Cijeli brojevi

1. Operacija dijeljenja u skupu Z i svojstva (dokazati).

Definicija: Neka su **a** i **b** cijeli brojevi. Kažemo da $a|b$ (**a** dijeli **b**) ako je $a \neq 0$ i postoji $k \in \mathbf{Z}$ takav da je $b = a\, k$. Broj **a** zovemo djeliteljem broja **b**, dok broj **b** zovemo višekratnikom broja **a**.

Propozicija: Operacija dijeljenja u skupu **Z** ima slijedeća svojstva:

a) Refleksivnost: $a|a \quad \forall a \neq 0$

b) Antisimetričnost: $a|b \wedge b|a \Longrightarrow a = \pm b$

c) Tranzitivnost: $a|b \wedge b|c \Longrightarrow a|c$

Dokaz:

a) Vrijedi: $a = a \cdot 1 \Rightarrow a|a$

b) $$\begin{aligned} a|b \wedge b|a &\Rightarrow b = k\cdot a \text{ i } a = \ell\cdot b \\ &\Rightarrow b = k\cdot\ell\cdot b \\ &\Rightarrow k\cdot\ell = 1 \\ &\Rightarrow k = \ell = \pm 1 \\ &\Rightarrow a = \pm b \end{aligned}$$

c) $$\begin{aligned} a|b \wedge b|c &\Rightarrow b = k\cdot a \text{ i } c = \ell\cdot b \\ &\Rightarrow c = k\cdot\ell\cdot a \\ &\Rightarrow a|c \end{aligned}$$

2. Zajednički djelitelj, najveća zajednička mjera i najmanji zajednički višekratnik dvaju (ili više) cijelih brojeva, osnovna svojstva.

Definicija: Ako su a, b, d $\in$ **Z** takvi da **d**|a i d|b, on d a d zovemo **zajedničkim djeliteljem** od a i b.

Ako je barem jedan od brojeva a i b različit od nule, onda postoji i najveći zajednički djelitelj kojeg nazivamo **najvećom zajedničkom mjerom** od a i b i pišemo Nzm(a, b).

Ako su brojevi a i b različiti od 0, onda najmanji prirodan broj čiji su a i b djelitelji zovemo **najmanjim zajedničkim višekratnikom** od a i b i pišemo nzv(a,b).

Na isti način za bilo koji konačan skup cijelih brojeva $a_1, a_2, ..., a_n$ možemo definirati $\mathrm{Nzm}(a_1, a_2, ..., a_n)$ i $\mathrm{nzv}(a_1, a_2, ..., a_n)$.

Osnovna svojstva:

- $\mathrm{Nzm}(a, b) > 0$
- $\mathrm{Nzm}(a, 0) = a$ za sve $a \in \mathbf{N}$
- $\mathrm{Nzm}(a, b) = \mathrm{Nzm}(b, a) = \mathrm{Nzm}(|a|, |b|)$
- $\mathrm{nzv}(a, b) = \mathrm{nzv}(b, a) = \mathrm{nzv}(|a|, |b|)$
- $\mathrm{Nzm}(a, b) \leq \min\{a, b\} \leq \max\{a, b\} \leq \mathrm{nzv}(a, b)$ za $a, b \in \mathbf{N}$
- $\mathbf{a} | b \Rightarrow \mathrm{Nzm}(a, b) = a$ za $a \in \mathbf{N}$ i $b \in \mathbf{Z}$

3. Teorem o dijeljenju (citirati i dokazati).

Teorem (o dijeljenu): Neka su dani $\mathbf{a} \in \mathbf{Z}$ i $\mathbf{b} \in \mathbf{N}$, onda postoje jedinstveni cijeli brojevi **q** i **r** takvi da je:

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

Broj **q** se zove **kvocijent** pri dijeljenje a sa b, a **r** ostatak.

Dokaz:

Da bismo pokazali da je rastav iskazan teoremom jedinstven, pretpostavit ćemo da pored ovog rastava postoji još jedan rastav:

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

gdje su $\mathbf{q_1}$ i $\mathbf{r_1}$ cijeli brojevi.

Tada vrijedi da je: $a = b\,q + r = b\,q_1 + r_1$

$$\Rightarrow \quad r - r_1 = b\,(q_1 - q)$$

$$\Rightarrow \quad b \mid (r - r_1)$$

Budući da je $|r - r_1| < b \;\Rightarrow\; r - r_1 = 0 \;\Rightarrow\; r_1 = r \;\Rightarrow\; q_1 = q$

4. Euklidov algoritam (citirati i dokazati teorem).

Propozicija: Neka su a, b, q, r $\in$ Z i $a = bq + r$. Onda je Nzm (a, b) = Nzm (b, r).

Teorem (Euklidov algoritam): Neka su dani $a \in Z$ i $b \in N$. Pretpostavimo da je uzastopnom primjenom teorema o dijeljenju dobiven niz jednakosti:

$$a = b \cdot q_1 + r_1 \quad , \qquad 0 < r_1 < b$$

$$b = r_1 \cdot q_2 + r_2 \quad , \qquad 0 < r_2 < r_1$$

$$r_1 = r_2 \cdot q_3 + r_3 \quad , \qquad 0 < r_3 < r_2$$

$$\vdots$$

$$r_{k-2} = r_{k-1} \cdot q_k + r_k \quad , \qquad 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_k \cdot q_{k+1}$$

Tada je Nzm (a, b) = r_k, tj. Nzm (a, b) jednako je posljednjem ostatku različitom od 0.

Dokaz: Prema prethodnoj propoziciji imamo da je:

Nzm (a, b) = Nzm (b, r_1) = Nzm (r_1, r_2) = ... = Nzm (r_{k-1}, r_k) = r_k
jer $r_k \mid r_{k-1}$.

5. Objasniti jednakost Nzm(a, b) = sa + tb.

Iz jednadžbi Euklidovog teorema:

$$
\begin{aligned}
a &= b \cdot q_1 + r_1 \quad , \qquad 0 < r_1 < b \\
b &= r_1 \cdot q_2 + r_2 \quad , \qquad 0 < r_2 < r_1 \\
r_1 &= r_2 \cdot q_3 + r_3 \quad , \qquad 0 < r_3 < r_2 \\
&\vdots \\
r_{k-2} &= r_{k-1} \cdot q_k + r_k \quad , \qquad 0 < r_k < r_{k-1} \\
r_{k-1} &= r_k \cdot q_{k+1}
\end{aligned}
$$

slijedi da je:

$$
\begin{aligned}
r_1 &= a + (-q_1)\, b \\
r_2 &= b - q_2\, r_1 = (-\, q_2)\, a + (1 + q_1\, q_2)\, b \\
&\vdots
\end{aligned}
$$

Dakle, možemo uzastopno sve ostatke izraziti kao cjelobrojnu linearnu kombinaciju **a** i **b**. Dakle, postoje brojevi s, t $\in$ **Z** takvi da je:

$$\mathrm{Nzm}(a, b) = r_k = s \cdot a + t \cdot b$$

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

Međutim, brojevi **s** i **t** nisu jednoznačno određeni, jer npr. vrijedi:

$$s\,a + t\,b = s\,a + t\,b + b\,a\ - a\,b = (s + b)\,a + (t - a)\,b = s_1 a + t_1 b$$

6. Kad kažemo da su cijeli brojevi relativno prosti?

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

Relativno prosti brojevi ne mogu se skratiti u razlomku $\frac{a}{b}$.

Npr. 9 i 4 su relativno prosti brojevi.

7. Što znamo o Diofantskoj jednadžbi ax+by = c ?
(Dokazati i ilustrirati primjerima)

Diofantska jednadžba - prvog stupnja s dvije varijable glasi:

$$a\,x + b\,y = c$$

gdje su a, b i c zadani cijeli brojevi, a traže se rješenja x i y u skupu cijelih brojeva.

Propozicija: Neka su a, b i c zadani cijeli brojevi. Diofantska jednadžba

$$a\,x + b\,y = c$$

ima rješenje onda i samo onda ako $\text{Nzm}(a, b) \mid c$.

Dokaz: Ako postoji cjelobrojno rješenje x, y promatrane Diofantske jednadžbe, onda Nzm (a, b) dijeli lijevu stranu jednadžbe pa time i desnu.

Obratno, pretpostavimo da $\quad \text{Nzm}(a, b) \mid c \quad \Rightarrow \quad c = k\cdot\text{Nzm}(a, b)$, $k \in \mathbf{Z}$.

Diofantska jednadžba: $\quad a\,x_1 + b\,y_1 = \text{Nzm}(a, b)$ ima cjelobrojno rješenje x_1, y_1.

Množenjem sa k dobivamo: $\quad a\,(k\,x_1) + b\,(k\,y_1) = k \cdot \text{Nzm}(a, b) = c$,

pa slijedi da je: $\quad x = k\,x_1, \quad y = k\,y_1$.

Primjeri:

a) Jednadžba $6x + 9y = 11$ nema rješenja jer Nzm (6, 9) = 3 ne dijeli 11.

b) Jednadžba $6x + 9y = 12$ ima rješenja jer Nzm (6, 9) = 3 | 12.

$9 = 6\cdot1 + 3$	$3 = -6 + 9$
$6 = \mathbf{3}\cdot2$	$x_1=-1$, $y_1=1$, $k = 12 / 3 = 4$
Nzm(6, 9) = 3	$x = -4$, $y = 4$

8. Što su to prosti, a što složeni brojevi? Eratostenovo sito.

Definicija: Za prirodni broj $p > 1$ kažemo da je **prost broj** (prim-broj) ako su mu jedini djelitelji 1 i p, tj. ako ima samo trivijalne djelitelje. Za prirodni broj $a > 1$ koji nije prost broj kaže se da je **složeni broj.**

Primjer: Prosti brojevi su 2, 3, 5, 7, 11, 13, ...

Ako želimo naći sve proste brojeve $\leq a$, koristimo jednostavni postupak kojeg nazivamo **Eratostenovo** sito:

- Ispisujemo, po redu, sve prirodne brojeve od 1 do a,
- Križamo 1,
- Zaokružimo 2 (prost) i križamo sve višekratnike od 2,
- Prvi preostali 3 (prost) zaokružimo i križamo sve višekratnike od 3 (koji nisu već prekriženi),
- Prvi preostali 5 (prost) zaokružimo i križamo sve višekratnike od 5 (koji nisu već prekriženi),
- ...
- Algoritam završava u konačno koraka, a zaokruženi brojevi su prosti.

9. Osnovni teorem aritmetike (citirati i dokazati).

Teorem (Rastav na proste faktore, Osnovni teorem aritmetike): Za svaki prirodni broj a > 1 postoji jedinstveni rastav na proste faktore:

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

gdje su $p_1 < p_2 < ... < p_k$ svi različiti prosti brojevi koji dijele a, dok broj $\alpha_i \in \mathbf{N}$ kratnost prostog broja p_i.

Dokaz: Neka je q_1 najmanji prosti faktor od a, tj. $a = q_1 a_1$.

Ako je $a_1 > 1$ $\Rightarrow$ $a_1 = q_2 a_2$ $\Rightarrow$ $a = q_1 q_2 a_2$.

Ako nastavimo isti niz, na kraju će biti $a = q_1 q_2 \cdots q_n$.

Neki od prostih brojeva q_i mogu biti jednaki. Nakon grupiranja po veličini, dobivamo rastav kao u teoremu.

Slijedi dokaz da je rastav broja **a** na proste faktore jedinstven (do na njihov poredak). Pretpostavimo da imamo još jedan rastav na m prostih faktora: $a = r_1 r_2 \cdots r_m$ poredanih po veličini.

Onda je: $q_1 q_2 \cdots q_n = r_1 r_2 \cdots r_m$.

Kako q_1 dijeli lijevu stranu, onda on dijeli i desnu stranu $\Rightarrow q_1 = r_1$.

Podijelimo li jednakost sa q_1 lijevo i desno, imamo da je:

$$q_2 \cdots q_n = r_2 \cdots r_m \quad \Rightarrow \quad q_2 = r_2$$

$$\Rightarrow \quad q_i = r_i \ \forall i \ , \quad n = m.$$

10. Dokazati da prostih brojeva ima beskonačno mnogo (Euklidov teorem).

Teorem (Eulkid): Skup svih prostih brojeva je beskonačan.

Dokaz: Dokaz se provodi kontradikcijom.

Pretpostavljamo da je skup prostih brojeva konačan: $P = \{p_1, p_2, ..., p_k\}$.

Pogledajmo prirodni broj $a = p_1 \cdot p_2 \cdots p_k + 1$.

On nije djeljiv ni s jednim od p-ova, jer je ostatak pri djeljenju s bilo kojim p_i jednak 1.

Prema osnovnom teoremu aritmetike, izabrani broj a ima rastav na proste faktore:

$$a = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_n^{\alpha_n}$$

Dakle, niti jedan od prostih brojeva $q_i \notin P$, a to je kontradiktorno s definicijom skupa P. Time je teorem dokazan.

11. Dokazati formulu Nzm(a, b) · nzv(a, b) = ab.

Propozicija: Neka su a, b $\in$ N, tada vrijedi: $\operatorname{nzv}(a,b)=\dfrac{a\,b}{\operatorname{Nzm}(a,b)}$.

Dokaz: Neka su

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} \quad \text{i} \quad b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$$

rastavi na proste faktore brojeva a i b, gdje su p_1, p_2, ..., p_k svi prosti faktori od a i b zajedno. To znači da, u općem slučaju, neki α_i i β_i mogu biti jednaki nuli.

Neka je $m_i=\min\{\alpha_i,\beta_i\}$, $M_i=\max\{\alpha_i,\beta_i\}$, tada vrijedi da je:

$$\operatorname{Nzm}(a,b)=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k} \quad \text{i} \quad \operatorname{nzv}(a,b)=p_1^{M_1}p_2^{M_2}\cdots p_k^{M_k}$$

Dakle, vrijedi da je:

$$a\,b=p_1^{\alpha_1+\beta_1}p_2^{\alpha_2+\beta_2}\cdots p_k^{\alpha_k+\beta_k}$$

$$\Rightarrow \qquad a\,b=p_1^{m_1+M_1}p_2^{m_2+M_2}\cdots p_k^{m_k+M_k}=\operatorname{Nzm}(a,b)\cdot\operatorname{nzv}(a,b) \quad .$$

Napomena: Za a, b $\in$ Z i a, b $\neq$ 0 imamo da je: $\operatorname{nzv}(a,b)=\dfrac{|a\,b|}{\operatorname{Nzm}(a,b)}$.

12. Dokaži formulu a | c i b | c $\Rightarrow$ nzv (a, b) | c

Propozicija: Neka su a, b, c $\in$ N. Ako a | c i b | c , onda nzv(a, b) | c .

Dokaz: Neka je **p** prost broj takav da je p^{α_1} djelitelj od a i p^{α_2} djelitelj od b. Budući da a i b dijele c, onda $p^{\max\{\alpha_1, \alpha_2\}}$ dijeli c. Prema tome c dijeli i produkt takvih brojeva, a produkt takvih brojeva je nzv (a, b). (Vidjeti dokaz za prethodno pitanje).

13. Kako se definira kongruencija po modulu n. Dokaži da je $\equiv$ (mod n) refleksivna, simetrična i tranzitivna.

Definicija: Ako prirodan broj **n** dijeli razliku $a - b$, onda **kažemo da je a kongruentno b po modulu n** i pišemo $a \equiv b \pmod{n}$.
U protivnom, kažemo da a nije kongruentno b po modulu n i pišemo $a \neq b \pmod{n}$

Propozicija: Kongruencija po modulu n ima slijedeća svojstva:

a) Refleksivnost: $x \equiv x \pmod{n}$

b) Simetričnost: $x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$

c) Tranzitivnost: $x \equiv y \pmod{n}$ i $y \equiv z \pmod{n} \Rightarrow x \equiv z \pmod{n}$

Dokaz:

a) Broj n dijeli $x - x = 0$

b) Ako n dijeli $x - y$, onda n dijeli i $-(x - y) = y - x$

c) Ako n dijeli $x - y$ i $y - z$, onda n dijeli i $(x - y) + (y - z) = x - z$

14. U kakvom su odnosu operacije zbrajanja, množenja (potenciranja), dijeljenja i relacija ≡ (mod n) (dokazati)?

Propozicija: Ako je $a_1 \equiv b_1 \pmod{n}$ i $a_2 \equiv b_2 \pmod{n}$, gdje je $n \in \mathbf{N}$, onda vrijedi:

a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$

b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$

Dokaz:

a) Budući da je $a_1 - b_1 = n k$ i $a_2 - b_2 = n\ell$ za neke $k, \ell \in \mathbf{Z}$,

onda vrijedi da je $(a_1 + a_2) - (b_1 + b_2) = n(k + \ell)$

$\Rightarrow \quad n \mid (a_1 + a_2) - (b_1 + b_2)$.

b) Vrijedi da je: $a_1 a_2 = (b_1 + n k)(b_2 + n \ell) = b_1 b_2 + n(b_1 \ell + b_2 k + k \ell n)$

$\Rightarrow \quad n \mid a_1 a_2 - b_1 b_2$

Propozicija: Ako je $a \equiv b \pmod{n}$ i $k, \ell \in \mathbf{Z}$ bilo koji cijeli brojevi, onda vrijedi:

a) $a + n k \equiv b + n \ell \pmod{n}$

b) $a k \equiv b k \pmod{n}$

c) $a^m \equiv b^m \pmod{n}$ za svaki $m \in \mathbf{N}$

d) $p(a) \equiv p(b) \pmod{n}$ za svaki polinom $p(x)$ s cjelobrojnim koeficijentima.

Dokazi za ovu propoziciju slijede iz prethodne propozicije. (Preskočeni)

Propozicija: Neka su $a, b, k \in \mathbf{Z}$ i $n \in \mathbf{N}$ takvi da je $a k \equiv b k \pmod{n}$ i Nzm $(k, n) = 1$. Onda kongruenciju smijemo skratiti (podijeliti) sa k, tj. tada vrijedi da je $a \equiv b \pmod{n}$.

Dokaz: $a k \equiv b k \pmod{n}$ znači da $n \mid k(a - b)$, a budući da je Nzm $(n, k) = 1$, to znači da $n \mid (a - b)$ što znači da vrijedi $a \equiv b \pmod{n}$.

15. Möbiusova funkcija (definicija).

Definicija: Möbiusova funkcija $\mu : \mathbf{N} \to \mathbf{R}$ je funkcija koja prirodnom broju n, s rastavom na proste faktore $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ pridružuje vrijednost:

$$\mu(n) = \begin{cases} (-1)^k & \text{ako je } \alpha_1 = \alpha_2 = ... = \alpha_k = 1 \\ 0 & \text{inace} \end{cases}$$

Također definiramo da je $\mu(1) = 1$.

16. Eulerova funkcija i njena svojstva (Gaussova formula, Eulerova kongruencija, multiplikativnost, ...).

Definicija: Neka je $\varphi(n)$ ukupni broj svih prirodnih brojeva koji su $< n$ i koji su relativno prosti sa n. Definiramo $\varphi(1) = 1$. Na taj način je definirana funkcija $\varphi : \mathbf{N} \to \mathbf{N}$ koju nazivamo **Eulerova funkcija**.

Dakle, $\varphi(n)$ je ukupni broj brojeva u nizu 1, 2, ..., (n-1) koji su relativno prosti sa n.

Svojstva Eulerove funkcije:

a) $\sum_{d|n} \varphi(d) = n$ (**Gaussova formula**) - suma je po svim djeliteljima d broja n

b) $a^{\varphi(n)} \equiv 1 \pmod{n}$ za Nzm (a, n) = 1 (**Eulerova kongruencija**)

c) $\varphi(m\,n) = \varphi(m)\,\varphi(n)$ za Nzm (m, n) = 1 (**multiplikativnost**)

d) $\varphi(p) = p - 1$ ako je p prost broj

e) Ako je p prost broj, onda za svaki $a \in N$ vrijedi da je: $a^p \equiv a \pmod{p}$.

U specijalnom slučaju kad a nije višekratnik od p je: $a^{p-1} \equiv 1 \pmod{p}$.

(**mali Fermatov stavak**)