

Skupovi

- pojavi koji se vodi aksiomski (ZF system)
- prethodni sistem (Kantorova mainna teorija) daje neke paradokse (Russelov paradoks $\{x \mid x \notin x\}$)

Neka su A i B neki skupovi.

Kazemo da je $A \subseteq B$ ukoliko svaka $x \in A$ takođe pripada i skupu B ($x \in A \Rightarrow x \in B$)

Kazemo da je $A = B$ ukoliko su im svi elementi jednaki (odnosno, ukoliko je $A \subseteq B$ i $B \subseteq A$)

Osnovne operacije na skupovima:

$$A \cup B = \{x \mid x \in A \text{ ili } x \in B\} = \{x \mid x \in A \vee x \in B\}$$

$$A \cap B = \{x \mid x \in A \text{ i } x \in B\} = \{x \mid x \in A \wedge x \in B\}$$

$$A \setminus B = \{x \mid x \in A \text{ i } x \notin B\} = \{x \mid x \in A \wedge \neg(x \in B)\}$$

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



Ako je $A \subseteq X$, gde je X neki ambijentalni skup tada je $A^c = X \setminus A$.

Osnovne osobine operacija:

$$A \cup A = A$$

$$A \cup B = B \cup A$$

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

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

$$(A \cap B)^c = A^c \cup B^c$$

$$A \cup \emptyset = A$$

$$A \Delta B = B \Delta A$$

$$A \cap B \subseteq A$$

$$A \subseteq A \cup B$$

$$A \cap A = A$$

$$A \cap B = B \cap A$$

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

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

$$(A \cup B)^c = A^c \cap B^c$$

$$A \cap \emptyset = \emptyset$$

$$A \Delta (B \Delta C) = (A \Delta B) \Delta C$$

$$A \cap B \subseteq B$$

$$B \subseteq A \cup B$$

1. Dokazati skupovni identitet:

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

Treba dokazati da je $L = D$, odnosno $L \subseteq D$ i $D \subseteq L$

(1) Neka je $x \in L$, tj. $x \in A \cap (B \cup C)$ akko

$x \in A$ i $x \in B \cup C$ akko $x \in A$ i $x \in (B \cap C) \cup (C \cap B)$

akko $x \in A$ i ($x \in B \cap C$ ili $x \in C \cap B$) akko

($x \in A$ i $x \in B \cap C$) ili ($x \in A$ i $x \in C \cap B$) akko

($x \in A$ i $x \in B$ i $x \notin C$) ili ($x \in A$ i $x \in C$ i $x \notin B$)

Γ Ako $x \notin C$, tada $x \notin A \cap C$

Ako $x \notin B$, tada $x \notin A \cap B$

Sledi

($x \in A \cap B$ i $x \notin A \cap C$) ili ($x \in A \cap C$ i $x \notin A \cap B$)

akko $x \in (A \cap B) \setminus (A \cap C)$ ili $x \in (A \cap C) \setminus (A \cap B)$

akko $x \in ((A \cap B) \setminus (A \cap C)) \cup ((A \cap C) \setminus (A \cap B))$ akko

$x \in \underbrace{(A \cap B) \Delta (A \cap C)}$

D Darbe, dokazali smo $L \subseteq D$

(2): $x \in D$ akko $x \in (A \cap B) \Delta (A \cap C)$ akko

$x \in (A \cap B) \setminus (A \cap C)$ ili $x \in (A \cap C) \setminus (A \cap B)$ akko

($x \in A \cap B$ i $x \notin A \cap C$) ili ($x \in A \cap C$ i $x \notin A \cap B$) akko

($x \in A \cap B$ i $x \in (A \cap C)^c$) ili ($x \in A \cap C$ i $x \in (A \cap B)^c$) akko

($x \in A \cap B$; $x \in A^c \cup C^c$) ili ($x \in A \cap C$ i $x \in A^c \cup B^c$)

akko ($x \in A \cap B$ i ($x \in A^c$ ili $x \in C^c$)) ili ($x \in A \cap C$ i ($x \in A^c$ ili $x \in B^c$))

akko ($(x \in A \cap B$ i $x \in A^c)$ ili ($x \in A \cap B$ i $x \in C^c$)) ili

($(x \in A \cap C$ i $x \in A^c)$ ili ($x \in A \cap C$ i $x \in B^c$)) akko

(($x \in A$ i $x \in B$ i $x \in A^c$) ili ($x \in A$ i $x \in B$ i $x \in C^c$)) ili

(($x \in A$ i $x \in C$ i $x \in A^c$) ili ($x \in A$ i $x \in C$ i $x \in B^c$))

akko ($x \notin \emptyset$ ili ($x \in A$ i $x \in D$ i $x \notin C$)) ili

($x \notin \emptyset$ ili ($x \in A$ i $x \in C$ i $x \notin B$))

akko ($x \in A$ i $x \in B \setminus C$) ili ($x \in A$ i $x \in C \setminus B$)

akko $x \in A$ i ($x \in B \cap C$ ili $x \in C \cap B$)

akko $x \in A$ i $x \in (B \cap C) \cup (C \cap B)$

akko $x \in A$ i $x \in B \Delta C$ akko $x \in \underbrace{A \cap (B \Delta C)}$

L

Dokazali smo da je $D \subseteq L$

2. Dokazati da je $A \cap (B \cup C) = (A \cap B) \cup C$ ako $C \subseteq A$.

\Rightarrow : Pretpostavimo da je $A \cap (B \cup C) = (A \cap B) \cup C$.

Pretpostavimo suprotno, tj. da nije $C \subseteq A$, tj. da postoji neko $y \in C$ i $y \notin A$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ y \in (A \cap B) \cup C & & y \notin A \cap (B \cup C) \end{array} \quad \begin{array}{l} \text{Dakle,} \\ C \subseteq A \end{array}$$

\Leftarrow Pretpostavimo $C \subseteq A$

$$\underbrace{A \cap (B \cup C)}_L = (A \cap B) \cup \underbrace{(A \cap C)}_C = \underbrace{(A \cap B)}_D \cup C$$

Dekartov proizvod skupova A i B je

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

Stan (kombinatorni princip proizvoda):

Ako je $|A|=m$, a $|B|=n$, tada je $|A \times B|=mn$

Partitivni skup skupa A je $P(A) = \{B \mid B \subseteq A\}$

Stan: Ako $|A|=n$, tada $|P(A)| = 2^n$

dokaz: Ako je B neki podskup skupa A , tada za svako $a \in A$ imamo tačno 2 mogućnosti

($a \in B$, ili $a \notin B$). Stoga, za $B \subseteq A$ imamo

$$\underbrace{2 \cdot 2 \cdots 2}_{n \text{ puta}} = 2^n \text{ mogućnosti.}$$

3. Naći $P(S)$ ukoliko je

a) $S = \{\emptyset\}$

b) $S = \{\{\emptyset\}\}$

c) $S = \{\emptyset, \{\emptyset\}\}$

Napomena:

$$\emptyset \subseteq S$$

$$S \subseteq S$$

a) $|S|=1 \Rightarrow |P(S)| = 2^1 = 2$

$$P(S) = \{\emptyset, \{\emptyset\}\}$$

b) $|S|=1 \Rightarrow |P(S)| = 2^1 = 2$

$$P(S) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$$

c) $|S|=2 \Rightarrow |P(S)| = 2^2 = 4$

$$P(S) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$$

4. Dokazati da važi:

- a) $P(A \cap B) = P(A) \cap P(B)$
- b) $P(A) \cup P(B) \subseteq P(A \cup B)$

Γ Zasto u b) ne važi obratna inkluzija u opštem slučaju! Uzimimo $a \in A \setminus B$ i $b \in B \setminus A$
Posmatrajmo $\{a, b\} \subseteq A \cup B \Leftrightarrow \{a, b\} \in P(A \cup B)$

$$\begin{array}{ll} \{a, b\} \notin A & \{a, b\} \notin B \\ \{a, b\} \notin P(A) & \{a, b\} \notin P(B) \\ \Rightarrow \{a, b\} \notin P(A) \cup P(B) \end{array}$$

$$\begin{array}{ccc} a) & x \in P(A \cap B) & x \in A \cap B \\ & x \subseteq A \text{ i } x \subseteq B & x \subseteq A \text{ i } x \subseteq B \\ & \text{akko} & \text{akko} \\ & x \in P(A) \cap P(B) & x \in P(A) \cap P(B) \end{array}$$

Dakle, $P(A \cap B) = P(A) \cap P(B)$.

$$b) x \in P(A) \cup P(B) \text{ sledi } x \in P(A) \text{ ili } x \in P(B)$$

slidi: $x \subseteq A$ ili $x \subseteq B$

$$\begin{array}{cc} \text{in} & \text{in} \\ A \cup B & A \cup B \end{array}$$

slidi: $x \subseteq A \cup B$ ili $x \subseteq A \cup B$

slidi: $x \in P(A \cup B)$ ili $x \in P(A \cup B)$

slidi: $x \in P(A \cup B)$

5. Dokazati da za sve skupove A, B, C, D važi
 $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

Γ Zasto u opštem slučaju ne važi obratna inkluzija?

Uzimimo $a \in A \setminus C$ i $d \in D \setminus B$

$$a \in A \cup C \quad d \in B \cup D$$

$$\Rightarrow (a, d) \in (A \cup C) \times (B \cup D)$$

$$(a, d) \notin A \times B \text{ jer } d \notin B$$

$$(a, d) \notin C \times D \text{ jer } a \notin C$$

$$(x, y) \in (A \times B) \cup (C \times D) \text{ akko } (x, y) \in A \times B \text{ ili } (x, y) \in C \times D$$

akko $(x \in A \text{ i } y \in B)$ ili $(x \in C \text{ i } y \in D)$

$$\begin{array}{cc} \text{in} & \text{in} \\ A \cup C & B \cup D \end{array}$$

$$\begin{array}{cc} \text{in} & \text{in} \\ A \cup C & B \cup D \end{array}$$

- slidi $(x \in A \cup C \text{ i } y \in B \cup D)$ ili $(x \in A \cup C \text{ i } y \in B \cup D)$
- akko $(x \in A \cup C \text{ i } y \in B \cup D)$
- akko $(x, y) \in (A \cup C) \times (B \cup D)$

6. Neka su A i B neprazni skupovi i
 $(A \times B) \cup (B \times A) = C \times D$. Dokazati da je $A=B=C=D$

Priuđemo da je $C \neq \emptyset$ i $D \neq \emptyset$

Kako su A i B neprazni $\Rightarrow (A \times B) \cup (B \times A) \neq \emptyset$, pa ne smeju biti prazni ni C ni D (jer je $\emptyset \times D = C \times \emptyset = \emptyset$)

Po prethodnom zadatku:

$$(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D) \text{ imamo:}$$

$$C \times D = (A \times B) \cup (B \times A) \subseteq (A \cup B) \times (A \cup B)$$

Kako su svi skupovi neprazni $\Rightarrow C \subseteq A \cup B$ i $D \subseteq A \cup B$

Sa druge strane, $A \times B \subseteq C \times D$

Šet, kako su A i B neprazni $\Rightarrow A \stackrel{1}{\subseteq} C$ i $B \stackrel{2}{\subseteq} D$

Analogno $B \times A \subseteq C \times D \Rightarrow A \stackrel{3}{\subseteq} D$ i $B \stackrel{4}{\subseteq} C$

Iz 1. i 4. zaključujemo $A \cup B \subseteq C$

Iz 2. i 3. zaključujemo $A \cup B \subseteq D$

Dakle, $C = A \cup B$ i $D = A \cup B$ (*)

Iz polazne jednakosti je $(A \times B) \cup (B \times A) = C \times D = (A \cup B) \times (A \cup B)$

Dovoljno je još dokazati da je $A \subseteq B$ i $B \subseteq A$

Potpustavimo suprotno, tj. da $A \not\subseteq B$, tj. da postoji $a \in A$ takvo da $a \notin B$.

Ako posmatravamo $(a, a) \in (A \cup B) \times (A \cup B)$

Međutim, $(a, a) \notin A \times B$ jer $a \notin B \Rightarrow (a, a) \notin$

Isto tako, $(a, a) \notin B \times A$ jer $a \notin B \Rightarrow (a, a) \notin (A \times B) \cup (B \times A)$

To je \$\not\models\$ sa (*)

Stoga, $A \subseteq B$. Potpuno analogno ispisati za $B \subseteq A$

$\Rightarrow B \subseteq A$, te je $A=B$, pa je $C = A \cup B = A \cup A = A$
 $D = A \cup B = A \cup A = A$

Dakle $A=B=C=D$.

Relacije

Def: Binarna relacija između elemenata skupa A i skupa B je bilo koji podskup $R \subseteq A \times B$. Za $A = B$, kažemo da je to relacija na skupu A .

Primer: $A = B = \mathbb{R}$ i posmatramo relaciju \leq
 $2 \leq 3$ Možemo pisati $(2, 3) \in \leq$
infiksna $(3, 2) \notin \leq$
notacija

Osnovne relacije $R \subseteq A^2 = A \times A$:

- \leq na \mathbb{R} 1) refleksivnost: aRa za svako $a \in A$ ($(a, a) \in R$ za svako a)
- \perp na skupu pravih 2) antirefleksivnost: $a \not\perp a$ ni za jedno $a \in A$ (ne postoji a koje je u relaciji R sa samim sobom)
- || na skupu pravih 3) simetričnost: Ako je aRb , tada je bRa za sve $a, b \in A$
- $<$ na \mathbb{R} 4) asimetričnost: Ako je aRb , tada nije bRa za sve $a, b \in A$
- \equiv na $P(S)$ 5) antisimetričnost: Ako je $aRb \wedge bRa$, tada je $a = b$
- $=$ na \mathbb{R} 6) tranzitivnost: Ako je $aRb \wedge bRc$, tada je aRc .

Def: Relacija $R \subseteq A \times A$ je relacija ekvivalencije (RST relacija) ako je refleksivna, simetrična i tranzitivna ($=, ||, \equiv, \sim, \equiv_{\text{modu}}, \dots$)

Relacija $R \subseteq A \times A$ je relacija poretku ako je refleksivna, antisimetrična i tranzitivna (\leq, \leq, \dots). Poredak je totalan (linearan) ako su svaka dva elementa upoređiva (za svaka dva $a, b \in A$ je aRb ili bRa).

Relacija $R \subseteq A \times A$ je relacija strogeg poretku ako je antirefleksivna i tranzitivna ($<$)

Kako je svaka relacija skup, sve skupove su podržane.

Def: Ako je $R \subseteq A \times B$ relacija, tada je uvoj inverzna relacija $R^{-1} \subseteq B \times A$ zadata sa: $(a, b) \in R$ akko $(b, a) \in R^{-1}$
 $a R b$ akko $b R^{-1} a$

Def: Ako je $R \subseteq A \times B$, a $S \subseteq B \times C$, definisemo relaciju $S \circ R \subseteq A \times C$ sa:
 $(a, c) \in S \circ R$ akko postoji $b \in B$ taj $(a, b) \in R$, a $(b, c) \in S$

Osobine operacija:

1) $T \circ (S \circ R) = (T \circ S) \circ R$

2) kompozicija relacija nije komutativna (jer ako je $S \circ R$ definisano, tada $R \circ S$ ni ne mora biti definisano)

3) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

4) $R \subseteq S \Rightarrow R^{-1} \subseteq S^{-1}$

dokaz: Znamo da ako $(a, b) \in R$, tada $(a, b) \in S$

Uzimimo proizvoljan element $x \in R^{-1}$ $x = (b, a) \in R^{-1}$ akko

$(a, b) \in R$, tada $(a, b) \in S$ akko $(b, a) \in S^{-1}$
 $x \in S^{-1}$

Zaključili smo $R^{-1} \subseteq S^{-1}$

5) $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$

dokaz: $(b, a) \in (R \cup S)^{-1}$ akko

$(a, b) \in R \cup S$ akko $(a, b) \in R$ ili $(a, b) \in S$

akko $(b, a) \in R^{-1}$ ili $(b, a) \in S^{-1}$ akko

$(b, a) \in R^{-1} \cup S^{-1}$

Stoga, $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$

c) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$

dokazati za dvači

7) $(R^{-1})^{-1} = R$

8) $R \circ (S_1 \cup S_2) = (R \circ S_1) \cup (R \circ S_2)$

9) $R \circ (S_1 \cap S_2) \subseteq (R \circ S_1) \cap (R \circ S_2)$

1. Ako su ρ_1 i ρ_2 relacije ekvivalencije, tada je $\rho_1 \cap \rho_2$ isto ekvivalencija. Da li isto to važi i za $\rho_1 \cup \rho_2$?

1) refleksivnost: $(a,a) \in \rho_1 \cap \rho_2$ za svako $a \in A$?

ρ_1 i ρ_2 jesu refleksivne, pa $(a,a) \in \rho_1 \wedge (a,a) \in \rho_2 \Rightarrow (a,a) \in \rho_1 \cap \rho_2$

2) simetričnost: $(a,b) \in \rho_1 \cap \rho_2$ povećaj $(b,a) \in \rho_1 \cap \rho_2$?

Neka je $(a,b) \in \rho_1 \cap \rho_2$. Tada $(a,b) \in \rho_1 \wedge (a,b) \in \rho_2$.

Kako su ρ_1 i ρ_2 simetrične, to je $(b,a) \in \rho_1 \wedge (b,a) \in \rho_2$, pa je $(b,a) \in \rho_1 \cap \rho_2$

3) tranzitivnost: Ako $(a,b) \in \rho_1 \cap \rho_2 \wedge (b,c) \in \rho_1 \cap \rho_2$, tada: $(a,c) \in \rho_1 \cap \rho_2$?

Ako $(a,b) \in \rho_1 \cap \rho_2 \wedge (b,c) \in \rho_1 \cap \rho_2 \Rightarrow$

$(a,b) \in \rho_1$ i $(a,b) \in \rho_2$ i $(b,c) \in \rho_1$; $(b,c) \in \rho_2$ \Rightarrow

Γ ρ_1 i ρ_2 su tranzitivne $\mid (a,c) \in \rho_1 \wedge (a,c) \in \rho_2 \Rightarrow (a,c) \in \rho_1 \cap \rho_2$

Pogledajmo stvar se desava za $\rho_1 \cup \rho_2$?

simetričnost i refleksivnost prolaze, ali tranzitivnost ne:

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

$\rho_1 = \{(a,a), (b,b), (c,c), (a,b), (b,a)\}$ jeste ekvivalencija

$\rho_2 = \{(a,a), (b,b), (c,c), (b,c), (c,b)\}$ jeste ekvivalencija

$\rho_1 \cup \rho_2$ sadrži (a,b) i (b,c)

Stoga, iz tranzitivnosti bismo imali da $(a,c) \in \rho_1 \cup \rho_2$, što nije tačno $\Rightarrow \rho_1 \cup \rho_2$ nije tranzitivna, pa nije ni ekvivalencija

2. Dopuniti $\rho = \{(1,1), (1,2), (2,3), (4,4), (4,5)\}$ do minimalne relacije ekvivalencije na skupu $\{1,2,3,4,5\}$.

	1	2	3	4	5
1	T	T	T		
2	T	T	T		
3	T	T	T		
4			T	T	
5			T	T	

Kako je svaka relacija ekvivalencije refleksivna, to moramo dodati $(2,2)$, $(3,3)$ i $(5,5)$

Da bismo ispostovili simetričnost, dodajemo $(2,1)$, $(3,2)$ i $(5,4)$

Kako imamo $(1,2)$ i $(2,3)$, to zbog tranzitivnosti moramo uzeti i $(1,3)$ Zbog simetričnosti, uzimamo i $(3,1)$

3. Neka su \mathcal{S} i Γ relacije poretka na skupu A. Dokazati da je $\mathcal{S} \cap \Gamma^{-1}$ relacija poretka.

(R): Pitamo se da li $(a,a) \in \mathcal{S} \cap \Gamma^{-1}$ za svako $a \in A$.

$(a,a) \in \mathcal{S}$ i $(a,a) \in \Gamma$ jer su \mathcal{S} i Γ refleksivne

$$\Rightarrow (a,a) \in \mathcal{S} \text{ i } (a,a) \in \Gamma^{-1} \Rightarrow (a,a) \in \mathcal{S} \cap \Gamma^{-1}. \quad \checkmark$$

(ANS): Ako $(a,b) \in \mathcal{S} \cap \Gamma^{-1}$ i $(b,a) \in \mathcal{S} \cap \Gamma^{-1}$, tada $a=b$
 $(a,b) \in \mathcal{S}$ i $(b,a) \in \mathcal{S}$. Kako je \mathcal{S} antisimetrična
 $\Rightarrow a=b \quad \checkmark$

(T): $(a,b) \in \mathcal{S} \cap \Gamma^{-1}$ i $(b,c) \in \mathcal{S} \cap \Gamma^{-1}$, tada $(a,c) \in \mathcal{S} \cap \Gamma^{-1}$

$$\underbrace{(a,b) \in \mathcal{S}}_{\mathcal{S} \text{ i } \Gamma \text{ su transitive jer su poredk}} \text{ i } \underbrace{(b,c) \in \mathcal{S}}_{\mathcal{S} \text{ i } \Gamma} \text{ i } \underbrace{(c,b) \in \Gamma}_{\Gamma}$$

\mathcal{S} i Γ su transitive jer su poredk)

$$\Rightarrow (a,c) \in \mathcal{S} \text{ i } (c,a) \in \Gamma \Rightarrow (a,c) \in \mathcal{S} \text{ i } (a,c) \in \Gamma^{-1} \Rightarrow (a,c) \in \mathcal{S} \cap \Gamma^{-1}.$$

4. Da li je relacija $|$ relacija poretka na skupu \mathbb{N} ?
A na skupu \mathbb{Z} ?

(R): $n|n \quad \checkmark$

(T): $m|n$ i $n|p \Rightarrow m|p \quad \checkmark$

(ANS): $m|n$ i $n|m \Rightarrow m=n \quad \checkmark$

} jeste poredek
(ali nije totalan)
 $2+3$ i 3×2

(R) $\checkmark \quad \Gamma$ obo? u teoriji brojeva:

\mathbb{Z} : (T) \checkmark $a|b$ akko postoji c t.dj $b=a\cdot c$

(ANS): Ne važi jer:

$$1|-1 \text{ i } -1|1, \text{ a nije } 1=-1.$$

nije poredek

1. Neka je na \mathbb{Z} data relacija ρ sa ašb
akko $3|a+2b$. Dokazati da je ρ ekvivalencija
i naci klase.

$$\begin{array}{ll} a \rho b \text{ akko } 3 | a+2b & \text{akko } 3 | a-b+3b \\ & \text{akko } 3 | a-b \\ a+3b=b & \text{akko } a \equiv b \pmod{3} \end{array}$$

Stoga, kako je kongruencija po modulu 3 ekvivalencija
to će biti i ρ .

Klase:

$$\{0, 3, -3, \dots\} = 3\mathbb{Z}$$

$$\{1, 4, -2, -5, \dots\} = 3\mathbb{Z} + 1$$

$$\{2, 5, -1, -4, \dots\} = 3\mathbb{Z} + 2$$

2. Neka je na skupu \mathbb{R} data relacija ρ sa ašb akko
 $a^3 + a^2b = ab^2 + b^3$. Dokazati da je ρ ekvivalencija:
naci klase.

$$(R): a^3 + a^2b \stackrel{?}{=} ab^2 + b^3$$

$$2a^3 = 2a^2 \quad \checkmark$$

$$(S): a \rho b \stackrel{?}{\Rightarrow} b \rho a$$

$$a^3 + a^2b = ab^2 + b^3 \Rightarrow b^3 + b^2a = ba^2 + a^3$$

$$\Rightarrow b \rho a \quad \checkmark$$

$$(T): a \rho b ; b \rho c \Rightarrow a \rho c$$

$$a^3 + a^2b = ab^2 + b^3$$

$$a^2(a+b) = b^2(a+b)$$

$$a^2(a+b) - b^2(a+b) = 0$$

$$(a^2 - b^2)(a+b) = 0$$

$$(a-b)(a+b)(a+b) = 0$$

$$(a-b)(a+b)^2 = 0$$

$$\begin{array}{c} \swarrow \quad \downarrow \\ a=b \quad a=-b \end{array}$$

Stoga, kako je $a \rho b$ i $b \rho c$, imamo 4 mogućnosti:

$$\begin{array}{l} 1^{\circ} a=b \text{ i } b=c \Rightarrow a=c \\ 2^{\circ} a=b ; b=-c \Rightarrow a=-c \\ 3^{\circ} a=-b ; b=c \Rightarrow a=-c \\ 4^{\circ} a=-b ; b=-c \Rightarrow a=c \end{array} \quad \left. \begin{array}{l} \Rightarrow a \rho c \\ \checkmark \end{array} \right.$$

$$\text{Klase: } \begin{cases} x, -x \\ 0 \end{cases} \quad \text{za } x \neq 0$$

Def: Neka je \leq relacija poretku na skupu A ,
 $B \subseteq A$ i $a \in A$.

- 1) a je gornje ograničenje skupa B ukoliko je $b \leq a$ za svako $b \in B$.
- 2) a je donje ograničenje skupa B ukoliko je $a \leq b$ za svako $b \in B$.
- 3) a je najveći element skupa B ukoliko $a \in B$ i a je gornje ograničenje za B .
- 4) a je najmanji element skupa B ukoliko $a \in B$ i a je donje ograničenje za B .
- 5) a je maksimalni element skupa B ukoliko ne postoji veći element skupa B .
- 6) a je minimalni element skupa B ukoliko ne postoji manji element skupa B .
- 7) a je supremum skupa B ako je a najmanje gornje ograničenje.
- 8) a je infimum skupa B ako je a najveće donje ograničenje.

Primer: 1) $A = \mathbb{R}$, \leq , $B = [0, 1)$

gornje ograničenje: 2
donje ograničenje: 0
najveći element: ne postoji
najmanji element: 0
maksimalni element: ne postoji
minimalni element: 0
supremum: 1
infimum: 0

$\overbrace{0,99\dots} = 1$
ne dozvoljavamo
zapise u
kojima ima
počev od rekog
mesta samo g
 $\boxed{1x=0,99\dots}$
 $\boxed{10x=9,99\dots}$
 $10x-x=9$
 $9x=9$
 $\boxed{x=1}$

2) Neka je X skup takav da je
 $|X|=n \geq 2$ i posmatramo na skupu
 $\mathcal{P}(X)$ relaciju \subseteq . $B = \mathcal{P}(X) \setminus \{\emptyset, X\}$
gornje ograničenje: X
donje ograničenje: \emptyset
najveći element: ne postoji
najmanji element: ne postoji
maksimalni element: svi oni sa $n-1$ elemenata
kojih ima $\binom{n}{n-1} = n \geq 2$
minimalni element: svi jednočlani kojih ima
 $n \geq 2$
supremum: X
infimum: \emptyset

Primeru: $X = \{a, b\}$ $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
 $B = \mathcal{P}(X) \setminus \{\emptyset, X\} = \{\{a\}, \{b\}\}$

istovremeno i
maksimalni i minimalni

3. Ako su $\mathfrak{S} \in \Gamma$ relacija poretka na skupu $A \times B$ redom dokazati da je i $\mathfrak{S} \times \Gamma$ zadata na $A \times B$ sa:
 $(a,b) \mathfrak{S} \times \Gamma (c,d)$ akko $a \mathfrak{S} c$ i $b \mathfrak{S} d$ takođe relacija poretka.

(2): $a \mathfrak{S} a$ za sve a i $b \mathfrak{S} b$ za sve b jer su $\mathfrak{S} \in \Gamma$ refleksivne
 $\Rightarrow (a,b) \mathfrak{S} \times \Gamma (a,b)$ ✓

(ANS): $(a,b) \mathfrak{S} \times \Gamma (c,d)$ i $(c,d) \mathfrak{S} \times \Gamma (a,b) \stackrel{?}{\Rightarrow} (a,b) = (c,d)$

$$\begin{array}{ccc} \underline{a \mathfrak{S} c} & \text{i} & \underline{c \mathfrak{S} a} \\ \backslash & & \diagup \\ a=c & \times & b=d \\ & & \diagdown \\ & & \Rightarrow (a,b) = (c,d) \end{array}$$

jer su $\mathfrak{S} \in \Gamma$ antisimetrične. ✓

(T): $(a,b) \mathfrak{S} \times \Gamma (c,d)$ i $(c,d) \mathfrak{S} \times \Gamma (u,v) \stackrel{?}{\Rightarrow} (a,b) \mathfrak{S} \times \Gamma (u,v)$

$$\begin{array}{ccc} \underline{a \mathfrak{S} c} & \text{i} & \underline{c \mathfrak{S} u} \\ \backslash & & \diagup \\ a \mathfrak{S} u & \times & b \mathfrak{S} v \\ & & \diagdown \\ & & \Rightarrow (a,b) \mathfrak{S} \times \Gamma (u,v) \end{array}$$

zbog tranzitivnosti $\mathfrak{S} \in \Gamma$ ✓

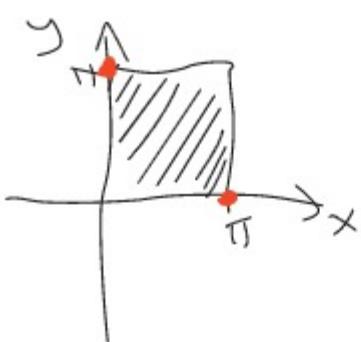
Napomena: Ako su $\mathfrak{S} \in \Gamma$ relacija totalnog poretka, $\mathfrak{S} \times \Gamma$ ne mora biti totalan poredak.

4. Neka je na $[0,\pi] \times [0,\pi]$ data relacija \mathfrak{S} sa
 $(x,y) \mathfrak{S} (z,w)$ akko $\cos x \leq \cos z$ i $y \leq w$. Dokazati da
 \mathfrak{S} poredak i odrediti minimalni, maksimalni,
"najveći", najmanji element skupa $[0,\pi] \times [0,\pi]$ i
kruga sa centrom u $(\frac{\pi}{2}, \frac{\pi}{2})$ poluprečnika $\frac{\pi}{2}$.

✓ Stav: Najveći, najmanji, supremum i infimum su jedinstveni ukoliko postoje.

Ako imamo jedinstveni minimalni, tada je on i najmanji.

Ako imamo jedinstveni maksimalni, tada je on i najveći. miro



$(x,y) \in P(z,w)$ ako $\cos x \leq \cos z$ i $y \leq w$.
 Kako je \cos opadajuća funkcija na $[0, \pi]$,
 to je uslov $\cos x \leq \cos z$ ekvivalentan
 uslovu $x \geq z$.

Dakle, $(x,y) \in P(z,w)$ ako $x \geq z$ i $y \leq w$

Stoga, relacija P je zapravo $\geq \times \leq$ (notacija iz prethodnog zadatka), pa kako su \geq i \leq relacije porekla, to je i P relacija porekla po prethodnom zadatku.

Najmanji element skupa $[0, \pi] \times [0, \pi]$ (x,y) treba da:

$(x,y) \in P(z,w)$ za sve $(z,w) \in [0, \pi] \times [0, \pi]$

$x \geq z$ za sve $z \in [0, \pi] \Rightarrow x = \pi$

$y \leq w$ za sve $w \in [0, \pi] \Rightarrow y = 0$

Dakle, $(\pi, 0)$ je najmanji element. To je i jedini minimalni element.

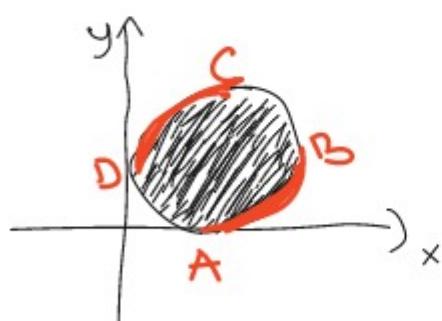
Najveći element skupa $[0, \pi] \times [0, \pi]$ (z,w) treba da:

$(x,y) \in P(z,w)$ za sve $(x,y) \in [0, \pi] \times [0, \pi]$.

$x \geq z$ za sve $x \in [0, \pi] \Rightarrow z = 0$

$y \geq w$ za sve $y \in [0, \pi] \Rightarrow w = \pi$

Dakle, $(0, \pi)$ je najveći element, pa i jedini maksimalni.



Minimalni elementi (x,y) treba da zadovoljavaju da su sto više desno i sto više gore \Rightarrow minimalni se nalaze na luku \widehat{AB} .

Maksimalni elementi (z,w) treba da zadovoljavaju da su sto više levo i sto više gore \Rightarrow maksimalni se nalaze na luku \widehat{CD} .

Kako minimalni i maksimalni elementi nisu jedinstveni \Rightarrow nemaju najveće i najmanje.

5. Neka je na skupu $A = \{1, 2, 3, 4, 5, 6, 7, 8\} \times [\frac{\pi}{2}, \pi]$ data relacija ρ sa $(m, x) \rho (n, y)$ akko $m|n$ i $\sin x \leq \sin y$. Nači najveći, najmanji, minimalni i maksimalni.

Kako je \sin opadajuća na $[\frac{\pi}{2}, \pi]$, to je uslov $\sin x \leq \sin y$ je ekivalentan uslovu $x \geq y$.

Dakle, $(m, x) \rho (n, y)$ akko $m|n$ i $x \geq y$.

Najmanji: (m, x) treba da ispunjava
 $m|n$ za svako $n \in \{1, \dots, 8\} \Rightarrow m=1$
 $x \geq y$ za svako $y \in [\frac{\pi}{2}, \pi] \Rightarrow x=\pi$

Dakle, $(1, \pi)$ je najmanji, pa i jedini minimalni.

Najveći: (n, y) treba da ispunjava
 $m|n$ za sve $m \in \{1, \dots, 8\}$ ne postoji
 $x \geq y$ za svako $x \in [\frac{\pi}{2}, \pi] \Rightarrow y=\frac{\pi}{2}$

Dakle, najveći ne postoji, pa tražimo maksimalne (n, y) . Dobili smo već da je $y=\frac{\pi}{2}$.

n ne smije deliti ništvo osim sebe $\Rightarrow n \in \{5, 6, 7, 8\}$

Stoga, maksimalni su: $(5, \frac{\pi}{2}), (6, \frac{\pi}{2}), (7, \frac{\pi}{2}), (8, \frac{\pi}{2})$.

Karakteristické funkce

Neka je X ambijentalni skup; i $A \subseteq X$.

Definisemo $\chi_A : X \rightarrow \{0, 1\}$

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases} \quad \text{indikator-Funktion}$$

Primer: $X = \{1, 2\}$ $A = \{1\}$

$$\chi_A(1) = 1 \quad \chi_A(2) = 0$$

Osobine;

$$1) \quad \chi_\phi(x) = 0 \quad \text{za wszystkie } x \in X$$

$$2) \chi_x(x) = 1 \quad \text{za} \quad x \in X$$

$$3) \chi_{A \cap B}(x) = \chi_A(x) \chi_B(x)$$

$$5) \chi_{A^c}(x) = 1 - \chi_A(x)$$

$$5) \chi_{A \setminus B}(x) = \chi_{A \cap B^c}(x) = \chi_A(x) \cdot \chi_{B^c}(x) = \chi_A(x) \cdot (1 - \chi_B(x)) =$$

$$\chi_A(x) - \chi_A(x) \chi_B(x)$$

$$6) \chi_{A \cup B}(x) = \chi_{(A^c \cap B^c)^c} = 1 - \chi_{A^c \cap B^c} = 1 - \chi_{A^c} \chi_{B^c} = \\ 1 - (1 - \chi_A(x))(1 - \chi_B(x)) = 1 - (1 - \chi_A(x) - \chi_B(x) + \chi_A(x)\chi_B(x)) \\ = \chi_A(x) + \chi_B(x) - \chi_A(x)\chi_B(x)$$

$$7) \chi_{A \Delta B}(x) = \chi_{(A \setminus B) \cup (B \setminus A)}(x) = \chi_{A \setminus B}(x) + \chi_{B \setminus A}(x) - \chi_{A \setminus B}(x)\chi_{B \setminus A}(x)$$

$$= (\chi_A(x) - \chi_A(x)\chi_B(x))(\chi_B(x) - \chi_B(x)\chi_A(x)) =$$

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

$$= \chi_A(x) \lambda_B(x) + \underset{\chi_A(x)}{\underset{||}{\chi_A^2(x)}} \underset{\chi_B(x)}{\underset{||}{\lambda_B(x)}} + \underset{\chi_B(x)}{\underset{||}{\lambda_A(x)}} \underset{\chi_A^2(x)}{\underset{||}{\chi_B^2(x)}} - \underset{\chi_A(x)}{\underset{||}{\chi_A^2(x)}} \underset{\chi_B(x)}{\underset{||}{\chi_B^2(x)}}$$

$$= \chi_A(x) - \lambda_A(x) \chi_B(x) + \lambda_B(x) - \lambda_A(x) \chi_B(x)$$

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

$$= \chi_A(x) + \chi_B(x) - 2 \chi_A(x) \chi_B(x)$$

Pozmatrajući skup $\mathbb{Z}_2 = \{0, 1\}$ i operacije + i · definisane na sledeći način:

$$0+0=0$$

$$0 \cdot 0 = 0$$

$$0+1=1$$

$$0 \cdot 1 = 0$$

$$1+0=1$$

$$1 \cdot 0 = 0$$

$$1+1=0$$

$$1 \cdot 1 = 1$$

U \mathbb{Z}_2 sabiranje je isto što i oduzimanje

$$a-b = a+(-b) = a+b$$

$-b$ je element suprotan elementu b , pa je u \mathbb{Z}_2

$$-b = b$$

U \mathbb{Z}_2 važi da je $a^2=a$ za svako a .

Stoga, dobijamo pojednostavljene formule:

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

$$\chi_A^c = 1 + \chi_A$$

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

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

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

Nadalje koristimo ove formule

Stan: Ako su A i B neki podskupovi antisimetričnog skupa X , tada je $A=B$ ukoliko $\chi_A = \chi_B$.

$$1. \quad \underbrace{A \cap (B \cup C)}_{L} = \underbrace{(A \cap B) \cup (A \cap C)}_{D}$$

$$\chi_L = \chi_{A \cap (B \cup C)} = \chi_A \chi_{B \cup C} = \chi_A \cdot (\chi_B + \chi_C + \chi_B \chi_C) =$$

$$\underline{\chi_A \chi_B + \chi_A \chi_C + \chi_A \chi_B \chi_C}$$

$$\chi_D = \chi_{(A \cap B) \cup (A \cap C)} = \chi_{A \cap B} + \chi_{A \cap C} + \chi_{A \cap B} \cdot \chi_{A \cap C} =$$

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

$$\chi_A \chi_B + \chi_A \chi_C + \chi_A^2 \chi_B \chi_C =$$

$$\underline{\chi_A \chi_B + \chi_A \chi_C + \chi_A \chi_B \chi_C}$$

Stoga, kako je $\chi_L = \chi_D$, pa po prethodnom stazu imamo

$$2. \quad \underbrace{A \setminus (B \setminus C)}_{L} = \underbrace{(A \setminus B) \cup (A \cap C)}_{D}$$

$$\chi_L: \quad \chi_{A \setminus (B \setminus C)} = \chi_A + \chi_A \chi_{B \setminus C} = \chi_A + \chi_A (\chi_B + \chi_B \chi_C)$$

$$\underline{= \chi_A + \chi_A \chi_B + \chi_A \chi_B \chi_C}$$

$$\chi_D: \quad \chi_{(A \setminus B) \cup (A \cap C)} = \chi_{A \setminus B} + \chi_{A \cap C} + \chi_{A \setminus B} \chi_{A \cap C} =$$

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

$$\chi_A + \chi_A \chi_B + \chi_A \chi_C + \chi_A^2 \chi_C + \chi_A^2 \chi_B \chi_C =$$

$$\chi_A + \chi_A \chi_B + \chi_A \chi_C + \chi_A \chi_C + \chi_A \chi_B \chi_C$$

$$\underline{= 0 \in \mathbb{Z}_2}$$

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

Dakle, $L=D$.

3. Naci potreban i dovoljan uslov da vazi
 $(A \setminus B) \setminus C = A \setminus (B \setminus C)$

$$(A \setminus B) \setminus C = A \setminus (B \setminus C) \text{ aako } \chi_{(A \setminus B) \setminus C} = \chi_{A \setminus (B \setminus C)} \text{ aako}$$

$$\begin{aligned} \chi_{A \setminus B} + \chi_{A \setminus B} \cdot \chi_C &= \chi_A + \chi_A \chi_{B \setminus C} \quad \text{ako} \\ \chi_A + \chi_A \chi_B + (\chi_A + \chi_A \chi_B) \chi_C &= \chi_A + \chi_A (\chi_B + \chi_B \chi_C) \end{aligned}$$

$$\text{ako } \cancel{\chi_A + \chi_A \chi_B + \chi_A \chi_C + \chi_A \cancel{\chi_B} \chi_C} = \cancel{\chi_A + \chi_A \chi_B + \cancel{\chi_A} \cancel{\chi_B} \chi_C}$$

$$\text{ako } \chi_A \chi_C = 0$$

$$\text{ako } \chi_{A \cap C} = 0$$

$$\text{ako } \chi_{A \cap C} = \chi_\emptyset \quad \text{ako } \boxed{A \cap C = \emptyset}$$

4. Ako je A proizvoljan skup, a X i Y skupovi za koje vazi $A \cap X = A \cap Y$; $A \cup X = A \cup Y$. Dokazati da je $X = Y$.

$$A \cap X = A \cap Y, \text{ pa je } \chi_{A \cap X} = \chi_{A \cap Y}, \text{ tj. } \chi_A \cdot \chi_X = \chi_A \cdot \chi_Y \rightarrow$$

$$A \cup X = A \cup Y, \text{ pa je } \chi_{A \cup X} = \chi_{A \cup Y}, \text{ tj. } \cancel{\chi_A + \chi_X + \chi_A \chi_X} = \cancel{\chi_A + \chi_Y + \chi_A \chi_Y}$$

$$\text{Ostaje } \chi_X = \chi_Y, \text{ tj. } X = Y$$

5. Dokazati da je $A = B \cup C$ aako $\underbrace{A \Delta B}_{L} = \underbrace{C \setminus B}_{D}$.

\Rightarrow : Prepostavljamo da je $A = B \cup C$ aako $\chi_A = \chi_{B \cup C}$
 $\text{aako } \chi_A = \chi_B + \chi_C + \chi_B \chi_C$

$$\chi_L = \chi_{A \Delta B} = \chi_A + \chi_B = \cancel{\chi_B + \chi_C + \chi_B \chi_C} + \cancel{\chi_B} = \underline{\chi_C + \chi_C \chi_B}$$

$$\chi_D = \chi_{C \setminus B} = \underline{\chi_C + \chi_C \chi_B}$$

$$\text{Imamo } \chi_L = \chi_D, \text{ tj. } L = D.$$

\Leftarrow : Prepostavimo da je $A \Delta B = C \setminus B$

$$\text{Stoga, } \chi_{A \Delta B} = \chi_{C \setminus B}$$

$$\chi_A + \chi_B = \chi_C + \chi_C \chi_B / + \chi_B$$

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

$$\chi_A = \chi_B + \chi_C + \chi_B \chi_C = \chi_{B \cup C}$$

$$\text{Stoga, } A = B \cup C.$$

6. Neka su A, B i C proizvoljni skupovi,

$$L = A \cap (B \cup C)$$

$$D = (A \cap B) \Delta (A \cap C),$$

a) Dokazati da je $L = D$ akko $A \cap B \cap C = \emptyset$

b) Ispitati da li u opštem slučaju važi barem jedna od inkluzija $L \subseteq D$ ili $D \subseteq L$

a) $L = D$ akko $\chi_L = \chi_D$ akko $\chi_{A \cap (B \cup C)} = \chi_{(A \cap B) \Delta (A \cap C)}$

$$\text{akko } \chi_A \cdot \chi_{B \cup C} = \chi_{A \cap B} + \chi_{A \cap C} \text{ akko}$$

$$\chi_A (\chi_B + \chi_C + \chi_B \chi_C) = \chi_A \chi_B + \chi_A \chi_C \text{ akko}$$

$$\cancel{\chi_A} \cancel{\chi_B} + \cancel{\chi_A} \cancel{\chi_C} + \cancel{\chi_A} \chi_B \chi_C = \cancel{\chi_A} \chi_B + \cancel{\chi_A} \chi_C \text{ akko}$$

$$\cancel{\chi_A} \chi_B \chi_C = 0 \text{ akko}$$

$$\chi_{A \cap B \cap C} = 0 \text{ akko}$$

$$\chi_{A \cap B \cap C} = \chi_\emptyset \text{ akko } A \cap B \cap C = \emptyset$$

b) I način: $A \subseteq B$ akko $A \cap B = A$

Da bismo videli da li je $L \subseteq D$ ili je $D \subseteq L$, posmatraćemo $L \cap D$, tj. računajemo $\chi_{L \cap D}$.

Dobiće se da je $\chi_{L \cap D} = \chi_D$, tj. $L \cap D = D$. Stoga $D \subseteq L$.

II način: $A \subseteq B$ akko $\chi_A \leq \chi_B$

$$\chi_L = \chi_A \chi_B + \chi_A \chi_C + \chi_A \chi_B \chi_C \quad \Rightarrow \quad \chi_L = \chi_D + \chi_A \chi_B \chi_C$$

$$\chi_L = \chi_A \chi_B + \chi_A \chi_C$$

$$\cancel{\chi_D} \quad \cancel{\chi_A} \leq \chi_L ?$$

Jedan slučaj je kritičan:

$$\chi_D = 1 \text{ i } \chi_A \chi_B \chi_C = 1$$

Dakle, to $x \in A$, $x \in B$, $x \in C$
 $\chi_A(x) = 1$, $\chi_B(x) = 1$, $\chi_C(x) = 1$

$$\chi_L(x) = 1 + 1 + 1 = 1$$

$$\chi_D(x) = 1 + 1 = 0$$

Kritičan
slučaj se
nikada ne
desava.

Dakle, $\chi_D \leq \chi_L$, pa je zaista $D \subseteq L$.

7. Dokazati da je $\underline{\chi_{A \cap (B \Delta C)}} = B$ ako $A \cap C = \emptyset$ i $B \subseteq A$.

\Leftarrow : $A \cap C = \emptyset$ i $B \subseteq A$

$$\underline{\chi_L} = \chi_{A \cap (B \Delta C)} = \chi_A \cdot (\chi_B + \chi_C) = \chi_A \chi_B + \chi_A \chi_C = \\ \underline{\chi_{A \cap B}} + \underline{\chi_{A \cap C}} = \underline{\chi_B} + 0 = \underline{\chi_B}$$

Stoga, $L = B$

\Rightarrow : $A \cap (B \Delta C) = B$ ako $\chi_A \chi_B + \chi_A \chi_C = \chi_B$

1^o $B \subseteq A$? Pretpostavimo suprotno, tj. da postoji $x \in B$ i $x \notin A$

$x \notin A \cap (B \Delta C)$ jer je $A \cap (B \Delta C) \subseteq A$
 $x \in B''$ Dakle, $B \subseteq A$.

2^o $A \cap C = \emptyset$? Pretpostavimo suprotno, tj. da postoji $x \in A \cap C$,

$$x \in A \quad ; \quad x \in C \\ \chi_A(x) = 1 \quad ; \quad \chi_C(x) = 1$$

ubacujemo
ovo $x \in A \cap C$

Imao možnosti:

$$1^o \quad x \in B \\ \chi_B(x) = 1$$

$$1 \cdot 1 + 1 \cdot 1 = 1$$

$$1 + 1 = 1$$

$$0 = 1$$

$$2^o \quad x \notin B \\ \chi_B(x) = 0$$

$$1 \cdot 0 + 1 \cdot 1 = 0$$

$$0 + 1 = 0$$

$$1 = 0$$

Pretpostavka je pogrešna, tj. $A \cap C = \emptyset$.

Funkcije

Def: Funkcija f iz skupa A u skup B ($f: A \rightarrow B$) je svaka relacija $f \subseteq A \times B$ takva da za svako $a \in A$ postoji tačno jedno $b \in B$ za koje je $(a, b) \in f$ (pišemo $b = f(a)$)

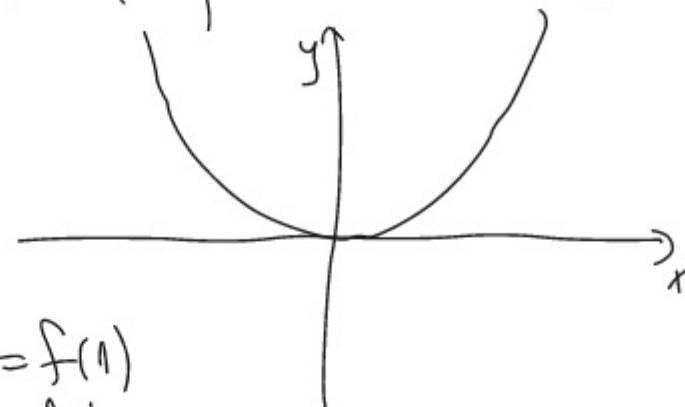
Def: Funkcija $f: A \rightarrow B$ je $"^{-1}"$ ukoliko za svaka dva $a_1, a_2 \in A$ važi: Ako je $a_1 \neq a_2$, tada je $f(a_1) \neq f(a_2)$ (ekvivalentno, ako je $f(a_1) = f(a_2)$, tada je $a_1 = a_2$)

Def: Funkcija $f: A \rightarrow B$ je $"\text{na}"$ ukoliko za svako $b \in B$ postoji $a \in A$ takvo da je $b = f(a)$

Def: Funkcija je bijekcija akko je $"^{-1}"$ i $"\text{na}"$.

Def: Za dve funkcije f i g kazemo da su jednake akko su im isti domeni, kodomeni i pravila dodelje.

Primer: 1) $f: \mathbb{R} \rightarrow \mathbb{R}$
 $f(x) = x^2$



f nije $"^{-1}"$ jer $f(-1) = 1 = f(1)$
 f nije $"\text{na}"$ jer -1 nije slika
nijednog argumenta

2) $f: \mathbb{R} \rightarrow [0, +\infty)$
 $f(x) = x^2$

f nije $"^{-1}"$
 f jeste $"\text{na}"$

3) $f: [0, +\infty) \rightarrow \mathbb{R}$
 $f(x) = x^2$

f jeste $"^{-1}"$
 f nije $"\text{na}"$

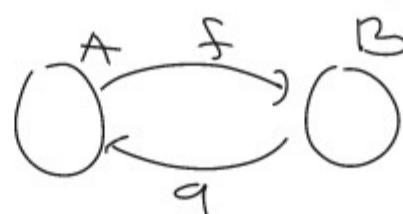
4) $f: [0, +\infty) \rightarrow [0, +\infty)$
 $f(x) = x^2$

f je bijekcija

Stav: Kompozicija funkcija je funkcija
 $f: A \rightarrow B$ $g: B \rightarrow C$ $g \circ f : A \rightarrow C$

Def: $\text{Id}_A: A \rightarrow A$ je funkcija koja svako $a \in A$ fiksira
 $\text{Id}_A(a) = a$

Stav: Ako je $f: A \rightarrow B$, tada postoji funkcija $g: B \rightarrow A$ za koju je $f \circ g = \text{Id}_B$ i $g \circ f = \text{Id}_A$ akko je f bijekcija.
 Funkciju g nazivamo inverznom funkcijom funkcije f (pišemo f^{-1})



Primer: $f: [0, +\infty) \rightarrow [0, +\infty)$
 $f(x) = x^2$
 $f^{-1}(x) = \sqrt{x}$

$$f(f^{-1}(x)) = f(\sqrt{x}) = (\sqrt{x})^2 = x$$

$$f^{-1}(f(x)) = f^{-1}(x^2) = \sqrt{x^2} = x$$

1. a) $f: A \rightarrow B$ je f^{-1} akko postoji $g: B \rightarrow A$ takva da je $g \circ f = \text{Id}_A$ (levi inverz)

b) $f: A \rightarrow B$ je "na" akko postoji $g: B \rightarrow A$ takva da je $f \circ g = \text{Id}_B$ (desni inverz)

a) $\Rightarrow: f: A \rightarrow B$ f^{-1}
 Trutjivo $g: B \rightarrow A$ taj $g \circ f = \text{Id}_A$

Ako je $b \in B$ proizvoljno, imamo mogućnosti:

- $b = f(a)$ za neko $a \in A$ jedinstveno
 Definišemo $g(b) = a$.
- b nije slika ni jednog elementa $a \in A$
 Definišemo $g(b)$ proizvoljno.

$g \circ f: A \rightarrow A$ $\text{Id}_A: A \rightarrow A$

$$g \circ f(a) = g(\underbrace{f(a)}_{\in B}) = a = \text{Id}_A(a)$$

\Leftarrow : Ako postoji $g: B \rightarrow A$ t.dj. $g \circ f = \text{Id}_A$ pretpostavimo da f nije $1-1$, što znači da postoji $a_1 \neq a_2$ tako da $f(a_1) = f(a_2)$

$$\begin{aligned} &| \\ &\swarrow \quad \searrow \\ g(f(a_1)) &= g(f(a_2)) \\ \text{Id}_A(a_1) &= \text{Id}_A(a_2) \\ a_1 &= a_2 \end{aligned}$$

Dakle, f jeste $1-1$.

b) \Rightarrow : $f: A \rightarrow B$ „na“ i konstruišemo $g: B \rightarrow A$ t.dj. $f \circ g = \text{Id}_B$
 g konstruišemo element po element
 $b \in B$, kako je f „na“, to postoji bar jedno $a \in A$
 $f(a) = b$. Uzimimo $g(b) = a$
 $f(g(b)) = f(a) = b = \text{Id}_B(b)$
 \uparrow
 za neko a
 koje se saf slika u b

\Leftarrow : Neka postoji $g: B \rightarrow A$ t.dj. $f \circ g = \text{Id}_B$
 Ako f nije „na“, tada postoji $b \in B$ koje nije slika nijednog a pri f . Tada b nije slika nijednog elementa ni pri $f \circ g$ jer ako bi bio slika nekog x

$$\begin{aligned} f(g(x)) &= b \\ \underbrace{f(g(x))}_{\in A} &= b \quad \text{pa je } b \text{ slika od } g(x) \text{ pri } f \end{aligned}$$

Dakle, f jeste „na“.

Id_B je bijekcija,
 pa je i „na“

2. $f: A \rightarrow B$ i $g: B \rightarrow C$

- a) $f \circ g$ $1-1 \Rightarrow g \circ f$ $1-1$
- b) $f \circ g$ „na“ $\Rightarrow g \circ f$ „na“
- c) $f \circ g$ bijekcije $\Rightarrow g \circ f$ bijekcija
- d) $g \circ f$ $1-1 \Rightarrow f$ $1-1$
- e) $g \circ f$ „na“ $\Rightarrow g$ „na“
- f) $g \circ f$ bijekcija $\Rightarrow f$ $1-1$ i g „na“

dokaz: a) Neka je $f: A \rightarrow B$ i $g: B \rightarrow C$.
 Tada je $g(f(a_1)) = g(f(a_2))$
 Ali g je $"1-1"$ pa je $f(a_1) = f(a_2)$
 Ali f je $"1-1"$ pa je $a_1 = a_2$

b) $\textcircled{1} \xrightarrow{f} \textcircled{2} \xrightarrow{g} \textcircled{3}$

$c \in C$ proizvoljno. Kako je g "na", to postoji $b \in B$ takav da je $g(b) = c$
 Za b postoji $a \in A$ takav da je $f(a) = b$
 Sada je $c = g(b) = g(f(a)) = gof(a)$
 Dakle, gof je "na"

c) direktna posledica od a) i b)

d) Pretpostavimo da f nije $"1-1"$, tj. da postoji $a_1 \neq a_2$ t.d. $f(a_1) = f(a_2)$
 $g(f(a_1)) = g(f(a_2))$
 $gof(a_1) = gof(a_2)$

Ali gof je $"1-1"$ pa je $a_1 = a_2$

e) gof je "na"
 $c \in C$ proizvoljno, postoji $a \in A$ t.d. $gof(a) = c$
 $\tilde{c} \in B$ $g(f(a)) = c$
 Dakle, $f(a) \in B$ pri g ide u c . Stoga, g je "na"

f) Direktna posledica d) i e)

3. Dokazati da je $f: X \rightarrow Y$ $"1-1"$ akko za bilo koji skup Z i bilo koje dve funkcije $g_1, g_2: Z \rightarrow X$ iz uslova da je $f \circ g_1 = f \circ g_2$ sledi $g_1 = g_2$.

\Rightarrow : I nacin:

Neka je $f: X \rightarrow Y$ $"1-1"$ i Z proizvoljni skup sa $g_1, g_2: Z \rightarrow X$ za koje je $f \circ g_1 = f \circ g_2$.

f je $"1-1"$ pa po zadatku 1. imamo $g: Y \rightarrow X$

takvu da je $g \circ f = \text{Id}_X$

$$\begin{aligned}
 f \circ g_1 &= f \circ g_2 \\
 g_1 \circ (f \circ g_1) &= g_1 \circ (f \circ g_2) \\
 (g_1 \circ f) \circ g_1 &= (g_1 \circ f) \circ g_2 \\
 \text{Id}_X \circ g_1 &= \text{Id}_X \circ g_2 \\
 g_1 &= g_2
 \end{aligned}$$

II nacin:

Pretpostavimo da $g_1 \neq g_2$, tj. postoji $z \in Z$ za koje je $g_1(z) \neq g_2(z)$

Tada $f(g_1(z)) \neq f(g_2(z))$. Jen je f "1-1"

Jen smo pp da $f \circ g_1 = f \circ g_2$

\Leftarrow : Pretpostavimo da f nije "1-1", tj. postoji

$x_1, x_2 \in X$ $x_1 \neq x_2$ i $f(x_1) = f(x_2)$

Uzmimo $Z = \{x\}$ $g_1, g_2: Z \rightarrow X$

$g_1(*) = x_1$ $g_2(*) = x_2$

$f \circ g_1: Z \rightarrow Y$ $f(g_1(*)) = f(x_1) = f(x_2) = f(g_2(*))$

$f \circ g_1 = f \circ g_2$

Ali $g_1 \neq g_2$



Stoga, f jeste "1-1"

Direktna i inverzna slika skupa

Def: Ako je $f: X \rightarrow Y$ i $A \subseteq X$, tada pod direktnom slikom skupa A pri f podrazumevamo

$$f[A] = \{f(a) \mid a \in A\} \subseteq Y$$

Def: Ako je $f: X \rightarrow Y$ i $B \subseteq Y$, tada pod inverznom slikom skupa B pri f podrazumevamo

$$f^{-1}[B] = \{x \in X \mid f(x) \in B\} \subseteq X$$

Primer: 1) $f: \{1, 2, 3\} \rightarrow \{a, b\}$

$$f(1) = f(2) = a$$

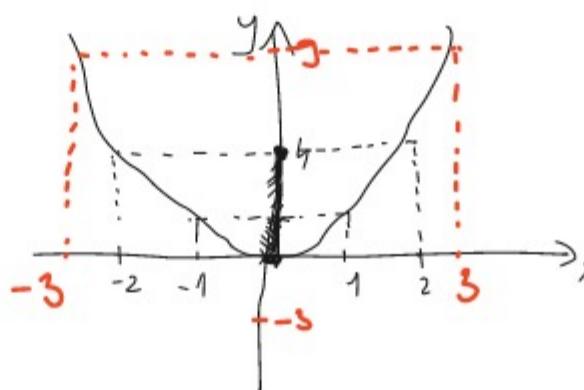
$$f(3) = b$$

$$f[\{1, 2\}] = \{a\}$$

$$f^{-1}[\{b\}] = \{3\}$$

$$f^{-1}[\{a\}] = \{1, 2\}$$

2) $f: \mathbb{R} \rightarrow \mathbb{R}$
 $f(x) = x^2$



a) $f[-2, 1] = [0, 4]$

b) $f^{-1}[-3, 9] = [-3, 3]$

c) $f[f^{-1}[-4, 4]] = f[-2, 2] = [0, 4] \Rightarrow f[f^{-1}[B]] \neq B$

d) $f^{-1}[f[1, 2]] = f^{-1}[1, 4] = [-2, 1] \cup [1, 2] \Rightarrow f^{-1}[f[A]] \neq A$

Osobine: Neka je $f: X \rightarrow Y$

- 1) $A \subseteq f^{-1}[f[A]]$ (jednakost važi ako je f "1-1") domaći
- 2) $f[f^{-1}[B]] \subseteq B$ (jednakost važi ako je f "na") domaći
- 3) $f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$ domaći
- 4) $f[A_1 \cap A_2] \subseteq f[A_1] \cap f[A_2]$ domaći
- 5) $f[A_1] \setminus f[A_2] \subseteq f[A_1 \setminus A_2]$
- 6) $f^{-1}[B_1 \cup B_2] = f^{-1}[B_1] \cup f^{-1}[B_2]$
- 7) $f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$
- 8) $f^{-1}[B_1 \setminus B_2] = f^{-1}[B_1] \setminus f^{-1}[B_2]$

1. Dokazati da je $f: X \rightarrow Y$ "1-1" tako
za sve $A, B \subseteq X$ važi $f[A \Delta B] = f[A] \Delta f[B]$

$$\Rightarrow f: X \rightarrow Y \text{ "1-1"} \\ f[A \Delta B] = f[(A \setminus B) \cup (B \setminus A)] \stackrel{(*)}{=} f[A \setminus B] \cup f[B \setminus A] \\ \stackrel{(*)}{=} (f[A] \setminus f[B]) \cup (f[B] \setminus f[A]) = f[A] \Delta f[B]$$

Imao, da je $f[A] \setminus f[B] \subseteq f[A \setminus B]$ po osobini 5) \Rightarrow 2 u (*)
 $f[B] \setminus f[A] \subseteq f[B \setminus A]$ po osobini 5)

$$\subseteq u (*) \quad y \in f[A \setminus B] \Rightarrow y \in f[A] \setminus f[B]$$

postoji $a \in A \setminus B$ taj $y = f(a)$

$a \in A$ i $a \notin B$ i $f(a) = y$

$$y \in f[A]$$

$y \notin f[B]?$ f je "1-1" pa ne može

postojati element razlicit od a koji sa f ide u y . Dakle, $y \notin f[B]$

Stoga, $y \in f[A] \setminus f[B]$. Dakle $f[A \setminus B] \subseteq f[A] \setminus f[B]$
Analognos $f[B \setminus A] \subseteq f[B] \setminus f[A]$.

↪ Pretpostavimo suprotno da f nije x^{1-1} , tj.

postoje $x_1 \neq x_2$ tako da $f(x_1) = f(x_2) = y$

$$A = \{x_1\} \quad B = \{x_2\}$$

$$A \Delta B = \{x_1, x_2\}$$

$$f[A \Delta B] = f[\{x_1, x_2\}] = \{y\}$$

$$f[A] = f[\{x_1\}] = \{y\} \quad \Rightarrow \quad f[A] \Delta f[B] = \emptyset$$

$$f[B] = f[\{x_2\}] = \{y\}$$

} ovi nisu
jednaki

1. Neka je $f: X \rightarrow Y$, $A \subseteq X$, $B \subseteq Y$, dokazati da je
 $f[A \cap f^{-1}[B]] = f[A] \cap B$

Znamo $f[A_1 \cap A_2] \subseteq f[A_1] \cap f[A_2]$

Stoga je $f[A \cap f^{-1}[B]] \subseteq f[A] \cap f[f^{-1}[B]] \subseteq f[A] \cap B$

Znamo $f[f^{-1}[B]] \subseteq B$

Stoga, dokazali smo $L \subseteq D$

\Leftarrow : $y \in f[A] \cap B \Rightarrow y \in f[A]; y \in B \Rightarrow$

postoji $a \in A$ $y \in B \quad \downarrow \quad \Rightarrow f(a) \in B$

$$y = f(a)$$

$a \in f^{-1}[B]$

$$a \in A$$

$$\overline{a \in A \cap f^{-1}[B]}$$

$$y = f(a) \in f[A \cap f^{-1}[B]]$$

Po definiciji je $D \subseteq L$

Dakle, $L = D$.

2. Neka je $f: X \rightarrow Y$. Dokazati da je f "1-1" akko

$$f^{-1}[f[A] \setminus (f[A] \cap B)] = A \setminus f^{-1}[B] \quad A \subseteq X \quad B \subseteq Y$$

\Leftarrow pretpostavimo suprotno, da f nije "1-1"

Dakle, postoji $x_1 \neq x_2$ takvi da $f(x_1) = f(x_2) = y$

$$A = \{x_1\} \quad B = \emptyset$$

$$D = A \setminus f^{-1}[B] = \{x_1\} \setminus f^{-1}[\emptyset] = \{x_1\} \setminus \emptyset = \{x_1\}$$

$$f^{-1}[f[\{x_1\}]] \setminus (f[\{x_1\}] \cap \emptyset) =$$

$$L = f^{-1}[\{y\}] \setminus \emptyset = f^{-1}[\{y\}] \supseteq \{x_1, x_2\}$$

$$|D| = 1 \quad |L| \geq 2 \quad \Rightarrow D \neq L \quad \text{Stoga, } f \text{ jeste } "1-1"$$

\Rightarrow učka je f^{-1}
 $x \in f^{-1}[f[A] \setminus (f[A] \cap B)]$ akko
 $f(x) \in f[A] \setminus (f[A] \cap B)$ akko
 $f(x) \in f[A] \text{ i } f(x) \notin (f[A] \cap B)$ akko
 $f(x) \in f[A] \text{ i } f(x) \in (f[A] \cap B)^c$ akko
 $f(x) \in f[A] \text{ i } f(x) \in (f[A]^c \cup B^c)$
 akko $f(x) \in f[A] \cap (f[A]^c \cup B^c)$
 akko $f(x) \in (f[A] \cap f[A]^c) \cup (f[A] \cap B^c)$
 akko $f(x) \in f[A] \cap B^c$
 $f(x) \in f[A] \text{ i } f(x) \notin B$
 $f \text{ je } f^{-1} \text{ } x \in A \quad (\text{u opštem slučaju, može postojati } A \ni a \neq x \text{ tako da } f(a) = f(x))$
 $x \in A \text{ i } f(x) \notin B$ akko
 $x \in A \text{ i } x \notin f^{-1}[B]$
 $x \in A \setminus f^{-1}[B]$

Dakle, $L = D$.

3. Ako su $f, g: X \rightarrow Y$, dokazati da je $f = g$ akko je za svaki $A \subseteq X$ ispunjeno $A \subseteq f^{-1}[g[A]]$.

\Rightarrow : Ako je $f = g$ tada je $f^{-1}[g[A]] = f^{-1}[f[A]]$
 a znamo da je $A \subseteq f^{-1}[f[A]]$

\Leftarrow : prepostavimo suprotno, tj. da je $f \neq g$.

Dakle, postoji $x \in X$ tako da $f(x) \neq g(x)$

$$A = \{x\}$$

$$f^{-1}[g[A]] = f^{-1}[g[\{x\}]] = f^{-1}[\{g(x)\}]$$

Dakle je $\{x\} \subseteq f^{-1}[\{g(x)\}]$
 akko $x \in f^{-1}[\{g(x)\}]$
 akko $f(x) \in \{g(x)\}$
 akko $f(x) = g(x)$

$$\text{Ali } f(x) \neq g(x)$$

$\Rightarrow \{x\} \not\subseteq f^{-1}[g[\{x\}]]$
 $A \not\subseteq f^{-1}[g[\{x\}]]$

Stoga, $f = g$

4. Dokazati da je $f: X \rightarrow Y$ "na" ako za svake dve funkcije $g, h: Y \rightarrow Z$ iz $g \circ f = h \circ f$ sledi $g = h$

\Rightarrow Neka je $f: X \rightarrow Y$ "na", pa postoji desni invert funkcije f i neka je to funkcija \tilde{f}

$$g \circ f = h \circ f$$

$$(g \circ f) \circ \tilde{f} = (h \circ f) \circ \tilde{f}$$

$$\underbrace{g \circ (f \circ \tilde{f})}_{\text{Id}} = \underbrace{h \circ (f \circ \tilde{f})}_{\text{Id}}$$

$$g = h$$

\Leftarrow Pretpostavimo suprotno, da f nije "na", tj. da postoji $y \in Y$ takvo da y nije slika ni jednog elementa iz X po f .



$$\text{Uzimimo } Z = \{a, b, c\}$$

Sve elemente iz $Y \setminus \{y\}$ pri g ih slikaju u a

$$\text{Da li je } g \circ f = h \circ f?$$

$$g(f(x)) = a$$

$$\underset{f[X]}{\underset{\uparrow}{\subseteq}} Y \setminus \{y\}$$

$$y \xrightarrow{g} b$$

$$y \xrightarrow{h} c$$

$$g + h$$

$$h(f(x)) = a$$

$$g \circ h, h \circ f: X \rightarrow Z$$

$$g \circ h = h \circ f = l_a$$



Funkcija koja sve slike u element a (konstantna funkcija)

Dakle, f mora biti "na".

Matematička indukcija

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

Princip matematičke indukcije:

Ako je $I(n)$ svojstvo nekog prirodnog broja, da bismo dokazati da to svojstvo važi za svaki prirodan broj, dokazujemo:

1° baza indukcije: $I(1)$

2° induktivska hipoteza: pretpostavimo da važi $I(n)$

3° induktivski korak: dokazemo da važi $I(n+1)$

osnovni princip matematičke indukcije

$$1. \text{ Dokazati } 1+2+\dots+n = \frac{n(n+1)}{2}$$

indukcija 1. Dokazati $1+2+\dots+n = \frac{n(n+1)}{2}$

1^o baza: dokazujemo za $n=1$:

$L=1$

$$D = \frac{1 \cdot 2}{2} = 1$$

2^o hipoteza: Neka važi $1+2+\dots+n = \frac{n(n+1)}{2}$

3^o korak: $1+2+\dots+n+(n+1) \stackrel{?}{=} \frac{(n+1)(n+2)}{2}$

$$\begin{aligned} 1+2+\dots+n+(n+1) &= \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} \\ &\stackrel{\text{hipoteza}}{=} \frac{(n+1)(n+2)}{2} \quad \checkmark \end{aligned}$$

2. $1^2+2^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$

1^o baza: $1^2 \stackrel{?}{=} \frac{1 \cdot 2 \cdot 3}{6}$

$$1 = 1 \quad \checkmark$$

2^o hipoteza: $1^2+2^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$

3^o korak: $\underbrace{1^2+2^2+\dots+n^2}_{n(n+1)(2n+1)} + (n+1)^2 \stackrel{?}{=} \frac{(n+1)(n+2)(2n+3)}{6}$

$$\begin{aligned} L &= \frac{n(n+1)(2n+1)}{6} + \frac{(n+1)^2}{6} = \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \frac{(n+1)(2n^2+n+6n+6)}{6} = \frac{(n+1)(2n^2+7n+6)}{6} \\ &\stackrel{\text{?}}{=} \frac{(n+1)(n+2)(2n+3)}{6} \quad \checkmark \end{aligned}$$

Neka je $k \in \mathbb{N}$

1^o baza indukcije: $I(1), I(2), \dots, I(k)$

2^o hipoteza: pretpostavimo da tvrdjenje važi
za $I(n), I(n+1), \dots, I(n+k-1)$
 $\underbrace{k \text{ uzastopnih}}$

3^o korak: dokazemo da $I(n+k)$

3. Fibonacijsku niz F_n $n \in \mathbb{N}$ je definisani na sledeći
nacin: $F_1 = F_2 = 1$
 $F_{n+2} = F_{n+1} + F_n$

indukcija
sa korakom
k

1, 1, 2, 3, 5, 8, -

Dokazati da je

$$F_n = \frac{\sqrt{5}}{5} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{\sqrt{5}}{5} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

baza: $1 = F_1 = \frac{\sqrt{5}}{5} \left(\frac{1+\sqrt{5}}{2} \right)^1 - \frac{\sqrt{5}}{5} \left(\frac{1-\sqrt{5}}{2} \right)^1$

$$= \frac{\sqrt{5}}{5} \left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2} \right) = \frac{\sqrt{5}}{5} \left(\frac{1+\sqrt{5}-1+\sqrt{5}}{2} \right)$$

$$= \frac{\sqrt{5}}{5} \cdot \frac{2\sqrt{5}}{2} = \frac{2 \cdot 5}{5 \cdot 2} = 1$$

Analogno se proveni za F_2 :

$$1 = F_2 = \frac{\sqrt{5}}{5} \cdot \left(\frac{1+\sqrt{5}}{2} \right)^2 - \frac{\sqrt{5}}{5} \left(\frac{1-\sqrt{5}}{2} \right)^2 = \dots = 1$$

hipoteza: pretpostavljamo da je $F_n = \frac{\sqrt{5}}{5} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{\sqrt{5}}{5} \left(\frac{1-\sqrt{5}}{2} \right)^n$

$$F_{n+1} = \frac{\sqrt{5}}{5} \left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \frac{\sqrt{5}}{5} \left(\frac{1-\sqrt{5}}{2} \right)^{n+1}$$

Korak:

$$\begin{aligned} F_{n+2} &= F_{n+1} + F_n = \frac{\sqrt{5}}{5} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} + \left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right] \\ &= \frac{\sqrt{5}}{5} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n \left(\frac{1+\sqrt{5}}{2} + 1 \right) - \left(\frac{1-\sqrt{5}}{2} \right)^n \left(\frac{1-\sqrt{5}}{2} + 1 \right) \right] \\ &= \frac{\sqrt{5}}{5} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n \left(\frac{3+\sqrt{5}}{2} \right) - \left(\frac{1-\sqrt{5}}{2} \right)^n \left(\frac{3-\sqrt{5}}{2} \right) \right] \end{aligned}$$

$$\frac{3+\sqrt{5}}{2} = \left(\frac{1+\sqrt{5}}{2} \right)^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2}$$

$$\frac{3-\sqrt{5}}{2} = \left(\frac{1-\sqrt{5}}{2} \right)^2 = \frac{1-2\sqrt{5}+5}{4} = \frac{6-2\sqrt{5}}{4} = \frac{3-\sqrt{5}}{2}$$

$$\hookrightarrow = \frac{\sqrt{5}}{5} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n \left(\frac{1+\sqrt{5}}{2} \right)^2 - \left(\frac{1-\sqrt{5}}{2} \right)^n \left(\frac{1-\sqrt{5}}{2} \right)^2 \right]$$

$$= \frac{\sqrt{5}}{5} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+2} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+2} \right] =$$

$$\frac{\sqrt{5}}{5} \left(\frac{1+\sqrt{5}}{2} \right)^{n+2} - \frac{\sqrt{5}}{5} \left(\frac{1-\sqrt{5}}{2} \right)^{n+2}$$

4. Niz prirodnih brojeva a_n nenužno definisan je sa:

$$a_0 = 2$$

$$a_1 = 3$$

$$a_{n+1} = 3a_n - 2a_{n-1}$$

Dokazati da je $a_n = 2^n + 1$

baza: $2 = a_0 \stackrel{?}{=} 2^0 + 1 = 1 + 1 = 2 \quad \checkmark$

$$3 = a_1 = 2^1 + 1 = 2 + 1 = 3 \quad \checkmark$$

li poteca: Neka je $a_{n-1} = 2^{n-1} + 1$

$$a_n = 2^n + 1$$

$$a_{n+1} = 3 \cdot (2^n + 1) - 2 \cdot (2^{n-1} + 1) = 3 \cdot 2^n + 3 - 2 \cdot 2^{n-1} - 2 =$$

$$3 \cdot 2^n + 3 - 2^n - 2 =$$

$$2 \cdot 2^n + 1 = 2^{n+1} + 1 \quad \checkmark$$

$$1. \quad g | n \cdot 4^{n+1} - (n+1) \cdot 4^n + 1 \quad \text{za svako } n \in \mathbb{N}$$

1^o baza: $n=1$

$$1 \cdot 4^2 - 2 \cdot 4^1 + 1 = 16 - 8 + 1 = 9 \quad \checkmark$$

$g | 9$

2^o hipoteza: neka

$$g | n \cdot 4^{n+1} - (n+1) \cdot 4^n + 1 \quad \text{za neko } n \in \mathbb{N}$$

3^o korak: za $n+1$

$$\begin{aligned} & (n+1) \cdot 4^{n+2} - (n+2) \cdot 4^{n+1} + 1 = \\ & n \cdot 4^{n+2} + 4^{n+2} - (n+1) \cdot 4^{n+1} - 4^{n+1} + 1 \\ & = \underbrace{4n \cdot 4^{n+1}}_{\substack{\text{deljivo sa } g \\ \text{po hipotezi}}} + 4^{n+2} - \underbrace{4(n+1) \cdot 4^n}_{\substack{\text{deljivo sa } g \\ \text{po hipotezi}}} - 4^{n+1} + \underbrace{4 - 3}_{\substack{\text{deljivo sa } g}} \end{aligned}$$

$\underbrace{n \cdot 4^{n+1} - (n+1) \cdot 4^n + 1}_{\substack{\text{deljivo sa } g \\ \text{po hipotezi}}}$

u maloj indukciji je dokazano
Dovoljno je još dokazati
da je $4^{n+2} - 4^{n+1} - 3$
deljiv sa g

to dokazujuemo indukcijom:

1^o baza: $n=1$

$$4^3 - 4^2 - 3 = 64 - 16 - 3 = 45 \quad \text{sto je deljivo sa } g$$

2^o hipoteza: neka $g | 4^{n+2} - 4^{n+1} - 3$

3^o korak: dokazujuemo za $n+1$:

$$\begin{aligned} & 4^{n+3} - 4^{n+2} - 3 = \\ & 4 \cdot 4^{n+2} - 4 \cdot 4^{n+1} - 4 \cdot 3 + 9 \\ & = \underbrace{4 \cdot (4^{n+2} - 4^{n+1} - 3)}_{\substack{\text{deljivo sa } g \\ \text{po hipotezi}}} + 9 \quad \Rightarrow \quad \text{deljivo sa } g \\ & \qquad \qquad \qquad \uparrow \\ & \qquad \qquad \qquad \text{deljivo sa } g \end{aligned}$$

2. Niz an je zadat sa:

$$a_0 = 0$$

$$a_1 = 1$$

$$a_2 = 4$$

$$a_{n+3} = 3a_{n+2} - 3a_{n+1} + a_n$$

Dokazati da je $a_n = n^2$.

Konstimo indukciju sa korakom 3.

1^o baza: $a_0 = 0^2$

$$a_1 = 1^2$$

$$a_2 = 2^2$$



2^o hipoteza: pretpostavimo da je

$$a_n = n^2$$

$$a_{n+1} = (n+1)^2$$

$$a_{n+2} = (n+2)^2$$

3^o korak:

$$\begin{aligned} a_{n+3} &= 3a_{n+2} - 3a_{n+1} + a_n = 3(n+2)^2 - 3(n+1)^2 + n^2 = \\ &= 3(n^2 + 4n + 4) - 3(n^2 + 2n + 1) + n^2 = \\ &= 3n^2 + 12n + 12 - 3n^2 - 6n - 3 + n^2 = n^2 + 6n + 9 = \\ &= (n+3)^2 \end{aligned}$$

Ponekad uko tvrđenje treba dokazati počev od nekog prirodnog broja n. U tom slučaju, modifikujemo bazu indukcije.

3. $2^n > n^2$ za $n \geq 5$

1^o baza: $n=5$

$$2^5 > 5^2$$

$$32 > 25 \quad \checkmark$$

2^o hipoteza: pretpostavimo da je $2^n > n^2$

3^o korak: dokazujemo za $n+1$:

$$L = 2^{n+1} = 2 \cdot 2^n \stackrel{\substack{\uparrow \\ \text{hipoteza}}}{>} 2 \cdot n^2$$

\Rightarrow Dovoljno je još dokazati
 $2n^2 > n^2 + 2n + 1$ za $n \geq 5$

$$D = (n+1)^2 = n^2 + 2n + 1$$

$$\Leftrightarrow n^2 - 2n - 1 > 0$$

$$\Leftrightarrow n^2 > 2n + 1 \quad \text{za } n \geq 5$$

sto opet dokazujemo
indukcijom

1^o baza: $n=5$

$$5^2 > 2 \cdot 5 + 1$$

$$25 > 11 \quad \checkmark$$

2^o hipoteza: neka je $n^2 > 2n+1$

3^o korak: dokazujemo $(n+1)^2 > 2(n+1)+1$

$$n^2 + 2n + 1 > 2n + 3$$

$$n^2 + 1 > 3$$

$$n^2 > 2 \text{ jer } n^2 \geq 25 > 2$$

sto jeste ispunjeno

4. Dokazati da je za svako $n \geq 2$

$$\frac{n}{2} < 1 + \underbrace{\frac{1}{2} + \dots + \frac{1}{2^n-1}}_{a_n} < n$$

1^o baza: $n=2$:

$$\frac{2}{2} < 1 + \frac{1}{2} + \dots + \frac{1}{2^2-1} < 2 ?$$

$$1 < 1 + \frac{1}{2} + \frac{1}{3} < 2 ?$$

$$1 < \frac{11}{6} < 2 ?$$

$$6 < 11 < 12 \quad \checkmark$$

2^o hipoteza: neka važi za n

3^o korak: za $n+1$

$$a_{n+1} = 1 + \frac{1}{2} + \dots + \frac{1}{2^{n+1}-1} = \underbrace{1 + \frac{1}{2} + \dots + \frac{1}{2^n-1}}_{a_n} + \underbrace{\frac{1}{2^n} + \dots + \frac{1}{2^{n+1}-1}}_{2^n \text{ sabiraka}}$$

$$a_{n+1} = a_n + \underbrace{\frac{1}{2^n} + \dots + \frac{1}{2^{n+1}-1}}_{S_n}$$

$$\frac{1}{2^n} > \frac{1}{2^{n+1}}$$

⋮

$$\frac{1}{2^{n+1}-1} > \frac{1}{2^{n+1}}$$

$$\Rightarrow S_n > \frac{1}{2^{n+1}} + \dots + \frac{1}{2^{n+1}}$$

$$= 2^n \cdot \frac{1}{2^{n+1}} = \frac{1}{2}$$

$$a_{n+1} = a_n + S_n > \frac{n}{2} + \frac{1}{2} = \frac{n+1}{2}$$

↑
po hipotezi

$$\left. \begin{array}{l} \frac{1}{2^n} \leq \frac{1}{2^n} \\ \frac{1}{2^{n+1}} < \frac{1}{2^n} \\ \vdots \\ \frac{1}{2^{n+1}-1} \leq \frac{1}{2^n} \end{array} \right\} \Rightarrow S_n < \underbrace{\frac{1}{2^n} + \dots + \frac{1}{2^n}}_{2^n \text{ sabiraka}} = 2^n \cdot \frac{1}{2^n} = 1$$

po hipotezi

Stoga, $a_{n+1} = a_n + S_n < n+1$

\uparrow
polihipotezi

Princip transfinитne indukcije (potpune):

Ako je $I(n)$ neko tvrdenje koje treba dokazati za svaki $n \in \mathbb{N}$, radiamo sledeće:

1º baza: proveravamo $I(1)$

2º hipoteza: pretpostavimo da važi za $I(1), \dots, I(n)$

3º korak: dokazemo $I(n+1)$

5. Neka je a_n niz zadat sa

$$a_0 = 1$$

$$a_n = a_{n-1} + a_{n-2} + \dots + a_1 + 2a_0 \quad \text{za } n \geq 1$$

Dokazati da je $a_n = 2^n$ za svako $n \in \mathbb{N}$.

Koristimo potpunu indukciju.

1º baza: $a_0 = 2^0$

$$a_0 = 1 \quad \checkmark$$

2º hipoteza: pretpostavimo da to važi za $a_0 = 2^0, a_1 = 2^1, \dots, a_{n-1} = 2^{n-1}$

3º korak: $a_n = a_{n-1} + \dots + a_1 + 2a_0 = 2^{n-1} + \dots + 2^1 + 2 \cdot 1 =$

$$\underbrace{2^{n-1} + \dots + 2^1}_{\text{geometrijska}} + 1 + 1 = 2^{n-1} + 1 = 2^n$$

suma

$$S = 2^{n-1} + \dots + 2^1 \quad / \cdot 2$$

$$2S = 2^n + \dots + 2^2 + 2$$

$$S = 2S - S = 2^n - 1$$

$$S = 2^n - 1$$

6. Bernoullijeva nejednakost:

za svako $x \geq -1$ važi

$$(1+x)^n \geq 1+nx \quad \text{za svako } n \in \mathbb{N}$$

1^o baza: $n=1$

$$(1+x)^1 \geq 1+1 \cdot x$$

$$1+x \geq 1+x \quad \checkmark$$

2^o hipoteza: $(1+x)^n \geq 1+nx$

3^o korak: za $n+1$:

$$\begin{aligned} \underbrace{(1+x)^{n+1}}_{\geq 0} &= \underbrace{(1+x)^n}_{\geq 0} \cdot \underbrace{(1+x)}_{\geq 0} \geq (1+nx)(1+x) = 1+x+nx+nx^2 \\ &= 1+(n+1)x + \underbrace{nx^2}_{\geq 0} \\ &\geq 1+(n+1)x \end{aligned}$$

7. Nad alfabetom $\{a, b, c\}$ data su pravila:

$$c \xrightarrow{(1)} ac$$

$$c \xrightarrow{(2)} b$$

a) Naći jedno izvođenje reči $aaab$ iz reči c

b) Dokazati da su reči izvodive iz reči c točas reči iz skupa $\{a^n c | n \geq 0\} \cup \{a^n b | n \geq 0\}$

a) $c \xrightarrow{(1)} ac \xrightarrow{(1)} aac \xrightarrow{(1)} aaac \xrightarrow{(2)} aaab$
Izvođenje dužine 4

b) (1) Dokazujemo da su sve reči

$$a^n c \quad n \geq 0$$

$$a^n b \quad n \geq 0$$

Izvodive iz reči c

(2) Dokazujemo da ništa osim ovih reči ne možemo dobiti

(1) Indukcijom po n :

1^o baza: $n=0$

$a^0 c = c$ izvodivo iz c izvođenjem dužine 0

$a^0 b = b$ izvodivo iz c izvođenjem dužine 1

2^o hipoteza: pretpostavimo da su reči $a^n c$ i $a^n b$ izvodive iz reči c

$$\underbrace{c \rightarrow \dots \rightarrow a^n c}_{T_1}$$

$$\underbrace{c \rightarrow \dots \rightarrow a^n b}_{T_2}$$

3^o korak: dokazujemo za $a^{n+1}c$ i $a^{n+1}b$

izvodive

$$c \xrightarrow{\text{---}} \underbrace{a^n c}_{T_1} \xrightarrow{(1)} a^n ac = a^{n+1} c \xrightarrow{(2)} a^{n+1} L$$

\uparrow
dobili smo
 $a^{n+1} c$

\uparrow
dobili smo
 $a^{n+1} L$

(2) Dokazujemo indukcijom po
dužini izvođenja

1^o baza: dužina = 0

$c = a^0 c$ što jeste u traženoj skupu

2^o hipoteza: pretpostavimo da kad god je izvođenje
dužine n dobijamo reč oblike

$a^k c$ ili $a^k b$ za neko $k \in \mathbb{N}$

3^o korak: posmatrajmo neko izvođenje dužine $n+1$:

$$c \xrightarrow{\text{---}} \underbrace{\dots}_{n \text{ koraka}} \xrightarrow{(*)} \dots$$

(*) po hipotezi
može biti samo
 $a^k c$ ili $a^k b$

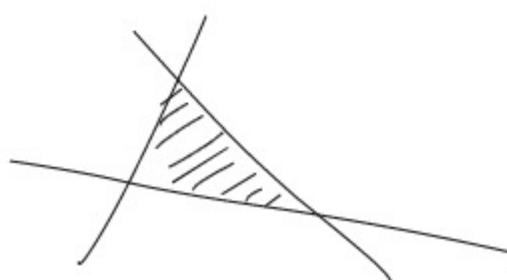
Ako je (*) $a^k c \xrightarrow{(1)} a^k ac = a^{k+1} c$
 $\quad \quad \quad \downarrow^{(2)}$ $a^k L$

Ako je (*) $a^k b$, ne možemo primeniti
nikakvu transformaciju, te on ni ne dolazi
u obzir jer smo krenuli od izvođenja dužine
 $n+1$.

8. Dokazati da n ≥ 3 pravih u ravi koje se nalaze
u opštem položaju (nikoje dve nisu paralelne i nikolic
tri se ne sekut u istoj tacki) deli ravnu na
oblasti od kojih je bar jedna oblast trougao.

1^o baza: $n=3$

trivijalno jeste
ispunjeno



2^o hipotezu; Neka ovo važi za neki $n \geq 3$

3^o korak: Proveravamo za $n+1$:

$n+1$ prava vidimo kao n pravih kojima dodajemo još jednu pravu.

Po hipotezi, n pravih daje oblast koja je trougao.

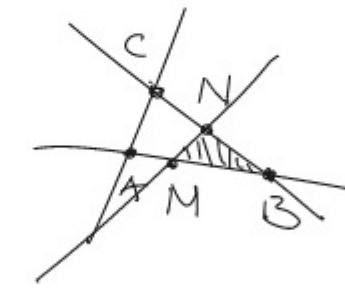
1^o dodata prava ne seče dati trougao, pa je on tu i dalje

2^o dodata prava seče dati trougao:

dodata prava ne prolazi kroz teme

datog trougla jer su prave u opštem položaju. Stoga, ona seče unutrasnjost ucke dve stranice trougla

Bez umanjenja opštosti (BVO) neka seče AB i BC u tačkama M, N . Tada je MBN trougao.



9. Dokazati da n pravih u ravni koje su u opštem položaju deli ravan na $\frac{n(n+1)}{2} + 1$ oblasti

1^o baza: $n=1$

$$\frac{1 \cdot 2}{2} + 1 = 1 + 1 = 2$$

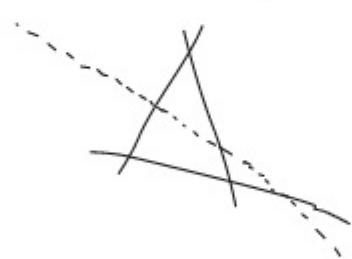


2^o hipoteza: neka važi za n

3^o korak: dokazujemo za $n+1$:

Izamo n pravih i dodajemo $n+1$.

Dodata prava seže sve ostale prave, pa ona ulazi u $n+1$ oblast i svaku od tih oblasti ona deli na dva dela, te smo dobili još $n+1$ novu oblast



Stoga, po hipotezi izamo sada

$$\frac{n(n+1)}{2} + 1 + n+1 = \frac{n(n+1) + 2(n+1)}{2} + 1$$

$$= \frac{(n+1)(n+2)}{2} + 1.$$

Teorija brojeva

- U \mathbb{Z} je dobro definisano deljenje sa ostatkom (euklidsko deljenje)

Primer: $25 : 3 = 8 \quad (1)$

$$25 = 3 \cdot 8 + 1$$

Stav: Ako je $a = b \cdot q + r$ (euklidski smo podelili broj a brojem b i dobili količnik q i ostatak r), tada je $\text{NzD}(a, b) = \text{NzD}(b, r)$

Stoga, za određivanje $\text{NzD}(a, b)$ možemo koristiti Euklidov algoritam

1. Naći $\text{NzD}(918, 252)$ i izraziti ga u obliku

\mathbb{Z} -linearne kombinacije brojeva 918 i 252

$$918 = 252 \cdot 3 + 162$$

$$\text{NzD}(918, 252) = \text{NzD}(252, 162)$$

$$252 = 162 \cdot 1 + 90$$

$$\text{NzD}(252, 162) = \text{NzD}(162, 90)$$

$$162 = 90 \cdot 1 + 72$$

$$\text{NzD}(162, 90) = \text{NzD}(90, 72)$$

$$90 = 72 \cdot 1 + \underline{18}$$

$$\text{NzD}(90, 72) = \text{NzD}(72, 18) = 18$$

$$72 = 18 \cdot 4 + 0 \Rightarrow 18 | 72$$

$$\Rightarrow \text{NzD}(918, 252) = 18$$

$$18 | 18$$

Euklidov algoritam daje da je $\text{NzD}(918, 252)$ zapravo poslednji nenukljivi ostatak Euklidovaog algoritma

$$\rightarrow 18 = 90 - 72 \cdot 1 = 90 - 1(162 - 1 \cdot 90) =$$

$$90 - 1 \cdot 162 + 1 \cdot 90 = 2 \cdot 90 - 1 \cdot 162 =$$

$$2 \cdot (252 - 1 \cdot 162) - 1 \cdot 162 =$$

$$2 \cdot 252 - 2 \cdot 162 - 1 \cdot 162 =$$

$$2 \cdot 252 - 3 \cdot 162 =$$

$$2 \cdot 252 - 3 \cdot (918 - 3 \cdot 252) =$$

$$2 \cdot 252 - 3 \cdot 918 + 9 \cdot 252 =$$

$$11 \cdot 252 - 3 \cdot 918$$

Koeficijenti su 11 i -3, što jesu celi brojevi.

2. Dokazati da su celi brojevi x i y uzajamno prosti ($\text{NzD}(x,y)=1$) akko postoji celi brojevi a i b takvi da je $a \cdot x + b \cdot y = 1$.

\Rightarrow : Neka je $\text{NzD}(x,y)=1$

Hodom unazad Euklidovim algoritmom (kao u prethodnom zadatku) dobijamo \mathbb{Z} -linearnu kombinaciju brojeva x i y koja je $= \text{NzD}(x,y)=1$

$$a \cdot x + b \cdot y = 1$$

\Leftarrow : Neka postoje $a, b \in \mathbb{Z}$ takvi da je $a \cdot x + b \cdot y = 1$

Neka je d neki zajednički delilac za x i y

$$\begin{aligned} d|x &\Rightarrow d|a \cdot x \\ d|y &\Rightarrow d|b \cdot y \end{aligned} \Rightarrow d|\underbrace{ax+by}_1 \Rightarrow d|1 \Rightarrow d \in \{1, -1\} \Rightarrow \text{NzD}(x,y)=1$$

3. Dokazati da je razlomak $\frac{21n+4}{14n+3}$ neskrativ za proizvoljno $n \in \mathbb{N}$

Dokazujemo da je $\text{NzD}(21n+4, 14n+3)=1$

Po prethodnom zadatku, dovoljno je naći ujihovu \mathbb{Z} -linearnu kombinaciju koja je $= 1$

$$a \cdot (21n+4) + b \cdot (14n+3) = 1$$

$$21an+4a+14bn+3b=1$$

$$(21a+14b)n + (4a+3b) = 1$$

Dovoljno je da $21a+14b=0$

$$4a+3b=1$$

$a = -2$ i $b = 3$ zadovoljuju ovo.

Dakle, $\text{NzD}(21n+4, 14n+3)=1$

4. Naći $\text{NzD}(93, 81)$; predstaviti ga preko matične \mathbb{Z} -linearne kombinacije brojeva 93 i 81.

$$93 = 1 \cdot 81 + 12$$

$$81 = 6 \cdot 12 + 9$$

$$12 = 1 \cdot 9 + 3$$

$$9 = 3 \cdot 3 + 0 \uparrow$$

$$\underline{\begin{pmatrix} 93 \\ 81 \end{pmatrix}} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 81 \\ 12 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 12 \\ 9 \end{pmatrix} =$$

poslednji
nenula ostatak

$$\begin{pmatrix} 7 & 1 \\ 6 & 1 \end{pmatrix} \begin{pmatrix} 12 \\ 9 \end{pmatrix} =$$

je NzD

$$\begin{pmatrix} 7 & 1 \\ 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 9 \\ 3 \end{pmatrix} =$$

$$\begin{aligned} & \left(\begin{array}{cc} 8 & 7 \\ 7 & 6 \end{array} \right) \left(\begin{array}{c} 9 \\ 3 \end{array} \right) = \\ & \left(\begin{array}{cc} 8 & 7 \\ 7 & 6 \end{array} \right) \left(\begin{array}{cc} 3 & 1 \\ 1 & 0 \end{array} \right) \left(\begin{array}{c} 3 \\ 0 \end{array} \right) \\ & = \left(\begin{array}{cc} 31 & 8 \\ 27 & 7 \end{array} \right) \left(\begin{array}{c} 3 \\ 0 \end{array} \right) \end{aligned}$$

stavljamo
1, a ne o
da bismo
dobili invertibilnu
matricu

$$\left(\begin{array}{c} 93 \\ 81 \end{array} \right) = \left(\begin{array}{cc} 31 & 8 \\ 27 & 7 \end{array} \right) \left(\begin{array}{c} 3 \\ 0 \end{array} \right) / \left(\begin{array}{cc} 31 & 8 \\ 27 & 7 \end{array} \right)^{-1} \quad \text{sa leve strane}$$

$$\left[\left(\begin{array}{cc} a & b \\ c & d \end{array} \right)^{-1} = \frac{1}{\det \left(\begin{array}{cc} a & b \\ c & d \end{array} \right)} \cdot \left(\begin{array}{cc} d & -b \\ -c & a \end{array} \right) \right]$$

$$\left(\begin{array}{cc} 31 & 8 \\ 27 & 7 \end{array} \right)^{-1} \left(\begin{array}{c} 93 \\ 81 \end{array} \right) = \left(\begin{array}{c} 3 \\ 0 \end{array} \right)$$

$$\underbrace{\frac{1}{31 \cdot 7 - 8 \cdot 27}}_{=1} \cdot \left(\begin{array}{cc} 7 & -8 \\ -27 & 31 \end{array} \right) \left(\begin{array}{c} 93 \\ 81 \end{array} \right) = \left(\begin{array}{c} 3 \\ 0 \end{array} \right)$$

$$\left(\begin{array}{cc} 7 & -8 \\ -27 & 31 \end{array} \right) \left(\begin{array}{c} 93 \\ 81 \end{array} \right) = \left(\begin{array}{c} 3 \\ 0 \end{array} \right)$$

$$\left(\begin{array}{c} 7 \cdot 93 - 8 \cdot 81 \\ -27 \cdot 93 + 31 \cdot 81 \end{array} \right) = \left(\begin{array}{c} 3 \\ 0 \end{array} \right)$$

$$3 = \underbrace{7 \cdot 93 - 8 \cdot 81}$$

\mathbb{Z} -linearna kombinacija
sa koeficijentima 7 i -8.

Stav: Postoji beskonačno mnogo prostih brojeva.

(1 nije prost broj, a ni složen)

Stav (osnovni stav aritmetike - jednoznačna faktorizacija):

Svaki prirodan broj $N > 1$ se na jedinstven način može predstaviti kao proizvod stepena prostih

$$N = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$$

(da je 1 prost broj, $N = 1 \cdot p_1^{d_1} \cdots p_k^{d_k} = 1^2 \cdot p_1^{d_1} \cdots p_k^{d_k}$
 $= 1^3 \cdot p_1^{d_1} \cdots p_k^{d_k} = \dots$)

Stav: Ako je $a = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ } uvek možemo dopuniti
 $b = p_1^{B_1} p_2^{B_2} \cdots p_k^{B_k}$ } faktorizacije za a i b
 tako da se pojave isti brojevi

$$\text{tada je } N \text{ZD}(a, b) = p_1^{\min\{d_1, B_1\}} p_2^{\min\{d_2, B_2\}} \cdots p_k^{\min\{d_k, B_k\}}$$

$$N \text{ZS}(a, b) = p_1^{\max\{d_1, B_1\}} p_2^{\max\{d_2, B_2\}} \cdots p_k^{\max\{d_k, B_k\}}$$

Posledica: Za svaka dva prirodna broja a, b je
 $\text{NZD}(a, b) \cdot \text{NZS}(a, b) = a \cdot b$

Stav: Ako je $n = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$, tada je broj delilaca od $n = (1+d_1)(1+d_2) \cdots (1+d_k)$

Stav: Ako je p prost broj, a n prirodan broj, tada je stepen broja p u faktorizaciji od $\frac{n}{p}$ bas-
 $\left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \cdots$ 1:2: ... n

$$\lceil x \rceil = \text{najveći ceo broj} \leq x \rfloor$$

5. Odrediti sa koliko mula se završava zapis broja $134!$.
Tražimo najveći stepen broja $10 = 2 \cdot 5$ koji deli $134!$
 $134! = \underbrace{1 \cdot 2 \cdot 3 \cdots}_{2 < 5, \text{ pa se } 2} \underbrace{\cdots \cdot 134}_{\text{svakako pojavljuje}} \text{ ceste od } 5$
Dakle, tražimo najveći stepen broja 5 koji deli $134!$

$$\begin{aligned} \text{Po prethodnom stavu, to je } & \left[\frac{134}{5} \right] + \left[\frac{134}{5^2} \right] + \left[\frac{134}{5^3} \right] + \left[\frac{134}{5^4} \right] + \cdots \\ & = 28 + 5 + 1 + 0 + 0 + 0 + \cdots \\ & = 34 \end{aligned}$$

Dakle, $134!$ se završava sa 34 nule.

Difantove jednacine

1. Rešiti po x, y jednacinu $x^2 - 7 = xy$ u \mathbb{Z}

$$x^2 - xy = 7$$

$$x(x-y) = 7 = 1 \cdot 7 = 7 \cdot 1 = (-1) \cdot (-7) = (-7) \cdot (-1)$$

$$\begin{array}{c} \uparrow \\ 1 \\ \uparrow \end{array} \quad \begin{array}{c} \uparrow \\ 7 \\ \uparrow \end{array}$$

$$\begin{cases} x=1 \\ x-y=7 \end{cases} \Rightarrow y=-6$$

$$\begin{cases} x=-1 \\ x-y=-7 \end{cases} \Rightarrow y=6$$

$$\begin{cases} x=7 \\ x-y=1 \end{cases} \Rightarrow y=6$$

$$\begin{cases} x=-7 \\ x-y=-1 \end{cases} \Rightarrow y=-6$$

$(1, -6), (7, 6), (-1, 6), (-7, -6)$ su sva rešenja

2. Naci proste brojeve p, g i r takve da je
 $(3p+g^2)r = 2010 = 2 \cdot 3 \cdot 5 \cdot 67$
Kako je r prost broj $\Rightarrow r \in \{2, 3, 5, 67\}$

1° $r=2$

$$3p+g^2 = \underbrace{3 \cdot 5 \cdot 67}_{\text{deljivo sa } 3} \Rightarrow 3 \mid 3p+g^2 \Rightarrow 3 \mid g^2 \Rightarrow 3 \mid g$$

ali g je prost $\Rightarrow g=3$

$$3p+3^2 = 3 \cdot 5 \cdot 67$$

$$3p = 3 \cdot 5 \cdot 67 - 9 = 996 \quad /:3$$

$$p = \underbrace{332}_{\text{ni je prost}}$$

ni je prost

$$2^\circ \quad r=5 \quad \Rightarrow \quad 3p+g^2 = 2 \cdot 3 \cdot 67 \quad \Rightarrow \quad g^2 = \underbrace{2 \cdot 3 \cdot 67 - 3p}_{\text{deljivo sa } 3}$$

$$\Rightarrow 3 \mid g^2 \Rightarrow 3 \mid g$$

$$3p+g = 2 \cdot 3 \cdot 67 \quad \Rightarrow \quad g=3$$

$$3p = 393 \quad /:3$$

$p = 131$ što jeste prost broj
 $(131, 3, 5)$ jcdno rešenje

$$3^\circ \quad r=67 \quad \Rightarrow \quad 3p+g^2 = 2 \cdot 3 \cdot 5 \quad \Rightarrow \quad g^2 = \underbrace{2 \cdot 3 \cdot 5 - 3p}_{\text{deljiv sa } 3}$$

$$\Rightarrow 3 \mid g^2 \Rightarrow 3 \mid g \Rightarrow g=3$$

$$3p+g = 30$$

$$3p=21$$

$$p=7$$

$(7, 3, 67)$

$$4^{\circ} \quad r=3 \Rightarrow 3p + q^2 = 2 \cdot 5 \cdot 67$$

$$q^2 = 2 \cdot 5 \cdot 67 - \underbrace{3 \cdot p}_{\geq 6 \text{ jer je } p \geq 2} \leq 667$$

$$q \leq \sqrt{667} \approx 25,82$$

$$\Rightarrow q \in \{2, \cancel{3}, 5, 7, 11, 13, 17, 19, 23\}$$

Provjrite sve mogućnosti

$$3p = 2 \cdot 5 \cdot 67 - q^2$$

$$3p = 670 - q^2 \Rightarrow 670 \equiv q^2 \pmod{3}$$

$$q^2 \equiv 1 \pmod{3}$$

kvadrati svih brojeva

koji nisu deljivi sa 3

daju ostatak 1 pri deljenju sa 3

Velika Fermatova teorema: Jednačina $x^n + y^n = z^n$
za $n \geq 3$ nemaju celobrojnih rešenja po $x, y, z \in \mathbb{Z}$

$$x^4 + y^4 = z^7$$

Andrew Wiles 1995.

Linearna Difantova jednačina

1) sa jednom nepoznatom:

$$a \cdot x = b \quad \text{za } a, b \in \mathbb{Z} \quad \text{i } a \neq 0$$

$$x = \frac{b}{a} \quad (\text{postoji ukoliko } a \neq 0)$$

2) sa dve nepoznate:

$$a \cdot x + b \cdot y = c \quad a, b, c \in \mathbb{Z} \quad a \neq 0 \quad \text{i } b \neq 0$$

a) Ako je $c = \text{NzD}(a, b)$, jedno rešenje po x i y dobijamo iz Euklidovog algoritma

b) Ako je $c \neq \text{NzD}(a, b)$, tada:

$$\begin{aligned} \text{NzD}(a, b) \mid a \\ \text{NzD}(a, b) \mid b \end{aligned} \Rightarrow \text{NzD}(a, b) \mid \underbrace{ax + by}_{=c} \Rightarrow \text{NzD}(a, b) \mid c$$

Stoga, $\text{NzD}(a, b) \mid c$ poulači da rešenje ne postoji.

Nadalje posmatramo situaciju u kojoj

$$\text{NzD}(a, b) \mid c \Leftrightarrow c = \text{NzD}(a, b) \cdot k \quad k \in \mathbb{Z}$$

(*) $ax + by = \text{NzD}(a, b)$ dobijamo rešenje i \exists Euklidovog algoritma

$$k \cdot (ax + by) = k \cdot \text{NzD}(a, b) = c$$

$$(**) a \cdot (kx) + b \cdot (ky) = c$$

Ako je (x_0, y_0) rešenje (*), tada je (kx_0, ky_0) rešenje za (**)

Ako je (x_0, y_0) jedno rešenje jednačine $ax + by = c$ ($\text{NzD}(a, b) \mid c$), a (u, v) neko drugo rešenje, tada:

$$a \cdot x_0 + b \cdot y_0 = c$$

$$- a \cdot u + b \cdot v = c$$

$$a \cdot (x_0 - u) + b \cdot (y_0 - v) = 0 \quad /: \text{NzD}(a, b)$$

$$\frac{a}{\text{NzD}(a, b)} (x_0 - u) = \frac{-b}{\text{NzD}(a, b)} \cdot (y_0 - v) = \frac{b}{\text{NzD}(a, b)} (v - y_0)$$

$$\frac{a}{\text{NzD}(a,b)} (x_0 - u) = \frac{b}{\text{NzD}(a,b)} (v - y_0)$$

$$\text{NzD}\left(\frac{a}{\text{NzD}(a,b)}, \frac{b}{\text{NzD}(a,b)}\right) = 1$$

$$\Rightarrow \frac{a}{\text{NzD}(a,b)} \mid \frac{b}{\text{NzD}(a,b)} \cdot (v - y_0) \Rightarrow \frac{a}{\text{NzD}(a,b)} \mid v - y_0$$

$$\Rightarrow \text{postoji } t \in \mathbb{Z} \text{ takav da je } v - y_0 = \frac{a}{\text{NzD}(a,b)} \cdot t$$

$$\Rightarrow v = \frac{a}{\text{NzD}(a,b)} \cdot t + y_0$$

$$\cancel{\frac{a}{\text{NzD}(a,b)}} \cdot (x_0 - u) = \frac{b}{\text{NzD}(a,b)} \cdot \cancel{\frac{a}{\text{NzD}(a,b)}} \cdot t \quad (a \neq 0)$$

$$u = x_0 - \frac{b}{\text{NzD}(a,b)} \cdot t$$

$$(u, v) = \left(x_0 - \frac{b}{\text{NzD}(a,b)} \cdot t, y_0 + \frac{a}{\text{NzD}(a,b)} \cdot t \right) \quad t \in \mathbb{Z}$$

(za $t=0$ dobijamo (x_0, y_0))

Stoga, ako rešenje postoji \Rightarrow imamo beskonačno mnogo rešenja.

1. Rešiti $27x + 59y = 20$.

Treba provjeriti da li $\text{NzD}(27, 59) \mid 20$

$$59 = 27 \cdot 2 + 5$$

$$27 = 5 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0 \uparrow$$

postledjući
nemala ostatak

je NzD

$1 \mid 20$, pa rešenje postoji.

Rešimo prvo jednačinu

$$27x + 59y = 1$$

Tedno rešenje ove jednačine je
 $(-24, 11)$

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (27 - 5 \cdot 5) = 5 - 2 \cdot 27 + 10 \cdot 5 = 11 \cdot 5 - 2 \cdot 27$$

$$= 11 \cdot (59 - 2 \cdot 27) - 2 \cdot 27 = 11 \cdot 59 - 22 \cdot 27 - 2 \cdot 27 =$$

$$11 \cdot 59 - 24 \cdot 27$$

$$27x + 59y = 20$$

ima jedno rešenje $(-480, 220)$

Stoga, sva druga rešenja imaju oblik:

$$\left(-480 - \frac{b}{\text{NZD}(a,b)} \cdot t, 220 + \frac{a}{\text{NZD}(a,b)} \cdot t \right) \quad \begin{array}{l} a=27 \\ b=59 \end{array}$$

$$\left\{ (-480 - 59t, 220 + 27t) \mid t \in \mathbb{Z} \right\} \quad \text{NZD}(a,b)=1$$

je skup rešenja.

Pitagorina jednačina

$$x^2 + y^2 = z^2$$

$$(3, 4, 5)$$

(x, y, z) rešenje \Rightarrow

$$(5, 12, 13)$$

$(\varepsilon_1 x, \varepsilon_2 y, \varepsilon_3 z)$ rešenja,

:

gde $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{-1, 1\}$

Primetimo da ako neko d istovremeno deli dva broja od x, y, z , tada d mora deliti i treći

$$\left. \begin{array}{l} \text{Neka } d|x \text{ i } d|z \Rightarrow y^2 = z^2 - x^2 \\ d^2|x^2; d^2|z^2 \Rightarrow d^2|z^2 - x^2 \end{array} \right\} \Rightarrow d|y$$

Stoga, možemo pretpostaviti da su oni u parovima užajdano prosti:

$$\text{NZD}(x, y) = \text{NZD}(y, z) = \text{NZD}(z, x) = 1$$

Dakle, specijalno jedan broj je paran, a druge dva neparna (ne mogu sva tri biti neparna)

z ne može biti paran, a ostala dva neparna jer onda: $z = 2k$

$$x = 2l+1$$

$$x^2 + y^2 = 4l^2 + 4l + 1 + 4p^2 + 4p + 1$$

$$y = 2p+1$$

$$\begin{aligned} &= 4(l^2 + l + p^2 + p) + 2 \leftarrow \text{ostatak 2 pri deljenju sa 4} \\ &z^2 = 4k^2 \leftarrow \text{ostatak 0 pri deljenju sa 4} \end{aligned}$$

Dakle, jedan od x/y je paran

BVO, neka je x paran.

$$(*) x = 2k \quad k \in \mathbb{Z}$$

$$x^2 = z^2 - y^2$$

$$4k^2 = (z-y)(z+y)$$

$y \neq z$ su neparni $\Rightarrow z-y$ i $z+y$ su parni

$$k^2 = \frac{z-y}{2} \cdot \frac{z+y}{2} \quad u = \frac{z-y}{2} \in \mathbb{Z}$$

$$v = \frac{z+y}{2} \in \mathbb{Z}$$

$$k^2 = u \cdot v$$

$$(*) \quad k = \sqrt{u \cdot v}$$

Dakle, u i v su uzajamno prosti brojevi čiji je proizvod kvadrat

$$u = m^2$$

$$v = n^2$$

$$\left. \begin{array}{l} u = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \\ v = q_1^{\beta_1} \cdots q_l^{\beta_l} \end{array} \right\} \begin{array}{l} \text{svi } p_i \text{ i} \\ \text{zj su razliciti} \\ \text{jer } N\text{zd}(u, v) = 1 \end{array}$$

$u \cdot v = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$ je kvadrat
 \Rightarrow svaki α_i i β_j mora biti paran

$$(*) \quad i \quad (**) \quad \text{daju } x = 2k = 2\sqrt{uv} = 2\sqrt{m^2n^2} = 2mn$$

$$y = u - v = m^2 - n^2$$

$$z = u + v = m^2 + n^2$$

$N\text{zd}(m, n) = 1$ jer su u i v uzajamno prosti

$$x^2 + y^2 = z^2 ?$$

$$(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2 ?$$

$$4m^2n^2 + m^4 - 2m^2n^2 + n^4 = m^4 + 2m^2n^2 + n^4 ?$$

$$m^4 + 2m^2n^2 + n^4 = m^4 + 2m^2n^2 + n^4 \quad \checkmark$$

Stoga, i ovde imamo beskonacno mnogo resenja.

Kongruencije

Def: Neka je $w \in \mathbb{N}_{>2}$ i neka su $a, b \in \mathbb{Z}$. Kazemo da je $a \equiv b \pmod{w}$ ukko $w \mid a-b$ akko $a \equiv b$ daju isti ostatak pri deljenju sa w .

Osobine: $\begin{cases} a \equiv b \pmod{w} \\ c \equiv d \pmod{w} \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d \pmod{w} \\ a \cdot c \equiv b \cdot d \pmod{w} \end{cases}$

1. Naci ostatak celog broja x pri deljenju sa 42 ako pri deljenju sa 2 daje ostatak 1, pri deljenju sa 3 daje ostatak 1, a pri deljenju sa 7 daje ostatak 2.

$$x = 2k+1 \quad \Rightarrow \quad 2k+1 = 3l+1$$

$$x = 3l+1$$

$$x = 7m+2$$

$$2k = 3l \Rightarrow 2 \mid 3l \Rightarrow 2 \mid l \Rightarrow l = 2 \cdot s$$

$$x = 3l+1 = 3 \cdot 2s + 1 =$$

$$x = 6s+1$$

$$7m+2 = 6s+1$$

$$6s = 7m+1$$

$$6s \equiv 1 \pmod{7}$$

Koji ostatak daje s pri deljenju sa 7?

$$\begin{cases} 6s \equiv 1 \pmod{7} \\ 6 \equiv 6 \pmod{7} \end{cases} \Rightarrow 6 \cdot 6s \equiv 6 \cdot 1 \pmod{7}$$

$$36s \equiv 6 \pmod{7}$$

$$36s = \underbrace{35s}_{\text{deljivo}} + 1$$

deljivo
sa 7

$$s \equiv 6 \pmod{7}$$

$$s = 7p+6$$

Izabrali smo
da uzmemo
brojem 6 jer
 $6 \cdot 6 \equiv 1 \pmod{7}$

Broj 6 tražimo preko
Euklidovog algoritma.
Tražimo a tako da je
 $a \cdot 6 \equiv 1 \pmod{7}$

$$a \cdot 6 = 7 \cdot b + 1$$

$$a \cdot 6 - b \cdot 7 = 1$$

$a \equiv b$ dobijamo
iz Euklidovog
algoritma za 6 i 7

$$7 = 1 \cdot 6 + 1$$

$6 = 6 \cdot 1 + 0$ poslednji
nenula ostatak

$$1 = 1 \cdot 7 - 1 \cdot 6$$

$$a = -1 \equiv \underbrace{7-1}_6 \pmod{7}$$

Teorema (Wilson): Broj p je prost akko

$$\text{je } (p-1)! \equiv -1 \pmod{p}$$

$$\equiv p-1 \pmod{p}$$

$$\equiv 2p-1 \pmod{p}$$

;

2. Ako je p prost broj, tada $p^3 \mid (p!)^2 - p^2$

$$p! = p \cdot (p-1)! \quad (p!)^2 - p^2 = (p \cdot (p-1)!)^2 - p^2 =$$

$$p^2 ((p-1)!)^2 - p^2 =$$

$$p^2 ((p-1)!)^2 - 1^2 =$$

$$p^2 \cdot ((p-1)! - 1) ((p-1)! + 1) \Rightarrow \text{deljivo sa } p^3.$$

↑
deljivo
sa p^2

Vilsonova teorema

$$(p-1)! \equiv -1 \pmod{p}$$

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

$\Rightarrow (p-1)! + 1$ je deljiv sa p

3. Nadi ostatak broja $97!$ pri deljenju sa 101 .

101 je prost broj $\Rightarrow 100! \equiv -1 \pmod{101}$

$$\text{Vilson} \quad 97! \cdot 98 \cdot 99 \cdot 100 \equiv -1 \pmod{101}$$

$$97! \cdot (-3)(-2)(-1) \equiv -1 \pmod{101}$$

$$- 97! \cdot 6 \equiv -1 \pmod{101}$$

$$6 \cdot 97! \equiv 1 \pmod{101}$$

Trifinio a tako da je $a \cdot 6 \equiv 1 \pmod{101}$

$$101 = 16 \cdot 6 + 5$$

$$6 = 1 \cdot 5 + 1$$

$$5 = 5 \cdot 1 + 0$$

ova je
NJD

$$1 = 6 - 1 \cdot 5 =$$

$$6 - (101 - 16 \cdot 6)$$

$$= 6 - 101 + 16 \cdot 6$$

$$= 17 \cdot 6 - 101$$

$$\Rightarrow 17 \cdot 6 = 101 + 1$$

$$17 \cdot 6 \equiv 1 \pmod{101}$$

$$a = 17$$

$$6 \cdot 97! \equiv 1 \pmod{101} / \cdot 17$$

$$17 \cdot 6 \cdot 97! \equiv 17 \pmod{101}$$

$$\underbrace{=}_{=1} \quad 97! \equiv 17 \pmod{101}$$

Dakle, ostatak je 17.

1. Odrediti dvocifreni završetak broja

$$x = \underbrace{6^6}_{2004 \text{ puta}}$$

dvocifreni završetak broja x je ostatak

broja x pri deljenju sa $10^2 = 100 = 4 \cdot 25 = 2^2 \cdot 5^2$

Tražimo ostatak pri deljenju sa 4 i pri deljenju sa 25

$$6 \equiv 2 \pmod{4}$$

$$6^1 \equiv 6 \pmod{25}$$

$$6^2 \equiv 0 \pmod{4}$$

$$6^2 \equiv 11 \pmod{25}$$

$$6^3 \equiv 0 \pmod{4}$$

$$6^3 \equiv 6 \cdot 11 \equiv 66 \equiv 16 \pmod{25}$$

$$\vdots$$

$$6^k \equiv 0 \pmod{4}, k \geq 2$$

$$6^4 \equiv 6 \cdot 16 \equiv 21 \pmod{25}$$

$$x \equiv 0 \pmod{4}$$

$$6^5 \equiv 1 \pmod{25}$$

$$6^6 \equiv 6 \pmod{25}$$

$$6^7 \equiv 11 \pmod{25}$$

Nakon 6^5 , ostaci kreću da se ciklično ponavljaju

$$\underbrace{6, 11, 16, 21}_\text{ciklus dužine 5}, 1$$

Ostatak od x zavisi od ostatka stepena pri deljenju sa 5

$$6 \equiv 1 \pmod{5}$$

$$\underbrace{6}_{2003 \text{ puta}}^6$$

$$6^2 \equiv 1 \pmod{5}$$

$$6^3 \equiv 1 \pmod{5}$$

$$\vdots$$

$$6^k \equiv 1 \pmod{5} \quad k \geq 1$$

Stoga, $x \equiv 6 \pmod{25}$

$$x \equiv 0 \pmod{4}$$

$$x = 4k \quad k \in \mathbb{Z}$$

$$x = 25l + 6$$

$$4k = 25l + 6$$

$$4k \equiv 6 \pmod{25}$$

Trazimo a tako da je $4 \cdot a \equiv 1 \pmod{25}$

$$25 = 6 \cdot 4 + 1 \Rightarrow 1 = 25 - 6 \cdot 4$$

$$\Rightarrow \text{Trazimo } a = -6 \equiv 25 - 6 = 19 \pmod{25}$$

$$4k \equiv 6 \pmod{25}$$

$$19 - 4k \equiv 19 - 6 \pmod{25}$$

$$k \equiv 14 \equiv 14 \pmod{25}$$

$$k = 25s + 14$$

$$x = hk = 4 \cdot (25s + 14) = 100s + 56$$

$\Rightarrow x$ daje ostatak 56 pri deljenju sa 100.

Def: Neka je $n \geq 2$

Kanonski potpun sistem ostataka po modulu n
je $\{0, 1, \dots, n-1\} = \mathbb{Z}_n$
Ojlerova funkcija $\varphi(n) = |\{x \in \mathbb{Z}_n \mid \text{NZD}(x, n) = 1\}|$

Primer:

$$n=3$$

$$\mathbb{Z}_3 = \{0, 1, 2\}$$

$$\varphi(3) = |\{1, 2\}| - 2$$

↑
 \mathbb{Z}_3

uzajamno
prosti sa 3

$$n=6$$

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

$$\varphi(6) = |\{1, 5\}| = 2$$

Osobine: 1) Ako je p prost $\Rightarrow \varphi(p) = p-1$ (svi osim
nule u \mathbb{Z}_p su uzajamno prosti sa p)

2) Ako je $\text{NZD}(m, n) = 1$, tada je
 $\varphi(m \cdot n) = \varphi(m) \varphi(n)$

3) Ako je p prost $\Rightarrow \varphi(p^k) = p^k - p^{k-1}$

($\mathbb{Z}_{p^k} = \{0, 1, \dots, p^k - 1\}$) $\leftarrow p^k$ elemenata
Koji su uzajamno prosti sa p^k ?

Svi oni koji nemaju p kao svoj faktor

Oni koji imaju p kao svoj faktor svi:

$0 \cdot p, 1 \cdot p, 2 \cdot p, \dots, (\underbrace{p^{k-1} - 1}_{p^k - p}) \cdot p \leftarrow p^{k-1}$ elemenata)

4) Ako je $n = p_1^{k_1} p_2^{k_2} \cdots p_e^{k_e}$

$$\varphi(n) = \varphi(p_1^{k_1} p_2^{k_2} \cdots p_e^{k_e}) \stackrel{def}{=} \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \cdots \varphi(p_e^{k_e})$$

$$\begin{aligned} &\stackrel{3)}{=} (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_e^{k_e} - p_e^{k_e-1}) \\ &= p_1^{k_1} \left(1 - \frac{1}{p_1}\right) p_2^{k_2} \left(1 - \frac{1}{p_2}\right) \cdots p_e^{k_e} \left(1 - \frac{1}{p_e}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_e}\right) \end{aligned}$$

$$\varphi(6) = 6 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 6 \cdot \frac{1}{2} \cdot \frac{2}{3} = 2$$

Teorema (Ojlerova): Ako su a i w ustanovno prosti, tada je $a^{\varphi(w)} \equiv 1 \pmod{w}$

Posledica (Ferma): Ako je a broj koji nije deljiv prostim brojem p , tada je

$$a^{p-1} \equiv 1 \pmod{p}$$

2. Odrediti ostatak pri deljenju broja 317^{259} sa 15.

$$\text{NOD}(317, 15) = 1 \quad \text{jer } 317 \text{ nije deljivo ni sa } 3 \text{ ni sa } 5$$

Po Ojlerovoj teoremi $317^{\varphi(15)} \equiv 1 \pmod{15}$

$$\varphi(15) = 15 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$$

$$317^8 \equiv 1 \pmod{15}$$

Zamislimo nas ostatak 259 pri deljenju sa 8

$$259 = 32 \cdot 8 + 3$$

$$317^{259} = 317^{8 \cdot 32 + 3} = \underbrace{(317^8)^{32}}_{\equiv 1 \pmod{15}} \cdot 317^3 \equiv 1 \cdot 317^3 \pmod{15}$$

$317 \equiv 2 \pmod{15}$ jer je 315 deljiv sa 15

$$317^3 \equiv 2^3 \pmod{15}$$

$$x \equiv 8 \pmod{15}$$

3. Dokazati da ne postoji n€N takav da je $\varphi(n) = 3$

Pretpostavimo da takvo n postoji:

1° Ako je n prost, tada je

$$3 = \varphi(n) = n-1 \Rightarrow n=4, \text{ što nije prost broj. } \checkmark$$

2° Ako n nije prost, neka je p neki vjegav prost faktor i k najveći stepen od p koji deli n
 $n = p^k \cdot m$, gde $p \nmid m$
 $NZD(p^k, m) = 1$

$$\begin{aligned} 3 = \varphi(n) &= \varphi(p^k \cdot m) = \varphi(p^k) \cdot \varphi(m) = (p^k - p^{k-1}) \cdot \varphi(m) \\ &= p^{k-1} (p-1) \cdot \varphi(m) \end{aligned}$$

$$\Rightarrow p-1 \mid 3 \Rightarrow p-1 \in \{1, 3\} \Rightarrow p \in \{2, 4\}$$

$p=4$ otpada jer 4 nije prost

Ako je $p=2$:

$$3 = 2^{k-1} \cdot (2-1) \cdot \varphi(m)$$

$$3 = 2^{k-1} \cdot \varphi(m) \Rightarrow k=1$$

$$3 = \varphi(m)$$

m ne može biti prost jer bi:

$$3 = \varphi(m) = m-1 \Rightarrow m=4, \text{ što nije prost broj}$$

Ako je g neki prost faktor broja m i l najveći stepen od g koji deli m

$$m = g^l \cdot s \quad NZD(g, s) = 1$$

$$\begin{aligned} 3 = \varphi(m) &= \varphi(g^l \cdot s) = \varphi(g^l) \cdot \varphi(s) = (g^l - g^{l-1}) \cdot \varphi(s) \\ &= g^{l-1} \cdot (g-1) \cdot \varphi(s) \end{aligned}$$

$$g-1 \mid 3 \Rightarrow g-1 \in \{1, 3\} \Rightarrow g \in \{2, 4\}$$

Ali $g \neq 2$ i $g \neq 4$ jer je g prost broj. \checkmark

Takav broj ne postoji.

4. Odrediti ostatak broja $9! \cdot 27!$ pri deljenju sa 33.

$$33 = 3^2 \cdot 37$$

$9! \cdot 27!$ je deljivo sa 9

$$9! \cdot 27! \equiv 0 \pmod{9}$$

37 je prost broj $\Rightarrow 36! \equiv -1 \pmod{37}$

$$-1 \equiv 36! = 27! \cdot 28 \cdot 29 \cdots 35 \cdot 36 \equiv 27! \cdot (-1)^9 \cdot 9!$$

$\begin{matrix} \text{||} & \text{||} \\ -9 & -8 \end{matrix} \quad \begin{matrix} \text{||} & \text{||} \\ -2 & -1 \end{matrix}$

$$-27! \cdot 9! \equiv -1 \pmod{37}$$

$$27! \cdot 9! \equiv 1 \pmod{37}$$

$$x \equiv 0 \pmod{9}$$

$$x \equiv 1 \pmod{37}$$

$$x = 9k$$

$$x = 37l + 1$$

$$k, l \in \mathbb{Z}$$

$$\begin{aligned} gk &= 37l + 1 \\ gk &\equiv 1 \pmod{37} \end{aligned}$$

$$37 = 4 \cdot 9 + 1 \Rightarrow 1 = 37 - 4 \cdot 9$$

$$\text{pa je traženi broj } -4 \equiv 33 \pmod{37}$$

-33

$$33 \cdot 9k \equiv 33 \pmod{37}$$

$$k \equiv 33 \pmod{37}$$

$$k = 37s + 33$$

$$x = 9k = 9 \cdot (37s + 33) = 333s + 297$$

$$x \equiv 297 \pmod{333}$$

5. Ako je p prost broj veći od 7, dokazati da

$$50^4 \mid p^6 - 1$$

$50^4 = 7 \cdot 8 \cdot 9$, dovoljno je da dokazemo da

$$7 \mid p^6 - 1$$

$$8 \mid p^6 - 1$$

$$9 \mid p^6 - 1$$

$NZD(p, 7) = 1$ jer su to dva razlicita prosti brojevi,

pa je po Fermatovoj teoremi

$$p^6 \equiv 1 \pmod{7}$$

$$p^6 - 1 \equiv 0 \pmod{7} \Leftrightarrow 7 \mid p^6 - 1$$

$\text{NZD}(p, g) = 1$ jer su p i g razliciti prosti brojevi

Po Ojlerovoj teoremi je

$$p^{\varphi(g)} \equiv 1 \pmod{g} \quad \varphi(g) = g(3^2) = 3^2 - 3 = 6$$

$$p^6 \equiv 1 \pmod{g} \Leftrightarrow p^6 - 1 \equiv 0 \pmod{g}$$

$$\Leftrightarrow g | p^6 - 1$$

$\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 8 - 4 = 4 \neq 6$, pa ne možemo ovako da dobijemo da $8 | p^6 - 1$

$$p^6 - 1 = (p^3)^2 - 1^2 = (p^3 - 1)(p^3 + 1) =$$

$$(p-1)(p^2 + p + 1)(p+1)(p^2 - p + 1)$$

p je nepravi, te su $p-1$ i $p+1$ parni brojevi koji su užastopni, te jedan od njih mora biti deljiv sa 4.

6. Ako su p i g razliciti prosti brojevi, dokazati da je $p^{2-1} + g^{p-1} \equiv 1 \pmod{pg}$

• $p^{2-1} \equiv 1 \pmod{g}$ po Fermatovoj teoremi

- $p^{2-1} \equiv 0 \pmod{p}$

• $g^{p-1} \equiv 0 \pmod{g}$

- $g^{p-1} \equiv 1 \pmod{p}$ po Fermatovoj teoremi

$$p^{2-1} + g^{p-1} \equiv 1 \pmod{g} \Leftrightarrow g | p^{2-1} + g^{p-1} - 1$$

$$p^{2-1} + g^{p-1} \equiv 1 \pmod{p} \Leftrightarrow p | p^{2-1} + g^{p-1} - 1$$

Kako su p i g uザajamno prosti, to

$$\begin{aligned} & \frac{pg}{\boxed{p^{2-1} + g^{p-1} - 1}} \\ \Leftrightarrow & \boxed{p^{2-1} + g^{p-1} \equiv 1 \pmod{pg}} \end{aligned}$$

7. Odrediti ostatak pri deljenju

$$x = (12!)^2 + 22^{19^{12}} \text{ sa } 143 = 11 \cdot 13$$

Tražim ostatak x pri deljenju sa 11 i pri deljenju sa 13

$$\text{Sa 11: } 12! = 1 \cdots \cdot 11 \cdot 12$$

$$11 \mid (12!)^2$$

$$\begin{array}{c} 11 \mid 22 \\ 11 \mid 22^{19^{12}} \end{array} \Rightarrow \begin{array}{l} 11 \mid x \\ x \equiv 0 \pmod{11} \end{array}$$

$$\text{Sa 13: } 12! \equiv -1 \pmod{13}$$

$$(12!)^2 \equiv 1 \pmod{13}$$

$$22 \equiv 9 \pmod{13}$$

$$22^{19^{12}} \equiv 9^{19^{12}} \pmod{13}$$

$$\text{NzD}(9, 13) = 1$$

$$\text{pa je } 9^{12} \equiv 1 \pmod{13}$$

po Fermatovoj teoremi

Stoga, određujemo 19^{12} pri deljenju sa 12.

Na kraju:

$$x \equiv 0 \pmod{11}$$

$$x \equiv \text{nesto} \pmod{13}$$

resimo ovaj sistem jednačina

Bullove algebre

Pod Bulovom algebrrom podrazumijevamo skup \mathcal{B} na kom su definisane operacije \vee, \wedge dužine 2, $'$ dužine 1 i u kom se nalaze 2 konstante koje obeležavamo sa 0 i 1

$$(\mathcal{B}, \vee, \wedge, ', 0, 1)$$

tako da važe osobine:

- | | |
|---|---|
| 1) $x \vee (y \vee z) = (x \vee y) \vee z$ | 2) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ |
| 3) $x \vee y = y \vee x$ | 4) $x \wedge y = y \wedge x$ |
| 5) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ | 6) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ |
| 7) $x \vee x' = 1$ | 8) $x \wedge x' = 0$ |
| 9) $x \vee 0 = x$ | 10) $x \wedge 1 = x$ |

Primer: Ako je S neki skup, tada je
 $(\mathcal{P}(S), \cup, \cap, ', \emptyset, S)$

Vazi dualnost u aksivima, to ako dokazemo da neko tvrdjenje vazi za Bulove algebre, tada automatski dobijamo i dokaz dualnog tvrdjenja (onog koji se dobije od polarnog tako sto se \wedge zameni sa \vee , \vee zameni sa \wedge , 0 zameni sa 1, a 1 zameni sa 0).

1. Dokazati da je u svakoj Bulovoj algebri

$$0' = 1 \quad ; \quad 1' = 0$$
$$0' \stackrel{g)}{=} 0' \vee 0 \stackrel{5)}{=} 0 \vee 0' \stackrel{7)}{=} 1$$

$$1' \stackrel{10)}{=} 1' \wedge 1 \stackrel{4)}{=} 1 \wedge 1' \stackrel{8)}{=} 0$$

2. Dokazati da je u svakoj Bulovoj algebri

$$x \wedge x = x \quad ; \quad x \vee x = x$$

$$x \wedge x \stackrel{g)}{=} (x \wedge x) \vee 0 \stackrel{8)}{=} (x \wedge x) \vee (x \wedge x') \stackrel{6)}{=} x \wedge (x \vee x') \stackrel{7)}{=} x \wedge 1 \stackrel{10)}{=} x$$

$$x \vee x \stackrel{10)}{=} (x \vee x) \wedge 1 \stackrel{7)}{=} (x \vee x) \wedge (x \vee x') \stackrel{5)}{=} x \vee (x \wedge x') \stackrel{8)}{=} x \vee 0 \stackrel{g)}{=} x$$

3. Dokazati da je u svakoj Bulovaškoj algebri

$$x \wedge 0 = 0 \quad ; \quad x \vee 1 = 1$$

$$\begin{aligned} x \wedge 0 &= (x \wedge 0) \vee 0 = (x \wedge 0) \vee (x \wedge x') = x \wedge (0 \vee x') = x \wedge (x' \vee 0) \\ &= x \wedge x' = 0 \end{aligned}$$

4. Dokazati da je u svakoj Bulovaškoj algebri

$$x \wedge (x \vee y) = x \quad ; \quad x \vee (x \wedge y) = x$$

zadatak 3.

$$x \wedge (x \vee y) = (x \vee 0) \wedge (x \vee y) = x \vee (0 \wedge y) = x \vee (y \wedge 0) \stackrel{\downarrow}{=} y$$

$$x \vee 0 = x \quad (\text{zakon apsorpcije})$$

5. Dokazati da je u svakoj Bulovaškoj algebri

$$(x \vee y)' = x' \wedge y' \quad ; \quad (x \wedge y)' = x' \vee y'$$

Da bismo ovo dokazali, dovoljno je dokazati da su $x \vee y$ i $x' \wedge y'$ međusobno komplementni

$$(x \vee y) \vee (x' \wedge y') = 1 :$$

$$= (x \vee y \vee x') \wedge (x \vee y \vee y')$$

$$= (x \vee x' \vee y) \wedge (x \vee y \vee y')$$

$$= (1 \vee y) \wedge (x \vee 1)$$

$$= 1 \wedge 1 = 1$$

$$(x \vee y) \wedge (x' \wedge y') = 0 :$$

$$= (x' \wedge y') \wedge (x \vee y)$$

$$= (x' \wedge y' \wedge x) \vee (x' \wedge y' \wedge y)$$

$$= (x' \wedge x \wedge y') \vee (x' \wedge y' \wedge y)$$

$$= (x \wedge x' \wedge y') \vee (x' \wedge y \wedge y')$$

$$= (0 \wedge y') \vee (x' \wedge 0)$$

$$= 0 \vee 0 = 0$$

zadatak 3

6. Dokazati da je u svakoj Bulovaškoj algebri

$$a \vee c = b \vee c \quad ; \quad a \vee c' = b \vee c' \Rightarrow a = b$$

$$\begin{aligned} a &= a \vee 0 = a \vee (c \wedge c') = (a \vee c) \wedge (a \vee c') = (b \vee c) \wedge (b \vee c') \\ &= b \vee (c \wedge c') = b \vee 0 = b \end{aligned}$$

Iskazna logika

Iskaz je rečenica kojoj možemo odrediti istinitosnu vrednost (tačno / netačno , T / L , 1 / 0). Skup svih iskaza obeležavamo sa P , a iskaze obeležavamo malim slovima latinske (p, q, r, ...)

U iskaznoj logici konstimo i veznike (logičke operacije) \neg , \wedge , \vee , \Rightarrow , \Leftarrow , \uparrow , \downarrow , ... i pomoćne simbole (zagrade (:))

Def: Formula iskazne logike je definisana induktivno:

- iskazna slova jesu formule
- Ako su A i B neke formule, tada su i :

 - $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, $(A \Leftarrow B)$
 - Isto iskazne formule

- pravila a) i b) smemo primeniti samo konačno mnogo puta.

Istinitosne vrednosti slova koja se pojavljuju u nekoj iskaznoj formuli diktiraju istinitosnu vrednost same formule:

A	$\neg A$
0	1
1	0

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

$A \wedge B$

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

$A \vee B$

ako A , onda B

A	B	$A \Rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

A akko B

A	B	$A \Leftarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

ili A ili B

A	B	$A \vee \neg B$
0	0	0
0	1	1
1	0	1
1	1	0

Def: Formula F iskazne logike je tautologija ako je uvek tačna, a kontradikcija ako je uvek netačna

Da je formula tautologija, proveravamo na sledeće načine:

- 1) tablicno
- 2) svodnjem na absurd (kontradikciju)
- 3) diskusijom po slovu

Primer: 1) Ispitati da li je formula
 $F = ((p \Rightarrow q) \wedge p) \Rightarrow q$
tautologija

p	q	$p \Rightarrow q$	$(p \Rightarrow q) \wedge p$	$((p \Rightarrow q) \wedge p) \Rightarrow q$	
0	0	1	0	1	
0	1	1	0	1	
1	0	0	0	1	
1	1	1	1	1	

Formula je uvek tačna, pa je i tautologija

$$2) F = ((p \Rightarrow q) \Rightarrow r) \rightarrow ((r \Rightarrow p) \Rightarrow (q \Rightarrow p))$$

Prepostavimo suprotno, tj. da formula F nije tautologija, tj. da postoji situacija u kojoj je formula netačna

$$1. ((p \Rightarrow q) \Rightarrow r) \Rightarrow ((r \Rightarrow p) \Rightarrow (q \Rightarrow p)) = 0$$

$$2. (p \Rightarrow q) \Rightarrow r = 1$$

$$3. (r \Rightarrow p) \Rightarrow (q \Rightarrow p) = 0$$

$$4. r \Rightarrow p = 1$$

$$5. q \Rightarrow p = 0$$

$$6. \quad 2=1$$

$$7. \quad p=0$$

$$8. \quad Iz 4. je r \Rightarrow 0 = 1, pa je r = 0$$

$$9. \quad Iz 2. je \underline{1} = (\underline{p \Rightarrow q}) \Rightarrow r = (0 \Rightarrow 1) = 0 = 1 \Rightarrow 0 = 0$$

Stoga, nasra pretpostavka je pogrešna,
te je F tautologija.

$$3) \quad F = ((p \Rightarrow q) \wedge \neg q) \Rightarrow \neg p$$

Diskutujmo po slovu p:

1° Ako je p netačno jer je tada $\neg p = 1$, a implikacija je tačna kad god je zaključak tačan

2° Ako je p tačno

$$((1 \Rightarrow q) \wedge \neg q) \Rightarrow 0$$

$$a) \quad q = 1$$

$$((1 \Rightarrow 1) \wedge \neg 1) \Rightarrow 0$$

$$(1 \wedge 0) \Rightarrow 0$$

$$0 \Rightarrow 0$$

$$1$$

$$b) \quad q = 0$$

$$((1 \Rightarrow 0) \wedge \neg 0) \Rightarrow 0$$

$$(0 \wedge 1) \Rightarrow 0$$

$$0 \Rightarrow 0$$

$$1$$

Bitne tautologije:

$$1) \quad p \vee \neg p \quad (\text{isključenje trećeg})$$

$$2) \quad p \Leftrightarrow \neg \neg p \quad (\text{dvojna negacija})$$

$$3) \quad (p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p) \quad (\text{kontrapozicija})$$

$$4) \quad (p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p)) \quad (\text{eliminacija } \Leftrightarrow) \text{ miro}$$

- 5) $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$ (eliminacija \Rightarrow)
- 6) $(p \Rightarrow (q \wedge \neg q)) \Rightarrow \neg p$ (svodjenje na absurd)
- 7) $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$ γ (De Morganovi zakoni)
- 8) $\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$
- 9) $((p \Rightarrow q) \wedge p) \Rightarrow q$ (modus ponens)
- 10) $((p \Rightarrow q) \wedge \neg q) \Rightarrow \neg p$ (modus tollens)

Skraćenja:

$$O \vee F = F$$

$$1 \vee F = 1$$

$$O \wedge F = O$$

$$1 \wedge F = F$$

$$O \Rightarrow F = 1$$

$$1 \Rightarrow F = F$$

$$F \Rightarrow 1 = 1$$

$$F \Rightarrow O = \neg F$$

$$1 \Leftarrow F = F$$

$$O \Leftarrow F = \neg F$$

$$O \vee \underline{F} = F$$

$$1 \vee \underline{F} = \neg F$$

Prvomana iskazne logike

1. Većeras je organizovana žurka o kojoj
znamo:

- 1) Ako dođe E, doći će H i D
- 2) Ako ne dođe G, doći će D i B
- 3) Ako dođe H, doći će F i D
- 4) Ako ne dođe G, neće doći C i F
- 5) Ako dođu A i B, doći će G
- 6) Ako ne dođu G i H, neće doći C
- 7) Ako dođe B i ne dođe F, neće doći C
- 8) Ne dolazi G.

Odrediti ko dolazi, a ko ne.

Neka je p iskaz „Osoba P dolazi na žurku“.

- 1) $e \Rightarrow (h \wedge d)$ = 1
 - 2) $\neg g \Rightarrow (d \wedge b)$ = 1
 - 3) $h \Rightarrow (f \wedge d)$ = 1
 - 4) $\neg g \Rightarrow (\neg c \wedge \neg f)$ = 1
 - 5) $(a \wedge b) \Rightarrow g$ = 1
 - 6) $(\neg g \wedge \neg h) \Rightarrow \neg c$ = 1
 - 7) $(b \wedge \neg f) \Rightarrow \neg c$ = 1
 - 8) $\neg g$ = 1 $\Leftrightarrow g = 0$
- | z 2) imamo $(d \wedge b) = 1$, dakle $d = 1$ i $b = 1$
| z 4) imamo $(\neg c \wedge \neg f) = 1$, dakle $\neg c = 1$ i $\neg f = 1$
| tj. $c = 0$ i $f = 0$

- | z 5) $a \wedge b = 0$, ali $b = 1$, pa mora biti $a = 0$
| z 3) imamo $f \wedge d = 0 \wedge 1 = 0$, pa je $h = 0$
| z 1) imamo $h \wedge d = 0 \wedge 1 = 0$, pa je $e = 0$

Dolaze B i D.

Ne dolaze A, C, E, F, G, H.

Ostrva

Imaće 4 vrste plemena:

- 1) Istinožborci (Vernici) - uvek govore istinu
- 2) Lažovi (Nevernici) - uvek lažu
- 3) Špijuni - govore istinu osobama iz svog plemena, a ostale lažu
- 4) Dvupli Agenti - lažu osobe iz svog plemena, a ostalima govore istinu

Posmatramo situaciju kada se na ostrvu nalaze 2 plemena i slušamo razgovor osobe A i osobe B. Zanima nas istinitosua vrednost iskata p koji je izgovoren od strane osobe A osobi B u zavisnosti od toga iž kojih su plemena one dve osobe.

(I) Ostrvo Istinožboraca i Lažova

$$a = \text{"A je Istinožborac"}$$

$$b = \text{"B je Istinožborac"}$$

a	b	p	$a \Leftrightarrow p = 1$
0	0	0	
0	1	0	
1	0	1	
1	1	1	

(II) Ostrvo Špijuna i Lažova

$$a = \text{"A je Špijun"}$$

$$b = \text{"B je Špijun"}$$

a	b	p	$a \wedge b \Leftrightarrow p = 1$
0	0	0	
0	1	0	
1	0	0	
1	1	1	

III

Ostrovo Istinozboraca i Duplicih Agenata

a = „A je Istinozborac“

b = „B je Istinozborac“

a	b	p
0	0	0
0	1	1
1	0	1
1	1	1

$$\boxed{a \vee b \Leftrightarrow p = 1}$$

IV

Ostrovo Istinozboraca i Špijuna

a = „A je Istinozborac“

b = „B je Istinozborac“

a	b	p
0	0	1
0	1	0
1	0	1
1	1	1

$$(b \Rightarrow a) \Leftrightarrow p$$

V

Ostrovo severnih i Južnih Špijuna

a = „A je Severni Špijun“

b = „B je Severni Špijun“

a	b	p
0	0	1
0	1	0
1	0	0
1	1	1

$$\boxed{(a \Leftrightarrow b) \Leftrightarrow p = 1}$$

VI

Ostrovo Severnih i Južnih Duplicih Agenata

a = „A je Severni Dupli Agent“

b = „B je Severni Dupli Agent“

a	b	p
0	0	0
0	1	1
1	0	1
1	1	0

$$\boxed{(a \vee b) \Leftrightarrow p = 1}$$

VII

Ostrvo Špijuna i Duplih Agenata

a = "A je Špijun"

b = "B je Špijun"

a	b	p
0	0	0
0	1	1
1	0	0
1	1	1

$$\boxed{b \Leftrightarrow p = 1}$$

VIII

Ostrvo Lazova i Duplih Agenata

a = "A je Lazov"

b = "B je Lazov"

a	b	p
0	0	0
0	1	1
1	0	0
1	1	0

$$\boxed{(a \wedge b) \Leftrightarrow p = 1}$$

a = "A je Dupli Agent"

b = "B je Dupli Agent"

a	b	p
0	0	0
0	1	0
1	0	1
1	1	0

$$\boxed{(a \wedge b) \Leftrightarrow p = 1}$$

2. Nalazimo se na ostrvu Špijuna i Lažova.

- 1) $A \rightarrow B$ "Ako je C Lažov, onda je H Špijun"
- 2) $B \rightarrow C$ "Ako je F Špijun, onda je A Lažov"
- 3) $C \rightarrow D$ "Ako je A Lažov, tada je B Lažov"
- 4) $E \rightarrow F$ "Ako je B Lažov, onda je C Špijun"
- 5) $F \rightarrow G$ "Ili je D Špijun, ili je A Lažov".
 $P =_{\text{def}} \text{Osoba } P \text{ je Špijun}"$

- 1) $(a \wedge b) \Leftrightarrow (\neg c \Rightarrow h) = 1$
- 2) $(b \wedge c) \Leftrightarrow (f \Rightarrow \neg a) = 1$
- 3) $(c \wedge d) \Leftrightarrow (\neg a \Rightarrow \neg b) = 1$
- 4) $(e \wedge f) \Leftrightarrow (\neg b \Rightarrow c) = 1$
- 5) $(f \wedge g) \Leftrightarrow (d \vee \neg a) = 1$

Diskutujemo po slouvu a:

$$\begin{aligned} 1^{\circ} \quad a=0 &\Rightarrow \neg a=1 \\ 1 \neq 1) \quad a \wedge b=0, \text{ pa je} \\ \neg c \Rightarrow h=0, \text{ tj.} \\ \neg c=1 \text{ i } h=0 \\ \underline{c=0 \text{ ; } h=0} \\ 1 \neq 2) \quad f \Rightarrow \neg a = f = 1 = 1 \\ b \wedge c = 1 \\ b=1 \quad \underline{c=1} \end{aligned}$$

$$\begin{aligned} 2^{\circ} \quad a=1 &\Rightarrow \neg a=0 \\ 1 \neq 3) \quad \text{je } \neg a \Rightarrow \neg b = 0 \Rightarrow \neg b=1, \\ \text{pa je } c \wedge d=1, \text{ tj.} \\ c=1 \text{ i } d=1 \\ 1 \neq 4) \quad \text{je } \neg b \Rightarrow c = \neg b \Rightarrow 1 = 1, \\ \text{pa je } e \wedge f=1, \text{ tj. } e=1 \text{ i } f=1 \\ 1 \neq 1) \quad \text{je } \neg c \Rightarrow h = 0 \Rightarrow h=1, \\ \text{pa je } a \wedge b=1, \text{ tj. } a=1 \text{ i } b=1 \\ 1 \neq 2) \quad b \wedge c = 1 \wedge 1 = 1 \\ f \Rightarrow \neg a = 1 \Rightarrow 0 = 0 \\ 1 \Leftrightarrow 0 = 1 \end{aligned}$$

Zadatak nema rešenje.

3. Nalazimo se na ostrvu Severnih i Južnih Špijuna

- 1) $A \rightarrow B$ "F je Južni i C je Južni"
- 2) $B \rightarrow C$ "E i F nisu istog plemena"
- 3) $C \rightarrow D$ "A i B su Severni"
- 4) $D \rightarrow E$ "A i F su Severni"

- 1) $(a \Leftrightarrow b) \Leftrightarrow (\neg f \wedge \neg c)$ = 1
 2) $(b \Leftrightarrow c) \Leftrightarrow (e \vee f)$ = 1
 3) $(c \Leftrightarrow d) \Leftrightarrow (a \wedge b)$ = 1
 4) $(d \Leftrightarrow e) \Leftrightarrow (a \wedge f)$ = 1

Diskutujemo po sloupu a

1^o a = 0

Iz ③) $a \wedge b = 0 \wedge b = 0$
 pa je $c \Leftrightarrow d = 0$, tj.
 C i D su iz razlicitih
 plemena.
 Iz ④) $a \wedge f = 0 \wedge f = 0$
 pa je $d \Leftrightarrow e = 0$, tj.
 D i E su iz razlicitih
 plemena.

a) $d = 1$
 $c = 0$
 $e = 0$

$f = 1$
 1) $(0 \Leftrightarrow b) \Leftrightarrow (0 \wedge 1)$
 $(0 \Leftrightarrow b) \Leftrightarrow 0$
 $b = 1$
 2) $(1 \Leftrightarrow 0) \Leftrightarrow (0 \vee 1)$
 $0 \Leftrightarrow 1$

$1 \Leftrightarrow 0$

$f = 0$
 1) $(0 \Leftrightarrow b) \Leftrightarrow$
 $(1 \wedge 1)$
 $b = 0$
 2)

$0 \Leftrightarrow 0$

Iz ①) $\neg f \wedge \neg c =$
 $\neg f \wedge 0 = 0$
 pa je
 $a \Leftrightarrow b = 0$
 pa je $b = 1$

Iz ②) $(1 \Leftrightarrow 1) \Leftrightarrow (1 \vee f)$

$1 \Leftrightarrow 1 \vee f$

pa je $f = 0$

Jeste konzistentno

- 2^o a = 1
- 1) $b \Leftrightarrow (\neg f \wedge \neg c)$
 2) $(b \Leftrightarrow c) \Leftrightarrow (e \vee f)$
 3) $(c \Leftrightarrow d) \Leftrightarrow b$
 4) $(d \Leftrightarrow e) \Leftrightarrow f$

a) $b = 1$

- 1) $\neg f \wedge \neg c = 1$
 $\neg f = 1 \quad \neg c = 1$
 $f = 0 \quad c = 0$
 2) $(1 \Leftrightarrow 0) \Leftrightarrow (e \vee 0)$
 $0 \Leftrightarrow (e \vee 0)$
 $e = 0$
 3) $(b \Leftrightarrow d) \Leftrightarrow 1$
 $d = 0$
 4) $(0 \Leftrightarrow 0) \Leftrightarrow 0$
 $1 \Leftrightarrow 0$

✓

b) $b = 0$

$f = 1$

$0 \Leftrightarrow (0 \wedge \neg c)$

$0 \Leftrightarrow 0$

Iz 3)

$c \Leftrightarrow d = 0$, tj.

C i D su iste

razlicitih

Iz 4)

$(d \Leftrightarrow e) \Leftrightarrow 1$, tj.

E i D su iste

istih plemena

X

$d = 0$

$e = 0$

$c = 1$, 2)

$(0 \Leftrightarrow 1) \Leftrightarrow 1$

$0 \Leftrightarrow 1$

$1 \Leftrightarrow 0$

✓

$f = 0$
 Stoga, $\neg c = 0$
 tj. $c = 1$

2) $(0 \Leftrightarrow 1) \Leftrightarrow (e \vee 0)$
 $0 \Leftrightarrow (e \vee 0)$

tj. $e = 0$

3) $(1 \Leftrightarrow d) \Leftrightarrow 0$
 $d = 0$

4) $(0 \Leftrightarrow 0) \Leftrightarrow 0$

$1 \Leftrightarrow 0$

✓

Dakle, $a = 0, b = 1, c = 1, d = 0, e = 1, f = 0$

4. Ostvovo Istinozboraca i Latova

- 1) A: „C je Istinozborac, D je Latov“
- 2) B: „Tačno jedan od A i F je Istinozborac“ (xor)
- 3) C: „H i E nisu iz istog plemena“ (xor)
- 4) D: „A i G su iz istog plemena“
- 5) E: „F i C nisu iz istog plemena“
- 6) F: „Bar jedan od B i H je Latov“.