Diskretne strukture 1

10. čas: Kontinuum. Aritmetika.

Skupovi moći kontinuuma

Definicija. $|\mathbb{N}| =: \aleph_0$. Skup A je prebrojiv ako je $|A| = \aleph_0$.

Primeri. $|\mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{Q}| = \aleph_0$.

Definicija. $|\mathbb{R}| =: \mathfrak{c}$. Skup A je moći kontinuuma ako je $|A| = \mathfrak{c}$.

Primeri.

- svi intervali su moći kontinuuma;
- $\mathbb{R} \times \mathbb{R}$ je moći kontinuuma;
- $\mathbb{C}$ je moći kontinuuma;
- $\mathcal{P}(\mathbb{N})$ je moći kontinuuma; po Kantorovoj teoremi, $\aleph_0 < \mathfrak{c}$.

Kantorov dijagonalni argument

Teorema. $(0,1)$ nije prebrojiv, pa $\aleph_0 < \mathfrak{c}$.

Zadatak. Neka je $A \subseteq \mathbb{R}$ prebrojiv skup. Dokazati da postoji $b \in \mathbb{R}$ tako da $A \cap (b + A) = \varnothing$.

Zadatak. Neka je $\mathcal{F}$ familija krugova u ravni takva da se nikoja dva kruga iz familije ne seku. Dokazati da je $\mathcal{F}$ najvišre prebrojiva.

Relacija deljivosti

Definicija. Relacija deljivosti na skupu $\mathbb{Z}$ definisana je sa $m \mid n$ akko $n = qm$ za neko $q \in \mathbb{Z}$.

Osobine.

(i) za sve $n \in \mathbb{Z}$ važi $n \mid n$ – refleksivnost;

(ii) ako $k \mid m$ i $m \mid n$, onda $k \mid n$ – tranzitivnost;

(iii) za sve $n \in \mathbb{Z}$ važi $1 \mid n$ i $-1 \mid n$;

(iv) za sve $n \in \mathbb{Z}$ važi $n \mid 0$;

(v) ako $n \mid 1$ ili $n \mid -1$, onda $n = 1$ ili $n = -1$;

(vi) ako $0 \mid n$, onda $n = 0$;

(vii) ako $k \mid m$ i $k \mid n$, onda $k \mid am + bn$ za sve $a, b \in \mathbb{Z}$;

(viii) ako $m \mid n$, onda $am \mid an$ za sve $a \in \mathbb{Z}$;

(ix) ako $am \mid an$ i $a \neq 0$, onda $m \mid n$;

(x) ako $m \mid n$ i $n \neq 0$, onda $|m| \leqslant |n|$.

Lema o ostatku

Teorema. Neka su $a, b \in \mathbb{Z}$, $b > 0$. Tada postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da $a = qb + r$ i $0 \leqslant r < b$.

Jedinstveni broj q je *količnik* pri celobrojnom deljenju a sa b, a jedinstveni broj r je *ostatak* pri celobrojnom deljenju a sa b.

Posledica. Neka su $a, b \in \mathbb{Z}$, $b \neq 0$. Tada postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da $a = qb + r$ i $0 \leqslant r < |b|$.

Prosti brojevi

Definicija. Broj $p \in \mathbb{N}$ je *prost* ako $p \neq 1$ i važi:

$$(\forall a, b \in \mathbb{N})(p \mid ab \to p \mid a \wedge p \mid b).$$

Lema. Neka $p, d \in \mathbb{N}$, p je prost i $d \mid p$, onda $d = 1$ ili $d = p$.

Teorema. Postoji beskonačno mnogo prostih brojeva.

Osnovna teorema aritmetike. Svaki broj $n > 1$ se na jedinstven način može zapisati kao proizvod prostih.

NZD i NZS

Definicija. Broj $d \in \mathbb{N}$ je NZD brojeva a i b, $d = (a, b)$, ako:

- $d \mid a$ i $d \mid b$;
- ako $e \mid a$ i $e \mid b$, onda i $e \mid d$.

Broj $s \in \mathbb{N}$ je NZS brojeva a i b, $d = [a, b]$, ako:

- $a \mid s$ i $b \mid s$;
- ako $a \mid t$ i $b \mid t$, onda i $s \mid t$.

Osobine. Neka $a, b \in \mathbb{N}$.

- $(a, b) = a$ akko $a \mid b$ akko $[a, b] = b$;
- $(a, 0) = a$ i $[a, 0] = 0$;
- $(1, b) = 1$ i $[1, b] = b$;
- $ab = (a, b)[a, b]$.

Bezuova lema

Teorema. Neka $a, b \in \mathbb{N}$. Postoje $p, q \in \mathbb{Z}$ tako da $pa + qb = (a, b)$.

Dokaz. Euklidov algoritam...