DELJIVOST CELIH BROJEVA

1 Osnovne osobine

Definicija 1.1 *Neka su $a \neq 0$ i b celi brojevi. Ako postoji ceo broj m takav da je $b = ma$, onda kažemo da je a* **delitelj** *ili* **faktor** *broja b, b je* **sadržalac**, **višekratnik** *ili* **umnožak** *broja broja a, dok je m* **količnik** *koji se dobija pri delenju broja b sa brojem a. Ako je b deljivo sa a, onda to označavamo sa $a|b$ i kažemo jednostavno da a deli b. Ako $a|b$ i ako je $a \neq b$, kažemo da je a* **pravi delitelj broja** *b.*

Ako $a|b$, očigledno je da $a|(-b)$, $(-a)|b$ i $(-a)|(-b)$. Stoga se pri razmatranju deljivosti obično ograničavamo na nenegativne cele brojeve.

Teorema 1.1 *Ako je ceo broj b deljiv celim brojem $a \neq 0$, onda je njihov količnik jednoznačno određen.*

Dokaz: Ako je broj b deljiv brojem a, onda postoji ceo broj m kao njihov količnik, tako da je $b = ma$. Ako bi postojao još neki količnik n koji se dobija pri delenju broja b brojem a, onda bi važila jednakost $b = na$, pa bi stoga bilo $ma = na$. Kako je $a \neq 0$, iz poslednje jednakosti dobijamo da je $m = n$.

Teorema 1.2 *Neka su a, b, c proizvoljni nenegativni celi brojevi. Tada važi:*
(a) ako $a|b$ i ako je $b \neq 0$, onda je $0 < a \leq b$;
(b) ako $a|b$ i $b|a$, $a \neq 0 \neq b$, onda je $a = b$;
(c) ako $a|b$ i $b|c$, onda $a|c$.

Dokaz: (a) Ako $a|b$, tada po definiciji postoji nenegativan ceo broj m takav da je $b = ma$. Kako je $b > 0$, brojevi a i m su pozitivni, tj. $1 \leq a$ i $1 \leq m$, pa je

$$b = ma \geq a \cdot 1 = a > 0\,.$$

(b) Pretpostavimo da $a|b$ i $b|a$. Tada je $a \leq b$ i $b \leq c$ na osnovu tvrđenja koje smo dokazali pod (a), pa je $a = b$ zbog antisimetričnosti relacije uređenja u skupu $\mathbb{N}$.

(c) Ako $a|b$ i $b|c$, onda postoje celi brojevi m i n takvi da je $b = ma$ i $c = nb$. No onda je $c = nma$, pa kako je nm ceo broj, sledi da $a|b$.

Posledica 1.1 *Relacija $|$ je relacija uređenja u skupu prirodnih brojeva $\mathbb{N}$.*

Teorema 1.3 *Neka su a, b, c, d proizvoljni celi brojevi. Tada važe sledeća tvrđenja:*
(a) ako $a|b$ i $a|c$, onda $a|(rb + sc)$ za proizvoljne cele brojeve r i s;
(b) ako $a|b$ i $c|d$, onda $ac|bd$;
(c) ako su brojevi b i c deljivi brojem a, i ako $b|c$, onda $\frac{b}{a}\big|\frac{c}{a}$.

Dokaz: (a) Ako $a|b$ i $a|c$, onda postoje celi brojevi m i n takvi da je $b = ma$ i $c = na$. No onda je

$$rb + sc = rma + sna = (rm + sn)a\,.$$

Kako je $rm + sn$ ceo broj, to $a|(rb + sc)$

(b) Kako $a|b$ i $c|d$, postoje celi brojevi m i n takvi da je $b = ma$ i $d = nc$. Odavde sledi da je $bd = (mn)ac$, pa kako je mn ceo broj, to $ac|bd$.

(c) Pošto su brojevi b i c deljivi brojem a, brojevi $\frac{b}{a}$ i $\frac{c}{a}$ su celi. Kako $b|c$, postoji ceo broj m takav da je $c = mb$, odakle sledi da je $\frac{c}{a} = m\frac{b}{a}$, što dokazuje da $\frac{b}{a}\big|\frac{c}{a}$.

Posledica 1.2 *Relacija | u skupu celih brojeva ima sledeća svojstva:*
(a) *ako $a|b$, tada $a|mb$ i $ma|mb$;*
(b) *ako $a|b$ i $a|c$, tada $a|(b + c)$ i $a|(b - c)$;*
(c) *ako $a_i|b_i$, $i = \overline{1,n}$, tada $a_1 \dots a_n|b_1 \dots b_n$;*
(d) *ako $a|b$, tada $a^n|b^n$ za svako $n \in \mathbb{N}$;*
(e) *ako su u jednakosti*

$$a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_m\,,$$

svi sabirci sem jednog deljivi celim brojem c, onda je i taj jedan deljiv brojem c.

Zadaci za vežbanje

1. Dokazati da $n|n + 1$ onda i samo onda ako je $n = \pm 1$.
2. Dokazati da svaki od brojeva $1, 2, \dots, k$ deli bar jedan od brojeva $n + 1, n + 2, \dots, n + k$. Ako je n neparan broj, dokazati da je $n(n^2 - 1$ deljiv sa 24.
3. Dokazati da je kvadrat celog broja deljiv sa 4 ili je oblika $8n + 1$.
4. Dokazati da je kvadrat brojeva koji nisu deljivi ni sa 2 ni sa 3 oblika $12n + 1$.
5. Dokazati da (a) $9|10^n - 1$; (b) $11|10^n + (-1)^{n-1}$
6. Dokazati da je zbir $2n + 1$ uzastopnih brojeva deljiv sa $2n + 1$.

2 Delenje sa ostatkom

Teorema 2.1 (Algoritam deljenja) *Za svaki par celih brojeva a i $b \neq 0$ jednoznačno je određen par celih brojeva q i r za koje je*

$$a = bq + r\,, \quad 0 \leq r < |b|\,.$$

Dokaz: Dokažimo najpre egzistenciju brojeva q i r. Razmotrimo najpre slučaj kada je $a \geq 0$. Označimo sa $S = \{m \in \mathbb{Z} : m|b| > a\}$. Kako je $a + 1 \in S$, to je S neprazan podskup skupa prirodnih brojeva $\mathbb{N}$, pa ima najmanji element.

Neka je $s = \min S$ i $q' = s - 1$. Tada $q' \notin S$, pa je stoga $q'|b| \leq a$. Stoga je $r = a - q'|b| \geq 0$. Sdruge strane je $s|b| > a$, jer je $s \in S$. Stoga je

$$|b| = s|b| - q'|b| > a - q'|b| = r\,,$$

čime smo pdokazali da je $0 \leq r < |b|$. Iz definicione jednakosti za r imamo da je $a = q'b + r$. Kako je $|b| = b \cdot \mathrm{sgn}(b)$, to je $a = bq + r$ za $q = q' \cdot \mathrm{sgn(b)}$.

Neka je sada $a < 0$. Kako je $-a > 0$, prema dokazanom slučaju postoje $s, r' \in \mathbb{Z}$ takvi da je $-a = s|b| + r'$ i $0 \leq r' < |b|$. Sada je $a = -s|b| - r'$ i $-|b| < r' \leq 0$. Ako je $r' = 0$, onda je za $q = -s \cdot \mathrm{sgn(b)}$ i $r = r' = 0$ tvrđenje zadovoljeno. Međutim, ako je $r' > 0$, onda $-r'$ ne zadovoljava tražene nejednakosti. Zbog toga radimo popravku:

$$a = -s|b| - r' = -s|b| - |b| + |b| - r' = (-s-1)|b| + (|b| - r')\,.$$

Neka je $q' = -s - 1$, $r = |b| - r'$. Sada je $a = |b|q' + r$. Proverimo nejednakosti za r. Kako je $0 < r' < |b|$, množenjem sa -1 dobijamo $-|b| < -r' < 0$. Dodavanjem $|b|$ dobijamo $0 < |b| - r' < |b|$, tj. $0 < r < |b|$. Za $q = q'\mathrm{sgn(b)}$ konačno imamo da je $a = bq + r$ i $0 < r < |b|$.

Ostaje da dokažemo jedinstvenost. Pretpostavimo da je $a = bq + r = bq_1 + r_1$, $0 \leq r, r_1 < |b|$. Ne umanjujući opštost dokaza možemo pretpostaviti da je $r \leq r_1$. Iz polazne jednakosti imamo da je $b(q - q_1) = r_1 - r$. Kako je $0 \leq r_1 - r < |b|$, to je $0 \leq |b(q - q_1)| < |b|$. Skraćivanjem sa $|b|$, dobijamo da je $0 \leq |q - q_1| < 1$. Kako je $|q - q_1|$ nenegativan ceo broj, to je $|q - q_1| = 0$. Otuda je $q = q_1$, pa je $r = r_1$.

Broj q u prethodno dokazanoj teoremi je **nepotpun količnik**, a r **ostatak pri delenju broja** a **brojem** b, ili kraće, samo ostatak. Ako je $r = 0$, onda je $a = bq$, tj. broj a je deljiv brojem b. Ako a nije deljivo sa b, uvek je $r \neq 0$.

Algoritam deljenja se često koristi u klasifikaciji brojeva. Na primer, za $b = 2$, ako je $r = 1$ imamo neparne brojeve oblika $a = 2q + 1$, dok za $r = 0$ imamo parne brojeve $a = 2q$. Sličnu situaciju imamo za $b = 3, 4, \ldots$ Tako dobijamo razbijanje skupa celih brojeva na disjunktne klase po modulu broja b. Dva cela broja pripadaju istoj klasi onda i samo onda ako je njihova razlika deljiva sa b. O ovome će više reči biti kada budemo govorili o kongruencijama.

Teorema 2.2 *Neka je b ceo broj veći od 1. Tada se svaki pozitivan ceo broj m na jedinstven način može prikazati u obliku*

$$m = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_0\,, \tag{1}$$

gde je $0 < a_n < b$ i $0 \leq a_i < b$, za $i = 0, 1, \ldots, n-1$.

Dokaz: Za dato $m \in \mathbb{Z}$ i $b > 1$ na osnovu Teoreme 2.1 postoje jedinstveno određeni celi brojevi q_0 i a_0 za koje važi

$$m = q_0 b + a_0\,, \qquad 0 \leq a_0 < b\,.$$

Očigledno je $q_0 \geq 0$. Ako je $q_0 = 0$ teorema je dokazana. Ako je q_0 pozitivan broj, deljenjem q_0 sa b dobijamo

$$q_0 = q_1 b + a_1, \qquad 0 \leq a_1 < b\,,$$

gde su q_1 i a_1 prema Teoremi 1. jedinstveno određeni celi brojevi. Nastavljajući ovaj postupak dobijamo

$$\begin{array}{lll}
m = q_0 b + a_0\,, & 0 \leq a_0 < b\,, & q_0 > 0\,,\\
q_0 = q_1 b + a_1\,, & 0 \leq a_1 < b\,, & q_1 > 0\,,\\
q_1 = q_2 b + a_2\,, & 0 \leq a_2 < b\,, & q_2 > 0\,,\\
\cdots & \cdots & \cdots\\
q_{n-2} = q_{n-1} b + a_{n-1}\,, & 0 \leq a_{n-1} < b\,, & q_{n-1} > 0\,,\\
q_{n-1} = q_n b + a_n\,, & 0 \leq a_n < b\,, & q_n = 0\,.
\end{array}$$

Kako je $m > q_0 > q_1 > \cdots > 0$ sledi da je na ovaj način jednoznačno određen ceo pozitivan broj q_{n-1} koji je manji od broja b. Iz poslednje jednakosti imamo da je $a_n = q_{n-1}$, pa je koeficijent a_n pozitivan broj.

Zamenom dobijamo da je

$$\begin{array}{rcl}
m & = & q_0 b + a_0 =\\
 & = & (q_1 b + a_1) b + a_0 = q_1 b^2 + a_1 b + a_0 =\\
 & & \cdots\cdots\cdots\\
 & = & (q_{n-1} b + a_{n-1}) b^{n-1} + \cdots + a_1 b + a_0 =\\
 & = & q_{n-1} b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 =\\
 & = & a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0\,.
\end{array}$$

Dobijena reprezentacija broja m je jedinstvena, jer su koeficijenti a_i, $i = 0, 1, \ldots, n$, na osnovu Teoreme 1. jednoznačno određeni.

Ako su zadovoljeni uslovi Teoreme 5., tada za broj m predstavljen u obliku (1) kažemo da je napisan u brojevnom sistemu za osnovu b. Broj **b** je **baza** ili **osnova** datog brojevnog sistema, a sam broj m zapisujemo u obliku

$$(a_n a_{n-1} \cdots a_0)_b\,.$$

Primer 2.1 Neka je $a \in \mathbb{Z}$, $n \in \mathbb{N}^+$. Označimo sa $rem_n(a)$ ostatak pri deljenju broja a brojem n. Funkcija $rem_n(a)$ preslikava skup $\mathbb{Z}$ u skup $\{0, 1, \ldots, n-1\}$. Da se sve vrednosti funkcije $rem_n(a)$ realizuju, neposredno sledi iz činjenice da je za $0 \leq a < n$ $rem_n(a) = a$. Tako npr. funkcija rem_2 ima vrednosti 0 i 1; $rem_2(2k) = 0$, dok je $rem_2(2k+1) = 1$ za svako $k \in \mathbb{Z}$. Funkcija rem_4 ima četiri vrednosti: $0, 1, 2, 3$. Za $i \in \{0, 1, 2, 3\}$ definišimo skup $\mathcal{C}_i = \{a \in \mathbb{Z} : rem_4(a) = i\}$. Familija $\{\mathcal{C}_i : i = \overline{0,3}\}$ čini particiju skupa $\mathbb{Z}$, tj. to su disjunktni skupovi i svaki ceo broj pripada jednom od njih. Primetimo da se sa ovim skupovima dosta pravilno računa. Pokažimo da je proizvod ma koja dva broja iz $\mathcal{C}_1$ opet u $\mathcal{C}_1$.

Neka su $a, b \in \mathcal{C}_1$. Tada postoje brojevi $k, l \in \mathbb{Z}$, tako da je $a = 4k + 1$ i $b = 4l + 1$, pa je

$$a \cdot b = (4k + 1)(4l + 1) = 16kl + 4k + 4l + 1 = 4(4kl + k + l) + 1\,,$$

što dokazuje da je $ab \in \mathcal{C}_1$. Slično se dokazuje da je za $a \in \mathcal{C}_1$ i $b \in \mathcal{C}_3$, $ab \in \mathcal{C}_3$. Čitaocu prepuštamo da ispita računanje sa klasama $\mathcal{C}_i$.

Definicija 2.1 *Neka je* $D(a) = \{b \in \mathbb{Z}^+ : b|a\}$*, gde je* $a \in \mathbb{Z}$*. Ako je* $a > 1$ *i* $D(a) = \{1, a\}$*, onda kažemo da je* a **prost broj**.

Nadalje ćemo proste brojeve označavati isključivo slovom p sa odgovarajućim indeksima.

Napomenimo da se u grafiku relacije | prosti brojevi nalaze u drugom nivou. Ako posmatramo skup $\mathbb{N}_2 := \mathbb{N}^+ \setminus \{1\}$ sa relacijom | koja je generisana sa $\mathbb{N}^+$, onda su prosti brojevi u prvom nivou delimično uređenog skupa $(\mathbb{N}_2, |\,)$ i pretstavljaju minimalne elemente. U matematici se uvek teži da se svi elementi neke strukture predstave pomoću minimalnih. U daljem izlaganju mi ćemo pokazati da se svaki ceo broj može prikazati pomoću prostih brojeva i da je taj prikaz jedinstven. Upravo ta činjenica najbolje govori o značaju prostih brojeva.

Definicija 2.2 *Neka je* $D(a, b) = D(a) \cap D(b)$*, gde su* $a, b \in \mathbb{Z}$*,* $a, b \neq 0$*. Broj* $(a, b) := \max D(a, b)$ *je* **najveći zajednički delilac** *brojeva* a *i* b*. Ako je* $(a, b) = 1$*, tada kažemo da su brojevi* a *i* b **uzajamno prosti**.

Pokažimo da je definicija korektna, tj. da za svaka dva broja $a, b \in \mathbb{Z} \setminus \{0\}$ postoji (a, b). Kako $1|a, b$, to je skup $D(a, b)$ neprazan. Osim toga je $c \leq |a|$ za svako $c \in D(a, b)$, pa je skup $D(a, b)$ ograničen neprazan skup prirodnih brojeva. Stoga $\max D(a, b)$, odn. (a, b) postoji. Primetimo na kraju da je za $a, b \in \mathbb{Z}$, $(a, b) = (|a|, |b|)$. Stoga u nastavku uvek pretpostavljamo da je u oznaci (a, b) $a, b \in \mathbb{N}^+$.

3 Ceo deo realnog broja

Neka su a i $b \neq 0$ celi brojevi. Pretpostavimo da b ne deli a. Na osnovu Teoreme 2.1 postoje jednoznačno određeni brojevi q i r takvi da je

$$a = bq + r\,, \qquad 0 < r < |b|\,,$$

odakle je za $b > 0$

$$\frac{a}{b} = q + \frac{r}{b}\,, \qquad 0 < \frac{r}{b} < 1\,. \tag{1}$$

Za $b < 0$ treba zameniti b sa $-b$, pa tako imamo prethodni slučaj. Prema tome $\frac{a}{b}$ je realan broj jednak zbiru celog broja q i pravog razlomka $\frac{r}{b}$. Iz relacije (1) dobijamo da je

$$q < \frac{a}{b} < q + 1\,,$$

odakle vidimo da je q najveći ceo broj koji nije veći od broja $\frac{a}{b}$. Broj q se naziva **ceo deo** realnog broja $\frac{a}{b}$ i označava sa $\left[\frac{a}{b}\right]$.

Još opštije: ceo deo realnog broja x je najveći ceo broj koji nije veći od x. Obeležava se sa $[x]$. Iz definicije sledi da je

$$[x] \leq x < [x] + 1\,,$$

a ako je x ceo broj, tada i samo tada je $[x] = x$. Iz definicije celog dela realnog broja sledi relacija

$$x = [x] + \{x\}\,, \quad \text{gde je} \quad 0 \leq \{x\} < 1\,.$$

Broj $\{x\}$ se naziva **decimalni deo** realnog broja X.

Teorema 3.1 *Neka su x i y realni brojevi, a m ceo broj. Tada je*

(*a*) $[x + m] = [x] + m$*;*

(*b*) $[x] + [y] \leq [x + y] \leq [x] + [y] + 1\,,$

ili, pošto su sva tri broja cela,

$$[x + y] = [x] + [y] \quad \textit{ili} \quad [x + y] = [x] + [y] + 1\,;$$

(*c*) $\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]\,, \quad m > 0\,.$

Dokaz: (a) Neka je $x = [x] + \{x\}$. Pošto je $x + m = [x] + \{x\} + m$, $0 \leq \{x\} < 1$, a $[x] + m$ je ceo broj, sleduje da je $[x + m] = [x] + m$.

(b) Pođimo od izraza $[x + y] = [x + \{x\} + y + \{y\}]$ i primenimo svojstvo celog dela koje smo dokazali pod (a):

$$[[x] + [y] + \{x\} + \{y\}] = [x] + [y] + [\{x\} + \{y\}]\,.$$

Tada je $[x + y] = [x] + [y] + [\{x\} + \{y\}]$. Kako je $0 \leq [\{x\} + \{y\}] < 2$, to je ceo broj $[\{x\} + \{y\}]$ jednak 0 ili 1. Stoga je

$$[x + y] = [x] + [y] \quad \text{ili} \quad [x + y] = [x] + [y] + 1\,,$$

čime smo dokazali da je

$$[x] + [y] \leq [x + y] \leq [x] + [y] + 1\,.$$

(c) Na osnovu Teoreme 2.1 za cele brojeve $[x]$ i $m \neq 0$ postoje celi brojevi q i r takvi da je

$$[x] = mq + r\,, \quad 0 \leq r < m\,. \tag{1}$$

Kako je $[x] = x - \{x\}$, to je $x = mq + r + \{x\}$, pa je

$$\frac{x}{m} = q + \frac{r + \{x\}}{m}\,. \tag{2}$$

Iz uslova koje zadovoljavaju brojevi r i $\{x\}$ takođe je

$$0 \leq \frac{r+\{x\}}{m} < 1\,, \tag{3}$$

pa je zbog (2) i (3)

$$\left[\frac{x}{m}\right] = q\,. \tag{4}$$

Kako je zbog (1)

$$\frac{[x]}{m} = q + \frac{r}{m}\,, \quad \text{gde je} \quad 0 \leq \frac{r}{m} < 1\,,$$

to je

$$\left[\frac{[x]}{m}\right] = q\,. \tag{5}$$

Sada iz jednakosti (4) i (5) sledi tražena jednakost.

Posledica 3.1 (*a*) *Ako je* $a > 0$ *ceo broj i* $[ax] = b$*, tada je*

$$[x] = \left[\frac{b}{a}\right];$$

(*b*) *Za svaki realan broj važi jedna od jednakosti*

$$[x] + [-x] = 0 \quad \textit{ili} \quad [x] + [-x] = -1\,,$$

prema tome da li je x *ceo broj ili ne;*

(*c*) *Za realne brojeve* $x_1, x_2, \ldots, x_n$ *važi jednakost*

$$[x_1] + [x_2] + \cdots + [x_n] \leq [x_1 + x_2 + \cdots + x_n] = [x_1] + [x_2] + \cdots + [x_n] + n - 1\,.$$

Dokaz: (a) Kako je $[ax] = b$ i a ceo broj različit od nule, to je prema svojstvu (c) koje smo dokazali u prethodnoj teoremi

$$\left[\frac{b}{a}\right] = \left[\frac{[ax]}{a}\right] = \left[\frac{ax}{a}\right] = [x]\,.$$

Dokaz: (b) Zamenom $y = -x$ u (b) prethodne teoreme odmah dobijamo da je $[x] + [-x] = [x + (-x)] = 0$ ili $[x] + [-x] + 1 = [x + (-x)] = 0$, već prema tome da li je x ceo broj ili ne.

Dokaz: (c) Dokaz se izvodi indukcijom. Za $n = 2$ jednakost važi na osnovu nejednakosti (b) dokazanoj u prethodnoj teoremi. Pretpostavimo da je tvrđenje tačno za $n = m$, tj. neka je

$$[x_1] + [x_2] + \cdots + [x_m] \leq [x_1 + x_2 + \cdots + x_m] \leq [x_1] + [x_2] + \cdots + [x_m] + m - 1\,.$$

Kako je

$$\begin{aligned}[x_1+x_2+\cdots+x_m]+[x_{m+1}] &\leq [x_1+x_2+\cdots+x_{m+1}]\leq \\ &\leq [x_1+x_2+\cdots+x_m]+[x_{m+1}]+1\,,\end{aligned}$$

sabiranjem poslednjih dveju dvostrukih nejednakosti imamo da je

$$\begin{aligned}[x_1]+x_2]+\cdots+[x_{m+1}] &\leq [x_1+x_2+\cdots+x_{m+1}]\leq \\ &\leq [x_1]+[x_2]+\cdots+[x_{m+1}]+m\,,\end{aligned}$$

što je i trebalo dokazati.

Zadaci za vežbanje

1. Ako je $\frac{k}{n}\leq x-[x]<\frac{k+1}{n}$, gde je $k<n$prirodan broj, dokazati da je $[nx]-n[x]=k$.
2. Dokazati da je

$$[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]=[nx]\,.$$

3. Ako je $(a,b)=d$, gde su a i b prirodni brojevi, dokazati da je

$$\sum_{n=1}^{n-1}\left[\frac{bn}{a}\right]=\frac{(a-1)(b-1)}{2}+\frac{d+1}{2}\,.$$

4. Dokazati da je

$$\sum_{k=1}^{n}(2k-1)\left[\frac{n}{k}\right]=\sum_{k=1}^{n}\left[\frac{n}{k}\right]^2\,.$$

4 Prosti brojevi

Teorema 4.1 *Za svaki prirodan broj $n\in\mathbb{N}_2$ postoji prost broj p takav da $p|n$.*

Dokaz: Tvrđenje dokazujemo transfinitnom indukcijom. Neka je $n\in\mathbb{N}_2$ i neka je tvrđenje tačno za sve prirodne brojeve iz $\mathbb{N}_2$ koji su manji od n. Razlikujemo dva slučaja.

Broj n je prost. Tada je n prost broj koji deli n.

Broj n je složen. U tom slučaju je $D(n)\neq\{1,n\}$. Neka je $k\in D(n)\setminus\{1,n\}$. Tada je $1<k<n$. Prema indukcijskoj hipotezi postoji prost broj p tako da $p|k$. Kako $k|n$, to $p|n$, pa je tvrđenje dokazano.

Teorema 4.2 *Neka je $n\in\mathbb{N}_2$ složen broj. Tada postoji prost broj $p\leq[\sqrt{n}]$.*

Dokaz: Kako je n složen broj, $D(n) \neq \{1, n\}$. Neka je $k \in D(n) \setminus \{1, n\}$. Pošto $k|n$, postoji prirodan broj l takav da je $n = kl$. Sobzirom na činjenicu da je $1 < k < n$, sledi da je i $1 < l < n$. Kako je $k \leq l$ ili $l \leq k$, ne umanjujući opštost dokaza, možemo pretpostaviti da je $l \leq k$. Prema prethodnom tvrđenju postoji prost broj p tako da $p|l$. Stoga je $p \leq l$, a time je $p \leq k$. Odatle je sada

$$p^2 \leq k \cdot l = n\,, \quad \text{tj.} \quad p \leq [\sqrt{n}]\,.$$

Primer 4.1 (Eratostenovo sito) Odredimo sve proste brojeve koju su manji od 100. Na osnovu prethodne teoreme dovoljno je, kao složene, odstraniti sve brojeve manje od 100 koji su deljivi sa 2,3,5,7 sem njih. Preostali brojevi manji od 100 su prosti. Tako imamo sledeću listu prostih brojeva koji su manji od 100:

$$2, 3, 5, 7, 11, 13, 17, 19, 13, 29, 31, 37, 41,$$
$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Teorema 4.3 *Prostih brojeva ima beskonačno mnogo.*

Dokaz: Dokaz izvodimo svođenjem na kontradikciju. Pretpostavimo da je skup P svih prostih brojeva konačan. Tada je $P = \{p_1, p_2, \ldots, p_n\}$ za neko $n \in \mathbb{N}$. Uočimo broj $M = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Kako je $M \in \mathbb{N}_2$, na osnovu Teoreme 4.1 postoji prost broj p takav da $p|M$. Kako je $p \in P$, to je $p = p_i$ za neko $i \leq n$. Dakle, $p_i|M$. Sdruge strane, kako je $M - 1 = p_i s$, gde je $s = p_1 \cdot \ldots \cdot_{i-1} p_{i+1} \cdot \ldots \cdot p_n$, to $p_i|M - 1$. No onda $p_i|M - (M - 1)$, tj. $p_i|1$. Kontradikcija.

Sledeća teorema je poznata kao OSNOVNA TEOREMA ARITMETIKE, što najbolje govori o njenom značaju u teoriji brojeva. Napomenimo da u formulaciji teoreme koristimo konvenciju da je proizvod po praznom skupu jednak 1.

Teorema 4.4 *Za svaki prirodan broj $n \in \mathbb{N}^+$ postoje jedinstveni $k \in \mathbb{N}$, prosti brojevi $p_1 < p_2 < \cdots < p_k$ i $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}^+$ tako da je*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}\,.$$

Izraz $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ nazivamo **prostom** *ili* **kanonskom faktorizacijom broja** n

Posledica 4.1 *Neka je $(p_n)_{n\in\mathbb{N}}$ skup prostih brojeva poređanih u rastući niz. Preslikavanje $f : \mathbb{N}^\omega \mapsto \mathbb{N}$ definisano sa*

$$f(\alpha_1, \ldots, \alpha_k) = p_1^{\alpha_1+1} \cdot \ldots \cdot p_k^{\alpha_k+1}$$

je 1-1 preslikavanje.

Dokaz: Neka je za $k, l \in \mathbb{N}^+$ i $(\alpha_1, \ldots, \alpha_k)\,,\ (\beta_1, \ldots, \beta_l)$

$$f(\alpha_1, \ldots, \alpha_k) = f(\beta_1, \ldots, \beta_l) = n\,.$$

Tada su $p_1^{\alpha_1+1} \cdot \cdots \cdot \ldots \cdot p_k^{\alpha_k+1}$ i $p_1^{\beta_1+1} \cdot \ldots \cdot p_l^{\beta_l+1}$ faktorizacije broja n. Kako n ima jedinstvenu faktorizaciju, to je $k = l$, pa je stoga za svako $i \leq k$ $\alpha_i + 1 = \beta_i + 1$. Time smo dokazali da je $(\alpha_1, \ldots, \alpha_k) = (\beta_1, \ldots, \beta_k)$. Dakle, f je 1-1 preslikavanje.

Posledica 4.2 *Prirodan broj je kvadrat onda i samo onda ako u prostoj faktorizaciji ima sve izložioce parne.*

Dokaz: Neka je $n \in \mathbb{N}_2$ i neka je $n = p_1^{\alpha_1} p_2 \alpha_2 \cdot \cdots \cdot \ldots \cdot p_k^{\alpha_k}$ kanonska faktorizacija broja n.

($\Rightarrow$) Neka je $n = m^2$ i neka je $m = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}$ kanonska faktorizacija broja m. Tada je

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = q_1^{2\beta_1} \cdot q_2^{2\beta_2} \cdot \ldots \cdot q_l^{2\beta_l}\,.$$

Kako je faktorizacija broja n jedinstvena, to je $k = l$, $p_i = q_i$ i $\alpha_i = 2\beta_i$ za svako $i \leq k$.

($\Leftarrow$) Pretpostavimo da broj n u svojoj kanonskoj faktorizaciji ima za izložioce parne brojeve. To znači da je $n = p_1^{2\alpha_1} \cdot p_2^{2\alpha_2} \cdot \ldots \cdot p_k^{2\alpha_k}$ za neko $k \in \mathbb{N}^+$, proste brojeve $p_1, \ldots, p_k$ i prirodne brojeve $\alpha, \ldots, \alpha_k$. Očigledno je da za $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ važi $n = m^2$.

Posledica 4.3 *Neka su $a, b, c \in \mathbb{N}^+$, $(a, b) = 1$ i $ab = c^2$. Tada postoje $k, l \in \mathbb{N}$ tako da je $a = k^2$ i $b = l^2$.*

Dokaz: Neka je $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, $b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}$. Kako je $(a, b) = 1$, to je $p_i \neq q_j$ za svako $i \leq k$ i svako $j \leq l$. Otuda je

$$c^2 = a \cdot b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}\,.$$

Kako je izraz na desnoj strani, do na uređivanje po veličini osnova, prosta faktorizacija broja c^2, to je prema prethodnom tvrđenju α_i paran broj za svako $i \leq k$, dok je β_j paran broj za svako $j \leq l$. To dokazuje da su a i b kvadrati prirodnih brojeva.

Zadaci za vežbanje

1. Jedina dva uzastopna prosta broja su 2 i 3. Dokazati.
2. Dokazati da je $n^4 + 1$ za $n > 1$ složen broj.
3. $4^{4n+2} + 1$ je složen broj za svako $n \geq 1$. Dokazati.
4. Dokazati da postoji proizvoljan broj uzastopnih brojeva koji nisu prosti.
5. Ako je n prirodan broj i $2^n - 1$ prost broj, dokazati da je n prost broj.

5 Relacija kongruencije po modulu

Definicija 5.1 *Neka su a, b i $m \neq 0$ celi brojevi. Broj a je* **kongruentan** *sa brojem b s obzirom na modul m, ako $m|a-b$ i to označavamo sa*

$$a \equiv b(\mathrm{mod}\, m) \quad \textit{ili sa} \quad a \equiv_m b\,.$$

Ako $a-b$ nije deljivo sa m tada je a **nekongruentno** sa b po modulu m. Ovo označavamo sa $a \not\equiv b(\mathrm{mod}\, m)$ ili sa $a \not\equiv_m b$.

Primer 5.1 Relacija

$$a \equiv 1(\mathrm{mod}\, 2)\,, \tag{1}$$

znači da je $a-1$ deljivo sa 2, tj. da postoji ceo broj m takav da je $a-1=2m$, odnosno $a=2m+1$. Dakle, a je neparan broj. Lako se proverava da važi i obrat. Naime, ako je a proizvoljan neparan broj, za njega važi relacija (1). Prema tome, relacija (1) je karakteristična za neparne brojeve.

Iz relacije (1) sledi da je $a^2 \equiv 1(\mathrm{mod}\, 8)$. Zaista, ako važi (1), onda je a neparan broj, dakle oblika $a=2m+1$, pa je $a^2=4m^2+4m+1$. Odavde sledi da je $a^2-1=4m(m+1)$. Brojevi m i $m+1$ su uzastopni, pa je jedan od njih paran. Stoga je a^2-1 deljivo sa 8, te je doista $a^2 \equiv 1(\mathrm{mod}\, 8)$.

Prema Definiciji 5.1, relacija

$$a \equiv b(\mathrm{mod}\, m) \tag{2}$$

označava da $m|a-b$, što opet znači da postoji ceo broj t takav da je $a-b=tm$, odnosno

$$a = b + tm\,. \tag{3}$$

Obratno, za svaki broj a oblika (3) važi relacija $m|a-b$, pa samim tim i (2). Na taj način smo dokazali da je *a kongruentno sa b po modulu m onda i samo onda ako postoji ceo broj t takav da je $a=b+mt$*. Ovaj iskaz možemo formulisati i na sledeći način.

Teorema 5.1 *Skup svih celih brojeva x kongruentnih sa a po modulu broja m dat je izrazom*

$$x = a + tm\,, \quad t = 0\,, \pm 1\,, \pm 2\,, \ldots$$

Teorema 5.2 *Brojevi a i b imaju jednake ostatke pri deljenju sa m onda i samo onda ako je $a \equiv b(\mathrm{mod}\, m)$.*

Dokaz: Ako je $a \equiv b(\mathrm{mod}\, m)$, tada postoji ceo broj t takav da je $a=b+tm$. Za brojeve b i $m \neq 0$ na osnovu Teoreme 2.1 postoje jednoznačno određeni celi brojevi q i r takvi da $b=qm+r$, $0 \leq r < |m|$, gde je r ostatak dobijen pri

deljenju broja b sa brojem m. Odavde sledi da je $a = m(q + t) + r$, gde je $0 \leq r < |m|$. Dakle, i broj a pri deljenju sa brojem m ima isti ostatak r.

Da dokažemo obrat, pretpostavimo da brojevi a i b imaju isti ostatak r pri deljenju sa brojem m. To znači da postoje celi brojevi q_1 i q_2 takvi da je $a = mq_1 + r$, $b = mq_2 + r$, $0 \leq r < |m|$. Odavde sledi da je $a - b = m(q_1 - q_2)$, tj. $a \equiv b (\mathrm{mod}\, m)$.

Sobzirom na ovu teoremu, relaciju kongruencije možemo definisati i na sledeći način:

a je kongruentno sa b po medulu m ako i samo ako brojevi a i b imaju iste ostatke pri deljenju sa m, ili simbolički,

$$a \equiv b (\mathrm{mod}\, m) \Leftrightarrow \mathrm{rem}_m(a) = \mathrm{rem}_m(b)\,.$$

Teorema 5.3 *Broj r je ostatak koji se dobija deobom celog broja a celim brojem $m \neq 0$ ako i samo ako je*

$$a \equiv r (\mathrm{mod}\, m)\,, \quad 0 \leq r < |m|\,. \tag{4}$$

Dokaz: Skup relacija (4) ekvivalentan je skupu relacija

$$a = r + mt\,, \quad 0 \leq r < m\,.$$

Međutim, broj r koji zadovoljava posledne dve relacije pretstavlja ostatak pri deljenju broja a brojem m. Prema tome, tvrđenje je doista tačno.

Navedimo sada neke osnovne osobine relacije kongruencije.

U tom smislu primetimo najpre da je relacija kongruencije po modulu zadatog broja $m \neq 0$ refleksivna, tj. za svaki ceo broj a važi $a \equiv a (\mathrm{mod}\, m)$, jer $m|a - a$.

Ako je $a \equiv b (\mathrm{mod}\, m)$, tada $m|a - b$. Odavde sledi da $m| - (b - a)$ odn. $m|b - a$, pa je $b \equiv a (\mathrm{mod}\, m)$. Prema tome, relacija kongruencije je i simetrična.

Ona je i tranzitivna. Zaista, ako je $a \equiv b (\mathrm{mod}\, m)$ i $b \equiv c (\mathrm{mod}\, m)$, tada postoje celi brojevi S i t takvi da je $a = b + sm$ i $b = c + tm$. No onda je $a = c + (s + t)m$, što dokazuje da je $a \equiv c (\mathrm{mod}\, m)$. Time smo dokazali sledeće tvrđenje:

Teorema 5.4 *Relacija kongruencije po modulu zadatog broja m je relacija ekvivalencije.*

Teorema 5.5 *Neka su a, b, c, d i $m \neq 0$ celi brojevi. Ako je*

$$a \equiv b (\mathrm{mod}\, m)\,, \quad c \equiv d (\mathrm{mod}\, m)\,, \tag{5}$$

tada je

$$a + c \equiv b + d (\mathrm{mod}\, m)\,, \quad a - c \equiv b - d (\mathrm{mod}\, m)\,. \tag{6}$$

Dokaz: S obzirom na relacije (5) postoje celi brojevi s i t takvi da je $a = b+sm$ i $c = d+tm$. Odavde se dobija da je $a+c = b+d+(s+t)m$ i $a-c = b-d+(s-t)m$, pa relacije (6) važe.

Posledica 5.1 *Neka su* $a_1, \ldots, a_k, b_1, \ldots, b_k$ *i* $m \neq 0$ *celi brojevi. Tada iz relacija*

$$a_i \equiv b_1 (\mathrm{mod}\, m)\,, \quad i = \overline{1,k}\,,$$

sledi relacija

$$a_1 + \cdots + a_k \equiv b_1 + \cdots + b_k (\mathrm{mod}\, m)\,.$$

Teorema 5.6 *Neka su* a, b, c *i* $m \neq 0$ *celi brojevi. Ako je*

$$a \equiv b (\mathrm{mod}\, m)\,,$$

tada je

$$ac \equiv bc (\mathrm{mod}\, m)\,, \quad i \quad ac \equiv bc (\mathrm{mod}\, cm)\,.$$

Dokaz: Ako je $a \equiv b (\mathrm{mod}\, m)$, tada $m|a-b$, pa tim pre $m|(a-b)c$, odn. $m|ac-bc$. Ali tada je $ac \equiv bc (\mathrm{mod}\, m)$, što je i trebalo dokazati. Iz $m|a-b$ takođe sledi da $mc|ac-bc$, što daje $ac \equiv bc (\mathrm{mod}\, cm)$.

Teorema 5.7 *Neka su* a, b, c, d *i* $m \neq 0$ *celi brojevi. Ako je*

$$a \equiv b (\mathrm{mod}\, m) \quad i \quad c \equiv d (\mathrm{mod}\, m)\,, \tag{7}$$

tada je

$$ac \equiv bd (\mathrm{mod}\, m)\,.$$

Dokaz: Na osnovu prethodne teoreme i relacija (7) proizilazi da je

$$ac \equiv bc (\mathrm{mod}\, m)\,, \quad \text{i} \quad bc \equiv bd (\mathrm{mod}\, m)\,,$$

odakle se zbog tranzitivnosti relacije kongruencije dobija

$$acd \equiv b (\mathrm{mod}\, m)\,.$$

Posledica 5.2 *Ako su* $a_1, \ldots, a_k, b_1, \ldots, b_k$ *i* $m \neq 0$ *celi brojevi za koje je važe relacije*

$$a_i \equiv b_i (\mathrm{mod}\, m)\,, \quad i = \overline{1,k}\,,$$

tada je

$$a_1 \cdot \ldots \cdot a_k \equiv b_1 \cdot \ldots \cdot b_k (\mathrm{mod}\, m)\,.$$

Posledica 5.3 *Neka su* a, b *i* $m \neq 0$ *celi brojevi, a* n *prirodan broj. Ako je* $a \equiv b (\mathrm{mod}\, m)$*, tada je*

$$a^n \equiv b^n (\mathrm{mod}\, m)\,.$$

Posledica 5.4 *Neka je*

$$P_n(x) = c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$$

polinom sa celim koeficijentima c_i, $i = \overline{0,n}$. *Ako je* $a \equiv b(\mathrm{mod}\, m)$, *tada je* $P_n(a) \equiv P_n(b)(\mathrm{mod}\, m)$.

Primer 5.2 U ovom primeru odredićemo kriterijum deljiosti broja $a = \overline{c_nc_{n-1}\cdots c_1c_0}$ sa brojevima 3,9 i 11. Primetimo najpre da se broj a može prikazati kao

$$a = 10^nc_n + 10^{n-1}c_{n-1} + \cdots + 10c_1 + c_0\,, \quad c_n \neq 0\,.$$

Pošto je $10 \equiv 1(\mathrm{mod}\, 9)$, to je

$$10^k \equiv 1(\mathrm{mod}\, 9)$$

za svaki prirodan broj k. Odavde na osnovu Posledice 5.4 imamo da je

$$a \equiv c_n + c_{n-1} + \cdots + c_1 + c_0(\mathrm{mod}\, 9)\,.$$

Dakle, $a \equiv 0(\mathrm{mod}\, 9)$ ako i samo ako je

$$c_n + c_{n-1} + \cdots + c_1 + c_0 \equiv 0(\mathrm{mod}\, 9)$$

Prema tome, broj je deljiv sa 9 onda i samo onda ako je zbir cifara tog broja deljiv sa 9. Pošto je $10 \equiv 1(\mathrm{mod}\, 3)$, lako zaključujemo da i za deljivost sa 3 važi sličan kriterijum. Ceo bro je deljiv sa 3 ond i samo onda ako je zbir njegovih cifara deljiv sa 3.

Pošto je $10 \equiv -1(\mathrm{mod}\, 11)$, takođe je

$$10^k \equiv (-1)^k(\mathrm{mod}\, 11)$$

za svaki nenegativan ceo broj k. Za prirodan broj a tada važi

$$a \equiv (-1)^nc_n + (-1)^{n-1}c_{n-1} + \cdots - c_1 + c_0(\mathrm{mod}\, 11)\,.$$

Dakle, ceo broj je deljiv sa 11 onda i samo onda ako je razlika zbirova cifara na parnim i neparnim mestima deljiva sa 11.

Primer 5.3 Odredimo ostatak koji se dobija pri deljenju broja 3^{100} sa 13.

Pođimo od relacije $3^3 \equiv 27(\mathrm{mod}\, 13)$. Kako je $27 \equiv 1(\mathrm{mod}\, 13)$, to je $3^3 \equiv 1(\mathrm{mod}\, 13)$. Odavde je $(3^3)^{33} \equiv 1^{33}(\mathrm{mod}\, 13)$, pa je konačno $3{\cdot}3^{99} \equiv 3{\cdot}1(\mathrm{mod}\, 13)$, odn. $3^{100} \equiv 3(\mathrm{mod}\, 13)$. Pošto je $0 < 3 < 13$, na osnovu Teoreme 5.2 zaključujemo da brojevi 3 i 3^{100} pri deljenju sa 13 imaju iste ostatke. Stoga je ostatak pri deljenju broja 3^{100} sa 13 jednak 3.

Teorema 5.8 *Ako je* $a \equiv b(\mathrm{mod}\, m)$ *i* $d|m$, *tada je* $a \equiv b(\mathrm{mod}\, d)$.

Dokaz: Kako je $a \equiv b(\mathrm{mod}\, m)$, to $m|a-b$. Pošto $d|m$, to zbog tranzitivnosti relacije $|$ sledi da $d|a-b$, pa je $a \equiv b(\mathrm{mod}\, d)$.

Iz prethodno dokazanih teorema vidimo da je rad sa relacijama kongruencije, kada su u pitanju sabiranje i množenje, isti kao i rad sa jednačinama. Međutim, kada je reč o deljenju, postoje izvesna ograničenja, o čemu govore sledeće tri teoreme.

Teorema 5.9 *Ako je* $a \equiv b(\mathrm{mod}\, m)$ *i ako* $c|a$ *i* $c|b$, *tada je*

$$\frac{a}{c} \equiv \frac{b}{c} \left(\mathrm{mod}\, \frac{m}{d}\right), \tag{8}$$

gde je $d = (c, m)$.

Dokaz: Iz relacije $a \equiv b(\mathrm{mod}\, m)$ sleduje da $m|a-b$, a isto tako i

$$\frac{m}{d} \Big| \frac{c}{d} \cdot \frac{a-b}{c}. \tag{9}$$

Kako je $(c, m) = d$, to je $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$. Prema tome, iz (9) proizilazi da $\frac{m}{d} \Big| \frac{a-b}{c}$, pa važi (8).

Teorema 5.10 *Neka su* a, b, c *i* $m \neq 0$ *celi brojevi, pri čemu je* $a \equiv b(\mathrm{mod}\, m)$. *Tada važe sledeća tvrđenja:*

(*a*) *ako* $c|a$, $c|b$ *i* $(c, m) = 1$, *tada je* $\frac{a}{c} \equiv \frac{b}{c}(\mathrm{mod}\, m)$;

(*c*) *ako* $c|a$, $c|b$ *i* $c|m$, *tada je* $\frac{a}{c} \equiv \frac{b}{c}(\mathrm{mod}\, \frac{m}{c})$.

Dokaz: (a) Pretpostavimo da $c|a$, $c|b$ i da je $(c, m) = 1$. Neka je $a_1 = \frac{a}{c}$, $b_1 = \frac{b}{c}$. Kako $m|a-b$, to $m|c(a_1 - b_1)$. Kako je $(c, m) = 1$, to $m|a_1 - b_1$, pa je $a_1 \equiv b_1(\mathrm{mod}\, m)$, odn. $\frac{a}{c} \equiv \frac{b}{c}(\mathrm{mod}\, m)$.

(b) Neka je $a = a_1 c$, $b = b_1 c$, $m = m_1 c$ i $a \equiv b(\mathrm{mod}\, m)$. Kako $m|b-a$, to je $b - a = mt$ za neko $t \in \mathbb{Z}$. Zamenom a, b i m u poslednjoj jednakosti dobijamo da je $b_1 c - a_1 c = m_1 t c$. Skraćivanjem ove jednakosti sa c imamo da je $b_1 - a_1 = m_1 t$. Otuda je $a_1 \equiv b_1(\mathrm{mod}\, m_1)$, što je i trebalo dokazati.

Primer 5.4 Sledeći primer pokazuje da skraćivanje može biti nekorektno ako uslovi prethodne teoreme nisu zadovoljeni.

Ako relaciju $20 \equiv 8(\mathrm{mod}\, 6)$ skratimo sa 4 dobijamo da je $5 \equiv 2(\mathrm{mod}\, 6)$, što naravno nije tačno, jer uslov $(4, 6) = 1$ pod (a) nije zadovoljen.

Primer 5.5 Dokažimo da za neparan broj a važi kongruencija

$$a^{2^n} \equiv 1(\mathrm{mod}\, 2^{n+2}), \quad n \geq 1.$$

Dokaz ćemo izvesti potpunom matematičkom indukcijom. Neka je $a = 2m-1$ i $n = 1$. Tada je $a^2 - 1 = 4m(m-1)$. Ovaj broj je deljiv sa $8 = 2^{1+2}$, pa tvrđenje važi za $n = 1$. Pretpostavimo da je tvrđenje tačno za $n = k$, tj. da je

$$a^{2^k} \equiv 1(\mathrm{mod}\, 2^{k+2}).$$

Pošto je

$$a^{2^{k+1}} - 1 = a^{2\cdot 2^k} - 1 = (a^{2^k} - 1)(a^{2^k} + 1)\,,$$

$2^{k+2} | a^{2^k} - 1$ po induktivnoj hipotezi, a $2 | a^{2^k} + 1$ jer je a prema pretpostavci neparan broj, to $2^{k+3} | a^{2^{k+1}} - 1$. Time smo dokazali da je

$$2^{2^{k+1}} \equiv 1 (\mathrm{mod}\, 2^{k+3})\,,$$

tj. da je tvrđenje tačno i za $n = k + 1$, pa dakle i za svako $n \in \mathbb{N}$.

Primer 5.6 Dokazati da je

$$9 \cdot 3^{2n} - 8n - 9 \equiv 0 (\mathrm{mod}\, 64)\,, \quad n \in \mathbb{N}\,.$$

Stavimo da je $f(n) = 9 \cdot 3^{2n} - 8n - 9$. Tada je

$$f(n+1) = 81 \cdot 3^{2n} - 8n - 17\,,$$
$$f(n+2) = 729 \cdot 3^{2n} - 8n - 25\,.$$

Eliminacijom izraza 3^{2n} i n iz ove tri jednačine dobijamo jednačinu

$$f(n+2) - 10f(n+1) + 9f(n) = 64\,,$$

odakle sleduje relacija

$$f(n+2) \equiv 10f(n+1) - 9f(n) (\mathrm{mod}\, 64)\,.$$

Pretpostavimo da je $f(n) \equiv 0 (\mathrm{mod}\, 64)$ i $f(n+1) \equiv 0 (\mathrm{mod}\, 64)$. Tada iz poslednje jednakosti sledi da je i $f(n+2) \equiv 0 (\mathrm{mod}\, 64)$. Pošto je $f(1) = 64 \equiv 0 (\mathrm{mod}\, 64)$ i $f(2) = 704 \equiv 0 (\mathrm{mod}\, 64)$, na osnovu principa matematičke indukcije sledi da je tvrđenje tačno za sve prirodne brojeve.

Zadaci za vežbanje

1. Odrediti ostatke pri deljenju brojeva (a) 3^{21} sa 11; (b) 11^{35} sa 13; (c) 8^{130} sa 131.
2. Odrediti ostatke pri deljenju brojeva (a)10! sa 11; (b) 16! sa 17; (c) 23! sa 24.
3. Odrediti ostatak deljenja broja $(12371^{56} + 34)^{28}$ sa 111.
4. Dat je polinom $f(x) = 3x^5 - 2x^4 + x^3 - 3x^2 + x - 7$. Odrediti ostatke pri deljenju brojeva $f(2)$ i $f(5)$ sa 9.
5. Odrediti kriterijume za deljivost brojeva napisanih u dekadnom brojevnom sistemu sa 7, 13 i 37.
6. Dokazati da je Mersenov broj $M_{37} = 2^{37} - 1$ deljiv sa 223.
7. Dokazati kongruencije

(a) $n^3 \equiv n (\mathrm{mod}\, 24)$, (n je neparan broj),
(b) $13^{2n} \equiv 1 (\mathrm{mod}\, 7)$,
(c) $11^n + 12^{2n+1} \equiv (\mathrm{mod}\, 133)$.