IPMVFMF 2025-03-21

Opomba: Vsak ostanek, ki ga dobimo
v Evklidovem algoritmu, se
izraža kot kombinacija prejšnjih ostankov.

$$r_{j-1} = k_{j+1} r_j + r_{j+1}.$$

$$r_{j+1} = r_{j-1} - k_{j+1} r_j$$

od tod lahko ugotovimo polinome
s_i, t_i ∋: $r_i = s_i p + t_i q$

$$r_0 = 1 \cdot p + 0 \cdot q$$
$$r_1 = 0 \cdot p + 1 \cdot q$$
$$r_2 = r_0 - k_2 \cdot r_1$$
$$r_3 = r_1 - k_3 \cdot r_2$$

„predpredzadnji ostanek odštejemo
k_2-kratnik predzadnjega."

r_i	s_i	t_i	k_i
r_0	1	0	//
r_1	0	1	//
r_2	1	$-k_2$	
r_3			
⋮			

Primeri od predavanj:

$$p = x^3 + 4x^2 + 3x + 2$$
$$q = x^3 + 3x^2 + 3x + 2$$

z REA dobimo tole tabelo:

	r_i	s_i	t_i	t_i
	x^3+4x^2+3x-2	1	0	
	x^3+3x^2+3x+2	0	1	
	x^2-4	1	-1	1
gcd	$7x+14$	$-(x+3)$	$x+4$	$x+3$
	0			$\frac{1}{7}(x-2)$

gcd (nenormaliziran): $7x+14$ in velja

$$7x+14 = -(x+3)\cdot p + (x+4)\cdot q$$

N

$p = x^3 + x^2 - x + 1 \qquad q = x^3 + x - 1 \quad$ v $\mathbb{Z}_2$

r_i	s_i	t_i	t_i
x^3+x^2-x+1	1	0	
x^3+x-1	0	1	
~~x^2~~	1	-1	1
$x-1$	$-x$	$1+x$	x
1	x^2+x+1	$-x^2$	$x+1$
0			

$$\gcd(p,q) = 1 = (x^2+x+1)\,p + (-x^2)\,q$$

[TELOBARDI]

def: Telobar je algebarska struktura $(K, +, \cdot)$, kjer velja

- $(K, +)$ je abelova grupa z enoto 0.
- $(K, \cdot)$ je polgrupa
  - ↪ zaprta za $\cdot$.
  - ↪ $\cdot$ je asoc.
- distributivnost z leve in z desne.

(komutativnosti v splošnem ne zahtevamo, niti ne zahtevamo obstoja multiplikativnih inverzov.)

če telobar ima enoto za množenje, rečemo ji 1, lahko govorimo o obrnljivih elementih (za $\cdot$).

- x je obrnljiv $\Leftrightarrow \exists y \neq 0 : xy = yx = 1$.

  oznaka: $y =: x^{-1}$ (enoličnost)

def: neničla $x \neq 0$ je delitelj nič $\Leftrightarrow \exists y \in K \setminus \{0\}$:

$x \cdot y = 0 \wedge y \cdot x = 0$.

Včasih razlikujemo se med levimi in desnimi delitelji niča.

N

Poišči vse obrnljive elemente in vse delitelje niča v naslednjih kolobarjih:

(a) $\mathbb{Z}_{10}$: delitelji niča: 2, 5, 4, 6, 8

obrnljivi elementi: 1, 3, 7, 9

(inverzi: 1, 7, 3, 9)

nič: 0

$$x \cdot y = 0 \quad \text{za} \quad x, y \neq 0$$

Opomba: element nikdar ni hkrati obrnljiv in delitelj niča:

$$x \cdot y = 0 \qquad x, y \neq 0$$

denimo, da ima x inverz:

„tak ne le otrepi, ne ubije" — Gorc

$$\underbrace{x^{-1} x}_{1} y = 0$$

$$\Rightarrow y = 0$$

x delitelj niča $\rightarrow \neg(x$ obrnljiv$)$

x obrnljiv $\overset{2}{\Rightarrow} \neg(x$ delitelj ničla$)$

V končnih kolobarjih velja, da je element Boolov delitelj ničla Boolov obrnljiv, dokaz na moodlu.

- $M_2(\mathbb{R})$: A obrn. $\Leftrightarrow \exists B: AB = I \Leftrightarrow \det A = 0 \Leftrightarrow$ rang $A = 2 \Leftrightarrow \ker A = \{0\} \Leftrightarrow \dim \ker A = 0$

A del. niza $\Leftrightarrow \exists B \neq 0: AB = 0$ ali $BA = 0$

Iščemo, kdaj so vse neobrnljive matrike $A \in M_2(\mathbb{R})$ delitelji ničla. Opazimo, da mora imeti A rang 1. To pomeni, da ima matrika linearno odvisni $\Rightarrow$ ima ničelnega istega vektorja $[a\ b]$.

$$A = \begin{bmatrix} ta & tb \\ la & lb \end{bmatrix} = \begin{bmatrix} t \\ l \end{bmatrix} [a\ b]$$

ter velja $[a\ b]\begin{bmatrix} -b \\ a \end{bmatrix} = 0$, lahko izračuno

$$B = \begin{bmatrix} -b & -b \\ a & a \end{bmatrix} \qquad AB = 0 \Rightarrow A \text{ delitelj ničla}$$

Opomba: podoben argument potrebe, da je matrika $A \in M_n(\mathbb{R}) \setminus \{0\}$ delitelj niča $\Leftrightarrow$ rang $A < n$.

Vemo: če $\operatorname{rang} A < n \Leftrightarrow \dim \operatorname{Ker} A < n$
$\Leftrightarrow \operatorname{Ker} A$ netrivialno $\Leftrightarrow \exists v \neq 0 : Av = 0 \Rightarrow$
za $B = [v\ v\ v\ \dots\ v]$ velja $AB = 0$

Komentar: Kolobarji, kjer so vsi neničelni elementi obrnljivi, pravimo obseg.

Primeri: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}_p$, $GF(p^k)$, $\mathbb{H}$ (kvaternioni)
p praštevilo
Galois-Field

Kolobarji, ki niso delitelji niča, so CEZ.

Primer: $\mathbb{Z}$, $F[x]$

$(K \setminus \{0\}, \cdot)$ je polgrupa

N

Opiši grupi obrnljivih elementov v kolobarjih $M_2(\mathbb{Z})$ in $M_2(\mathbb{Z}_2)$

$M_2(\mathbb{Z})$: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

formula velja za matrike v $M_2(\mathbb{R})$. Če želimo dobiti inverz v $M_2(\mathbb{Z})$, mora zgornja matrika imeti celoštevilske elemente.

Če je $\det A = \pm 1$, dobimo matriko v $M_2(\mathbb{Z})$, torej je A obrnljiva. Tudi, da velja tudi obratno, t.j. če je A obrnljiva, je $\det A = \pm 1$. Let B inverz A: $AB = I$,

$$\det A \cdot \det B = 1 \Rightarrow \det A = \det B = \pm 1$$

□

$$M_2[\mathbb{Z}_2] = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} ; \; a,b,c,d \in \mathbb{Z}_2 \right\}$$