# Opakování: zbytkové třídy

*Definice.* Nechť $m \in \mathbb{N}$. Pro libovolné $a \in \mathbb{Z}$ definujeme množinu $[a]_m = \{a + k \cdot m;\ k \in \mathbb{Z}\}$, kterou nazýváme zbytková třída modulo $m$ obsahující $a$.

*Poznámka.* Množina $[a]_m$ se skládá z právě těch celých čísel, která mají stejný zbytek po dělení číslem $m$ jako číslo $a$.

*Věta.* *Pro libovolná $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ nastává $[a]_m = [b]_m$ právě tehdy, když $m \mid a - b$, tj. právě když $a \equiv b \pmod{m}$.*

*Označení.* Množinu všech zbytkových tříd modulo $m \in \mathbb{N}$ značíme $\mathbb{Z}_m$. Je tedy

$$\mathbb{Z}_m = \big\{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\big\}.$$

# Opakování: operace na množině $\mathbb{Z}_m$

*Věta.* *Nechť $m \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$ jsou libovolná. Jestliže platí $[a]_m = [c]_m$, $[b]_m = [d]_m$, pak také*

$$[a + b]_m = [c + d]_m, \qquad [a \cdot b]_m = [c \cdot d]_m.$$

*Důsledek.* *Nechť $m \in \mathbb{N}$. Vztahy*

$$[a]_m + [b]_m = [a + b]_m,$$
$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

*pro libovolná $a, b \in \mathbb{Z}$ definují operace $+$ a $\cdot$ na množině $\mathbb{Z}_m$. Tato množina s těmito operacemi tvoří komutativní okruh $(\mathbb{Z}_m, +, \cdot)$. Tento okruh je obor integrity, právě tehdy, když je tento okruh těleso, což nastává právě tehdy, když je $m$ prvočíslo.*

# Zbytkové třídy polynomů nad okruhem zbytkových tříd

*Definice.* Nechť $m \in \mathbb{Z}$, $m > 1$. Zvolme pevně normovaný polynom $f(x) \in \mathbb{Z}_m[x]$, $\mathrm{st}(f(x)) > 1$. Pro libovolný polynom $g(x) \in \mathbb{Z}_m[x]$ definujeme množinu

$$[g(x)]_{f(x)} = \{g(x) + k(x) \cdot f(x);\ k(x) \in \mathbb{Z}_m[x]\},$$

kterou nazveme zbytková třída okruhu polynomů $\mathbb{Z}_m[x]$ modulo $f(x)$ obsahující polynom $g(x)$.

*Věta.* *Nechť $m \in \mathbb{Z}$, $m > 1$ a polynom $f(x) \in \mathbb{Z}_m[x]$ je normovaný,* $\mathrm{st}(f(x)) > 1$. *Pro libovolný polynom $g(x) \in \mathbb{Z}_m[x]$ se množina $[g(x)]_{f(x)}$ skládá z právě těch polynomů ze $\mathbb{Z}_m[x]$, které mají stejný zbytek po dělení polynomem $f(x)$ jako polynom $g(x)$ (polynomem $f(x)$ můžeme dělit se zbytkem díky tomu, že je normovaný).*
*Pro libovolné polynomy $g(x), h(x) \in \mathbb{Z}_m[x]$ nastává $[g(x)]_{f(x)} = [h(x)]_{f(x)}$ právě tehdy, když $f(x) \mid g(x) - h(x)$.*

# Množina zbytkových tříd polynomů

*Označení.* Množinu všech zbytkových tříd okruhu polynomů $\mathbb{Z}_m[x]$ modulo $f(x) \in \mathbb{Z}_m[x]$ značíme $\mathbb{Z}_m[x]/(f(x))$. Je tedy

$$\mathbb{Z}_m[x]/(f(x)) = \left\{[g(x)]_{f(x)} \mid g(x) \in \mathbb{Z}_m[x]\right\}.$$

*Poznámka.* Uvedené označení je speciální případ označení obecnější konstrukce (tzv. faktorizace okruhů podle ideálu), použili jsme jej, protože označení analogické označení okruhu zbytkových tříd (tedy označení $(\mathbb{Z}_m[x])_{f(x)}$ nebo něco podobného) se v této situaci nepoužívá. Zřejmě pro každou zbytkovou třídu platí, že společný zbytek jejích prvků po dělení polynomem $f(x)$ je také jejím prvkem, proto

$$\mathbb{Z}_m[x]/(f(x)) = \left\{[g(x)]_{f(x)} \mid g(x) \in \mathbb{Z}_m[x], \mathrm{st}(g(x)) < \mathrm{st}(f(x))\right\}.$$

Protože různé zbytky patří do různých tříd, má množina $\mathbb{Z}_m[x]/(f(x))$ právě $m^{\mathrm{st}(f(x))}$ prvků.

# Příklad: množina $\mathbb{Z}_2[x]/(x^2+x+[1]_2)$

*Příklad.* Zvolme $m = 2$, $f(x) = x^2 + x + [1]_2 \in \mathbb{Z}_2[x]$. Zbytek po dělení kvadratickým polynomem je polynom stupně menšího než dva, proto máme právě čtyři možné zbytky, totiž polynomy $[0]_2, [1]_2, x, x + [1]_2$. Proto je množina

$$\mathbb{Z}_2[x]/(x^2+x+[1]_2) = \left\{ \left[[0]_2\right]_{f(x)}, \left[[1]_2\right]_{f(x)}, \left[x\right]_{f(x)}, \left[x+[1]_2\right]_{f(x)} \right\}$$

čtyřprvková.

Tento přesný zápis je poněkud nepřehledný, proto pro zjednodušení zápisu budeme dále tyto zbytky psát jako $0, 1, x, x + 1$ a polynom $f(x)$ jako $x^2 + x + 1$. Tedy

$$\mathbb{Z}_2[x]/(x^2+x+1) = \left\{ [0]_{x^2+x+1}, [1]_{x^2+x+1}, [x]_{x^2+x+1}, [x+1]_{x^2+x+1} \right\}.$$

# Operace na množině $\mathbb{Z}_m[x]/(f(x))$

*Věta.* *Nechť* $m \in \mathbb{Z}$, $m > 1$ *a polynom* $f(x) \in \mathbb{Z}_m[x]$ *je normovaný,* $\mathrm{st}(f(x)) > 1$. *Jestliže pro polynomy* $g(x), h(x), r(x), s(x) \in \mathbb{Z}_m[x]$ *platí* $[g(x)]_{f(x)} = [r(x)]_{f(x)}$, $[h(x)]_{f(x)} = [s(x)]_{f(x)}$, *pak také platí*
$[g(x) + h(x)]_{f(x)} = [r(x) + s(x)]_{f(x)}$,
$[g(x) \cdot h(x)]_{f(x)} = [r(x) \cdot s(x)]_{f(x)}$.

*Důsledek.* *Nechť* $m \in \mathbb{Z}$, $m > 1$ *a polynom* $f(x) \in \mathbb{Z}_m[x]$ *je normovaný,* $\mathrm{st}(f(x)) > 1$. *Vztahy*

$$[g(x)]_{f(x)} + [h(x)]_{f(x)} = [g(x) + h(x)]_{f(x)},$$
$$[g(x)]_{f(x)} \cdot [h(x)]_{f(x)} = [g(x) \cdot h(x)]_{f(x)}$$

*pro libovolné polynomy* $g(x), h(x) \in \mathbb{Z}_m[x]$ *definují operace* $+$ *a* $\cdot$ *na množině* $\mathbb{Z}_m[x]/(f(x))$. *Tato množina s těmito operacemi tvoří netriviální komutativní okruh* $(\mathbb{Z}_m[x]/(f(x)), +, \cdot)$. *Tento okruh je obor integrity, právě tehdy, když je tento okruh těleso, což nastává právě tehdy, když je* $m$ *prvočíslo a současně polynom* $f(x)$ *je ireducibilní nad* $\mathbb{Z}_m$.

*Důkaz.* Z předchozí věty plyne korektnost uvedených definic obou operací (tedy nezávislost výsledku operace na zvolených reprezentantech). Každý z axiomů komutativního okruhu pro novou algebraickou strukturu $(\mathbb{Z}_m[x]/(f(x)), +, \cdot)$ plyne z platnosti tohoto axiomu pro komutativní okruh $\mathbb{Z}_m[x]$, ukažme si to například na komutativitě sčítání: pro libovolné polynomy $g(x), h(x) \in \mathbb{Z}_m[x]$ platí

$$[g(x)]_{f(x)} + [h(x)]_{f(x)} = [g(x) + h(x)]_{f(x)} = \\ = [h(x) + g(x)]_{f(x)} = [h(x)]_{f(x)} + [g(x)]_{f(x)}.$$

Nulou (resp. jedničkou) v novém okruhu je třída obsahující konstantní polynom $[0]_m$ (resp. $[1]_m$).
Třída $[-g(x)]_{f(x)}$ je opačným prvkem ke třídě $[g(x)]_{f(x)}$.
Je tedy $\mathbb{Z}_m[x]/(f(x))$ netriviální komutativní okruh. Protože je konečný, je to obor integrity, právě když je to těleso.
Jestliže $m$ není prvočíslo, existují $r, s \in \mathbb{Z}$, $r > 1$, $s > 1$, $rs = m$, a náš okruh obsahuje dělitele nuly $[r]_m$, $[s]_m$, protože $[r]_m \neq [0]_m \neq [s]_m$, $[r]_m \cdot [s]_m = [m]_m = [0]_m$.

Nechť je dále $m$ prvočíslo.
Jestliže polynom $f(x)$ není ireducibilní nad $\mathbb{Z}_m$, existují $r(x), s(x) \in \mathbb{Z}_m[x]$, $\mathrm{st}(r(x)) > 0$, $\mathrm{st}(s(x)) > 0$, $r(x) \cdot s(x) = f(x)$, a náš okruh obsahuje dělitele nuly $[r(x)]_{f(x)}$, $[s(x)]_{f(x)}$, protože $\mathrm{st}(s(x)) < \mathrm{st}(f(x))$, $\mathrm{st}(r(x)) < \mathrm{st}(f(x))$, a tedy tyto prvky jsou nenulové, přitom $[r(x)]_{f(x)} \cdot [s(x)]_{f(x)} = [f(x)]_{f(x)} = [[0]_m]_{f(x)}$, což je nula našeho okruhu.
Nechť je dále polynom $f(x)$ ireducibilní nad $\mathbb{Z}_m$.
Zvolme libovolně nenulový prvek $[g(x)]_{f(x)} \in \mathbb{Z}_m[x]/(f(x))$. Tedy $g(x) \in \mathbb{Z}_m[x]$ není dělitelný polynomem $f(x)$. Protože $\mathbb{Z}_m$ je těleso, z ireducibibity $f(x)$ plyne $(g(x), f(x)) = [1]_m$ a z Bezoutovy rovnosti dostáváme existenci polynomů $a(x), b(x) \in \mathbb{Z}_m[x]$ takových, že $a(x) \cdot g(x) + b(x) \cdot f(x) = [1]_m$. Pak

$$\begin{aligned}[[1]_m]_{f(x)} &= [a(x) \cdot g(x) + b(x) \cdot f(x)]_{f(x)} = \\ &= [a(x)]_{f(x)} \cdot [g(x)]_{f(x)} + [b(x)]_{f(x)} \cdot [f(x)]_{f(x)} = \\ &= [a(x)]_{f(x)} \cdot [g(x)]_{f(x)},\end{aligned}$$

a tedy $[a(x)]_{f(x)}$ je inverzní prvek k prvku $[g(x)]_{f(x)}$.
Dostali jsme, že $\mathbb{Z}_m[x]/(f(x))$ je těleso.

# Příklad: čtyřprvkové těleso $\mathbb{Z}_2[x]/(x^2+x+[1]_2)$

*Příklad.* Opět zvolme $m = 2$, $f(x) = x^2 + x + [1]_2 \in \mathbb{Z}_2[x]$. Víme, že

$$\mathbb{Z}_2[x]/(x^2+x+1) = \left\{[0]_{x^2+x+1}, [1]_{x^2+x+1}, [x]_{x^2+x+1}, [x+1]_{x^2+x+1}\right\}.$$

Operace na této množině provádíme pomocí reprezentantů, pokud při násobení reprezentantů dostaneme polynom příliš vysokého stupně, nahradíme jej zbytkem po dělení polynomem $x^2 + x + 1$, například

$$\begin{aligned}
[x]_{x^2+x+1} + [x+1]_{x^2+x+1} &= [x + (x+1)]_{x^2+x+1} = [1]_{x^2+x+1}, \\
[x]_{x^2+x+1} \cdot [x+1]_{x^2+x+1} &= [x \cdot (x+1)]_{x^2+x+1} = \\
&= [x^2 + x]_{x^2+x+1} = [1]_{x^2+x+1},
\end{aligned}$$

kde poslední rovnost jsme dostali z toho, že zbytek po dělení polynomu $x^2 + x$ polynomem $x^2 + x + 1$ je 1.

# Jiný příklad: devítiprvkové těleso

*Příklad.* Sestrojme devítiprvkové těleso. K tomu potřebujeme normovaný ireducibilní kvadratický polynom $f(x) \in \mathbb{Z}_3[x]$. Pro kvadratické (a kubické) polynomy platí, že jsou ireducibilní nad $\mathbb{Z}_m$, právě když nejsou dělitelné lineárním polynomem ze $\mathbb{Z}_m[x]$, tj. právě když nemají kořen v $\mathbb{Z}_m$.
Snadno se ověří, že tuto podmínku splňuje polynom $x^2 + 1 \in \mathbb{Z}_3[x]$ (stejně jako dříve budeme používat tento přehlednější zápis místo přesnějšího $x^2 + [1]_3$). Zřejmě

$$\begin{aligned}\mathbb{Z}_3[x]/(x^2+1) = \{&[0]_{x^2+1}, [1]_{x^2+1}, [2]_{x^2+1},\\ &[x]_{x^2+1}, [x+1]_{x^2+1}, [x+2]_{x^2+1},\\ &[2x]_{x^2+1}, [2x+1]_{x^2+1}, [2x+2]_{x^2+1}\}.\end{aligned}$$

Ukažme si, že důkaz existence inverzního prvku na konci důkazu předchozí věty byl konstruktivní a dává nám užitečný algoritmus: spočítejme inverzní prvek $[2x+1]^{-1}_{x^2+1}$ k prvku $[2x+1]_{x^2+1}$.

Nejprve pomocí Eukleidova algoritmu najdeme největší společný dělitel polynomů $x^2+1, 2x+1 \in \mathbb{Z}_3[x]$, přestože předem víme, že jsou nesoudělné.
Největší společný dělitel najdeme v tomto případě jediným dělením:

$$x^2+1 = (2x+1)(2x-1)+2,$$

kde jsme užili $4x^2 = x^2$, neboť počítáme v $\mathbb{Z}_3[x]$, a tedy

$$1 = -(x^2+1)+(2x+1)(2x-1),$$

proto $[2x+1]^{-1}_{x^2+1} = [2x-1]_{x^2+1}$.

Pro jistotu si udělejme zkoušku: skutečně platí

$$[2x+1]_{x^2+1} \cdot [2x-1]_{x^2+1} = [4x^2-1]_{x^2+1} = [x^2-1]_{x^2+1} = \\ = [-2]_{x^2+1} = [1]_{x^2+1}.$$