Algebra - třetí díl

Lenka Zalabová

Ústav matematiky a biomatematiky, Přírodovědecká fakulta, Jihočeská univerzita v Českých Budějovicích

zima 2012

Obsah

Dělitelnost celých čísel

Definition

Řekneme, že celé číslo a *dělí* celé číslo b, jestliže existuje celé číslo q takové, že

$$b = a \cdot q.$$

V takovém případě píšeme $a \mid b$.

V opačném případě říkáme, že a *nedělí* b, a píšeme $a \nmid b$.

Dělitelnost celých čísel

Definition

Řekneme, že celé číslo a *dělí* celé číslo b, jestliže existuje celé číslo q takové, že

$$b = a \cdot q.$$

V takovém případě píšeme $a \mid b$.

V opačném případě říkáme, že a *nedělí* b, a píšeme $a \nmid b$.

Example

Platí: $7 \mid 35$ protože $35 = 7 \cdot 5$,

Dělitelnost celých čísel

Definition

Řekneme, že celé číslo a *dělí* celé číslo b, jestliže existuje celé číslo q takové, že

$$b = a \cdot q.$$

V takovém případě píšeme $a \mid b$.

V opačném případě říkáme, že a *nedělí* b, a píšeme $a \nmid b$.

Example

Platí: $7 \mid 35$ protože $35 = 7 \cdot 5$, $8 \nmid 60$,

Dělitelnost celých čísel

Definition

Řekneme, že celé číslo a *dělí* celé číslo b, jestliže existuje celé číslo q takové, že

$$b = a \cdot q.$$

V takovém případě píšeme $a \mid b$.

V opačném případě říkáme, že a *nedělí* b, a píšeme $a \nmid b$.

Example

Platí: $7 \mid 35$ protože $35 = 7 \cdot 5$, $8 \nmid 60$, $-2 \mid 6$,

Dělitelnost celých čísel

Definition

Řekneme, že celé číslo a *dělí* celé číslo b, jestliže existuje celé číslo q takové, že

$$b = a \cdot q.$$

V takovém případě píšeme $a \mid b$.

V opačném případě říkáme, že a *nedělí* b, a píšeme $a \nmid b$.

Example

Platí: $7 \mid 35$ protože $35 = 7 \cdot 5$, $8 \nmid 60$, $-2 \mid 6$, $5 \nmid -71$, ...

Nějaké vlastnosti

1. Platí $a \mid a$ pro každé $a \neq 0, a \in \mathbb{Z}$.

Nějaké vlastnosti

1. Platí $a \mid a$ pro každé $a \neq 0, a \in \mathbb{Z}$.
2. Pokud $a \mid b$ a zároveň $b \mid c$ pro nějaká $a, b, c \in \mathbb{Z}$, pak také $a \mid c$.

Nějaké vlastnosti

1. Platí $a \mid a$ pro každé $a \neq 0, a \in \mathbb{Z}$.
2. Pokud $a \mid b$ a zároveň $b \mid c$ pro nějaká $a, b, c \in \mathbb{Z}$, pak také $a \mid c$.
3. Pokud $a \mid b$ a zároveň $a \mid c$ pro nějaká $a, b, c \in \mathbb{Z}$, pak také $a \mid (bx + cy)$ pro každé $x, y \in \mathbb{Z}$.

Nějaké vlastnosti

1. Platí $a \mid a$ pro každé $a \neq 0, a \in \mathbb{Z}$.
2. Pokud $a \mid b$ a zároveň $b \mid c$ pro nějaká $a, b, c \in \mathbb{Z}$, pak také $a \mid c$.
3. Pokud $a \mid b$ a zároveň $a \mid c$ pro nějaká $a, b, c \in \mathbb{Z}$, pak také $a \mid (bx + cy)$ pro každé $x, y \in \mathbb{Z}$.
4. Pokud $a \mid b$ pro nějaká $a \in \mathbb{Z}$ a $b \neq 0$, $b \in \mathbb{Z}$, pak také $|a| \leq |b|$.

Nějaké vlastnosti

1. Platí $a \mid a$ pro každé $a \neq 0, a \in \mathbb{Z}$.
2. Pokud $a \mid b$ a zároveň $b \mid c$ pro nějaká $a, b, c \in \mathbb{Z}$, pak také $a \mid c$.
3. Pokud $a \mid b$ a zároveň $a \mid c$ pro nějaká $a, b, c \in \mathbb{Z}$, pak také $a \mid (bx + cy)$ pro každé $x, y \in \mathbb{Z}$.
4. Pokud $a \mid b$ pro nějaká $a \in \mathbb{Z}$ a $b \neq 0$, $b \in \mathbb{Z}$, pak také $|a| \leq |b|$.
5. Pokud $a \mid b$, pak také $a^n \mid b^n$ pro každé $n \in \mathbb{N}$,

Nějaké vlastnosti

1. Platí $a \mid a$ pro každé $a \neq 0, a \in \mathbb{Z}$.
2. Pokud $a \mid b$ a zároveň $b \mid c$ pro nějaká $a, b, c \in \mathbb{Z}$, pak také $a \mid c$.
3. Pokud $a \mid b$ a zároveň $a \mid c$ pro nějaká $a, b, c \in \mathbb{Z}$, pak také $a \mid (bx + cy)$ pro každé $x, y \in \mathbb{Z}$.
4. Pokud $a \mid b$ pro nějaká $a \in \mathbb{Z}$ a $b \neq 0$, $b \in \mathbb{Z}$, pak také $|a| \leq |b|$.
5. Pokud $a \mid b$, pak také $a^n \mid b^n$ pro každé $n \in \mathbb{N}$,
6. Pokud $a \mid b$ a zároveň $b \mid a$ pro nějaká $a \neq 0, b \neq 0, a, b \in \mathbb{Z}$, pak $|a| = |b|$.

Dělení se zbytkem

Theorem

Mějme celá čísla $a > 0$ a $b \geq 0$. Pak existuje jediná dvojice celých čísel q, r takových, že

- $q \geq 0$,

Dělení se zbytkem

Theorem

Mějme celá čísla $a > 0$ a $b \geq 0$. Pak existuje jediná dvojice celých čísel q, r takových, že

- $q \geq 0$,
- $0 \leq r < a$,

Dělení se zbytkem

Theorem

Mějme celá čísla $a > 0$ a $b \geq 0$. Pak existuje jediná dvojice celých čísel q, r takových, že

- $q \geq 0$,
- $0 \leq r < a$,
- $b = a \cdot q + r$.

Proof: ...

Dělení se zbytkem

Theorem

Mějme celá čísla $a > 0$ a $b \geq 0$. Pak existuje jediná dvojice celých čísel q, r takových, že

- $q \geq 0$,
- $0 \leq r < a$,
- $b = a \cdot q + r$.

Proof: ...

- q ... *podíl* po dělení čísla b číslem a
- r ... *zbytek* po dělení čísla b číslem a

Dělení se zbytkem

Theorem

Mějme celá čísla $a > 0$ a $b \geq 0$. Pak existuje jediná dvojice celých čísel q, r takových, že

- $q \geq 0$,
- $0 \leq r < a$,
- $b = a \cdot q + r$.

Proof: ...

- q ... *podíl* po dělení čísla b číslem a
- r ... *zbytek* po dělení čísla b číslem a

Example

Pro $a = 7$ a $b = 36$ dostaneme $q = 5$ a $r = 1$, t.j. $36 = 7 \cdot 5 + 1$.

Největší společný dělitel

Definition

- *Společný dělitel* celých čísel a, b je celé číslo c takové, že $c \mid b$ a zároveň $c \mid a$.
- Největší číslo s touto vlastností se nazývá *největší společný dělitel* čísel a, b.
- Označujeme jej $NSD(a, b)$.
- Čísla a, b se nazývají *nesoudělná*, jestliže $NSD(a, b) = 1$.

Eukleidův algoritmus

- Jedná se o algoritmus pro nalezení největšího společného dělitele dvou přirozených čísel.
- Protože platí:
  - $NSD(0,0)$ neexistuje,
  - $NSD(0,b) = |b|$ pro $b \neq 0, b \in \mathbb{Z}$,
  - $NSD(a,b) = NSD(|a|,|b|)$ pro $a \neq 0, b \neq 0; a,b \in \mathbb{Z}$,

  můžeme použít Eukleidův algoritmus k nalezení největšího společného dělitele dvou celých čísel.

Eukleidův algoritmus

Mějme přirozená čísla a, b a provádějme postupně dělení se zbytkem :

$$\begin{aligned}
a &= b \cdot q_0 + r_0 \\
b &= r_0 \cdot q_1 + r_1 \\
r_0 &= r_1 \cdot q_2 + r_2 \\
r_1 &= r_2 \cdot q_3 + r_3 \\
&\vdots \\
r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1} \\
r_{n-2} &= r_{n-1} \cdot q_n + r_n \\
r_{n-1} &= r_n \cdot q_{n+1}
\end{aligned}$$

Poněvadž $b > r_0 > r_1 > r_2 \ldots$, skutečně existuje n takové, že $r_n \mid r_{n-1}$, tedy $r_{n+1} = 0$.

Eukleidův algoritmus

Theorem

$$NSD(a, b) = r_n.$$

Proof: ...

Nějaké příklady

Najděte největšího společného dělitele čísel:

1. $125, 36$
2. $121, 4593$
3. $-9, 279$
4. $315, 427$

Bezoutova rovnost

Theorem

Pro libovolná celá čísla a, b existují celá čísla u, v taková, že

$$a \cdot u + b \cdot v = NSD(a, b).$$

Proof: ...

Bezoutova rovnost

Theorem

Pro libovolná celá čísla a, b existují celá čísla u, v taková, že

$$a \cdot u + b \cdot v = NSD(a, b).$$

Proof: ...

Example

Pro $a = 6$ a $b = 4$ dostaneme $NSD(a, b) = 2$ a platí

$$2 = 6 \cdot 3 + 4 \cdot (-4).$$

Nějaké další příklady

Najděte největší společný dělitel čísel a koeficienty v příslušné Bezoutovy rovnosti.

1. $168, 90$
2. $675, 1107$
3. $4597, 2$

Důležité důsledky

Corollary

Celá čísla a, b jsou nesoudělná, právě když existují celá čísla u, v taková, že $a \cdot u + b \cdot v = 1$.

Proof: ...

Důležité důsledky

Corollary

Celá čísla a, b jsou nesoudělná, právě když existují celá čísla u, v taková, že $a \cdot u + b \cdot v = 1$.

Proof: ...

Corollary

Jestliže pro celá čísla a, b, c platí $a \mid b \cdot c$ a $NSD(a, b) = 1$, pak $a \mid c$.

Proof: ...

Prvočísla

Definition

Přirozené číslo $p > 1$ se nazývá *prvočíslo*, jestliže jeho jediným dělitelem větším než 1 je p samotné.

Prvočísla

Definition

Přirozené číslo $p > 1$ se nazývá *prvočíslo*, jestliže jeho jediným dělitelem větším než 1 je p samotné.

Theorem

1. *Libovolné přirozené číslo $a > 1$ je buď prvočíslo, nebo jej lze právě jedním způsobem rozložit na součin prvočísel.*
2. *Prvočísel je nekonečně mnoho.*

Proof: ...

Kongruence

Definition

Buď n přirozené číslo. Dvě celá čísla a, b se nazývají *kongruentní podle modulu n*, jestliže $n \mid a - b$. Píšeme

$$a \equiv b \mod n.$$

Kongruence

Definition

Buď n přirozené číslo. Dvě celá čísla a, b se nazývají *kongruentní podle modulu n*, jestliže $n \mid a - b$. Píšeme

$$a \equiv b \mod n.$$

Example

Platí

$$25 \equiv 7 \mod 6,$$

protože $6 \mid 25 - 7 = 18$.

Zbytkové třídy

Definition

Buď n přirozené číslo. Množiny

$$[a]_n = \{a + k \cdot n : k \in \mathbb{Z}\},$$

kde $a \in \mathbb{Z}$, se nazývají *zbytkové třídy podle modulu n*.

Zbytkové třídy

Definition

Buď n přirozené číslo. Množiny

$$[a]_n = \{a + k \cdot n : k \in \mathbb{Z}\},$$

kde $a \in \mathbb{Z}$, se nazývají *zbytkové třídy podle modulu n*.

Example

$$\begin{aligned}[7]_6 &= \{7 + k \cdot 6 : k \in \mathbb{Z}\} \\ &= \{\ldots, -11, -5, 1, 7, 13, 19, 25, 31, \ldots\}\end{aligned}$$

Zbytkové třídy

Definition

Buď n přirozené číslo. Množiny

$$[a]_n = \{a + k \cdot n : k \in \mathbb{Z}\},$$

kde $a \in \mathbb{Z}$, se nazývají *zbytkové třídy podle modulu n*.

Example

$$\begin{aligned}[7]_6 &= \{7 + k \cdot 6 : k \in \mathbb{Z}\} \\ &= \{\ldots, -11, -5, 1, 7, 13, 19, 25, 31, \ldots\}\end{aligned}$$

Množinu všech zbytkových tříd podle modulu n označujeme symbolem $\mathbb{Z}_n$.

Jaký je vztah kongruencí a zbytkových tříd?

Theorem

$$[a]_n = [b]_n \quad \textit{právě když} \quad a \equiv b \mod n.$$

Proof: ...

Důsledky

- Zbytkové třídy podle modulu n nejsou navzájem různé. Neboli: Různá čísla mohou zadávat stejnou zbytkovou třídu modulo n.

Důsledky

- Zbytkové třídy podle modulu n nejsou navzájem různé. Neboli: Různá čísla mohou zadávat stejnou zbytkovou třídu modulo n.

Example

Protože platí, $25 \equiv 7 \mod 6$, pak platí i $[7]_6 = [25]_6$. Tedy 25 a 7 zadávají stejnou zbytkovou třídu podle modulu 6.

Důsledky

- Zbytkové třídy podle modulu n nejsou navzájem různé. Neboli: Různá čísla mohou zadávat stejnou zbytkovou třídu modulo n.

Example

Protože platí, $25 \equiv 7 \mod 6$, pak platí i $[7]_6 = [25]_6$. Tedy 25 a 7 zadávají stejnou zbytkovou třídu podle modulu 6.

- Zbytková třída $[a]_n$ se rovná zbytkové třídě $[r]_n$, kde r je zbytek po dělení čísla a číslem n.

Důsledky

- Zbytkové třídy podle modulu n nejsou navzájem různé. Neboli: Různá čísla mohou zadávat stejnou zbytkovou třídu modulo n.

Example

Protože platí, $25 \equiv 7 \mod 6$, pak platí i $[7]_6 = [25]_6$. Tedy 25 a 7 zadávají stejnou zbytkovou třídu podle modulu 6.

- Zbytková třída $[a]_n$ se rovná zbytkové třídě $[r]_n$, kde r je zbytek po dělení čísla a číslem n.

Example

Protože platí $25 = 6 \cdot 4 + 1$, dostaneme $[25]_6 = [1]_6$.
Analogicky, protože $7 = 6 \cdot 1 + 1$, dostaneme $[7]_6 = [1]_6$.

Důsledky

- Tedy $[r_n]$ se skládá ze všech čísel, jejichž zbytek po dělení číslem n je roven číslu r.

Důsledky

- Tedy $[r_n]$ se skládá ze všech čísel, jejichž zbytek po dělení číslem n je roven číslu r.

Example

$$\begin{aligned}[1]_6 &= \{1 + k \cdot 6 : k \in \mathbb{Z}\} \\ &= \{\ldots, -11, -5, 1, 7, 13, 19, 25, 31, \ldots\}\end{aligned}$$

Důsledky

- Tedy $[r_n]$ se skládá ze všech čísel, jejichž zbytek po dělení číslem n je roven číslu r.

Example

$$\begin{aligned}[1]_6 &= \{1 + k \cdot 6 : k \in \mathbb{Z}\} \\ &= \{\ldots, -11, -5, 1, 7, 13, 19, 25, 31, \ldots\}\end{aligned}$$

- Platí $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-2]_n, [n-1]_n\}$.

Důsledky

- Tedy $[r_n]$ se skládá ze všech čísel, jejichž zbytek po dělení číslem n je roven číslu r.

Example

$$\begin{aligned}[1]_6 &= \{1 + k \cdot 6 : k \in \mathbb{Z}\} \\ &= \{\ldots, -11, -5, 1, 7, 13, 19, 25, 31, \ldots\}\end{aligned}$$

- Platí $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-2]_n, [n-1]_n\}$.

Example

$$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}.$$

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ je množina sudých čísel,
- $[1]_2 = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$ je množina lichých čísel.

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ je množina sudých čísel,
- $[1]_2 = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ je množina sudých čísel,
- $[1]_2 = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$ sudé,

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$ je množina sudých čísel,
- $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$ sudé,
  sudé $+$ liché $=$

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$ je množina sudých čísel,
- $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$ sudé,
  sudé $+$ liché $=$ liché,

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$ je množina sudých čísel,
- $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$ sudé,
  sudé $+$ liché $=$ liché,
  liché $+$ liché $=$

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$ je množina sudých čísel,
- $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$ sudé,
  sudé $+$ liché $=$ liché,
  liché $+$ liché $=$ sudé,

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$ je množina sudých čísel,
- $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$ sudé,
  sudé $+$ liché $=$ liché,
  liché $+$ liché $=$ sudé,
- sudé $\cdot$ sudé $=$

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$ je množina sudých čísel,
- $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$ sudé,
  sudé $+$ liché $=$ liché,
  liché $+$ liché $=$ sudé,
- sudé $\cdot$ sudé $=$ sudé,

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$ je množina sudých čísel,
- $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$ sudé,
  sudé $+$ liché $=$ liché,
  liché $+$ liché $=$ sudé,
- sudé $\cdot$ sudé $=$ sudé,
  sudé $\cdot$ liché $=$

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$ je množina sudých čísel,
- $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$ sudé,
  sudé $+$ liché $=$ liché,
  liché $+$ liché $=$ sudé,
- sudé $\cdot$ sudé $=$ sudé,
  sudé $\cdot$ liché $=$ sudé,

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$ je množina sudých čísel,
- $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$ sudé,
  sudé $+$ liché $=$ liché,
  liché $+$ liché $=$ sudé,
- sudé $\cdot$ sudé $=$ sudé,
  sudé $\cdot$ liché $=$ sudé,
  liché $\cdot$ liché $=$

Motivace ze $\mathbb{Z}_2$

Máme $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, kde

- $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$ je množina sudých čísel,
- $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$ je množina lichých čísel.

Při počítání se sudými s lichými čísly platí následující pravidla:

- sudé $+$ sudé $=$ sudé,
  sudé $+$ liché $=$ liché,
  liché $+$ liché $=$ sudé,
- sudé $\cdot$ sudé $=$ sudé,
  sudé $\cdot$ liché $=$ sudé,
  liché $\cdot$ liché $=$ liché.

Motivace ze $\mathbb{Z}_2$

Toto lze realizovat pomocí sčítání a násobení na $\mathbb{Z}_2$ následujícím způsobem:

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\cdot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

Motivace ze $\mathbb{Z}_2$

Toto lze realizovat pomocí sčítání a násobení na $\mathbb{Z}_2$ následujícím způsobem:

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\cdot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

Neboli: Součet libovolných dvou prvků z $[0]_2$ je vždycky prvek $[0]_2$, součet libovolného prvku $[0]_2$ s libovolným prvkem $[1]_2$ je vždy prvek $[1]_2$, atd.

Operace na zbytkových třídách

Toto lze zobecnit na zbytkové třídy podle libovolného modulu:

Theorem

Buď n přirozené číslo. Vztahy

- $[a]_n + [b]_n = [a + b]_n$,
- $[a]_n \cdot [b]_n = [a \cdot b]_n$

definují korektně operace $+$ a $\cdot$ na množině $\mathbb{Z}_n$.

Proof:

Operace na zbytkových třídách

Toto lze zobecnit na zbytkové třídy podle libovolného modulu:

Theorem

Buď n přirozené číslo. Vztahy

- $[a]_n + [b]_n = [a + b]_n$,
- $[a]_n \cdot [b]_n = [a \cdot b]_n$

definují korektně operace $+$ a $\cdot$ na množině $\mathbb{Z}_n$.

Proof: Ukážeme, že když $[a]_n = [c]_n$ a $[b]_n = [d]_n$, pak

- $[a + b]_n = [c + d]_n$,
- $[a \cdot b]_n = [c \cdot d]_n$.

Grupa zbytkových tříd

Theorem

Dvojice $(\mathbb{Z}_n, +)$ *tvoří komutativní grupu pro libovolné přirozené číslo n.*

Proof: ...

Pologrupa zbytkových tříd

Theorem

Dvojice $(\mathbb{Z}_n, \cdot)$ *tvoří komutativní pologrupu s jednotkovým prvkem pro libovolné přirozené číslo n.*

Proof: ...

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

Theorem

Buď n přirozené číslo a a celé číslo. Zbytková třída $[a]_n \in \mathbb{Z}_n$ má inverzi v $(\mathbb{Z}_n, \cdot)$ právě tehdy když čísla a, n jsou nesoudělná.

Proof: ...

Nějaké příklady

- Rozhodněte, zda prvek $[35]_{37}$ má inverzi v $(\mathbb{Z}_{37}, \cdot)$. Pokud ano, najděte ji.

Nějaké příklady

- Rozhodněte, zda prvek $[35]_{37}$ má inverzi v $(\mathbb{Z}_{37}, \cdot)$. Pokud ano, najděte ji.
- Rozhodněte, zda prvek $[12]_{52}$ má inverzi v $(\mathbb{Z}_{52}, \cdot)$. Pokud ano, najděte ji.

Grupa zbytkových tříd

Theorem

Buď n prvočíslo a symbolem $\mathbb{Z}_n^*$ označme množinu všech nenulových zbytkových tříd podle modulu n, t.j.

$$\mathbb{Z}_n = \{[1]_n, [2]_n, \ldots, [n-2]_n, [n-1]_n\}.$$

Pak $(\mathbb{Z}_n^*, \cdot)$ je grupa.

Proof: ...

Kódování

- Přenášíme-li zprávu nějakým kanálem, v němž je šum, může dojít ke zkreslení zprávy.
- Kódování umožňuje odhalit, zda ke zkreslení došlo nebo dokonce opravit chyby.
- Efektivní kód by
  - měl umět opravovat chyby (s určitou pravděpodobností),
  - neměl být náročný (například by neměl výrazně prodlužovat vysílanou zprávu).
- Efektivní kódy opravující chyby lze získat pomocí konečných grup.

Hammingovy kódy

- Uvedeme dva příklady, které využívají $\mathbb{Z}_2$.
- Budeme předpokládat, že zpráva se skládá ze čtyřciferných čísel složených pouze z cifer 1 a 0.
- Jedná se o speciální případy kódů, které vymyslel americký matematik Richard Hamming v roce 1950.
- Jedná se o tzv. *lineární kódy*.

První příklad

Uvažujme matici

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Mějme $a, b, c, d \in \mathbb{Z}_2$ a nechť $abcd$ je slovo, které chceme přenést. Vytvořme vektor

$$C = \begin{pmatrix} x & y & a & z & b & c & d \end{pmatrix}^T,$$

kde $x, y, z \in \mathbb{Z}_2$ jsou takové, že

$$\begin{aligned} x + a + b + d &= 0 \\ y + a + c + d &= 0 \\ z + b + c + d &= 0. \end{aligned}$$

Tedy platí $H \cdot C = 0$, kde součin matic uvažujeme nad $\mathbb{Z}_2$, t.j. sčítáme a násobíme v $\mathbb{Z}_2$.

První příklad

Místo *abcd* přenesme *xyazbcd*. Předpokládejme, že příjemce dostane vektor *R*.

Mohou nastat tyto možnosti:

První příklad

Místo *abcd* přenesme *xyazbcd*. Předpokládejme, že příjemce dostane vektor R.

Mohou nastat tyto možnosti:

- $R = C$ ... Pak $H \cdot R = 0$.

První příklad

Místo *abcd* přenesme *xyazbcd*. Předpokládejme, že příjemce dostane vektor R.

Mohou nastat tyto možnosti:

- $R = C$ ... Pak $H \cdot R = 0$.
- R se liší od C v jedné cifře ... Pak $H \cdot R =$ některý sloupec matice H. Navíc poloha sloupce určuje pozici, ve které nastala chyba. Protože sloupce H jsou navzájem různé, příjemce to zjistí jednoznačně.

První příklad

Místo *abcd* přenesme *xyazbcd*. Předpokládejme, že příjemce dostane vektor R.

Mohou nastat tyto možnosti:

- $R = C$ ... Pak $H \cdot R = 0$.
- R se liší od C v jedné cifře ... Pak $H \cdot R =$ některý sloupec matice H. Navíc poloha sloupce určuje pozici, ve které nastala chyba. Protože sloupce H jsou navzájem různé, příjemce to zjistí jednoznačně.
- R se liší od C ve více cifrách ... Pak $H \cdot R =$ součet několika sloupců matice H. Ten může být nulový, nebo roven nějakému sloupci z H. Příjemce nezjistí nic.

Jak to funguje?

Označme $E := R - C$ rozdíl mezi přijatou a vyslanou zprávou.
Pro $R = C + E$ pak platí

$$H \cdot R = H \cdot C + H \cdot E = 0 + H \cdot E = H \cdot E.$$

Jak to funguje?

Označme $E := R - C$ rozdíl mezi přijatou a vyslanou zprávou.
Pro $R = C + E$ pak platí

$$H \cdot R = H \cdot C + H \cdot E = 0 + H \cdot E = H \cdot E.$$

- Pokud $R = C$, pak E je nulový vektor a $H \cdot R = H \cdot E = 0$.

Jak to funguje?

Označme $E := R - C$ rozdíl mezi přijatou a vyslanou zprávou. Pro $R = C + E$ pak platí

$$H \cdot R = H \cdot C + H \cdot E = 0 + H \cdot E = H \cdot E.$$

- Pokud $R = C$, pak E je nulový vektor a $H \cdot R = H \cdot E = 0$.
- Pokud R se liší od C v jedné cifře, pak E je vektor, který má jedničku na místě, kde se stala chyba, jinak samé nuly. Pak z vlastností násobení matic plyne, že $H \cdot R = H \cdot E$ se rovná sloupci, ve kterém nastala chyba.

Jak to funguje?

Označme $E := R - C$ rozdíl mezi přijatou a vyslanou zprávou. Pro $R = C + E$ pak platí

$$H \cdot R = H \cdot C + H \cdot E = 0 + H \cdot E = H \cdot E.$$

- Pokud $R = C$, pak E je nulový vektor a $H \cdot R = H \cdot E = 0$.
- Pokud R se liší od C v jedné cifře, pak E je vektor, který má jedničku na místě, kde se stala chyba, jinak samé nuly. Pak z vlastností násobení matic plyne, že $H \cdot R = H \cdot E$ se rovná sloupci, ve kterém nastala chyba.
- Pokud R se liší od C ve více cifrách, pak E je vektor, který má jedničku na všech místech kde se stala chyba, jinak samé nuly. Pak z vlastností násobení matic plyne, že $H \cdot R = H \cdot E$ je rovno součtu sloupců z H, jejichž poloha odpovídá poloze jedniček v E, t.j. poloze chyb. Ten může být nulový, nebo roven sloupci z H.

První příklad

Příjemce dekóduje následujícím způsobem:

- Vypočítá $H \cdot R$.
- Je-li výsledek nulový, cifra je předána správně. Je-li nenulový, změní cifru na indikovaném místě.
- Pokud není víc než jedna chyba v cifře, pak příjemce dostal správnou zprávu.

Druhý příklad

Uvažujme matici

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Mějme $a, b, c, d \in \mathbb{Z}_2$ a nechť $abcd$ je slovo, které chceme přenést. Vytvořme vektor

$$C = \begin{pmatrix} w & x & y & a & z & b & c & d \end{pmatrix}^T,$$

tak, aby $H \cdot C = 0$.

Druhý příklad

Označme R vektor, který dostal příjemce. Nastanou tyto možnosti:

Druhý příklad

Označme R vektor, který dostal příjemce. Nastanou tyto možnosti:

- $R = C$ ... Pak $H \cdot R = 0$.

Druhý příklad

Označme R vektor, který dostal příjemce. Nastanou tyto možnosti:

- $R = C$ ... Pak $H \cdot R = 0$.
- R se liší od C v jedné cifře ... Opravíme ji jako v prvním příkladě.

Druhý příklad

Označme R vektor, který dostal příjemce. Nastanou tyto možnosti:

- $R = C$ ... Pak $H \cdot R = 0$.
- R se liší od C v jedné cifře ... Opravíme ji jako v prvním příkladě.
- R se liší od C ve dvou cifrách ... Pak $H \cdot R =$ součet dvou sloupců z H. Ten na prvním místě má $1 + 1 = 0$ a není to tedy sloupec z H. Příjemce pozná chyby, ale neví, kde se nacházejí.