Predavanje 1

DELJIVOST I DELJENJE SA OSTATKOM

U najužem smislu, zadatak teorije brojeva (artimetike) jeste izučavanje strukture prstena celih brojeva $(\mathbb{Z}, +, \cdot)$. Zapravo, ovaj prsten je *integralni domen*, tj. u pitanju je komutativan prsten sa jedinicom koji nema *delitelje nule*: zaista, za dva cela broja $a, b \in \mathbb{Z}$ važi $ab = 0$ ako i samo ako je $a = 0$ ili $b = 0$. Posmatrano šire, predmet teorije brojeva je u tesnoj vezi sa ispitivanjem osobina relacije deljivosti u različitim integralnim domenima (ne samo u $\mathbb{Z}$) čiji su elementi kompleksni brojevi. Na primer, ova relacija u integralnom domenu $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ ima sasvim drugačija svojstva nego u $\mathbb{Z}$, no upravo ta informacija u određenim situacijama može imati značajne posledice po pitanja koja se tiču celih brojeva.

Definicija 1.1. Za ceo broj b kažemo da je *delilac* broja $a \in \mathbb{Z}$, odnosno da *deli* a (u oznaci $b \mid a$), ako postoji $q \in \mathbb{Z}$ tako da je

$$a = bq.$$

Na primer, 0 je deljiva svim delim brojevima, budući da je $0 = b \cdot 0$ za sve $b \in \mathbb{Z}$. Takodje, $2 \mid 4$, dok $3 \nmid 5$.

Definicija 1.2. Broj $\varepsilon \in \mathbb{Z}$ koji deli svaki ceo broj zovemo *jediničnim* elementom prstena $\mathbb{Z}$.

Tvrđenje 1.3. *Prsten $\mathbb{Z}$ ima tačno dva jedinična elementa: 1 i -1.*

Dokaz. Očigledno, 1 i -1 su jedinični elementi u $\mathbb{Z}$, budući da za sve $a \in \mathbb{Z}$ važi $a = \pm 1 \cdot \pm a$.

S druge strane, neka je ε jedinični ceo broj. Tada, specijalno, važi $\varepsilon \mid 1$, pa je $1 = \varepsilon q$ za neko $q \in \mathbb{Z}$. Jasno, ni ε ni q ne mogu biti 0, pa je $|\varepsilon|, |q| \geqslant 1$. Tako $1 = \varepsilon q$ povlači da je $|\varepsilon| = 1$, tj. $\varepsilon \in \{1, -1\}$. □

S druge strane, ako na analogan način definišemo deljivost u prstenu $\mathbb{Z}[\sqrt{2}]$, dobijamo da on ima *beskonačno mnogo* jediničnih elemenata: na primer, $a + b\sqrt{2}$ je jedinični kad god važi $a^2 - 2b^2 = 1$. (Kasnije ćemo videti da ova diofantska jednačina ima beskonačno mnogo rešenja.) Međutim, prsten parnih brojeva $2\mathbb{Z}$ (koji je potprsten od $\mathbb{Z}$) uopšte nema jedinične elemente: svaki paran broj k koji nije deljiv sa 4 (na primer, 10) uopšte nema nijedan delitelj u ovom prstenu, jer ne postoje parni brojevi ℓ_1 i ℓ_2 tako da je $k = \ell_1 \ell_2$.

Tvrđenje 1.4. *Ako su ε, δ jedinični celi brojevi i važi $b \mid a$, tada važi i $\varepsilon b \mid \delta a$.*

Dokaz. Kako $\varepsilon \mid 1$, to je $1 = \varepsilon\alpha$ za neko $\alpha \in \mathbb{Z}$. Stoga, ako važi $b \mid a$, odnosno $a = bq$ za neko $q \in \mathbb{Z}$, tada je $\delta a = \delta \cdot bq \cdot 1 = (\varepsilon b)(\alpha\delta q)$. Dakle, $\varepsilon b \mid \delta a$. □

Prethodno tvrđenje nam u stvari omogućava da ispitivanje deljivosti brojeva svedemo, po potrebi, isključivo na nenegativne cele, odnosno *prirodne* brojeve. Predznak (tj. množenje jediničnim elementom) nema nikakvu bitnu ulogu kada je u pitanju deljivost celih brojeva.

Tvrđenje 1.5.

(1) *Za sve* $a \in \mathbb{Z}$ *važi* $a \mid a$.
(2) *Za sve* $a, b, c \in \mathbb{Z}$, *ako* $a \mid b$ *i* $b \mid c$, *tada* $a \mid c$.
(3) *Za sve* $a, b, c \in \mathbb{Z}$, *ako* $a \mid b$ *i* $b \mid a$, *tada postoji jedinični element* ε *tako da je* $a = b\varepsilon$.
(4) *Ako* $c \mid a$ *i* $c \mid b$ *za neke* $a, b, c \in \mathbb{Z}$ *tada* $c \mid (a + b)$, $c \mid (a - b)$ *i* $c \mid ka$ *za sve* $k \in \mathbb{Z}$. *Zapravo, tada za sve* $\alpha, \beta \in \mathbb{Z}$ *važi* $c \mid (\alpha a + \beta b)$.

Dokaz. Dokazujemo samo stavku (3), pošto se ostala tvrđenja dokazuju neposredno na osnovu definicije deljivosti. Zaista, ako važi $a \mid b$ i $b \mid a$, tada je $b = aq$ i $a = bs$ za neke $q, s \in \mathbb{Z}$. Otuda je $b = b(sq)$. Ako je $b = 0$, tada je nužno $a = 0$, pa je $a = b \cdot 1$. U suprotnom, sledi $sq = 1$, pa je element s jedinični, što uz $a = bs$ daje željeni rezultat. □

Prema tome, ako relaciju deljivosti $\mid$ ograničimo na skup $\mathbb{Z}^+$ pozitivnih celih brojeva, dobijamo relaciju poretka, tj. parcijalno uređenje ovog skupa.

Naredni rezultat prirodno vodi ka poznatim pojmovima celobrojnog količnika i ostatka pri deljenju sa nekim celim brojem različitim od nule.

Teorema 1.6. *Za sve* $a, b \in \mathbb{Z}$, $b \neq 0$, *postoje jedinstveni brojevi* $q, r \in \mathbb{Z}$ *tako da je*

$$a = qb + r \quad i \quad 0 \leqslant r < |b|.$$

Dokaz. Razmotrimo najpre slučaj $b > 0$. Dati uslovi su očito ekvivalentni egzistenciji i jedinstvenosti celih brojeva q, r tako da je

$$0 \leqslant r = a - qb < b,$$

što je, dalje, ekvivalentno dvostrukoj nejednakosti

$$qb \leqslant a < (q + 1)b,$$

tj. $a/b \in [q, q + 1)$. Međutim, postoji jedinstven ceo broj q sa prethodnom osobinom: to je baš $q = \lfloor a/b \rfloor$, najveći ceo broj koji nije veći od a/b. Pri tome odmah sledi da je i tražno r jedinstveno; naime, mora biti

$$r = a - \left\lfloor \frac{a}{b} \right\rfloor b.$$

S druge strane, ako je $b < 0$, tada uslovi

$$0 \leqslant r = a - bq < |b| = -b$$

analogno kao i malopre vode dvostrukoj nejednakosti $q \geqslant a/b > q - 1$, što ponovo jedinstveno određuje q; naime, mora biti $q = \lceil a/b \rceil$. Jedinstvenost r opet sledi neposredno. □

Gornji postupak kojim se za date brojeve $a, b \in \mathbb{Z}$ dobijaju jedinstveni brojevi q, r zovemo *deljenje sa ostatkom*; pri tome je q *celobrojni količnik* (pri deljenju a sa b) dok je r *ostatak*. Primetimo da važi $b \mid a$ ako i samo ako je ostatak pri deljenju a sa b jednak 0.

Postupak deljenja sa ostatkom nam omogućava—između ostalog—da prirodne brojeve izražavamo u *brojevnim sistemima* sa datom osnovom (binarnom, dekadnom, ...). Ovo je precizirano narednim tvrđenjem.

Teorema 1.7. *Neka je $B > 1$ ceo broj. Tada se svako $A \in \mathbb{Z}^+$ na jedinstven način može zapisati u obliku*

$$A = a_n B^n + a_{n-1} B^{n-1} + \cdots + a_1 B + a_0, \tag{1.1}$$

gde je $a_n \neq 0$ i $0 \leqslant a_i < B$ za sve $0 \leqslant i \leqslant n$.

Dokaz. Teoremu dokazujemo indukcijom (po A). Tvrđenje je jasno ako je $A \in \{1, \ldots, B-1\}$. Zato pretpostavimo da se svaki broj manji od A na jedinstven način zapisuje u željenom obliku, pri čemu je $A \geqslant B$. Budući da dati uslovi zahtevaju da bude $0 \leqslant a_0 < B$ i $B \mid (A - a_0)$, sledi da a_0 mora biti upravo ostatak broja A pri deljenju sa B, tj. a_0 je jedinstveno određeno. Posmatrajmo sada broj $A' = (A - a_0)/B$, celobrojni količnik A pri deljenju sa B. Pošto je $0 < A' < A$, po induktivnoj pretpostavci imamo da se A' na jedinstven način zapisuje u traženom obliku:

$$A' = a_m B^m + a_{m-1} B^{m-1} + \cdots + a_2 B + a_1.$$

Kako je $A = A'B + a_0$, sledi da je $A = a_{m+1} B^{m+1} + a_m B^m + \cdots + a_1 B + a_0$, pa dobijamo željeni zapis za A. On je jedistven, jer ako bi bilo $A = a'_k B^k + \cdots + a'_1 B + a'_0$, gde je $a'_k \neq 0$ i $0 \leqslant a'_j < B$ za sve $0 \leqslant j \leqslant k$, tada na osnovu ranijeg zaključka imamo $a'_0 = a_0$, pa je

$$a'_k B^{k-1} + \cdots + a'_1 = a_m B^m + \cdots + a_1.$$

Deo induktivne pretpostavke koji se odnosi na jedinstvenost povlači da mora biti $k = m$ i $a'_i = a_i$ za sve $1' \leqslant i' \leqslant m$, što se i tražilo. □

Za reprezentaciju (zapis) broja A u obliku (1.1) kažemo da je *u sistemu sa osnovom B*, dok su a_i *cifre* tog zapisa. Kraće, možemo pisati i

$$A = \overline{a_n a_{n-1} \ldots a_1 a_0}_{[B]},$$

s tim da se u dekadnom sistemu (sistemu sa osnovom 10) indeks $_{[10]}$ najčešće izostavlja.