

Увод у теорију скупова

Берберинов парадокс: Ситновник села се или брије сам или га брије Берберин. Ко брије Берберина?

Раселов парадокс

$$S = \{x, x \notin X\} \quad S \stackrel{?}{\in} S$$

$$S \in S \Rightarrow S \notin S$$

$$S \notin S \Rightarrow S \in S$$

← ово не можемо
стаирати скупом

Формирање скупова

- релација припадности ($A \in B$)

- скупови се дефинишу аксиоматски

(Зермело - Френкелова (ЗФ) теорија скупова)

① Аксиома екстензије (екстензионалности или обухватајућности)

$$S_1 = S_2 \Leftrightarrow \forall s_1 \in S_1, s_1 \in S_2 \wedge \forall s_2 \in S_2, s_2 \in S_1$$

Редослед елемената није важан

② Аксиома празног скупа (постоји празан скуп $\emptyset$)
јединствен по А1

③ Аксиома пара: за две скупе x и y постоји z чији су они једини елементи $z = \{x, y\}$

$$u \in \{x, y\} \Leftrightarrow u = x \wedge u = y$$

$\Rightarrow \{x, x\} \leftarrow$ постоји према аксиоми пара

$$\{1, 1, 1, 2, 3\} = \{1, 2, 3\}$$

$\{x, x\} = \{x\} \leftarrow$ према аксиоми екстензије

④ Аксиома уније $\forall x \exists z, u \in z \Leftrightarrow u \in x, u \in x$
 $z = \bigcup x$

Скуп a је подскуп скупа b ($a \subseteq b$) ако $\{ \forall x \in a \mid x \in b \}$

пр. скуп $\emptyset$ је подскуп сваког скупа $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

$$a \subseteq b \wedge a \neq b \Rightarrow a \subset b \text{ (правни подскуп)}$$

⑤ Aksioma partitivnosti skupa

$\forall x \exists z, z = P(x) \leftarrow$ skup svih podskupova x

$$x \in \{a, b\} \Rightarrow P(x) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

$$\cancel{P(\emptyset)} P(\emptyset) = \{\emptyset\}$$

$$a \neq \{a\}, \emptyset \neq \{\emptyset\}$$

$$P(x) = \{A \mid A \subseteq x\} \quad |x| = n \quad |P(x)| = 2^n$$

⑥ Aksioma izdvajanja podskupova (separacije)

$\forall a \forall \phi(x) \mid \{x \in a \mid \phi(x)\}$ je skup

$$\{x \in \mathbb{N} \mid \underbrace{2 \mid x}_{\phi(x)}\}$$

ПРЕСЕК:

$$A \cap B = \{x \in A \mid x \in B\}$$

НА ОСНОВУ
АКСИОМА СЕПАРАЦИЈЕ

УНИВЕРЗУМ

РАЗЛИКА:

$$A \setminus B = \{x \in A \mid x \notin B\}$$

$$A^c = \{x \in U \mid x \notin A\}$$

КОМПЛЕМЕНТ СКУПА A У
ОДНОСУ НА СКУП U

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

симетрична разлика

Уређени парови

$$\{a, b\} = \{c, d\} \Leftrightarrow (a=c \wedge b=d) \vee (a=d \wedge b=c) \quad (*)$$

доказ:

$$\Leftarrow \text{важи } (a=c \wedge b=d) \vee (a=d \wedge b=c)$$

$$1^\circ a=c \wedge b=d$$

$$\{a, b\} = \{c, d\}$$

$$2^\circ a=d \wedge b=c$$

$$\{a, b\} = \{d, c\} = \{c, d\}$$

$$\Rightarrow \text{важи } \{a, b\} = \{c, d\}$$

$$a \in \{a, b\} \Rightarrow a \in \{c, d\}$$

$$1^\circ a=c$$

$$\{a, b\} = \{a, d\}$$

$$d \in \{a, d\} \Rightarrow d \in \{a, b\}$$

$$a) d=a$$

$$\{a, b\} = \{c, d\} = \{a, a\} = \{a\}$$

$$\Rightarrow b=a \Rightarrow a=b=c=d$$

$$b) a=d \dots$$

$$2^\circ a=d$$

$$\{a, b\} = \{c, a\}$$

$$c \in \{c, a\} \Rightarrow c \in \{a, b\}$$

$$a) c=a$$

$$\{a, b\} = \{c, d\} = \{a, a\} = \{a\}$$

$$\Rightarrow b=a \Rightarrow a=b=c=d$$

$$b) c=b \dots$$

Уређени пар (a, b) скупова a и b је $\{\{a\}, \{a, b\}\}$

$$(a, b) = \{\{a\}, \{a, b\}\}$$

тврђење: За уређене парове (a, b) и (c, d) важи

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$$

доказ:

$\Leftarrow$ тривијално

$\Rightarrow$ важи $(a, b) = (c, d)$

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$$

$$\stackrel{T(*)}{\Rightarrow} \underbrace{(\{a\} = \{c\} \wedge \{a, b\} = \{c, d\})}_{1^\circ} \vee \underbrace{(\{a\} = \{c, d\} \wedge \{a, b\} = \{c\})}_{2^\circ}$$

$1^\circ \{a\} = \{c\} \Rightarrow a = c$ аксиома екстензије

$$\{a, b\} = \{c, d\} \Rightarrow \{a, b\} = \{a, d\} \Rightarrow b = d$$

$2^\circ \{a\} = \{c, d\} \Rightarrow c, d \in \{a\} \Rightarrow c = d = a$

$$\{a, b\} = \{c\} \Rightarrow a, b \in \{c\} \Rightarrow a = b = c \Rightarrow a = b = c = d$$

Декартов производ скупова A и B је $A \times B = \{(a, b) \mid a \in A, b \in B\}$

не мора важити $A \times B = B \times A$

$$A \times B = \emptyset \Leftrightarrow A = \emptyset \vee B = \emptyset$$

Особине: $(A \cup B) \times C = (A \times C) \cup (B \times C)$

$$(A \cap B) \times C = (A \times C) \cap (B \times C)$$

Уређена n -торка елемената $a_1, a_2, \dots, a_n$ је објекат $(a_1, a_2, \dots, a_n)$ такав да важи

$$(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n) \Leftrightarrow \forall i, 1 \leq i \leq n \mid a_i = b_i$$

дефиниција преко уређеног пара $(a_1, a_2, \dots, a_n) := (a_1, (a_2, (\dots, (a_{n-1}, a_n) \dots)))$

Декартов производ скупова

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}$$

важан је поредок

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Да ли је дефиниција Декартовог производа коректна?

$$a \in A, b \in B$$

$$\{a\}, \{a, b\} \subseteq A \cup B \Rightarrow \{a\}, \{a, b\} \in \mathcal{P}(A \cup B)$$

$$\{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B) \Rightarrow \{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$$

Алтернативна дефиниција $A \times B = \{z \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid \exists a \in A, \exists b \in B \mid z = \{a, b\}\}$
 $\uparrow$ АКСИОМА ИЗДВАЈАЊА ПОДСКУПА

Релације

пример $\leq, =, \subseteq$

деф. A, B скупови $\rho \subseteq A \times B$ - релација $(a, b) \in \rho, a \rho b$
 $A = B \Rightarrow \rho$ је бинарна релација

$$\text{Dom } \rho = \{a \in A \mid (\exists b \in B) a \rho b\} \leftarrow \text{домен}$$

$$\text{Im } \rho = \{b \in B \mid (\exists a \in A) a \rho b\} \leftarrow \text{слика}$$

$$\rho^{-1} = \{(b, a) \in B \times A \mid (a, b) \in \rho\} \subseteq B \times A \text{ инверзна релација}$$

$$\text{Dom}(\rho^{-1}) = \text{Im } \rho \quad \text{Im}(\rho^{-1}) = \text{Dom } \rho$$

композиција релација $\rho \subseteq A \times B, \tau \subseteq B \times C$

$$\tau \circ \rho = \{(a, c) \in A \times C \mid (\exists b \in B) (a, b) \in \rho \wedge (b, c) \in \tau\} \subseteq A \times C$$

$$a(\tau \circ \rho)c \Leftrightarrow a \rho b \wedge b \tau c, b \in B$$

Особине:

$$1) \rho \subseteq A \times B, \tau \subseteq B \times C, \gamma \subseteq C \times D \quad (\gamma \circ \tau) \circ \rho = \gamma \circ (\tau \circ \rho)$$

доказ: ~~W/B~~ ~~W/B~~ $\tau \circ \tau \subseteq B \times D, \tau \circ \rho \subseteq A \times C, (\tau \circ \tau) \circ \rho, \tau \circ (\tau \circ \rho) \subseteq A \times D$

$$(a, d) \in (\tau \circ \tau) \circ \rho \Leftrightarrow \exists b \in B \mid \begin{array}{l} (a, b) \in \rho \\ (b, d) \in \tau \circ \tau \end{array} \quad (a, d) \in \tau \circ (\tau \circ \rho) \Leftrightarrow \exists c \in C \mid \begin{array}{l} (a, c) \in \tau \circ \rho \\ (c, d) \in \tau \end{array}$$

$$(b, d) \in \tau \circ \tau \Leftrightarrow \exists c \in C \mid \begin{array}{l} (b, c) \in \tau \\ (c, d) \in \tau \end{array} \quad (a, c) \in \tau \circ \rho \Leftrightarrow \exists b \in B \mid \begin{array}{l} (a, b) \in \rho \\ (b, c) \in \tau \end{array}$$

$$\Rightarrow (a, d) \in (\tau \circ \tau) \circ \rho \Leftrightarrow \begin{array}{l} \exists b \in B \\ \exists c \in C \end{array} \mid \begin{array}{l} (a, b) \in \rho \\ (b, c) \in \tau \\ (c, d) \in \tau \end{array} \quad \Rightarrow (a, d) \in \tau \circ (\tau \circ \rho) \Leftrightarrow \begin{array}{l} \exists c \in C \\ \exists b \in B \end{array} \mid \begin{array}{l} (a, b) \in \rho \\ (b, c) \in \tau \\ (c, d) \in \tau \end{array}$$

$$A = \{1, 2, 3, 4\} \quad \rho = \{(1, 3), (4, 2), (1, 1)\} \subseteq A \times A \quad \beta = \{(3, 4), (2, 1), (4, 2)\} \subseteq A \times A$$

$$A = \{1, 2, 3, 4\} \quad \rho = \{(1, 3), (4, 2), (1, 1)\} \subseteq A \times A \quad \beta = \{(3, 4), (2, 1), (4, 2)\} \subseteq A \times A$$

$$\beta \circ \rho = \{(1, 4), (4, 1)\} \quad \rho \circ \beta = \{(3, 2), (2, 3), (2, 1)\} \Rightarrow \beta \circ \rho \neq \rho \circ \beta$$

$$2) \quad \rho \subseteq \beta \Rightarrow \rho^{-1} \subseteq \beta^{-1}$$

$$(a, b) \in \rho^{-1} \Rightarrow (b, a) \in \rho$$

$$\rho \subseteq \beta \Rightarrow (b, a) \in \beta \Rightarrow (a, b) \in \beta^{-1}$$

$$3) (\rho^{-1})^{-1} = \rho \quad (a, b) \in \rho \Leftrightarrow (b, a) \in \rho^{-1} \Leftrightarrow (a, b) \in (\rho^{-1})^{-1}$$

$$4) (\beta \cup \rho)^{-1} = \beta^{-1} \cup \rho^{-1}$$

$$(b, a) \in (\beta \cup \rho)^{-1} \Leftrightarrow (a, b) \in \beta \cup \rho$$

$$\Leftrightarrow (a, b) \in \beta \vee (a, b) \in \rho$$

$$\Leftrightarrow (b, a) \in \beta^{-1} \vee (b, a) \in \rho^{-1}$$

$$\Leftrightarrow (b, a) \in \beta^{-1} \cup \rho^{-1}$$

$$5) (\beta \cap \rho)^{-1} = \beta^{-1} \cap \rho^{-1}$$

$$(b, a) \in (\beta \cap \rho)^{-1} \Leftrightarrow (a, b) \in \beta \cap \rho$$

$$\Leftrightarrow (a, b) \in \beta \wedge (a, b) \in \rho$$

$$\Leftrightarrow (b, a) \in \beta^{-1} \wedge (b, a) \in \rho^{-1}$$

$$\Leftrightarrow (b, a) \in \beta^{-1} \cap \rho^{-1}$$

$$6) (\beta \circ \rho)^{-1} = \rho^{-1} \circ \beta^{-1} \quad \rho \subseteq A \times B \quad \beta \subseteq B \times C$$

$$(c, a) \in (\beta \circ \rho)^{-1} \Leftrightarrow (a, c) \in \beta \circ \rho$$

$$\Leftrightarrow \exists b \in B \mid (a, b) \in \rho \wedge (b, c) \in \beta$$

$$\Leftrightarrow \exists b \in B \mid (b, a) \in \rho^{-1} \wedge (c, b) \in \beta^{-1}$$

$$\Leftrightarrow (c, a) \in \rho^{-1} \circ \beta^{-1}$$

ρ бинарна релација на A ($\rho \subseteq A \times A$)

дијагонала
 $\Delta_A = \{(a, a) \in A \times A\} \subseteq A \times A$

- рефлексивна: $\forall a \in A (a, a) \in \rho$ ($\Delta_A \subseteq \rho$)
- антирефлексивна: $\forall a \in A (a, a) \notin \rho$ ($\Delta_A \cap \rho = \emptyset$)
- симетрична: $\forall a, b \in A (a \rho b \Rightarrow b \rho a)$ ($\rho = \rho^{-1}$)
- антисиметрична: $\forall a, b \in A ((a \rho b) \wedge (b \rho a) \Rightarrow a = b)$ ($\rho \cap \rho^{-1} \subseteq \Delta_A$)
- транзитивна: $\forall a, b, c \in A ((a \rho b) \wedge (b \rho c) \Rightarrow (a \rho c))$ ($\rho \circ \rho \subseteq \rho$)

ρ је симетрична акко $\rho \subseteq \rho^{-1}$

$$\Rightarrow \left. \begin{array}{l} \rho \text{ је симетрична} \\ (x, y) \in \rho \end{array} \right\} \Leftrightarrow \left. \begin{array}{l} \rho \subseteq \rho^{-1} \\ (x, y) \in \rho \end{array} \right\} \Rightarrow (x, y) \in \rho^{-1} \Rightarrow (y, x) \in \rho$$

$$\rho \text{ је симетрична па } (y, x) \in \rho \Rightarrow (x, y) \in \rho^{-1} \Rightarrow \rho \subseteq \rho^{-1} \Rightarrow \rho \text{ је симетрична}$$

$$\left. \begin{array}{l} \rho \subseteq \rho^{-1} \\ \rho^{-1} \subseteq (\rho^{-1})^{-1} \Rightarrow \rho^{-1} \subseteq \rho \end{array} \right\} \Rightarrow \rho = \rho^{-1}$$

ρ је антисиметрична акко $\rho \cap \rho^{-1} \subseteq \Delta_A$

$$\Rightarrow \left. \begin{array}{l} \rho \text{ је антисиметрична} \\ (x, y) \in \rho \cap \rho^{-1} \end{array} \right\} \Leftrightarrow \left. \begin{array}{l} \rho \cap \rho^{-1} \subseteq \Delta_A \\ (x, y) \in \rho \wedge (y, x) \in \rho \end{array} \right\} \Rightarrow (x, y) \in \rho \wedge (x, y) \in \rho^{-1} \Rightarrow (x, y) \in \rho \cap \rho^{-1} \subseteq \Delta_A$$

$$\Rightarrow (x, y) \in \rho \wedge (y, x) \in \rho \wedge \text{антисиметрична} \mid x = y, \rho \text{ је антисиметрична}$$

$$\Rightarrow x = y \Rightarrow (x, y) = (x, x) \in \Delta_A \mid$$

ρ је транзитивна акко $\rho \circ \rho \subseteq \rho$

$$\Rightarrow \left. \begin{array}{l} \rho \text{ је транзитивна} \\ (x, y) \in \rho \circ \rho \end{array} \right\} \Leftrightarrow \left. \begin{array}{l} \rho \circ \rho \subseteq \rho \\ (x, y) \in \rho \wedge (y, z) \in \rho \end{array} \right\} \Rightarrow (x, z) \in \rho \circ \rho \Rightarrow (x, z) \in \rho$$

$$\text{Како је } \rho \text{ транзитивно } \Rightarrow (x, y) \in \rho$$

$$\Rightarrow \rho \circ \rho \subseteq \rho$$

	$\subseteq$ НА $\mathbb{R}$	ПАРАЛЕЛНОСТ ПРАВИХ НА СКУПУ ПРАВИХ У ПРОСТОРИ	НОРМАЛНОСТ ПРАВИХ НА СКУПУ ПРАВИХ У ПРОСТОРИ	ρ	ζ
рефлексивност	✓	✓	/	/	/
антирефлексивност	/	/	✓	/	✓
симетричност	/	✓	✓	✓	/
антисиметричност	✓	/	/	/	✓
транзитивност	✓	✓	/	✓	/

$(b,c) \notin \zeta$

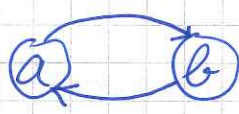
$$A = \{a, b, c\} \quad \rho = \{(a,a), (b,b), (a,b), (b,a)\} \subseteq A^2$$

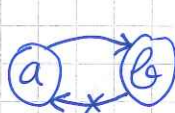
$$\zeta = \{(a,c), (b,a)\} \subseteq A^2$$

Матрични приказ особина релација

рефлексивност  $\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$

антирефлексивност  $\begin{pmatrix} 0 & & \\ & 0 & \\ & & 0 \end{pmatrix}$

симетричност  $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$

антисиметричност  $\begin{pmatrix} & 0 \\ 1 & \end{pmatrix}$

Матрица композиција релација
Нека $R, S \in M_n(\{0,1\})$. Булов производ матрица
 $R = [r_{ij}]$ и $S = [s_{ij}]$ $(R \circ S)$ је матрица

Матрица релације

$$A = \{a_1, a_2, \dots, a_m\} \quad B = \{b_1, b_2, \dots, b_n\} \quad \rho \subseteq A \times B$$

$$M_\rho = [m_{ij}]_{m \times n} \quad m_{ij} = \begin{cases} 1, & (a_i, b_j) \in \rho \\ 0, & (a_i, b_j) \notin \rho \end{cases}$$

$$M_{\rho^{-1}} = M_\rho^T$$

$$R \in M_{m \times n}(\{0, 1\}) \quad S \in M_{n \times k}(\{0, 1\})$$

Бинов производ матрица $R = [r_{ij}]$ и $S = [s_{ij}]$ $R \odot S$ је матрица $T = [t_{ij}] \in M_{m \times k}(\{0, 1\})$

$$t_{ij} = (r_{i1} \wedge s_{1j}) \vee (r_{i2} \wedge s_{2j}) \vee \dots \vee (r_{in} \wedge s_{nj})$$

три келу су бинарне $\wedge, \vee: \{0, 1\} \times \{0, 1\} \rightarrow \{0, 1\}$ дефинисане

1	0	1
0	0	0
1	0	1

1	0	1
0	0	1
1	1	1

$$\begin{matrix} \begin{bmatrix} \vdots \\ r_{i1} & r_{i2} & r_{in} \\ \vdots \end{bmatrix} & \otimes & \begin{bmatrix} s_{1j} \\ \vdots \\ s_{nj} \end{bmatrix} = \begin{bmatrix} \vdots \\ t_{ij} \\ \vdots \end{bmatrix} \\ R & & S \quad T \end{matrix}$$

$$\rho \subseteq A \times B$$

$$\delta \subseteq B \times C$$

$$M_{\delta \circ \rho} = M_\rho \odot M_\delta$$

доказ: $A = \{a_1, a_2, \dots, a_m\} \quad B = \{b_1, b_2, \dots, b_n\} \quad C = \{c_1, c_2, \dots, c_k\}$

$$M_\rho \in M_{m \times n}(\{0, 1\}) \quad M_\delta \in M_{n \times k}(\{0, 1\})$$

$$\delta \circ \rho \subseteq A \times C \quad M_{\delta \circ \rho} \in M_{m \times k}(\{0, 1\}) \quad M_\rho \odot M_\delta \in M_{m \times k}(\{0, 1\})$$

$$\Rightarrow [M_{\delta \circ \rho}]_{ij} = [M_\rho \odot M_\delta]_{ij} \quad \forall i \in \{1, \dots, m\} \quad \forall j \in \{1, \dots, k\}$$

$$\bullet [M_{\delta \circ \rho}]_{ij} = 1 \Rightarrow (a_i, c_j) \in \delta \circ \rho \Rightarrow \exists b_d \in B \mid (a_i, b_d) \in \rho \wedge (b_d, c_j) \in \delta$$

$$\Rightarrow [M_\rho]_{id} = 1 \wedge [M_\delta]_{dj} = 1$$

$$\Rightarrow [M_\rho \odot M_\delta]_{ij} = ([M_\rho]_{i1} \wedge [M_\delta]_{1j}) \vee \dots \vee ([M_\rho]_{id} \wedge [M_\delta]_{dj}) \vee \dots \vee ([M_\rho]_{in} \wedge [M_\delta]_{nj}) = 1$$

$$\bullet [M_{\delta \circ \rho}]_{ij} = 0 \Rightarrow (a_i, c_j) \notin \delta \circ \rho \Rightarrow \nexists b_d \in B \mid (a_i, b_d) \in \rho \wedge (b_d, c_j) \in \delta$$

$$\Rightarrow [M_\rho]_{id} = 0 \vee [M_\delta]_{dj} = 0 \quad \forall d \in \{1, \dots, n\}$$

$$\Rightarrow [M_\rho \odot M_\delta]_{ij} = ([M_\rho]_{i1} \wedge [M_\delta]_{1j}) \vee \dots \vee ([M_\rho]_{id} \wedge [M_\delta]_{dj}) \vee \dots \vee ([M_\rho]_{in} \wedge [M_\delta]_{nj}) = 0$$

Транзитивност и матрица релације

$$\begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$R \qquad R \qquad R^2 \subseteq R$

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$R \qquad R \qquad R^2 \not\subseteq R$

Релација еквиваленције

ρ - бинарна релација на скупу A ($\sim$)

ρ је релација еквиваленције ако је
рефлексивна, симетрична и транзитивна

$$\Delta_A \subseteq \rho$$

$$\rho = \rho^{-1}$$

$$\rho \circ \rho \subseteq \rho$$

Ако је релација рефлексивна и транзитивна онда $\rho \circ \rho \subseteq \rho$
 $(a, b) \in \rho, \Delta_A \subseteq \rho \Rightarrow (a, b) \in \rho \wedge (b, b) \in \rho \Rightarrow (a, b) \in \rho \circ \rho$

Класе еквиваленције

$\sim$ је релација еквиваленције на A

Класа еквиваленције елемента $a \in A$ је скуп

$$C_a = \{x \in A \mid a \sim x\} \subseteq A$$

Означавало ~~је~~ је и са $[a]$ и кажемо да је
елемент a представник класе C_a

Особине класа:

1. Све класе ~~су~~ еквиваленције су нејразни скупови
због рефлексивности важи $a \sim a$ па $a \in C_a \Rightarrow C_a \neq \emptyset$

2. $a, b \in A, C_a \cap C_b \neq \emptyset \Rightarrow C_a = C_b$

Покажимо да $C_a \subseteq C_b$: $C_a \cap C_b \neq \emptyset \Rightarrow \exists z \in C_a \cap C_b$

$$z \in C_a \wedge z \in C_b$$

$$\exists x \in C_a, x \sim a \Big\} \begin{matrix} \vdash \\ \vdash \end{matrix} \begin{matrix} x \sim z \\ a \sim z \end{matrix}$$

$$\begin{matrix} z \sim a \\ \downarrow \text{св} \\ a \sim z \end{matrix} \quad z \sim b$$

$$\begin{matrix} x \sim z \\ z \sim b \end{matrix} \Big\} \begin{matrix} \vdash \\ \vdash \end{matrix} x \sim b \Rightarrow x \in C_b$$

ИСТО
ВАЖИ И
 $C_b \subseteq C_a$

3. Унија свих класа еквиваленције је A
из дефиниције важи $\bigcup_{x \in A} C_x \subseteq A$

$$a \in A, a \sim a \Rightarrow a \in C_a \Rightarrow a \in \bigcup_{x \in A} C_x$$

Свака релација еквиваленције дели скуп на коме
је дефинисана на ~~непразне~~ непразне, међусобно
дисјунктне скупове чија унија је једнака том скупу.
Таква подела се зове партиција скупа.

Космички скупи скупа A за $\sim$ је $A/\sim = \{C_x | x \in A\}$

$A/\sim$ је једна партиција скупа

$$A/\sim \subseteq \mathcal{P}(A) \quad \text{јер важи } C_a \subseteq A, \forall a \in A$$

Својине:

$$1. X, Y \in A/\sim \wedge X \neq Y \Rightarrow X \cap Y = \emptyset$$

$$2. \bigcup A/\sim = \bigcup_{x \in A/\sim} X = A$$

Релација партицијалног уређења (поретка) ($\leq$)

$\mathcal{R}$ - бинарна релација на скупу A

$\mathcal{R}$ је релација партицијалног уређења ако је
рефлексивна, антисиметрична и транзитивна

$$\Delta_A \subseteq \mathcal{R}$$

$$\mathcal{R} \cap \mathcal{R}^{-1} = \Delta_A$$

$$\mathcal{R} \circ \mathcal{R} = \mathcal{R}$$

$\mathcal{R}$ је антисиметрична ако $\mathcal{R} \cap \mathcal{R}^{-1} \subseteq \Delta_A$

$\mathcal{R}$ је рефлексивна ако $(x, x) \in \Delta_A \Rightarrow (x, x) \in \mathcal{R} \Rightarrow (x, x) \in \mathcal{R}^{-1} \Rightarrow \Delta_A \subseteq \mathcal{R} \cap \mathcal{R}^{-1}$

$\mathcal{R} \circ \mathcal{R} = \mathcal{R}$ је последица рефлексивности и транзитивности

Скуп A на коме је дефинисана релација $\leq$ називамо
партицијално уређен скуп или посет. $(A, \leq)$

$\forall a, b \in A \mid a \leq b \vee b \leq a \leftarrow$ скуп је потпуно (линеарно) уређен скуп

$\rho \subseteq A^2$ поредак. a и b су упоредиви ако $a \rho b \vee b \rho a$
 У супротном, a и b су неупоредиви
 $a \rho b$: a је ρ -мање од b / b је ρ -веће од a

Поредак је линеаран (тоталан) ако су свака два елемента упоредива. У супротном, поредак је парцијалан.

- Линеарно уређен подскуп неког парцијално уређеног скупа назива се ланец.
- Подскупове парцијалног уређеног скупа у којима су свака два елемента неупоредива називамо антиланци.

Пример: 1) релација мање или једнако на $\mathbb{R}$: $\leq$
 посет: $(\mathbb{R}, \leq)$

рефлексивност: $x \leq x$ ✓

антисиметричност: $\left. \begin{matrix} x \leq y \\ y \leq x \end{matrix} \right\} \Rightarrow x = y$ ✓

транзитивност: $\left. \begin{matrix} x \leq y \\ y \leq z \end{matrix} \right\} \Rightarrow x \leq z$ ✓

2) релација деливости на скупу природних бројева: $|$
 $(\mathbb{N}, |)$

P : $x | x$

AC : $\left. \begin{matrix} x | y \\ y | x \end{matrix} \right\} \Rightarrow x = y$

$x | y \Rightarrow y = k \cdot x, k \in \mathbb{N}$

$y | x \Rightarrow x = k' \cdot y, k' \in \mathbb{N}$

$y = x \cdot k = (y \cdot k') \cdot k = y \cdot \underbrace{(k' \cdot k)}_{\in \mathbb{N}}$

$\left. \begin{matrix} k k' = 1 \\ k, k' \in \mathbb{N} \end{matrix} \right\} \Rightarrow k = k' = 1 \Rightarrow x = y$

T : $\left. \begin{matrix} x | y \\ y | z \end{matrix} \right\} \Rightarrow x | z$

$x | y \Rightarrow y = k \cdot x$

$y | z \Rightarrow z = k' \cdot y$ $k, k' \in \mathbb{N}$

$z = (k \cdot k') \cdot x \Rightarrow x | z$

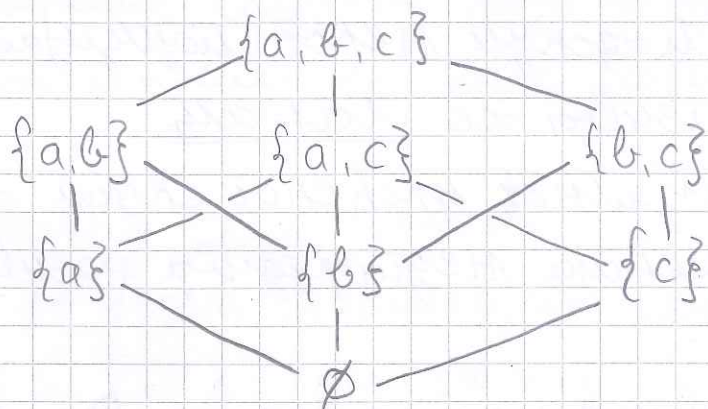
* На $\mathbb{Z}$ $\left. \begin{matrix} -1 | 1 \\ 1 | -1 \end{matrix} \right\}$ али $-1 \neq 1$

није АС на $\mathbb{Z}$

Парцијално уређени скупови могу се графички представити помоћу Хасеовог дијаграма.

- сваком ел. скупа A одговара једна тачка у равни
- тачке које одговарају елементима $x, y \in A$ су спојене линијама ако $x \leq y$, x ниже на цртењу

$X = \{a, b, c\}$ $P(X)$ уређен релацијом $\subseteq$



ρ релација парцијалног поретка на A , $B \subseteq A$. $a \in A$ је:

- МИНИМАЛАН ЕЛЕМЕНТ B ако $a \in B \mid (\forall x \in B) (x, a) \in \rho \Rightarrow x = a$
- МАКСИМАЛАН ЕЛЕМЕНТ B ако $a \in B \mid (\forall x \in B) (a, x) \in \rho \Rightarrow x = a$
- најмањи елемент (минимум) B ако $a \in B \mid (\forall x \in B) (a, x) \in \rho$
 $a = \min(B)$
- највећи елемент (максимум) B ако $a \in B \mid (\forall x \in B) (x, a) \in \rho$
 $a = \max(B)$

Ако постоји најмањи елемент, тада је он једини такав претпостављено супротно: a_1 и a_2 су најмањи

$$\Rightarrow a_1 \leq a_2 \wedge a_2 \leq a_1$$

$$\stackrel{AC}{\Rightarrow} a_1 = a_2$$

(СЛИЧНО СЕ МОЖЕ ДОКАЗАТИ ЗА НАЈВЕЋИ ЕЛЕМЕНТ)

Ако постоји најмањи елемент скупа B , тада је и једини минималан елемент: a минимум

$$(\forall x \in B) a \leq x \Rightarrow x \leq a \stackrel{AC}{\Rightarrow} x = a \leftarrow a \text{ је минимални ел.}$$

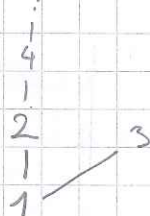
$$b \text{ минимални ел. } x \leq b \Rightarrow x = b \Rightarrow a \leq b \Rightarrow a = b$$

- Уколико постоји минималан елемент, не мора нужно постојати најмањи елемент.
- Ако постоји највећи елемент скупа B , онда је он јединствен (аналогно с најмањим доказ)
- Ако постоји највећи елемент скупа B , тада је и једини максималан елемент (исто)
- Уколико постоји максималан елемент, не мора нужно постојати највећи елемент

$$B = \{2^n \mid n \geq 0\} \cup \{3\}$$

релација деливости

ХАСЕОВ
ДИЈАГРАМ:

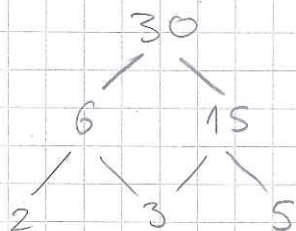


3 је једини максималан елемент
(дели сам себе и ниједан други ел.)

не постоји највећи ел. (ел. ког деле сви други елементи из B)

$$A = \{2, 3, 5, 6, 15, 30\}$$

релација деливости



НАЈМАЊИ ЕЛЕМЕНТ: /
НАЈВЕЋИ ЕЛЕМЕНТ: 30
МАКСИМАЛНА ЕЛЕМЕНТИ: 30
МИНИМАЛНИ ЕЛЕМЕНТИ: 2, 3, 5

$\leq$ -релација парцијалног уређења на скупу A

$B \subseteq A$ и $a \in A$. a је:

- доње ограничење скупа B ако $a \leq b$ ($\forall b \in B$) (МИНОРАНТА)
- горње ограничење скупа B ако $b \leq a$ ($\forall b \in B$) (МАЈОРАНТА)

ако постоји највеће доње ограничење $\leftarrow$ инфимум скупа B $\inf(B)$

ако постоји најмање горње ограничење $\leftarrow$ супремум скупа B $\sup(B)$

$$I = (0, 1) \subseteq \mathbb{R}, \leq \text{ на } \mathbb{R}$$

доња ограничења $\in (-\infty, 0]$ $\inf(I) = 0$
горња ограничења $\in [1, +\infty)$ $\sup(I) = 1$

$\cdot$ B -парцијално уређен скуп

1) Ако постоји минимум у скупу B , онда је он једнак инфимуму скупа B

доказ: b - минимум скупа B

$\Rightarrow (\forall x \in B) \quad b \leq x \Rightarrow b$ је једно доње ограничење B

b' неко доње ограничење. $b' \leq x \quad (\forall x \in B)$

специјално $b' \leq b \Rightarrow b = \inf(B)$

2) Ако постоји максимум у скупу B , онда је он једнак супремуму скупа B

доказ: b - максимум скупа B

$\Rightarrow (\forall x \in B) \quad x \leq b \Rightarrow b$ је једно горње ограничење B

b' неко горње ограничење $\Rightarrow (\forall x \in B) \quad x \leq b'$

специјално $b \leq b' \Rightarrow b = \sup(B)$

ПРИМЕР 2.39 Нека је на скупу $\mathbb{R}^2$ дефинисана бинарна релација $\leq$: $(a, b) \leq (a', b') \Leftrightarrow a \leq a' \wedge b \leq b'$

$\leq$ поредак на $\mathbb{R} \Rightarrow \leq$ је поредак на $\mathbb{R}^2$

$\leq$ није релација тоталног поретка, слика:



— 113401.jpg

КЊИТА 51 стр.

ПРЕЗ 32 слика

Функције

$f \subseteq A \times B$ релација f је функција ако $(\forall a \in \text{Dom}) \exists_1 b \in B$
т.д. $(a, b) \in f$

$b = f(a)$ b -слика елемента a при функцији f

$\text{Dom}(f) = A : f: A \rightarrow B$ f је функција из A у B
 A - ~~домен~~ домен функције B - кодомен

$f: A \rightarrow B$ и $C \subseteq A$ $f|_C := \{(x, y) \in f \mid x \in C\}$ РЕСТРИКЦИЈА ФУНКЦИЈЕ
 f НА ПОДСКУП C

Инверзна функција

$f: A \rightarrow B$ функција $\rightarrow f^{-1}$ је инверзна релација
(НЕ МОРА БИТИ ФУНКЦИЈА)

$(\forall b \in B \exists a \in A) f(a) = b$ сурјекција („на“)

$f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ ($\forall a_1, a_2 \in A$) инјекција („1-1“)

функција је бијекција ако је инјекција и сурјекција

Релација $f^{-1} \subseteq B \times A$ је функција која слика B у A
ако је $f: A \rightarrow B$ бијекција

$$\text{Dom}(f^{-1}) = \text{Im}(f) = \{ \forall b \in B \exists a \in A \mid (a, b) \in f \}$$

• потребно је да за свако $b \in \text{Dom}(f^{-1}) \exists_1 a \in A \mid f(a) = b$
 $\Rightarrow f(a_1) = f(a_2) \Rightarrow a_1 = a_2$

• ако желимо да $f^{-1}: B \rightarrow A \Rightarrow \text{Dom}(f^{-1}) = B$
 $\forall b \exists_1 a \mid f(a) = b$

Ако су релације $f \subseteq A \times B$ и $g \subseteq B \times C$ функције,
 онда је и релација $g \circ f \subseteq A \times C$ функција и важи
 $(g \circ f)(a) = g(f(a))$ за свако $a \in \text{Dom}(g \circ f)$

доказ: $g \circ f \subseteq A \times C$ ф-ја

$$\exists a \in \text{Dom}(g \circ f) \Rightarrow \exists c_1, c_2 \in C \mid (a, c_1) \in g \circ f \wedge (a, c_2) \in g \circ f \\ \Rightarrow \exists b_1, b_2 \in B \mid (a, b_1) \in f, (b_1, c_1) \in g, (a, b_2) \in f, (b_2, c_2) \in g$$

$$f \text{ је функција} \Rightarrow \begin{matrix} (a, b_1) \in f \\ (a, b_2) \in f \end{matrix} \Rightarrow b_1 = b_2 = b$$

$$g \text{ је функција} \Rightarrow \begin{matrix} (b, c_1) \in g \\ (b, c_2) \in g \end{matrix} \Rightarrow c_1 = c_2 \Rightarrow g \circ f \text{ је функција}$$

$$a \in \text{Dom}(g \circ f) \Rightarrow (\exists c \in C) (a, c) \in g \circ f$$

$$\Rightarrow (\exists b \in B) (a, b) \in f \wedge (b, c) \in g$$

$$f(a) = b \wedge g(b) = c \Rightarrow c = (g \circ f)(a) = g(b) = g(f(a))$$

$$f: A \rightarrow B \quad g: B \rightarrow C \Rightarrow g \circ f: A \rightarrow C \Rightarrow \text{Dom}(g \circ f) = A$$

$$\cdot \text{Dom}(g \circ f) \subseteq A, (\forall a \in A) f(a) \in B \wedge g(f(a)) = (g \circ f)(a) \in C$$

$$\Rightarrow a \in \text{Dom}(g \circ f) \Rightarrow A \subseteq \text{Dom}(g \circ f) \Rightarrow \text{Dom}(g \circ f) = A$$

$$f: A \rightarrow B, g: B \rightarrow C, g \circ f: A \rightarrow C \quad (g \circ f)(x) = g(f(x)) \quad \forall x \in A$$

композиција релација је асоцијативна $(h \circ g) \circ f = h \circ (g \circ f)$

Нека је $f: A \rightarrow B$. f је бијекција ако $\exists g: B \rightarrow A$ т.а.
 $g \circ f = \text{id}_A$ и $f \circ g = \text{id}_B$ ($g = f^{-1}$)

$$\text{id}_A: A \rightarrow A \quad f(a) = a \leftarrow \text{идентитетна функција на } A$$

доказ

$$\Rightarrow f: A \rightarrow B \text{ бијекција} \Rightarrow \exists f^{-1}: B \rightarrow A \Rightarrow g = f^{-1}$$

$$\text{провера: } (g \circ f)(a) = g(f(a)) = f^{-1}(f(a)) = a = \text{id}_A(a) \quad \forall a \in A$$

$$(f \circ g)(b) = f(g(b)) = f(f^{-1}(b)) = b = \text{id}_B(b) \quad \forall b \in B$$

$$\Leftarrow \exists g: B \rightarrow A \quad g \circ f = \text{id}_A \quad \wedge \quad f \circ g = \text{id}_B$$

покажимо да је f сурјекција:

$$\text{"1-1"} \quad a_1, a_2 \in A$$

$$f(a_1) = f(a_2) \stackrel{?}{\Rightarrow} a_1 = a_2$$

$$f(a_1) = f(a_2) \quad / g$$

$$g(f(a_1)) = g(f(a_2))$$

$$\underbrace{(g \circ f)(a_1)}_{\text{id}_A} = \underbrace{(g \circ f)(a_2)}_{\text{id}_A}$$

$$\text{id}_A(a_1) = \text{id}_A(a_2)$$

$$a_1 = a_2$$

$$\text{"на"} \quad b \in B$$

$$f(?) = b$$

$$(f \circ g)(b) = b$$

$$f(g(b)) = b$$

$$\Rightarrow ? = g(b)$$

$$f: A \rightarrow B \text{ сурјекција} \Rightarrow f^{-1}: B \rightarrow A \text{ сурјекција}$$

$$\left. \begin{array}{l} f^{-1} \circ f = \text{id}_A \\ f \circ f^{-1} = \text{id}_B \end{array} \right\} \Rightarrow (f^{-1})^{-1} = f$$

$$f, g \text{ сурјекције} \Rightarrow g \circ f: A \rightarrow C \text{ сурјекција, } (g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

$g \circ f$ сурјекција:

$$\text{"1-1"}: (g \circ f)(a_1) = (g \circ f)(a_2)$$

$$\Rightarrow g(f(a_1)) = g(f(a_2))$$

$$g \text{ инјекција: } f(a_1) = f(a_2)$$

$$f \text{ инјекција: } a_1 = a_2$$

$$\Rightarrow g \circ f \text{ инјекција}$$

$$\text{"на"}: c \in C$$

$$g \text{ сурјекција: } (\exists b \in B) \quad g(b) = c$$

$$f \text{ сурјекција: } (\exists a \in A) \quad f(a) = b$$

$$\Rightarrow g(f(a)) = c$$

$$\Rightarrow g \circ f \text{ сурјекција}$$

$g \circ f$ сурјекција

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ (\text{id}_B \circ f) = f^{-1} \circ f = \text{id}_A$$

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ ((f \circ f^{-1}) \circ g^{-1}) = g \circ (\text{id}_B \circ g^{-1}) = g \circ g^{-1} = \text{id}_C$$

$$\Rightarrow (g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

$g \circ f: A \rightarrow C$ бијекција $\Rightarrow f$ инјекција, g сурјекција

f „1-1“: $a_1, a_2 \in A$

$$f(a_1) = f(a_2)$$

$$\Rightarrow g(f(a_1)) = g(f(a_2))$$

$$\Rightarrow (g \circ f)(a_1) = (g \circ f)(a_2)$$

$g \circ f$ инјекција: $a_1 = a_2$

g „на“: $c \in C$

$$? (\exists b \in B) g(b) = c$$

$(g \circ f)$ сурјекција:

$$(\exists a \in A) (g \circ f)(a) = g(f(a)) = c$$

$$\Rightarrow b = f(a)$$

f је инјективна ако је ~~g~~ $g \circ f$ инјективна

g не мора да буде инјективна

Директна и инверзна слика

$$f: X \rightarrow Y \quad A \subseteq X$$

$$f[A] = \{f(x) \mid x \in A\} \leftarrow \text{директна слика скупа } A$$

$$f: X \rightarrow Y \quad A \subseteq X, B \subseteq Y \quad f[A] \subseteq B$$

$$f|_{A \rightarrow B} := f \cap (A \times B) \leftarrow \text{сужење функције } f \text{ са } A \text{ у } B$$

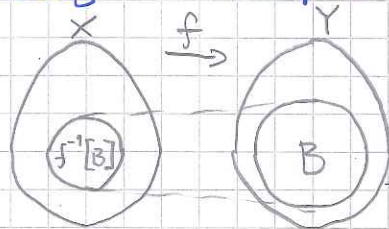
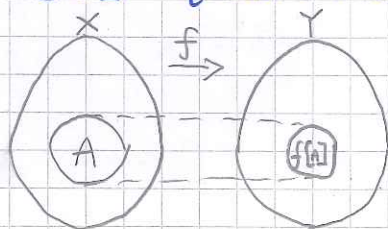
за разлику од рестрикције функције на неки подскуп,

где „смањено“ само домен функције, у сужењу

„смањено“ и домен и кодомен

$$f: X \rightarrow Y \quad B \subseteq Y$$

$$f^{-1}[B] = \{x \in X \mid f(x) \in B\} \leftarrow \text{инверзна слика скупа } B$$



$$y \in f[A] \Leftrightarrow (\exists x \in A) f(x) = y$$

$$x \in f^{-1}[B] \Leftrightarrow f(x) \in B$$

Инверзна слика скупа $f^{-1}[B]$ је дефинисана без обзира на то да ли постоји инверзна функција f^{-1}

Особине директне и инверзне слике

$$f: X \rightarrow Y \quad \text{~~A, B \subseteq X~~ \quad A, B \subseteq X}$$

$$1. f[\emptyset] = \emptyset \quad \wedge \quad f^{-1}[\emptyset] = \emptyset \quad C, D \subseteq Y$$

($\forall x \in \emptyset$) x не постоји

$$2. A \subseteq B \Rightarrow f[A] \subseteq f[B]$$

$$y \in f[A] \Rightarrow (\exists x \in A) y = f(x) \quad \left. \begin{array}{l} A \subseteq B \\ \end{array} \right\} x \in B \Rightarrow y \in f[B]$$

$$3. C \subseteq D \Rightarrow f^{-1}[C] \subseteq f^{-1}[D]$$

$$x \in f^{-1}[C] \Rightarrow f(x) \in C \quad \left. \begin{array}{l} C \subseteq D \\ \end{array} \right\} \Rightarrow f(x) \in D \Rightarrow x \in f^{-1}[D]$$

$$\bullet A, B \subseteq X \quad f: X \rightarrow Y \quad ? (f[A \cup B] = f[A] \cup f[B])$$

$$a \in f[A] \Rightarrow (\exists x \in A) a = f(x) \quad \left. \begin{array}{l} A \subseteq (A \cup B) \\ \end{array} \right\} x \in A \cup B \Rightarrow a \in f[A \cup B]$$

$$b \in f[B] \Rightarrow (\exists y \in B) b = f(y) \quad \left. \begin{array}{l} B \subseteq (A \cup B) \\ \end{array} \right\} y \in A \cup B \Rightarrow b \in f[A \cup B]$$

$$\Rightarrow f[A] \subseteq f[A \cup B] \quad \wedge \quad f[B] \subseteq f[A \cup B]$$

$$\Rightarrow f[A] \cup f[B] \subseteq f[A \cup B]$$

$$y \in f[A \cup B] \Rightarrow (\exists \underbrace{x \in A \cup B}_{x \in A \vee x \in B}) y = f(x) \Rightarrow y = f(x) \in f[A] \vee y = f(x) \in f[B] \\ \Rightarrow y \in f[A] \cup f[B]$$

$$\Rightarrow f[A] \cup f[B] = f[A \cup B]$$

$$\bullet A, B \subseteq Y \quad \wedge \quad f: X \rightarrow Y \quad \stackrel{?}{\Rightarrow} f^{-1}[A \setminus B] = f^{-1}[A] \setminus f^{-1}[B]$$

$$x \in f^{-1}[A \setminus B] \Leftrightarrow f(x) \in A \setminus B$$

$$\Leftrightarrow f(x) \in A \quad \wedge \quad f(x) \notin B$$

$$\Leftrightarrow x \in f^{-1}[A] \quad \wedge \quad x \notin f^{-1}[B]$$

$$\Leftrightarrow x \in f^{-1}[A] \setminus f^{-1}[B]$$

$$f: X \rightarrow Y \quad A \subseteq X \quad B \subseteq Y$$

$$\bullet f^{-1}[f[A]] \supseteq A \quad f \text{ "1-1"} \Rightarrow f^{-1}[f[A]] = A$$

$$x \in A \Rightarrow f(x) \in f[A] \Rightarrow x \in f^{-1}[f[A]]$$

$$x \in f^{-1}[f[A]] \Rightarrow f(x) \in f[A]$$

↑
У ГЕНЕРАЛНОМ СЛУЧАЈУ x НЕ МОРА БИТИ
ЕЛЕМЕНТ СКУПА A

нпр.: (*)

$$A = \{1\}$$

$$f[A] = \{a\}$$

$$f(2) = a \in f[A], \text{ али } 2 \notin A$$

Ако је f инјективна $\Rightarrow (\nexists x' \in A) f(x) = f(x') \in f[A]$

$$\Rightarrow f \text{ "1-1"}: f(x) \in f[A] \Rightarrow x \in A$$

$$\Rightarrow \left. \begin{array}{l} f^{-1}[f[A]] \subseteq A \\ f^{-1}[f[A]] \supseteq A \end{array} \right\} \Rightarrow f^{-1}[f[A]] = A$$

$$\bullet f[f^{-1}[B]] \subseteq B \quad f \text{ "на"} \Rightarrow f[f^{-1}[B]] = B$$

$$y \in f[f^{-1}[B]] \Rightarrow \exists \underbrace{x \in f^{-1}[B]}_{f(x) \in B} \quad (y = f(x))$$

$$\left. \begin{array}{l} y = f(x) \\ f(x) \in B \end{array} \right\} \Rightarrow y \in B \Rightarrow f[f^{-1}[B]] \subseteq B$$

$$\boxed{y \in B}$$

$$f \text{ "на"} \Rightarrow (\exists x \in X) y = f(x)$$

$$\left. \begin{array}{l} y = f(x) \in B \rightarrow x \in f^{-1}[B] \\ y = f(x) \end{array} \right\} \Rightarrow y \in f[f^{-1}[B]]$$

ако f није сурјективно, једнакост не важи

нпр. $B = \{c, d\}$

$$f^{-1}[B] = \{4\}$$

$$f[f^{-1}[B]] = f[\{4\}] = \{c\}$$

$$f[f^{-1}[B]] \subsetneq B$$

Характеристичне функције скупа

$Y^X = \{f \mid f: X \rightarrow Y\} \leftarrow$ скуп ф-ја које сликају скуп X у Y

$X, A \subseteq X \quad \chi_A: X \rightarrow \{0, 1\} \leftarrow$ КАРАКТЕРИСТИЧНА ФУНКЦИЈА СКУПА A

$$\chi_A(x) = \begin{cases} 0, & x \notin A \\ 1, & x \in A \end{cases}$$



$$\chi_\emptyset = 0 \quad (0: X \rightarrow \{0, 1\} \quad \forall x \in X \quad 0(x) = 0)$$

$$\chi_x = 1$$

X — амбијент простора

• За скупове A и B важи: $A = B$ акко $\chi_A = \chi_B$

$$\Rightarrow A = B$$

$$\Leftarrow \chi_A = \chi_B$$

$$\begin{aligned} \chi_A(x) = 1 & \Leftrightarrow x \in A \\ & \Leftrightarrow x \in B \\ & \Leftrightarrow \chi_B(x) = 1 \end{aligned}$$

$$A = \{x \mid \chi_A(x) = 1\} = \{x \mid \chi_B(x) = 1\} = B$$

$$\begin{aligned} \chi_A(x) = 0 & \Leftrightarrow x \notin A \\ & \Leftrightarrow x \notin B \\ & \Leftrightarrow \chi_B(x) = 0 \end{aligned}$$

$$\Rightarrow \chi_A = \chi_B$$

• Функција $\Phi: \mathcal{P}(X) \rightarrow \{0, 1\}^X$ дефинисана са $\Phi(A) = \chi_A$ је бијекција.

„1-1”: $\Phi(A) = \Phi(B)$

$$\Rightarrow \chi_A = \chi_B$$

$$\Rightarrow A = B$$

„на”:

$$f \in \{0, 1\}^X \quad f: X \rightarrow \{0, 1\}$$

$$? ((\exists A \subseteq X) \Phi(A) = f)$$

$$A = \{x \in X \mid f(x) = 1\} \Rightarrow f = \chi_A$$

$$\Phi(A) = \chi_A = f$$

59. стр

Нека су операције сабирања и множења на скупу $\{0, 1\}$ дефинисане:

$$\forall f, g, h \in \{0, 1\}^X$$

$$f + g = g + f$$

$$f \cdot g = g \cdot f$$

$$f + (g + h) = (f + g) + h$$

$$f \cdot (g \cdot h) = (f \cdot g) \cdot h$$

$$f(g + h) = f \cdot g + f \cdot h$$

$$(g + h) \cdot f = g \cdot f + h \cdot f$$

$$f + f = 0$$

$$f \cdot f = f$$

дефиницијом збир $f + g$
и произвог $f \cdot g$

$$(f + g)(x) \stackrel{\text{def}}{=} f(x) + g(x)$$

$$(f \cdot g)(x) \stackrel{\text{def}}{=} f(x) \cdot g(x)$$

$$\chi_{\emptyset} = 0 \quad \chi_X = 1 \quad (\text{константные функции})$$

$$\chi_{A \cap B} = \chi_A \chi_B$$

$$\chi_{A \cap B}(x) = 1 \Leftrightarrow x \in A \cap B$$

$$\Leftrightarrow x \in A \wedge x \in B$$

$$\Leftrightarrow \chi_A(x) = 1 \wedge \chi_B(x) = 1$$

$$\Leftrightarrow \chi_A(x) \chi_B(x) = 1$$

$$\chi_{A \cap B}(x) = 0 \Leftrightarrow x \notin A \cap B$$

$$\Leftrightarrow x \notin A \vee x \notin B$$

$$\Leftrightarrow \chi_A(x) = 0 \vee \chi_B(x) = 0$$

$$\Leftrightarrow \chi_A(x) \chi_B(x) = 0$$

$$\chi_{A \cup B} = \chi_A + \chi_A \chi_B + \chi_B$$

$$x \in A \cup B \Leftrightarrow x \in (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$$

$$\chi_A + \chi_A \chi_B$$

$$\chi_B + \chi_A \chi_B$$

$$\chi_A \chi_B$$

$$\Rightarrow \chi_A + \chi_A \chi_B + \chi_B + \chi_A \chi_B + \chi_A \chi_B = \chi_A + \chi_A \chi_B + \chi_B$$

$$\chi_{A^c} = 1 + \chi_A$$

$$\chi_{A^c} \Leftrightarrow x \in A^c$$

$$\Leftrightarrow x \notin A$$

$$\Leftrightarrow \chi_A = 0$$

$$\chi_A = 1$$

$$\Leftrightarrow 1 + \chi_A = 1$$

$$1 + \chi_A = 0$$

$$\chi_{A \setminus B} = \chi_A + \chi_A \chi_B$$

$$A \setminus B = A \cap B^c = \chi_A \chi_B^c = \chi_A (1 + \chi_B)$$

$$= \chi_A + \chi_A \chi_B$$

$$\chi_A \chi_A = \chi_A$$

$$\chi_A \chi_A = \chi_{A \cap A} = \chi_A$$

$$\chi_{A \Delta B} = \chi_A + \chi_B$$

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

$$= \chi_{A \setminus B} + \chi_{B \setminus A}$$

$$= \chi_A + \chi_A \chi_B + (\chi_A + \chi_A \chi_B)(\chi_B + \chi_A \chi_B) + \chi_B + \chi_A \chi_B$$

$$= \chi_A + \chi_B + \chi_A \chi_B + \chi_A \chi_A \chi_B + \chi_A \chi_B \chi_B + \chi_A \chi_B \chi_A \chi_B$$

$$= \chi_A + \chi_B + \chi_A \chi_B + \chi_A \chi_B + \chi_A \chi_B + \chi_A \chi_B$$

$$= \chi_A + \chi_B$$

$$\chi_A + \chi_A = 0$$

$$1^\circ \chi_A = 1$$

$$1 + 1 = 0$$

$$2^\circ \chi_A = 0$$

$$0 + 0 = 0$$

Канторов теорема

Нека је X произвољан скуи. Постоји инјекција из X у $\mathcal{P}(X)$, али не постоји бијекција између тих скуиова

доказ: $f: X \rightarrow \mathcal{P}(X)$

$$f(a) = \{a\}$$

$$a \in X, \{a\} \in \mathcal{P}(X)$$

f је инјективно

$$f(a) = f(b) \Rightarrow \{a\} = \{b\}$$

$$\Rightarrow a \in \{b\} \Rightarrow a = b$$

п.п.с. постоји бијекција

$$h: X \rightarrow \mathcal{P}(X)$$

$$(\forall x \in X) h(x) \in \mathcal{P}(X)$$

дефинишемо функцију

$$g: X \rightarrow \{0, 1\}$$

$$g(x) = \chi_{h(x)}(x) + 1$$

g је карактеристична

ф-ја неког скуиа A

$$g = \chi_A, A \subseteq X$$

$$A \subseteq X \text{ тј } A \in \mathcal{P}(X) \left\{ \Rightarrow (\exists x_0) h(x_0) = A \right.$$

h је „на“

$$g = \chi_A = \chi_{h(x_0)}$$

$$(\forall x \in X) g(x) = \chi_{h(x_0)}(x)$$

специјално, за $x = x_0$

$$g(x_0) = \chi_{h(x_0)}(x_0)$$

$$= \chi_{h(x_0)}(x_0) + 1$$

(Канторов метод
дијагонализације)



Природни бројеви

- Аксиома доброг заснивања или регуларности
 $\forall A \neq \emptyset \quad a \in A \quad A \cap a = \emptyset$

последице:

1. $(\exists x) \quad x \in x$
2. $(\exists x, y) \quad x \in y \wedge y \in x$
3. $(\exists x_0, x_1, x_2 \dots) \quad x_0 \ni x_1 \ni x_2 \ni \dots$

1. нпс $(\exists x) \quad x \in x$

$$A = \{x\}$$

$$\left. \begin{array}{l} x \in A \\ x \in x \end{array} \right\} \Rightarrow x \in A \cap x \Rightarrow A \cap x \neq \emptyset$$

x је једини ел. скупа A

$$A \cap x \neq \emptyset$$

$\hookrightarrow$ у супротности са аксиомом регуларности

2. нпс $(\exists x, y) \quad x \in y \wedge y \in x$

$$A = \{x, y\}$$

$$\left. \begin{array}{l} x \in y \\ x \in A \end{array} \right\} x \in A \cap y \Rightarrow A \cap y \neq \emptyset$$

$$\left. \begin{array}{l} y \in x \\ y \in A \end{array} \right\} y \in A \cap x \Rightarrow A \cap x \neq \emptyset$$

$$\left. \begin{array}{l} x \text{ и } y \text{ су једини елементи } A \\ A \cap x \neq \emptyset \\ A \cap y \neq \emptyset \end{array} \right\}$$

$\hookrightarrow$ са аксиомом регуларности

3. нпс $(\exists x_0, x_1, x_2 \dots) \quad x_0 \ni x_1 \ni x_2 \ni \dots$

$$A = \{x_0, x_1, x_2, \dots\}$$

$$x_{i+1} \in x_i \quad \forall i \geq 0$$

$$\left. \begin{array}{l} x_{i+1} \in x_i \\ x_{i+1} \in A \end{array} \right\} x_{i+1} \in A \cap x_i \Rightarrow A \cap x_i \neq \emptyset$$

$x_i, i \geq 0$ су једини елементи скупа A $A \cap x_i \neq \emptyset \hookrightarrow$ са аксиомом РЕГУЛАРНОСТИ

$$x \cup \{x\} = y \cup \{y\} \Rightarrow x = y$$

ппс $x \neq y$

$$x \in x \cup \{x\} \Rightarrow x \in y \cup \{y\} \begin{cases} x \in y & \text{јер } x \neq y \\ x = y \end{cases}$$

$$y \in y \cup \{y\} \Rightarrow y \in x \cup \{x\} \begin{cases} y \in x & \text{јер } x \neq y \\ y = x \end{cases} \Rightarrow x \in x \quad \begin{matrix} \text{СА ДРУГОМ} \\ \text{ПОСЛЕДИЦОМ} \\ \text{АКСИОМЕ} \\ \text{РЕГУЛАРНОСТИ} \end{matrix}$$

Пеанове аксиоме

' - функција следбеника, МОРА БИТИ ИНЈЕКТИВНА „1-1“ ДА БИСМО МОГЛИ ДА КРЕИРАМО ДРУГЕ БРОЈЕВЕ

- П1 0 је природан број
- П2 АКО ЈЕ x ПРИРОДАН БРОЈ, ОНДА ЈЕ И x' ПРИРОДАН БРОЈ
- П3 АКО СУ x И y ПРИРОДНИ БРОЈЕВИ И $x' = y'$, ОНДА ЈЕ $x = y$
- П4 ЗА СВАКИ ПРИРОДАН БРОЈ x ВАНИ $x' \neq 0$
- П5 НЕКА ЈЕ Φ СВОЈСТВО ПРИРОДНИХ БРОЈЕВА ЗА КОЈЕ ВАНИ:
- 1) 0 има својство Φ
 - 2) АКО ПРИРОДАН БРОЈ x ИМА СВОЈСТВО Φ , ТАДА И x' ИМА СВОЈСТВО Φ
- тада сваки природни број има својство Φ

0 - симбол константе ' - унарни функцијски симбол

Пеанове аксиоме описују природне бројеве али не говоре на коју структуру се тачно мисли!

Фон Нойманов модел природних бројева заснован на теорији скупова: $0 := \emptyset$ $1 := \{0\}$ $2 := \{0, 1\}$ $3 := \{0, 1, 2\}$
 прецизније $0 := \emptyset$, $n' = n \cup \{n\}$, $\mathbb{N} := \{0, 1, 2, \dots\}$

НЕ МОРА БИТИ ЈЕДИНИ МОДЕЛ ПРИРОДНИХ БРОЈЕВА, БИТИНО ЈЕ ДА ЗАДОВОЉАВА ПЕАНОВЕ АКСИОМЕ

Фон Нойманов модел природних бројева задовољава Пеанове аксиоме

доказ: Π_1 и Π_2 важе на основу дефиниције
пр. бр. у Фон Ноймановом моделу

$$\Pi_3: X' = Y' \Rightarrow X = Y$$

$$X \cup \{x\} = Y \cup \{y\} \Rightarrow X = Y$$

$$\Pi_4: X' \neq \emptyset$$

$$X' = X \cup \{x\} \Rightarrow x \in X' \Rightarrow X' \neq \emptyset \Rightarrow X' \neq 0$$

$$0 = \emptyset$$

Π_5 : Нека је $\Phi(0)$ тачно, и нека је $\Phi(x')$ тачно
кад год је $\Phi(x)$ тачно

ппс $(\exists n \in \mathbb{N}) \Phi(n)$ не важи

како је $\Phi(0)$ тачно $\Rightarrow n \neq 0$

$$\Rightarrow (\exists n_1) n = n_1'$$

важи да је $\Phi(n) = \Phi(n_1')$ нетачно па је на
основу 2. претпоставке и $\Phi(n_1)$ нетачно

$\Phi(n_1)$ је нетачно $\Rightarrow n \neq 0$

$$\Rightarrow (\exists n_2) n_1 = n_2'$$

нетачно је $\Phi(n_1) = \Phi(n_2') \Rightarrow$ нетачно је $\Phi(n_2)$ итд

$$n_1' = n_1 \cup \{n_1\} = n \Rightarrow n_1 \in n$$

$$n_2' = n_2 \cup \{n_2\} = n_1 \Rightarrow n_2 \in n_1$$

$$\vdots$$

$n \ni n_1 \ni n_2 \ni \dots$ $\hookrightarrow$ са 3. последњом
аксиоме рекурзије

Принцип математичке индукције

Нека је Φ својство природних бројева за које важи

1) тачно је $\Phi(0)$ - база индукције

2) ако је за пр.бр. n тачно $\Phi(n)$, онда је тачно и $\Phi(n+1)$
ИНДУКТИВНИ КОРАК

$\Phi(n)$ — ИНДУКТИВНА ПРЕТПОСТАВКА (хипотеза)

Има аритметичких тврђења која не важе за неколико најмањих пр.бр., али су тачна за све остале ($2^n > n+1$, $n \geq 2$). У тим случајевима можемо користити мало измењен принцип:

Нека је Φ својство природних бројева за које важи

1) тачно је $\Phi(k)$

2) ако за природан број $n \geq k$ тачно $\Phi(n)$, онда је тачно и $\Phi(n+1)$

Тада је за сваки природан број $n \geq k$ тачно $\Phi(n)$

Принцип потпуне индукције

Нека је Φ својство природних бројева и нека важи:

ако су $\Phi(0), \Phi(1), \Phi(2), \dots, \Phi(n)$ тачни, тачно је и $\Phi(n')$,
за све $n \in \mathbb{N}$. Тада $\Phi(n)$ важи за све природне бројеве n .

$\Phi(0), \Phi(1), \dots, \Phi(n) \Rightarrow \Phi(n+1) \Rightarrow \Phi(n+2) \Rightarrow \dots$

доказ: Ψ својство

$\Psi(n)$: $\Phi(k)$ је тачно за све $k \leq n$

показује да је Ψ тачно за све $\mathbb{N}$ применом мат. индук.

база: $\Psi(0)$?

$\Psi(0)$: $\Phi(0)$ је тачно

индуктивни корак: $\Psi(n) \stackrel{?}{\Rightarrow} \Psi(n+1)$

$\Psi(n)$: $\Phi(k)$ је тачно за $k \leq n$

$\Psi(n+1)$: $\Phi(k)$ је тачно за $k \leq n+1$

тачно је $\Psi(n)$, тј. тачно је $\Phi(0), \Phi(1), \dots, \Phi(n)$

$\stackrel{п.и.}{\Rightarrow} \Phi(n+1) \Rightarrow$ тачно је $\Phi(0), \Phi(1), \dots, \Phi(n), \Phi(n+1)$
 $\Psi(n+1)$

Ψ је тачно за све природне бројеве
 m је произвољан $\mathbb{N}$

важи $\Psi(m)$, тј. тачно је $\Phi(0), \Phi(1), \dots, \Phi(m)$

Дакле, за произвољан природан број m важи $\Phi(m)$

За природне бројеве x и y операција сабирања дефинисана:

$$m+0 := m$$

$$m+n' := (m+n)'$$

Својине сабирања: $\forall m, n, k \in \mathbb{N}$

$$1. (m+n)+k = m+(n+k) = \Phi(k)$$

индукција по k

бп: $\Phi(0)$

$$(m+n)+0 = m+n$$

$$m+(n+0) = m+n$$

ик: $\Phi(k) \Rightarrow \Phi(k')$

важи: $(m+n)+k = m+(n+k)$

доказујемо: $(m+n)+k' = m+(n+k')$

$$(m+n)+k' = ((m+n)+k)' \stackrel{ix}{=} (m+(n+k))'$$

$$= m+(n+k)' = m+(n+k')$$

$$2. m+0 = 0+m = m$$

$$m+0 = m \checkmark$$

$$0+m = m? = \Phi(m)$$

индукција по m

бп: $\Phi(0) = ?$

$$0+0 = 0 \quad \oplus$$

ик: $\Phi(m) \Rightarrow \Phi(m')$

важи $0+m = m$ (и x)

доказујемо $0+m' = m'$

$$0+m' = (0+m)' \stackrel{ix}{=} m'$$

$$m+0 = m = 0+m$$

$$3. m+1 = 1+m = m'$$

$$m+1 = m+0' = (m+0)' = m'$$

$\Phi(m): m+1 = 1+m$

индукција
по m

бп: $\Phi(0) = ?$

$$0+1 = 0+0' = (0+0)' = 0' = 1$$

$$1+0 = 1$$

ик: $\Phi(n) \Rightarrow \Phi(n+1)$

и x : $m+1 = 1+m$

доказујемо: $m'+1 = 1+m'$

$$1+m' = (1+m)' \stackrel{ix}{=} (m+1)' = m'+1$$

$$= m+1+1 = m'+1$$

$$4. m+n = n+m$$

$$\phi(n): m+n = n+m$$

$$\text{б.и.} : m+0 = 0+m \quad \textcircled{+}$$

$$\text{и.к.} : \phi(n) \stackrel{?}{=} \phi(n+1)$$

$$\text{важни } m+n = n+m \text{ (и } x)$$

$$\text{доказујемо: } m+n' = n'+m$$

$$m+n' = (m+n)' \stackrel{\text{и.к.}}{=} (n+m)'$$

$$= n+m' = n+1+m$$

$$= (n+1)+m = n'+m$$

$$5. m+n=0 \Rightarrow m=0 \vee n=0$$

$$\text{п.н.с. } m \neq 0$$

$$(\exists k \in \mathbb{N}) m=k'$$

$$m+n = k'+n = n+k' = (n+k)' \neq 0 \quad \nabla$$

(јер је следбеник неког природног броја)

$$\text{и.к. } m+k=n+k \Rightarrow m=n$$

$$\text{п.н.с. } m \neq n$$

$$(m+k_1)' = (m+k_2)'$$

$$n+k_1' = (n+k_2)'$$

$$6. m+k = n+k \Rightarrow m=n$$

$$k=0 \quad m+0 = n+0 \Rightarrow m=n$$

$$k>0 \quad \text{заменујемо } k \text{ његовим претходником док не сведемо на } k=0$$

$$k=k_1'$$

$$m+k_1' = n+k_1'$$

$$(m+k_1)' = (n+k_1)'$$

$$k_1=k_2'$$

$$(m+k_2')' = (n+k_2)''$$

За бројеве $x, y \in \mathbb{N}$ за које је $x=y+z$, за неко $z \in \mathbb{N}$, дефинишемо разлику броја x и y као

$$x-y \stackrel{\text{def}}{=} \quad (\text{дефинисана само за неке пр. бр.})$$

За $x, y \in \mathbb{N}$ операција множења дефинише се са:

$$m \cdot 0 \stackrel{\text{def}}{=} 0$$

$$m \cdot n' = m \cdot n + m$$

Особине множења: $\forall m, n, k \in \mathbb{N}$

$$1. m \cdot (n+k) = m \cdot n + m \cdot k$$

доказ индукцијом по k

$$\text{б.и. } k=0$$

$$m \cdot (n+0) = m \cdot n$$

$$m \cdot n + m \cdot 0 = m \cdot n + 0 = m \cdot n$$

$$\text{и.к. } k \rightarrow k'$$

$$(\text{и } x) \quad m \cdot (n+k) = m \cdot n + m \cdot k$$

$$\text{доказујемо } m \cdot (n+k') = m \cdot n + m \cdot k'$$

$$m \cdot (n+k') = m \cdot (n+k)' = m \cdot (n+k) + m$$

$$\stackrel{\text{и.к.}}{=} (m \cdot n + m \cdot k) + m = m \cdot n + (m \cdot k + m)$$

$$= m \cdot n + m \cdot k'$$

$$2. (m \cdot n) \cdot k = m \cdot (n \cdot k)$$

индукција по k

$$(m \cdot n) \cdot 0 = m \cdot (n \cdot 0)$$

$$0 = m \cdot 0$$

$$0 = 0$$

$$k \rightarrow k'$$

$$(m \cdot n) \cdot k' = (m \cdot n) \cdot k + m \cdot n$$

$$\stackrel{ux}{=} m \cdot (n \cdot k) + m \cdot n$$

$$= m \cdot (n \cdot k + n)$$

$$= m \cdot (n \cdot k')$$

$$4. 1 \cdot m = m$$

индукција по m

$$\text{бу: } 1 \cdot 0 = 0$$

$$0 = 0$$

$$\text{ик: } m \rightarrow m'$$

$$(\text{их}) 1 \cdot m = m$$

$$1 \cdot m' = m'$$

$$1 \cdot m' = (1 \cdot m)'$$

$$\stackrel{ux}{=} m'$$

$$6. m \cdot n = n \cdot m$$

индукција по n

$$\text{бу: } m \cdot 0 = 0 \cdot m$$

$$0 = 0 \quad (3^\circ)$$

$$\text{ик: } n \rightarrow n'$$

$$\text{их: } m \cdot n = n \cdot m$$

$$\text{доказати } m \cdot n' = n' \cdot m$$

$$m \cdot n' = m \cdot n + \stackrel{ux}{m} = n \cdot m + m$$

$$= n \cdot m + 0' \cdot m \stackrel{5}{=} (n + 0') \cdot m$$

$$= n' \cdot m$$

$$3. 0 \cdot m = 0$$

индукција по m

$$\text{бу: } m = 0 \quad 0 \cdot 0 = 0$$

$$0 = 0 \quad \checkmark$$

$$\text{ик: } m \rightarrow m' \quad (\text{их}) 0 \cdot m = 0$$

$$0 \cdot m' = 0 \quad \text{доказуемо}$$

$$0 \cdot m' = 0 \cdot m + 0 = 0 \cdot m \stackrel{ux}{=} 0$$

$$5. (m+n) \cdot k = m \cdot k + n \cdot k$$

индукција по k

$$\text{бу: } (m+n) \cdot 0 = m \cdot 0 + n \cdot 0$$

$$0 = 0 + 0$$

$$0 = 0 \quad \checkmark$$

$$\text{их: } (m+n) \cdot k = m \cdot k + n \cdot k$$

$$\text{ик: } k \rightarrow k'$$

$$(m+n) \cdot k' = (m+n) \cdot k + m + n \stackrel{ux}{=} m \cdot k + n \cdot k + m + n$$

$$= m \cdot k' + m + n \cdot k' + n = m \cdot k' + n \cdot k'$$

$$7. x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$$

лине матрица глас,

осла би за суапа.

ПРИМЕР 4.15: пооп. циф $2^{2^n} + 1$ је 7
за све $n \geq 2$

Делљивост

Еуклидово дељење

$a, b \in \mathbb{N}$ a дели b / b је дељив са a $(a|b)$
ако $(\exists c \in \mathbb{N}) b = a \cdot c$

- релација поретка (на скупу $\mathbb{N}$)

• антисиметричност

$$a|b \Rightarrow b = a \cdot k_1$$

$$b|a \Rightarrow a = b \cdot k_2$$

$$b = a \cdot k_1 = b \cdot k_2 \cdot k_1$$

$$k_1 \cdot k_2 = 1 \Rightarrow k_1 = k_2 = 1 \Rightarrow a = b$$

($\exists a \in \mathbb{N}$)

РЕФЛЕКСИВНОСТ

$$a|a \quad \checkmark$$
$$a = 1 \cdot a$$

ТРАНЗИТИВНОСТ

$$a|b \quad b|c$$

$$b = da \quad c = eb$$

$$c = e b = e d a$$
$$a|c$$

(O Еуклидовом дељењу) $a, b \in \mathbb{N}$ и $b \neq 0 \Rightarrow \exists q, r \in \mathbb{N}$
 ~~$a = b \cdot q + r$~~

$$a = b \cdot q + r, \quad 0 \leq r < b$$

доказ:

јединственост

п.п.с. приказ није јединствен

$$a = b \cdot q + r, \quad 0 \leq r < b$$

$$a = b \cdot q' + r', \quad 0 \leq r' < b$$

$$r \neq r'$$

$$r > r':$$

$$0 = b \cdot (q - q') + r - r'$$

$$b \cdot (q' - q) = r - r'$$

$$\Rightarrow b | r - r'$$

$$\left. \begin{array}{l} 0 \leq r - r' < b \\ b | r - r' \end{array} \right\} \Rightarrow \begin{array}{l} r - r' = 0 \\ r = r' \end{array}$$

↓

егзистенција

$$S = \{a - bx \mid x \in \mathbb{N}, a - bx \in \mathbb{N}\}$$

$$a = a - b \cdot \underbrace{0}_{\in \mathbb{N}} \in \mathbb{N} \Rightarrow a \in S \Rightarrow S \neq \emptyset$$

Нека је r најм. ел. скупа S
(постоји јер $S \neq \emptyset$)

$$\Rightarrow r = a - bq, \quad \text{за неко } q \in \mathbb{N}$$
$$r < b?$$

п.п.с. $r \geq b$

$$0 \leq r - b = a - b \cdot \underbrace{(q+1)}_{\in \mathbb{N}} \in \mathbb{N}$$

$$\Rightarrow r - b \in S$$

како је $r - b < r$ } јер је r најмањи елемент скупа S

$$\Rightarrow r < b \quad r = a - bq \Rightarrow a = bq + r$$

$0 \leq r < b$

Нека су $a, b \in \mathbb{Z}$ а глн b / b је глн са a
($a|b$) ~~ако~~ ако $(\exists c \in \mathbb{Z}) b = a \cdot c$

Нека су $a, b \in \mathbb{Z}$ и $b \neq 0$ $\exists q, r \in \mathbb{Z}$
 $a = q \cdot b + r$ $0 \leq r < |b|$

доказ. 1° $a \geq 0, b > 0$ своди се на претходну теорему

2° $a \geq 0, b < 0$

$$a \in \mathbb{N} - b \in \mathbb{N}$$

$$a = (-b)q + r, 0 \leq r < -b$$

$$a = b(-q) + r, 0 \leq r < b$$

$$b < 0 \Rightarrow |b| = -b$$

3° $a \leq 0, b > 0$

$$-a, b \in \mathbb{N}$$

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

$$a = \underbrace{b \cdot (-q)}_{-b} + \underbrace{(-r)}_{+b}$$

$$a = b(-q-1) + (b-r)$$

$$b > r \Rightarrow b-r \geq 0$$

$$b-r < b$$

$$a = b(-q-1) + r', 0 \leq r' < b$$

$$r' = b-r$$

4° $a \leq 0, b < 0$

$$-a, -b \in \mathbb{N}$$

$$-a = (-b)q + r, 0 \leq r < -b$$

$$a = \underbrace{b \cdot q}_{+b} + \underbrace{(-r)}_{-b}$$

$$a = b(q+1) + \underbrace{(-b-r)}_{r'}$$

$$r' \geq 0$$

$$r' < -b = |b|$$

$$0 \leq r' < |b|$$

$$a = b(q+1) + r'$$

48 страна

83 стр

НЗД и НЗС

$d \in \mathbb{N}$ је заједнички ~~делител~~ делилац $a, b \in \mathbb{N}$ ако $d|a$ и $d|b$
 d је највећи заједнички делилац бројева a и b ако
 $d'|d$ за сваки заједнички делилац d' тих бројева
 $d = \text{НЗД}(a, b)$

$s \in \mathbb{N}$ је заједнички садржалац $a, b \in \mathbb{N}$ ако $a|s$ и $b|s$
 s је најмањи заједнички садржалац бројева a и b ако
 $s|s'$ за сваки заједнички садржалац s' тих бројева
 $s = \text{НЗС}(a, b)$

Ако је $a = bq + r$ онда је $\text{НЗД}(a, b) = \text{НЗД}(b, r)$

доказ:

$$S_1 = \{d \mid d|a, d|b\}$$

$$S_2 = \{d \mid d|b, d|r\}$$

$$S_1 \subseteq S_2$$

$$d \in S_1 \Rightarrow d|a \text{ и } d|b$$

$$r = \underbrace{a}_{d|} - \underbrace{bq}_{d|} \Rightarrow d|r \Rightarrow d \in S_2$$

$$S_2 \subseteq S_1$$

$$d \in S_2 \Rightarrow d|b \text{ и } d|r$$

$$a = \underbrace{bq}_{d|} + \underbrace{r}_{d|} \Rightarrow d|a \Rightarrow d \in S_1$$

$$S_1 = S_2 \Rightarrow \max_{\text{НЗД}(a, b)} S_1 = \max_{\text{НЗД}(b, r)} S_2$$

Евклидов алгоритам

поступак за одређивање НЗД (a, b) $a, b \in \mathbb{Z} \setminus \{0\}$
Састоји се од узастопног примењивања теореме о
евклидском дељењу за целе бројеве

- број a при дељењу са b даје неки количник q_1
и остатак r_1

ако је $r_1 \neq 0$ настављамо поступак са b и $r_1 \Rightarrow q_2, r_2$

поступак се завршава када добијемо остатак $= 0$

Шема:

$$a = b q_1 + r_1 \quad 0 \leq r_1 < |b|$$

$$b = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2$$

$\vdots$

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} \quad 0 \leq r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1} q_n + r_n \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1} + \boxed{r_{n+1}} \quad 0 \leq r_{n+1} < r_n$$

$$r_n = r_{n+1} \cdot q_{n+2}$$

← последњи НЕ-НУЛА ОСТАТАК

$$r_1 > r_2 > \dots > r_{n-1} > r_n > r_{n+1} \geq 0$$

серија опадајућих низ природних бројева
ограничен нулом $\Rightarrow \exists n \in \mathbb{N}$ тд $r_n = 0$

Односно, алгоритам се сигурно завршава у
коначно многу корака

$$\begin{aligned} \text{НЗД}(a, b) &= \text{НЗД}(b, r_1) = \text{НЗД}(r_1, r_2) = \dots = \text{НЗД}(r_{n-2}, r_{n-1}) = \text{НЗД}(r_{n-1}, r_n) \\ &= \text{НЗД}(r_n \cdot q_{n+1}, r_n) = r_n \end{aligned}$$

$\parallel$
 $r_n \cdot q_{n+1}$

Безуова релација $\text{HЗД}(a, b) = d \Rightarrow (\exists x, y) ax + by = d$

доказ: $\text{HЗД}(a, b) = r_n$

$$= r_{n-2} - r_{n-1} \cdot q_n$$

$$= r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1}) q_n$$

$$= \underline{\hspace{1cm}} \cdot r_{n-3} + \underline{\hspace{1cm}} \cdot r_{n-2}$$

:

$$= \underline{\hspace{1cm}} r_0 + \underline{\hspace{1cm}} r_1$$

$$= \underline{\hspace{1cm}} r_0 + \underline{\hspace{1cm}} \cdot (b - r_0 \cdot q_1)$$

$$= \underline{\hspace{1cm}} b + \underline{\hspace{1cm}} r_0$$

$$= \underline{\hspace{1cm}} b + \underline{\hspace{1cm}} (a - b q_0)$$

$$= \underline{\hspace{1cm}}_x a + \underline{\hspace{1cm}}_y b$$

ПРИМЕР: $\text{HЗД}(75, 13) = 1 = 10 - 3 \cdot 3$

$$= 10 - 3(13 - 10) = 4 \cdot 10 + (-3) \cdot 13$$

$$= 4(75 - 13 \cdot 5) + (-3) \cdot 13$$

$$= \underline{\hspace{1cm}}_x 4 \cdot 75 + \underline{\hspace{1cm}}_y (-23) \cdot 13$$

$$a, b \in \mathbb{Z} \quad M_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Матрицу M_{n+1} добијемо од M_n једном од следећих трансформација:

T1: МНОЖЕЊЕ ВРСТЕ ЦЕЛИМ БРОЈЕМ И ДОДАВАЊЕ ДРУГОЈ ВРСТИ

T2: МНОЖЕЊЕ ВРСТЕ СА -1

T3: ЗАМЕНА МЕСТА ВРСТАМА

Нека је $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$. Тада је $\begin{matrix} x = ap + bq \\ y = as + bt \end{matrix}$

доказ: индукцијом по n

$$\boxed{UK} \quad M_n \rightarrow M_{n+1}$$

бн: $n=0$

$$M_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

$$M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$$

$$UX: \text{ВАЖИ} \quad \begin{matrix} x = ap + bq \\ y = as + bt \end{matrix}$$

$$M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix}$$

$$\text{доказујемо} \quad \begin{matrix} x' = ap' + b \cdot q' \\ y' = as' + b \cdot t' \end{matrix}$$

$$\begin{matrix} a = a \cdot 1 + b \cdot 0 = a \\ b = a \cdot 0 + b \cdot 1 = b \end{matrix} \quad \textcircled{T}$$

$$1^\circ M_n \xrightarrow{T_1} M_{n+1}$$

$$M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix}$$

$$= \begin{bmatrix} x & p & q \\ y+\alpha x & s+\alpha p & t+\alpha q \end{bmatrix}$$

$$x' = x \stackrel{ux}{=} a \cdot p + b \cdot q = a \cdot p' + b \cdot q'$$

$$y' = y + \alpha x \stackrel{ux}{=} a s + b t + \alpha(a p + b q)$$

$$= a(s + \alpha p) + b(t + \alpha q)$$

$$= a \cdot s' + b \cdot t'$$

$$2^\circ M_n \xrightarrow{T_2} M_{n+1}$$

$$M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix}$$

$$= \begin{bmatrix} -x & -p & -q \\ y & s & t \end{bmatrix}$$

$$x' = -x \stackrel{ux}{=} -(a p + b q) = a(-p) + b(-q)$$

$$= a p' + b q'$$

$$y' = y \stackrel{ux}{=} a s + b t = a s' + b t'$$

$$3^\circ M_n \xrightarrow{T_3} M_{n+1}$$

$$M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix}$$

$$= \begin{bmatrix} y & s & t \\ x & p & q \end{bmatrix}$$

$$x' = y \stackrel{ux}{=} a s + b t = a p' + b q'$$

$$y' = x \stackrel{ux}{=} a p + b q = a s' + b t'$$

Нека је $M_n = \begin{bmatrix} x & p & q \\ y & s & t \end{bmatrix}$. Тада је $\text{HЗД}(a, b) = \text{HЗД}(x, y)$

[дн] $n=0$

$$M_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

$$\text{HЗД}(a, b) \stackrel{\oplus}{=} \text{HЗД}(a, b)$$

[нх] важи $\text{HЗД}(a, b) = \text{HЗД}(x, y)$

$$M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix}$$

доказујемо да је
 $\text{HЗД}(a, b) = \text{HЗД}(x', y')$

$$1^\circ M_n \xrightarrow{T_1} M_{n+1}$$

$$M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix} = \begin{bmatrix} x & p & q \\ y+\alpha x & s+\alpha p & t+\alpha q \end{bmatrix}$$

$$\text{HЗД}(x', y') = \text{HЗД}(x, y + \alpha x) \stackrel{ux}{=} \text{HЗД}(x, y) \stackrel{ux}{=} \text{HЗД}(a, b)$$

$$2^\circ M_n \xrightarrow{T_2} M_{n+1}$$

$$M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix} = \begin{bmatrix} -x & -p & -q \\ y & s & t \end{bmatrix}$$

$$\text{HЗД}(x', y') = \text{HЗД}(-x, y) = \text{HЗД}(x, y) \stackrel{ux}{=} \text{HЗД}(a, b)$$

$$3^\circ M_n \xrightarrow{T_3} M_{n+1}$$

$$M_{n+1} = \begin{bmatrix} x' & p' & q' \\ y' & s' & t' \end{bmatrix} = \begin{bmatrix} y & s & t \\ x & p & q \end{bmatrix}$$

$$\text{HЗД}(x', y') = \text{HЗД}(y, x) = \text{HЗД}(x, y) \stackrel{ux}{=} \text{HЗД}(a, b)$$

Ако у неком кораку стигнемо до матрице облика

$$M_n = \begin{bmatrix} d & p & q \\ 0 & s & t \end{bmatrix}$$

Тада је $\text{HЗД}(a, b) = \text{HЗД}(d, 0) = d$ и још ће важити $d = ap + bq$

(добивамо Безову релацију)

$$\text{HЗД}(75, 13)$$

$$\begin{bmatrix} 75 & 1 & 0 \\ 13 & 0 & 1 \end{bmatrix} \xrightarrow{(-5)} \sim \begin{bmatrix} 10 & 1 & -5 \\ 13 & 0 & 1 \end{bmatrix} \xrightarrow{(-1)} \sim \begin{bmatrix} 10 & 1 & -5 \\ 3 & -1 & 6 \end{bmatrix} \xrightarrow{-3} \sim \begin{bmatrix} 1 & 4 & -23 \\ 3 & -1 & 6 \end{bmatrix} \xrightarrow{-3}$$

$$\text{HЗД}(75, 13) = 1$$

$$1 = 75 \cdot 4 + 13 \cdot (-23)$$

$$\sim \begin{bmatrix} 1 & 4 & -23 \\ 0 & -13 & 75 \end{bmatrix}$$

Бројеви су узajамно прости ако је $\text{НЗД}(a, b) = 1$
 $a, b \in \mathbb{Z}$

• $a | b$ и $\text{НЗД}(a, b) = 1 \Rightarrow a | c$

доказ: Бекетова релација

$$1 = a \cdot x + b \cdot y \quad | \cdot c$$

$$c = \underbrace{acx}_{a|} + \underbrace{bcy}_{a|} \Rightarrow a | c$$

• $d = \text{НЗД}(a, b) \Rightarrow \text{НЗД}(a, b) = \frac{|ab|}{d}$

$$a = da', \quad b = db' \Rightarrow \text{НЗД}(a', b') = 1$$

доказ: претпоставимо супротно $\text{НЗД}(a', b') = d' > 1$

$$\left. \begin{array}{l} a' = d' \cdot a'' \quad a = d \cdot d' \cdot a'' \\ b' = d' \cdot b'' \quad b = d \cdot d' \cdot b'' \end{array} \right\} \Rightarrow \left. \begin{array}{l} d \cdot d' | a, b \\ d' > 1 \Rightarrow d \cdot d' > d \end{array} \right\} \downarrow \text{jer je } d = \text{НЗД}(a, b)$$

Диофантове једначине

Диофантова једначина је једначина са целим бројним коефицијентима код које тражимо решења у $\mathbb{Z}$

Пр. Једначина $ax = b$, $a, b \in \mathbb{Z}$ и $a \neq 0$ је Диофантова јна.

Има решења у $\mathbb{Z}$ ако $a | b$

$$ax + by = c \quad a, b, c \in \mathbb{Z} \quad a, b \neq 0$$

Има целим бројна решења ако $\text{НЗД}(a, b) | c$

$$\Rightarrow x_0, y_0 \in \mathbb{Z} \text{ решења јне} \quad (\Leftrightarrow d = \text{НЗД}(a, b) | c)$$

$$ax_0 + by_0 = c$$

$$d = \text{НЗД}(a, b)$$

$$\left. \begin{array}{l} d | ax_0 \\ d | by_0 \end{array} \right\} \begin{array}{l} d | ax_0 + by_0 \\ d | c \end{array}$$

Обрнути Буклигов алгоритам

$$(\exists p, q \in \mathbb{Z}) \quad ap + bq = d \quad | \cdot c_1$$

$$d | c \Rightarrow c = c_1 \cdot d$$

$$a(\underbrace{p \cdot c_1}_{x_0}) + b(\underbrace{q \cdot c_1}_{y_0}) = c$$

(px_1, qy_1) - једно решење јне

(ПАРТИКУЛАРНО РЕШЕЊЕ)

Како изнега опште решење једначине?

(x_0, y_0) — партикуларно решење $(x, y) = ?$

$$\begin{aligned} ax_0 + by_0 &= c \\ ax + by &= c \end{aligned} \stackrel{?}{=} \Rightarrow a(x - x_0) + b(y - y_0) = 0$$

$$d = \text{НЗД}(a, b)$$

$$\begin{aligned} a &= a_1 d \\ b &= b_1 d \\ c &= c_1 d \end{aligned}$$

$$\begin{aligned} a(x - x_0) &= -b(y - y_0) \quad / : d \\ a_1(x - x_0) &= -b_1(y - y_0) \end{aligned}$$

$$\left. \begin{aligned} \text{НЗД}(a_1, b_1) &= 1 \\ b_1(a_1(x - x_0)) & \end{aligned} \right\} \Rightarrow b_1 \mid x - x_0$$

опште решење:

$$(x_0 + b_1 t, y_0 - a_1 t), \quad t \in \mathbb{Z}$$

има решења колико и
целих бројева

$$\left(p \cdot \frac{c}{\text{НЗД}(a, b)} + \frac{b}{\text{НЗД}(a, b)} \cdot t, \right.$$

$$\left. q \cdot \frac{c}{\text{НЗД}(a, b)} - \frac{a}{\text{НЗД}(a, b)} \cdot t \right) t \in \mathbb{Z}$$

$$x - x_0 = b_1 \cdot t, \quad t \in \mathbb{Z} \quad / + x_0$$

$$x = x_0 + b_1 t, \quad t \in \mathbb{Z}$$

$$\Rightarrow a(x_0 + b_1 t - x_0) = -b_1(y - y_0)$$

$$a_1 b_1 t = -b_1(y - y_0)$$

$$a_1 t = -y + y_0$$

$$y = y_0 - a_1 t, \quad t \in \mathbb{Z}$$

$$ap + bq = d = \text{НЗД}(a, b)$$

Закључак:

Једначина $ax + by = c$, $a, b \in \mathbb{Z}$, $a, b \neq 0$ има
целобројна решења ако $\text{НЗД}(a, b) \mid c$

У том случају је опште решење ове једначине

$$x = p \frac{c}{\text{НЗД}(a, b)} + \frac{b}{\text{НЗД}(a, b)} \cdot t$$

$$y = q \frac{c}{\text{НЗД}(a, b)} - \frac{a}{\text{НЗД}(a, b)} \cdot t$$

$$t \in \mathbb{Z}$$

где су p и q добијени помоћу обрнутог Еуклидовог
алгоритма такви да важи $ap + bq = \text{НЗД}(a, b)$

Прости бројеви

Цео број $p > 1$ је прост ако су му једини делници 1 и p
Цео број $n > 1$ који није прост је сложен.

• Постоји бесконачно много простих бројева

нпс $\{p_1, p_2, \dots, p_k\}$ — скуп свих простих бројева

$\Rightarrow p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$ је сложен

$\Rightarrow \exists p_i \mid p_1 p_2 \cdot \dots \cdot p_k + 1$ $\left\{ \begin{array}{l} \text{остатак при дељењу са } p_i \\ i \in \{1, \dots, k\} \end{array} \right\} \downarrow$ је 1 $\neq 0$

$\Rightarrow$ простих бројева има бесконачно много

• Ако је p прост број и $p \nmid a$, онда је $p \mid a$ или $p \nmid a$

* $\text{НЗД}(p, x) \in \{1, p\}$ $\left\{ \begin{array}{l} \text{ако } x \text{ није дељиво са } p \\ \text{ако је } x \text{ дељиво са } p \end{array} \right.$

доказ: претпоставимо да $p \nmid a$ и покажимо да тада $p \nmid a$

$\text{НЗД}(p, a) \in \{1, p\}$ $\left\{ \begin{array}{l} p \nmid a \\ p \mid a \end{array} \right. \Rightarrow \text{НЗД}(a, b) = 1$

$p \nmid a$ $\left\{ \begin{array}{l} \text{доказано раније} \\ \text{НЗД}(p, a) = 1 \end{array} \right. \Rightarrow p \nmid a$

• Сваки природан број већи од 1 је прост или се може представити као производ простих бројева

доказ: Математичком индукцијом по природном броју $n > 1$

тврђење

$\Phi(n)$: n је прост или је производ

база : $n=2$ $\Phi(2)$ је тачно јер је 2 прост број

и х : $\Phi(k)$ важи за све $k < n$

и к : $\Phi(n)$?

n може бити : $\cdot$ прост $\Rightarrow$ важи $\Phi(n)$

$\cdot$ сложен $\Rightarrow n = k_1 k_2 \quad k_1, k_2 < n$

На k_1 и k_2 можемо да применимо ИНДУКТИВНУ ХИПОТЕЗУ

$\Rightarrow k_1, k_2$ су прости или производи простих
па је $n = k_1 k_2$ производ простих $\Rightarrow$ важи $\Phi(n)$

(Основна теорема аритметике)

Сваки природан број већи од 1 се може представити у облику производа простих бројева на јединствен начин (до на редослед простих фактора)

доказ: доказати смо да $\forall a \in \mathbb{N}, a > 1$

може бити представљен као производ простих, остаје доказати јединственост приказа

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \dots \cdot q_\ell^{\beta_\ell}$$

$p_i, i \in \{1, \dots, k\}$
 $q_j, j \in \{1, \dots, \ell\}$ > прости бројеви

$\forall i \in \{1, \dots, k\}$ важи $p_i \mid q_1^{\beta_1} q_2^{\beta_2} \dots q_\ell^{\beta_\ell}$

$\Rightarrow \exists j \in \{1, \dots, \ell\}$ так да $p_i \mid q_j \Rightarrow p_i = q_j$

$$\{p_1, \dots, p_k\} \subseteq \{q_1, \dots, q_\ell\}$$

Слично, доказујемо да је $\{q_1, \dots, q_\ell\} \subseteq \{p_1, \dots, p_k\}$

$$\Rightarrow \{p_1, \dots, p_k\} = \{q_1, \dots, q_\ell\} \Rightarrow k = \ell$$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} \quad / : p_1^{\alpha_1}$$

$p_1 < p_2 < \dots < p_k$
 $q_1 < q_2 < \dots < q_\ell$
тада је $p_1 = q_1, \dots$

ппс $\alpha_1 \neq \beta_1$

без губитка општости нека је $\alpha_1 < \beta_1$

$$\underbrace{p_2^{\alpha_2} \dots p_k^{\alpha_k}}_{p \nmid} = \underbrace{p_1^{\beta_1 - \alpha_1} p_2^{\beta_2} \dots p_k^{\beta_k}}_{p \mid}$$



$$\Rightarrow \alpha_1 = \beta_1$$

$$p_2^{\alpha_2} \dots p_k^{\alpha_k} = p_2^{\beta_2} \dots p_k^{\beta_k}$$

Слично показујемо

$$\alpha_2 = \beta_2, \dots$$

КОНГРУЕНЦИЈЕ

$$m \in \mathbb{N}, m > 1$$

$a, b \in \mathbb{Z}$ су конгруентни по модулу m ако $m \mid (a-b)$

$$a \equiv b \pmod{m}$$
$$a \equiv_m b$$

Релација $\equiv_m$ је релација еквиваленције

доказ:

РЕФЛЕКСИВНОСТ $x \equiv_m x \Rightarrow m \mid x-x \Rightarrow m \mid 0 \quad \checkmark$

СИМЕТРИЧНОСТ $x \equiv_m y \stackrel{?}{\Rightarrow} y \equiv_m x$

$$m \mid x-y \quad m \mid y-x$$

$$m \mid x-y \Rightarrow x-y = km$$

$$y-x = -km$$

$$m \mid y-x \Rightarrow y \equiv_m x$$

ТРАЗИТИВНОСТ: $\left. \begin{array}{l} x \equiv_m y \\ y \equiv_m z \end{array} \right\} \stackrel{?}{\Rightarrow} x \equiv_m z$

$$m \mid x-y \Rightarrow x-y = mk_1$$

$$m \mid y-z \Rightarrow y-z = mk_2 \quad k_1, k_2 \in \mathbb{Z}$$

$$x-z = x-y + y-z = mk_1 + mk_2 = m(k_1 + k_2) \Rightarrow x \equiv_m z$$

$$C_a = \{x \in \mathbb{Z} \mid a \equiv_m x\}$$

$$= \{x \in \mathbb{Z} \mid a-x = mt, t \in \mathbb{Z}\}$$

$$= \{a+mt \mid t \in \mathbb{Z}\} \rightarrow \text{сви цели бројеви који имају исти остатак као и } a \text{ при дељењу са } m$$

КЛАСЕ $[0], [1], \dots, [m-1]$

$\downarrow$
укупно има m КЛАСА $[m+1]$

$\parallel$
 $[-1]$

$$* \quad m-1 \equiv_m -1$$

$$m \mid m-1 \Rightarrow m \mid (m-1)+m \Rightarrow m \mid -1$$

Ako je $a \equiv a_1 \pmod{m}$ i $b \equiv b_1 \pmod{m}$ onda je
 $1^\circ a + b \equiv a_1 + b_1 \pmod{m}$

$$a + b - (a_1 + b_1) = \underbrace{(a - a_1)}_{m \mid} + \underbrace{(b - b_1)}_{m \mid} \Rightarrow m \mid (a + b) - (a_1 + b_1)$$

$$2^\circ a \cdot b \equiv a_1 b_1 \pmod{m}$$

$$ab - a_1 b_1 = ab - b_1 a + b_1 a - a_1 b_1 = a \underbrace{(b - b_1)}_{m \mid} + b_1 \underbrace{(a - a_1)}_{m \mid}$$

$$\Rightarrow m \mid ab - a_1 b_1 \quad ab \equiv_m a_1 b_1$$

$$3^\circ a^n \equiv a_1^n \pmod{m} \quad \forall n \geq 1$$

gore: indukcijom po n

БН $n=1$: $a \equiv a_1 \pmod{m}$

$n=2$: $a \cdot a \equiv a_1 a_1 \pmod{m}$ (бази на основу 2°)

ИХ $a^{n-1} \equiv a_1^{n-1} \pmod{m}$

ИК доказујемо да $a^n \equiv a_1^n \pmod{m}$

$$\left. \begin{array}{l} a \equiv a_1 \pmod{m} \\ \text{(ИХ)} \quad a^{n-1} \equiv a_1^{n-1} \pmod{m} \end{array} \right\} \stackrel{2^\circ}{\Rightarrow} a \cdot (a^{n-1}) \equiv a_1 \cdot (a_1^{n-1}) \pmod{m}$$

$$a^n \equiv a_1^n \pmod{m}$$

Нека $d \mid a, b, m$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$ $m' = \frac{m}{d}$

$a \equiv b \pmod{m}$ ако $a' \equiv_{m'} b'$

gore: $a = a_1 d$ $b = b_1 d$ $m = m_1 d$

$a \equiv b \pmod{m} \Leftrightarrow a_1 \equiv b_1 \pmod{m_1}$

$\Rightarrow a \equiv_m b$

$m \mid a - b$

$a - b = m t$ $\forall d \mid t \in \mathbb{Z}$

$a_1 - b_1 = m_1 t$

$m_1 \mid a_1 - b_1$

$a_1 \equiv_{m_1} b_1$

$\Leftarrow a_1 \equiv_{m_1} b_1$

$m_1 \mid a_1 - b_1$

$a_1 - b_1 = m_1 t$ $\forall d \mid t \in \mathbb{Z}$

$a_1 d - b_1 d = (m_1 d) t$

$a - b = m \cdot t$

$m \mid a - b \quad a \equiv_m b$

Једначине са контреницијом

Када има и шта су решења јне ~~ax ≡ b~~ $ax \equiv b \quad a, b \in \mathbb{Z}$

Када има?

$$ax \equiv_m b$$

$$m \mid ax - b$$

$$ax - b = m(-t) \quad -t \in \mathbb{Z}$$

$$ax + mt = b$$

јна има решења

када $\text{HЗД}(a, m) \mid b$

Шта су решења?

$$d = \text{HЗД}(a, m)$$

$$a = d \cdot a_1 \quad m = d \cdot m_1$$

$$d \mid b \Rightarrow b = d \cdot b_1$$

уместо јне $ax \equiv_m b$ можемо посматрати јну $a_1 x \equiv_{m_1} b_1$

(„скратити“ смо $ax \equiv_m b$ са d)

$$\text{HЗД}(a_1, m_1) = 1$$

$$\Rightarrow (\exists p, q \in \mathbb{Z}) \quad a_1 p + m_1 q = 1 \quad / \cdot b_1$$

$$a_1 (p b_1) + m_1 q b_1 = b_1$$

$$a_1 (p b_1) - b_1 = m_1 q b_1$$

$$m_1 \mid a_1 (p \cdot b_1) - b_1$$

$$a_1 (\underbrace{p \cdot b_1}_{x_0}) \equiv_{m_1} b_1$$

$$x \equiv_{m_1} p \cdot b_1$$

$$\boxed{a_1 x \equiv_{m_1} b_1} \quad \text{ако } x \equiv_{m_1} p \cdot b_1$$

$$\Rightarrow a_1 x \equiv_{m_1} b_1 \quad / \cdot p$$

$$a_1 p x \equiv_{m_1} b_1 p \quad \Rightarrow x \equiv_{m_1} b_1 p$$

$$a_1 p \equiv_{m_1} 1$$

из безгвола

решења су облика
$$\begin{aligned} x &\equiv_{m_1} p b_1 \\ x &= p b_1 + m_1 t \\ t &\in \mathbb{Z} \end{aligned}$$

Једначина $a_1 x \equiv_{m_1} b_1$ у интервалу $[0, m_1)$ има тачно једно реш.

Нека је то решење x_0 (и се садити у m пута)

Једначина $ax \equiv_m b$ има d решења у интервалу $[0, m]$ и то су реш.:

$$[0, m_1), [m_1, 2m_1), [2m_1, 3m_1), \dots, [(d-1)m_1, d m_1)$$

$$x_0 + m_1$$

$$x_0 + m_1$$

$$x_0 + (d-1)m_1$$

(Вилсонова теорема) Ако је p прост број тада је
 $(p-1)! \equiv -1 \pmod{p}$

доказ: $p=2 \quad (2-1)! = 1! = 1 \equiv -1 \pmod{2} \quad 2 \nmid 1 - (-1)$

$p=3 \quad (3-1)! = 2! = 2 \equiv -1 \pmod{3} \quad 3 \nmid 2 - (-1)$

Нека је $p \geq 5 \quad a \in \{2, \dots, p-2\}$

Посматрамо једначину $ax \equiv 1 \pmod{p} \quad (*)$

$\text{HЗР}(a, p) = 1 \Rightarrow (*)$ има тачно једно решење у интервалу $[0, p)$

Нека је то решење $x_a \in \{0, \dots, p-1\}$
 $\leftarrow p-3$ чланова

Покажимо да $x_a \in \{2, \dots, p-2\}$ (да не може да буде $0, 1, p-1$)

$x_a = 1 \Rightarrow a \equiv 1 \pmod{p} \quad \downarrow$

$x_a = 0 \Rightarrow 0 \equiv 1 \pmod{p} \quad \downarrow$

$x_a = p-1 \Rightarrow a(p-1) \equiv 1 \pmod{p} =$

$\Rightarrow ap - a \equiv a \pmod{p} \equiv 1 \pmod{p} \quad \downarrow$

Види $x_a \neq a$

ако је $x_a = a$

$a^2 \equiv 1 \pmod{p}$

$a^2 - 1 \equiv 0 \pmod{p}$

прост $\leftarrow p \mid (a-1)(a+1)$

• ако $p \mid a-1$

$\rightarrow$ пошто је $a \in \{2, \dots, p-2\}$

$1 \leq a-1 \leq p-3 \Rightarrow p \nmid a-1$

• ако $p \mid a+1$

$3 \leq a+1 \leq p-1 \Rightarrow p \nmid a+1$

$\Rightarrow p \nmid a^2 - 1$

$\Rightarrow \boxed{x_a \neq a}$

скупи $\{2, \dots, p-2\}$ смо поделили на парове (a, x_a) такве да је
 $ax_a \equiv 1 \pmod{p}$

$(2, x_2), (3, x_3), \dots, \left(\frac{p-3}{2}, x_{\frac{p-3}{2}}\right)$

зато што смо их груписали у парове

$(p-1)! = \underbrace{1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-2)}_{2 \cdot x_2 \cdot 3 \cdot x_3 \cdot \dots \cdot \frac{p-3}{2} \cdot x_{\frac{p-3}{2}}} \cdot (p-1) \pmod{p}$

$(p-1)! \equiv (1 \cdot (1)^{\frac{p-3}{2}} \cdot p-1) \pmod{p}$

$(p-1)! \equiv p-1 \pmod{p} \equiv -1 \pmod{p}$

Системи конгруенција

(Кинеска теорема о остацима)

Нека су $m_1, m_2, \dots, m_n \geq 2$ узajамно прости у паровима и нека $a_1, a_2, \dots, a_n \in \mathbb{Z}$

$$(*) \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

$$\text{НЗД}(m_i, m_j) = 1 \text{ за све } 1 \leq i, j \leq n$$

Систем конгруенција има решење.

Решење је јединствено у интервалу $[0, m_1 \cdot m_2 \cdot \dots \cdot m_n)$
а опште решење је облика $x = x_0 + m_1 \cdot m_2 \cdot \dots \cdot m_n \cdot t \quad t \in \mathbb{Z}$

доказ: $M = m_1 \cdot m_2 \cdot \dots \cdot m_n$

$$M_i = \frac{M}{m_i}$$

$$M_1 = m_2 \cdot m_3 \cdot \dots \cdot m_n$$

$$M_2 = m_1 \cdot m_3 \cdot \dots \cdot m_n$$

$\vdots$

$$M_n = m_1 \cdot m_2 \cdot \dots \cdot m_{n-1}$$

$$\text{НЗД}(M_i, m_i) = 1$$

$$x_0 \in [0, m_1 \cdot m_2 \cdot \dots \cdot m_n)$$

На основу обрнутог

Еуклидовог алгоритма

постоје $p_i, q_i \in \mathbb{Z}$ т.д.д.

$$p_i M_i + q_i m_i = 1$$

$$p_i M_i \equiv 1 \pmod{m_i}$$

$$p_i M_i \equiv 0 \pmod{m_j} \quad j \neq i$$

$$x = p_1 M_1 a_1 + p_2 M_2 a_2 + \dots + p_i M_i a_i + \dots + p_n M_n a_n$$

$$x \equiv a_i \pmod{m_i}$$

$$\forall i \in \{1, \dots, n\} \text{ важи } x \equiv a_i \pmod{m_i}$$

једначина $(*)$ има решење

• решење у интервалу $[0, m_1 \cdot m_2 \cdot \dots \cdot m_n)$ је остатак при дељењу решења x са M

• Нека је то решење x_0

$$x \equiv x_0 \pmod{m}$$

$$m \mid x - x_0$$

$$m_i \mid x - x_0 \quad \forall i \in \{1, \dots, n\}$$

$$\left. \begin{array}{l} x \equiv x_0 \pmod{m_i} \\ x \equiv a_i \pmod{m_i} \end{array} \right\} \Rightarrow x_0 \equiv a_i \pmod{m_i}$$

x_0 jeste решење система (*)

$\bar{x}$ - било koje решење система

$$\left. \begin{array}{l} \bar{x} \equiv a_i \pmod{m_i} \\ x_0 \equiv a_i \pmod{m_i} \end{array} \right\} \Rightarrow \bar{x} \equiv x_0 \pmod{m_i}, \quad i \in \{1, \dots, n\}$$

$$\left. \begin{array}{l} m_1 \mid \bar{x} - x_0 \\ m_2 \mid \bar{x} - x_0 \\ \vdots \\ m_n \mid \bar{x} - x_0 \\ \text{HЗД}(m_i, m_j) = 1 \end{array} \right\} \Rightarrow m \mid \bar{x} - x_0$$

$$\bar{x} = x_0 + mt, \quad t \in \mathbb{Z}$$

$$= x_0 + m_1 m_2 \dots m_n t$$

Кинеска теорема о остацима (опште твђење)

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_n \pmod{m_n}$$

$i \neq j$

Систем конјункција има решење ако $\text{HЗД}(m_i, m_j) \mid (a_i - a_j)$

Ако је $\bar{x}$ неко решење тог система, онда је опште решење облика $x = \bar{x} + \text{HЗС}(m_1, \dots, m_n) \cdot t \quad t \in \mathbb{Z}$

Доказ: индукцијом по броју једначина n

БИ: $n = 1$

$$x \equiv a_1 \pmod{m_1}$$

$$x = a_1 + m_1 t, \quad t \in \mathbb{Z}$$

ИХ твђење важи за све системе за n једначина

и К показујемо да тврђење важи и за системе са $n+1$ једначина

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

$$x \equiv a_{n+1} \pmod{m_{n+1}}$$

На основу (иХ) решење првих n једначина је

$$x = \bar{x} + \text{HЗС}(m_1, \dots, m_n) \cdot t, \quad t \in \mathbb{Z}$$

Да ли је x решење и последње решење?

$$\bar{x} + \text{HЗС}(m_1, \dots, m_n) \cdot t \equiv a_{n+1} \pmod{m_{n+1}}$$

$$\text{HЗС}(m_1, \dots, m_n) \cdot t \equiv a_{n+1} - \bar{x} \pmod{m_{n+1}}$$

$$\text{HЗД}(\text{HЗС}(m_1, \dots, m_n), m_{n+1}) \mid a_{n+1} - \bar{x}$$

$$\rightarrow \text{HЗД}(\text{HЗС}(m_1, \dots, m_n), m_{n+1})$$

$$= \text{HЗС}(\text{HЗД}(m_1, m_{n+1}), \text{HЗД}(m_2, m_{n+1}), \dots, \text{HЗД}(m_n, m_{n+1}))$$

$$\text{Да ли } \text{HЗД}(m_i, m_{n+1}) \mid a_{n+1} - \bar{x}$$

$$a_{n+1} - \bar{x} = \underbrace{a_{n+1} - a_i}_{\text{HЗД}(m_i, m_{n+1})} + \underbrace{a_i - \bar{x}}_{m_i}$$

$$\left. \begin{array}{l} \text{HЗД}(m_{n+1}, m_i) \mid m_i \\ m_i \mid a_i - \bar{x} \end{array} \right\} \Rightarrow \text{HЗД}(m_{n+1}, m_i) \mid a_i - \bar{x}$$

$$\Rightarrow \text{HЗД}(m_{n+1}, m_i) \mid a_{n+1} - \bar{x} \quad \text{за све } i$$

$$\Rightarrow \text{HЗС}(\text{HЗД}(m_{n+1}, m_1), \dots, \text{HЗД}(m_{n+1}, m_n)) \mid a_{n+1} - \bar{x}$$

$\bar{x}$ јесте решење и последње једначине

$$\left. \begin{array}{l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{array} \right\} \Rightarrow \left. \begin{array}{l} \bar{x} \equiv a_1 \pmod{m_1} \\ \bar{x} \equiv a_2 \pmod{m_2} \\ \vdots \\ \bar{x} \equiv a_n \pmod{m_n} \end{array} \right\} \Rightarrow \left. \begin{array}{l} x \equiv \bar{x} \pmod{m_1} \\ x \equiv \bar{x} \pmod{m_2} \\ \vdots \\ x \equiv \bar{x} \pmod{m_n} \end{array} \right\} \Rightarrow \begin{array}{l} m_1 | x - \bar{x} \\ m_2 | x - \bar{x} \\ \vdots \\ m_n | x - \bar{x} \end{array}$$

$$\Rightarrow \text{HЗС}(m_1, \dots, m_n) | x - \bar{x}$$

$$x = \bar{x} + \text{HЗС}(m_1, \dots, m_n) \cdot t \quad | \quad t \in \mathbb{Z}$$

-120206.jpg

Ојлерова функција

Нека је $n \in \mathbb{N}$, $n > 1$. Са $\varphi(n)$ означавамо број природних бројева m тако да $1 \leq m < n$ и $\text{HЗД}(m, n) = 1$

Функција φ се назива Ојлерова функција.

• за прост број p важи $\varphi(p) = p - 1$

ТРИВИЈАЛНО

• $k \geq 1$ $\varphi(p^k) = p^k - p^{k-1}$ (p прост)

колико има бројева мањих од p^k и деливих са p

$$\Rightarrow \{kp \mid 1 < kp < p^k\} = \{kp \mid 1 \leq k \leq p^{k-1}\} \quad \begin{array}{l} \text{ИМА ИХ} \\ p^{k-1} \end{array}$$

$$\Phi(n) = \{k \mid 1 \leq k \leq n-1, \text{HЗД}(k, n) = 1\} \leftarrow \text{Ојлеров скуп}$$

$$\varphi(n) = |\Phi(n)|$$

• $m, n > 1$ природни бројеви такви да је $\text{HЗД}(m, n) = 1$

Тогда је $\varphi(mn) = \varphi(m) \varphi(n)$ тј Ојлерова функција је мултипликативна

Покажимо да постоји функција

$f: \Phi(mn) \rightarrow \Phi(m) \times \Phi(n)$ бијекција

$$f(k) = (g_m(k), g_n(k))$$

$$g_n(x) \in \begin{array}{l} \text{ОСТАТАК ПРИ ДЕЉЕЊУ} \\ x \text{ са } n \quad (x \% n) \end{array}$$

$$g_n(x) \in \{0, 1, \dots, n-1\}$$

прво проверавамо да ли је f добро дефинисана
 тј да ли $\varphi_m(a) \in \Phi(m)$ и $\varphi_n(a) \in \Phi(n)$

$$a \in \Phi(mn) \Rightarrow \text{HЗД}(a, mn) = 1 \Rightarrow \begin{matrix} \text{HЗД}(a, m) = 1 \\ \text{HЗД}(a, n) = 1 \end{matrix}$$

$$a = mq + r \quad \text{"} \varphi_m(a) \text{"}$$

$$1 = \text{HЗД}(a, m) = \text{HЗД}(m, \varphi_m(a)) \Rightarrow \varphi_m(a) \in \Phi(m)$$

слично $\varphi_n(a) \in \Phi(n)$

f бијекција?

"1-1"

$$a, b \in \Phi(mn)$$

$$f(a) = f(b) \Rightarrow a = b$$

$$(\varphi_m(a), \varphi_n(a)) = (\varphi_m(b), \varphi_n(b))$$

$$\varphi_m(a) = \varphi_m(b) \Rightarrow a \equiv b \pmod{m} \Rightarrow m | a - b$$

$$\left. \begin{array}{l} \varphi_n(a) = \varphi_n(b) \Rightarrow a \equiv b \pmod{n} \Rightarrow n | a - b \\ \text{HЗД}(m, n) = 1 \end{array} \right\} \Rightarrow mn | a - b$$

$$a, b \in \Phi(mn) \quad 1 \leq a, b < mn$$

$$\left. \begin{array}{l} -mn < a - b < mn \\ mn | a - b \end{array} \right\} \Rightarrow a - b = 0 \quad a = b \Rightarrow f \text{ је "1-1"}$$

"на"

$$(r, s) \in \Phi(m) \times \Phi(n)$$

Да ли постоји $a \in \Phi(mn)$ тј $f(a) = (r, s)$, $(r, s) = (\varphi_m(a), \varphi_n(a))$

Да ли постоји $a \in \Phi(mn)$ тј $a \equiv r \pmod{m}$ и $a \equiv s \pmod{n}$?

$$(*) \begin{cases} x \equiv r \pmod{m} \\ x \equiv s \pmod{n} \end{cases} \quad \begin{array}{l} \text{Нека је } a \text{ то решење} \\ a \in [0, mn) \end{array}$$

$$\text{тако да постоји} \quad \begin{array}{l} a \equiv r \pmod{m} \\ a \equiv s \pmod{n} \end{array}$$

$$\text{ако } (*) \text{ има решење}$$

$$\text{Да ли } a \in \Phi(mn), \text{ тј да ли је } \text{HЗД}(a, mn) = 1$$

$$\begin{array}{l} \text{како } \text{HЗС}(m, n) = mn \\ \text{HЗД}(m, n) = 1 \\ \text{систем има решење} \\ \text{у интервалу } [0, mn) \end{array}$$

$$\left. \begin{array}{l} a \equiv r \pmod{m}, \quad r \equiv 1 \pmod{m} \\ \text{HЗД}(r, m) = 1 \\ r \in \Phi(m) \end{array} \right\} \Rightarrow a \equiv 1 \pmod{m} \quad \text{HЗД}(a, m) = 1$$

$$a \equiv s \pmod{n}, \quad \begin{array}{l} s \equiv 1 \pmod{n} \\ s \in \Phi(n) \\ \text{HЗД}(s, n) = 1 \end{array} \Rightarrow a \equiv 1 \pmod{n} \quad \text{HЗД}(a, n) = 1$$

$$\Rightarrow \left. \begin{array}{l} \text{HЗД}(a, m) = 1 \\ \text{HЗД}(a, n) = 1 \end{array} \right\} \Rightarrow \text{HЗД}(a, mn) = 1$$

$$a \in \Phi(mn) \Rightarrow f \text{ je "на"}$$

$\Rightarrow f$ je bijekcija

$$\underbrace{|\Phi(mn)|}_{\varphi(mn)} = \underbrace{|\Phi(m)|}_{\varphi(m)} \cdot \underbrace{|\Phi(n)|}_{\varphi(n)}$$

$$\varphi(m) = \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n})$$

$$= \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \dots \cdot \varphi(p_n^{\alpha_n})$$

$$= (p_1^{\alpha_1} - p_1^{\alpha_1-1}) (p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdot \dots \cdot (p_n^{\alpha_n} - p_n^{\alpha_n-1})$$

ИЗВЛАЧИМО
ФАКТОРЕ ИСПРЕД

$$= p_1^{\alpha_1} p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_n}\right)$$

$$= m \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_n}\right)$$

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = (2^2 - 2)(5^2 - 5) = 2 \cdot 20 = 40$$

$$= 100 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

Ејлерова теорема: $a, n \in \mathbb{N}, a, n > 0, \text{HЗД}(a, n) = 1$
 $a^{\varphi(n)} \equiv 1 \pmod{n}$

доказ: $k = \varphi(n) \quad \Phi(n) = \{r_1, r_2, \dots, r_k\} \quad \text{HЗД}(n, r_i) = 1$

$$\left. \begin{array}{l} \text{HЗД}(a, n) = 1 \\ \text{HЗД}(r_i, n) = 1 \end{array} \right\} \Rightarrow \text{HЗД}(ar_i, n) = 1$$

$$s_i = p_n(ar_i)$$

$$\left. \begin{array}{l} ar_i \equiv 1 \pmod{n} \\ ar_i \equiv s_i \pmod{n} \end{array} \right\} \Rightarrow s_i \equiv 1 \pmod{n} \quad \text{HЗД}(s_i, n) = 1$$

$$\left. \begin{array}{l} 0 \leq S_i < n \\ \text{H3D}(S_i, n) = 1 \end{array} \right\} \Rightarrow S_i \in \Phi(n)$$

$$S_i \neq S_j, \quad i \neq j$$

ako je $S_i = S_j$

$$g_n(a r_i) = g_n(a r_j)$$

$$a r_i \equiv a r_j \pmod{n}$$

$$\left. \begin{array}{l} n \mid a(r_i - r_j) \\ \text{H3D}(n, a) = 1 \end{array} \right\} \Rightarrow n \mid r_i - r_j$$

$$\left. \begin{array}{l} -n < r_i - r_j < n \\ n \mid r_i - r_j \end{array} \right\} \Rightarrow r_i = r_j \quad \nleftrightarrow \text{ jer je } i \neq j$$

$$k = \varphi(n)$$

$$\Phi(n) = \{r_1, \dots, r_k\} = \{s_1, \dots, s_k\}$$

$$a r_1 \equiv s_1 \pmod{n}$$

$$a r_2 \equiv s_2 \pmod{n}$$

$$\vdots$$

$$a r_k \equiv s_k \pmod{n}$$

$$a^k (r_1 r_2 \dots r_k) \equiv s_1 s_2 \dots s_k \pmod{n}$$

$$a^{\varphi(n)} \cdot x \equiv x \pmod{n}$$

$$\left. \begin{array}{l} x = r_1 r_2 \dots r_k \\ \text{H3D}(r_i, n) = 1 \end{array} \right\} \Rightarrow \text{H3D}(x, n) = 1$$

$$n \mid a^{\varphi(n)} \cdot x - x$$

$$\left. \begin{array}{l} n \mid x (a^{\varphi(n)} - 1) \\ \text{H3D}(n, x) = 1 \end{array} \right\} \Rightarrow n \mid a^{\varphi(n)} - 1$$

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Malá Fermatova věta

Ako je p úprostí broj, mága je $a^p \equiv a \pmod{p}$

gokaz: • pla $a^p \equiv 0 \pmod{p}$, $a \equiv 0 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$

• pta $\Rightarrow \text{H3D}(p, a) = 1 \Rightarrow a^{\varphi(p)} \equiv 1 \pmod{p}$

odgovor $a^{p-1} \equiv 1 \pmod{p} \quad | \cdot a$
 věta $a^p \equiv a \pmod{p}$

Кардиналности скупова

Нека су A и B скупови

- Кажемо да је скупи A кардиналности мање или једнаке од B , и пишемо $|A| \leq |B|$ ако постоји $f: A \xrightarrow{1-1} B$
- Кажемо да је кардиналности скупа A једнака кардиналности скупа B , и пишемо $|A| = |B|$, ако постоји $f: A \xrightarrow{\text{бијекција}} B$
- Кажемо да је скупи A кардиналности строго мање од B , и пишемо $|A| < |B|$, ако је $|A| \leq |B|$ и $|A| \neq |B|$

Особине кардиналности

A, B, C скупови

① $|A| = |A|$ $\text{id}_A: A \xrightarrow[HA]{1-1} A$

② $|A| = |B| \Rightarrow |B| = |A|$

$f: A \rightarrow B$ бијекција

$f^{-1}: B \rightarrow A$

f^{-1} је „1-1“:

$$f^{-1}(y_1) = f^{-1}(y_2) \Rightarrow y_1 = y_2$$

$$f(f^{-1}(y_1)) = f(f^{-1}(y_2))$$

$$(f \circ f^{-1})(y_1) = (f \circ f^{-1})(y_2)$$

$$\text{id}_B(y_1) = \text{id}_B(y_2)$$

$$y_1 = y_2$$

f^{-1} је „Ha“: $x \in A$

$$f^{-1}(?) = x$$

$$f(x) = y$$

$$f^{-1}(y) = f^{-1}(f(x)) = \underbrace{(f^{-1} \circ f)}_{\text{id}_A}(x)$$

$$= \text{id}_A(x) = x$$

③ $|A| = |B| \wedge |B| = |C| \Rightarrow |A| = |C|$

$$f: A \xrightarrow[HA]{1-1} B \quad g: B \xrightarrow[HA]{1-1} C$$

$$A \xrightarrow{f} B \xrightarrow{g} C$$

$\underbrace{\hspace{10em}}_{g \circ f}$

$$g \circ f: A \rightarrow C$$

$g \circ f$ je "1-1":

$$(g \circ f)(x_1) = (g \circ f)(x_2) \stackrel{?}{\Rightarrow} x_1 = x_2$$

$$g(f(x_1)) = g(f(x_2))$$

$$\stackrel{f \text{ je "1-1"}}{\Rightarrow} f(x_1) = f(x_2)$$

$$\stackrel{f \text{ je "1-1"}}{\Rightarrow} x_1 = x_2$$

$g \circ f$ je "na" $z \in C$ $(g \circ f)(?) = z$

$(\exists y \in B) g(y) = z$ jer je g "na"

$(\exists x \in A) f(x) = y$ jer je f "na"

$$(g \circ f)(x) = g(f(x)) = g(y) = z$$

$\Rightarrow g \circ f$ jeste "na"

④ Ако je $|A| = |B|$, onda je $|A| \leq |B|$ и $|B| \leq |A|$

$$f: A \xrightarrow{1-1} B$$

$$f: A \xrightarrow{1-1} B \Rightarrow |A| \leq |B|$$

$$f^{-1}: B \xrightarrow{1-1} A \Rightarrow |B| \leq |A|$$

~~КАР~~

⑤ $|A| \leq |B| \wedge |B| \leq |C| \Rightarrow |A| \leq |C|$

$$f: A \xrightarrow{1-1} B \quad g: B \xrightarrow{1-1} C$$

$$g \circ f: A \xrightarrow{1-1} C \Rightarrow |A| \leq |C|$$

⑥ Кантор - Бернштајнова теорема

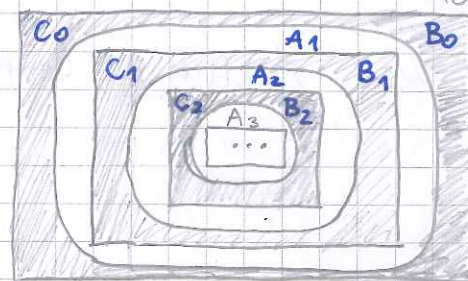
$$|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|$$

лема: Ако je $A_0 \supseteq B_0 \supseteq A_1$ и $|A_1| = |A_2|$, onda je $|A_0| = |B_0|$

доказ леме:

$$f: A_0 \xrightarrow{1-1} A_1 \quad A_0 \supseteq B_0 \supseteq A_1 \quad / f[]$$

$$A_1 = f[A_0] \quad \underbrace{f[A_0]}_{A_1} \supseteq \underbrace{f[B_0]}_{B_1} \supseteq \underbrace{f[A_1]}_{A_2}$$



$$A_{n+1} := f[A_n]$$

$$B_{n+1} := f[B_n]$$

$$A_n \supseteq B_n \supseteq A_{n+1} \quad / f[]$$

$$\underbrace{f[A_n]}_{A_{n+1}} \supseteq \underbrace{f[B_n]}_{B_{n+1}} \supseteq \underbrace{f[A_{n+1}]}_{A_{n+2}}$$

$$A_n \supseteq B_n \supseteq A_{n+1}$$

$$C := A_0 \setminus B_0$$

$$C_n := A_n \setminus B_n$$

$$f[C_n] = f[A_n \setminus B_n] = f[A_n] \setminus f[B_n] = A_{n+1} \setminus B_{n+1} = C_{n+1}$$

$$f[C_n] = C_{n+1}$$

$C = \bigcup_{n=0}^{\infty} C_n$ - унија свих шрафираних делова

$C' = \bigcup_{n=1}^{\infty} C_n$ - унија свих шрафираних делова сем C_0

D - све што није шрафирано на слици

$$A_0 = C \cup D \quad B_0 = C' \cup D$$

$$f[C] = f\left[\bigcup_{n \geq 0} C_n\right] = \bigcup_{n \geq 0} f[C_n] = \bigcup_{n \geq 0} C_{n+1} = \bigcup_{n \geq 1} C_n = C'$$

$$\begin{array}{ccc} A_0 = C \cup D & & \\ \downarrow f & \downarrow \text{id} & \\ B_0 = C' \cup D & & \end{array}$$

$$h: A_0 \rightarrow B_0 \quad h(x) = \begin{cases} f(x), & x \in C \\ x, & x \in D \end{cases}$$

$$h \text{ je "1-1"} : h(x_1) = h(x_2) \stackrel{?}{\Rightarrow} x_1 = x_2$$

$$1^\circ h(x_1), h(x_2) \in C'$$

$$2^\circ h(x_1), h(x_2) \in D$$

$$h(x_1) = f(x_1), h(x_2) = f(x_2)$$

$$x_1 = h(x_1) = h(x_2) = x_2$$

$$f(x_1) = h(x_1) = h(x_2) = f(x_2)$$

$$\Rightarrow h \text{ je "1-1"}$$

$$f \text{ je "1-1"} \Rightarrow x_1 = x_2$$

$$\Rightarrow h \text{ je "1-1"}$$

$$h \text{ je "на"} : y \in B_0 = C' \cup D$$

$$1^\circ y \in C'$$

$$2^\circ y \in D$$

$$y = f(x) \left\{ \begin{array}{l} f \text{ je "на"} \\ x \in A_0 \end{array} \right.$$

$$h(y) = y$$

$$f(x) = h(x) \Rightarrow y = h(x)$$

$$y \in D \subseteq A_0$$

$$\Rightarrow h \text{ jeste "на"}$$

$$\Rightarrow h \text{ je биекција} \Rightarrow |A_0| = |B_0|$$

доказ Кантор-Бернштајнове теореме

$$f: A \xrightarrow{1-1} B \quad g: B \xrightarrow{1-1} A$$

$$f[A] \subseteq B \quad |g|$$

$$g[f[A]] \subseteq g[B] \subseteq A$$

$$A \supseteq g[B] \supseteq g[f[A]]$$

$$B \supseteq f[A]$$

$$A \xrightarrow[f]{1-1} f[A] \xrightarrow[g]{1-1} g[f[A]]$$

$$\left. \begin{array}{l} A \xrightarrow[f]{1-1} g[f[A]] \\ A \supseteq g[B] \supseteq g[f[A]] \end{array} \right\} \xRightarrow{\text{лема}} |A| = |g[B]|$$

$$B \xrightarrow[g]{1-1} g[B]$$

$$|B| = |g[B]|$$

$$|A| = |g[B]|$$

$$|g[B]| = |B|$$

$$\Rightarrow |A| = |B|$$

7. (Бернштајнова теорема)

За свака два скупа A и B важи $|A| \leq |B|$ или $|B| \leq |A|$

(ПРЕКО АКСИОМЕ ИЗБОРА) A10

Пребројиви скупови

Скуп A је пребројив ако је исте кардиналности као и скуп природних бројева ($|A| = |\mathbb{N}|$).

$$|\mathbb{N}| = \aleph_0 \text{ (алеф-нула)}$$

- X - пребројив

$$f: \mathbb{N} \xrightarrow[\text{на } A]{1-1} X$$

$$f(0) = x_0$$

$$f(1) = x_1$$

$\vdots$

$$f(n) = x_n$$

$\vdots$

$$x \in \{x_0, x_1, \dots, x_n, \dots\}$$

елементе скупа X можемо поређати у низ који је индексирани скупом $\mathbb{N}$

• Скуп A је коначан ако $\exists n \in \mathbb{N}$ такав да постоји бијекција $f: A \rightarrow \{1, 2, \dots, n\}$

Ако A није коначан, кажемо да је бесконачан

• Скуп A је бесконачан ако постоји прави подскуп $A' \subset A$ такав да су A и A' у бијекцији

$\mathbb{N}_n := \{0, 1, \dots, n\}$ A је коначан ако постоји бијекција $\mathbb{N}_n \rightarrow A$

• Скуп $\mathbb{N}$ је бесконачан

$$\text{доказ: } A = \{n \in \mathbb{N} \mid n \geq 2\} = \{2, 3, 4, \dots\} = \mathbb{N}_{\geq 2}$$

$$A \subset \mathbb{N}$$

$$f: \mathbb{N} \xrightarrow[\text{на } A]{1-1} A \quad f(n) = n+2$$

$f: \mathbb{N} \rightarrow A$ је бијекција $\Rightarrow \mathbb{N}$ је бесконачан

$$A \subset \mathbb{N}$$

Ако је скупи A коначан или прбројив, кажемо да је највише прбројив. Ако скупи није највише прбројив, онда је непрбројив.

Примери прбројивих скупова:

① $\mathbb{Z}$ је прбројив

$$f: \mathbb{N} \xrightarrow[\text{нп}]{1-1} \mathbb{Z}$$

(ПАРНЕ СЛИКАМО У ПОЗИТИВНЕ)
(НЕПАРНЕ У НЕГАТИВНЕ)

$$f(n) = \begin{cases} \frac{n}{2}, & 2|n \\ -\frac{n+1}{2}, & 2 \nmid n \end{cases}$$

f је „на“ $z \in \mathbb{Z}$

$$1^\circ z \geq 0$$

$$2^\circ z < 0$$

$$f(2z) = z$$

$$f(-2z-1) = z$$

$$\Rightarrow |\mathbb{Z}| = |\mathbb{N}|$$

② Ако је $A \subseteq \mathbb{N}$, онда је A прбројив

$$A_0 = A \quad a_0 = \min(A_0)$$

$$A_1 = A_0 \setminus \{a_0\} \quad a_1 = \min(A_1)$$

$$A_2 = A_1 \setminus \{a_1\} \quad a_2 = \min(A_2)$$

$\vdots$

$$A_{n+1} = A_n \setminus \{a_n\} \quad a_{n+1} = \min(A_{n+1})$$

$$A = \{a_0, a_1, \dots\}$$

$$f: \mathbb{N} \rightarrow A$$

$$f(n) = a_n$$

$$\text{пример: } 3\mathbb{N} = \{0, 3, 6, 9, \dots\}$$

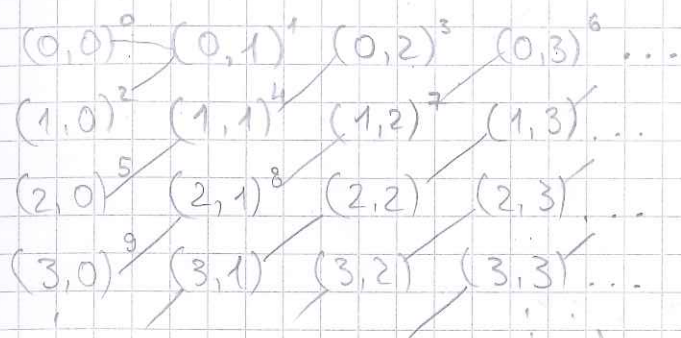
$$g: \mathbb{N} \rightarrow 3\mathbb{N}$$

$$g(n) = 3n$$

бијекција

③ $\mathbb{N} \times \mathbb{N}$ je prebrojiva

$$f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$



m elemenata na
 $m+n$ -toj dijagonali
pre elemenata $m+n$

$$1+2+3+\dots+(m+n)$$

ukupan broj elemenata
pre elemenata $(0, m+n)$

$$\frac{(m+n)(m+n+1)}{2} + m = \frac{m^2 + mn + m + n^2 + n}{2} + m$$

$$= \frac{m^2 + 2mn + n^2 + m + n}{2} + m$$

==

$$1+2+3+\dots+(m+n)+m$$

$$f(m, n) = \frac{(m+n)(m+n+1)}{2} + m$$

④ Ако је $P_{fin}(X) = \{A \subseteq X \mid A \text{ је коначан}\}$ тада је $P_{fin}(\mathbb{N})$ пребројив
 $\uparrow$ скуп коначних низова

$$f: \mathbb{N} \rightarrow P_{fin}(\mathbb{N})$$

$$n \mapsto \{n\}$$

$$g: P_{fin}(\mathbb{N}) \rightarrow \mathbb{N}$$

$$\{a_0, a_1, \dots, a_k\} \xrightarrow{g} 2^{a_0} + 2^{a_1} + \dots + 2^{a_k}$$

$$g(\{a_0, a_1, \dots, a_k\}) = g(\{b_0, b_1, \dots, b_\ell\}) \stackrel{?}{\Rightarrow} \{a_0, a_1, \dots, a_k\} = \{b_0, b_1, \dots, b_\ell\}$$

$$2^{a_0} + 2^{a_1} + \dots + 2^{a_k} = 2^{b_0} + 2^{b_1} + \dots + 2^{b_\ell}$$

доказујемо да је $a_k = b_\ell$

и не $a_k \neq b_\ell$ $a_k < b_\ell$

$$1 + 2^1 + 2^2 + \dots + 2^i = 2^{i+1} - 1 \quad i \geq 1$$

$$2^{a_k} < 2^{b_\ell} \Rightarrow 2^{a_k+1} \leq 2^{b_\ell}$$

$$2^{a_0} + 2^{a_1} + \dots + 2^{a_k} \leq 2^0 + 2^1 + \dots + 2^{a_k} \stackrel{\substack{\text{геометријски} \\ \text{низ}}}{\downarrow}}{=} 1 \cdot \frac{(1 - 2^{a_k+1})}{1-2}$$

$$= 2^{a_k+1} - 1 \leq 2^{a_k+1} \leq 2^{b_\ell}$$

$$\Rightarrow 2^{a_0} + 2^{a_1} + \dots + 2^{a_k} < 2^{b_\ell} \quad \Downarrow \quad a_k = b_\ell$$

слично доказујемо за $a_{k+1} = b_{\ell-1} \dots$

$$\left. \begin{array}{l} f: \mathbb{N} \xrightarrow{1-1} P_{fin}(\mathbb{N}) \\ g: P_{fin}(\mathbb{N}) \rightarrow \mathbb{N} \end{array} \right\} \xrightarrow{\text{к.б.т}} |\mathbb{N}| = |P_{fin}(\mathbb{N})|$$

други начин: $3^{a_0} \cdot 5^{a_1} \cdot 7^{a_2} \cdot \dots \cdot p(k)^{a_k}$

⑤ $\mathbb{Q}$ je prebrojiv

$$\mathbb{N} \xrightarrow{1-1} \mathbb{Q}$$

$$n \mapsto n$$

$$|\mathbb{N}| \leq |\mathbb{Q}|$$

$$\mathbb{Q} \xrightarrow{1-1} \mathbb{Z} \times \mathbb{N}$$

$$\frac{m}{n} \mapsto \left(\underset{\mathbb{Z}}{m}, \underset{\mathbb{N}}{n} \right)$$

m, n uzajamno
prosti

$$m \in \mathbb{Z} \quad n \in \mathbb{N}$$

$$|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}|$$

$$\mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$$

$$f: \mathbb{Z} \xrightarrow[n \neq 0]{1-1} \mathbb{N}$$

$$(z, n) \mapsto (f(z), n)$$

$$|\mathbb{Z} \times \mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$$

$$|\mathbb{N}| \leq |\mathbb{Q}|$$

$$|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$$

$$\left. \begin{array}{l} |\mathbb{Q}| \leq |\mathbb{N}| \\ |\mathbb{N}| \leq |\mathbb{Q}| \end{array} \right\} \xrightarrow{\text{K.B.T.}} |\mathbb{N}| = |\mathbb{Q}|$$

Примери скупова који нису пребројиви

① $\mathbb{R}$ није пребројив

довољно је доказати да $(0, 1)$ није пребројив

нпс. $(0, 1)$ јесте пребројив

$$(0, 1) \in \{a_0, a_1, a_2, a_3, \dots\}$$

$$a_0 = 0, \quad \boxed{a_{00}} \quad a_{01} \quad a_{02} \quad \dots \quad a_{0n} \quad \dots$$

$$a_1 = 0, \quad a_{10} \quad \boxed{a_{11}} \quad a_{12} \quad \dots \quad a_{1n} \quad \dots$$

$$a_2 = 0, \quad a_{20} \quad a_{21} \quad \boxed{a_{22}} \quad \dots \quad a_{2n} \quad \dots$$

$\vdots$

$$a_n = 0, \quad a_{n0} \quad a_{n1} \quad a_{n2} \quad \dots \quad \boxed{a_{nn}} \quad \dots$$

$$\bar{a} = 0, \quad \bar{a}_0 \quad \bar{a}_1 \quad \bar{a}_2 \quad \dots \quad \bar{a}_n \quad \dots$$

$$\bar{a}_n = \begin{cases} 1, & a_{nn} = 0 \\ 0, & a_{nn} \neq 0 \end{cases} \quad n \in \mathbb{N}$$

супротивни од датог
за свако једно
члану

$$\forall n \in \mathbb{N} \quad \bar{a} \neq a_n \quad \text{jer je } a_n \neq \bar{a}_{nn}$$

$$\left. \begin{array}{l} \bar{a} \in (0, 1) \\ \bar{a} \notin \{a_0, a_1, \dots\} \end{array} \right\} \nRightarrow (0, 1) \text{ није пребројив}$$

$$b) \{0,1\}^{\mathbb{N}} = 2^{\mathbb{N}}$$

$$|P(\mathbb{N})| = |\{0,1\}^{\mathbb{N}}|$$

3.23. Функција $\Phi: P(X) \rightarrow \{0,1\}^X$ дефинисана са $\Phi(A) = \chi_A$ је бијекција.

$$a) |\{0,1\}^{\mathbb{N}}| \leq |\mathbb{R}|$$

$$\{0,1\}^{\mathbb{N}} = \{f \mid f: \mathbb{N} \rightarrow \{0,1\}\}$$

$$G: \{0,1\}^{\mathbb{N}} \rightarrow \mathbb{R}$$

$$G(f) = \underbrace{0, f_0, f_1, f_2, \dots, f_n, \dots}_{\text{децималан запис}} \quad f_i = f(i) \quad \forall i \in \mathbb{N}$$

$$(\forall f, f' \in \{0,1\}^{\mathbb{N}}) f \neq f' \Rightarrow G(f) \text{ и } G(f') \text{ ИМАЈУ РАЗЛ. ДЕЦИМАЛЕ}$$

$$\Rightarrow G(f) \neq G(f') \Rightarrow G \text{ инјективно} \Rightarrow |\{0,1\}^{\mathbb{N}}| \leq |\mathbb{R}|$$

$$\Rightarrow \left. \begin{array}{l} |\mathbb{R}| \leq |P(\mathbb{N})| \\ |P(\mathbb{N})| \leq |\mathbb{R}| \end{array} \right\} \xrightarrow{\text{К.Б.Т.}} |P(\mathbb{N})| = |\mathbb{R}|$$

Скуп A је моћи континуума ако је $|A| = |\mathbb{R}| = c$

Булове алгебре

Увео их је Џорџ Бул средином XIX века.

Алгебарска структура $B = (B, \vee, \wedge, ', 0, 1)$, где је $B \neq \emptyset$, $0, 1 \in B$, $\vee$ и $\wedge$ су бинарне а $'$ унарна операција на скупу B , је Булова алгебра уколико су задовољене следеће аксиоме:

$$A1: x \vee y = y \vee x$$

$$A2: x \wedge y = y \wedge x$$

$$A3: x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

$$A4: x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

$$A5: x \vee 0 = x$$

$$A6: x \wedge 1 = x$$

$$A7: x \vee x' = 1$$

$$A8: x \wedge x' = 0$$

$$A9: 0 \neq 1$$

$$\forall x, y, z \in B$$

$\vee$ - Буловска дисјункција

$\wedge$ - Буловска конјункција

$'$ - Буловски комплемент

B - домен

Уколико је скупу B коначан, кажемо да је Булова алгебра B коначна, иначе кажемо да је бесконачна.

Прекидачка алгебра $2 = (\{0, 1\}, \vee, \wedge, \neg, 0, 1)$

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

$\neg$	0	1
0	1	0
1	0	1

$$x \vee y = y \vee x$$

$$x \wedge y = y \wedge x$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

$$x \vee 0 = x$$

$$x \wedge 1 = x$$

$$x \vee \neg x = 1$$

$$x \wedge \neg x = 0$$

$$0 \neq 1$$

Алгебра булевих скупи

$$X \neq \emptyset, P(X), P(X) = (P(X), \cup, \cap, ^c, \emptyset, X)$$

$$A, B, C \in P(X)$$

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup \emptyset = A$$

$$A \cap X = A$$

$$A \cup A^c = X$$

$$A \cap A^c = \emptyset$$

$$X \neq \emptyset$$

Принцип дуалности

Идентичности (формуле) F_1 и F_2 су дуални ако се идентичност F_2 може добити од идентичности F_1 тако што се свако појављивање операције $\cup$ замени са $\cap$, свако појављивање операције $\cap$ замени са $\cup$, свако појављивање 0 замени са 1 и свако појављивање 1 замени са 0.

$$(X \cup Y) \cap Y' = X$$

$$(X \cap Y) \cup Y' = X$$

дуални
идентичности

$$(X \cap 0) \cup (1 \cup X) = X' \cup 0$$

$$(X \cup 1) \cap (0 \cap X) = X' \cap 1$$

У произвојној буљевој алгебри $B = (B, \cup, \cap, ', 0, 1)$ за све $x, y, z \in B$ важе:

$$1. 0' = 1, 1' = 0 \quad 0' \stackrel{A5}{=} 0' \cup 0 \stackrel{A1}{=} 0 \cup 0' \stackrel{A7}{=} 1, 1' \stackrel{A6}{=} 1' \cap 1 \stackrel{A2}{=} 1 \cap 1' \stackrel{A8}{=} 0$$

$$2. X \cup X = X, X \cap X = X \text{ (закон идишотенције)}$$

$$X \stackrel{A5}{=} X \cup 0 \stackrel{A8}{=} X \cup (X \cap X') \stackrel{A3}{=} (X \cup X) \cap (X \cup X') \stackrel{A7}{=} (X \cup X) \cap 1 \stackrel{A6}{=} X \cup X$$

$$X \stackrel{A6}{=} X \cap 1 \stackrel{A7}{=} X \cap (X \cup X') \stackrel{A4}{=} (X \cap X) \cup (X \cap X') \stackrel{A8}{=} (X \cap X) \cup 0 \stackrel{A5}{=} X \cap X$$

$$3. X \cup (X \cap Y) = X, X \cap (X \cup Y) = X \text{ (закон апсорбције)}$$

$$1) 1 \cup X = 1 \Rightarrow 1 \cup X \stackrel{A6}{=} (1 \cup X) \cap 1 \stackrel{A7}{=} (1 \cup X) \cap (X \cup X') \stackrel{A1}{=} (X \cup 1) \cap (X \cup X') \stackrel{A3}{=} X \cup (1 \cap X') \stackrel{A2}{=} X \cup (X' \cap 1) \stackrel{A6}{=} X \cup X' \stackrel{A7}{=} 1$$

$$2) 0 \cap X = 0 \Rightarrow \text{ВАНИ ЈЕР ЈЕ ДУАЛНИ ИДЕНТИТЕТ } 1 \cup X = 1$$

$$3) X \cup (X \cap Y) = X \Rightarrow X \cup (X \cap Y) \stackrel{A6}{=} (X \cap 1) \cup (X \cap Y) \stackrel{A4}{=} X \cap (1 \cup Y) = X \cap 1 \stackrel{A6}{=} X$$

$$4. X \vee Y = 1 \quad 1 \quad X \wedge Y = 0 \quad \Rightarrow \quad X = Y' \quad (\text{јединственост комплемента})$$

$$5. (X')' = X \quad (\text{закон инволуције})$$

$$6. X \vee (Y \vee Z) = (X \vee Y) \vee Z$$

$$X \wedge (Y \wedge Z) = (X \wedge Y) \wedge Z \quad (\text{закон асоцијативности})$$

$$7. (X \wedge Y)' = X' \vee Y'$$

$$(X \vee Y)' = X' \wedge Y' \quad (\text{де Морганови закони})$$

Булово уређење

Нека је структура $B = (B, \vee, \wedge, ', 0, 1)$

На скупу B можемо дефинисати релацију парцијалног уређења на следећи начин

$$X \leq Y \text{ акко } X \wedge Y = X$$

$$\boxed{P} \quad X \wedge X = X$$

$$\boxed{AC} \quad X \leq Y \wedge Y \leq X \Rightarrow X \wedge Y = X \wedge Y \wedge X = Y \Rightarrow X = Y$$

$$\boxed{T} \quad X \leq Y \wedge Y \leq Z \Rightarrow X \wedge Y = X \wedge Y \wedge Z = Y$$

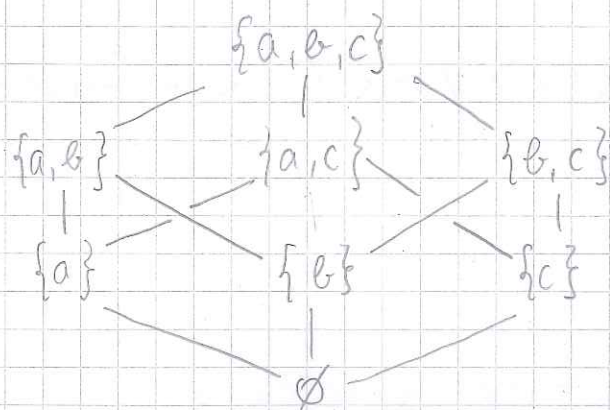
$$\Rightarrow X \wedge Z = (X \wedge Y) \wedge Z = X \wedge (Y \wedge Z) = X \wedge Y = X \Rightarrow X \leq Z$$

Пар $(B, \leq)$ је парцијално уређен скуп.

Уколико је домен B коначан, Булову алгебру B можемо представити графички помоћу Хасеовог дијаграма

• На скупу $P(\{a, b, c\}) = \{P(\{a, b, c\}), \cup, \cap, ^c, \emptyset, \{a, b, c\}\}$ дефинисано је Булово уређење $\leq$ са:

$$A \leq B \text{ акко } A \cap B = A \text{ акко } A \subseteq B$$



ПРИМЕР На скупу $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ дефиниција броја 30, дефинисане су бинарне операције $\text{H3C}(x, y)$ и $\text{H3D}(x, y)$ и УНАРНА ОПЕРАЦИЈА $30/x$, за све $x, y \in D_{30}$. Структура $D_{30} = (D_{30}, \text{H3C}, \text{H3D}, 30/x, 1, 30)$ је Булова алгебра. За све $x, y, z \in D_{30}$, испуњени су:

- A1: $\text{H3C}(x, y) = \text{H3C}(y, x)$
- A2: $\text{H3D}(x, y) = \text{H3D}(y, x)$
- A3: $\text{H3C}(x, \text{H3D}(y, z)) = \text{H3D}(\text{H3C}(x, y), \text{H3C}(x, z))$
- A4: $\text{H3D}(x, \text{H3C}(y, z)) = \text{H3C}(\text{H3D}(x, y), \text{H3D}(x, z))$
- A5: $\text{H3C}(x, 1) = x$
- A6: $\text{H3D}(x, 30) = x$
- A7: $\text{H3C}(x, 30/x) = 30$
- A8: $\text{H3D}(x, 30/x) = 1$
- A9: $1 \neq 30$

Булово уређење $\leq$ на скупу D_n :

$$x \leq y \text{ акко } \text{H3D}(x, y) = x \text{ акко } x \mid y$$

Сваки елемент $A \in \mathcal{P}(X)$ Булове алгебре $\mathcal{P}(X)$ се може записати као коначна унија једношланих елемената од X (синимона).

Атоми

Нека је $B = (B, \cup, \cap, ', 0, 1)$ произвољна Булова алгебра. Елемент $a \in B$ је атом уколико важи следеће:

1) $0 < a$

2) ако постоји $y \in B$ тд. $0 < y < a$, тада је $y = 0$ или $y = a$

У генералном случају, Булова алгебра не мора да садржи атоме. Уколико Булова алгебра не садржи ниједан атом, кажемо да је безатомична.

Коначне Булове алгебре увек имају атоме.

Штавише, сваки сл. произвољне коначне Булове алгебре може се представити као дисјункција атома.

Нека је $B = (B, \vee, \wedge, ', 0, 1)$ коначна Бурова алгебра,
тада важи следеће:

$$1. \quad x \neq 0 \wedge x \in B \Rightarrow (\exists a \in B) \overset{\text{атом}}{a} \leq x$$

$$2. \quad x \neq 0 \wedge x \in B \Rightarrow x = \vee \{a \mid a \in B \text{ је атом и } a \leq x\}$$

$$1. \quad x \text{ је атом} \Rightarrow a = x$$

$$x \text{ није атом} \Rightarrow (\exists x_1 \in B) \quad 0 < x_1 < x$$

$$x_1 \text{ је атом} \Rightarrow a = x_1$$

$$x_1 \text{ није атом} \Rightarrow (\exists x_2 \in B) \quad 0 < x_2 < x_1 < x$$

$\vdots$

Поступак се мора завршити у коначно много
корак јер је домен B коначан

$$(\exists x_n, n \in \mathbb{N}) \quad 0 < x_n < \dots < x_3 < x_2 < x_1 < x \quad \text{и } x_n \text{ је атом}$$

$$2. \quad \{a \mid a \in B \text{ је атом и } a \leq x\} = \{a_1, a_2, \dots, a_k\}$$

$$\text{Обележимо са } y = \vee \{a \mid a \in B \text{ је атом и } a \leq x\} = a_1 \vee a_2 \vee \dots \vee a_k$$

$$a_i \leq x \Rightarrow a_i \wedge x = a_i \quad i \in \{1, \dots, k\}$$

$$\Rightarrow y \wedge x = (a_1 \vee a_2 \vee \dots \vee a_k) \wedge x$$

$$= (a_1 \wedge x) \vee (a_2 \wedge x) \vee \dots \vee (a_k \wedge x)$$

$$= a_1 \vee a_2 \vee \dots \vee a_k = y$$

$$y \wedge x = y \quad \text{тј.} \quad y \leq x \quad \text{покажимо да је } y = x$$

$$\text{и/с } y < x$$

$$\text{погледајмо ел. } y' \wedge x$$

$$\Rightarrow 0 \leq y' \wedge x \quad (\text{јер је } 0 \text{ најмањи ел. скуп } B)$$

$$y' \wedge x = 0 \Rightarrow y \wedge x = (y \wedge x) \vee 0 = (y \wedge x) \vee (y' \wedge x) = (y \vee y') \wedge x$$

$$= 1 \wedge x = x \quad \text{тј.} \quad x \leq y \quad \nmid$$

$$\Rightarrow y' \wedge x \neq 0$$

$$\Rightarrow (\exists c \in B \text{ је атом}) \quad c \leq y' \wedge x$$

$$\Rightarrow c \leq \inf\{x, y'\}$$

$\inf\{x, y'\} \leq x, y'$ на основу транзитивности
булвог уређења $\Rightarrow c \leq y'$ и $c \leq x$

С обзиром да је c атом и $c \leq x \Rightarrow c = a_i$ $i \in \{1, \dots, k\}$

На основу закона апсорбује:

$$c \wedge y = a_i \wedge (a_1 \vee a_2 \vee \dots \vee a_k) = a_i = c \quad \text{тј} \quad c \leq y$$

$$\Rightarrow c \leq y' \wedge c \leq y \Rightarrow c = c \wedge c = (c \wedge y') \wedge (c \wedge y) = c \wedge y \wedge y' = c \wedge 0 = 0$$

$$c \text{ атом} \Rightarrow c \neq 0$$

$$\Downarrow \Rightarrow x = x$$

Изоморфизам булових алгебри

$$P(\{a, b\}) = (P(\{a, b\}), \cup, \cap, ^c, \emptyset, \{a, b\})$$

$$D_6 = (\{1, 2, 3, 6\}, \mid, \wedge, \vee, /, 1, 6)$$

$$\begin{array}{ccc} \{a\} & \text{---} \{a, b\} & \text{---} \{b\} \\ & \searrow \emptyset & \swarrow \end{array} \quad \text{и} \quad \begin{array}{ccc} & 6 & \\ 2 & \swarrow & \searrow 3 \\ & 1 & \end{array}$$

трећосходна два дијаграма су идентична
(до на ознаку елемената).

С обзиром да имају идентичну структуру,

$$\emptyset \leftrightarrow 1 \quad \{a\} \leftrightarrow 2 \quad \{b\} \leftrightarrow 3 \quad \{a, b\} \leftrightarrow 6$$

могу се поистовештити.

Када су две булве алгебре формално различите
али структурно исте кажемо да су изоморфне.

• Булве алгебре $B = (B, \vee, \wedge, ', 0, 1)$ и
 $B^* = (B^*, \vee^*, \wedge^*, ', 0^*, 1^*)$ су изоморфне уколико постоји
бијекција $f: B \rightarrow B^*$
за коју важи:

$$\begin{array}{l} 1) f(xy) = f(x) \vee^* f(y) \\ 2) f(x \wedge y) = f(x) \wedge^* f(y) \\ 3) f(x') = f(x)' \end{array}$$

$$B \cong B^*$$

(Ситонова теорема) Ако је $B = (B, \vee, \wedge, ', 0, 1)$ коначна Булова алгебра. Тада постоји коначан скуи S такав да је $B \cong \mathcal{P}(S)$

S - скуи свих атома у B

Функција $f: B \rightarrow \mathcal{P}(S)$ дефинисана је за све

$$x \in B: f(x) = \{a \mid a \text{ је атом и } a \leq x\}$$

↑
добро дефинисана јер је B коначна и садржи атоме

$$A = \{a_1, a_2, \dots, a_k\} \in \mathcal{P}(S) \quad x = a_1 \vee a_2 \vee \dots \vee a_k \quad A = f(x)?$$

$$a \in A \Rightarrow a = a_i \quad \exists i \in \{1, 2, \dots, k\}$$

$$\Rightarrow a_i \wedge x = a_i \wedge (a_1 \vee a_2 \vee \dots \vee a_k) = a_i$$

$$\Rightarrow a = a_i \leq x \text{ и } a \text{ је атом} \Rightarrow a \in f(x)$$

$$\Rightarrow A \subseteq f(x)$$

обрнуто $b \in f(x)$ тј b је атом и $b \leq x$

$$\Rightarrow b = b \wedge x = b \wedge (a_1 \vee a_2 \vee \dots \vee a_k) = (b \wedge a_1) \vee (b \wedge a_2) \vee \dots \vee (b \wedge a_k)$$

$$b \text{ атом} \Rightarrow \forall i \in \{1, 2, \dots, k\}, b \wedge a_i = 0 \text{ или } b \wedge a_i = b$$

$$\Rightarrow \text{постоји бар једно } (a_i \in A) \text{ } b \wedge a_i = b \text{ ај } b \leq a_i$$

$$a_i \text{ је атом} \Rightarrow b = a_i$$

⋮

$\Rightarrow$ Конечну булову алгебру могуће је конструисати само на скуновима који имају 2^m елемената $m \geq 1$

Исказна логика

исказна алгебра: $2 = \{0, 1\}$

унарна операција: $\begin{array}{c|c} p & \neg p \\ \hline 0 & 1 \\ 1 & 0 \end{array}$

бинарне операције:

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

$\Rightarrow$
 $(=)$
 $\vee$

Језик исказне алгебре L :

- логичке константе $\{T, \perp\}$
- пребројиви скуп исказних слова P
- логички ~~везани~~ везници
- заграда $(,)$

$\{p, q, r, s, t, \dots\}$
 $\{p_0, p_1, p_2, \dots\}$

$\{\neg, \wedge, \vee, \Rightarrow, \Leftarrow, \equiv\}$

Формуле: језика L :

- 1° исказна слова и логичке константе су исказне ф-је
- 2° ако су A и B исказне формуле, тада су исказне ф-је и $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftarrow B)$, $(A \equiv B)$
- 3° исказне формуле се добијају једино коначном применом правила 1° и 2°

$For L$ - скуп формула над језиком L
правило брисања спољашњих заграда

приоритет: $\neg$
 $\wedge$ $\vee$
 $\Rightarrow$ $\Leftarrow$ $\equiv$

• Валуација је било која функција $v: P \rightarrow \{0,1\}$

ПРИМЕР $P = \{p, q, r\}$

са $v(p)=0$, $v(q)=1$ и $v(r)=0$ је задата једна
валуација

$$\Rightarrow v: \begin{pmatrix} p & q & r \\ 0 & 1 & 0 \end{pmatrix}$$

• Сваку валуацију $v: P \rightarrow \{0,1\}$ можемо проузгнати до функције $v: For \rightarrow \{0,1\}$ на следећи начин:

$$v(\neg A) = \neg v(A)$$

$$v(A \wedge B) = v(A) \wedge v(B)$$

$$v(A \vee B) = v(A) \vee v(B)$$

$$v(A \Rightarrow B) = v(A) \Rightarrow v(B)$$

$$v(A \Leftrightarrow B) = v(A) \Leftrightarrow v(B)$$

$$v(A \perp B) = v(A) \perp v(B)$$

за све $A, B \in For$

• Формула A је таутологија ако је $v(A)=1$ за све валуације v . Ако $\nexists$ за сваку валуацију v важи $v(A)=0$, онда кажемо да је A контрадикција.

• Формула A је задовољива ако постоји валуација v тако да је $v(A)=1$. Скуп формула Φ је задовољив ако постоји валуација v тако да је $v(A)=1$ за све формуле $A \in \Phi$

• Формула A је порецљива ако постоји валуација v тако да је $v(A)=0$

• Формуле A и B су логички (елементарно, семантички) еквивалентне ако за сваку валуацију v важи $v(A)=v(B)$. Пишемо $A \equiv B$

$\equiv$ је релација еквиваленције

$(For, \perp, \wedge, \vee, \neg, \Rightarrow, \Leftrightarrow, 0, 1)$ - Линденбаум-Тарски алгебра

3. Формула A је логичка (семантичка) последица формуле B ако за сваку валуацију v за коју је $v(B)=1$ важи да је $v(A)=1$ ОЗНАКА $B \models A$

• формула A је логичка последица формуле B ако је $B \Rightarrow A$ тавтологија

Нормалне форме

ЛИТЕРАЛ — логичко слово или негација логичког слова

ДИСЈУНКТИВНА НОРМАЛНА ФОРМА: $F_1 \vee F_2 \vee \dots \vee F_k$ ДНФ
где је свако $i \in \{1, 2, \dots, k\}$, F_i конјункција ЛИТЕРАЛА

КОНЈУНКТИВНА НОРМАЛНА ФОРМА: $F_1 \wedge F_2 \wedge \dots \wedge F_k$ КНФ
 $i \in \{1, \dots, k\}$, F_i дисјункција литерала

КНФ-ДНФ алгоритам

свака логичка ϕ -та еквивалентна је некој формули која је у ДНФ/КНФ

1° елиминисамо везике који се примењују на логичке константе T и $\perp$

2° $p \vee q \equiv \neg(p \Rightarrow q)$

3° $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$

4° $p \Rightarrow q \equiv \neg p \vee q$

5° 2е Морганови закони

$$\begin{aligned}\neg(p \wedge q) &\equiv \neg p \vee \neg q \\ \neg(p \vee q) &\equiv \neg p \wedge \neg q\end{aligned}$$

6° $\neg\neg p \equiv p$

7° ЗАКОНИ ДИСТРИБУЦИЈЕ

Савршене нормалне форме
 исказна формула A у којој се појављују
 искључиво исказна слова $p_1, p_2, \dots, p_n$ може
 се представити у следеће две форме

$$1^\circ \text{SDNF}(A) = \bigvee_{u \in \{0,1\}^n \mid v(A)=1} (p_1^{u(p_1)} \wedge p_2^{u(p_2)} \wedge \dots \wedge p_n^{u(p_n)})$$

— савршена (канонска, потпуна) дисјунктивна
 нормална форма ф-ле A (СДНФ)

$$2^\circ \text{СКНФ}(A) = \bigwedge_{u \in \{0,1\}^n \mid v(A)=0} (p_1^{u(p_1)} \vee p_2^{u(p_2)} \vee \dots \vee p_n^{u(p_n)})$$

$$p_i^0 := \neg p_i, \text{ а } p_i^1 := p_i$$

Предикатска логика

• језик предикатске логике

- скуи променљивих $\text{Var} \quad \{x, y, z, \dots\}$
- логички везници $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$
- квантификатори $\forall, \exists$
- интерпункцијски знаци (запрез, затраге)
- знак једнакости $=$ $\{f, g, h, \dots\}$
- скуи функцијских (или операцијских) симбола Fun
- скуи релацијских (или предикатских) симбола $\text{Rel} \quad \{r, q, t, \dots\}$
- скуи константи $\text{Const} \quad \{a, b, c, \dots\}$

• Релацијски и функцијски симболи имају своју дужину
 $n \in \mathbb{N}, n > 0$ и која се назива и орност релације или функције
 симбол: a_n

• Избором скупова $\text{Fun}, \text{Rel}, \text{Const}$ бирамо конкретан језик
 предикатске логике. $\mathcal{L} = \text{Fun} \sqcup \text{Rel} \sqcup \text{Const}$

Синтакса предикатске логице

ТЕРМ (ИЗРАЗ)

Терми језика L :

- 1° Променљиве и константе су терми
- 2° Ако су $t_1, \dots, t_n$ терми и f функцијски симбол дужине n онда је $f(t_1, \dots, t_n)$ терм
- 3° Терми се могу добити једино коначном применом правила 1° и 2°

Скуп терма означавамо са $Term$

Атомичке формуле језика L :

- 1° Ако су t_1 и t_2 терми, онда је $t_1 = t_2$ ^{АТОМИЧКА ФОРМУЛА}
- 2° Ако су $t_1, \dots, t_n$ терми и R релацијски симбол дужине n , онда је $R(t_1, \dots, t_n)$ атомичка формула

Формуле језика L :

- 1° Атомичка формула је формула
 - 2° Ако су A и B формуле, онда су формуле и $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$, $\forall x A$, $\exists x A$
 - 3° Формуле се добијају једино коначном применом 1° и 2°
- Скуп формула означавамо са For

ПРИОРИТЕТ ОПЕРАЦИЈА

$\neg$	$\forall$	$\exists$
$\Rightarrow$	$\wedge$	$\vee$
	$(=)$	$\underline{\vee}$

Пример: $Fun = \{f, g\}$ $Rel = \{p, q\}$ $Const = \{a\}$
 $ar(f) = ar(g) = 1$ и $ar(p) = ar(q) = 2$

$\forall x \forall y \ p(x, y)$ формула

$g(f(x), a)$ терм

$\forall x \ f(x)$ ни једно ни друго $f(x)$ -терм

$g(x, y) = a$ формула (атомичка)

$p(x, q(x))$ ни једно ни друго $q(x)$ -формула

$\forall x (p(x, y) \Rightarrow q(x, y))$

— II —

p - релацијски симбол
 g - функцијски симбол

26.1.2018

 $\forall n \in \mathbb{N}, n \geq 1$

$$IH: \frac{3}{4} + \frac{5}{36} + \dots + \frac{2n+1}{n^2(n+1)^2} = 1 - \frac{1}{(n+1)^2}$$

$$n=1: \frac{3}{4} = 1 - \frac{1}{(1+1)^2} \quad \frac{3}{4} \checkmark \frac{3}{4}$$

$$n=n+1: \underbrace{\frac{3}{4} + \frac{5}{36} + \dots + \frac{2n+1}{n^2(n+1)^2}}_{IH} + \frac{2(n+1)+1}{(n+1)^2(n+1+1)^2} = 1 - \frac{1}{(n+1+1)^2}$$

$$1 - \frac{1}{(n+1)^2} + \frac{2n+3}{(n+1)^2(n+2)^2} = 1 - \frac{1}{(n+2)^2}$$

$$1 - \frac{(n+2)^2 - 2n - 3}{(n+1)^2(n+2)^2} = 1 - \frac{1}{(n+2)^2}$$

$$\frac{n^2+4n+4-2n-3}{n^2+2n+1} = \frac{n^2+2n+1}{(n+1)^2}$$

$$1 - \frac{n^2+4n+4-2n-3}{(n+1)^2(n+2)^2} = 1 - \frac{1}{(n+2)^2}$$

$$1 - \frac{1}{(n+2)^2} \checkmark 1 - \frac{1}{(n+2)^2}$$

Доказујемо да $\frac{3}{4} + \frac{5}{36} + \dots + \frac{2n+1}{n^2(n+1)^2} = 1 - \frac{1}{(n+1)^2}$

важи за сваку $n \in \mathbb{N}, n \geq 1$

$$3. \quad x \equiv 1 \pmod{4}$$

$$m = 4 \cdot 5 \cdot 9 = 180$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{9}$$

$$t_1 \equiv 1 \pmod{4}$$

$$t_2 \equiv 0 \pmod{4}$$

$$t_3 \equiv 0 \pmod{4}$$

$$t_1 \equiv 0 \pmod{5}$$

$$t_2 \equiv 1 \pmod{5}$$

$$t_3 \equiv 0 \pmod{5}$$

$$t_1 \equiv 0 \pmod{9}$$

$$t_2 \equiv 0 \pmod{9}$$

$$t_3 \equiv 1 \pmod{9}$$

$$H3D(5, 9) = 1$$

$$H3D(4, 9) = 1$$

$$H3D(4, 5) = 1$$

$$(5 \cdot 9)_k \equiv 1 \pmod{4}$$

$$(4 \cdot 9)_k \equiv 1 \pmod{5}$$

$$(4 \cdot 5)_k \equiv 1 \pmod{9}$$

$$k=1: 45 \checkmark \equiv 1 \pmod{4}$$

$$k=1: 36 \checkmark \equiv 1 \pmod{5}$$

$$k=1: 20 \equiv 1 \pmod{9} \times$$

$$t_1 = 45 + 180k$$

$$t_2 = 36 + 180k$$

$$k=2: 40 \equiv 1 \pmod{9} \times$$

$$k=3: 60 \equiv 1 \pmod{9} \times$$

$$k=5: 100 \equiv 1 \pmod{9} \checkmark$$

$$t_3 = 100 + 180k$$

$$x \equiv (a_1 t_1 + a_2 t_2 + a_3 t_3) \pmod{u}$$

$$x \equiv (1 \cdot 45 + 3 \cdot 36 + 2 \cdot 100) \pmod{180}$$

$$x \equiv (45 + 108 + 200) \pmod{180}$$

$$x \equiv 353 \pmod{180}$$

$$x \equiv 173 \pmod{180} \Rightarrow x = 173 + 180k \quad \checkmark$$

$$V(x) = 1 \leftarrow \text{истинно всегда}$$

$$V(x) = 0 \leftarrow \text{глаголю аистин}$$

$$(a \vee b) \Leftrightarrow (c \vee f)$$

$$(b \vee c) \Leftrightarrow (d \wedge f)$$

$$(c \vee d) \Leftrightarrow (a \vee b)$$

$$(d \vee e) \Leftrightarrow (c \Leftrightarrow f)$$

Закрепим по таблице

$$V(c) = 1$$

$$(V(a) \vee V(b)) \Leftrightarrow (1 \vee V(f))$$

$$(V(b) \vee 1) \Leftrightarrow (V(d) \wedge V(f))$$

$$(1 \vee V(d)) \Leftrightarrow (V(a) \vee V(b))$$

$$(V(d) \vee V(e)) \Leftrightarrow (1 \Leftrightarrow V(f))$$

$$V(a) \vee V(b) \Leftrightarrow \neg V(f)$$

$$V(d) \wedge V(f) \Rightarrow V(f) = 1, V(d) = 1$$

$$V(a) \vee V(b)$$

$$V(d) \vee V(e) \Leftrightarrow V(f)$$

$$v(c)=1, v(d)=1, v(f)=1$$

$$v(a) \vee v(b) \Leftrightarrow 0 \quad (\Rightarrow) \neg(v(a) \vee v(b)) \Leftrightarrow \neg v(a) \wedge \neg v(b) \quad \begin{matrix} v(a)=0 \\ v(b)=0 \end{matrix}$$

$$v(a) \vee v(b)$$

$$1 \vee v(e) \Leftrightarrow 1 \quad (\Rightarrow) v(e) = *$$

$$v(a)=0 \quad v(b)=0 \quad v(c)=0 \quad v(d)=1 \quad v(e)=*$$

$$\begin{matrix} \hookrightarrow \\ \hookrightarrow \end{matrix} v(a) \vee v(b) \Leftarrow \quad 0 \vee 0 \Leftrightarrow 0 \quad \Downarrow$$

Ано сы $v(a)$ и $v(b) = 0$, формула не байна

$$v(c)=0$$

$$(v(a) \vee v(b)) \Leftrightarrow (0 \vee v(f))$$

$$(v(b) \vee 0) \Leftrightarrow (v(d) \wedge v(f))$$

$$(0 \vee v(d)) \Leftrightarrow (v(a) \vee v(b))$$

$$(v(d) \vee v(e)) \Leftrightarrow (0 \Leftrightarrow v(f))$$

$$(v(a) \vee v(b)) \Leftrightarrow v(f)$$

$$v(b) \Leftrightarrow (v(d) \wedge v(f))$$

$$v(d) \Leftrightarrow (v(a) \vee v(b))$$

$$(v(d) \vee v(e)) \Leftrightarrow \neg v(f)$$

$$v(f)=1:$$

$$(v(a) \vee v(b)) \Leftrightarrow 1$$

$$v(b) \Leftrightarrow (v(d) \wedge 1)$$

$$v(d) \Leftrightarrow (v(a) \vee v(b))$$

$$(v(d) \vee v(e)) \Leftrightarrow 0$$

$$v(a) \vee v(b)$$

$$v(b) \Leftrightarrow v(d)$$

$$v(d) \Leftrightarrow (v(a) \vee v(b)) \quad v(e)=0$$

$$\neg(v(d)) \wedge \neg(v(e)) \Rightarrow v(d)=0$$

$$v(a) \vee v(b) \quad v(a)=1$$

$$v(b)=0 \quad \Downarrow$$

$$(v(a) \vee v(b)) \Leftrightarrow 0 \quad v(a)=0$$

$$v(d)=0 \quad v(e)=0$$

$$v(f)=0:$$

$$v(a) \vee v(b) \Leftrightarrow 0$$

$$v(b) \Leftrightarrow v(d) \wedge 0$$

$$v(d) \Leftrightarrow v(a) \vee v(b)$$

$$v(d) \vee v(e) \Leftrightarrow 1$$

$$\neg(v(a) \vee v(b)) \quad v(a)=0 \quad v(b)=0$$

$$\neg v(b) \quad v(b)=0$$

$$v(d) \Leftrightarrow v(a) \vee v(b)$$

$$v(d) \vee v(e)$$

$$v(a)=0 \quad v(b)=0$$

$$v(d) \Leftrightarrow 0 \vee 0 \quad v(d)=0$$

$$v(d) \vee v(e) \quad v(e)=1$$

$$v = \begin{pmatrix} a & b & c & d & e & f \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \checkmark$$

ГЕОМЕТРИЈСКИ ННЗ

$$y_0 = b$$

$$y_{n+1} = y_n \cdot b$$

$$S_n = \frac{a^{n+1} - 1}{a - 1}$$

АРИТМЕТИЧКИ ННЗ

$$S_n = (n+1)a + \frac{n(n+1)}{2} d$$

4.14 НЗД(18876, 5775).

18876	5775	3	1551
5775	1551	3	1122
1551	1122	1	429
1122	429	2	264
429	264	1	165
264	165	1	99
165	99	1	66
99	66	1	<u>33</u>
66	33	2	0

$$\begin{aligned}
 33 &= 99 - 66 = 99 - (165 - 99) = 2 \cdot 99 - 165 = 2(264 - 165) - 165 \\
 &= 2 \cdot 264 - 3 \cdot 165 = 2 \cdot 264 - 3(429 - 264) = -3 \cdot 429 + 8 \cdot 264 \\
 &= -3 \cdot 429 + 8(1122 - 2 \cdot 429) = 8 \cdot 1122 - 19 \cdot 429 \\
 &= 8 \cdot 1122 + 19(1551 - 1122) = -19 \cdot 1551 + 27 \cdot 1122 \\
 &= -19 \cdot 1551 + 27(5775 - 3 \cdot 1551) = 27 \cdot 5775 - 100 \cdot 1551 \\
 &= 27 \cdot 5775 - 100(18876 - 3 \cdot 5775) = -100 \cdot 18876 + 327 \cdot 5775.
 \end{aligned}$$

X

$$4.15 \quad 6006x + 1955y = 30$$

6006	1955	3	141
1955	141	13	122
141	122	1	19
122	19	6	8
19	8	2	3
8	3	2	2
3	2	1	1
2	1	2	0

$$+13 \Delta (6006, 1955) = 1$$

$$\begin{aligned}
 1 &= 3 - 2 = 3 - (8 - 2 \cdot 3) = -8 + 3 \cdot 3 \\
 &= -8 + 3(19 - 2 \cdot 8) = 3 \cdot 19 - 7 \cdot 8 \\
 &= 3 \cdot 19 - 7(122 - 6 \cdot 19) = -7 \cdot 122 + 45 \cdot 19 \\
 &= -7 \cdot 122 + 45(141 - 122) = 45 \cdot 141 - 52 \cdot 122 \\
 &= 45 \cdot 141 - 52(1955 - 13 \cdot 141) = -52 \cdot 1955 + 721 \cdot 141 \\
 &= -52 \cdot 1955 + 721(6006 - 3 \cdot 1955) = \underbrace{721 \cdot 6006}_p - \underbrace{2215 \cdot 1955}_q
 \end{aligned}$$

$$x = p \cdot \frac{c}{H3\Delta(a,b)} + \frac{b}{H3\Delta(a,b)} \cdot t$$

$$y = q \cdot \frac{c}{H3\Delta(a,b)} - \frac{a}{H3\Delta(a,b)} \cdot t \quad t \in \mathbb{Z} \quad H3\Delta(a,b) = 1$$

$$x = 721 \cdot 30 + 1955t = 21630 + 1955t$$

$$y = (-2215) \cdot 30 - 6006t = -66450 - 6006t \quad t \in \mathbb{Z}$$

$$4.17 \quad 437 \mid 18! + 1 \quad 437 = 23 \cdot 19$$

$$19 \mid 18! + 1 \quad 23 \mid 18! + 1$$

$$\begin{aligned}
 18! &\equiv -1 \pmod{19} \\
 (19-1)! &\equiv -1 \pmod{19}
 \end{aligned}$$

✓

$$18! \equiv -1 \pmod{23}$$

$$(23-1)! = 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18!$$

$$\begin{aligned}
 &\equiv (-1)(-2)(-3)(-4) \cdot 18! \pmod{23} \\
 &\equiv 24 \cdot 18! \pmod{23} \\
 &\equiv 1 \cdot 18! \pmod{23}
 \end{aligned}$$

4.16

$19! + 19$

$20! + 19$

$H3D = ?$

$H3D(19! + 19, 20! + 19) = d$

$d > 1$

$19 \mid \frac{19(18! + 1)}{19(20 \cdot 18! + 1)}$

$19! \equiv -19 \pmod{d}$

$20! \equiv -19 \pmod{d}$

$20 \cdot 19! \equiv -19 \pmod{d}$

$20(-19) \equiv -19 \pmod{d}$

$-380 \equiv -19 \pmod{d}$

$-361 \equiv 0 \pmod{d}$

$\Rightarrow d \mid 361$

$20! + 19 \equiv -361 \pmod{d}$

$361 = 19^2 \stackrel{?}{\Rightarrow} d \in \{19, 361\}$

$$\frac{19! + 19}{19} = 18! + 1; \quad \frac{20! + 19}{19} = 20 \cdot 18! + 1 = (1 + 19)18! + 1$$

$$= 18! + 19 \cdot 18! + 1 = \underbrace{18! + 1}_{19!} + \underbrace{19 \cdot 18!}_{19!}$$

Виксонова теорема $19 \mid 18! + 1$

$19 \mid \frac{19! + 19}{19}$

$19 \mid \frac{20! + 19}{19}$

$19^2 \mid 19! + 19$

$19^2 \mid 20! + 19$

$d = 361$

$2. A \cup B = A \cup C \Rightarrow B = C$

$A = \{1, 2, 3, 4\}$

$B = \{1, 2, 3, 5\}$

$C = \{5\}$

$A \cup B = \{1, 2, 3, 4, 5\}$

$A \cup C = \{1, 2, 3, 4, 5\}$

$\cancel{X_A + X_A X_B + X_B = X_A + X_A X_C + X_C}$

$\cancel{X_A + X_A X_A X_B + X_A X_C + X_B + X_C = 0}$

$\cancel{X_A(X_B + X_C) + X_B + X_C = 0}$

$\cancel{(X_B + X_C)(X_A + 1) = 0}$

$$5. (18!)^3 + 34^{19^{12}} \equiv x \pmod{323}$$

$$A \equiv 0 \pmod{17}$$

$$17 \mid 18!$$

$$17 \mid 34$$

$$18! \equiv -1 \pmod{19}$$

$$(18!)^3 \equiv (-1)^3 \pmod{19}$$

$$(18!)^3 \equiv -1 \pmod{19}$$

$$19 \nmid 34$$

МАЛА ФЕРМАОВА
 $a^p \equiv a \pmod{p}$
 $a^{p-1} \equiv 1 \pmod{p}$

$$\Rightarrow 34^{18} \equiv 1 \pmod{19}$$

$$19^{12} \equiv 9 \pmod{18}$$

$$19 \equiv 1 \pmod{18}$$

$$1^{12} \equiv 1 \pmod{18}$$

$$\Rightarrow 34^{19^{12}} \equiv 34 \equiv 15 \pmod{19}$$

$$A \equiv -1 + 15 \equiv 14 \pmod{19}$$

$$A = 17k = 19\ell + 14 \quad k, \ell \in \mathbb{Z}$$

$$19\ell + 14 \equiv 0 \pmod{17}$$

$$2\ell + 14 \equiv 0 \pmod{17}$$

$$17 - 14 = 3$$

$$2\ell \equiv 3 \pmod{17}$$

$$3 + 17 = 20$$

$$2\ell \equiv 20 \pmod{17}$$

$$\text{НОД}(2, 17) = 1$$

$$\ell \equiv 10 \pmod{17}$$

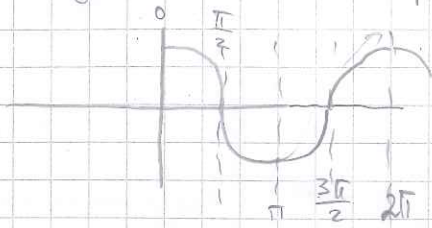
$$\ell = 17m + 10$$

$$A = 19\ell + 14 = 19(17m + 10) = 323m + 190 + 14$$

$$4. A = \{2, 4, 6, 8, 10, 12, 14, 16\} \times \left[\frac{3\pi}{2}, 2\pi\right]$$

релација поретка ρ $(m, x) \rho (n, y)$ ако $m \wedge n$ $\cos x \geq \cos y$

2 део сваки број из првог део уређеног пара



$\cos 2\pi$ је највећа могућа вредност

$\cos \frac{3\pi}{2}$ је најмања —||—

НАЈМАЊИ ЕЛ $(2, 2\pi)$

МАКСИМАЛНИ ЕЛЕМЕНТИ $(10, \frac{3\pi}{2}), (12, \frac{3\pi}{2})$ 16 14

2021/22 ЈАН 2

$$3. (A \setminus B) \Delta C = (A \Delta C) \cup (B \cap C) \quad \text{ако } (A \cap B) \setminus C = \emptyset$$

$$(\chi_A + \chi_A \chi_B) \Delta C = (\chi_A + \chi_C) \cup (\chi_B \chi_C)$$

$$(\chi_A \chi_B) \setminus C = \emptyset$$

$$\chi_A \chi_B + \chi_A \chi_B \chi_C = 0$$

$$\chi_A \chi_B = \chi_A \chi_B \chi_C$$

$$\chi_A + \chi_A \chi_B + \chi_C = \chi_A + \chi_C + (\chi_A + \chi_C) \chi_B \chi_C + \chi_B \chi_C$$

$$\chi_A + \chi_A \chi_B + \chi_C = \chi_A + \chi_C + \chi_A \chi_B \chi_C + \chi_C \chi_B \chi_C + \chi_C \chi_C$$

$$\chi_A + \chi_A \chi_B + \chi_C = \chi_A + \chi_A \chi_B \chi_C + \chi_C$$

$$\chi_A + \chi_A \chi_B + \chi_C = \chi_A + \chi_A \chi_B + \chi_C$$

$$5. 2017^{2018^{2019}} \equiv x \pmod{100}$$

$$a^p \equiv a_1^p \pmod{x}$$

$$\begin{array}{r} 17 \cdot 17 \\ 119 \\ + 17 \\ \hline 289 \end{array}$$

$$\begin{array}{r} 89 \cdot 17 \\ 623 \\ + 89 \\ \hline 1513 \end{array}$$

$$\begin{array}{r} 13 \cdot 17 \\ 91 \\ + 13 \\ \hline 221 \end{array}$$

$$100 = 4 \cdot 25$$

$$2017 \equiv 1 \pmod{4}$$

25, 2017 узаймно прости (ојерова теорема)

$$\varphi(25) = 25 \cdot \left(1 - \frac{1}{5}\right) = 25 \cdot \frac{4}{5} = 20$$

$$2017^{20} \equiv 1 \pmod{25}$$

$$\Rightarrow 2017^{2018^{2019}} \equiv 1 \pmod{4}$$

$$2018^{2019} \equiv a \pmod{20}$$

$$20 = 4 \cdot 5$$

$$\text{H3D}(4, 5) = 1$$

$$2018 \equiv 2 \pmod{4}$$

$$\Rightarrow 2018^4 \equiv 1 \pmod{5}$$

$$2018^{2019} \equiv 2^{2019} \pmod{4}$$

$$2019 \equiv 3 \pmod{4}$$

$$4 \mid 2^{2019} = 4 \mid 4 \cdot 2^{2017}$$

$$\Rightarrow 2018^{2019} \equiv 2018^3 \pmod{5}$$

$$\begin{array}{r} 18 \cdot 18 \\ 64 \\ \hline 64 \end{array}$$

$$\Rightarrow 2018^{2019} \equiv 2 \pmod{5}$$

$$2018^{2019} \equiv a \pmod{20}$$

$$4 \mid 2018^{2019} \quad 1 \quad 2018^{2019} \equiv 3 \pmod{5}$$

$$2a = 4k = 5l + 2$$

$$5l \equiv -2 \pmod{4}$$

$$5l \equiv -2 \pmod{4}$$

$$l \equiv -2 \pmod{4}$$

$$\Rightarrow l = 4m + 2$$

$$2018^{2019} = 5(4m+2) + 2 = 20m + 12$$

$$2018^{2019} \equiv \overbrace{20m}^{20} + 12 \pmod{20}$$

$$\equiv 12 \pmod{20}$$

$$\Rightarrow 2017^{2018^{2019}} \equiv 2017^{12} \pmod{25}$$

$$\begin{array}{r} 1 \ 2 \\ 2017 \cdot 2017 \\ \hline 119 \\ + 7 \\ \hline 89 \equiv 14 \pmod{25} \end{array}$$

$$\begin{array}{r} 1 \\ 14 \cdot 14 \\ \hline 56 \\ + 14 \\ \hline 196 \equiv 21 \pmod{25} \end{array} \quad 2017^4$$

$$\Rightarrow 2017^{2018^{2019}} \equiv 11 \pmod{25}$$

$$\begin{array}{l} 2017^{2018^{2019}} \equiv 1 \pmod{4} \\ 2017^{2018^{2019}} \equiv 11 \pmod{25} \end{array}$$

$$\begin{array}{r} 21 \cdot 21 \\ \hline 21 \\ + 42 \\ \hline 441 \equiv 16 \pmod{25} \end{array} \quad 2017^8$$

$$\begin{array}{r} 16 \cdot 21 \\ \hline 16 \\ + 32 \\ \hline 336 \equiv 11 \pmod{25} \end{array}$$

$$a) \quad \alpha = 2017^{2018^{2019}} = 4k + 1 = 25l + 11$$

$$25l + 11 \equiv 1 \pmod{4}$$

$$l + 3 \equiv 1 \pmod{4}$$

$$l \equiv 2 \pmod{4}$$

$$l = 4m + 2$$

$$2017^{2018^{2019}} = 25(4m+2) + 11$$

$$= 100m + 61$$

$$2017^{2018^{2019}} \equiv 61 \pmod{100}$$

$$2. \sum_{k=1}^n \frac{1}{k(k+1)(k+2)} = \frac{1}{4} - \frac{1}{2(n+1)(n+2)} \quad n \geq 1$$

базис индукции $n=1$

$$\frac{1}{1(1+1)(1+2)} = \frac{1}{4} - \frac{1}{2(1+1)(1+2)}$$

$$\frac{1}{2 \cdot 3} = \frac{1}{4} - \frac{1}{2 \cdot 2 \cdot 3}$$

$$\frac{1}{2} \cdot \frac{1}{3} = \frac{1}{2} \left(\frac{1}{2} - \frac{1}{6} \right)$$

$\frac{3}{6} - \frac{1}{6} = \frac{2}{6} = \frac{1}{3} \quad \checkmark$

$$\text{UX: } \sum_{k=1}^n \frac{1}{k(k+1)(k+2)} = \frac{1}{4} - \frac{1}{2(n+1)(n+2)}$$

UK: $n = n+1$

$$\sum_{k=1}^{n+1} \frac{1}{k(k+1)(k+2)} = \frac{1}{4} - \frac{1}{2(n+1+1)(n+1+2)}$$

$$\left(\sum_{k=1}^n \frac{1}{k(k+1)(k+2)} \right) + \frac{1}{(n+1)(n+1+1)(n+1+2)} = \frac{1}{4} - \frac{1}{2(n+2)(n+3)}$$

$$\text{UX} \Rightarrow \frac{1}{4} - \frac{1}{2(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} = \frac{1}{4} - \frac{1}{2(n+2)(n+3)}$$

$$\frac{1}{4} - \frac{1}{(n+1)(n+2)} \left(\frac{1}{2} - \frac{1}{n+3} \right) = \frac{1}{4} - \frac{1}{2(n+2)(n+3)}$$

$$\frac{1}{2} - \frac{1}{n+3} = \frac{n+3-2}{2(n+3)} = \frac{n+1}{2(n+3)}$$

$$\frac{1}{4} - \frac{1}{(n+1)(n+2)} \cdot \frac{n+1}{2(n+3)} = \frac{1}{4} - \frac{1}{2(n+2)(n+3)} \quad \checkmark$$

доказано что индуктивный шаг выполнен

1.

$$a \Leftrightarrow g \vee e$$

$$b \Leftrightarrow e \vee \neg c$$

$$c \Leftrightarrow (b \vee e)$$

$$d \Leftrightarrow (\neg c \Rightarrow \neg f)$$

$$e \Leftrightarrow \neg g \wedge \neg f$$

гужыца на аловы

$$a \Rightarrow b \Leftrightarrow \neg a \vee b$$

$$1^\circ \quad v(e) = 1$$

$$v(a) \Leftrightarrow v(g) \vee 1$$

$$v(b) \Leftrightarrow 1 \vee \neg v(c)$$

$$v(c) \Leftrightarrow (v(b) \vee 1)$$

$$v(d) \Leftrightarrow (\neg v(c) \Rightarrow \neg v(f))$$

$$1 \Leftrightarrow \neg v(g) \wedge \neg v(f)$$

$$v(a) \Leftrightarrow 1$$

$$v(a) = 1$$

$$v(b) \Leftrightarrow 1$$

$$v(b) = 1$$

$$v(c) \Leftrightarrow \neg v(b)$$

$$v(c) = 0$$

$$v(d) \Leftrightarrow v(c) \vee \neg v(f)$$

$$\neg v(g) \wedge \neg v(f)$$

$$v(d) \Leftrightarrow 0 \vee \neg v(f) \quad v(d) \Leftrightarrow \neg v(f)$$

$$\neg v(g) \wedge \neg v(f)$$

$$1.1^\circ \quad v(f) = 1$$

$$1.2^\circ \quad v(f) = 0$$

$$v(d) = 0$$

$$v(d) = 1$$

$$\neg v(g) \wedge 0 \quad \downarrow$$

$$\neg v(g) \wedge 1$$

$$v(g) = 0$$

$$v = \begin{pmatrix} a & b & c & d & e & f & g \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

$$4. f: X \longrightarrow Y \quad f \text{ "1-1" } a \neq 0 \quad (B, C \in Y, A \subseteq X) \quad f^{-1}[f[A] \setminus B] \setminus f^{-1}[C] = A \setminus f^{-1}[B \cup C]$$

$$B, C \in Y \quad A \subseteq X$$

$$f^{-1}[f[A] \setminus B] \setminus f^{-1}[C] = A \setminus f^{-1}[B \cup C]$$

$$A \setminus B \cup C = (A \setminus B) \cap (A \setminus C)$$

$$\Rightarrow f \text{ инъективна} \quad (f^{-1}[f[A]] = A)$$

$$f^{-1}[f[A] \setminus B] = A \setminus f^{-1}[B] \quad ; \quad f^{-1}[B \cup C] = f^{-1}[B] \cup f^{-1}[C]$$

$$(A \setminus f^{-1}[B]) \setminus f^{-1}[C] = A \setminus (f^{-1}[B] \cup f^{-1}[C])$$

$$\Leftarrow \text{mnc} \quad \exists x, y \in X, \quad x \neq y \quad f(x) = f(y) = a$$

$$A = \{x\} \quad B = C = \emptyset$$

$$f^{-1}[f[A] \setminus B] \setminus f^{-1}[C] = f^{-1}[\{a\} \setminus \emptyset] \setminus \emptyset = \{x, y\}$$

$$A \setminus f^{-1}[B \cup C] = \{x\} \setminus \emptyset = \{x\} \quad x \neq y$$

21/22 г. 1

$$4. (A \cup X) \cap (B \setminus X) = ((A \cap B) \cup X)^c$$

$$(\chi_A + \chi_A \chi_X + \chi_X) \cap (\chi_B + \chi_B \chi_X) = ((\chi_A \chi_B) \cup X)^c$$

$$(\chi_A + \chi_A \chi_X + \chi_X)(\chi_B + \chi_B \chi_X) = (\chi_A \chi_B + \chi_A \chi_B \chi_X + \chi_X)^c$$

$$\chi_A \chi_B + \chi_A \chi_B \chi_X + \chi_A \chi_B \chi_X + \chi_A \chi_B \chi_X + \chi_B \chi_X + \chi_B \chi_X = 1 + \chi_A \chi_B + \chi_A \chi_B \chi_X + \chi_X$$

$$\chi_A \chi_B + \chi_A \chi_B \chi_X = 1 + \chi_A \chi_B + \chi_A \chi_B \chi_X + \chi_X \quad \chi_X = 1$$

$$\chi_A \chi_B + \chi_A \chi_B = 1 + \chi_A \chi_B + \chi_A \chi_B + 1$$

$$0 = 0$$

$$H_{32}(4, 7) = 1$$

$$5. \quad X \equiv 16! 19! \pmod{37}$$

$$X \equiv 4^{22^{56}} \pmod{7}$$

$$X \equiv a \pmod{259}$$

$$4^6 \equiv 1 \pmod{7}$$

$$\Rightarrow 22^{56} \equiv a \pmod{6}$$

$$22 \equiv 4 \pmod{6}$$

$$\Rightarrow 22^{56} \equiv 4 \pmod{6}$$

$$\Rightarrow 4^4 \equiv 256 \equiv 4 \pmod{7}$$

$$16! \equiv (-36)(-35) \dots (-22)(-21) \equiv 36 \cdot 35 \dots 22 \cdot 21 \pmod{37}$$

$$16! \cdot 19! \equiv 19! \cdot 24 \cdot 22 \dots 35 \cdot 36 \equiv 20x \equiv -1 \pmod{37}$$

~~премиса да се да му је јачно~~ $x \equiv 24 \pmod{37}$

$$x = 37k + 24 = 7l + 4$$

$$37k + 24 \equiv 4 \pmod{7}$$

$$2k + 3 \equiv 4 \pmod{7} \quad / \cdot 4$$

$$8k + 12 \equiv 16 \pmod{7}$$

$$k + 5 \equiv 2 \pmod{7}$$

$$k \equiv -3 \pmod{7} \quad 4$$

$$k = 7m + 4$$

$$x = 37(7m + 4) + 24 = 259m + 148 + 24 = 259m + 172$$

$$3. \quad \rho \subseteq \mathbb{R} \times \mathbb{R} \quad (a^2 - b^2)(a^2 b^2 - 16) = 0$$

ДА ЛИ ЈЕ РЕЛАЦИЈА ЕКВИВ.

РЕФЛЕКСИВНА $(a, a) \in \rho$

$$(a^2 - a^2)(a^2 a^2 - 16) = 0$$

$$0 \cdot (a^4 - 16) \neq 0$$

СИМЕТРИЧНА $(a, b) \in \rho \quad (b, a) \in \rho$

$$(a^2 - b^2)(a^2 b^2 - 16) = 0$$

$$\Rightarrow -(b^2 - a^2)(a^2 b^2 - 16) = 0 \quad / \cdot -1$$

$$(b^2 - a^2)(b^2 a^2 - 16) = 0 \quad \checkmark$$

ТРАНЗИТИВНА $\{(a, b), (b, c)\} \subseteq \rho \stackrel{?}{\Rightarrow} (a, c) \in \rho$

$$a^2 - b^2 = 0 \quad \wedge \quad b^2 - c^2 = 0 \stackrel{+}{\Rightarrow} a^2 - b^2 + b^2 - c^2 = 0 \rightarrow a^2 - c^2 = 0 \quad \checkmark$$

$$a^2 b^2 - 16 = 0 \quad \wedge \quad b^2 - c^2 = 0 \Rightarrow b^2 = c^2 \Rightarrow a^2 c^2 - 16 = 0$$

$$b^2 c^2 - 16 = 0 \quad \wedge \quad a^2 - b^2 = 0 \Rightarrow a^2 = b^2 \Rightarrow a^2 c^2 - 16 = 0$$

$$a^2 b^2 - 16 = 0 \quad \wedge \quad b^2 c^2 - 16 = 0 \Rightarrow a, b, c \neq 0 \Rightarrow a^2 b^2 = 16 = b^2 c^2$$

$$a^2 = c^2 \Rightarrow (a^2 - c^2) = 0$$

$$\text{Класа еквивал. } a \quad (a^2 - x^2)(a^2 x^2 - 16) = 0$$

$$a^2 - x^2 = 0 : \quad x = \pm a$$

$$a^2 x^2 - 16 = 0 : \quad (ax)^2 = 16$$

$$ax = \pm 4$$

$$x = \pm \frac{4}{a}$$

$$\text{Класа еквивалентности } a \neq 0 \quad \{a = \pm a, \pm \frac{4}{a}\}$$

$$C_0 \quad -x^2 \cdot (-16) = 0$$

$$16x^2 = 0$$

$$x = 0$$

$$C_0 = \{0\}$$

2026

$$S. \quad 539 \mid 25^{86} \cdot x + 3^{420}$$

$$539 \mid 3^{420}$$

$$\Rightarrow 539 \mid 25^{86} \cdot x + 1$$

$$539 = 49 \cdot 11$$

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$$3^{\varphi(539)} \equiv 1 \pmod{539}$$

$$\begin{aligned} \varphi(539) &= 7^2 \cdot 11 \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{11}\right) \\ &= 7^2 \cdot 11 \cdot \frac{6}{7} \cdot \frac{10}{11} = 420 \end{aligned}$$

$$3^{420} \equiv 1 \pmod{539}$$

$$25^{86} x \equiv -1 \pmod{11}$$

$$5^{172} \cdot x \equiv -1 \pmod{11}$$

$$\varphi(11) = 10$$

$$5^{10} \equiv 1 \pmod{11}$$

$$5^2 \cdot x \equiv -1 \pmod{11}$$

$$(22+3) \quad 25x \equiv -1 \pmod{11}$$

$$3x \equiv -1 \pmod{11} / \cdot 4$$

$$12x \equiv -4 \pmod{11}$$

$$x \equiv -4 \pmod{11}$$

$$25^{86} x \equiv -1 \pmod{49}$$

$$\varphi(49) = 7^2 - 7^{2-1} = 42$$

$$5^{42} \equiv 1 \pmod{49}$$

$$\Rightarrow 5^4 \cdot x \equiv -1 \pmod{49}$$

$$\begin{array}{r} 25 \cdot 25 \\ 125 \\ + 50 \\ \hline 625 \end{array}$$

$$625x \equiv -1 \pmod{49}$$

$$37x \equiv -1 \pmod{49}$$

$$12x \equiv 1 \pmod{49} / \cdot 4$$

$$-48x \equiv -1 \pmod{49}$$

$$x \equiv -1 \pmod{49}$$

$$x = 11k - 4 = 49l - 1$$

$$49l - 1 \equiv -4 \pmod{11}$$

$$5l \equiv -3 \pmod{11} / \cdot (-2)$$

$$-10l \equiv 6 \pmod{11}$$

$$l \equiv 6 \pmod{11}$$

$$l = 11m + 6$$

$$49(11m + 6) - 1 = 536m + 294 - 1 = 536m + 293$$

$$5. (12!)^2 + 2^{19^{12}} \equiv x \pmod{143} \quad 143 = 11 \cdot 13$$

$$(12!)^2 \equiv a \pmod{13} \quad (12!)^2 \equiv a \pmod{11}$$

$$(13-1)! \equiv -1 \pmod{13} \quad 12 \cdot 11 \cdot 10! \text{ je potrebno sa 11}$$

$$(12!)^2 \equiv 1 \pmod{13} \quad = (12!)^2 \equiv 0 \pmod{11}$$

$$(12!)^2 = 13k + 1 = 11l$$

$$\begin{aligned} 13k + 1 &\equiv 0 \pmod{11} \\ 2k &\equiv -1 \pmod{11} \quad / \cdot 6 \\ 12k &\equiv -6 \pmod{11} \\ k &\equiv 5 \pmod{11} \\ k &= 11m + 5 \end{aligned}$$

$$\begin{aligned} (12!)^2 &= 13(11k + 5) + 1 \\ &= 143k + 66 \end{aligned}$$

$$\Rightarrow (12!)^2 \equiv 66 \pmod{143}$$

$$\text{HSD}(2, 11) = 1$$

$$2^{19^{12}} \equiv a \pmod{13}$$

$$2^{\varphi(13)} \equiv 1 \pmod{13}$$

$$2^{12} \equiv 1 \pmod{13}$$

$$\text{HSD}(19, 12) = 1$$

$$19^{12} \equiv 0 \pmod{12}$$

$$\varphi(12) = 2 \cdot 2 \cdot 3 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$$

$$19^4 \equiv 1 \pmod{12}$$

$$\Rightarrow 19^{4 \cdot 3} \equiv 1 \pmod{12}$$

$$\Rightarrow 2^1 \equiv 2 \pmod{13}$$

$$(12!)^2 + 2^{19^{12}} \equiv 66 + 2 \pmod{143}$$

U potpunosti sam
pretracao

$$2^{19^{12}} \equiv a \pmod{11}$$

$$2^{\varphi(11)} \equiv 1 \pmod{11}$$

$$2^{10} \equiv 1 \pmod{11}$$

$$19^{12} \equiv 0 \pmod{10}$$

$$\varphi(10) = 8 \cdot 2 \cdot \frac{1}{2} \cdot \frac{4}{8} = 4$$

$$19^4 \equiv 1 \pmod{10}$$

$$\Rightarrow 19^{4 \cdot 3} \equiv 1 \pmod{10}$$

$$\Rightarrow 2^1 \equiv 2 \pmod{11}$$

$$2^{19^{12}} \equiv 13k + 2 = 11l + 2$$

$$13k + 2 \equiv 2 \pmod{11}$$

$$2k \equiv 0 \pmod{11} \quad / \cdot 6$$

$$k \equiv 0 \pmod{11}$$

$$k = 11m$$

$$= 13 \cdot 11m + 2$$

$$4. a) f: X \rightarrow Y \text{ "на" akkor } (\forall B \subseteq Y) f[f^{-1}[B]] = B$$

$$\Rightarrow f \text{ "на"}$$

$$(\forall y \in Y) (\exists x \in X) f(x) = y$$

$$\Leftrightarrow (\forall y \in Y) y \in f[f^{-1}[B]] \Leftrightarrow y \in B$$

$$\Leftrightarrow (\forall y \in Y) ((\exists x \in f^{-1}[B]) f(x) = y \Leftrightarrow y \in B)$$

$$\Leftrightarrow \text{nn} (\exists y \in Y) (\forall x \in X) f(x) = y$$

$$B = \{y\} \quad f[f^{-1}[B]] = f[\emptyset] = \emptyset \quad \downarrow$$

$$5) f: X \rightarrow Y \text{ "на" } \exists g \text{ "1-1" } P(Y) \text{ y } P(X)$$

$$g: P(Y) \rightarrow P(X) \quad g(B) = f^{-1}[B] \text{ "1-1" ?}$$

$$B_1, B_2 \subseteq Y \quad g(B_1) = g(B_2), \quad f^{-1}[B_1] = f^{-1}[B_2]$$

$$\Rightarrow f[f^{-1}[B_1]] = f[f^{-1}[B_2]] \quad f \text{ "на" } \Rightarrow B_1 = B_2$$

$$\Rightarrow g \text{ "1-1"}$$

$$2. \sum_{k=1}^n \frac{2k+1}{k^2(1+k)^2} = 1 - \frac{1}{(n+1)^2} \quad \forall n \geq 1$$

$$n=1 \quad \frac{2 \cdot 1 + 1}{1^2(1+1)^2} = 1 - \frac{1}{(1+1)^2}$$

$$\frac{3}{4} = \frac{3}{4}$$

UX:

$$UK: n = n+1$$

$$\sum_{k=1}^{n+1} \frac{2k+1}{k^2(1+k)^2} = 1 - \frac{1}{(n+1+1)^2}$$

$$\left(\sum_{k=1}^n \frac{2k+1}{k^2(1+k)^2} \right) + \frac{2(n+1)+1}{(n+1)^2(1+n+1)^2} = 1 - \frac{1}{(n+2)^2}$$

$$\stackrel{ux}{=} 1 - \frac{1}{(n+1)^2} + \frac{2n+3}{(n+1)^2(n+2)^2} = 1 - \frac{1}{(n+2)^2}$$

$$1 - \frac{(n+2)^2 - 2n - 3}{(n+1)^2(n+2)^2} = 1 - \frac{1}{(n+2)^2}$$

$$1 - \frac{n^2 + 4n + 4 - 2n - 3}{(n+1)^2(n+2)^2} = 1 - \frac{1}{(n+2)^2}$$

$$1 - \frac{(n+1)^2}{(n+1)^2(n+2)^2} = 1 - \frac{1}{(n+2)^2} \quad \checkmark$$

$$3. ((A \Delta B) \setminus (C \setminus A))^c = A^c \cap B \cap C \quad \text{акко} \quad \begin{matrix} A \Delta B = X \\ \chi_A + \chi_B = \chi_X \end{matrix}$$

$$((\chi_A + \chi_B) \setminus (\chi_C + \chi_A \chi_C))^c = (1 + \chi_A) \chi_B \chi_C$$

$$1 + \chi_A + \chi_B + (\chi_A + \chi_B)(\chi_C + \chi_A \chi_C) = \chi_A \chi_B \chi_C + \chi_B \chi_C$$

$$1 + \chi_A + \chi_B + \chi_A \chi_C + \chi_A \chi_C + \chi_B \chi_C + \chi_A \chi_B \chi_C = \chi_A \chi_B \chi_C + \chi_B \chi_C$$

$$1 + \chi_A + \chi_B + \chi_B \chi_C + \chi_A \chi_B \chi_C = \chi_A \chi_B \chi_C + \chi_B \chi_C$$

$$\chi_A + \chi_B = 1 \quad (\Rightarrow) \quad A \Delta B = X$$