Zbytkové třídy

Nechť $n \in \mathbb{N}$ a nechť $a, b \in \mathbb{Z}$. Řekneme, že čísla a, b jsou **kongruentní podle modulu** n, jestliže $n \mid a - b$. Pak píšeme $a \equiv b \pmod{n}$. Je jasné, že tato okolnost nastane, právě když čísla a, b dají po dělení číslem n stejný zbytek.

Zvolíme-li dále číslo $n \in \mathbb{N}$ pevně, pak uvedeným předpisem je definována binární relace na množině $\mathbb{Z}$, které říkáme relace kongruence podle modulu n. Je zřejmé, že tato relace je ekvivalence na $\mathbb{Z}$. Příslušnou faktorovou množinu, to znamená rozklad množiny $\mathbb{Z}$ podle této ekvivalence pak značíme $\mathbb{Z}_n$. Pro každé číslo $a \in \mathbb{Z}$ značíme $[a]_n$ třídu tohoto rozkladu obsahující a, takže máme

$$[a]_n = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\},$$

a nazýváme tuto množinu **zbytkovou třídou** čísla a podle modulu n. Pak ovšem můžeme psát

$$\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}.$$

Podle prvního tvrzení v kapitole o ekvivalencích a rozkladech ovšem pro libovolná čísla $a, b \in \mathbb{Z}$ máme

$$[a]_n = [b]_n \iff a \equiv b \pmod{n},$$

a to nastane právě tehdy, když čísla a, b dají po dělení číslem n stejný zbytek. Je-li přitom r zbytek po dělení čísla $a \in \mathbb{Z}$ číslem n, pak ovšem $n \mid a - r$, takže $a \equiv r \pmod{n}$, a tedy $[a]_n = [r]_n$. Navíc pak $r \in \{0, 1, \ldots, n-1\}$. Odtud plyne, že

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

Přitom pro $s, t \in \{0, 1, \ldots, n-1\}$ splňující $s \neq t$ zřejmě máme $[s]_n \cap [t]_n = \emptyset$. Je tedy v posledním zápisu faktorové množiny $\mathbb{Z}_n$ každá zbytková třída podle modulu n uvedena právě jednou.

Tvrzení. Pro libovolné $n \in \mathbb{N}$ a pro libovolná $a, b, c, d \in \mathbb{Z}$ platí:

$$[a]_n = [c]_n \;\&\; [b]_n = [d]_n \implies [a+b]_n = [c+d]_n.$$

Důkaz. Je-li $[a]_n = [c]_n$ a $[b]_n = [d]_n$, pak $a \equiv c \pmod{n}$ a $b \equiv d \pmod{n}$, takže existují $p, q \in \mathbb{Z}$ taková, že $a - c = n{\cdot}p$ a $b - d = n{\cdot}q$. Odtud plyne $(a+b) - (c+d) = n{\cdot}(p+q)$, takže $a+b \equiv c+d \pmod{n}$, a tedy $[a+b]_n = [c+d]_n$.

Z tohoto tvrzení plyne, že na faktorové množině $\mathbb{Z}_n$ je možno korektně definovat binární operaci $+$ následujícím způsobem. Pro libovolná $a, b \in \mathbb{Z}$ klademe

$$[a]_n + [b]_n = [a+b]_n.$$

Z úvah souvisejících s výše uvedeným výčtem všech zbytkových tříd podle modulu n pak plyne, že $[a]_n + [b]_n$ je zbytková třída $[r]_n$, kde r je zbytek po dělení součtu $a+b$ číslem n.

Věta. Pro libovolné $n \in \mathbb{N}$ je $(\mathbb{Z}_n, +)$ komutativní grupa.

Důkaz. Bezprostředně z definice operace $+$ na $\mathbb{Z}_n$ plyne, že tato operace je asociativní a komutativní — tyto vlastnosti se dědí ze sčítání čísel v $\mathbb{Z}$. Podobně se ověří, že zbytková třída $[0]_n$ je jednotkovým prvkem vzhledem k této operaci a že pro liobovolné $a \in \mathbb{Z}$ je třída $[-a]_n$ inverzním prvkem ke třídě $[a]_n$.

Tvrzení. Pro libovolné $n \in \mathbb{N}$ a pro libovolná $a, b, c, d \in \mathbb{Z}$ platí:

$$[a]_n = [c]_n \;\&\; [b]_n = [d]_n \implies [a{\cdot}b]_n = [c{\cdot}d]_n.$$

Důkaz. Je-li $[a]_n = [c]_n$ a $[b]_n = [d]_n$, pak opět $a \equiv c \pmod{n}$ a $b \equiv d \pmod{n}$, takže existují $p, q \in \mathbb{Z}$ taková, že $a - c = n{\cdot}p$ a $b - d = n{\cdot}q$. Odtud plyne $a{\cdot}b - c{\cdot}d = a{\cdot}b - c{\cdot}b + c{\cdot}b - c{\cdot}d = (a-c){\cdot}b + c{\cdot}(b-d) = n{\cdot}p{\cdot}b + c{\cdot}n{\cdot}q = n{\cdot}(p{\cdot}b + q{\cdot}c)$, takže zase $a{\cdot}b \equiv c{\cdot}d \pmod{n}$, a tedy $[a{\cdot}b]_n = [c{\cdot}d]_n$.

Z tohoto tvrzení plyne, že na faktorové množině $\mathbb{Z}_n$ je možno korektně definovat také binární operaci $\cdot$ následujícím způsobem. Pro libovolná $a, b \in \mathbb{Z}$ klademe

$$[a]_n \cdot [b]_n = [a{\cdot}b]_n.$$

Opět z úvah souvisejících s dříve uvedeným výčtem zbytkových tříd podle modulu n pak plyne, že $[a]_n \cdot [b]_n$ je zbytková třída $[r]_n$, kde r je tentokrát zbytek po dělení součinu $a{\cdot}b$ číslem n.

Věta. Pro libovolné $n \in \mathbb{N}$ je $(\mathbb{Z}_n, \cdot)$ komutativní monoid.

Důkaz. Analogicky jako v důkazu předchozí věty se přímo z definice operace $\cdot$ na $\mathbb{Z}_n$ odvodí, že tato operace je asociativní a komutativní. Podobně se rovněž ověří, že zbytková třída $[1]_n$ je jednotkovým prvkem vzhledem k této operaci.

Věta. Nechť $n \in \mathbb{N}$ a nechť $a \in \mathbb{Z}$. Pak zbytková třída $[a]_n$ má inverzní prvek v monoidu $(\mathbb{Z}_n, \cdot)$ právě tehdy, když $(a, n) = 1$, to jest právě tehdy, když čísla a, n jsou nesoudělná.

Důkaz. Nechť nejprve $b \in \mathbb{Z}$ je takové, že třída $[b]_n$ je inverzním prvkem ke třídě $[a]_n$ v $(\mathbb{Z}_n, \cdot)$. Pak $[a]_n \cdot [b]_n = [1]_n$, čili $[a{\cdot}b]_n = [1]_n$, takže $a{\cdot}b \equiv 1 \pmod{n}$. To znamená, že $n \mid a{\cdot}b - 1$, takže existuje $q \in \mathbb{Z}$ takové, že $a{\cdot}b - 1 = n{\cdot}q$, a tedy $a{\cdot}b - n{\cdot}q = 1$. Je-li nyní $e \in \mathbb{N}$ takové číslo, že $e \mid a$ a $e \mid n$, pak odtud plyne, že $e \mid 1$, takže $e = 1$. To ukazuje, že $(a, n) = 1$.

Nechť naopak $(a, n) = 1$. Pak z Bezoutovy rovnosti víme, že existují $u, v \in \mathbb{Z}$ taková, že $1 = a{\cdot}u + n{\cdot}v$. Odtud plyne, že $1 - a{\cdot}u = n{\cdot}v$, což znamená, že $1 \equiv a{\cdot}u \pmod{n}$, takže pak $[1]_n = [a{\cdot}u]_n$, a tedy $[1]_n = [a]_n \cdot [u]_n$. Poněvadž operace $\cdot$ je komutativní v $\mathbb{Z}_n$, ukazuje to, že třída $[u]_n$ je inverzním prvkem ke třídě $[a]_n$ v $(\mathbb{Z}_n, \cdot)$.

Pro libovolné $n \in \mathbb{N}$ položme

$$\mathbb{Z}_n^{\#} = \{[a]_n \mid a \in \mathbb{Z},\ (a, n) = 1\}.$$

Podle předchozí věty to tedy znamená, že $\mathbb{Z}_n^{\#}$ je právě množinou všech invertibilních prvků monoidu $(\mathbb{Z}_n, \cdot)$. Odtud a z posledního důsledku kapitoly o monoidech a grupách pak ihned plyne následující fakt.

Důsledek. Pro libovolné $n \in \mathbb{N}$ je $(\mathbb{Z}_n^{\#}, \cdot)$ komutativní grupa.

Závěrem poznamenejme, že na základě druhé části důkazu poslední věty této kapitoly víme, že inverzní prvky v $(\mathbb{Z}_n^{\#}, \cdot)$ umíme počítat kombinací Euklidova algoritmu s postupem naznačeným v důkazu Bezoutovy rovnosti.