# Osnovni rezultati teorije brojeva

## Deljenje celih brojeva 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.

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

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

**Tvrđenje 1.** *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 $\varepsilon$ jedinični ceo broj. Tada, specijalno, važi $\varepsilon \mid 1$, pa je $1 = \varepsilon q$ za neko $q \in \mathbb{Z}$. Jasno, ni $\varepsilon$ ni $q$ ne mogu biti $0$, pa je $|\varepsilon|, |q| \geq 1$. 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, element $a + b\sqrt{2}$ je jedinični kad god važi $a^2 - 2b^2 = 1$. (Ova jednačina koja pripada klasi diofantskih jednačina poznatih kao *Pelove jednačine* 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 $\ell_1$ i $\ell_2$ tako da je $k = \ell_1\ell_2$.

**Tvrđenje 2.** *Ako su $\varepsilon, \delta$ 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 3.**

*(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 $\varepsilon$ 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 nekim celim brojem različitim od nule.

**Teorema 4.** *Za sve $a, b \in \mathbb{Z}$, $b \neq 0$, postoje jedinstveni brojevi $q, r \in \mathbb{Z}$ tako da je*

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

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

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

što je, dalje, ekvivalentno dvostrukoj nejednakosti

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

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

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

analogno kao i malopre vode dvostrukoj nejednakosti $q \geq a/b > q - 1$, 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 da, između ostalog, prirodne brojeve izražavamo u *brojevnim sistemima* sa datom osnovom (binarnom, dekadnom, ...). Ovo je precizirano narednim tvrđenjem.

**Posledica 5.** *Neka je $B > 1$ ceo broj. Tada se svako $A \in \mathbb{Z}^+$ na jedinstven način može zapisati u obliku*

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

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

Za reprezentaciju (zapis) broja $A$ u obliku (1) kažemo da je *u sistemu sa osnovom* $B$, dok su $a_i$ *cifre* tog zapisa. Kraće, možemo pisati i

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

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

## NZD i Euklidov algoritam

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 $|c| \leq |d|$.

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 6.** *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 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:

$$\begin{aligned}
a &= q_1 b + r_1, && \text{gde je } 0 \leq r_1 < |b|,\\
b &= q_2 r_1 + r_2, && \text{gde je } 0 \leq r_2 < r_1,\\
r_1 &= q_3 r_2 + r_3, && \text{gde je } 0 \leq r_3 < r_2,\\
&\vdots && \vdots\\
r_{k-1} &= q_{k+2} r_k + r_{k+1}, && \text{gde je } 0 \leq r_{k+1} < r_k,\\
&\vdots && \vdots\\
r_{n-2} &= q_n r_{n-1} + r_n, && \text{gde je } 0 \leq r_n < r_{n-1},\\
r_{n-1} &= q_{n+1} r_n && (r_{n+1} = 0).
\end{aligned}$$

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 $(a, b) \leq r_n$. 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 $r_n \leq (a, b)$. Prema tome, $r_n = (a, b)$, kao što se i tražilo. □

**Posledica 7.** *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 8.** *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 $ax + by = c$.*

**Tvrđenje 9.** *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 $1 \leq i \leq k$. 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 $k \geq 2$) *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 10.** *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 6 i njenoj Posledici 7 važi $c \mid (ab, cb) = (a, c)b = b$. □

## Prosti i nerazloživi brojevi, osnovna teorema aritmetike

Videli smo 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 $\varepsilon$ 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 11.** *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 Lemi 10 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.

**Primedba 12.** Pojmove *nerazloživog* odnosno *prostog* elementa je 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).

**Teorema 13** (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 $1 \leq i \leq r$, $1 \leq j \leq s$, tada je $r = s$ i postoji permutacija $\pi$ skupa $\{1, 2, \dots, r\}$ tako da je $p_i = q_{\pi(i)}$ za sve $1 \leq i \leq r$.*

*Dokaz. Egzistencija:* 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:* Pretpostavimo da je $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$; bez umanjenja opštosti, neka je $r \leq s$. 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 $1 \leq i \leq r$ 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 $\pi$ definisana sa $\pi(i) = j_i$ $(1 \leq i \leq r)$ 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:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}. \tag{2}$$

Razlaganje (2) 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 $p_1 < p_2 < \dots < p_k$). 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 14.** *Neka je $n > 1$ prirodan broj čiji je kanonički oblik dat sa* (2). *Tada $d \mid n$ ako i samo ako je*

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

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

*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 $0 \leq \beta_i \leq \alpha_i$ 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 15.** *Broj delilaca broja $n$, izražnog u kanoničkom obliku* (2)*, 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 $0 \leq \beta_i \leq \alpha_i$, $1 \leq i \leq k$. 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 $\beta_i$ 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 16.** *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 $\alpha_i, \beta_j \geq 0$ za sve $1 \leq i, j \leq k$. 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 $\min(\alpha_i, \beta_i) \leq \alpha_i$ i $\min(\alpha_i, \beta_i) \leq \beta_i$, 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 14, tada je

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

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

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 $c \geq m$.

NZS brojeva $a$ i $b$ označavamo sa $[a, b]$. Očito, $[a, b] \leq ab$, 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 $c \geq m$ 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 17.**

*(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 $\alpha_i, \beta_j \geq 0$ za sve $1 \leq i, j \leq k$, 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 14, 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 $\alpha_i \leq \gamma_i$ i $\beta_i \leq \gamma_i$ za sve $1 \leq i \leq k$. Sledi da je $\max(\alpha_i, \beta_i) \leq \gamma_i$, pa važi $m \mid c$, tj. $m = [a, b]$.

(2) je direktna posledica tačke (1).

(3) sledi iz tačke (1), Tvrđenja 16, kao i činjenice da je

$$\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$$

za bilo koja dva realna broja $\alpha, \beta$. □

## Prsteni ostataka po modulu, Vilsonova teorema

Imajući u vidu postupak deljenja sa ostatkom, prirodno je izvršiti klasifikaciju skupa $\mathbb{Z}$ celih brojeva na klase brojeva koji daju isti ostatak pri deljenju nekim fiksnim deliteljem $m$. Ovo se realizuje binarnom relacijom *kongruencije po modulu* $m$. Naime, definišemo da je

$$a \equiv b \pmod{m} \quad \text{ako i samo ako} \quad m \mid a - b.$$

Pri tome ne predstavlja nikakvo ograničenje opštosti ako pretpostavimo da je $m > 0$, budući da $m \mid a - b$ ako i samo ako $-m \mid a - b$.

Termin "kongruencija" ovde nije odabran slučajno; sledeće tvrđenje pokazuje da je $\cdot \equiv \cdot \pmod{m}$ zaista kongruencija prstena $\mathbb{Z}$.

**Tvrđenje 18.** *Za sve $a, b, c, d \in \mathbb{Z}$ i $m > 0$ važi:*

*(i)* $a \equiv a \pmod{m}$.

*(ii)* $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

*(iii)* $a \equiv b \pmod{m},\ b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

*(iv)* $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \Rightarrow$
$a+c \equiv b+d \pmod{m},\ a-c \equiv b-d \pmod{m}$.

*(v)* $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.

*Dokaz.* Ilustracije radi, pokazaćemo samo (v). Po datim uslovima, imamo da $m \mid a-b$ i $m \mid c-d$. Zbog toga,

$$m \mid c(a-b)+b(c-d) = ac-bd,$$

tj. $ac \equiv bd \pmod m$. □

Obratno, nije teško pokazati da su sve kongruencije prstena $\mathbb{Z}$ iscrpljene kongruencijama po modulu $m > 0$.

Za $a \in \mathbb{Z}$ i fiksan modul $m$, klasu ekvivalencije elementa $a$ u odnosu na relaciju $\cdot \equiv \cdot \pmod m$ označavamo sa $(a)_m$ i zovemo je *klasa ostatka*. Na taj način, imamo particiju skupa $\mathbb{Z}$ na $m$ klasa, od kojih je svaka (dvostrano) beskonačna aritmetička progresija. Proizvoljna transverzala ove particije (skup brojeva takav da svakoj klasi pripada tačno jedan odabrani broj) je *potpun sistem ostataka*. Očigledno, $0, 1, \ldots, m-1$ jeste jedan potpun sistem ostataka; njega zovemo *standardnim*.

Na skupu svih klasa ostataka $(a)_m$ po modulu $m$ definiše se algebarska struktura uvođenjem operacija $+$ i $\cdot$ definisanih sa

$$(a)_m + (b)_m = (a+b)_m,$$
$$(a)_m (b)_m = (ab)_m.$$

Ove definicije su logički dobre, tj. ne zavise od izbora predstavnika $a, b$, budući da smo u Tvrđenju 18 pokazali da je $\cdot \equiv \cdot \pmod m$ zaista kongruencija prstena $\mathbb{Z}$. Na taj način, skup svih klasa ostataka $\{(a)_m : 0 \le a \le m-1\}$ zajedno sa opisanim operacijama takođe čini prsten, koji zovemo *prsten ostataka po modulu* $m$ i označavamo sa $\mathbb{Z}_m$. Naime, ako je $m\mathbb{Z}$ ideal od $\mathbb{Z}$ koji se sastoji od svih celih brojeva deljivih sa $m$, tada je $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$. Drugim rečima, preslikavanje koje svakom celom broju dodeljuje njegovu klasu ostatka po modulu $m$ je sirjektivni homomorfizam prstena $\mathbb{Z} \to \mathbb{Z}_m$, i jezgro tog homomorfizma je baš $m\mathbb{Z}$. Prsten $\mathbb{Z}_m$ je, baš kao i $\mathbb{Z}$, komutativan i ima jedinicu – u pitanju je klasa $(1)_m$.

Aditivna grupa $(\mathbb{Z}_m, +)$ prstena ostataka je uvek ciklična: ona je očito generisana klasom $(1)_m$, pošto je

$$(a)_m = \underbrace{(1)_m + \cdots + (1)_m}_{a \text{ sabiraka}}$$

i $(0)_m = (m)_m$. S druge strane, u odnosu na množenje imamo komutativni monoid sa nulom $(\mathbb{Z}_m, \cdot)$ koji u opšem slučaju nije grupa, budući da ne moraju svi njegovi (nenula) elementi biti invertibilni u odnosu na jedinicu $(1)_m$.

**Tvrđenje 19.** *$(a)_m$ je invertibilan element prstena $\mathbb{Z}_m$ ako i samo ako važi $(a, m) = 1$.*

Kako je invertibilnost elementa $(a)_m$, tj. postojanje klase $(x)_m$ takve da je $(a)_m(x)_m = (1)_m$, ekvivalentna egzistenciji rešenja kongruencije

$$ax \equiv 1 \pmod{m},$$

prethodno tvrđenje je neposredna posledica sledećeg.

**Tvrđenje 20.** *Kongruencijska jednačina*

$$ax \equiv b \pmod{m}$$

*ima rešenja ako i samo ako $(a, m) \mid b$.*

*Dokaz.* Neka je $s \in \mathbb{Z}$ tako da je $as \equiv b \pmod{m}$. Tada postoji $c \in \mathbb{Z}$ tako da je $as - b = mc$, odnosno $as + m(-c) = as - mc = b$. Prema tome, diofantska jednačina $ax+my = b$ ima rešenja, što je po Tvrđenju 9 ekvivalentno uslovu $(a, m) \mid b$. Obratno, ako važi ovaj uslov, tada i jednačina $ax + my = b$ ima rešenje $(x_0, y_0)$. Ali, tada je $ax_0 \equiv b \pmod{m}$, pa posmatrana linearna kongruencija ima rešenje. □

Klasa $(a)_m$ je *redukovana* ako je $(a, m) = 1$. Primetimo da je skup svih redukovanih klasa zatvoren na množenje: ako je $(a, m) = (b, m) = 1$, tada je i $(ab, m) = 1$, tj. $(ab)_m$ je takođe redukovana klasa. Prema tome, redukovane klase u odnosu na množenje čine podmonoid od $(\mathbb{Z}_m, \cdot)$ u kojem svaki element ima inverz; dakle, u pitanju je grupa, koju označavamo sa $\mathcal{U}_m$. Budući da su sve nenula klase po modulu $m$ redukovane ako i samo ako je $m$ prost broj, odmah imamo sledeći zaključak.

**Posledica 21.** *$\mathbb{Z}_m$ je polje ako i samo ako je $m$ prost broj.*

Kao što je poznato, u konačnom polju je proizvod svih nenula elemenata jednak $-1$. Specijalan slučaj ovog tvrđenja za polje $\mathbb{Z}_p$ ostataka po prostom modulu $p$ je u teoriji brojeva poznato kao *Vilsonova teorema*.

**Teorema 22** (Vilsonova teorema)**.** *Neka je $p$ prost broj. Tada je*

$$(p - 1)! \equiv -1 \pmod{p}.$$

*Dokaz.* Tvrđenje teoreme je očito tačno za $p = 2, 3$, pa pretpostavimo da je $p \geq 5$. Dokazaćemo da se skup $\{2, 3 \ldots, p-2\}$ može razbiti u $(p-3)/2$ parova tako da proizvod svakog para daje ostatak 1 pri deljenju sa $p$.

Naime, za svako $2 \leq a \leq p-2$, po Posledici 6.3, postoji tačno jedno rešenje linearne kongruencije

$$ax \equiv 1 \pmod{p}$$

u skupu $\{0, 1, \ldots, p-1\}$. Međutim, to rešenje očito nije $x = 0$, kao ni $x \in \{1, p-1\}$ (jer bi u suprotnom bilo $a \equiv \pm 1 \pmod{p}$, što nije slučaj). Prema tome, to rešenje, koje ćemo označiti sa $f(a)$, takođe pripada skupu $\{2, 3, \ldots, p-2\}$. Ovim smo definisali jednu transformaciju posmatranog skupa, tj. funkciju $f : \{2, 3, \ldots, p-2\} \to \{2, 3, \ldots, p-2\}$. Ova funkcija ima sledeća svojstva:

1. $af(a) \equiv 1 \pmod{p}$;
2. $f(f(a)) = a$, tj. ako je $f(a) = b$, tada je $f(b) = a$ (ovo je posledica prethodne tačke i jedinstvenosti rešenja kongruencije $f(a)x \equiv 1 \pmod{p}$ u skupu $\{2, 3, \ldots, p-2\}$);
3. $f(a) \neq a$ za sve $a \in \{2, 3, \ldots, p-2\}$ (u suprotnom bi bilo $a^2 \equiv 1 \pmod{p}$, tj. $p \mid a^2 - 1 = (a-1)(a+1)$, što je moguće samo ako je $a \equiv \pm 1 \pmod{p}$).

Drugim rečima $\{\{a, f(a)\} : a \in \{2, 3, \ldots, p-2\}\}$ predstavlja upravo traženo sparivanje.

Otuda odmah sledi da je

$$(p-1)! = 1 \cdot [(2 \cdot f(2)) \cdots] \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod{p},$$

što se i tražilo. □

Pri tome važi i obrat ove teoreme: ukoliko za neki prirodan broj $n \geq 2$ važi $(n-1)! \equiv -1 \pmod{n}$, tada $n$ mora biti prost; naime, ako je $n$ složen i $n \neq 4$, tada $n \mid (n-1)!$ (direktno se proverava da je $3! = 6 \equiv 2 \pmod{4}$).

## Ojlerova funkcija i Ojlerova teorema

*Ojlerova funkcija* $\varphi$ se definiše kao $\varphi(n) = |\mathcal{U}_n|$, broj redukovanih klasa ostataka po modulu $n$. Drugim rečima, $\varphi(n)$ je broj svih $a \in \{1, \ldots, n-1\}$ takvih da je $(a, n) = 1$.

Kada je $n$ stepen prostog broja, veoma je lako izračunati $\varphi(n)$.

**Lema 23.** *Za svaki prost broj $p$ i $\alpha \geq 1$ važi $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*

*Dokaz.* Za prirodan broj $m < p^\alpha$ važi $(m, p^\alpha) = 1$ ako i samo ako je $(m, p) = 1$, odnosno, ako i samo ako $p \nmid m$. Dakle, $\varphi(p^\alpha)$ je broj svih elemenata skupa $\{0, 1, \ldots, p^\alpha - 1\}$ koji nisu deljivi sa $p$, a što je očito $p^\alpha - \lfloor p^\alpha/p \rfloor = p^\alpha - p^{\alpha-1}$. □

Za kompleksnu funkciju $f : \mathbb{Z} \to \mathbb{C}$ jedne celobrojne promenljive (ovakve funkcije se ponekad zovu i *aritmetičke*) kažemo da je *multiplikativna* ako za sve $a, b \in \mathbb{Z}$ takve da je $(a, b) = 1$ važi

$$f(ab) = f(a)f(b).$$

Osim u slučaju kada je funkcija $f$ konstantna nula-funkcija, imamo da je $f(1) = 1$ i $f(-1) \in \{1, -1\}$ (iz tog razloga su zanimljivi jedino pozitivni argumenti, budući da za $a > 0$ važi $f(-a) = f(-1)f(a)$).

Sledeće tvrđenje navodimo bez dokaza.

**Lema 24.** *Ojlerova funkcija je multiplikativna.*

Eksplicitna formula za $\varphi(n)$ sada lako sledi iz zapažanja da, uz kanonički oblik (2) broja $n$, multiplikativno svojstvo Ojlerove funkcije implicira da je

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}).$$

**Teorema 25.** *Neka je $n > 1$ prirodan broj dat u kanoničkom obliku. Tada je*

$$\varphi(n) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \cdot \prod_{\substack{p \mid n \\ p \text{ prost}}} \left(1 - \frac{1}{p}\right).$$

Leonard Ojler (Leonhard Euler, 1707–1783) je 1736. dokazao tvrđenje u kome funkcija koja danas nosi njegovo ime igra centralnu ulogu i koje predstavlja uopštenje od ranije poznate "male" Fermaove teoreme.

**Teorema 26** (Ojlerova teorema)**.** *Neka je $a \in \mathbb{Z}$ i $m > 0$ tako da je $(a, m) = 1$. Tada je*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

*Dokaz.* Posledica Lagranžove teoreme je da u svakoj konačnoj grupi $G$ i za svako $g \in G$ važi

$$g^{|G|} = 1.$$

Tako, ako je $(a, m) = 1$, tj. $(a)_m \in \mathcal{U}_m$ je redukovana klasa, tada je

$$(a)_m^{|\mathcal{U}_m|} = (1)_m.$$

No, kako je $|\mathcal{U}_m| = \varphi(m)$, kongruencija u formulaciji teoreme je samo drugi način da se zapiše gornja jednakost iz grupe $\mathcal{U}_m$ invertibilnih elemenata prstena $\mathbb{Z}_m$. □

**Posledica 27** (Mala Fermaova teorema)**.** *Neka je $p$ prost broj i $a \in \mathbb{Z}$ takav da $p \nmid a$. Tada je*

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Drugim rečima, za sve cele brojeve $a$ važi $a^p \equiv a \pmod{p}$.*

*Dokaz.* Sledi direktno iz Ojlerove teoreme, pošto je $\varphi(p) = p - 1$ za svaki prost broj $p$. □

Prethodna teorema nosi ime po Pjeru de Fermau (Pierre de Fermat, 1601–1665), francuskom pravniku, jednom od najznačajnijih i najuspešnijih matematičara-amatera svih vremena.