y) &= f(y) \square f(x) , \\ X \square Y &= Y \square X . \end{aligned}$$

Další vlastnosti homomorfizmu

Podobně by se dalo dokázat, že homomorfizmus přenáší i další vlastnosti struktury $[A; \bullet]$ na její homomorfní obraz $[B; \square]$.

Homomorfní zobrazení přenáší asociativitu operace, vlastnost existence neutrálního prvku i vlastnost existence inverzních prvků.

Platí tedy například věta:

Homomorfním obrazem komutativní grupy je komutativní grupa.

Důsledky pro struktury zbytkových tříd

Vzhledem k tomu, že ve struktuře $[N_0 ; + ; .]$ jsou obě operace komutativní, asociativní a mají neutrální prvky, přenáší se tyto vlastnosti i na strukturu zbytkových tříd $[Z_m ; + ; .]$ podle libovolného modulu m .

Není těžké odůvodnit, že tyto struktury mají i další vlastnosti, které způsobují, že jsou buď tělesem anebo okruhem s děliteli nuly podle toho, zda je modul m prvočíslem či číslem složeným.

Děkuji za pozornost

