Predavanje 2

NAJVEĆI ZAJEDNIČKI DELILAC, NERAZLOŽIVI I PROSTI BROJEVI

Kažemo da je $d \in \mathbb{Z}$ *najveći zajednički delilac (NZD)* celih brojeva a i b ako važi:

(i) $d \mid a$, $d \mid b$.
(ii) Za sve $c \in \mathbb{Z}$ takve da $c \mid a$ i $c \mid b$ važi $|c| \leqslant |d|$.

Primetimo da par $(0, 0)$ nema najveći zajednički delilac; međutim, za svaki drugi par celih brojeva postoje tačno dva cela broja koji zadovoljavaju gornje uslove, i oni su jedan drugom suprotni. Ako je d najveći zajednički delilac za a, b, to pišemo $d = (a, b)$, pri čemu se ova notacija najčešće odnosi na *pozitivan* NZD za a i b (što ćemo od sada i podrazumevati, ukoliko eksplicitno nije naznačeno suprotno).

Po upravo datoj definiciji, $d = (a, b)$ je najveći *po apsolutnoj vrednosti* element skupa $D_{a,b} = \{c \in \mathbb{Z} : c \mid a,\ c \mid b\}$ svih zajedničkih delitelja brojeva a, b koji je (sem u slučaju $a = b = 0$) konačan. Međutim, ova definicija se vrlo retko koristi u operativnom smislu, budući da se ona poziva na *poredak* na celim brojevima, a ne na njihove artimetičke osobine koje proizilaze iz relacije deljivosti. Srećom, NZD dva cela broja ima jednu izuzetnu osobinu, koju u gotovo svim relevantnim situacijama u teoriji brojeva koristimo kao alternativnu definiciju najvećeg zajedničkog delioca: naime, NZD za a, b je (do na predznak jedinstveni) broj koji je *deljiv* svim zajedničkim deliocima a i b (tj. svim elementima skupa $D_{a,b}$).

Teorema 2.1. *Neka su $a, b, c \in \mathbb{Z}$ takvi da (a, b) postoji, $c \mid a$ i $c \mid b$. Tada $c \mid (a, b)$.*

Dokaz. Ovo značajno tvrđenje dokazujemo primenom jednog od najstarijih poznatih algoritama u matematici — u pitanju je *Euklidov algoritam* za nalaženje NZD-a dva broja. On se sastoji u tome da se pođe od datih brojeva a, b i da se jedan od njih celobrojno podeli drugim uz odgovarajući ostatak. U svakom koraku, broj kojim smo prethodno delili postaje broj koji se deli (deljenik), a ostatak iz prethodnog koraka se uzima kao novi delitelj. Postupak se nastavlja sve dok neki od ostataka ne bude jednak 0; pri tome je poslednji nenula ostatak u nizu upravo traženi NZD. Dakle, ako je, na primer, $b \neq 0$, tada smo izvršili sledeća celobrojna deljenja:

$$\begin{aligned} a &= q_1 b + r_1, && \text{gde je } 0 \leqslant r_1 < |b|, \\ b &= q_2 r_1 + r_2, && \text{gde je } 0 \leqslant r_2 < r_1, \\ r_1 &= q_3 r_2 + r_3, && \text{gde je } 0 \leqslant r_3 < r_2, \\ &\vdots && \vdots \end{aligned}$$

$$\begin{aligned} r_{k-1} &= q_{k+2}r_k + r_{k+1}, && \text{gde je } 0 \leqslant r_{k+1} < r_k, \\ &\vdots && \vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, && \text{gde je } 0 \leqslant r_n < r_{n-1}, \\ r_{n-1} &= q_{n+1} r_n && (r_n = 0). \end{aligned}$$

Primetimo da se postupak sigurno završava u konačno mnogo koraka, budući da niz

$$|b| > r_1 > r_2 > \cdots > r_k > \cdots$$

mora biti konačan.

Tvrdimo da je $r_n = (a, b)$, odakle odmah sledi tvrđenje teoreme, budući da se lako pokazuje da za svaki zajednički delilac c brojeva a, b mora biti $c \mid r_k$ za sve k (pa tako i za $k = n$); naime, iz $r_{k-2} = q_{k+1}r_{k-1} + r_k$ dobijamo $r_k = r_{k-2} - q_{k+1}r_{k-1}$, pa zaključujemo da iz (induktivne) pretpostavke $c \mid r_{k-2}, c \mid r_{k-1}$ sledi $c \mid r_k$.

Pošto malopređašnji sled zaključaka važi za svaki zajednički delilac c brojeva a, b, sledi da on važi i za $c = (a, b)$; zbog toga odmah imamo $(a, b) \mid r_n$, a samim tim i $(a, b) \leqslant r_n$. S druge strane, pokažimo da r_n jeste zajednički delilac za a i b. Neposredno, imamo da $r_n \mid r_{n-1}$. Sada pretpostavka da $r_n \mid r_{k+1}$ i $r_n \mid r_{k+2}$ povlači, na osnovu jednakosti $r_k = q_{k+2}r_{k+1} + r_{k+2}$, da $r_n \mid r_k$. Tako dolazimo da zaključka da $r_n \mid a$ i $r_n \mid b$. Po definiciji NZD-a, odavde sledi $r_n \leqslant (a, b)$. Prema tome, $r_n = (a, b)$, kao što se i tražilo. □

Posledica 2.2. *Za sve $a, b \in \mathbb{Z}$, $c \in \mathbb{Z}^+$ važi $(ca, cb) = c(a, b)$.*

Dokaz. Zapravo, ovo je više posledica *dokaza* nego samog tvrđenja prethodne teoreme. Naime, posmatrajmo jednakosti koje smo dobili tokom Eukidovog algoritma za izračunavanje (a, b): ovaj algoritam rezultuje poslednjim nenula ostatkom $r_n = (a, b)$. Pomnožimo sada sve te jednakosti sa c; na taj način dobijamo upravo jednakosti koje proističu iz instance Euklidovog algoritma za nalaženje (ca, cb). Poslednji nenula ostatak koji taj algoritam daje je baš $(ca, cb) = cr_n = c(a, b)$. □

Tvrđenje 2.3. *Najveći zajednički delilac brojeva $a, b \in \mathbb{Z}$ se može izraziti u obliku*

$$(a, b) = \alpha a + \beta b$$

za pogodno odabrane $\alpha, \beta \in \mathbb{Z}$.

Dokaz. Indukcijom po k dokazujemo da se svaki ostatak r_k u Euklidovom algoritmu za izračunavanje (a, b) može izraziti kao $r_k = \alpha_k a + \beta_k b$ za neke $\alpha_k, \beta_k \in \mathbb{Z}$. Zaista, to je tačno za same brojeve $a = 1 \cdot a + 0 \cdot b$ i $b = 0 \cdot a + 1 \cdot b$, kao i za $r_1 = a - q_1 b = 1 \cdot a + (-q_1) \cdot b$. Zato pretpostavimo da važi $r_{k-1} = \alpha_{k-1}a + \beta_{k-1}b$ i $r_k = \alpha_k a + \beta_k b$ za neke $\alpha_{k-1}, \alpha_k, \beta_{k-1}, \beta_k \in \mathbb{Z}$. Tada je

$$r_{k+1} = r_{k-1} - q_{k+1}r_k = (\alpha_{k-1} - q_{k+1}\alpha_k)a + (\beta_{k-1} - q_{k+1}\beta_k)b,$$

pa je sada dovoljno definisati $\alpha_{k+1} = \alpha_{k-1} - q_{k+1}\alpha_k$ i $\beta_{k+1} = \beta_{k-1} - q_{k+1}\beta_k$. Specijalno, sledi $(a, b) = r_n = \alpha_n a + \beta_n b$, pa $\alpha = \alpha_n$ i $\beta = \beta_n$ predstavljaju adekvatan izbor traženih koeficijenata. □

Ovo tvrđenje ima značajnu posledicu u vezi sa rešivošću linearne *diofantske jednačine* $ax+by=c$. (Pod diofanskom jednačinom podrazumevamo algebarsku jednačinu sa celim koeficijentima čija rešenja tražimo samo u skupu celih brojeva. Ovde su a, b, c fiksirani koeficijenti, dok pod rešenjem podrazumevamo par celih brojeva x, y.)

Tvrđenje 2.4. *Neka su $a, b, c \in \mathbb{Z}$ tako da je $a \neq 0$ ili $b \neq 0$. Tada diofantska jednačina $ax + by = c$ ima rešenja ako i samo ako $(a, b) \mid c$.*

Dokaz. ($\Rightarrow$): Neka je (x_0, y_0) neko rešenje date jednačine. Pošto $(a, b) \mid a$ i $(a, b) \mid b$, važi

$$(a, b) \mid ax_0 + by_0 = c.$$

($\Leftarrow$): Pretpostavimo da $(a, b) \mid c$, tj. da je $c = (a, b)c'$. Po prethodnom tvrđenju, postoje $\alpha, \beta \in \mathbb{Z}$ tako da je $(a, b) = \alpha a + \beta b$. To znači da je

$$c = a(\alpha c') + b(\beta c'),$$

odnosno, $x = \alpha c'$, $y = \beta c'$ je jedno rešenje date jednačine. □

Sada možemo definisati i najveći zajednički delilac za proizvoljan neprazan skup celih brojeva: naime, ako je $a_1, \ldots, a_k \in \mathbb{Z}$ (pri čemu je bar jedan od brojeva nenula), tada je njihov NZD, u oznaci $(a_1, \ldots, a_k)$, najveći (po apsolutnoj vrednosti) broj d takav da $d \mid a_i$ za sve $1 \leqslant i \leqslant k$. Ponovo se pokazuje da je posredi broj koji je deljiv svakim zajedničkim deliocem datih brojeva (pri čemu je redosled njihovog navođenja nebitan). Pri tome je

$$(a_1, \ldots, a_k) = (\ldots((a_1, a_2), a_3), \ldots, a_k).$$

Kažemo da su brojevi $a_1, \ldots, a_k \in \mathbb{Z}$ (gde je $k \geqslant 2$) *uzajamno prosti* ako je $(a_1, \ldots, a_k) = 1$. Ovi brojevi su *po parovima uzajamno prosti* ako je $(a_i, a_j) = 1$ za sve indekse i, j, $i \neq j$. Svaki skup po parovima uzajamno prostih brojeva čini ujedno i skup uzajamno prostih brojeva; primer brojeva $6, 10, 15$ pokazuje da obratna implikacija ne važi.

Naredno tvrđenje povezano sa uzajamno prostim brojevima će u daljem imati vešestruku primenu i značaj.

Lema 2.5. *Neka su $a, b, c \in \mathbb{Z}$ takvi da $c \mid ab$. Ako je $(c, a) = 1$, tada $c \mid b$.*

Dokaz. Očigledno, $c \mid cb$, pa je c zajednički delilac za ab i cb. Međutim, tada po Teoremi 2.1 i njenoj Posledici 2.2 važi $c \mid (ab, cb) = (a, c)b = b$. □

U prethodnom smo videli da u odnosu na relaciju deljivosti 0, kao i jedinični elementi $1, -1$ imaju posebnu ulogu: nula je deljiva svim celim brojevima, dok jedinični elementi dele sve brojeve: $\varepsilon \mid a$ za svaki jedinični element ε i proizvoljno $a \in \mathbb{Z}$. Osim toga, važi i $\varepsilon a \mid a$. Ovo su tzv. *trivijalni* delioci broja a. Nas će naročito interesovati brojevi koji imaju isključivo trivijalne delioce — to su nerazloživi brojevi. Preciznije, broj p različit od 0 i jediničnih elemenata je *nerazloživ* ako za bilo koje razlaganje

$$p = ab$$

važi da je jedan od elemenata a, b jedinični. U suprotnom, p je *složen* broj.

S druge strane, za nenula i nejedničan broj p kažemo da je *prost* ako za sve $a, b \in \mathbb{Z}$ takve da $p \mid ab$ važi $p \mid a$ ili $p \mid b$.

Tvrđenje 2.6. *Ceo broj je prost ako i samo ako je nerazloživ.*

Dokaz. ($\Rightarrow$): Pretpostavimo da je p prost broj; posmatrajmo proizvoljnu faktorizaciju $p = ab$. Kako sada $p \mid ab$, sledi da $p \mid a$ ili $p \mid b$. U prvom slučaju $ab \mid a$, tj. $a = abq$ za neko $q \in \mathbb{Z}$, odakle je $bq = 1$ i b mora biti jedinični broj. Slično se u drugom slučaju zaključuje da a mora biti jedinični.

($\Leftarrow$): Pretpostavimo sada da je broj p nerazloživ. Neka su $a, b \in \mathbb{Z}$ takvi da $p \mid ab$. Ukoliko pri tome $p \mid a$, tvrđenje je dokazano; zato pretpostavimo da $p \nmid a$. Budući da važi $(p, a) \mid p$, zbog nerazloživosti p mora biti $(p, a) = 1$. No, tada po prethodnoj lemi odmah sledi $p \mid b$. □

S obzirom na prethodno tvrđenje, u daljem ćemo brojeve sa svojstvom nerazloživosti zvati prostim brojevima, kao što je to u teoriji (celih) brojeva i uobičajeno.

Napominjemo da je pojmove *nerazloživog*, odnosno *prostog* elementa moguće definisati u svakom integralnom domenu, pa i šire, u proizvoljnim prstenima. Međutim, u opštem slučaju, nerazloživi i prosti elementi ne moraju da se poklapaju. Na primer, u prstenu $2\mathbb{Z}$ parnih brojeva svaki element oblika $4n + 2$ je nerazloživ (jer svaki složen element mora očito biti deljiv sa 4), ali nijedan od njih nije prost: naime, $4n + 2 \mid (4n + 2)^2$, ali $4n + 2$ ne deli samog sebe u ovom prstenu (što je posledica nepostojanja jediničnih elemenata u njemu).