Predavanje 3

OSNOVNA TEOREMA ARITMETIKE

Prvi ključni rezultat teorije brojeva koji praktično predstavlja "odskočnu dasku" za bilo kakva ozbiljnija ispitivanja strukture prstena $\mathbb{Z}$ jeste *osnovna teorema aritmetike* koja tvrdi da skup prostih brojeva—zajedno sa 0 i -1—čini jedinstveni minimalni generatorni skup multiplikativne polugrupe celih brojeva.

Teorema 3.1 (Osnovna teorema aritmetike)**.** *Svaki prirodan broj $a > 1$ može se prikazati kao proizvod (pozitivnih) prostih brojeva i pri tome je ta faktorizacija jedinstvena do na poredak faktora: drugim rečima, ako važi*

$$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s,$$

gde su p_i, q_j prosti brojevi za sve $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$, tada je $r = s$ i postoji permutacija π skupa $\{1, 2, \dots, r\}$ tako da je $p_i = q_{\pi(i)}$ za sve $1 \leqslant i \leqslant r$.

Dokaz. (Egzistencija razlaganja): Tvrđenje da *postoji* razlaganje broja $a > 1$ na proste faktore dokazujemo (totalnom) indukcijom. Ono je evidentno za $a = 2$, pošto je posredi prost broj. Zato pretpostavimo da svi brojevi iz $\{2, \dots, a-1\}$ imaju bar po jedno razlaganje u proizvod prostih brojeva.

Ako je sam broj a prost, tada nema šta da se dokazuje; u suprotnom, neka je $p > 1$ najmanji netrivijalni delilac broja a. Očito, p mora biti prost broj, jer bi u suprotnom a imao delilac manji od p, što je u suprotnosti sa izborom p. Prema tome, važi $a = pa'$, gde je $1 < a' < a$; zbog toga je induktivna pretpostavka primenljiva na a', tj. a' je proizvod prostih brojeva: $a' = p_1 \dots p_m$. No, tada je

$$a = pp_1 \dots p_m,$$

što okončava induktivni dokaz.

(Jedinstvenost razlaganja): Pretpostavimo da je $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$; bez umanjenja opštosti, neka je $r \leqslant s$. Pošto $p_1 \mid q_1 q_2 \dots q_s$ i p_1 je prost broj, zaključujemo da $p_1 \mid q_{j_1}$ za neko j_1; međutim, i q_{j_1} je, kao i p_1, (pozitivan) prost broj, pa je $p_1 = q_{j_1}$. Isto zaključivanje se može ponoviti i za $p_2, \dots, p_r$, pa za svako $1 \leqslant i \leqslant r$ postoji indeks j_i tako da je $p_i = q_{j_i}$. Pri tome su svi indeksi $j_1, \dots, j_r$ međusobno različiti. Ukoliko bi bilo $r < s$, tada bismo, po označavanju $\{k_1, \dots, k_{s-r}\} = \{1, \dots, s\} \setminus \{j_1, \dots, j_r\}$, dobili da je

$$1 = q_{k_1} \dots q_{k_{s-r}},$$

što je očito nemoguće. Dakle, mora biti $r = s$; osim toga, permutacija π definisana sa $\pi(i) = j_i$ $(1 \leqslant i \leqslant r)$ ima sve tražene osobine. □

U razlaganju $n = p_1 \dots p_r$ se jedan dati prost broj može pojaviti više puta kao faktor. Zbog toga je uobičajeno da u razlaganju broja na proste činioce identične faktore "okupimo" u stepene *različitih* prostih brojeva:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}. \tag{3.1}$$

Razlaganje (3.1) broja n se zove *kanonički oblik* za $n > 1$. Iz osnovne teoreme aritmetike neposredno sledi da je on jedinstven do na poredak stepeni prostih brojeva $p_i^{\alpha_i}$ (i zapravo je jedinstven ako, na primer, zahtevamo da je $p_1 < p_2 < \cdots < p_k$). Primetimo da se zapravo i broj $n = 1$ može zapisati u ovom obliku, kao $1 = p_1^0 \dots p_k^0$, ali se tada gubi na jedinstvenosti razlaganja. Ipak, u mnogim situacijama je pogodno da se broj 1 prikazuje na ovakav način.

Kanonički oblik prirodnog broja nam omogućava veoma dobru "kontrolu" nad njegovim deliocima, kao što to naredno tvrđenje pokazuje.

Tvrđenje 3.2. *Neka je $n > 1$ prirodan broj čiji je kanonički oblik dat sa* (3.1)*. Tada $d \mid n$ ako i samo ako je*

$$d = p_1^{\beta_1} \dots p_k^{\beta_k},$$

gde je $0 \leqslant \beta_i \leqslant \alpha_i$ za sve $1 \leqslant i \leqslant k$.

Dokaz. ($\Rightarrow$): Ako $d \mid n$, tada je $n = dq$ za neko $q \in \mathbb{Z}^+$; stoga se kanonički oblik broja n dobija množenjem kanoničkih oblika brojeva d i q. To znači, između ostalog, da je svaki prost faktor p koji se pojavljuje u kanoničkom obliku broja d sa nenula eksponentom prisutan i u n sa nenula eksponentom, i pri tome se p pojavljuje u n sa najmanje onolikim stepenom kao u d. Otuda mora biti $0 \leqslant \beta_i \leqslant \alpha_i$ za sve i.

($\Leftarrow$): Ako je d oblika kao u formulaciji tvrđenja, tada za

$$q = p_1^{\alpha_1 - \beta_1} \dots p_k^{\alpha_k - \beta_k} \in \mathbb{Z}^+$$

važi $n = dq$, tj. $d \mid n$. □

Broj delilaca prirodnog broja $n > 0$ označavamo sa $d(n)$. Primetimo da je broj n prost ako i samo ako je $d(n) = 2$. Funkcija $d(n)$ se veoma lako izračunava na osnovu kanoničkog oblika broja n.

Posledica 3.3. *Broj delilaca broja n, izražnog u kanoničkom obliku* (3.1)*, jednak je*

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1).$$

Dokaz. Po prethodnom tvrđenju, d je delilac broja n ako i samo ako je

$$d = p_1^{\beta_1} \dots p_k^{\beta_k}$$

za neke $0 \leqslant \beta_i \leqslant \alpha_i$, $1 \leqslant i \leqslant k$. Prema tome, svaki niz brojeva $(\beta_1, \dots, \beta_k)$ sa datim ograničenjima opisuje jedan delilac broja n; osnovna teorema aritmetike obezbeđuje da različiti nizovi eksponenata daju različite delioce. Broj β_i se u tom nizu može izabrati na $\alpha_i + 1$ načina; kako su svi ti izbori nezavisni, rezultat sledi. □

U sličnom stilu se može izraziti i NZD dva broja.

Tvrđenje 3.4. *Neka su prirodni brojevi $a, b > 0$ dati u svojim "proširenim" kanoničkim oblicima*

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \qquad b = p_1^{\beta_1} \dots p_k^{\beta_k},$$

što znači da je $\alpha_i, \beta_j \geqslant 0$ *za sve* $1 \leqslant i, j \leqslant k$. *Tada je*

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} \dots p_k^{\min(\alpha_k, \beta_k)}.$$

Dokaz. Neka je

$$d = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}.$$

Pošto je $\min(\alpha_i, \beta_i) \leqslant \alpha_i$ i $\min(\alpha_i, \beta_i) \leqslant \beta_i$, sledi da $d \mid a$ i $d \mid b$, tj. d je zajednički delilac za a i b. S druge strane, neka je c zajednički delilac za a i b. Po Tvrđenju 3.2, tada je

$$c = p_1^{\gamma_1} \dots p_k^{\gamma_k},$$

pri čemu je $\gamma_i \leqslant \alpha_i$ i $\gamma_i \leqslant \beta_i$ za sve $1 \leqslant i \leqslant k$. Prema tome, $\gamma_i \leqslant \min(\alpha_i, \beta_i)$, odakle $c \mid d$. Stoga je $d = (a, b)$. □

Međutim, treba skrenuti pažnju da gornje tvrđenje—iako deluje veoma jednostavno i intuitivno—zapravo nije pogodno za praktične, računske primene, i da sa stanovišta teorije algoritamske složenosti daje loše rezultate. Naime, Euklidov algoritam nalazi NZD dva broja u *polinomnom vremenu*, tačnije, broj elementarnih operacija potrebnih za nalaženje (a, b) se može ograničiti kvadratnom funkcijom po broju cifara većeg od brojeva a, b. S druge strane, nalaženje NZD-a na osnovu gornjeg tvrđenja pretpostavlja da su dati brojevi već faktorisani na proste činioce, tj. dati u svojim kanoničkim oblicima. Upravo tu se nalazi problem: nije poznato da li uopšte postoji (brz) algoritam koji radi u polinomnom vremenu, a koji razlaže dati broj na proste faktore. Zapravo, značajan deo kriptografije, zaštite komunikacija i, specijalno, dobar deo bezbednosti bankarskih sistema zasniva se na (slepoj) pretpostavci da takav algoritam za faktorizaciju ne postoji.

Kažemo da je $m \in \mathbb{Z}^+$ *najmanji zajednički sadržalac (NZS)* celih brojeva $a, b > 0$ ako važi:

(i) $a \mid m$, $b \mid m$.
(ii) Za sve $c \in \mathbb{Z}^+$ takve da $a \mid c$ i $b \mid c$ važi $c \geqslant m$.

NZS brojeva a i b označavamo sa $[a, b]$. Očito, $[a, b] \leqslant ab$, budući da je ab svakako zajednički sadržalac za a i b, odakle je očita egzistencija (i jedinstvenost) NZS-a. Slično kao i u slučaju NZD-a može se pokazati da se uslov $c \geqslant m$ iz tačke (ii) može zameniti sa $m \mid c$: NZS dva broja je delilac svakog njihovog zajedničkog sadržaoca. Međutim, to se može sada i neposredno zaključiti iz osnovne teoreme aritmetike. Neka od najbitnijih svojstava NZS-a su sumirana u narednom tvrđenju.

Tvrđenje 3.5.

(1) *Za prirodne brojeve* $a, b > 0$ *date u svojim proširenim kanoničkim oblicima*

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \qquad b = p_1^{\beta_1} \dots p_k^{\beta_k},$$

gde je $\alpha_i, \beta_j \geqslant 0$ *za sve* $1 \leqslant i, j \leqslant k$, *važi*

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} \dots p_k^{\max(\alpha_k, \beta_k)}.$$

(2) *Za sve prirodne brojeve* $a, b, c > 0$ *važi* $a \mid c$ *i* $b \mid c$ *ako i samo ako* $[a, b] \mid c$.
(3) *Za sve prirodne brojeve* $a, b, c > 0$ *važi*

$$(a, b)[a, b] = ab.$$

Dokaz. (1) Neka je

$$m = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}.$$

Prema Tvrđenju 3.2, važi $a \mid m$ i $b \mid m$, tako da je m zajednički sadržalac za a i b. Ako je c pak proizvoljan sadržalac brojeva a i b, tada je, po istom tom tvrđenju, $c = p_1^{\gamma_1} \dots p_k^{\gamma_k}$, pri čemu je $\alpha_i \leqslant \gamma_i$ i $\beta_i \leqslant \gamma_i$ za sve $1 \leqslant i \leqslant k$. Sledi da je $\max(\alpha_i, \beta_i) \leqslant \gamma_i$, pa važi $m \mid c$, tj. $m = [a, b]$.

(2) je direktna posledica tačke (1).

(3) sledi iz tačke (1), Tvrđenja 3.4, kao i činjenice da je $\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$ za bilo koja dva realna broja α, β. □

Iz osnovne teoreme aritmetike takođe sledi zaključak da su dva prirodna broja uzajamno prosta ako i samo ako nemaju zajednički *prost* delilac. To odmah daje sledeći rezultat.

Lema 3.6. *Za sve prirodne brojeve* $a, b, c > 0$ *važi* $(c, ab) = 1$ *ako i samo ako je* $(c, a) = 1$ *i* $(c, b) = 1$.

Na kraju dajemo rezultat koji opisuje kanonički oblik za $n!$, a koji je zgodan i primenljiv u mnogim zadacima. Primetimo da ako $p \mid n!$ za neki prost broj p, tada mora biti $p \mid m$ za neko $m \leqslant n$, pa samim tim imamo da je $p \leqslant n$.

Teorema 3.7 (Ležadrova formula)**.** *Ako je*

$$n = \prod_{p \leqslant n} p^{\alpha_p}$$

kanonički oblik broja $n!$*, tada je*

$$\alpha_p = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

Dokaz. Najpre, primetimo da je suma u gornjoj formuli zapravo konačna, jer se njen poslednji nenula sabirak pojavljuje kada je $k = \max(0, \lfloor \log_p n \rfloor)$. Neka je u daljem $p \leqslant n$ fiksiran prost broj.

Za $m \leqslant n$, označimo sa $\alpha_p(m)$ najveći prirodan broj α tako da $p^\alpha \mid m$; po uslovima teoreme,

$$\alpha_p = \alpha_p(1) + \dots + \alpha_p(n).$$

Ako sa ξ_k, $k \geqslant 1$, označimo broj elemenata m skupa $\{1, \dots, n\}$ za koje je $\alpha_p(m) = k$ (dakle, broj takvih m za koje $p^k \mid m$, ali $p^{k+1} \nmid m$), tada je

$$\alpha_p = \xi_1 + 2\xi_2 + \dots + k\xi_k + \dots . \tag{3.2}$$

Međutim, zbir

$$\xi_k' = \xi_k + \xi_{k+1} + \dots$$

za svako $k \geqslant 1$ predstavlja broj elemenata skupa $\{1, \ldots, n\}$ za koje je $\alpha_p(m) \geqslant k$, što je zapravo broj svih elemenata skupa $\{1, \ldots, n\}$ deljivih sa p^k. Očito,

$$\xi'_k = \left\lfloor \frac{n}{p^k} \right\rfloor .$$

S druge strane, iz (3.2) sledi

$$\alpha = \xi'_1 + \xi'_2 + \cdots + \xi'_k + \cdots ,$$

odakle odmah dobijamo traženu formulu. □