Zbytkové třídy

Jan Paseka

Masarykova univerzita Brno

Abstrakt

V této kapitole se budeme zabývat počítáním se zbytkovými třídami.

Abstrakt

V této kapitole se budeme zabývat počítáním se zbytkovými třídami.

Budeme definovat sčítání a násobení zbytkových tříd.

Abstrakt

V této kapitole se budeme zabývat počítáním se zbytkovými třídami.

Budeme definovat sčítání a násobení zbytkových tříd.

Ukážeme, že zbytkové třídy tvoří komutativní grupu vzhledem k takto definovanému sčítání a komutativní monoid vzhledem k násobení.

Abstrakt

V této kapitole se budeme zabývat počítáním se zbytkovými třídami.

Budeme definovat sčítání a násobení zbytkových tříd.

Ukážeme, že zbytkové třídy tvoří komutativní grupu vzhledem k takto definovanému sčítání a komutativní monoid vzhledem k násobení.

Budeme charakterizovat invertibilní prvky vůči operaci násobení.

Obsah přednášky

- Kongruence $a \equiv b \pmod{n}$ podle modulu n.
- Faktorová množina $\mathbb{Z}_n$.
- Množina zbytkových tříd a operace na ní.

Obsah přednášky

- Kongruence $a \equiv b \pmod{n}$ podle modulu n.
- Faktorová množina $\mathbb{Z}_n$.
- Množina zbytkových tříd a operace na ní.

- $(\mathbb{Z}_n, +)$ je komutativní grupa.
- $(\mathbb{Z}_n, \cdot)$ je komutativní monoid.
- Invertibilní prvky v $(\mathbb{Z}_n, \cdot)$.

Kongruence podle modulu

Nechť $n \in \mathbb{N}$ a nechť $a, b \in \mathbb{Z}$. Řekneme, že čísla a, b jsou **kongruentní podle modulu** n, jestliže $n \mid a - b$.

Kongruence podle modulu

Nechť $n \in \mathbb{N}$ a nechť $a, b \in \mathbb{Z}$. Řekneme, že čísla a, b jsou **kongruentní podle modulu** n, jestliže $n \mid a - b$.

Píšeme $\boxed{a \equiv b \pmod{n}}$.

Kongruence podle modulu

Nechť $n \in \mathbb{N}$ a nechť $a, b \in \mathbb{Z}$. Řekneme, že čísla a, b jsou **kongruentní podle modulu** n, jestliže $n \mid a - b$.

Píšeme $\boxed{a \equiv b \pmod{n}}$.

$a \equiv b \pmod{n}$, právě když čísla a, b dají po dělení číslem n stejný zbytek.

Relace kongruence

Zvolme číslo $n \in \mathbb{N}$ pevně.

Relace kongruence

Zvolme číslo $n \in \mathbb{N}$ pevně.

Uvedeným předpisem je definována binární relace na množině $\mathbb{Z}$, které říkáme **relace kongruence podle modulu** n.

Relace kongruence

Zvolme číslo $n \in \mathbb{N}$ pevně.

Uvedeným předpisem je definována binární relace na množině $\mathbb{Z}$, které říkáme **relace kongruence podle modulu** n.

Tato relace je ekvivalence na $\mathbb{Z}$.

Relace kongruence

Zvolme číslo $n \in \mathbb{N}$ pevně.

Uvedeným předpisem je definována binární relace na množině $\mathbb{Z}$, které říkáme **relace kongruence podle modulu** n.

Tato relace je ekvivalence na $\mathbb{Z}$.

Příslušnou faktorovou množinu, to znamená rozklad množiny $\mathbb{Z}$ podle této ekvivalence pak značíme $\mathbb{Z}_n$.

Zbytková třída podle modulu

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.

Zbytková třída podle modulu

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.
Můžeme pak psát

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

Zbytková třída podle modulu

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.
Můžeme pak psát

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

Někdy též píšeme

$$\mathbb{Z}_n = \{k \in \mathbb{Z};\ k < n\} = \{0, 1, \dots, n-1\}.$$

Vlastnosti zbytkových tříd

Pro libovolná čísla $a, b \in \mathbb{Z}$ máme

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

Vlastnosti zbytkových tříd

Pro libovolná čísla $a, b \in \mathbb{Z}$ máme

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

Je-li r zbytek po dělení čísla $a \in \mathbb{Z}$ číslem n, platí $n \mid a - r$. Tedy $a \equiv r \pmod{n}$.

Vlastnosti zbytkových tříd

Pro libovolná čísla $a, b \in \mathbb{Z}$ máme

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

Je-li r zbytek po dělení čísla $a \in \mathbb{Z}$ číslem n, platí $n \mid a - r$. Tedy $a \equiv r \pmod{n}$.

Odtud $[a]_n = [r]_n$, $r \in \{0, 1, \ldots, n-1\}$. Zároveň pro $s, t \in \{0, 1, \ldots, n-1\}$ splňující $s \neq t$ máme $[s]_n \cap [t]_n = \emptyset$.

Vlastnosti zbytkových tříd

Pro libovolná čísla $a, b \in \mathbb{Z}$ máme

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

Je-li r zbytek po dělení čísla $a \in \mathbb{Z}$ číslem n, platí $n \mid a - r$. Tedy $a \equiv r \pmod{n}$.

Odtud $[a]_n = [r]_n$, $r \in \{0, 1, \ldots, n-1\}$. Zároveň pro $s, t \in \{0, 1, \ldots, n-1\}$ splňující $s \neq t$ máme $[s]_n \cap [t]_n = \emptyset$.

Celkem

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

$(\mathbb{Z}_n, +)$ je grupoid

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

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

$(\mathbb{Z}_n, +)$ je grupoid

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

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

Na faktorové množině $\mathbb{Z}_n$ lze korektně definovat binární operaci $+$. Pro $a, b \in \mathbb{Z}$ klademe

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

$(\mathbb{Z}_n, +)$ je grupoid

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

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

Na faktorové množině $\mathbb{Z}_n$ lze korektně definovat binární operaci $+$. Pro $a, b \in \mathbb{Z}$ klademe

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

$[a]_n + [b]_n$ je zbytková třída $[r]_n$, kde r je zbytek po dělení součtu $a+b$ číslem n.

Sčítání v $\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tabulka sčítání v $\mathbb{Z}_5$.

$(\mathbb{Z}_n, +)$ je komutativní grupa

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

$(\mathbb{Z}_n, +)$ je komutativní grupa

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

$+$ na $\mathbb{Z}_n$ je asociativní a komutativní.

$(\mathbb{Z}_n, +)$ je komutativní grupa

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

$+$ na $\mathbb{Z}_n$ je asociativní a komutativní.

zbytková třída $[0]_n$ je jednotkovým prvkem vzhledem k operaci $+$.

$(\mathbb{Z}_n, +)$ je komutativní grupa

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

$+$ na $\mathbb{Z}_n$ je asociativní a komutativní.

zbytková třída $[0]_n$ je jednotkovým prvkem vzhledem k operaci $+$.

Pro libovolné $a \in \mathbb{Z}$ je třída $[-a]_n$ inverzním prvkem ke třídě $[a]_n$.

$(\mathbb{Z}_n, \cdot)$ je grupoid

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

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

$(\mathbb{Z}_n, \cdot)$ je grupoid

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

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

Na faktorové množině $\mathbb{Z}_n$ lze korektně definovat také binární operaci $\cdot$. Pro $a, b \in \mathbb{Z}$ klademe

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

$(\mathbb{Z}_n, \cdot)$ je grupoid

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

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

Na faktorové množině $\mathbb{Z}_n$ lze korektně definovat také binární operaci $\cdot$. Pro $a, b \in \mathbb{Z}$ klademe

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

$[a]_n \cdot [b]_n$ je zbytková třída $[r]_n$, kde r je zbytek po dělení součinu $a{\cdot}b$ číslem n.

Násobení v $\mathbb{Z}_5$.

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tabulka násobení v $\mathbb{Z}_5$.

$(\mathbb{Z}_n, \cdot)$ je komutativní monoid

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

$(\mathbb{Z}_n, \cdot)$ je komutativní monoid

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

$\cdot$ na $\mathbb{Z}_n$ je asociativní a komutativní.

$(\mathbb{Z}_n, \cdot)$ je komutativní monoid

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

$\cdot$ na $\mathbb{Z}_n$ je asociativní a komutativní.

zbytková třída $[1]_n$ je jednotkovým prvkem vzhledem k operaci $\cdot$.

Inverzní prvky v $(\mathbb{Z}_n, \cdot)$

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.

Inverzní prvky v $(\mathbb{Z}_n, \cdot)$

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.

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

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

Inverzní prvky v $(\mathbb{Z}_n, \cdot)$

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.

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

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

$\mathbb{Z}_n^\#$ je právě množinou všech invertibilních prvků monoidu $(\mathbb{Z}_n, \cdot)$.

$(\mathbb{Z}_n^{\#}, \cdot)$ je komutativní grupa

Fakt: Součin nesoudělných prvků s n je nesoudělný prvek s n.

$(\mathbb{Z}_n^{\#}, \cdot)$ je komutativní grupa

Fakt: Součin nesoudělných prvků s n je nesoudělný prvek s n.

Tedy $(\mathbb{Z}_n^{\#}, \cdot)$ je komutativní monoid.

$(\mathbb{Z}_n^{\#}, \cdot)$ je komutativní grupa

Fakt: Součin nesoudělných prvků s n je nesoudělný prvek s n.

Tedy $(\mathbb{Z}_n^{\#}, \cdot)$ je komutativní monoid.

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

$(\mathbb{Z}_n^{\#}, \cdot)$ je komutativní grupa

Fakt: Součin nesoudělných prvků s n je nesoudělný prvek s n.

Tedy $(\mathbb{Z}_n^{\#}, \cdot)$ je komutativní monoid.

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

Pro libovolné $a \in \mathbb{Z}, (a, n) = 1$ existují $u, v \in \mathbb{Z}, (u, n) = 1$ taková, že $1 = a{\cdot}u + n{\cdot}v$. Tedy $[1]_n = [a]_n \cdot [u]_n$ a třída $[u]_n$ je inverzním prvkem ke třídě $[a]_n$.