PETI TJEDAN

1. **Za cijele brojeve a i b definirati relaciju "a dijeli b". (Propoziciju 1, na str. 44 ćemo raditi nakon poglavlja Binarne relacije).**

Neka su a i b cijeli brojevi. Kažemo da **a dijeli b** ako je a ≠ 0 i b je višekratnik od a tj. postoji k ∈ Z tako da je b = ka. Pišemo a|b i čitamo "a dijeli b". Broj a zovemo djeliteljem broja b, a broj b višekratnik broja a.

Primjer Ako su $a, b, c \in \mathbb{Z}$, onda iz $a\,|b$ i $a\,|c$ slijedi $a\,|(nb + mc)$ za bilo koja dva cijela broja m i n.

Primjer 1. $a|b$ i $a|c \Rightarrow a|n\cdot b+m\cdot c$, $\quad a,b,c,m,n \in \mathbb{Z}$

Dokaz: $a|b \overset{Def.}{\Longrightarrow} (\exists k\in\mathbb{Z})\,\boxed{b=k\cdot a}$

$a|c \overset{def.}{\Longrightarrow} (\exists l\in\mathbb{Z})\,\boxed{c=l\cdot a}$ } pp-ke

$$n\cdot b+m\cdot c = n\cdot(k\cdot a)+m\cdot(l\cdot a) = \underbrace{(nk+ml)}_{\in\mathbb{Z}}a \overset{def.}{\Longrightarrow} a\,|\,nb+mc$$

npr. $2|6$ i $2|8$

$2\,|\,6\cdot3+8\cdot5$

2. **Definirati pojmove: najveća zajednička mjera i najmanji zajednički višekratnik te navesti njihova svojstva (Primjeri 2, 3 i 4 iz udžbenika).**

Definicija Ako su $a, b, d \in \mathbb{Z}$ takvi da je $d\,|a$ i $d\,|b$, onda d nazivamo *zajedničiki djelitelj* od a i b.

Ako je barem jedan od brojeva a i b različit od 0, onda postoji i najveći zajednički djelitelj kojeg nazivamo *najveća zajednička mjera (Nzm)* od a i b i označavamo sa $M(a,b)$ ili $Nzm(a,b)$.

Ako su brojevi a i b različiti od 0, onda najmanji prirodan broj čiji su a i b djelitelji nazivamo *najmanji zajednički višekratnik (nzv)* od a i b i označavamo sa $v(a,b)$ ili $nzv(a,b)$.

Svojstva su u primjeru:

Primjer:

- $Nzm(a, b) > 0$;
- $Nzm(a, 0) = a$, za sve $a \in \mathbb{N}$;
- $Nzm(a, b) = Nzm(b, a) = Nzm(|a|, |b|)$
  $nzv(a, b) = nzv(b, a) = nzv(|a|, |b|)$
- Ako su $a, b \in \mathbb{N}$ onda je

  $$Nzm(a, b) \leq \min\{a, b\} \leq \max\{a, b\} \leq nzv(a, b);$$

- Ako je $a \in \mathbb{N}$ i $b \in \mathbb{Z}$ onda

  $$a \,|b \Longrightarrow Nzm(a, b) = a.$$

Napomena: Na sličan način možemo definirati, za bilo koji konačan skup cijelih brojeva $a_1, a_2, ..., a_n$, $Nzm(a_1, a_2, ..., a_n)$ i $nzv(a_1, a_2, ..., a_n)$.

3. **Ako su u jednakosti $a_1 + a_2 + \ldots + a_r = b_1 + b_2 + \ldots + b_s$ svi navedeni cijeli brojevi, osim jednoga, djeljivi nekim prirodnim brojem d, dokazati da onda i taj jedan cijeli broj mora biti djeljiv s d.**

Propozicija 2 Neka su $a_1, a_2, ..., a_r$ i $b_1, b_2, ..., b_s$ cijeli brojevi i neka je

$$a_1 + a_2 + \ldots + a_r = b_1 + b_2 + \ldots + b_s.$$

Ako su svi gornji brojevi djeljivi s $d \in \mathbb{N}$ osim jednog onda je i taj broj djeljiv s d.

Prop. 2. (1) $a_1 + a_2 + \cdots + a_m = b_1 + b_2 + \cdots + b_n$

$i = 2, \ldots, m,\ j = 1, \ldots, n \Rightarrow a_i, b_j$ su djeljivi sa $d \in \mathbb{N}$

osim npr. a_1

T: a_1 mora biti djeljiv sa d tj. $\boxed{d \,|\, a_1}$

Dokaz: Iz (1) slijedi $a_1 = \underbrace{b_1 + b_2 + \cdots + b_n - a_2 - \cdots - a_m}_{\text{svi su djeljivi sa } d}$ // (2)

onda je i ova njihova lin. komb. također djeljiva sa d zbog PRIMJERA 1

$a|b$ i $a|c \Rightarrow a \,|\, nb + mc$

$\Rightarrow$ Iz (2) slijedi $d \,|\, a_1$ □

Pomnožili sa cijelim brojevima (neke s 1 neke s -1) i povezali u linearnu kombinaciju.

Mogli smo izraziti bilo koji broj umjesto a_1.

4. Iskazati i dokazati teorem o dijeljenju.

Teorem 1 (o dijeljenju) Neka su dani $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ onda postoje jedinstveni cijeli brojevi q i r, $0 \le r < b$, takvi da je

$$a = bq + r.$$

Broj q se naziva <u>*kvocijent*</u> pri dijeljenju a i b, a r <u>*ostatak*</u>.

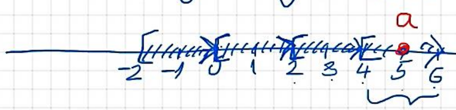
∃! – postoji jedinstveni

Dokaz se provodi u dva koraka: prvo dokazujemo egzistenciju; postoje q i r takvi da teorem vrijedi, a onda dokazujemo jedinstvenost brojeva q i r.

Tm o dijeljenju: $\boxed{a \in \mathbb{Z},\ b \in \mathbb{N}}$

T: $\exists!\ q, r \in \mathbb{Z}$, $a = b\cdot q + r$, $0 \le r < b$.

Dokaz: (i) Egzistencija: neka su zadani $a \in \mathbb{Z}$, $b \in \mathbb{N}$ npr. $a = 5$, $b = 2$



$\mathbb{Z}$ ćemo podijeliti na poluotvorene intervale $I_k = [kb, (k+1)b\rangle$, $k \in \mathbb{Z}$

$k=0$ $I_0 = [0,2\rangle$
$k=1$ $I_1 = [2,4\rangle$
$k=2$ $I_2 = [4,6\rangle$
$k=-1$ $I_{-1} = [-2,0\rangle$

Sada $a \in I_k$ za neki k npr. za $k = q$ tj. $\boxed{a \in I_q}$

$I_q = [qb, (q+1)b\rangle$ pa ako je $a \in I_q = [qb, (q+1)b\rangle$ onda je $\Rightarrow a = 5 \in I_2$

$qb \le a < (q+1)\cdot b$

$qb \le a < qb + b \quad / -qb$

$0 \le \underbrace{a - qb}_{:=r} < b \Rightarrow a - qb = r \Rightarrow \boxed{a = qb + r}$ i $0 \le r < b$

B može biti i cijeli broj nego je uzet prirodan zbog jednostavnosti zapisivanja (bili bi drugačiji predznaci).

(ii) Jedinstvenost: pp-mo suprotno tj. neka postoje q, r i q_1, r_1 t.d. vrijedi:

$0 \le r < b$
$0 \le r_1 < b$

$$\begin{cases} a = bq + r \\ a = bq_1 + r_1 \end{cases} \quad / -$$

$$0 = b(q - q_1) + r - r_1$$

$|r - r_1| \in \{0, 1, \dots, b-1\}$

$\boxed{r - r_1 = b\underbrace{(q_1 - q)}_{\in\mathbb{Z}}} \Rightarrow$ (def. rel. dijeli) $b \mid r - r_1$

$b \mid (r - r_1) \Rightarrow r - r_1$ je višekratnik od b

$b \mid 0 \Rightarrow r - r_1 = 0 \Rightarrow \boxed{r = r_1}$

$\Downarrow$ $0 = b(q_1 - q)$

$\Rightarrow q_1 - q = 0$

$\boxed{q_1 = q}$

$\Rightarrow$ q i r su jedins

5. **Iskazati i dokazati teorem koji daje Euklidov algoritam za nalaženje najveće zajedničke mjere i propoziciju na kojoj se taj algoritam zasniva.**

Propozicija 4 Neka su $a, b, q, r \in \mathbb{Z}$ i $a = bq + r$. Onda je svaki zajednički djelitelj od a i b ujedno i zajednički djelitelj od b i r. Posebno vrijedi $Nzm(a, b) = Nzm(b, r)$.

Teorem 2 (Euklidov algoritam za nalaženje Nzm) Neka su dani $a \in \mathbb{Z}$ i $b \in \mathbb{N}$. Pretpostavimo da je uzastopnom primjenom Teorema1 dobiven niz jednakosti

$$
\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < b \\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \qquad (*) \\
&\vdots \\
r_{k-2} &= r_{k-1} q_k + r_k, \quad 0 < r_k < r_{k-1} \\
r_{k-1} &= r_k q_{k+1}.
\end{aligned}
$$

Tada je $Nzm(a, b) = r_k$, tj. $Nzm(a, b)$ jednako je posljednjem ostatku različitom od 0. Nadalje, postoje brojevi $s, t \in \mathbb{Z}$ takvi da je

$$Nzm(a, b) = r_k = sa + tb, \qquad (**)$$

tj. r_k se može izraziti kao linearna kombinacija od a i b.

Nastavljamo s dijeljenjem sve dok ostatak nije = 0.

PROP. 1 (udžb. str. 46) $\quad a = bq + r$

Dokaz: $d \mid a$ i $d \mid b \Rightarrow d \mid r$

$a = bq + r \Rightarrow r = \underbrace{a - bq}_{\text{lin. komb.}}$

Prema Pr. 1.

$d \mid a$ i $d \mid b$

$\Rightarrow d \mid \underbrace{a - bq}_{r} \Rightarrow d \mid r$

$\Rightarrow Nzm(a, b) = Nzm(b, r)$

Za Euklidov algoritam:

DOKAZ. Iz gornjih nejednakosti vidimo da je slijed r_k opadajuć: $b > r_2 > r_3 > r_4 > \ldots \geqslant 0$. Kako je slijed omeđen odozdol s nulom, te kako se radi o cijelim brojevima, onda mora postajati indeks za koji će odgovarajući r biti jednak nula, recimo $r_{k+1} = 0$, a prethodni $r_k > 0$, gdje je

$$\begin{aligned} r_{k-2} &= r_{k-1}q_{k-1} + r_k \quad 0 < r_k < r_{k-1}, \\ r_{k-1} &= r_k q_k. \end{aligned} \tag{1'}$$

Prema prethodnoj propoziciji imamo $\mathrm{Nzm}(a,b) = \mathrm{Nzm}(b,r_2)$, $\mathrm{Nzm}(b,r_2) = \mathrm{Nzm}(r_2,r_3)$, $\mathrm{Nzm}(r_2,r_3) = \mathrm{Nzm}(r_3,r_4), \ldots, \mathrm{Nzm}(r_{k-2},r_{k-1}) = \mathrm{Nzm}(r_{k-1},r_k)$. Prema tome je $\mathrm{Nzm}(a,b) = \mathrm{Nzm}(r_{k-1},r_k) = r_k$, gdje smo u zadnjoj jednakosti koristili činjenicu da $r_k \mid r_{k-1}$. Q.E.D.

Napomena

- U Euklidovom algoritmu smo pretpostavili da je $b > 0$ što nije bitno ograničenje jer je $Nzm(a,b) = Nzm(|a|,|b|)$;

- ako su $a, b \in \mathbb{N}$ i $a < b$, onda u prvom koraku imamo $a = b \cdot 0 + a$, pa a i b zamijene mjesta.

- Primijetimo da je

$$\left\lfloor \frac{a}{b} \right\rfloor = q_1, \quad \left\lfloor \frac{b}{r_1} \right\rfloor = q_2, \quad \left\lfloor \frac{r_1}{r_2} \right\rfloor = q_3 \ \ldots,$$

  gdje je $\lfloor x \rfloor$ *najveći cijeli dio* od x, tj. $\lfloor x \rfloor = q$ gdje je q najveći cijeli broj $\leq x$.

- Brojevi $s, t \in \mathbb{Z}$ u (**) nisu jednoznačno određeni, jer je npr.

$$Nzm(a,b) = sa + tb = (s+b)\,a + (t-a)\,b,$$

Posljedica 1 Neka su $a, b \in \mathbb{Z}$ i $d \in \mathbb{N}$ takvi da $d \mid a$ i $d \mid b$. Onda $d \mid Nzm(a,b)$.

6. Definirati pojam relativno prostih brojeva te dokazati:

Za cijele brojeve a i b kažemo da su **relativno prosti** ako je Nzm (a, b) = 1, tj. jedini zajednički djelitelj im je 1.

a) ako su a, b, c ∈ Z takvi da su a i b relativno prosti i b|ac onda b|c,

PROP. 5 (udžb. str. 48) a i b rel. pr. i $a \mid b\cdot c$

$\Rightarrow \boxed{a \mid c}$.

Dokaz: 1) a i b rel. pr. $\overset{def.}{\Leftrightarrow}$ $\boxed{Nzm(a,b) = 1}$ $\Rightarrow$ $\exists s,t \in \mathbb{Z}$ $\underbrace{\boxed{sa + tb = 1}}_{Nzm(a,b)}$ $/\cdot c$

2) $a \mid bc$ $\Rightarrow$ $(\exists k \in \mathbb{Z})$ $\boxed{bc = ka}$

$$sac + tbc = c$$

$$sac + tka = c$$

$$a\cdot\underbrace{(s\cdot c + t\cdot k)}_{\in \mathbb{Z}\,=\,m} = c$$

$$(\exists m \in \mathbb{Z})\ c = ma \Rightarrow a \mid c$$

$\Rightarrow a \mid c$

b) ako su a, b 2 ∈ i c ∈ N onda vrijedi Nzm (ca, cb) = c· Nzm (a, b),

DOKAZ. (i) Možemo bez gubitka općenitosti pretpostaviti da je b pozitivan. U postupku provođenja Euklidova algoritma pomnožimo sve relacije u (1) sa c. Onda a i b prelaze u ca i cb, svi r-ovi u cr, dok q-ovi ostaju isti. Dobivamo dakle Euklidov algoritam za ca i cb (primijetite da je pritom $0 \leqslant cr_i < cr_{i-1}$). Prema Teoremu 2 je onda $\mathrm{Nzm}(ca, cb) = cr_k$. Međutim je $r_k = \mathrm{Nzm}(a, b)$, što dokazuje tvrdnju.

$$\begin{aligned} a &= bq_1 + r_2 & 0 &\leqslant r_2 < b, \\ b &= r_2q_2 + r_3 & 0 &\leqslant r_3 < r_2, \\ r_2 &= r_3q_3 + r_4 & 0 &\leqslant r_4 < r_3, \\ &\ \vdots \end{aligned} \qquad (1)$$

c) ako su a, b ∈ Z i c ∈ N, c|a i c|b onda je Nzm $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} \cdot$ Nzm (a, b).

(ii) Zbog (i) je $c \cdot \mathrm{Nzm}\left(\frac{a}{c}, \frac{b}{c}\right) = \mathrm{Nzm}\left(c\frac{a}{c}, c\frac{b}{c}\right) = \mathrm{Nzm}(a, b)$

7. Što su diofantske jednadžbe prvog stupnja s dvije varijable? Dokazati: diofantska jednadžba ax + by = c ima rješenje akko Nzm (a, b)|c, a, b, c ∈ Z.

Jednadžbu oblika

$$ax + by = c, \qquad (1)$$

gdje su a, b, c zadani cijeli brojevi kojoj tražimo cjelobrojna rješenja x i y nazivamo <u>Diofantska jednadžba</u> prvog stupnja s dvije varijable.

Prvi smjer:

$$\overset{a}{6}x+\overset{b}{4}y=\overset{c}{16} \Rightarrow Nzm(a,b)=2 \mid 16 = c \rightarrow \exists x_0, y_0 \in \mathbb{Z}$$

$$6x+4y=15 \qquad 2 \nmid 15 \Rightarrow \nexists x_0, y_0 \in \mathbb{Z}$$

PROP. 9 (str. 49) $ax+by=c$ ima cjelobr. rj. $\Leftrightarrow Nzm(a,b) \mid c$.

Dokaz: $\boxed{\Rightarrow}$ pp. uz da $\boxed{\exists x_0, y_0 \in \mathbb{Z}}$ t.d. je $\boxed{ax_0+by_0 = c}$. $(*)$ Treba dz. $Nzm(a,b) \mid c$.

Vrijedi: $Nzm(a,b) \mid a$ i $Nzm(a,b) \mid b$

$(\exists k \in \mathbb{Z})\ a = k \cdot Nzm(a,b)\ / \cdot x_0 \qquad (\exists l \in \mathbb{Z})\ b = l \cdot Nzm(a,b)\ / \cdot y_0$

$ax_0 = kx_0 \cdot Nzm(a,b) \qquad + \qquad by_0 = ly_0 \cdot Nzm(a,b)$

$$\Rightarrow \underbrace{ax_0+by_0}_{(*)} = (kx_0+ly_0) \cdot Nzm(a,b)$$

$$c = (\underbrace{kx_0+ly_0}_{\in \mathbb{Z}}) \cdot Nzm(a,b) \Rightarrow Nzm(a,b) \mid c$$

Drugi smjer:

$\Rightarrow$ Neka $Nzm(a,b) \mid c$. Treba dz: $\exists x_0, y_0 \in \mathbb{Z}$ t.d. $ax_0+by_0 = c$

$(\exists k \in \mathbb{Z})\ c = k \cdot Nzm(a,b)$

$(\exists s, t \in \mathbb{Z})\ Nzm(a,b) = sa+tb$

$$c = k \cdot (sa + t \cdot b)$$

$$c = \underbrace{(k \cdot s)}_{x_0} a + \underbrace{(k \cdot t)}_{y_0} \cdot b$$

$\Rightarrow \exists\ \underbrace{x_0 = k \cdot s}_{\in \mathbb{Z}}$ i $\underbrace{y_0 = k \cdot t}_{\in \mathbb{Z}}$ takvi $ax_0+by_0 = c$

8. Spomenula, ali bez dokaza:

Teorem 4. *Neka su a i b cijeli brojevi koji nisu oba jednaki 0. Onda je minimalan pozitivan broj u skupu $S := \{sa+tb : s, t \in \mathbf{Z}\}$ jednak $Nzm(a,b)$. Drugim riječima*

$$Nzm(a,b) = \min\{sa+tb : s, t \in \mathbf{Z},\ sa+tb > 0\}.$$