TEORIJA BROJEVA

djeljivost i kongruencije

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

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Kažemo da broj $a \in \mathbb{N}$ **dijeli** broj $b \in \mathbb{N}$ ako postoji broj $k \in \mathbb{N}$ takav da je $b = ka$.

Zapis: $a \mid b$

b je djeljiv s a, a je djelitelj (divizor) od b,

b je višekratnik od a.

Ako $a \in \mathbb{N}$ ne dijeli $b \in \mathbb{N}$, pišemo $a \nmid b$.

paran broj, neparan broj

Svojstva:

a) $\forall a \in \mathbb{N}, \quad a \mid a$

b) $\forall a, b \in \mathbb{N}, \quad a \mid b \;\text{ i }\; b \mid a \;\Rightarrow\; a = b$

c) $\forall a, b, c \in \mathbb{N}, \quad a \mid b \;\text{ i }\; b \mid c \;\Rightarrow\; a \mid c$

djeljivost je parcijalni uređaj, ali ne potpuni uređaj

a) $\forall a \in \mathbb{N}, \quad a \mid a \qquad\qquad a = 1 \cdot a$

b) $\forall a, b \in \mathbb{N}, \quad a \mid b \;\text{ i }\; b \mid a \;\Rightarrow a = b$

$b = k \cdot a,\ a = l \cdot b \;\ldots\; b = kl \cdot b \;\ldots\; k \cdot l = 1 \;\ldots$

$k = l = 1 \;\ldots\; a = b$

c) $\forall a, b, c \in \mathbb{N}, \quad a \mid b \;\text{ i }\; b \mid c \;\Rightarrow\; a \mid c$

$b = k \cdot a,\ c = l \cdot b \;\ldots\; c = lk \cdot a \;\ldots\; a \mid c$

Svojstva:

d) $\forall a, b, c \in \mathbb{N}, \quad a \mid b \;\text{ i }\; a \mid c \;\Rightarrow\; a \mid b + c$

e) $\forall a, b, c \in \mathbb{N}, \quad a \mid b \;\Rightarrow\; a \mid bc$

$b = k \cdot a,\ c = l \cdot a \quad \ldots \quad b + c = ka + la = (k + l)a$

$\ldots \quad a \mid b + c$

$b = k \cdot a \quad \ldots \quad bc = (ka)c = (kc) \cdot a \ \ldots \quad a \mid bc$

Djeljivost na skupu $\mathbb{Z}$

Svojstva:

a) $\forall a \in \mathbb{Z} \setminus \{0\}, \quad a \mid a$

b) $\forall a, b \in \mathbb{Z}, \quad a \mid b \;\text{ i }\; b \mid a \;\Rightarrow\; a = \pm b$

c) $\forall a, b, c \in \mathbb{Z}, \quad a \mid b \;\text{ i }\; b \mid c \;\Rightarrow\; a \mid c$

d) $\forall a, b, c \in \mathbb{Z}, \quad a \mid b \;\text{ i }\; a \mid c \;\Rightarrow\; a \mid b \pm c$

e) $\forall a, b, c \in \mathbb{Z}, \quad a \mid b \;\Rightarrow\; a \mid bc$

Teorem o dijeljenju s ostatkom

Za svako $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ postoje jedinstveni brojevi $q, r \in \mathbb{Z}$ takvi da je

$$0 \leq r < b \qquad \text{i} \qquad a = qb + r.$$

Primjer:

$29 : 7 = 4$ i ost. $1 \quad 29 = 4 \cdot 7 + 1 \quad q = 4,\ r = 1$

$(-29) : 7 \quad -29 = (-5) \cdot 7 + 6 \quad q = -5,\ r = 6$

Prirodan broj $p > 1$ koji je djeljiv samo s 1 i samim sobom zove se **prost broj** ili **prim broj**.

Ostali prirodni brojevi zovu se **složeni brojevi**.

Broj 1 nije ni prost ni složen.

$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots\}$

Eratostenovo sito.

Teorem: Prostih brojeva ima beskonačno mnogo.

Lema: Svaki prirodan broj veći od 1 može se prikazati kao umnožak od jednog ili više prostih brojeva.

Teorem (osnovni teorem aritmetike)
Za svaki prirodan broj $n > 1$ postoje jedinstveni $k \in \mathbb{N}$, prosti $p_1 < p_2 < \ldots < p_k$ i $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ takvi da je

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Kongruencije (Gauss)

Neka su $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$.

Kažemo da je a **kongruentno** b **modulo** n i pišemo $a \equiv b \pmod{n}$ ako $n \mid a - b$.

$17 \equiv 32 \pmod{5}$, $17 \equiv -3 \pmod{5}$,

$17 \equiv 26 \pmod{3}$, $17 \not\equiv 26 \pmod{5}$

Svojstva: Neka je $n \in \mathbb{N}$.

a) $\forall a \in \mathbb{Z}, \quad a \equiv a \,(\text{mod } n)$

b) $\forall a, b \in \mathbb{Z}, \quad a \equiv b \,(\text{mod } n) \;\Rightarrow\; b \equiv a \,(\text{mod } n)$

c) $\forall a, b, c \in \mathbb{Z}, \quad a \equiv b \,(\text{mod } n)$ i $b \equiv c \,(\text{mod } n)$

$\Rightarrow \;\; a \equiv c \,(\text{mod } n)$

Relacija $\equiv (\text{mod } n)$

je relacija ekvivalencije na skupu $\mathbb{Z}$

Klase ekvivalencije

$$a \equiv b \,(\mathrm{mod}\ n) \ \Rightarrow\ n \mid b-a \ \Rightarrow\ b-a = kn,\ k \in \mathbb{Z}$$

$$\Rightarrow\ b = a + kn,\ k \in \mathbb{Z}$$

Klasa ostataka modulo n

$$[a] = \{a + kn \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}$$

Propozicija: Postoji točno n različitih klasa ostataka modulo n.

Potpun sustav ostataka modulo 5

je skup $\{0, 1, 2, 3, 4\}$, ali i $\{15, 26, 32, -12, 44\}$

Svojstva: Neka je $n \in \mathbb{N}$ i $a, b, c, d \in \mathbb{Z}$ takvi da vrijedi $a \equiv c \pmod{n}$ i $b \equiv d \pmod{n}$.
Tada

$$a + b \equiv c + d \pmod{n},$$

$$a\,b \equiv c\,d \pmod{n}.$$