Počinjemo u 8:15.

Osnovne informacije o kolegiju

Predavanja 2020/2021: Andrej Dujella i Filip Najman

Vježbe 2020/2021: Tomislav Gužvić i Antonela Trbović

Održavanje kolegija:
1,2,5,6,10,11,14,15 tjedan: Predavanja za obje grupe su ponedjeljkom 8-10 (Zoom), bit će snimljena i objavljena na Meduzi.
Vježbe će biti snimljene i objavljivane na Meduzi.
3,4,12,13 tjedan: Uživo na fakultetu prema rasporedu.

Konzultacije: Po dogovoru.

Sadržaj:

Literatura:

- `https://web.math.pmf.unizg.hr/~duje/utb.html`;
- Andrej Dujella, *Uvod u teoriju brojeva,* skripta (PMF-MO), `https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`
- A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

Način polaganja predmeta

Kolokviji i završni ispit: Tijekom semestra pišu se dva kolokvija (na svakom će maksimalan broj bodova biti 60).

Aktivnost na nastavi: Na vježbama i predavanjima zadavat će se zadatci za samostalno rješavanje. Studenti koji budu najuspješniji u rješavanju tih zadataka, dobit će u pravilu za svaki zadatak po 5 bodova. Maksimalan broj bodova koji će se moći sakupiti u ovoj komponenti je 20. Sa sakupljenih 15 bodova, studenti će se moći osloboditi završnog ispita. Možete maksimalno 15 bodova skupiti na vježbama, a 5 se može skupiti na predavanju.

Završni ispit: Završni ispit je usmeni; ispituje se sadržaj obrađen na predavanjima. Uvjet za pristup završnom ispitu je ukupno barem 40 bodova prikupljenih na 2 kolokvija i aktivnostima na nastavi. Maksimalan broj bodova koji je moguće dobiti na završnom ispitu je 60. Studenti koji kroz aktivnosti na nastavi sakupe barem 15 bodova ne moraju izaći na završni ispit, već mogu uzeti ocjenu dobivenu na osnovu 2 kolokvija i aktivnosti na nastavi.

Način polaganja predmeta

Popravni ispit: Može se popravljati najviše jedan od kolokvija ili završni ispit. Nakon drugog kolokvija piše se popravak kolokvija na kojem studenti mogu pisati ili popravak prvog ili popravak drugog kolokvija. Nema uvjeta za izlazak na taj popravak. Studenti koji nisu zadovoljni rezultatom završnog ispita i koji nisu pisali popravak kolokvija, mogu izaći na popravni završni ispit. Taj ispit bi bio u istom terminu kad i završni ispit za studente koji su pisali popravak kolokvija.

Zaključivanje ocjene: zbrojit će se bodovi iz 1. kolokvija (max. 60), 2. kolokvija (max.60), aktivnosti na nastavi (max.20) i završnog ispita (max.60). Studentima koji budu oslobođeni završnog ispita, zbrojit će se bodovi iz prve 3 komponente.

Način polaganja predmeta

Ocjene:

1. $\geq$ 85% bodova - ocjena 5
2. $70 - 85\%$ bodova - ocjena 4
3. $55 - 70\%$ bodova- ocjena 3
4. $40 - 55\%$ bodova - ocjena 2
5. $<$ 40% bodova - ocjena 1.

Uvod

- Teorija brojeva (klasična) se bavi ponajprije svojstima prirodnih brojeva, te cijelih i racionalnih brojevima.

Neka svojstva skupa prirodnih i skupa cijelih brojeva koja ćemo koristiti:

- Na skupu $\mathbb{N}$ ($\mathbb{Z}$) su definirane operacije zbrajanja i množenja koje zadovoljavaju svojstva komutativnosti, asocijativnosti i distributivnosti;
- Na skupu $\mathbb{N}$ ($\mathbb{Z}$) imamo uređaj takav da za svaka dva različita elementa $m, n \in \mathbb{N}$ ($\mathbb{Z}$) vrijedi ili $m < n$ ili $n < m$;
- Svaki neprazan podskup skupa $\mathbb{N}$ ima najmanji element i vrijedi princip matematičke indukcije;
- Osim svojstava skupa $\mathbb{N}$, proučavat ćemo i svojstva skupa cijelih brojeva $0, \pm 1, \pm 2, \pm 3, \ldots$ kojeg ćemo označavati sa $\mathbb{Z}$, te skupa racionalnih brojeva, tj. brojeva oblika $\frac{p}{q}$ za $p \in \mathbb{Z}$, $q \in \mathbb{N}$, kojeg ćemo označavati s $\mathbb{Q}$.

1. Djeljivost

Definicija (1.1)

Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da a dijeli b, odnosno da je b djeljiv s a, ako postoji cijeli broj x takav da je $b = ax$. To zapisujemo s $a \mid b$. Broj a nazivamo djelitelj broja b, a broj b višekratnik broja a.
Ako b nije djeljiv s a, onda pišemo $a \nmid b$. Oznaku $a^k \parallel b$, $k \in \mathbb{N}$ ćemo koristiti kada $a^k \mid b$ i $a^{k+1} \nmid b$.

Zadatak (1.1)

Pokažite da je relacija "biti djeljiv" relacija parcijalnog uređaja na skupu $\mathbb{N}$, odnosno da za prirodne brojeve a, b, c vrijedi:

- $a \mid a$ *(refleksivnost)*;
- $a \mid b$ *i* $b \mid c \implies a \mid c$ *(tranzitivnost)*;
- $a \mid b$ *i* $b \mid a \implies a = b$ *(antisimetričnost)*.

Napomena:

- Relacija "biti djeljiv" nije relacija parcijalnog uređaja na skupu $\mathbb{Z} \setminus \{0\}$ jer $a \,|\, b$ i $b \,|\, a$, povlači $a = \pm b$, pa ne vrijedi antisimetričnost;
- Za svaki cijeli broj a vrijedi $1 \,|\, a$.
- Za svaki cijeli broj $a \neq 0$ vrijedi $a \,|\, 0$.

Zadatak (1.2)

Ako su $a, b, d, m, n \in \mathbb{Z}$, $d \neq 0$, *onda vrijedi:*

- $d \,|\, a$ *i* $d \,|\, b \implies d \,|\, (an + bm)$;
- $d \,|\, a \implies md \,|\, ma$;
- $md \,|\, ma \implies d \,|\, a$;
- $d \,|\, a \implies \frac{a}{d} \,|\, a$,
  kad god je djelitelj različit od 0.

Teorem o dijeljenju s ostatkom

Teorem (1.1 (Teorem o dijeljenju s ostatkom))

Za proizvoljan prirodan broj a i proizvoljan cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je

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

Dokaz: Dokažimo prvo postojanje takvih q i r.

Promotrimo skup $S = \{b - am : m \in \mathbb{Z}\}$.

Definirajmo $r := \min(S \cap \mathbb{N}_0)$.

Tada je $0 \leq r < a$, pošto ako nije onda je $r - a \in S$, te $0 \leq r - a < r$, što je kontradikicja s minimalnošću od r.

Neka je $q \in \mathbb{Z}$ takav da je $b - qa = r$, tj. $b = qa + r$, čime smo završili dokaz postojanja.

Teorem o dijeljenju s ostatkom

Dakle postoje q, r takvi da je

$$b = aq + r \quad \text{i} \quad 0 \leq r < a.$$

Da bi dokazali jedinstvenost od q i r, pretpostavimo da postoji još jedan par q_1, r_1 koji zadovoljava iste uvjete, tj. $b = aq_1 + r_1$.

Pokažimo najprije da je $r_1 = r$.

Pretpostavimo da je npr. $r < r_1$.

Tada je $0 < r_1 - r < a$, dok je s druge strane
$r_1 - r = a(q - q_1) \geq a$, što je kontradikcija.

Prema tome je $r_1 = r$, pa je stoga i $0 = r_1 - r = a(q_1 - q)$, iz čega zaključujemo da je $q = q_1$.

Napomena: Broj r iz Teorema 1.1 nazivamo ostatak, a broj q kvocijent, pri dijeljenju b s a. Uočimo da je u Teoremu 1.1 $r = 0$ ako i samo ako a dijeli b. Dakle, a dijeli b ako i samo ako je ostatak pri dijeljenju b s a jednak 0.

Definicija (1.2)

Broj $d \in \mathbb{Z}$ nazivamo zajednički djelitelj od a i b ako $d \mid a$ i $d \mid b$. Ako je barem jedan od brojeva a i b različit od nule, onda postoji konačno mnogo zajedničikih djeliteja od a i b i najveći među njima nazivamo najveći zajednički djelitelj od a i b i označavamo s

$$\gcd(a, b) \text{ ili } nzd(a, b) \text{ ili samo } (a, b).$$

Na sličan način definiramo najveći zajednički djelitelj za bilo koji konačan skup cijelih brojeva $a_1, a_2, \ldots, a_n$, a označavamo ga s $(a_1, a_2, \ldots, a_n)$.

Uočimo:

- Svaki prirodan broj $a > 1$ ima uvijek dva djelitelja 1 i a. Njih nazivamo *trivijalni djelitelji*.
- $(a, b) \geq 1$.
- $(a, 0) = |a|$, za svaki $a \in \mathbb{Z}$, $a \neq 0$.

Teorem (1.2)

Neka su $b, c \in \mathbb{Z}$ od kojih je barem jedan različit od nule. Neka je

$$S = \{bx + cy : x, y \in \mathbb{Z}\} \cap \mathbb{N},$$

tada je $(b, c) = \min S$.

Dokaz:
Neka je $g = (b, c)$, te neka je
$l := \min S = \min(\{bx + cy : x, y \in \mathbb{Z}\} \cap \mathbb{N}$.

To znači da postoje cijeli brojevi x_0 i y_0 takvi da je $l = bx_0 + cy_0$.

Pokažimo da $l|b$ i $l|c$. Pretpostavimo da npr. $l \nmid b$.

Tada po Teoremu 1.1. postoje cijeli brojevi q i r takvi da je
$b = lq + r$ i $0 < r < l$.

Sada je

$$r = b - lq = b - q(bx_0 + cy_0) = b(1 - qx_0) + c(-qy_0) \in S,$$

što je u suprotnosti s minimalnošću od l.

Dakle, $l|b$, a na isti način se pokazuje da $l|c$. To znači da je $l \leq g$.

Imamo kao i prije $g = (b, c)$, te neka je
$l := \min S = \min(\{bx + cy \,:\, x, y \in \mathbb{Z}\} \cap \mathbb{N}$.

Dakle do sada smo dokazali da je $l \leq g$, dokažimo sada i $l \geq g$.

Budući da je $g = (b, c)$, postoje $\beta, \gamma \in \mathbb{Z}$ takvi da je $b = g\beta$, $c = g\gamma$, pa je $l = bx_0 + cy_0 = g(\beta x_0 + \gamma y_0)$.

Odavde slijedi da $g \mid l$, pa je onda $g \leq l$, te smo dokazali da je $g = l$. □

Ako se cijeli broj d može prikazati u obliku $d = bx + cy$, onda je (b, c) djelitelj od d. Posebno, ako je $bx + cy = 1$, onda je $(b, c) = 1$.

Ako je d zajednički djeljitelj od b i c, onda $d \mid (b, c)$. Zaista, d dijeli b i c, pa onda dijeli i $bx + cy$, te tvrdnja slijedi iz Teorema 1.2.

Definicija (1.3)

Kažemo da su cijeli brojevi a i b relativno prosti, ako je $(a, b) = 1$.

Za cijele brojeve $a_1, a_2, \ldots, a_n$ kažemo da su relativno prosti ako je $(a_1, a_2, \ldots, a_n) = 1$, a da su u parovima relativno prosti ako je $(a_i, a_j) = 1$ za sve $1 \leq i, j \leq n$, $i \neq j$.

Napomena

Biti u parovima relativno prost je jače svojstvo od biti relativno prost, tj. ako su $a_1, a_2, \ldots, a_n$ u parovima relativno prosti, onda su oni relativno prosti, ali obrnuto ne vrijedi!

Zadatak

Nađite kontraprimjer koji dokazuje drugu tvrdnju iz prethodne napomene!

Propozicija (1.1)

Neka su $a, b, m \in \mathbb{Z}$. *Ako je* $(a, m) = (b, m) = 1$, *onda je* $(ab, m) = 1$.

Dokaz:

Po Teoremu 1.2. postoje $x_0, y_0, x_1, y_1 \in \mathbb{Z}$ takvi da je

$$1 = ax_0 + my_0 \quad \text{i} \quad 1 = bx_1 + my_1.$$

Odavde je

$$ax_0 bx_1 = (1 - my_0)(1 - my_1) = 1 - m(y_0 + y_1 - my_0 y_1) = 1 - my_2,$$

gdje je $y_2 = y_0 + y_1 - my_0 y_1$.

Sada iz $ab(x_0 x_1) + m(y_2) = 1$ zaključujemo da je $(ab, m) = 1$.

Propozicija (1.2)

Neka su $a, b \in \mathbb{Z}$, *tada je* $(a, b) = (a, b + ax)$ *za svaki* $x \in \mathbb{Z}$.

Dokaz:

Označimo $(a, b) = d$, $(a, b + ax) = g$.

Po Teoremu 1.2. postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $d = ax_0 + by_0$, odnosno dodavanjem i oduzimanjem axy_0,

$$d = a(x_0 - xy_0) + (b + ax)y_0.$$

Odavdje slijedi da $g|d$, pošto je $(a, b + ax) = g$. Pokažimo sada da $d|g$.

Budući $d|a$ i $d|b$, imamo da $d|(b + ax)$.

Dakle, d je zajednički djelitelj od a i $b + ax$, pa po Teoremu 1.2. imamo da $d|g$.

Pošto su brojevi d i g pozitivni po definiciji, iz $d|g$ i $g|d$ slijedi da je $d = g$.

Teorem (1.3 Euklidov algoritam)

Neka su dani $b \in \mathbb{Z}$ i $c \in \mathbb{N}$. Pretpostavimo da je uzastopnom primjenom Teorema 1.1 dobiven niz jednakosti

$$\begin{aligned}
b &= cq_1 + r_1, \quad 0 < r_1 < c, \\
c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\dots \\
r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\
r_{j-1} &= r_j q_{j+1}.
\end{aligned}$$

Tada je $(b, c) = r_j$, tj. (b, c) jednak je posljednjem ostatku različitom od 0.
Brojevi $x_0, y_0 \in \mathbb{Z}$ takvi da je

$$(b, c) = r_j = bx_0 + cy_0, \qquad (**)$$

mogu se dobiti izražavanjem svakog r_i kao lin. kombinacije od a i b.

Dokaz: Prepišimo:

$$\begin{aligned}
b &= cq_1 + r_1, \quad 0 < r_1 < c, \\
c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\dots \\
r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\
r_{j-1} &= r_j q_{j+1}.
\end{aligned}$$

Doakzujemo prvo da je $(b, c) = r_j$.

Po Propoziciji 1.2 imamo

$$(b, c) = (b - cq_1, c) = (r_1, c) = (r_1, c - r_1 q_2) = (r_1, r_2)$$

$$= (r_1 - r_2 q_3, r_2) = (r_3, r_2).$$

Nastavljajući ovaj proces, dobivamo:
$(b, c) = (r_{j-1}, r_j) = (r_j, 0) = r_j$.

Prepišimo opet:

$$\begin{aligned} b &= cq_1 + r_1, \quad 0 < r_1 < c, \\ c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\ &\dots \\ r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_j q_{j+1}. \end{aligned}$$

Sada indukcijom dokazujemo da je svaki r_i linearna kombinacija od b i c.

To je točno za

$$r_1 = b - cq_1 \qquad \text{i}$$

$$r_2 = c - r_1 q_2 = c - (b - cq_1)q_2 = -bq_1 + c(1 + q_1 q_2),$$

pa pretpostavimo da vrijedi za r_{i-1} i r_{i-2}.

Budući da je r_i linearna kombinacija od r_{i-1} i r_{i-2}, po pretpostavci indukcije dobivamo da je i linearna kombinacija od b i c.

Napomena

- *U Euklidovom algoritmu smo pretpostavili da je* $c > 0$ *što nije bitno ograničenje jer je* $(b, c) = (|b|, |c|)$;
- *Ako su* $b, c \in \mathbb{N}$ *i* $b < c$, *onda u prvom koraku imamo* $b = c \cdot 0 + a$, *pa* b *i* c *zamijene mjesta;*
- *Primijetimo da je (konačan) niz ostataka u (*)* $r_0 = c$, $r_1, r_2, \ldots, r_k$ *strogo padajući niz;*
- *Primijetimo da je*

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

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

- *Brojevi* $x_0, y_0 \in \mathbb{Z}$ *u (**) nisu jednoznačno određeni, jer je npr.*

$$(b, c) = bx_0 + cy_0 = (x_0 + c)\, b + (y_0 - b)\, c.$$

Rješenja jednadžbe $bx + cy = (b, c)$ mogu se efikasno dobiti na slijedeći način: ako je

$$\begin{aligned} r_{-1} &= b, \quad r_0 = c; \quad r_i = r_{i-2} - q_i r_{i-1}; \\ x_{-1} &= 1, \quad x_0 = 0; \quad x_i = x_{i-2} - q_i x_{i-1}; \\ y_{-1} &= 0, \quad y_0 = 1; \quad y_i = y_{i-2} - q_i y_{i-1}, \end{aligned}$$

onda je

$$bx_i + cy_i = r_i, \quad \text{za } i = -1, 0, 1, \ldots, j+1.$$

Ova formula je točna za $i = -1$ i $i = 0$, pa tvrdnja trivijalno slijedi indukcijom, jer obje strane formule zadovoljavaju istu rekuzivnu relaciju. Posebno, vrijedi:

$$bx_j + cy_j = (b, c).$$

Primjer (1.1)

Odredimo $d = (252, 198)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 252 *i* 198.

Rješenje:

$$\begin{aligned} 252 &= 198 \cdot 1 + 54 \\ 198 &= 54 \cdot 3 + 36 \\ 54 &= 36 \cdot 1 + 18 \\ 36 &= 18 \cdot 2 \end{aligned}$$

Nadalje, imamo:

$$\begin{aligned} 18 &= 54 - 36 \cdot 1 = 54 - (198 - 54 \cdot 3) \cdot 1 = 4 \cdot 54 - 1 \cdot 198 \\ &= 4 \cdot (252 - 198 \cdot 1) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198. \end{aligned}$$

Zadatak

Odredite $g = (423, 198)$ *i nađite cijele brojeve* x, y *takve da je* $423x + 198y = g$.

Zadatak

Odredite cijele brojeve x, y *takve da je*

a) $71x + 50y = 1$, *b)* $93x + 81y = 3$.