UNIVERZITET U BEOGRADU
MATEMATIČKI FAKULTET

Olga Mitrinović 1079/2020

ZAKONITOSTI VEZANE ZA DELJIVOST BROJEVA

master rad

Beograd, 2022.

Mentor:

dr Tanja Stojadinović
Univerzitet u Beogradu, Matematički fakultet

Članovi komisije:

dr Nebojša Ikodinović
Univerzitet u Beogradu, Matematički fakultet

dr Marko Radovanović
Univerzitet u Beogradu, Matematički fakultet

Datum odbrane: 10.6.2022.

Sadržaj

Glava 1

Uvod

Dokaz je od centralne važnosti u matematici i njenim primenama. Ipak, njegova uloga u matematici osnovnih i srednjih škola je tradicionalno marginalizovana i jedini dodir đaka sa njim je isključivo kroz geometriju. Nedostatak dokaza izvan geometrije prouzrokuje pogrešno predstavljanje prirode matematike i predstavlja značajni defekt u modernom edukativnom sistemu. Suprotno verovanju današnjeg nastavnog programa, dokaz nije stvar odvojiva od matematike, već esencijalna komponenta u razumevanju, komunikaciji i razvoju matematike. Takođe, predočavanje deci važnosti deduktivnog zaključivanja naspram empirijskog, koje im je intuitivnije, ali, vrlo često ih dovodi do nepravilnih zaključaka, je imperativ u njihovom obrazovanju i pravilnom formiranju načina razmišljanja.

Osim što je dokaz neophodan za pokazivanje tačnosti tvrdnje, njegov značaj ne staje tu, već pojedini primeri dokaza predstavljaju uvod u nove tehnike za rešavanje matematičkih problema ili pružaju razumevanje nečeg šireg i drugačijeg od originalnog konteksta.

Uzimajući u obzir sve ovo, ovaj rad će se fokusirati na dokazivanje teorema i pravila, kao i davanje primera njihove primene, koja se deci u školama obično predstavljaju bez pokazivanja tačnosti, stavljanjem u prvi plan ne samo da li je nešto tačno, već i zašto je tačno, što je veliki korak u oformljavanju kritičkog mladog uma.

Glava 2

Deljivost celih brojeva

2.1 Osnovni pojmovi

Definicija 2.1.1. Ceo broj a deljiv je celim brojem b, različitim od nule, ako postoji ceo broj q takav da je $a = bq$. Ako je broj a deljiv brojem b, pisaćemo $b|a$ („b deli a“).

Teorema 2.1.1 (Osnovne osobine deljivosti)**.** *Neka su a, b, c, d celi brojevi. Tada važi:*

1. $a|a$, *za* $a \neq 0$
2. *Ako* $a|b$ *i* $b|c$, $a \neq 0$, $b \neq 0$, *onda* $a|c$.
3. *Ako* $a|b$ *i* $b|a$, $a \neq 0$, $b \neq 0$, *onda* $|a| = |b|$.
4. *Ako* $a|b$, $a \neq 0$, *onda* $a|bc$, *za svako* $c \in \mathbb{Z}$.
5. *Ako* $a|b$ *i* $a|c$, $a \neq 0$, *onda* $a|bx + cy$ *za sve* $x, y \in \mathbb{Z}$
6. *Ako za cele brojeve* a *i* b, $a \neq 0$, $b \neq 0$, *važi* $a|b$, *onda* $|a| \leq |b|$.

Dokaz.

1. Trivijalno, iz definicije, $a = a \cdot 1$.
2. Po definiciji, ako $a|b$ i $b|c$, onda je $b = a \cdot k$, a $c = b \cdot l$, za neke $k, l \in \mathbb{Z}$. Tada je $c = a(kl)$, odnosno $a|c$.
3. Po definiciji, ako $a|b$ i $b|a$, onda je $b = a \cdot k$, a $a = b \cdot l$. Tada je $a = akl$, odnosno $1 = kl$. Dakle, k i l moraju oba biti ili 1 ili -1, jer je u svim ostalim slučajevima proizvod $kl \neq 1$.
4. Ako $a|b$ onda je $b = a \cdot d$ za neko $d \in \mathbb{Z}$, odnosno $bc = a(dc)$, odakle je jasno da $a|bc$.
5. Po definiciji, ako $a|b$ i $a|c$, onda je $b = a \cdot d$, a $c = a \cdot l$, za neke $d, l \in \mathbb{Z}$. Odavde imamo da za neke cele x i y važi $bx = adx$ i $cy = aly$, odnosno

$bx + cy = adx + aly = a(dx + ly)$, tj. $a|(bx + cy)$.

6. Neka je $b = a \cdot d$. Odatle sledi $|b| = |a| \cdot |d|$. Kako je $b \neq 0$, važi $|d| \geq 1$, iz čega sledi tvrdnja.

□

Sledi jedna od osnovnih teorema u teoriji brojeva.

Teorema 2.1.2 (Teorema o deljenju sa ostatkom). *Svaki ceo broj a može se na jedinstven način pomoću celog broja b, različitog od nule, prikazati u obliku*

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

gde su q i r celi brojevi. Pri tom se q naziva količnikom, a r ostatkom pri deljenju broja a brojem b.

Dokaz. Posmatrajmo skup celih brojeva

$$S = \{a - bx | x \in \mathbb{Z}\}$$

i izaberimo u njemu najmanji broj koji je prirodan ili jednak 0. Neka je to r i neka važi $r = a - bq$.

Tada je

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

jer bi u slučaju $r \geq |b|$ važilo $0 \leq r - |b| = a - bq - |b| = a - b(q \pm 1) \in S$, tj. broj $a - bq - |b|$, koji je manji od $a - bq$, bi bio prirodan ili jednak nuli. Time je dokazana egzistencija brojeva q i r. Dokažimo jedinstvenost tih brojeva. Pretpostavimo da postoji još jedan par (q_1, r_1), takav da je $a = bq_1 + r_1$ i $0 \leq r_1 < |b|$. Oduzimanjem dve jednakosti dobijamo

$$0 = b(q - q_1) + (r - r_1),$$

odnosno $b|r - r_1$. Zbog $|r - r_1| < |b|$ imamo da je $r - r_1 = 0$, tj. $r = r_1$, a zbog toga i $q = q_1$. □

Definicija 2.1.2. Ceo broj d je zajednički delilac brojeva a i b ako $d|a$ i $d|b$. Najveći zajednički delilac brojeva a i b je ceo broj $d > 0$ ako važi:

- d je zajednički delilac a i b
- Za sve $c \in \mathbb{Z}$ takve da $c|a$ i $c|b$ važi i $c|d$.

Najveći zajednički delilac brojeva a i b ćemo obeležavati sa (a, b).

Definicija 2.1.3. Zajedničkim sadržaocem celih brojeva a i b, različitih od nule, nazivamo svaki broj koji je deljiv i sa a i sa b. Najmanji zajednički sadržalac brojeva a i b je ceo broj $s > 0$ ako važi:

- s je zajednički sadržalac a i b

- Za sve $c \in \mathbb{Z}$ takve da $a|c$ i $b|c$ važi i $s|c$.

Najmanji zajednički sadržalac brojeva a i b ćemo obeležavati sa $[a, b]$.

Definicija 2.1.4. Za cele brojeve a i b kažemo da su uzajamno (relativno) prosti ako je $(a, b) = 1$.

Definicija 2.1.5. Ceo broj $p > 1$ je prost ako p nema nijedan delilac d, $1 < d < p$. Ceo broj $m > 1$ je složen ako nije prost.

Teorema 2.1.3. *Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$.*

Teorema 2.1.4 (Osnovni stav aritmetike). *Svaki prirodan broj a veći od 1 može se jednoznačno (do na poredak) izraziti u obliku proizvoda prostih činilaca.*

Dokaz. (Egzistencija): Tvrđenje da postoji razlaganje broja $a > 1$ na proste faktore dokazujemo totalnom indukcijom. Za $a = 2$, tvrđenje važi jer je 2 prost broj. Pretpostavimo da svi brojevi iz $2, ..., a-1$ imaju bar po jedno razlaganje na 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 $1 < a' < a$. Induktivna pretpostavka je primenljiva na a', tj. a' je proizvod prostih brojeva: $a' = p_1 p_2 ... p_n$. Tada je $a = pp_1 p_2 ... p_n$ što je trebalo dokazati.
(Jedinstvenost): Pretpostavimo da je $a = p_1 p_2 ... p_r = q_1 q_2 ... q_s$. Bez umanjenja opštosti neka je $r \leq s$. Pošto $p_1 | q_1 q_2 ... q_s$ i p_1 je prost broj, sledi da je $p_1 = q_{j_1}$. Isto zaključivanje se može ponoviti i za $p_2, ..., p_r$, 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 $j_1, ..., j_r$ međusobno različiti. Ukoliko bi bilo $r < s$, tada bismo dobili da je $1 = q_{k_1} ... q_{k_{s-r}}$, što je očito nemoguće. Dakle, mora biti $r = s$. □

Ako se u razlaganju broja a neki činioci ponavljaju, pa se, recimo p_1 javlja α_1 puta, p_2 javlja α_2 puta, ... , p_k javlja α_k puta, onda se oblik

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$$

zove kanonski oblik prirodnog broja a (kanonska faktorizacija).

Teorema 2.1.5. *Neka je $n > 1$ prirodan broj čiji je kanonski oblik dat sa $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$. Tada $d|n$ ako i samo ako je*

$$d = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$$

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

Dokaz. ($\Longrightarrow$): Ako $d|n$, tada je $n = dq$ za neki pozitivan ceo broj q; stoga se kanonski oblik broja n dobija množenjem kanonskih oblika brojeva d i q. To znači, između ostalog, da je svaki prost faktor p koji se pojavljuje u kanonskom obliku broja d sa nenula eksponentom prisutan i u n sa najmanje onolikim stepenom kao u d. Odatle mora biti $0 \leq \beta_i \leq \alpha_i$ za sve i.

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

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

važi $n = dq$, tj. $d|n$. □

Posledica 2.1.5.1. Broj pozitivnih delilaca broja $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ (uključujući i 1 i samo a) je

$$(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$$

Dokaz. Po prethodnoj teoremi, d je delilac broja n ako i samo ako je $d = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$ za neke $0 \leq \beta_i \leq \alpha_i$, $1 \leq i \leq k$. Prema tome, svaki niz brojeva $(\beta_1, ..., \beta_k)$ 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 različiti izbori nezavisni, rezultat sledi. □

Definicija 2.1.6. Ukupan broj pozitivnih delilaca prirodnog broja n označavamo sa

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

ako je $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ njegova kanonska faktorizacija.

U sledećoj tablici date su vrednosti funkcije τ na nekoliko prvih prirodnih brojeva

n	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6

Teorema 2.1.6. *Ako je proizvod dva uzajamno prosta prirodna broja kvadrat celog broja $ab = c^2$, tada su a i b kvadrati celih brojeva, tj. $a = a_1^2$ i $b = b_1^2$.*

Dokaz. Broj je potpun kvadrat ako i samo ako su mu svi eksponenti u kanonskoj faktorizaciji parni. Kako su a i b uzajamno prosti, svaki prost delilac broja c^2 se javlja ili u a ili u b, ali ne u oba. Zato, prosti faktori brojeva a i b moraju imati parne eksponente. $\square$

2.2 Primeri

U ovom odeljku će biti predstavljen određen broj primera čijem rešavanju se pristupa direktnim korišćenjem teorema i njihovih posledica iz prethodnog odeljka.

Primer 2.2.1. Dokazati da je proizvod tri uzastopna cela broja deljiv sa 6, proizvod četiri uzastopna cela broja deljiv sa 24.

Rešenje. Od tri uzastopna prirodna broja, jedan je deljiv sa 3 i bar jedan je paran, pa je proizvod deljiv sa 6.
Od četiri uzastopna prirodna broja, jedan je deljiv sa 3, dva su parna i to su uzastopni parni brojevi, pa je jedan deljiv sa 4. Zbog toga je njihov proizvod deljiv sa $3 \cdot 2 \cdot 4 = 24$.

Primer 2.2.2. Dokazati da je broj $m^5 - m$, $m \in \mathbb{N}$, deljiv sa 30.

Rešenje. Kako je $m^5 - m = m(m-1)(m+1)(m^2+1)$, a proizvod tri uzastopna broja mora biti deljiv sa 6 (po prethodnom primeru), dati broj je deljiv sa 6. Ako je broj m oblika $5k$, $5k+1$ ili $5k-1$, onda je m, odnosno $m-1$, odnosno $m+1$ deljivo sa 5. Ako je m oblika $5k+2$ ili $5k-2$, onda je $m^2+1 = (5k \pm 2)^2 + 1 = 5(5k^2 \pm 4k + 1)$ deljivo sa 5.

Primer 2.2.3. Dokazati da je broj $n^3 + 2n$ deljiv sa 3 za sve prirodne brojeve n.

Rešenje. Mogući ostaci pri deljenju sa 3 su 0, 1 i 2, pa imamo 3 slučaja:

1. $n = 3k$, $k \in \mathbb{N}$ $n^3 + 2n = (3k)^3 + 2 \cdot 3k = 27k^3 + 6k = 3(9k^3 + 2k)$, što je deljivo sa 3.
2. $n = 3k+1$, $k \in \mathbb{N}$ $n^3+2n = (3k+1)^3+2\cdot(3k+1) = 27k^3+27k^2+9k+1+6k+2 = 3(9k^3 + 9k^2 + 5k + 1)$, što je deljivo sa 3.
3. $n = 3k+2$, $k \in \mathbb{N}$ $n^3 + 2n = (3k+2)^3 + 2 \cdot (3k+2) = 27k^3 + 54k^2 + 36k + 8 + 6k + 4 = 3(9k^3 + 18k^2 + 14k + 4)$, što je deljivo sa 3.

Primer 2.2.4. Odrediti sve proste brojeve p takve da je i broj: $p^2 + 1999$ prost.

Rešenje. Proverimo prvo za $p = 2$: $p^2 + 1999 = 2003$, što je prost broj.
Svi ostali prosti brojevi moraju biti neparni (2 je jedini paran prost broj), pa su oblika $p = 2k + 1$.
Broj $p^2 + 1999 = 4k^2 + 4k + 1 + 1999 = 2(2^k + 2k + 1000)$ je deljiv sa 2, pa mora biti složen.

Primer 2.2.5. Odrediti prost broj p takav da je broj $8p^2 + 1$ takođe prost.

Rešenje. Proverimo prvo za 2 i 3.

- $p = 2$, $8p^2 + 1 = 33 = 3 \cdot 11$, dakle 2 nije traženi broj.
- $p = 3$, $8p^2 + 1 = 73$, što je prost broj.

Prosti brojevi veći od 3 mogu da daju ostatke 1 i 2 pri deljenju sa 3. Zato imamo dva slučaja:

- $p = 3k+1$, $8p^2+1 = 8(9k^2+6k+1)+1 = 72k^2+48k+9 = 3(24k^2+16k+3)$, što je deljivo sa 3; dakle, broj je složen.
- $p = 3k + 2$, $8p^2 + 1 = 8(9k^2 + 12k + 4) + 1 = 72k^2 + 96k + 32 + 1 = 3(24k^2 + 32k + 11)$, što je deljivo sa 3; dakle, broj je složen.

Zaključujemo da je jedino rešenje $p = 3$.

Primer 2.2.6. Naći sve proste brojeve p takve da je svaki od pet brojeva $p + 2$, $p + 6$, $p + 8$, $p + 12$ i $p + 14$ takođe prost.

Rešenje. Lako proverimo da brojevi manji od 5 ne zadovoljavaju uslove zadatka.
Ako je $p = 5$, imamo proste 7, 11, 13, 17 i 19.
Ako je $p > 5$, p može biti oblika:

- $p = 5k + 1$. Tada je $p + 14$ deljiv sa 5, dakle složen.
- $p = 5k + 2$. Tada je $p + 8$ deljiv sa 5, dakle složen.
- $p = 5k + 3$. Tada je $p + 12$ deljiv sa 5, dakle složen.
- $p = 5k + 4$. Tada je $p + 6$ deljiv sa 5, dakle složen.

Jedino rešenje je $p = 5$.

Primer 2.2.7. Dokazati da zbir kvadrata 5 uzastopnih prirodnih brojeva ne može biti potpun kvadrat.

Rešenje. Neka su to brojevi $n-2$, $n-1$, n, $n+1$ i $n+2$. Imamo da je $(n-2)^2+(n-1)^2+n^2+(n+1)^2+(n+2)^2 = n^2-4n+4+n^2-2n+1+n^2+n^2+2n+1+n^2+4n+4 = 5(n^2+2)$, što je deljivo sa 5. Posmatrajmo broj n:

- $n = 5k$. Tada je $n^2 + 2 = 25k^2 + 2$ što nije deljivo sa 5.

- $n = 5k + 1$. Tada je $n^2 + 2 = 25k^2 + 10k + 3$ što nije deljivo sa 5.
- $n = 5k + 2$. Tada je $n^2 + 2 = 25k^2 + 20k + 6$ što nije deljivo sa 5.
- $n = 5k + 3$. Tada je $n^2 + 2 = 25k^2 + 30k + 11$ što nije deljivo sa 5.
- $n = 5k + 4$. Tada je $n^2 + 2 = 25k^2 + 40k + 18$ što nije deljivo sa 5.

Dakle, broj $n^2 + 2$ nije deljiv sa 5, odnosno posmatrani zbir je deljiv sa 5, ali nije sa 25, pa ne može biti potpun kvadrat.

Primer 2.2.8. Odrediti sve proste brojeve p takve da je $\frac{7}{6} > \frac{5}{p} > \frac{2}{5}$.

Rešenje. Iz datog odnosa među razlomcima sledi da je $\frac{5}{2} > \frac{p}{5} > \frac{6}{7}$. Proširimo date razlomke tako da ih dovedemo na jednake imenioce: $\frac{175}{70} > \frac{14p}{70} > \frac{60}{70}$, odnosno $175 > 14p > 60$. Odavde je $\frac{175}{14} > p > \frac{60}{14}$, pa je $p \in \{5, 7, 11\}$.

Primer 2.2.9. Svaki prost broj veći od 5 je oblika $6k + 1$ ili $6k + 5$, za neko $k \in \mathbb{N}$. Dokazati.

Rešenje. Sve prirodne brojeve veće od 5 možemo predstaviti na jedan od sledećih šest načina:

$$6k + 1,\ 6k + 2,\ 6k + 3,\ 6k + 4,\ 6k + 5,\ 6k,$$

gde je k prirodan broj. Kako su brojevi oblika $6k+2$, $6k+4$ i $6k$ deljivi sa 2, to su oni složeni. Brojevi oblika $6k+3$ su deljivi sa 3, pa su i oni složeni. Ostaju samo brojevi oblika $6k + 1$ i $6k + 5$, među kojima su prosti brojevi. Ovde je bitno napomenuti da nisu svi ovakvi brojevi prosti, već da su svi prosti brojevi ovakvi.

Primer 2.2.10. Zbir dvocifrenih brojeva $\overline{ab}$ i $\overline{ba}$ je potpun kvadrat. Koliko ima ovakvih brojeva?

Rešenje. Tvrđenje: ako je p prost i $p|n^2 \implies p^2|n^2$.
Naime, ako $p|n \cdot n$ onda, po teoremi 2.1.3 važi $p|n$, a samim tim i $p^2|n^2$.
$\overline{ab}+\overline{ab} = 10a+b+10b+a = 11(a+b) = n^2$, odakle vidimo da $11|n^2$. Po prethodnom tvrđenju mora biti i $121|n^2$. Pošto su a i b cifre $a+b \in [0, 18]$, tj. $n^2 = 11(a+b) \leq 198$, vidimo da je jedina mogućnost $n^2 = 121$, odnosno $n = 11 = (a+b)$. Traženih brojeva ima 8 i to: 29, 38, 47, 56, 65, 74, 83, 92.

Primer 2.2.11. Naći najmanji prirodan broj koji pomnožen sa 450 daje kvadrat prirodnog broja.

Rešenje. Rastavimo broj 450 na činioce. $450 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 2^1 \cdot 3^2 \cdot 5^2$
Da bi broj bio potpun kvadrat neophodno je da ima sve parne eksponente u kanonskom obliku; vidimo da samo broj 2 nema parni eksponent, pa je broj 450 neophodno pomnožiti sa 2 da bi se dobio potpun kvadrat.

Primer 2.2.12. Sa koliko nula se završava 100!?

Rešenje. Da bi se broj završavao sa n nula, mora biti deljiv sa 10^n. Dakle, tražimo koliko desetki imamo u proizvodu 10!. Svaka desetka je dobijena kao proizvod 2 i 5, pa brojimo ukupan broj takvih parova. Očigledno je da petica ima manje i zato prebrojavamo njih. Kako je svaki peti broj deljiv sa 5, u prvih 100 brojeva ih ima $\frac{100}{5} = 20$. Takođe, moramo uzeti i u obzir i brojeve koje u faktorizaciji imaju 5^2 i to su: $25 = 5^2$, $50 = 2 \cdot 5^2$, $75 = 3 \cdot 5^2$ i $100 = 4 \cdot 5^2$: oni proizvodu dodaju još 4 nule, što sve ukupno čini 24 nule.

Primer 2.2.13. Naći faktorizaciju najmanjeg prirodnog broja koji ima tačno 2015 različitih pozitivnih delilaca.

Rešenje. Neka je n prirodan broj i $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ njegova kanonska faktorizacija, gde su p_i prosti brojevi, $p_1 < p_2 < ... < p_k$, $\alpha_i \in \mathbb{N}$, $i \in \{1, 2, ..., k\}$. Broj delilaca broja n je $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$.
Kako je $2015 = 5 \cdot 13 \cdot 31$, moguća predstavljanja broja 2015 su:

$$2015 = 2015,\ 2015 = 5 \cdot 403,\ 2015 = 13 \cdot 155,\ 2015 = 65 \cdot 31,\ 2015 = 5 \cdot 13 \cdot 31$$

Svakom od ovih predstavljanja odgovara po jedan najmanji prirodan broj sa tačno 2015 različitih delilaca. Upoređivanjem njihovih faktorizacija:

$$n_1 = 2^{2014},\ n_2 = 2^{402} \cdot 3^4,\ n_3 = 2^{154} \cdot 3^{12},\ n_4 = 2^{64} \cdot 3^{30},\ n_5 = 2^{30} \cdot 3^{12} \cdot 5^4$$

zaključujemo da je n_5 najmanji od ovih brojeva. Tražena faktorizacija najmanjeg prirodnog broja koji ima tačno 2015 različitih delilaca je $2^{30} \cdot 3^{12} \cdot 5^4$.

Primer 2.2.14. Ako su $p_1, p_2, ..., p_n$ međusobno različiti prosti brojevi, dokazati da $\frac{1}{p_1} + \frac{1}{p_2} + ... + \frac{1}{p_n}$ nije ceo broj.

Rešenje. Svedimo navedene razlomke na zajednički imenilac.

$$\frac{1}{p_1} + \frac{1}{p_2} + ... + \frac{1}{p_n} = \frac{p_2 p_3 ... p_n + p_1 p_3 ... p_n + p_1 p_2 .. p_{n-1}}{p_1 p_2 ... p_n}$$

Vidimo da su svi sabirci u brojiocu, osim prvog, deljivi sa p_1, zbog čega brojilac nije deljiv sa p_1. Pošto je imenilac deljiv sa p_1, posmatrani razlomak ne može biti ceo broj.

Primer 2.2.15. Naći prirodan broj a ako $3|a$ i $4|a$ i $\tau(a) = 14$.

Rešenje. Ako je $a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ kanonska faktorizacija broja a, imamo da je njegov broj delilaca $\tau(a) = (\alpha_1+1)(\alpha_2+1)...(\alpha_k+1)$. Kako je $14 = 2\cdot 7$, mora biti $\alpha_1+1 = 2$ i $\alpha_2 + 1 = 7$, odnosno $\alpha_1 = 1$, a $\alpha_2 = 6$. Dakle, $a = p_1 {p_2}^6$. Kako $3|a$ i $4|a$, mora biti $p_1 = 3$, a $p_2 = 2$, odnosno $a = 192$.

Primer 2.2.16. Prirodan broj n ima tačno 80 prirodnih delilaca, uključujući i 1 i n. Dokazati da je proizvod tih delilaca jednak n^{40}.

Rešenje. Neka su ti delioci $k_1, k_2, ..., k_{80}$. Pošto svaki od k_i, $i \in \{1, 2, ..., 80\}$ ima svog parnjaka u skupu delilaca n, takvog da je njihov proizvod jednak n, imamo da je $(k_1 k_2 ... k_{80})(k_1 k_2 ... k_{80}) = n^{80}$, odnosno $k_1 k_2 ... k_{80} = n^{40}$.

Primer 2.2.17. Ako $m|(m-1)! + 1$, tada je m prost broj. Dokazati.

Rešenje. Pretpostavimo suprotno, tj. da m ima prost delilac p, $p < m$. Tada bi bilo $p|(m-1)!$, odnosno broj $(m-1)! + 1$ ne bi mogao da bude deljiv sa p, pa samim tim ni sa m. Dakle, m mora biti prost broj.

Glava 3

Kongruencije i primene

3.1 Relacija kongruencije

Ako ceo broj a delimo sa 2, možemo dobiti da je broj deljiv ili da daje ostatak 1. Na osnovu ovoga možemo skup celih brojeva podeliti na dva disjunktna skupa, parne i neparne. Prirodno se nameće da posmatramo deljenje bilo kojim prirodnim brojem m i moguće ostatke pri tome.

Definicija 3.1.1. Neka je dat prirodan broj m, veći od 1. Dva cela broja a i b su kongruentna po modulu m ako daju isti ostatak pri deljenju sa m. Simbolički se to zapisuje $a \equiv b(\text{mod } m)$.

Teorema 3.1.1. *$a \equiv b(mod\ m)$ ako i samo ako je $a - b$ deljivo sa m.*

Dokaz. Ako je $a \equiv b(\text{mod } m)$, onda, na osnovu date definicije, a i b pri deljenju sa m imaju jednake ostatke, tj. $a = km+r$ i $b = lm+r$. Tada je $a-b = km+r-(lm+r) = m(k-l)$. Dakle, $a - b$ je deljivo sa m.
Obrnuto, neka je $a = pm + r_1$ i $b = qm + r_2$, $0 \leq r_1, r_2 < m$ i neka je $a - b$ deljivo sa m, tj. neka je $a - b = km$. Tada se oduzimanjem jednakosti dobija $a - b = pm + r_1 - (qm + r_2) = m(p - q) + r_1 - r_2 = km$. Kako je desna strana jednakosti deljiva sa m, to mora biti i leva, pa je $r_1 - r_2$ deljivo sa m. Tada je, zbog uslova $0 \leq r_1, r_2 < m$, $r_1 - r_2 = 0$. To znači da su r_1 i r_2 jednaki, pa a i b pri deljenju sa m imaju iste ostatke, a to znači da je $a \equiv b(\text{mod } m)$. □

Teorema 3.1.2. *1. Ako je $a \equiv b(mod\ m)$ i $c \equiv d(mod\ m)$ onda je $ax + cy \equiv bx + dy(mod\ m)$ za svaka dva cela broja x, y.*

2. Ako je $a \equiv b(mod\ m)$ i $c \equiv d(mod\ m)$ onda je $ac \equiv bd(mod\ m)$.

3. *Ako* $a \equiv b(mod\ m)$ *i* $m = \alpha d$, $d > 1$, *onda je* $a \equiv b(mod\ d)$.

Dokaz. 1. Po prethodnoj teoremi, imamo da $m|a-b$ i $m|c-d$. Takođe, $m|x(a-b)$ i $m|y(c-d)$ za neke cele brojeve x i y. Sledi da $m|x(a-b)+y(c-d) = ax+cy-(bx+dy)$, odnosno $ax+cy \equiv bx+dy(\text{mod } m)$

2. Po prethodnoj teoremi imamo da je $a = b + mt_1$ i $c = d + mt_2$ za neke cele brojeve t_1 i t_2. Množenjem dobijamo da je $ac = bd + mt_3$ za $t_3 = t_1 d + t_2 b + mt_1 t_2$, pa je $ac \equiv bd(\text{mod } m)$.
3. Kako važi $m|a-b$, odnosno, po tvrđenju, $\alpha d|a-b$, jasno je da važi i $d|a-b$, odnosno $a \equiv b(\text{mod } d)$.

□

Teorema 3.1.3. *Relacija kongruencije po modulu je saglasna sa operacijama sabiranja, oduzimanja, množenja i stepenovanja (prirodnim brojem).*

Dokaz. Ako je $a \equiv b(\text{mod } m)$ i $c \equiv d(\text{mod } m)$, onda je $a - b = km$ i $c - d = lm$. Sabiranjem jendakosti se dobija $a-b+c-d = km+lm$, tj. $a+c-(b+d) = m(k+l)$, a to znači da je $a + c \equiv b + d(\text{mod } m)$. Na sličan način se dokazuje saglasnost sa oduzimanjem.
Neka je, opet, $a \equiv b(\text{mod } m)$ i $c \equiv d(\text{mod } m)$. Posmatrajmo razliku $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d)$. Kako važi $m|a - b$ i $m|c - d$, to znači da i $m|c(a - b) + b(c - d)$, odnosno $m|ac - bd$, tj. $ac \equiv bd(\text{mod } m)$. Saglasnost sa stepenovanjem je direktna posledica saglasnosti sa množenjem. □

Teorema 3.1.4. 1. *Ako je* $(a, m) = 1$ *i* $ax \equiv ay(mod\ m)$, *onda je* $x \equiv y(mod\ m)$.

2. $ax \equiv ay(mod\ m)$ *ako i samo ako* $x \equiv y(mod\ \dfrac{m}{(a,m)})$.
3. $x \equiv y(mod\ a)$ *i* $x \equiv y(mod\ b)$ *ako i samo ako* $x \equiv y(mod\ [a, b])$.

Dokaz. 1. Ako je $ax \equiv ay(\text{mod } m)$, onda je $a(x - y) = km$. Pošto je $(a, m) = 1$, mora biti $x - y = \alpha m$, odnosno $x \equiv y(\text{mod } m)$

2. Neka je $(a, m) = d$. Kongruencija $ax \equiv ay(\text{mod } m)$ ekvivalentna je uslovu $m|a(x - y)$. On je, dalje, ekvivalentan sa $\dfrac{m}{d}|(x - y)\dfrac{a}{d}$.
Pošto je $(\dfrac{m}{d}, \dfrac{a}{d}) = 1$, gornja deljivost važi ako i samo ako $\dfrac{m}{d}|x - y$, odnosno $x \equiv y(\text{mod } \dfrac{m}{d})$.
3. Ako je $x \equiv y(\text{mod } a)$ i $x \equiv y(\text{mod } b)$ onda je $x-y = \alpha a$ i $x-y = \beta b$, odnosno $x - y$ je zajednički sadržalac brojeva a i b, pa prema tome $x - y = \gamma[a, b]$. Onda je $x \equiv y(\text{mod } [a, b])$. Obrnuti smer sledi iz treće stavke teoreme 3.1.2.

□

3.2 Sistemi ostataka

Svi celi brojevi koji su međusobno kongurentni po datom modulu obrazuju jednu klasu brojeva. Tako po modulu 3 imamo 3 klase brojeva:

- klasu brojeva oblika $3k$, koji su deljivi sa 3,
- klasu brojeva oblika $3k+1$, koji pri deljenju sa 3 daju ostatak 1 i
- klasu brojeva oblika $3k+2$, koji pri deljenju sa 3 daju ostatak 2.

Neka je dat prirodan broj $m > 1$. Posmatrajmo klase celih brojeva koji su redom kongruentni brojevima 0, 1, 2, ..., $m-1$. Jasno je da je na ovaj način skup celih brojeva razdvojen na m klasa koje međusobno nemaju zajedničkih elemenata. Svaka od ovih klasa je okarakterisana brojevima 0, 1, 2, ..., $m-1$, pa ih možemo izabrati kao reprezente svojih klasa. Skup izabranih reprezenata se naziva potpuni sistem ostataka po modulu m. Jasno je da odabir reprezenata nije jedinstven, ali se najčešće koriste navedeni „sistem najmanjih nenegativnih ostataka“, kao i „sistem ostataka najmanjih po modulu“ koji za neparno m čine:

$$-\frac{m-1}{2}, ..., -1, 0, 1, ..., \frac{m-1}{2}$$

a za parno m:

$$-\frac{m}{2}+1, ..., -1, 0, 1, ..., \frac{m}{2}$$

ili

$$-\frac{m}{2}, ..., -1, 0, 1, ..., \frac{m}{2}+1$$

Od posebnog je značaja posmatranje svedenog sistema ostataka koji se dobija kada se iz potpunog sistema ostataka po modulu m odstrane svi brojevi koji nisu uzajamno prosti sa m. Na primer za $m = 18$ svedeni sistem ostataka je $\{1, 5, 7, 11, 13, 17\}$.

3.3 Ojlerova teorema

Definicija 3.3.1. Broj prirodnih brojeva koji nisu veći od datog prirodnog broja m i relativno su prosti sa njim, tj. broj elemenata svedenog sistema ostataka po modulu m se označava sa $\varphi(m)$. Funkcija φ se zove Ojlerova funkcija.

U sledećoj tablici date su vrednosti funkcije φ na nekoliko prvih prirodnih brojeva

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Kako su za prost broj p svi elementi skupa 1, 2, ..., p, sem p, uzajamno prosti sa p, to je $\varphi(p) = p - 1$.

Teorema 3.3.1. *Neka je $(a, m) = 1$ i neka je $\{\alpha_1, \alpha_2, ..., \alpha_k\}$ proizvoljan potpun sistem ostataka po modulu m. Tada je i $\{a\alpha_1, a\alpha_2, ..., a\alpha_k\}$ potpun sistem ostataka po modulu m.*

Dokaz. Brojeva $a\alpha_i$ ima koliko i brojeva α_i, pa treba dokazati da je $a\alpha_i \not\equiv a\alpha_j$ ako je $i \neq j$, odnosno da brojevi $a\alpha_i$ i $a\alpha_j$ pripadaju različitim klasama. Ako bi bilo $a\alpha_i \equiv a\alpha_j(\text{mod } m)$, zbog $(a, m) = 1$ po teoremi 3.1.4. imali bismo da je $\alpha_i \equiv \alpha_j(\text{mod } m)$, što je nemoguće. Ako se radi o svedenom sistemu ostataka, tj. ako je $(\alpha_i, m) = 1$ za $i = 1, 2, ..., k$, onda je i $(a\alpha_i, m) = 1$, pa i skup svih $a\alpha_i$ predstavlja svedeni sistem ostataka po modulu m. □

Teorema 3.3.2 (Ojlerova teorema)**.** *Neka je n prirodan broj. Za svaki ceo broj a uzajamno prost sa n važi*

$$a^{\varphi(n)} \equiv 1(mod\ n).$$

Dokaz. Neka je $\{\alpha_1, \alpha_2, ..., \alpha_{\varphi(n)}\}$ svedeni sistem ostataka po modulu n. Onda je, prema teoremi 3.3.1. i $\{a\alpha_1, a\alpha_2, ..., a\alpha_{\varphi(n)}\}$ svedeni sistem ostataka po modulu n. Prema tome, za svaki broj α_i postoji jedan i samo jedan broj α_j takav da je $a\alpha_j \equiv \alpha_i(\text{mod } n)$. Ako pomnožimo sve kongruencije ovog oblika (ima ih tačno $\varphi(n)$), dobijamo da je

$$a^{\varphi(n)}\alpha_1\alpha_2...\alpha_{\varphi(n)} \equiv \alpha_1\alpha_2...\alpha_{\varphi(n)}(\text{mod } n).$$

Pošto je $(\alpha_i, n) = 1$ za $i = 1, 2, ..., \varphi(n)$, to se prema prvoj stavci teoreme 3.1.4. može izvršiti skraćivanje, pa je $a^{\varphi(n)} \equiv 1(\text{mod } n)$ □

Teorema 3.3.3 (Mala Fermaova teorema)**.** *Neka je p prost broj i neka p ne deli a. Onda je*

$$a^{p-1} \equiv 1(mod\ p)$$

Dokaz. Pošto je $(a, p) = 1$ i $\varphi(p) = p-1$ za svaki prost broj p, ovo je samo specijalan slučaj već dokazane Ojlerove teoreme. □

3.4 Primeri i primene

U ovom odeljku će biti predstavljen određen broj primera čijem rešavanju se pristupa direktnim korišćenjem teorema i njihovih posledica iz prethodnog odeljka.

Primer 3.4.1. Dokazati da je broj $7^{2000} - 1$ deljiv sa 10.

Rešenje. Dokažimo tvrđenje na dva načina:

(I) Posmatrajmo poslednju cifru stepena broja 7:

broj	cifra jedinica
7^1	7
7^2	9
7^3	3
7^4	1
7^5	7
7^6	9
7^7	3

Primetimo da se ciklično ponavlja poslednja cifra i to kao ciklus 1, 7, 9, 3, odnosno svaki četvrti stepen brpja 7 ima istu poslednju cifru.

broj	cifra jedinica
7^{4k}	1
7^{4k+1}	7
7^{4k+2}	9
7^{4k+3}	3

Pošto je 2000 deljivo sa 4, broj 7^{2000} se završava jedinicom, pa se $7^{2000} - 1$ završava nulom, odnosno deljivo je sa 10.

(II) Kako je $(7, 10) = 1$, možemo da primenimo Ojlerovu teoremu: $\varphi(10) = 4$ i $7^4 \equiv 1 (\text{mod } 10)$, odnosno $7^{2000} \equiv 1 (\text{mod } 10)$, tj. $7^{2000} - 1$ je deljiv sa 10.

Primer 3.4.2. Dokazati da je broj $n^3 + 2n$ deljiv sa 3 za sve prirodne brojeve n.

Rešenje. Ovo je primer koji je već predstavljen u Glavi 2, ali ćemo ga ovde uraditi primenom kongruencije. Koristeći osnovne osobine konkruencije imamo da broj n može biti kongruentan sa: 0, 1 ili 2 po modulu 3.

n	0	1	2
$2n$	0	2	1
n^3	0	1	2
$n^3 + 2n$	0	0	0

Vidimo da je $2n$ onda kongruentan sa 0, 2 ili 1 po modulu 3, tim redom, a n^3 je kongruentan sa 0, 1 ili 2 po modulu 3, tim redom. Njihov zbir je u sva tri slučaja kongruentan sa 0 po modulu 3, odnosno deljiv sa 3.

Primer 3.4.3. Postoji li prirodan broj n takav da je broj $n^2 + n + 1$ deljiv sa 5?

Rešenje. Kao i u prethodnom primeru, posmatrajmo ostatke koje daju brojevi n i $n^2 + n + 1$ pri deljenju sa 5.

n	0	1	2	3	4
n^2	0	1	4	4	1
$n^2 + n$	0	2	1	2	0

Primetimo da broj $n^2 + n$ daje ostatke 0, 2 ili 1 pri deljenju sa 5. Posmatrajmo, onda, tri slučaja:

(i) $n^2 + n \equiv 0 (\mathrm{mod}\ 5)$, odnosno $n^2 + n + 1 \equiv 1 (\mathrm{mod}\ 5)$

(ii) $n^2 + n \equiv 2 (\mathrm{mod}\ 5)$, odnosno $n^2 + n + 1 \equiv 3 (\mathrm{mod}\ 5)$

(iii) $n^2 + n \equiv 1 (\mathrm{mod}\ 5)$, odnosno $n^2 + n + 1 \equiv 2 (\mathrm{mod}\ 5)$

Zaključujemo da ne postoji $n \in \mathbb{N}$ takvo da $5 | n^2 + n + 1$.

Primer 3.4.4. Dokazati da jednačina $x^2 - 5y = 10z + 3$ nema rešenja u skupu celih brojeva.

Rešenje. Posmatramo poslednje cifre leve i desne strane, tj. ostatke pri deljenju sa 10. $D = 10z + 3 \equiv 3 (\mathrm{mod}\ 10)$

$x (\mathrm{mod}\ 10)$	0	1	2	3	4	5	6	7	8	9
$x^2 (\mathrm{mod}\ 10)$	0	1	4	9	6	5	6	9	4	1

Vidimo da x^2 može davati ostatke iz skupa $\{0, 1, 4, 5, 6, 9\}$ pri deljenju sa 10, a znamo da $5y$ može davati ostatke 0 ili 5, odnosno $x^2 - 5y$ može davati samo ostatke iz skupa $\{0, 1, 4, 5, 6, 9\}$ tj. nikada ne može biti 3 kao na desnoj strani. Dakle, jednačina nema rešenja.

Primer 3.4.5. Dokazati da je broj $2222^{5555} + 5555^{2222}$ deljiv sa 7.

Rešenje. Kako je $2222 \equiv 3 (\mathrm{mod}\ 7)$, to je $2222^{5555} \equiv 3^{5555} (\mathrm{mod}\ 7)$

$$3^1 \equiv 3 (\mathrm{mod}\ 7) \quad 3^2 \equiv 2 (\mathrm{mod}\ 7) \quad 3^3 \equiv 6 (\mathrm{mod}\ 7)$$
$$3^4 \equiv 4 (\mathrm{mod}\ 7) \quad 3^5 \equiv 5 (\mathrm{mod}\ 7) \quad 3^6 \equiv 1 (\mathrm{mod}\ 7)$$

Dakle, $3^6 \equiv 1(\text{mod } 7)$, odnosno $3^{6k} \equiv 1^k(\text{mod } 7) \equiv 1(\text{mod } 7)$. Ovde treba napomenuti i da smo sa nalaženjem odgovarajućeg stepena mogli da stanemo još kod $3^3 \equiv 6(\text{mod } 7)$ jer je $3^3 \equiv 6(\text{mod } 7) \equiv -1(\text{mod } 7)$. Kvadriranjem poslednje kongruencije dobijamo $3^6 \equiv 1(\text{mod } 7)$. $3^{5555} = 3^{6\cdot 925+5} = (3^6)^{925} \cdot 3^5 \equiv 3^5(\text{mod } 7) \equiv 5(\text{mod } 7)$. Na sličan način imamo $5555 \equiv 4(\text{mod } 7)$. Dalje je

$$4^1 \equiv 4(\text{mod } 7) \quad 4^2 \equiv 2(\text{mod } 7) \quad 4^3 \equiv 1(\text{mod } 7)$$

Dakle, $4^{3k} \equiv 1(\text{mod } 7)$. $4^{2222} = 4^{3\cdot 740+2} = (4^3)^{740} \cdot 4^2 \equiv 4^2(\text{mod } 7) \equiv 2(\text{mod } 7)$ Konačno $2222^{5555} + 5555^{2222} \equiv (5+2)(\text{mod } 7) \equiv 0(\text{mod } 7)$

Primer 3.4.6. Pronaći poslednje dve cifre broja 99^{123}.

Rešenje. Kako je $99 \equiv -1(\text{mod } 100)$, korišćenjem osobina kongruencije imamo da je $99^{123} \equiv (-1)^{123}(\text{mod } 100) \equiv -1(\text{mod } 100) \equiv 99(\text{mod } 100)$.

Primer 3.4.7. Odrediti poslednju cifru broja $7^{7^{7^7}}$.

Rešenje. Kako je $7 \equiv -1(\text{mod } 4)$, to je $7^{7^7} \equiv -1(\text{mod } 4)$, jer je 7^7 neparan broj. Dakle, $7^{7^7} = 4k+3$, za neki $k \in \mathbb{N}$. Pošto je $7^2 \equiv -1(\text{mod } 10)$, to je $7^4 \equiv 1(\text{mod } 10)$, pa je $7^{4k} \equiv 1(\text{mod } 10)$. Dakle,

$$7^{7^{7^7}} = 7^{4k+3} = 7^{4k} \cdot 7^3 \equiv 7^3 \equiv 3(\text{mod } 10)$$

Primer 3.4.8. Dokazati da $13 | 2^{70} + 3^{70}$.

Rešenje. Po Maloj Fermaovoj teoremi, imamo da $2^{12} \equiv 1(\text{mod } 13)$, odakle sledi $2^{60} \equiv 1(\text{mod } 13)$. Kako je $2^5 \equiv 6(\text{mod } 13)$ sledi da $2^{10} \equiv -3(\text{mod } 13)$. Dalje sledi $2^{70} = 2^{60} \cdot 2^{10} \equiv 1 \cdot (-3)(\text{mod } 13) \equiv -3(\text{mod } 13)$.
Sa druge strane, $3^3 \equiv 1(\text{mod } 13)$, odakle sledi $3^{69} \equiv 1(\text{mod } 13)$ i $3^{70} \equiv 3(\text{mod } 13)$. Dakle, $2^{70} + 3^{70} \equiv (-3+3)(\text{mod } 13) \equiv 0(\text{mod } 13)$, odnosno $13 | 2^{70} + 3^{70}$, što je i trebalo dokazati.

Primer 3.4.9. Dokazati da ako za neke cele brojeve a, b i c važi $9 | a^3 + b^3 + c^3$, onda barem jedan od brojeva a, b, c mora biti deljiv sa 3.

Rešenje. Neka nijedan od a, b, c nije deljiv sa 3, odnosno, neka su oni oblika $x = 3k \pm 1$. Njihovi kubovi su tada oblika $x^3 = 27k^3 \pm 27k^2 + 9k \pm 1$. Vidimo da oni tada daju ostatak 1 ili -1 pri deljenju sa 9. Odavde sledi da ako nijedan od a, b, c nije deljiv sa 3, onda zbir $a^3 + b^3 + c^3$ daje ostatak $\pm 1 \pm 1 \pm 1$ pri deljenju sa 9, tj. ni za koju kombinaciju znakova + i - nije deljiv sa 9. Dakle, početna pretpostavka je netačna, odnosno barem jedan od a, b i c mora biti deljiv sa 3.

Primer 3.4.10. Dokazati da je broj $n^n - n$ deljiv sa 24 za svaki neparan prirodan broj n.

Rešenje. Kako je $24 = 8 \cdot 3$, dovoljno je dokazati da je $n^n - n$ deljivo sa 3 i sa 8. Primetimo prvo da je $n^n - n = n(n^{n-1} - 1)$. Kako je $n-1$ paran, a n neparan i kako kvadrat neparnog prirodnog broja daje ostatak 1 pri deljenju sa 8, to je $n^{n-1} - 1$ deljivo sa 8. Dalje, ukoliko je n deljivo sa 3 tada je i $n^n - n = n(n^{n-1} - 1)$ očigledno deljivo sa 3. Ukoliko n nije deljiv sa 3 tada, kako je $n-1$ paran, to n^{n-1} daje ostatak 1 pri deljenju sa 3, pa je $n^{n-1} - 1$ deljiv sa 3.

Primer 3.4.11. Za koje prirodne brojeve n je $2^n - 1$ potpun kvadrat. A $2^n + 1$?

Rešenje. Za $n = 1$ imamo da $2^1 - 1 = 1^2$. Ako je $n > 1$, broj 2^n je deljiv sa 4, tj. $2^n - 1 \equiv 3 (\text{mod } 4)$. Kvadrati prirodnih brojeva daju ostatke 0 ili 1 pri deljenju sa 4, što se može videti u sledećoj tablici:

$x(\text{mod } 4)$	0	1	2	3
$x^2(\text{mod } 4)$	0	1	0	1

Dakle, $n = 1$ je jedino rešenje.
Posmatrajmo sada brojeve oblika $2^n + 1$. Ako je $2^n + 1 = k^2$ za neki ceo broj k, imamo da je $2^n = k^2 - 1 = (k-1)(k+1)$, odnosno $k - 1 = 2^l$, a $k + 1 = 2^m$, za neke prirodne k i m. Jasno je da je $2 = 2^m - 2^l$, odnosno mora biti $m = 1$, a $l = 2$. Dakle, $n = 3$ je jedino rešenje.

Primer 3.4.12. Dokazati da postoji beskonačno mnogo prirodnih brojeva n takvih da $n | 2^n + 1$. Naći sve takve proste brojeve.

Rešenje. Dokažimo da tvrđenje važi za sve prirodne brojeve oblika 3^s, gde je s prirodan broj, koristeći indukciju.
Imamo da važi $3 | 2^3 + 1$.
Ako za neko prirodno m važi $3^m | 2^{3^m} + 1$, onda je $2^{3^m} = 3^m k - 1$, gde je k prirodan broj. Sledi da je:

$$2^{3^{m+1}} = (3^m k - 1)^3 = 3^{3m} k^3 - 3^{2m+1} k^2 + 3^{m+1} k - 1 = 3^{m+1} t - 1,$$

gde je t neki prirodan broj. Dakle, $3^{m+1} | 2^{3^{m+1}} + 1$, pa, po indukciji važi $3^m | 2^{3^m} + 1$ za $m = 1, 2, ...$ Dakle, brojeva koji zadovoljavaju traženi uslov ima beskonačno mnogo.
Neka je n prost i važi $n | 2^n + 1$. Po Maloj Fermaovoj teoremi imamo $n | 2^{n-1} - 1$, tj. $n | 2^n - 2$. Kako važi i $n | 2^n + 1$, mora biti $n | 3$. Pošto je n prost, mora biti $n = 3$ i to je jedino rešenje.

Primer 3.4.13. Naći sve proste brojeve p, q i r koji zadovoljavaju jednačinu $p^q + q^p = r$.

Rešenje. Brojevi p, q i r ne mogu svi biti neparni, jer ako bi bili, sa leve strane jednakosti bi bio zbir dva neparna broja koji je paran, a sa desne neparan broj. Znači, bar jedan od njih je paran, pa kako je i prost on je jednak 2. Kako je $p^q + q^p > 2$, to ne može biti $r = 2$, pa je jedan od brojeva p ili q jednak 2.
Neka je $p = 2$. Data jednačina postaje $2^q + q^2 = r$. Kako je $r > 2$, to je r neparan, pa je i q neparan. Kako je q neparan, to je $2^q \equiv 2(\text{mod } 3)$, pa ukoliko q nije deljivo sa 3, njegov kvadrat daje ostatak 1 pri deljenju sa 3, odnosno $3|2^q + q^2$. Međutim tada i $3|r$, pa je $r = 3$, što je nemoguće, jer je $2^q + q^2 > 3$. Znači mora biti $q = 3$. Sada je $r = 2^3 + 3^2 = 17$.
Sva rešenja su trojke $(2, 3, 17)$ i $(3, 2, 17)$.

Primer 3.4.14. Da li jednačina $x^5 + y^5 + z^5 = 2006$ ima rešenja u skupu celih brojeva?

Rešenje. Prema Maloj Fermaovoj teoremi, za svaki broj koji nije deljiv sa 11 važi $x^{10} \equiv 1(\text{mod } 11)$, tj. $11|x^{10} - 1 = (x^5 - 1)(x^5 + 1)$. Samim tim $x^5 \equiv \pm 1(\text{mod } 11)$, pa su jedini mogući ostaci pri deljenju petih stepena sa 11 jednaki 0, 1, -1. Kako 2006 daje ostatak 4 pri deljenju sa 11, to je očigledno da data jednačina nema rešenja.

Primer 3.4.15. Dokazati da $21|a^2 + b^2$ povlači $441|a^2 + b^2$.

Rešenje. Kako $21|a^2+b^2$, to $3|a^2+b^2$ i $7|a^2+b^2$. Kako su ostaci kvadrata pri deljenju sa 3 ili 0 ili 1, to i a i b moraju biti deljivi sa 3, pa je $a^2 + b^2$ deljivo sa 9. Takođe, kako kvadarati pri deljenju sa 7 daju ostatke 0, 1, 2 i 4, to i a i b moraju biti deljivi sa 7, pa je $a^2 + b^2$ deljivo sa 49. Znači $9 \cdot 49 = 441|a^2 + b^2$.

Primer 3.4.16. Naći sve prirodne brojeve $n > 1$ takve da je $1^n + 2^n + ... + (n-1)^n$ deljivo sa n.

Rešenje. Neka je n neparan broj veći od 1. Tada je $\dfrac{n-1}{2}$ pozitivan ceo broj i za $k = 1, 2, ..., \dfrac{n-1}{2}$ kao posledicu leme 4.1.1.(2), koja sledi (ako su a i b celi brojevi i $a \neq -b$, onda važi $a + b|a^{2m+1} + b^{2m+1}$), lako vidimo

$$n|k^n + (n-k)^n$$

Dakle, $n|1^n + 2^n + ... + (n-1)^n$.

Neka je n paran broj i neka je 2^s najveći stepen 2 koji deli n (s je pozitivan ceo broj). S obzirom da je $2^s > s$, za parne k imamo $2^s|k^n$, odakle sledi

$$2^n + 4^n + ... + (n-4)^n + (n-2)^n \equiv 0(\mathrm{mod}\ 2^s),$$

a za neparne k (broj takvih k u sekvenci $1, 2, ..., n-1$ je $\frac{1}{2}n$) imamo, prema Ojlerovoj teoremi, $k^{2^{s-1}} \equiv 1(\mathrm{mod}\ 2^s)$ (jer je $\varphi(2^m) = 2^{m-1}$). Odavde sledi $k^n \equiv 1(\mathrm{mod}\ 2^s)$ (jer mora biti $2^{s-1}|n$). Stoga

$$1^n + 3^n + ... + (n-3)^n + (n-1)^n \equiv \frac{1}{2}n(\mathrm{mod}\ 2^s),$$

odakle sledi

$$1^n + 2^n + ... + (n-2)^n + (n-1)^n \equiv \frac{1}{2}n(\mathrm{mod}\ 2^s),$$

Sada, ako bi bilo $n|1^n + 2^n + ... + (n-1)^n$, onda koristeći $2^s|n$, imali bismo da je $\frac{1}{2}n \equiv 0(\mathrm{mod}\ 2^s)$, odakle $2^s|\frac{1}{2}n$ i $2^{s+1}|n$, što je u kontradikciji sa definisanjem s. Stoga, za parno n: $n \nmid 1^n + 2^n + ... + (n-1)^n$.

Glava 4

Kriterijumi deljivosti

4.1 Osnovni kriterijumi

Teorema 4.1.1. *Za prirodan broj* $n = \overline{a_m a_{m-1} ... a_1 a_0}$ *važi* $2^k | n$ *ako i samo ako* $2^k | \overline{a_{k-1} a_{k-2} ... a_1 a_0}$.

Dokaz. $n = (a_m 10^m + ... + a_k 10^k) + (a_{k-1} 10^{k-1} + ... + a_1 \cdot 10 + a_0)$. Svaki od sabiraka u prvoj zagradi je deljiv sa 2^k pa n i $a_{k-1} 10^{k-1} + ... + a_1 \cdot 10 + a_0 = \overline{a_{k-1} a_{k-2} ... a_1 a_0}$ daju isti ostatak pri deljenju sa 2^k. □

Posledica ove teoreme su dobro poznata pravila za deljenje sa 2 (prirodan broj n je deljiv sa 2 ako i samo ako mu je poslednja cifra deljiva sa 2), 4 (prirodan broj n je deljiv sa 4 ako i samo ako mu je dvocifreni završetak deljiv sa 4) i 8 (prirodan broj n je deljiv sa 8 ako i samo ako mu je trocifren završetak deljiv sa 8) itd.

Važi i slično pravilo za deljivost broja stepenom broja 5 i s obzirom na sličnost sa prethodnim dokazom, teorema će ovde biti samo navedena.

Teorema 4.1.2. *Za prirodan broj* $n = \overline{a_m a_{m-1} ... a_1 a_0}$ *važi* $5^k | n$ *ako i samo ako* $5^k | \overline{a_{k-1} a_{k-2} ... a_1 a_0}$.

Teorema 4.1.3. *Svaki prirodan broj* n *i zbir njegovih cifara* $S(n)$ *pri deljenju sa 3 i sa 9 daju iste ostatke.*

Dokaz. Ako je $n = a_0 + 10a_1 + 10^2 a_2 + ... + 10^k a_k$, onda je $S(n) = a_0 + a_1 + a_2 + ... + a_k$. Kako je $10 \equiv 1 (\mathrm{mod}\ 9)$, onda je i $10^k \equiv 1 (\mathrm{mod}\ 9)$, odnosno $a_k 10^k \equiv a_k (\mathrm{mod}\ 9)$ za svako prirodno k. Dakle, imamo da važi: $n = a_0 + 10a_1 + 10^2 a_2 + ... + 10^k a_k \equiv a_0 + a_1 + a_2 + ... + a_k = S(n) (\mathrm{mod}\ 9)$. Iz činjenice da je $n \equiv S(n) (\mathrm{mod}\ 9)$ sledi da n i $S(n)$ imaju isti ostatak pri deljenju sa 9. Analogno ovome se dokazuje i za 3. □

Lema 4.1.1. Neka su a i b celi brojevi. Tada važi:

1. $a - b | a^n - b^n$, gde je $a \neq b$
2. $a + b | a^{2n+1} + b^{2n+1}$, gde je $a \neq -b$

Dokaz.

1. Važi $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$. Kako je desna strana deljiva sa $a - b$, mora biti i leva, tj. $a - b | a^n - b^n$
2. Važi $a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + ... - ab^{2n-1} + b^{2n})$. Kako je desna strana deljiva sa $a + b$, mora biti i leva, tj. $a + b | a^{2n+1} + b^{2n+1}$

□

Teorema 4.1.4. *Broj $n = \overline{a_m a_{m-1} ... a_1 a_0}$ daje isti ostatak pri deljenju sa 11 kao i razlika suma njegovih cifara na parnim i neparnim mestima.*

Dokaz. Kako je 11 = 10 + 1 = 10 - (-1), po prethodnoj lemi, imamo $11 | 10^k - (-1)^k$. Broj 10^k daje isti ostatak kao broj $(-1)^k$ pri deljenju sa 11. Sledi $n = \overline{a_m a_{m-1} ... a_1 a_0} = a_m 10^m + ... + a_1 \cdot 10 + a_0 \equiv a_m(-1)^m + a_{m-1}(-1)^{m-1} + ... + a_1(-1) + a_0$, što je zapravo razlika sume cifara na parnim i neparnim mestima broja n. □

Teorema 4.1.5. *Broj je deljiv sa 7, 11, 13 kada je razlika između zbira trocifrenih klasa koje u broju stoje na neparnim mestima i zbira trocifrenih klasa koje stoje na parnim mestima deljiva sa datim od brojeva.*

Dokaz. Neka je $n = \overline{a_m a_{m-1} ... a_1 a_0}$ i neka je s broj koji se dobija na način opisan u teoremi, odnosno: $s = a_0 + 10a_1 + 100a_2 - (a_3 + 10a_4 + 100a_5) + (a_6 + 10a_7 + 100a_8) - (a_9 + 10a_{10} + 100a_{11}) + ...$
Posmatrajmo razliku
$n - s = a_0 + 10a_1 + 100a_2 + .. + 10^m a_m - (a_0 + 10a_1 + 100a_2) + (a_3 + 10a_4 + 100a_5) - (a_6 + 10a_7 + 100a_8) + (a_9 + 10a_{10} + 100a_{11}) - ...)$
$= a_3(10^3 + 1) + 10a_4(10^3 + 1) + 100a_5(10^3 + 1) + a_6(10^6 - 1) + 10a_7(10^6 - 1) + 100a_8(10^6 - 1) + ... + a_9(10^9 + 1) + 10a_{10}(10^9 + 1) + 100a_{11}(10^9 + 1) + ...$
$= (10^3 + 1)(a_3 + 10a_4 + 100a_5) + (10^6 - 1)(a_6 + 10a_7 + 100a_8) + (10^9 + 1)(a_9 + 10a_{10} + 100a_{11} + ...)$.
Vidimo da su sabirci oblika $((10^3)^k - (-1)^k)(a_{3k} + 10a_{3k+1} + 100a_{3k+2})$.
Koristeći lemu 4.1.4. imamo da je $(10^3)^k - (-1)^k$ deljivo sa 1001. Kako je $1001 = 7 \cdot 11 \cdot 13$ onda 7, 11 i 13 dele svaki od sabiraka u $n - s$, odnosno n je deljiv sa 7, 11 i 13 ako i samo ako je s deljiv sa 7, 11 i 13, tim redom. □

Na primer, broj 539 693 385 ima razliku ovih klasa 539-693+385=231, pa je deljiv sa 7, 11 i 77, a nije deljiv sa 13, 91, 143 i 1001.

4.2 Primeri

Primer 4.2.1. Proizvod šest uzastopnih prirodnih brojeva je sedmocifreni broj 216*16*. Odrediti nepoznate cifre zamenjene zvezdicama.

Rešenje. Proizvod šest uzastopnih prirodnih brojeva je deljiv sa 2, 3, 4, 5, 6, kao i $2 \cdot 5 = 10$ i 9 (pošto imamo dva broja deljiva sa 3). Ako je deljiv sa 10 mora se završavati nulom, pa je poslednja zvezdica 0. Ako je deljiv sa 9, zbir cifara mu je deljiv sa 9: $2+1+6+*+1+6+0 = 16+*$. S obzirom na to da su ovde u pitanju cifre, jedina mogućnost za * je 2. Traženi broj je 2162160.

Primer 4.2.2. Odrediti sve petocifrene brojeve oblika $\overline{34x5y}$ koji su deljivi brojem 36.

Rešenje. Da bi broj bio deljiv sa 36, mora biti deljiv sa 4 i sa 9. Da bi broj bio deljiv sa 4, njegov dvocifreni završetak mora biti deljiv sa 4. Jedine mogućnosti su nam 52 i 56, tj. $y \in \{2, 6\}$.

(i) Ako je $y = 2$, broj $\overline{34x52}$ mora biti deljiv sa 9. Da bi broj bio deljiv sa 9, zbir njegovih cifara mora biti deljiv sa 9. Imamo da $S(\overline{34x52}) = 3+4+x+5+2 = 14+x$ mora biti deljivo sa 9. Kako je x cifra, jedina mogućnost nam je $x = 4$, odnosno $n_1 = 34452$.

(ii) Ako je $y = 6$, broj $\overline{34x56}$ mora biti deljiv sa 9. Imamo da $S(\overline{34x56}) = 3+4+x+5+6 = 18+x$ mora biti deljivo sa 9. Kako je x cifra, jedine mogućnosti su nam $x \in \{0, 9\}$, odnosno $n_2 = 34056$ i $n_3 = 34956$.

Primer 4.2.3. Koliko ima četvorocifrenih brojeva oblika $\overline{*97*}$ koji su deljivi brojem 45?

Rešenje. Da bi broj bio deljiv sa 45, mora biti deljiv sa 5 i sa 9. Da bi broj bio deljiv sa 5, poslednja cifra mu mora biti 0 ili 5. Da bi broj bio deljiv sa 9, zbir cifara mu mora biti deljiv sa 9.

(i) Ako je poslednja zvezdica 0, tj. imamo broj $\overline{*970}$, zbir cifara broja je $9+7 = 16$ i zbog deljivosti sa 9, jedina mogućnost za prvu zvezdicu nam je 2, odnosno, traženi broj je 2970.

(ii) Ako je poslednja zvezdica 5, tj. imamo broj $\overline{*975}$, zbir cifara broja je $9+7+5 = 21$ i zbog deljivosti sa 9, jedina mogućnost za prvu zvezdicu nam je 6, odnosno, traženi broj je 6975.

Primer 4.2.4. Vrednosti razlomaka $\dfrac{\overline{42*4*}}{72}$ i $\dfrac{\overline{32*60}}{56}$ predstavljaju prirodne brojeve. Koji od razlomaka je veći?

Rešenje. Posmatrajmo prvi razlomak. Broj $\overline{42*4*}$ mora biti deljiv sa 72, odnosno sa 8 i sa 9. Zbir njegovih cifara je $10+*+*$, što mora biti deljivo sa 9. S obzirom na to da su * cifre, mogućnosti za zbir $*+*$ su nam 8 i 17. Takođe, važi i da trocifreni završetak *4* mora biti deljiv sa 8. Isprobavanjem svih mogućnosti dobijamo kandidate: 42048, 42246, 42444, 42642, 42840, 42948 (posmatramo samo parne brojeve zbog deljivosti sa 8). Proverom vidimo da su samo 42048 i 42840 deljivi sa 8, pa su samo oni i rešenja.
Posmatrajmo sada drugi razlomak. Broj $\overline{32*60}$ mora biti deljiv sa 56, odnosno sa 8 i sa 7. Zbog deljivost sa 8, *60 mora biti deljivo sa 8, pa su kandidati: 32160, 32360, 32560, 32760 i 32960. Proverimo sada da li su ovi brojevi deljivi sa 7:

Broj	Provera deljivosti	Deljiv sa 7
32160	160 - 32 = 128	ne
32360	360 - 32 = 328	ne
32560	560 - 32 = 528	ne
32760	760 - 32 = 728	da
32960	960 - 32 = 928	ne

Dakle, vrednost prvog razlomka je: ili $\dfrac{42840}{72} = 595$ ili $\dfrac{42048}{72} = 584$, a drugog: $\dfrac{32760}{56} = 585$. Vidimo da poredak ova dva razlomka nije jednoznačno određen.

Primer 4.2.5. Broju 10 dopisati sleva i zdesna po jednu cifru tako da dobijeni broj bude deljiv sa 36.

Rešenje. Neka je traženi broj $\overline{x10y}$. Da bi broj bio deljiv sa 36 mora biti deljiv i sa 4 i sa 9. Zbog deljivisti sa 4, cifra y može biti 0, 4, ili 8. Zbir cifara je tada $x+1$, $x+5$ ili $x+9$. Prema tome x je tada 8, 4 ili 9, tj. radi se o brojevima 8100, 4104 i 9108.

Primer 4.2.6. Dat je broj 19911991...19911991 (1992 puta je napisan broj 1991). Dokazati da je dati broj deljiv sa 33, a nije deljiv sa 66 ni sa 99.

Rešenje. Broj 19911991...1991 (1992 puta) ima zbir cifara $1992 \cdot 20 = 3 \cdot 664 \cdot 20$, pa je deljiv sa 3, ali nije sa 9. Zbir cifara na parnim mestima jednak je zbiru cifara na neparnim mestima pa je broj deljiv i sa 11, tj. deljiv je sa 33. Broj nije deljiv sa 66 jer je neparan, pa nije deljiv sa 2. Nije deljiv ni sa 99 jer nije deljiv sa 9.

Primer 4.2.7. Neki broj se piše u dekadnom zapisu pomoću 300 jedinica i izvesnog broja nula. Može li on biti potpun kvadrat?

Rešenje. Zbir cifara datog broja je 300. Kako $3|300$ i $9 \nmid 300$, dati broj ne može biti kvadrat prirodnog broja.

Primer 4.2.8. Ako je broj deljiv sa 99, tada zbir njegovih cifara ne može biti manji od 18. Dokazati.

Rešenje. Posmatrani broj je deljiv sa 9 i sa 11. Neka je x zbir cifara broja na parnim mestima, a y zbir cifara broja na neparnim mestima ($x \geq 0$, $y \geq 0$) i neka je $x \geq y$. Tada, po pravilima deljivosti za 9 i 11, važi $11|x-y$ i $9|x+y$. Iz prve deljivosti je $x-y \in \{0, 11, 22, ...\}$. S obzirom da je zbir $x+y$ deljiv sa 9, $x+y \in \{9, 18, 27, ...\}$ (ne može biti 0 jer je bar jedan od brojeva x i y veći od 0). Ako je $x-y=0$, tj. $x=y$, ne može biti $x+y=9$. Ako je $x-y \geq 11$, njihov zbir ne može biti manji od 11, jer su u pitanju nenegativni brojevi. Dakle, $x+y \geq 18$. Ako je $x<y$, posmatramo $y-x$ koje je iz skupa $\{11, 22, ...\}$, pa se slučaj svodi na prethodni.

Primer 4.2.9. Dokazati da $5|9^{100}+4^{101}$.

Rešenje. Broj je deljiv sa 5 ako mu je poslednja cifra 0 ili 5. Posmatrajmo poslednju cifru stepena broja 9:

Broj	Poslednja cifra
9^1	9
9^2	1
9^3	9
9^4	1

Primetimo da se ciklično ponavljaju završeci 9 i 1 i to: kada je eksponent paran, broj se završava sa 1, a kada je neparan sa 9. Dakle 9^{100} se završava sa 1. Posmatrajmo poslednju cifru stepena broja 4:

Broj	Poslednja cifra
4^1	4
4^2	6
4^3	4
4^4	6

Primetimo da se ciklično ponavljaju završeci 4 i 6 i to: kada je eksponent paran, broj se završava sa 6, a kada je neparan sa 4. Dakle 4^{101} se završava sa 4. Sledi da se zbir $9^{100} + 4^{101}$ završava sa $4 + 1 = 5$, odnosno posmatrani broj je deljiv sa 5.

Primer 4.2.10. Svi dvocifreni brojevi od 19 do 92 su ispisani jedan za drugim i time je dobijen prirodan broj $n = 19202122...909192$. Neka je 3^k najveći stepen broja 3 koji je činilac broja n. Pronaći vrednost k.

Rešenje. Za zapisivanje svih brojeva treće desetice upotrebljeno je 10 dvojki (za cifre desetica) i cifre 0, 1, 2, ... , 9 za cifre jedinica. Slično je i za brojeve četvrte desetice, gde je upotrebljeno 10 trojki za cifre desetica i cifre 0, 1, 2, ... , 9 za cifre jedinica, itd.
Neka je $S(n)$ zbir cifara broja n.
$S(n) = 1 + 9 + (10 \cdot 2 + 0 + 1 + 2 + .. + 9) + (10 \cdot 3 + 0 + 1 + 2 + .. + 9) + ... + (10 \cdot 8 + 0 + 1 + 2 + .. + 9) + 9 + 0 + 9 + 1 + 9 + 2 = 1 + 9 + 9 + 0 + 9 + 1 + 9 + 2 + 10(2 + 3 + 4 + ... + 8) + 7(0 + 1 + 2 + .. + 9) = 40 + 10 \cdot 35 + 7 \cdot 45 = 705$. Zbir cifara broja 705 je 12, i $12 \equiv 3(\text{mod } 9)$, pa broj n nije deljiv sa 9, ali jeste deljiv sa 3, tako da je $k = 1$.

Primer 4.2.11. Dat je izraz

$$*1 * 3 * 3^2 * 3^3 * ... * 3^{2021} * 3^{2022}.$$

Ana i Branislav naizmenično zamenjuju po jednu zvezdicu sa + ili -. Branislav nastoji da broj koji se dobije posle zamene i poslednje zvezdice, bude deljiv sa 7. Može li Ana da ga spreči ako ona prva igra?

Rešenje. Dokažimo da važi $7|3^n + 3^{n+3}$ za $n \geq 0$.
Kako je $3^n + 3^{n+3} = 3^n \cdot (1 + 3^3) = 3^n \cdot 28$, važi $7|3^n + 3^{n+3}$ za $n \geq 0$.
Anina taktika će biti sledeća: prvim potezom ona zamenjuje prvu zvezdicu(ispred broja 1) znakom $+$. Zatim preostalih 2022 člana grupiše u 337 šestorki uzastopnih stepena, a u okviru svake šestorke formira tri para oblika $(3^{6k+1}, 3^{6k+4})$, $(3^{6k+2}, 3^{6k+5})$, $(3^{6k+3}, 3^{6k+6})$ $(k = 0, 1, 2, ..., 337)$. Kad Branislav zameni zvezdicu nekim znakom, Ana zamenjuje istim znakom zvezdicu ispred drugog broja iz istog para. Dobijeni broj pri deljenju sa 7 daje ostatak 1.

Primer 4.2.12. Dokazati da je cifra stotina broja $2^{1999} + 2^{2000} + 2^{2001}$ parna.

Rešenje. Kako je $2^{1999} + 2^{2000} + 2^{2001} = 2^{1999} \cdot 7$, to je dati broj očigledno deljiv sa 8, pa mu je trocifreni završetak deljiv sa 8, a dvocifreni sa 4. Odredimo ostatak datog broja pri deljenju sa 25. Kako je $2^{10} = 1024 \equiv -1 (\bmod 25)$, to je $2^{20} \equiv 1 (\bmod 25)$ pa je $2^{1999} + 2^{2000} + 2^{2001} \equiv 13 + 1 + 2 (\bmod 25) \equiv 16 (\bmod 25)$. Sada je jasno da dvocifreni završetak broja mora biti jedan od brojeva 16, 41, 56, 81, pa kako on mora biti deljiv sa 4, jedine mogućnosti su 16 i 56. Ukoliko je $\overline{abc}$ trocifreni završetak datog broja, on mora biti deljiv sa 8, pa kako je $\overline{abc} = 100a + \overline{bc}$, a $\overline{bc}$ je jedan od brojeva 16 ili 56 koja su oba deljiv sa 8, to mora biti i $100a$ deljivo sa 8. Samim tim je a paran.

Glava 5

Zaključak

Cilj ovog rada je da se na jednom mestu sakupe, objasne i pobroje tipični zadaci iz teorije brojeva. Akcenat je na dokazivanju svih teorema i posledica teorema koje se đacima u osnovnim i srednjim školama samo navode. Osim toga, na kraju svake glave je obrađeno gradivo primenjeno u primerima čija težina je takva da se počinje od onih najlakših, prikladnih mlađim razredima osnovnih škola, preko onih malo ozbiljnijih koji se mogu raditi u starijim razredima, pa do onih najtežih, koji se mogu obrađivati u srednjim školama. Ideja rada je da predstavlja dosta skraćenu verziju priručnika za sve zainteresovane za teoriju brojeva. Može predstavljati izvesni vodič predavačima, kao i izvor informacija i instrukcija učenicima.

U drugoj glavi su izloženi osnovni pojmovi iz deljivosti brojeva i dokazane osnovne teoreme o svojstvima deljivosti, kao i uvedeni pojmovi delilaca, prostih brojeva i kanonske faktorizacije. U trećoj glavi su uvedeni pojmovi kongruencije, njene osnovne karakteristike, sistema ostataka kao i dve značajne teoreme u teoriji brojeva: Ojlerova teorema i Mala Fermaova teorema. Četvrta glava sadži najčešće korišćene kriterijume deljivosti. S obzirom na to da se oni prvi put obrađuju u osnovnim školama, tvrđenja su dokazana tako da ih i mlađi učenici mogu razumeti.

Od velike je važnosti predstavljanje dokaza učenicima u ranom dobu, da bi dobili priliku da sagledaju njegovu ulogu i dobiju osećaj šta je prihvatljivo kao dokaz i kao logika u pozadini. Iskazivanje sumnji treba ohrabrivati i razvijati argumentovane rasprave sa ciljem da ubedimo druge (a i sebe). Dokaz treba posmatrati kao argument dovoljno jak da ubedi razumnog skeptika.

Ne predstavljaju svakako sve hipoteze i teoreme dobru osnovu za konstrukciju dokaza koji mogu biti od edukativnog značaja, ali je na predavačima da njihovu važnost prepoznaju i izvrše selekciju onih najkorisnijih. Ako predavači stvore prilike za edukaciju učenika o raznim tipovima dokaza, učenici mogu razviti ne samo dublje razumevanje materije, već i dublje razumevanje same matematike. Učionice u kojima su učenici ohrabreni da predstave svoja mišljenja i u kojima svi doprinose procenom tuđih opažanja pružaju bogato okruženje za učenje matematičkog rezonovanja. Na kraju, istinsko razumevanje zahteva da đaci vide *zašto* je nešto slučaj, tj. zašto je nešto tačno, kao i, zašto nešto *uvek* mora biti tačno, a razumevanje ovoga je najbolje kroz matematički dokaz.

Bibliografija

[1] Vladimir Mićić, Zoran Kadelburg, Dušan Đukić. Uvod u teoriju brojeva, Beograd, 2004.

[2] Ivan Matić. Uvod u teoriju brojeva, Osijek, 2014.

[3] Eric J. Knuth. Proof as a Tool for Learning Mathematics, http://web.mit.edu/

[4] Waclaw Sierpinski. 250 Problems in Elementary Number Theory, Warszava, 1970.

[5] Waclaw Sierpinski. Elementary Theory of Numbers, Monografie Matematyczne 42, Warszawa, 1964.

[6] Zoran Kadelburg, Srđan Ognjanović, Sonja Čukić. Analiza sa algebrom 1 - Udžbenik sa zbirkom zadataka za 1. razred Matematičke gimnazije, Beograd, 2021.

[7] Srđan Ognjanović , Vladimir Mićić , Zoran Kadelburg. Analiza sa algebrom 2 - Udžbenik sa zbirkom zadataka za 2. razred Matematičke gimnazije, Beograd, 2017.

[8] Srđan Ognjanović. Matematika 7d - Zbirka zadataka sa rešenjima za dodatnu nastavu, Beograd, 2018

[9] Srđan Ognjanović. Matematika 10^+ - Rešeni zadaci sa prijemnih ispita u Matematičkoj gimnaziji 1975-2010, Beograd, 2010.

[10] Marija Stanić, Nebojša Ikodinović. Teorija brojeva - Zbirka zadataka, Beograd, 2004.

[11] A. Zolić, S. Ognjanović. Materijali za upis u VII razred Matematičke gimnazije - Zbirka pripremnih zadataka, Beograd 2005.

[12] Vladimir Baltić. Teorija brojeva, pripreme za JBMO, https://www.mg.edu.rs/sr/takmicenja/pripreme-za-takmicenja/pripreme-iz-matematike 2004.

[13] Matematička gimnazija - Dodatna nastava za prvi razred šk. 2005/06, Uvod u kongruencije i deljivost https://www.mg.edu.rs/sr/takmicenja/pripreme-za-takmicenja/pripreme-iz-matematike

[14] https://dms.rs/dodatna-nastava-matematike-za-ucenike-osnovnih-skola

[15] https://matematiranje.in.rs