Okruh $\mathbb{Z}_m$

Minule:

1. Slepování prvků $\mathbb{Z}$ modulo m: množina $\mathbb{Z}_m$.
2. Operace na $\mathbb{Z}_m$: $\oplus_m$ (sčítání), $\odot_m$ (násobení).
3. Speciální prvky: $[0]_m$ a $[1]_m$.
4. Vlastnosti $\langle \mathbb{Z}_m, \oplus_m, \odot_m, [0]_m, [1]_m \rangle$? Velmi podobné $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$!
   Jde o komutativní okruh s jednotkou.

Definice

Ať K je neprázdná množina, na ní dvě binární operace $+ : K \times K \to K$ (čteme: sčítání) a $\cdot : K \times K \to K$ (čteme: násobení).

Uspořádaná trojice $\langle K, +, \cdot \rangle$ je okruh, pokud platí:

1. Operace $+$ je komutativní, asociativní, má neutrální prvek 0 (čteme: nula) a existují inversní prvky vzhledem k $+$.
2. Operace $\cdot$ je asociativní.
3. Operace $\cdot$ je distributivní vzhledem k operaci $+$.

Okruh $\langle K, +, \cdot \rangle$ je komutativní, pokud i operace $\cdot$ je komutativní.

Okruh $\langle K, +, \cdot \rangle$ je okruh s jednotkou, pokud i operace $\cdot$ má neutrální prvek 1 (čteme: jednička, jednotka).

Značíme: $\langle K, +, \cdot, 0, 1 \rangle$.

Příklady okruhů

1. Celá čísla: $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$. Komutativní okruh s jednotkou.
2. Celá čísla modulo m: $\langle \mathbb{Z}_m, +, \cdot, 0, 1 \rangle$. Komutativní okruh s jednotkou.
3. Reálné matice $\mathrm{Mat}_{n \times n}(\mathbb{R})$, $n \geq 2$: okruh s jednotkou, není komutativní.
4. Reálná čísla: $\langle \mathbb{R}, +, \cdot, 0, 1 \rangle$. Komutativní okruh s jednotkou. Navíc: pro každé $x \neq 0$ existuje inverse vzhledem k násobení.

Příklad

Vyřešte $6x = 12$ v $\mathbb{R}$.

$$
\begin{array}{rcll}
6x & = & 12 & \text{(6 má inversi a násobení je operace)} \\
6^{-1} \cdot (6x) & = & 6^{-1} \cdot 12 & \text{(násobení je asociativní)} \\
(6^{-1} \cdot 6) \cdot x & = & 6^{-1} \cdot 12 & (6^{-1} \cdot 6 = 1) \\
1 \cdot x & = & 6^{-1} \cdot 12 & \text{(1 je neutrální k násobení)} \\
x & = & 6^{-1} \cdot 12 &
\end{array}
$$

Příklad

Vyřešte $6x = 12$ v $\mathbb{Z}_{13}$.
Uhodneme: $6^{-1} = 11$ v $\mathbb{Z}_{13}$, protože $6 \cdot 11 = 66 = 5 \cdot 13 + 1 = 1$ v $\mathbb{Z}_{13}$.
Pak počítáme stejně:

$$\begin{array}{rcll} 6x & = & 12 & \text{(6 má inversi a násobení je operace)} \\ 6^{-1} \cdot (6x) & = & 6^{-1} \cdot 12 & \text{(násobení je asociativní)} \\ (6^{-1} \cdot 6) \cdot x & = & 6^{-1} \cdot 12 & (6^{-1} \cdot 6 = 1) \\ 1 \cdot x & = & 6^{-1} \cdot 12 & \text{(1 je neutrální k násobení)} \\ x & = & 6^{-1} \cdot 12 & (= 11 \cdot 12 = 132 = 10 \cdot 13 + 2 = 2) \end{array}$$

Vada na kráse: hádali jsme inversi.

Příklad

Vyřešte: $6x = 12$ v $\mathbb{Z}_{15}$.

Číslo 6 nemá v $\mathbb{Z}_{15}$ inversi. (Vyzkoušením všech kandidátů.)

Daná rovnice má přesně tři různá řešení: $x_1 = 2$, $x_2 = 7$ a $x_3 = 12$. (Vyzkoušením všech kandidátů.)

Vada na kráse: hrubá síla.

Věta o řešitelnosti lineárních rovnic v $\mathbb{Z}_m$

Ať a a m jsou přirozená čísla, $m \geq 2$. Ať $\gcd(a, m) = d > 0$.
Potom lineární rovnice

$$ax = b \quad \text{v } \mathbb{Z}_m$$

má řešení právě tehdy, když $d \mid b$.

Navíc, jestliže $d \mid b$, má tato rovnice v $\mathbb{Z}_m$ právě d různých řešení.

Důsledek: existence inversí

Rovnice $ax = 1$ má v $\mathbb{Z}_m$ řešení právě tehdy, když $\gcd(a, m) = 1$.
Toto řešení je jednoznačné.

Příklad

Nalezněte (pokud existuje) inversi k 6 v $\mathbb{Z}_{13}$.

Postup:

1. $\gcd(13, 6) = 1$, takže inverse existuje.
2. Bezoutova rovnost: $\gcd(13, 6) = 1 = 1 \cdot 13 + (-2) \cdot 6$ v $\mathbb{Z}$.
3. Bezoutova rovnost, přečtená v $\mathbb{Z}_{13}$: $1 = (-2) \cdot 6$ v $\mathbb{Z}_{13}$.
4. Inverse 6 v $\mathbb{Z}_{13}$: $6^{-1} = (-2) = 11$ v $\mathbb{Z}_{13}$.

Příklad

Vyřešte: $6x = 12$ v $\mathbb{Z}_{15}$.

Číslo 6 nemá v $\mathbb{Z}_{15}$ inversi, protože $\gcd(15, 6) = 3 \neq 1$.

Protože $3 \mid 12$, má daná rovnice řešení.

Řešení jsou přesně tři. Jejich nalezení:

1. $6x = 12$ v $\mathbb{Z}_{15}$ iff $6x + 15k = 12$ v $\mathbb{Z}$ pro nějaké k iff $2x + 5k = 4$ v $\mathbb{Z}$ pro nějaké k iff $2x = 4$ v $\mathbb{Z}_5$.
2. $\gcd(5, 2) = 1$, tudíž $x = 2$ v $\mathbb{Z}_5$.
3. $x_1 = 2$, $x_2 = 2 + 1 \cdot 5 = 7$, $x_3 = 2 + 2 \cdot 5 = 12$ v $\mathbb{Z}_{15}$.

Definice

Komutativní okruh s jednotkou $\langle K, +, \cdot, 0, 1\rangle$ je těleso, když platí:

$$x \neq 0 \text{ iff existuje } x^{-1}.$$

Důsledek

$\mathbb{Z}_m$ je těleso právě když m je prvočíslo.

Slogan (reklamní heslo, nikoli matematická věta):

1. V obecném $\mathbb{Z}_m$ si můžu dovolit pouze to, co si můžu dovolit v $\mathbb{Z}$.
   Jde totiž o komutativní okruhy s jednotkou.
2. V $\mathbb{Z}_p$, p prvočíslo, si můžu dovolit to, co si můžu dovolit v $\mathbb{R}$.
   Jde totiž o tělesa.

Důsledky sloganu:

1. Nad $\mathbb{Z}_p$ by měla jít vybudovat lineární algebra.
2. Měla by mít stejné vlastnosti jako lineární algebra nad $\mathbb{R}$.

Gaussova eliminace nad $\mathbb{R}$: Karl Friedrich Gauss (1777–1855)

Převod na matici v horním blokovém tvaru povolenými úpravami:

1. Prohodit dva řádky matice.
2. Vynásobit řádek matice nenulovým reálným číslem.
3. Přičíst k danému řádku lineární kombinaci ostatních řádků.

Gaussova eliminace nad $\mathbb{Z}_p$, p prvočíslo

Převod na matici v horním blokovém tvaru povolenými úpravami:

1. Prohodit dva řádky matice.
2. Vynásobit řádek matice nenulovým číslem v $\mathbb{Z}_p$.
3. Přičíst k danému řádku lineární kombinaci ostatních řádků.

Poznámky ke GEM (Gaussově eliminační metodě)

1. GEM používáme pouze v $\mathbb{Z}_p$, p prvočíslo.
2. Hodnost matice $\mathbb{A}$ je číslo $\mathrm{rank}(\mathbb{A})$. Jde o počet nenulových řádků po skončení GEM.
3. Algoritmy založené na GEM: řešení soustav lineárních rovnic, výpočet inversní matice

$$(\mathbb{A}|\mathbb{E}) \sim \cdots \sim (\mathbb{E}|\mathbb{A}^{-1})$$

   apod.
4. V $\mathbb{Z}_m$, m složené, GEM nedefinujeme. Tudíž: řešení soustav lineárních rovnic nebudeme popisovat, výpočet inversní matice jiným algoritmem.

Věta (Frobeniova věta nad $\mathbb{Z}_p$)

Soustava $\mathbb{A}x = b$ *má řešení právě tehdy, když* $\operatorname{rank}(\mathbb{A}) = \operatorname{rank}(\mathbb{A}|b)$.
Obecné řešení je pak ve tvaru

$$x_p + \sum_{i=1}^{k} \alpha_i x_i, \quad \alpha_i \in \mathbb{Z}_p$$

kde

1. $k =$ *počet sloupců*$(\mathbb{A}) - \operatorname{rank}(\mathbb{A})$
2. x_p *je jakékoli řešení* $\mathbb{A}x = b$ *(tzv. partikulární řešení)*
3. $x_1, \ldots, x_k$ *jsou lineárně nezávislá řešení* $\mathbb{A}x = 0$ *(tzv. fundamentální systém)*

Příklad

Vyřešte nad $\mathbb{Z}_{13}$:

$$\begin{array}{ccccccccccc} 2x & + & 7y & + & 8z & + & u & + & 2v & = & 3 \\ 3x & + & y & + & 4z & & & + & 2v & = & 4 \\ 9x & & & + & 4z & + & 5u & + & 5v & = & 5 \end{array}$$

Postup:

1. 13 je prvočíslo: smíme použít GEM a Frobeniovu větu.
2. Provedeme GEM (značení řádkových úprav = duš. hygiena):

$$\left(\begin{array}{ccccc|c} 2 & 7 & 8 & 1 & 2 & 3 \\ 3 & 1 & 4 & 0 & 2 & 4 \\ 9 & 0 & 4 & 5 & 5 & 5 \end{array}\right) \sim \begin{array}{l} \left(\begin{array}{ccccc|c} 2 & 7 & 8 & 1 & 2 & 3 \\ 0 & 10 & 5 & 5 & 12 & 6 \\ 0 & 1 & 7 & 7 & 9 & 11 \end{array}\right) \end{array} \begin{array}{l} R_1 \\ R_2 + 5R_1 \\ R_3 + 2R_1 \end{array}$$

Příklad (pokrač.)

$$\left(\begin{array}{ccccc|c} 2 & 7 & 8 & 1 & 2 & 3 \\ 0 & 10 & 5 & 5 & 12 & 6 \\ 0 & 1 & 7 & 7 & 9 & 11 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 2 & 7 & 8 & 1 & 2 & 3 \\ 0 & 10 & 5 & 5 & 12 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)\begin{array}{l} R_1 \\ R_2 \\ 3R_3 + R_2 \end{array}$$

GEM skončila.

3. $\mathrm{rank}(\mathbb{A}) = \mathrm{rank}(\mathbb{A}|b) = 2$: řešení existuje. (Frobeniova věta!)
4. Frobeniova věta: řešení je ve tvaru

$$x_p + \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \alpha_3 \cdot x_3, \quad \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_{13}$$

(metoda organizovaného hádání).

Příklad (pokrač.)

$$\left(\begin{array}{ccccc|c} 2 & 7 & 8 & 1 & 2 & 3 \\ 0 & 10 & 5 & 5 & 12 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Partikulární řešení:

1. $x_p = (-, -, 0, 0, 0)$ (co nejvíce nul).
2. Dopočteme druhou souřadnici: $10 \cdot y = 6$ v $\mathbb{Z}_{13}$ iff $y = 11$ v $\mathbb{Z}_{13}$.
   $x_p = (-, 11, 0, 0, 0)$.
3. Dopočteme první souřadnici: $2 \cdot x + 77 = 3$ v $\mathbb{Z}_{13}$ iff $2x = 4$ v $\mathbb{Z}_{13}$ iff $x = 2$ v $\mathbb{Z}_{13}$.
   $x_p = (2, 11, 0, 0, 0)$.

Příklad (pokrač.)

$$\left(\begin{array}{ccccc|c} 2 & 7 & 8 & 1 & 2 & 0 \\ 0 & 10 & 5 & 5 & 12 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Fundamentální systém:

1. Lineární nezávislost:
$$\begin{aligned} x_1 &= (-,-,1,0,0) \\ x_2 &= (-,-,0,1,0) \\ x_3 &= (-,-,0,0,1) \end{aligned}$$
2. Dopočteme x_1 analogicky předchozímu:
$10 \cdot y + 5 = 0$ v $\mathbb{Z}_{13}$ iff $10y = 8$ v $\mathbb{Z}_{13}$ iff $y = 6$ v $\mathbb{Z}_{13}$.
$x_1 = (-, 6, 1, 0, 0)$.
$2 \cdot x + 42 + 8 = 0$ v $\mathbb{Z}_{13}$ iff $2x = 2$ v $\mathbb{Z}_{13}$ iff $x = 1$ v $\mathbb{Z}_{13}$.
$x_1 = (1, 6, 1, 0, 0)$.

Příklad (pokrač.)

3. Analogicky x_2 a x_3:
   $x_2 = (11, 6, 0, 1, 0)$, $x_3 = (11, 4, 0, 0, 1)$.
4. Celkové řešení: $(2, 11, 0, 0, 0) + \alpha_1 \cdot (1, 6, 1, 0, 0) + \alpha_2 \cdot (11, 6, 0, 1, 0) + \alpha_3 \cdot (11, 4, 0, 0, 1), \quad \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_{13}$