Djeljivost cijelih brojeva

Jakše, Anita

Djeljivost cijelih brojeva

Jakše, Anita

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Anita Jakše

Djeljivost cijelih brojeva

Diplomski rad

Voditelj rada:
prof. dr. sc. Dijana Ilišević

Zagreb, srpanj 2020.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

No amount of money ever bought a second of time.

Sadržaj

Uvod

Zbroj, razlika i umnožak cijelih brojeva je također cijeli broj, pa kažemo da je skup cijelih brojeva zatvoren na zbrajanje, oduzimanje i množenje. Međutim, dijeljenjem dva cijela broja ne dobivamo uvijek cijeli broj. Ako dijeljenjem cijelog broja m cijelim brojem n kao rezultat dobijemo cijeli broj, tada kažemo da je m djeljiv sa n. Tako dolazimo do pojma djeljivosti koji je jedan od najvažnijih pojmova teorije brojeva.

Ovaj rad podijeljen je na četiri poglavlja u kojima su objašnjeni pojmovi vezani uz djeljivost cijelih brojeva te izloženi mnogi teoremi o djeljivosti. Svako poglavlje sadrži i zadatke s osnovnoškolskih i srednjoškolskih natjecanja koji su poredani po razini, razredu i godini.

Prvo poglavlje sadrži osnovne pojmove i rezultate vezane uz djeljivost cijelih brojeva kao što su: pravila djeljivosti, teorem o dijeljenju s ostatkom, najveći cijeli dio nekog broja i slično. Osnovni pojmovi koji su u ovom poglavlju definirani, kao i teoremi koji su dokazani, ključni su za ostala poglavlja.

Drugo poglavlje temelji se na rezultatima o najvećem zajedničkom djelitelju i najmanjem zajedničkom višekratniku te se u njemu uvodi i pojam prostih brojeva, koji se kasnije detaljnije obrađuje u četvrtom poglavlju. Ovo poglavlje sadrži dokaz Euklidovog algoritma i primjere vezane uz isti. Također, dokazuje se osnovna veza između najvećeg zajedničkog djelitelja i namjanjeg zajedničkog višekratnika.

Tema trećeg poglavlja su linearne i nelinearne diofantske jednadžbe i neke od metoda za njihovo rješavanje koje su opisane i ilustrirane primjerima.

Zadnje poglavlje, kao što je već spomenuto, temelji se na prostim djeliteljima. Dokazuju se teoremi vezani uz proste djelitelje općenito, rastav na proste faktore te operacije minimum i maksimum.

Poglavlje 1

Osnovni pojmovi

1.1 Djeljivost cijelih brojeva

Rezultat dijeljenja dvaju brojeva naziva se **količnik** ili **kvocijent**. U skupu cijelih brojeva dijeljenje nije uvijek moguće, što nas dovodi do pojma djeljivosti.

Definicija 1.1.1. *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b **djeljiv** sa a, odnosno da a **dijeli** b, ako postoji cijeli broj c takav da je $b = ac$. Tada pišemo $a \mid b$. U suprotnom, pišemo $a \nmid b$. Ako $a \mid b$, kažemo da je a **djelitelj** broja b. Ako je cijeli broj c takav da je $b = ac$, tada i $c \mid b$. Brojeve a i c nazivamo **komplementarnim djeliteljima** broja b.*

Ako je dijeljenje moguće, rezultat dijeljenja je jedinstven, što dokazujemo u sljedećem teoremu.

Teorem 1.1.2. *Ako je b djeljiv sa $a \neq 0$, njihov količnik je jednoznačno određen.*

Dokaz. Neka je b djeljiv sa $a \neq 0$. Tada, po prethodnoj definiciji, postoji $c \in \mathbb{Z}$ takav da je $b = ac$. Kada bi c' zadovoljavao isto, vrijedilo bi $b = ac'$, odakle slijedi da je $ac = ac'$. Kako je $a \neq 0$, slijedi $c = c'$. Dakle, količnik je jednoznačno određen. □

S obzirom na jednoznačnost količnika, mogu se odrediti neki posebni (trivijalni) djelitelji. Djelitelji broja $a \in \mathbb{Z}$ su uvijek brojevi ± 1 i $\pm a$. Pritom je broj 0 djeljiv sa svakim cijelim brojem $a \neq 0$, ali nije djelitelj niti jednog broja.

Ako je a prirodan broj veći od 1 kojemu su 1 i a jedini djelitelji, tada kažemo da je a **prost** broj. Za prirodan broj veći od 1 koji nije prost kažemo da je **složen**.

Teorem 1.1.3. *Ako je a djelitelj broja b, tada je i $-a$ njegov djelitelj. Brojevi b i $-b$ imaju iste djelitelje.*

Dokaz. Pretpostavimo da a dijeli b. Iz definicije slijedi da postoji $c \in \mathbb{Z}$ takav da je $b = ac$. Kako je $b = -a \cdot (-c)$ i $-b = a \cdot (-c)$, slijedi da je $-a$ djelitelj broja b te da je a djelitelj broja $-b$. Sada je očito i da b i $-b$ imaju iste djelitelje. □

Primjer 1.1.4. *Broj* 4 *je djelitelj broja* 20*, ali očito je i* -4 *djelitelj broja* 20*. Promotrimo sada brojeve* -20 *i* 20*. Djelitelji broja* -20 *su* ± 1*,* ± 2*,* ± 4*,* ± 5*,* ± 10 *i* ± 20*, a djelitelji broja* 20 *su* ± 1*,* ± 2*,* ± 4*,* ± 5*,* ± 10 *i* ± 20*. Dakle, vidimo da su djelitelji brojeva* 20 *i* -20 *isti.*

Promotrimo li, npr., brojeve 8, 4 i 48, vidimo da je broj 8 djeljiv s 4, a 48 djeljiv s 8. Logično bi bilo zaključiti da je onda broj 48 djeljiv s 4, što zbilja i jest. Dokažimo odgovarajuću opću tvrdnju sljedećim teoremom.

Teorem 1.1.5. *Neka su* $a, b, c \in \mathbb{Z}$*. Ako je* b *djeljiv sa* a *i ako je* c *djeljiv sa* b*, onda je* c *djeljiv sa* a*. Kraće zapisujemo: ako* $a \mid b$ *i* $b \mid c$*, onda* $a \mid c$*.*

Dokaz. S obzirom da $a \mid b$ i $b \mid c$, tada iz definicije slijedi da postoje cijeli brojevi q i q' takvi da je $b = aq$ i $c = bq'$. Iz toga slijedi da je $c = aqq'$, pa zaključujemo da je c djeljiv sa a. □

Analogno se dokazuje sljedeći teorem.

Teorem 1.1.6. *Neka su* $a, b, c, d \in \mathbb{Z}$*. Ako* $a \mid b$ *i* $c \mid d$*, onda* $ac \mid bd$*.*

Navedeni teorem može se poopćiti. U tu svrhu uzimamo cijele brojeve a_i i b_i, $i = 1, 2, 3, \ldots, n$. Ako $a_i \mid b_i$, $i = 1, 2, 3, \ldots, n$, tada $a_1 a_2 \cdots a_n \mid b_1 b_2 \cdots b_n$. Ovo se dokazuje matematičkom indukcijom po n. Iz promatranja djeljivosti umnožaka slijedi i djeljivost količnika, stoga imamo sljedeći teorem.

Teorem 1.1.7. *Neka su* b *i* c *cijeli brojevi djeljivi cijelim brojem* a *i neka* $b \mid c$*. Tada* $\frac{b}{a} \mid \frac{c}{a}$*.*

Dokaz. Zbog $b \mid c$ postoji cijeli broj q takav da je $c = bq$, iz čega zaključujemo da je $\frac{c}{a} = \frac{b}{a}q$. Dakle, $\frac{b}{a} \mid \frac{c}{a}$. □

Nadalje, promatramo li zbroj ili razliku, ne možemo zaključiti dijeli li cijeli broj a broj $b \pm c$ (npr. 2 ne dijeli $3 + 4$, ali 2 dijeli $5 + 3$). No, ako a dijeli oba broja b i c, tada znamo da dijeli i njihov zbroj i njihovu razliku.

Teorem 1.1.8. *Neka su* $a, b, c \in \mathbb{Z}$*. Ako* $a \mid b$ *i* $a \mid c$*, tada* $a \mid (b \pm c)$*.*

Dokaz. Ako $a \mid b$ i $a \mid c$, onda po definiciji slijedi $b = aq$ i $c = aq'$, $q, q' \in \mathbb{Z}$. Zbrojimo li ili oduzmemo b i c, imamo: $b \pm c = a(q \pm q')$. Sada je očito da $a \mid (b \pm c)$. □

Ako $c \mid a$ i $c \mid b$, onda $c \mid ax$ i $c \mid by$, pa prethodni teorem povlači $c \mid (ax + by)$. Ovaj zaključak možemo poopćiti: ako $c \mid a_i$ te ako su x_i cijeli brojevi ($i = 1, 2, \ldots, n$), tada $c \mid (a_1x_1 + a_2x_2 + \cdots + a_nx_n)$.

Teorem 1.1.9. *Ako je cijeli broj b djeljiv cijelim brojem $a \neq 0$, tada je ili $b = 0$ ili $|b| \geq |a|$.*

Dokaz. Neka je $b \neq 0$. Kako $a \mid b$, po definiciji djeljivosti cijelih brojeva postoji cijeli broj $q \neq 0$ takav da je $a = bq$. Iz toga slijedi $|b| = |aq| = |a||q|$. Kako je q cijeli broj i $q \neq 0$, vrijedi da je $|q| \geq 1$, pa slijedi $|b| \geq |a|$. □

Prema prethodnom teoremu, za svaki djelitelj b od a vrijedi $-|a| \leq b \leq |a|$, pa je skup svih djelitelja svakog cijelog broja različitog od 0 konačan. Sljedeći teorem govori o slučaju kada je $|b| = |a|$.

Teorem 1.1.10. *Dva cijela broja a i b su međusobno djeljiva ($a \mid b$ i $b \mid a$) ako i samo ako je $|a| = |b|$. Nadalje, ako $a \mid 1$, tada je $|a| = 1$.*

Dokaz. Pretpostavimo da $a \mid b$ i $b \mid a$. Iz prethodnog teorema slijedi $|a| \geq |b|$ i $|b| \geq |a|$. Dakle, $|a| = |b|$.

Obrnuto, iz $|a| = |b|$ slijedi da je $b = \pm a$, iz čega je očito da $a \mid b$ i $b \mid a$.

Ako $a \mid 1$, obzirom da $1 \mid a$, iz prethodne tvrdnje zaključujemo $|a| = 1$. □

Učenici 6. razreda osnovne škole susreću se sa sljedećim pravilima djeljivosti koje ćemo ukratko prokomentirati.

(i) Broj je djeljiv brojem 2 ako i samo ako mu je zadnja znamenka djeljiva s 2.
Neka je broj n dan kao

$$n = \overline{a_1a_2 \ldots a_{k-1}a_k} = a_1 \cdot 10^{k-1} + a_2 \cdot 10^{k-2} + \cdots + a_{k-1} \cdot 10^1 + a_k.$$

Ako je $k = 1$, tvrdnja je očigledna. Ako je $k \geq 2$, tada je

$$\begin{aligned} n &= 10 \cdot (a_1 \cdot 10^{k-2} + \cdots + a_{k-1}) + a_k \\ &= 2 \cdot 5 \cdot (a_1 \cdot 10^{k-2} + \cdots + a_{k-1}) + a_k, \end{aligned}$$

pa je prema teoremu 1.1.8, n djeljiv s 2 ako i samo ako je a_k djeljiv s 2.

(ii) Broj je djeljiv s 3 ako i samo ako mu je zbroj znamenaka djeljiv s 3.
Neka su $a_1, a_2, \ldots, a_{k-1}, a_k$ redom znamenke broja n,

$$n = \overline{a_1a_2 \cdots a_{k-1}a_k} = a_1 \cdot 10^{k-1} + a_2 \cdot 10^{k-2} + \cdots + a_{k-1} \cdot 10^1 + a_k.$$

Ova jednadžba ekvivalentna je sljedećoj:

$$n = a_1 \cdot (10^{k-1} - 1) + a_2 \cdot (10^{k-2} - 1) + \cdots + a_{k-1} \cdot (10 - 1) + (a_1 + a_2 + \cdots + a_{k-1} + a_k).$$

Svaki od izraza $10^{k-1}-1, 10^{k-2}-1, \cdots, 10-1$ djeljiv je sa $10-1=9$, pa i sa 3. Zato je n djeljiv s 3 ako i samo ako je $a_1+a_2+\cdots+a_{k-1}+a_k$ djeljiv s 3.

(iii) Broj je djeljiv s 4 ako i samo ako mu je dvoznamenkasti završetak djeljiv s 4.
Neka je

$$n=\overline{a_1a_2\ldots a_{k-1}a_k}=a_1\cdot 10^{k-1}+a_2\cdot 10^{k-2}+\cdots+a_{k-1}\cdot 10^1+a_k.$$

Ako je $k=1$ ili $k=2$, tvrdnja je očigledna. Ako je $k\geq 3$, tada je

$$\begin{aligned} n &= 100\cdot(a_1\cdot 10^{k-3}+\cdots+a_{k-2})+10\cdot a_{k-1}+a_k \\ &= 4\cdot 25\cdot(a_1\cdot 10^{k-3}+\cdots+a_{k-2})+\overline{a_{k-1}a_k}. \end{aligned}$$

Iz teorema 1.1.8 sada slijedi da je n djeljiv s 4 ako i samo ako je $\overline{a_{k-1}a_k}$ djeljiv s 4.

(iv) Broj je djeljiv s 5 ako i samo ako završava znamenkom 0 ili 5.
Neka je

$$n=\overline{a_1a_2\cdots a_k}=a_1\cdot 10^{k-1}+a_2\cdot 10^{k-2}+\cdots+a_{k-1}\cdot 10^1+a_k.$$

Ako je n djeljiv s 5, onda po teoremu 1.1.8 slijedi da je i $a_1\cdot 10^{k-1}+a_2\cdot 10^{k-2}+\cdots+a_{k-1}\cdot 10^1+a_k$ djeljivo s 5. Kako je $a_k\in\{0,1,2,\ldots,9\}$, broj n je djeljiv s 5 ako i samo ako je $a_k=0$ ili $a_k=5$.

(v) Broj je djeljiv sa 6 ako i samo ako je djeljiv i s 2 i s 3.
Ako je n djeljiv sa 6, tada postoji cijeli broj q takav da je

$$n=6q=2\cdot(3q)=3\cdot(2q),$$

pa je n djeljiv i s 2 i s 3.

Obratno, ako je n djeljiv i s 2 i s 3, tada postoje cijeli brojevi q_1 i q_2 takvi da je $n=2q_1=3q_2$. Tada je

$$n=6n-3n-2n=6n-3(2q_1)-2(3q_2)=6(n-q_1-q_2)$$

djeljiv sa 6.

(vi) Broj je djeljiv s 8 ako i samo ako mu je troznamenkasti završetak djeljiv s 8.
Neka je

$$n=\overline{a_1a_2\ldots a_{k-1}a_k}=a_1\cdot 10^{k-1}+a_2\cdot 10^{k-2}+\cdots+a_{k-2}\cdot 10^2+a_{k-1}\cdot 10^1+a_k.$$

Tvrdnja je očigledna za $k\leq 3$. Ako je $k\geq 4$, tada je

$$\begin{aligned} n &= 1000\cdot(a_1\cdot 10^{k-4}+\cdots+a_{k-3})+100\cdot a_{k-2}+10\cdot a_{k-1}+a_k \\ &= 8\cdot 125\cdot(a_1\cdot 10^{k-4}+\cdots+a_{k-3})+\overline{a_{k-2}a_{k-1}a_k}. \end{aligned}$$

Teorem 1.1.8 sada povlači da je n djeljiv s 8 ako i samo ako je $\overline{a_{k-2}a_{k-1}a_k}$ djeljiv s 8.

(vii) Broj je djeljiv s 9 ako i samo ako mu je zbroj znamenaka djeljiv s 9.
U dokazu djeljivosti brojem 3 iz jednakosti

$$n = a_1 \cdot (10^{k-1} - 1) + a_2 \cdot (10^{k-2} - 1) + \cdots + a_{k-1} \cdot (10 - 1) + (a_1 + a_2 + \cdots + a_{k-1} + a_k)$$

zaključujemo da je svaki od izraza $10^{k-1} - 1, 10^{k-2} - 1, \cdots, 10 - 1$ djeljiv s $10 - 1 = 9$, pa je n djeljiv s 9 ako i samo ako je $a_1 + \cdots + a_k$ djeljiv s 9, što je i trebalo dokazati.

(viii) Broj je djeljiv s 10 ako i samo ako završava znamenkom 0.
Neka je

$$\begin{aligned} n &= \overline{a_1 a_2 \cdots a_{k-1} a_k} = a_1 \cdot 10^{k-1} + a_2 \cdot 10^{k-2} + \cdots + a_{k-1} \cdot 10^1 + a_k \\ &= 10 \cdot (a_1 \cdot 10^{k-2} + \cdots + a_{k-1}) + a_k. \end{aligned}$$

Prema teoremu 1.1.8, n je djeljiv s 10 ako i samo ako je a_k djeljiv s 10. Kako je $a_k \in \{0, 1, 2, \ldots, 9\}$, to je a_k djeljiv s 10 ako i samo ako je $a_k = 0$.

1.2 Dijeljenje s ostatkom

U prethodnom potpoglavlju smo se bavili pitanjem djeljivosti brojeva. No, dva broja ne moraju nužno biti djeljiva, čime dobivamo ostatak.

Teorem 1.2.1 (Teorem o dijeljenju s ostatkom)**.** *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je $b = aq + r$, $0 \leq r < a$.*

Dokaz. Prvo dokažimo egzistenciju. Promotrimo skup $S = \{b - am : m \in \mathbb{Z}\}$. Označimo sa r najmanji nenegativni element skupa S. Tada je očito $r \geq 0$. Kako je $r \in S$, postoji cijeli broj q takav da je $b - aq = r$, odnosno $b = aq + r$. Kada bi vrijedilo $r \geq a$, onda bismo imali

$$b = aq + r \geq aq + a = a(q + 1),$$

pa je $b - a(q+1)$ nenegativan element skupa S i stoga $b - a(q+1) \geq r$. Slijedi $b - a(q+1) \geq b - aq$, pa je $a \leq 0$, što nije moguće jer je a prirodan broj. Dakle, $r < a$.

Sada dokažimo jedinstvenost. Pretpostavimo da postoji još jedan par q_1, r_1 koji zadovoljava iste uvjete. Želimo dokazati $r = r_1$. Pretpostavimo suprotno i bez smanjenja općenitosti uzmimo $r < r_1$. Tada je $0 < r_1 - r$. Kako su, po pretpostavci, $0 \leq r_1 < a$ i $0 \leq r < a$, onda je i $r_1 - r < a$. Dakle, $0 < r_1 - r < a$. Kako je $0 < r_1 - r = a(q - q_1)$, to je $q - q_1 > 0$, a kako je $q - q_1$ cijeli broj, to je $q - q_1 \geq 1$. Slijedi $r_1 - r = a(q - q_1) \geq a$, čime dolazimo do kontradikcije. Dakle, $r_1 = r$, pa je i $q_1 = q$, odnosno r i q su jedinstveni. □

Broj q nazivamo **nepotpun količnik**, a broj r **ostatak**. Ako je $r = 0$, onda je $b = aq$, odnosno b je djeljiv brojem a.

Korolar 1.2.2. *Za proizvoljne cijele brojeve a i b, $a \neq 0$, postoje jedinstveni cijeli brojevi q i r takvi da je $b = aq + r$ i $0 \leq r < |a|$.*

Dokaz. Ako je a pozitivan, to je tvrdnja teorema 1.2.1. Ako je a negativan, tada je $-a$ prirodan broj, pa teorem 1.2.1 povlači egzistenciju cijelih brojeva q_1 i r takvih da je $b = (-a) \cdot q_1 + r$, gdje je $0 \leq r < -a$. Stavimo li $q = -q_1$, tada je $b = aq + r$, gdje je $0 \leq r < |a|$. Jedinstvenost slijedi iz jedinstvenosti u teoremu 1.2.1. □

Teorem 1.2.1 podrazumijeva da je ostatak r pozitivan cijeli broj. No, postoji i jedinstven par q_1, r_1 takav da je ostatak r_1 negativan cijeli broj. Iz teorema o dijeljenju s ostatkom, za proizvoljne a i b, $a \in \mathbb{N}, b \in \mathbb{Z}$, postoje q i r iz $\mathbb{Z}$ takvi da vrijedi $b = aq + r,\ 0 < r < a$. Ova jednakost je ekvivalentna jednakosti $b = aq + a - a + r$, odnosno $b = a(q + 1) - a + r,$ a vrijedi $-a < -a + r < 0$. Definiramo li $q_1 = q + 1$ i $r_1 = -a + r$, dobivamo $b = aq_1 + r_1$, pri čemu su q_1 i r_1 cijeli brojevi i vrijedi $-a < r_1 < 0$. Jedinstvenost ovakvog prikaza slijedi iz jedinstvenosti prikaza iz teorema o dijeljenju s ostatkom.

Korolar 1.2.3. *Ako je r pozitivan, a r_1 negativan ostatak pri dijeljenju cijelog broja b prirodnim brojem a, onda je $|r| + |r_1| = a$.*

Iz ovog korolara se vidi da za barem jedan ostatak vrijedi $|r| \leq \frac{a}{2}$. Očito je da je $|r| = \frac{a}{2}$ ako i samo ako je $|r| = |r_1|$.

Teorem 1.2.4. *Neka je r ostatak pri dijeljenju cijelog broja b prirodnim brojem a te m cijeli broj. Tada je mr ostatak pri dijeljenju broja mb brojem ma.*

Dokaz. Pretpostavimo $b = aq+r$. Iz ove jednakosti se dobije $mb = maq+mr$. Ako je $r = 0$, onda je i $mr = 0$, pa je tvrdnja očita. Ako je $r \neq 0$, iz $0 < r < a$ slijedi i $0 < |mr| < |ma|$, pa zaključujemo da je mr ostatak. □

S obzirom da je m cijeli broj, mr može biti i pozitivan i negativan ostatak. Pozitivan je ako su m i r istog predznaka, a negativan ako su različitog.

1.3 Cijeli dio realnog broja

Prema teoremu o dijeljenju s ostatkom, za prirodan broj a i cijeli broj b postoje cijeli brojevi q i r takvi da je $b = aq + r$ i $0 \leq r < a$. Podijelimo li ovu jednakost prirodnim brojem a, dobijemo

$$\frac{b}{a} = q + \frac{r}{a}, \quad 0 \leq \frac{r}{a} < 1$$

i vidimo da je razlomak $\frac{b}{a}$ jednak zbroju cijelog broja q i broja $\frac{r}{a} \in [0, 1\rangle$. Uočimo da je q najveći cijeli broj koji nije veći od $\frac{b}{a}$ i označavamo ga sa $\left\lfloor \frac{b}{a} \right\rfloor$.

Teorem 1.3.1. *Za svaki realni broj x postoji jedinstven cijeli broj k takav da je $k \leq x < k+1$.*

Dokaz. Prvo dokažimo egzistenciju. Neka je $x \geq 0$ te skup $S = \{n \in \mathbb{N} : x < n\}$. Arhimedov aksiom (za $x, y \in \mathbb{R}, x > 0$ postoji $n \in \mathbb{N}$ takav da $nx > y$) povlači da postoji prirodan broj n takav da je $n \cdot 1 > y$. To znači da je skup S neprazan, pa postoji najmanji element tog skupa. Označimo ga sa m. Vrijedi $m \in S$, pa je $x < m$. Pretpostavimo da je i $m-1 \in S$. Kako je $m = \min S$, to je $m \leq m-1$, pa smo došli do kontradikcije. Iz $m-1 \notin S$ slijedi da je $x \geq m-1$, pa je $m-1 \leq x < m$. Dovoljno je staviti $k = m-1$ i dokazali smo egzistenciju cijelog broja k sa svojstvom $k \leq x < k+1$. Ako je $x < 0$, onda za $-x > 0$ postoji cijeli broj m takav da je $m \leq -x < m+1$, odnosno $-m \geq x > -m-1$. Ako je $-m > x > -m-1$, onda je dovoljno staviti $k = -m-1$, a za $x = -m$ stavimo $k = -m$.

Dokažimo sada jedinstvenost. Zbrajanjem $k \leq x < k+1$ i $-(l+1) < -x \leq -l$ dobije se $k-l-1 < 0 < k-l+1$. Slijedi $-1 < k-l < 1$. Kako je $k-l$ cijeli broj, to mora biti $k-l = 0$. □

Definicija 1.3.2. *Svaki realni broj x možemo zapisati u obliku $x = k + t$, gdje je k cijeli broj, a broj t iz intervala $[0, 1\rangle$. Broj k označavamo sa $\lfloor x \rfloor$ i zovemo* ***najveće cijelo od x****, a broj t nazivamo* ***razlomljenim dijelom od x*** *(ili decimalnim dijelom realnog broja x).*

Primjer 1.3.3. $\lfloor 2.15 \rfloor = 2$, $\lfloor -9.205 \rfloor = -10$.

Teorem 1.3.4. *Neka su x i y realni brojevi, a m cijeli broj. Vrijedi:*

(i) $\lfloor x + m \rfloor = \lfloor x \rfloor + m$;

(ii) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$;

(iii) $\left\lfloor \dfrac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \dfrac{x}{m} \right\rfloor$, $m \neq 0$.

Dokaz. Neka je $x = \lfloor x \rfloor + \theta$, $0 \leq \theta < 1$ i $y = \lfloor y \rfloor + \theta'$, $\quad 0 \leq \theta' < 1$.

(i) Kako je $x = \lfloor x \rfloor + \theta$, $0 \leq \theta < 1$, to je $x + m = \lfloor x \rfloor + m + \theta$, odnosno $\lfloor x + m \rfloor = \lfloor x \rfloor + m$, jer je $\lfloor x \rfloor + m$ cijeli broj. Time je tvrdnja (i) dokazana.

(ii) Koristeći početno zadane x i y i prethodnu tvrdnju, raspišimo izraz $\lfloor x + y \rfloor$:

$$\lfloor x + y \rfloor = \lfloor \lfloor x \rfloor + \lfloor y \rfloor + \theta + \theta' \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \theta + \theta' \rfloor, \quad 0 \leq \theta + \theta' < 2,$$

pa je $\lfloor \theta + \theta' \rfloor$ ili 0 ili 1. Dakle,

$$\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor \qquad \text{ili} \qquad \lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + 1,$$

iz čega slijedi

$$\lfloor x + y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1,$$

što je i trebalo dokazati.

(iii) Za cijele brojeve $\lfloor x \rfloor$ i $m \neq 0$ postoje cijeli brojevi q i r takvi da je $\lfloor x \rfloor = mq + r$, $0 \leq r < m$. Iz $x = \lfloor x \rfloor + \theta$ slijedi $\lfloor x \rfloor = x - \theta$, pa je $x = mq + r + \theta$, iz čega slijedi $\frac{x}{m} = q + \frac{r+\theta}{m}$. Iz uvjeta $0 \leq \theta < 1$ i $0 \leq r < m$ slijedi $0 \leq \frac{r+\theta}{m} < 1$. Zbog toga vrijedi $\left\lfloor \frac{x}{m} \right\rfloor = q$. No, iz $\lfloor x \rfloor = mq + r$ također slijedi $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = q$, pa zaključujemo $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$, čime smo dokazali tvrdnju (iii). □

Posljedica tvrdnje (iii) je da iz $\lfloor ax \rfloor = b$, $a, b \in \mathbb{Z}$, slijedi $\lfloor x \rfloor = \left\lfloor \frac{b}{a} \right\rfloor$. Nadalje, tvrdnja (ii) može se poopćiti na n realnih brojeva:

$$\lfloor x_1 \rfloor + \lfloor x_2 \rfloor + \cdots + \lfloor x_n \rfloor \leq \lfloor x_1 + x_2 + \cdots + x_n \rfloor \leq \lfloor x_1 \rfloor + \lfloor x_2 \rfloor + \cdots + \lfloor x_n \rfloor + n - 1,$$

što se dokazuje matematičkom indukcijom po n.

Sljedeći teoremi odnose se na višekratnike danog broja. Za cijeli broj c, **višekratnik** broja c je svaki broj oblika kc, gdje je k cijeli broj.

Teorem 1.3.5. *Ako je n prirodan broj i x nenegativan realan broj, onda ima* $\left\lfloor \frac{x}{n} \right\rfloor$ *prirodnih brojeva manjih od ili jednakih x i djeljivih sa n.*

Dokaz. Brojevi djeljivi sa n su njegovi višekratnici: $n, 2n, 3n, \ldots$. Neka je k broj prirodnih brojeva manjih od ili jednakih x i djeljivih sa n. Tada je $kn \leq x$. Kako je $k \leq x$, onda je $k + 1 > x$, pa je

$$kn \leq x < n(k+1),$$

odnosno

$$k \leq \frac{x}{n} < k + 1.$$

Iz definicije 1.3.2 slijedi $k = \left\lfloor \frac{x}{n} \right\rfloor$. □

Teorem 1.3.6. *Neka su a, b, c cijeli brojevi takvi da vrijedi* $a < b$ *i* $c > 0$*. Broj višekratnika kc broja c koji zadovoljavaju nejednakost* $a < kc \leq b$ *jednak je* $\left\lfloor \frac{b}{c} \right\rfloor - \left\lfloor \frac{a}{c} \right\rfloor$.

Dokaz. S obzirom da je $c > 0$ i $a < kc \leq b$, slijedi $\frac{a}{c} < k \leq \frac{b}{c}$. Očito je broj cijelih brojeva koji zadovoljavaju ovu nejednakost jednak $\left\lfloor \frac{b}{c} \right\rfloor - \left\lfloor \frac{a}{c} \right\rfloor$, pa je to i broj višekratnika broja c. Posebno, za $a = 0$, odnosno $b > 0$, broj višekratnika $kc \leq b$ jednak je $\left\lfloor \frac{b}{c} \right\rfloor$. □

Teorem 1.3.7. *Neka je p prost broj,* $n \in \mathbb{N}$ *i a najveći stupanj broja p takav da je* p^a *djelitelj broja n!. Tada je* $a = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$.

Dokaz. Zbroj $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots$ je konačan, jer za $m \geq \left\lfloor \frac{\log n}{\log p} \right\rfloor + 1$ vrijedi $\left\lfloor \frac{n}{p^m} \right\rfloor = 0$. Niz $1, 2, 3, \ldots, n$ sadrži $\left\lfloor \frac{n}{p} \right\rfloor$ brojeva djeljivih sa p. Iz toga slijedi:

$$n! = p \cdot 2p \cdot 3p \cdots \left\lfloor \frac{n}{p} \right\rfloor \cdot p \cdot m_1 = p^{\left\lfloor \frac{n}{p} \right\rfloor} \cdot \left\lfloor \frac{n}{p} \right\rfloor ! \cdot m_1,$$

pri čemu je m_1 prirodan broj koji nije djeljiv sa p. Promotrimo niz $1, 2, 3, \ldots, \left\lfloor \frac{n}{p} \right\rfloor$. Zbog $\left\lfloor \frac{\frac{n}{p}}{p} \right\rfloor = \left\lfloor \frac{n}{p^2} \right\rfloor$, imamo:

$$n! = p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor} \cdot \left\lfloor \frac{n}{p^2} \right\rfloor ! \cdot m_2,$$

gdje je m_2 prirodan broj koji nije djeljiv sa p. Nastavimo li postupak dobit ćemo $n! = p^a \cdot m$, pri čemu je m prirodan broj koji nije djeljiv sa p. □

1.4 Zadatci

Zadatak 1.4.1. *Dokažite da je za sve cijele brojeve $n \geq 0$ broj $11^{n+2} + 12^{2n+1}$ djeljiv sa 133:*

Rješenje. Zadani broj želimo broj prikazati u obliku zbroja brojeva tako da je svaki od pribrojnika djeljiv sa 133:

$$\begin{aligned} 11^{n+2} + 12^{2n+1} &= 121 \cdot 11^n + 12 \cdot 12^{2n} \\ &= (133 - 12) \cdot 11^n + 12 \cdot 12^{2n} \\ &= 133 \cdot 11^n - 12 \cdot 11^n + 12 \cdot 12^{2n} \\ &= 133 \cdot 11^n + 12 \cdot (144^n - 11^n). \end{aligned}$$

Prvi pribrojnik $(133 \cdot 11^n)$ je očito djeljiv sa 133. Dokažimo još da je i $12 \cdot (144^n - 11^n)$ djeljivo sa 133:

$$\begin{aligned} 144^n - 11^n &= (144 - 11) \cdot (144^{n-1} + 144^{n-2} \cdot 11 + \cdots + 144 \cdot 11^{n-2} + 11^{n-1}) \\ &= 133 \cdot (144^{n-1} + 144^{n-2} \cdot 11 + \cdots + 144 \cdot 11^{n-2} + 11^{n-1}). \end{aligned}$$

Vidimo da je i $12 \cdot (144^n - 11^n)$ djeljivo sa 133. Dakle, $11^{n+2} + 12^{2n+1}$ je djeljivo sa 133. □

Zadatak 1.4.2 (Školsko/gradsko natjecanje, 1. razred srednje škole, 2019.)**.** *Dokažite da je broj $6^{2n+2} - 2^{n+3} \cdot 3^{n+2} + 36$ djeljiv s 900 za sve prirodne brojeve n.*

Rješenje. Dani izraz napišimo kao umnožak dva prirodna broja:

$$\begin{aligned} 6^{2n+2} - 2^{n+3} \cdot 3^{n+2} + 36 &= 6^{2n} \cdot 36 - 2^n \cdot 8 \cdot 3^n \cdot 9 + 36 \\ &= 6^{2n} \cdot 36 - 6^n \cdot 72 + 36 \\ &= 36(6^{2n} - 2 \cdot 6^n + 1) \\ &= 36(6^n - 1)^2 \end{aligned}$$

Vidimo da je dobiveni izraz djeljiv sa 36. Broj $6^n - 1$ je djeljiv sa 5, za svaki prirodan broj n,a je $(6^n - 1)^2$ djeljiv sa 25. Zaključujemo da je cijeli izraz djeljiv sa $36 \cdot 25 = 900$. □

Zadatak 1.4.3. *Dokažite: ako je $n = \overline{a_1a_2a_3a_4a_5a_6}$ šesteroznamenkasti broj i ako je razlika $\overline{a_1a_2a_3} - \overline{a_4a_5a_6}$ djeljiva sa 7, onda je i n djeljiv sa 7.*

Rješenje. Označimo $n_1 = \overline{a_1a_2a_3}$ i $n_2 = \overline{a_4a_5a_6}$. Tada je $n = 1000n_1 + n_2$. Raspišimo n:

$$n = 1000n_1 + n_2 = 1001n_1 - n_1 + n_2 = 1001n_1 - (n_1 - n_2).$$

Iz pretpostavke je $n_1 - n_2$ djeljivo sa 7, ali i broj $1001 = 7 \cdot 143$ je djeljiv sa 7, pa zaključujemo da je n djeljiv sa 7. □

Zadatak 1.4.4. *Odredite zadnju znamenku broja 2^{50}.*

Rješenje. Da bismo odredili zadnju znamenku broja 2^{50}, promatrat ćemo ostatke pri dijeljenju brojem 10. Raspišimo neke potencije broja 2 i njihove ostatke pri dijeljenju s 10.

2^n	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9
ostatak	2	4	8	6	2	4	8	6	2

Iz tablice se vidi da se ostatci periodično ponavljaju, s periodom 4. Pri dijeljenju broja 50 sa 4 dobijemo ostatak 2, pa brojevi 2^{50} i 2^2 pri dijeljenju s 10 daju isti ostatak, a to je 4. Dakle, zadnja znamenka broja 2^{50} je 4. □

Zadatak 1.4.5. *Odredite zadnju znamenku broja 777^{777}.*

Rješenje. Broj 777^{777} može se zapisati na sljedeći način:

$$777^{777} = (770 + 7)^{777} = 10k + 7^{777}, \quad k \in \mathbb{Z}.$$

S obzirom da je $7^4 = 2401$, imamo: $7^{777} = (7^4)^{194} \cdot 7 = (2400 + 1)^{194} \cdot 7$. Očito je da je ovom broju zadnja znamenka 7, pa je i početnom broju zadnja znamenka 7. □

Zadatak 1.4.6. *Dokažite da je broj $n(2n + 1)(7n + 1)$ djeljiv sa 6 za svaki cijeli broj n.*

Rješenje. Imamo 3 faktora: $n, 2n+1$ i $7n+1$. Jedan od ova tri faktora će sigurno biti paran. Ako je n paran, preostala dva su neparna, a ako je n neparan, onda je faktor $7n+1$ paran. Dakle, umnožak je sigurno djeljiv brojem 2. Stoga je dovoljno dokazati da je umnožak djeljiv brojem 3. Za $n = 3k$ tvrdnja je očita. Uzmimo $n = 3k+1$. Sada je s 3 djeljiv faktor $2n+1$ jer je $2n+1 = 6k+3$, pa je i početni umnožak djeljiv s 3. Sada provjerimo još za $n = 3k+2$. Uvrstimo li ovaj n u faktore, vidjet ćemo da je sada $7n+1$ djeljiv s 3 jer je onda $7n+1 = 21k+15$. Ovime smo razmotrili sve slučajeve i zaključili da je umnožak djeljiv s 3. S obzirom da je umnožak djeljiv i s 2 i s 3, zaključujemo da je djeljiv i sa 6, što smo i trebali dokazati. □

Zadatak 1.4.7 (Županijsko natjecanje, 3. razred srednje škole, 2020.)**.** *Odredi sve uređene parove* (a, b) *prirodnih brojeva za koje je* $(a+b^2)(a^2+b)$ *potencija broja* 2*.*

Rješenje. Kako je umnožak $(a+b^2)(a^2+b)$ potencija broja 2, to su faktori $a+b^2$ i a^2+b potencije broja 2, pa su oba broja jednaka barem 2. Zbog toga postoje prirodni brojevi m i n takvi da je $a+b^2 = 2^m$ i $a^2+b = 2^n$. Kako je broj $a+b^2$ paran, to su a i b iste parnosti. Bez smanjenja općenitosti, pretpostavimo da je $a \leq b$, što znači da je $n \leq m$. Imamo:

$$2^n(2^{m-n}-1) = 2^m - 2^n = b^2 - a^2 - (b-a) = (b-a)(b+a-1).$$

Kako su a i b iste parnosti, onda je $b+a-1$ neparan. Tada 2^n dijeli $b-a$. Zbog $2^n = a^2+b$, a^2+b je djelitelj od $b-a$. Ako je $b-a > 0$, onda je $a^2+b \leq b-a$, što je kontradikcija. Dakle, $a = b$, što znači da je $a^2+a = a(a+1)$ potencija broja 2, pa su i a i $a+1$ potencije broja 2. To je moguće jedino ako jw $a = 1$. Dakle, jedino rješenje je $(a, b) = (1, 1)$. □

Zadatak 1.4.8 (Školsko/gradsko, 4. razred srednje škole, 2020.)**.** *Odredi zbroj svih prirodnih brojeva n manjih od* 1000 *za koje je* $2^n + 1$ *djeljiv s* 11*.*

Rješenje: Treba odrediti zbroj svih prirodnih brojeva $n < 1000$ takvih da broj 2^n pri dijeljenju s 11 daje ostatak 10. U tu svrhu promatrat ćemo ostatke koje brojevi 2^n daju pri dijeljenju s 11:

2^n	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
ostatak	2	4	8	5	10	9	7	3	6	1	2

Dakle, za $n = 10k+5 = 5(2k+1), k \geq 0, 2^n$ daje ostatak 10 pri dijeljenju s 11. Određujemo zbroj:

$$5 + 5\cdot 3 + 5\cdot 5 + \cdots + 5\cdot 197 + 5\cdot 199 = 5(1+3+5+\cdots+197+199) = 5\cdot 100^2 = 50000.$$

□

Poglavlje 2

Najveći zajednički djelitelj i najmanji zajednički višekratnik

2.1 Najveći zajednički djelitelj

U prethodnom poglavlju definirali smo pojam djeljivosti cijelih brojeva te dokazali neke rezultate vezane uz djeljivost. Sada ćemo se dotaći zajedničkih djelitelja dvaju ili više cijelih brojeva.

Definicija 2.1.1. *Neka su b i c cijeli brojevi. Cijeli broj a zovemo* ***zajedničkim djeliteljem*** *od b i c ako $a \mid b$ i $a \mid c$.*

Na osnovi teorema 1.1.9 zaključuje se da je skup svih djelitelja bilo kojeg cijelog broja, različitog od nule, konačan. Stoga, ako je bar jedan od cijelih brojeva b i c različit od nule, postoji samo konačno mnogo zajedničkih djelitelja od b i c. Najveći među njima zove se **najveći zajednički djelitelj** od b i c i označava se sa (b, c).

Primjer 2.1.2. *Djelitelji broja* 25 *su* ± 1*,* ± 5 *i* ± 25*, a djelitelji broja* 20 *su* ± 1*,* ± 2*,* ± 4*,* ± 5*,* ± 10 *i* ± 20*. Dakle, zajednički djelitelji brojeva* 25 *i* 20 *su* ± 1 *i* ± 5*, pa je najveći zajednički djelitelj* $(25, 20) = 5$.

Iz ovog primjera vidimo da najveći zajednički djelitelj brojeva 25 i 20 postoji i da je pozitivan. Uvjerimo se da je to uvijek tako.

Teorem 2.1.3. *Za svaki par cijelih brojeva a i b, od kojih je bar jedan različit od nule, postoji najveći zajednički djelitelj. Najveći zajednički djelitelj je pozitivan broj.*

Dokaz. Neka je $a \neq 0$ i d zajednički djelitelj. Iz definicije zajedničkog djelitelja slijedi da $d \mid a$ i $d \mid b$, pa je $d \leq |a|$ (po teoremu 1.1.9). Dakle, skup zajedničkih djelitelja je ograničen

odozgo, pa najveći zajednički djelitelj postoji. S obzirom da i $1 \mid a$ i $1 \mid b$ zaključujemo da je najveći zajednički djelitelj uvijek pozitivan broj. □

Osim što je najveći zajednički djelitelj uvijek pozitivan broj, vrijedi i sljedeće svojstvo.

Teorem 2.1.4. *Neka su b i c cijeli brojevi. Vrijedi:* $(b, c) = min(\{bx + cy : x, y \in \mathbb{Z}\} \cap \mathbb{N})$.

Dokaz. Neka je $g = (b, c)$ i l najmanji pozitivan član skupa $S = \{bx + cy : x, y \in \mathbb{Z}\}$. To znači da postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $l = bx_0 + cy_0$. Želimo dokazati da $l \mid b$ i $l \mid c$. Pretpostavimo da $l \nmid b$. Tada po teoremu o dijeljenju s ostatkom postoje $q, r \in \mathbb{Z}$ takvi da je

$$b = lq + r, \quad 0 < r < l.$$

Kako je $l = bx_0 + cy_0$, imamo

$$r = b - lq = b - q(bx_0 + cy_0) = b(1 - qx_0) + c(-qy_0) \in S\,,$$

pa l nije najmanji pozitivni član skupa S. Dakle, $l \mid b$. Analogno se dokazuje da $l \mid c$. Zaključujemo da je $l \leq g$. S obzirom da je $g = (b, c)$, onda postoje $u, v \in \mathbb{Z}$ takvi da je $b = gv$, $c = gu$. Iz toga slijedi da je $l = gvx_0 + guy_0 = g(vx_0 + uy_0)$. Zaključujemo da je $g \leq l$. Dakle, $g = l$, čime smo dokazali tvrdnju. □

Najveći zajednički djelitelj je jednoznačno određen jer je i najveći element nekog skupa jednoznačno određen. U teoremu 1.1.3 dokazano je da brojevi b i $-b$ imaju iste djelitelje. Zbog toga vrijedi: $(a, b) = (a, -b) = (-a, b) = (-a, -b)$, odnosno $(a, b) = (|a|, |b|)$. Iz definicije direktno slijedi: $(a, -a) = |a|, (a, \pm 1) = 1$ i $(0, a) = |a|$. Dogovorno uzimamo $(0, 0) = 0$. Intuitivno se pitamo postoje li cijeli brojevi a i b takvi da je barem jedan od njih različit od nule i da vrijedi $(a, b) = 1$. Zato slijedi definicija.

Definicija 2.1.5. *Kažemo da je prirodan broj p* ***prost*** *ako vrijedi:*

(i) $p > 1$,

(ii) ima točno dva djelitelja: 1 *i p.*

Prirodan broj veći od 1, koji nije prost, nazivamo ***složen***.

Definicija 2.1.6. *Cijeli brojevi a i b za koje je* $(a, b) = 1$ *nazivaju se* ***relativno prostim*** *brojevima.*

Primjer 2.1.7. *Djelitelji broja* 20 *su* ± 1, ± 2, ± 4, ± 5, ± 10 *i* ± 20, *a djelitelji broja* 9 *su* ± 1, ± 3 *i* ± 9. *Očito su im jedini zajednički djelitelji* ± 1, *pa slijedi da je* $(20, 9) = 1$. *Dakle, brojevi* 20 *i* 9 *su relativno prosti.*

Primjer 2.1.8. *Djelitelji broja* 8 *su* ± 1, ± 2, ± 4 *i* ± 8, *a djelitelji broja* 24 *su* ± 1, ± 2, ± 3, ± 4, ± 6, ± 8, ± 12 *i* ± 24. *Vidimo da je 24 djeljivo s 8 i da se njihovi zajednički djelitelji podudaraju sa svim djeliteljima broja* 8.

Od sada pa nadalje ćemo, proučavajući (a, b), uvijek pretpostavljati da je bar jedan od brojeva a i b različit od nule. Dokažimo sada da ako $b \mid a$, $a, b \in \mathbb{Z}$, onda je $(a, b) = |b|$, kao što smo vidjeli u primjeru 2.1.8.

Teorem 2.1.9. *Ako $b \mid a$, zajednički djelitelji brojeva a i b i djelitelji broja b se podudaraju i $(a, b) = |b|$.*

Dokaz. S obzirom da $b \mid a$, svaki zajednički djelitelj brojeva a i b je djelitelj i samog broja b. Ako cijeli broj d, $d \neq 0$, dijeli b, iz $b \mid a$ slijedi i da $d \mid a$. Dakle, svaki djelitelj od b je zajednički djelitelj od a i b, odnosno svi zajednički djelitelji brojeva a i b se podudaraju s djeliteljima broja b. Kako je najveći djelitelj od b broj $|b|$, slijedi da je $(a, b) = |b|$. □

Neposredna posljedica ovog teorema je: ako je $(a, b) = 1$, za $|a|, |b| \neq 1$, onda $a \nmid b$ niti $b \nmid a$.

Tražimo li zajedničke djelitelje, po definiciji se podrazumijeva da govorimo o dijeljenju bez ostatka. No, iako djelitelja ne možemo naći ako brojevi nisu djeljivi, možemo naći vezu djelitelja i ostatka. O tome govori sljedeći teorem.

Teorem 2.1.10. *Neka su a, b, c i q cijeli brojevi i $a = bq + c$. Zajednički djelitelji brojeva a i b podudaraju se sa zajedničkim djeliteljima brojeva b i c. Vrijedi:* $(a, b) = (b, c)$.

Dokaz. Iz $a = bq + c$ slijedi da je $c = a - bq$. S obzirom da je $c = a - bq$, iz teorema 1.1.8 slijedi da je svaki djelitelj brojeva a i b također djelitelj broja c. Zaključujemo da je svaki zajednički djelitelj od a i b također zajednički djelitelj od b i c.

Iz $a = bq + c$ slijedi obratno, tj. da je svaki zajednički djelitelj brojeva b i c djelitelj i od a i b.

Dakle, djelitelji od a i b podudaraju se s djeliteljima od b i c, odnosno $(a, b) = (b, c)$. □

Ilustrirajmo ovaj teorem na konkretnom primjeru.

Primjer 2.1.11. *Vrijedi:* $42 = 9 \cdot 4 + 6$. *Zajednički djelitelji od $a = 42$ i $b = 9$ su* ± 1 *i* ± 3. *Zajednički djelitelji od $b = 9$ i $c = 6$ su* ± 1 *i* ± 3. *Očito se zajednički djelitelji podudaraju i vrijedi* $(a, b) = (b, c)$.

Primijetimo da su u prethodnom primjeru zajednički djelitelji brojeva 42 i 9 brojevi ± 1 i $\pm$ 3 te $(42, 9) = 3$, ali djelitelji broja 3 su također $\pm$ 1 i $\pm$ 3. Stoga se iz primjera može zaključiti da su zajednički djelitelji brojeva 42 i 9 jednaki djeliteljima njihovog najvećeg zajedničkog djelitelja, odnosno broja 3. Vrijedi sljedeći teorem.

Teorem 2.1.12. *Zajednički djelitelji brojeva a i b podudaraju se s djeliteljima njihovog najvećeg zajedničkog djelitelja. Kraće zapisujemo: $d \mid a$ i $d \mid b$ ako i samo ako $d \mid (a, b)$.*

Dokaz. Pretpostavimo $b \neq 0$. Prema korolaru 1.2.2 postoje $q_1, r_1 \in \mathbb{Z}$ takvi da je

$$a = bq_1 + r_1, \quad 0 \leq r_1 < |b|.$$

Ako je $r_1 = 0$, onda je, po teoremu 2.1.9, očito $(a, b) = |b|$ i $|b| \mid (a, b)$. Neka je $r_1 \neq 0$. Tada za brojeve b i r_1 postoje $q_2, r_2 \in \mathbb{Z}$ takvi da je

$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

Ako je $r_2 = 0$, onda je $(b, r_1) = r_1$, pa iz $a = bq_1 + r_1, 0 \leq r_1 < b$, zbog teorema 2.1.10, slijedi $(a, b) = (b, r_1)$. Dakle, $(a, b) = r_1$. Iz istog teorema i prethodnog zaključka slijedi da svaki zajednički djelitelj brojeva a i b dijeli njihov najveći zajednički djelitelj. Ako je $r_2 \neq 0$, postoje $q_3, r_3 \in \mathbb{Z}$ takvi da je

$$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2.$$

Ako je $r_3 \neq 0$ nastavljamo isti postupak. Time dobivamo jednakost:

$$r_{k-2} = r_{k-1} q_k + r_k, \quad 0 \leq r_k < r_{k-1}.$$

Niz $|b|, r_1, r_2, \ldots, r_k, \ldots$ je padajući niz cijelih brojeva koji je ograničen odozdo (nulom), pa je konačan. Posljednji pozitivan član ovog niza, r_n, će ujedno biti i najmanji pozitivan broj u tom nizu. Vrijedi:

$$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1}.$$

No, i za r_{n-1} i r_n postoje $q_{n+1}, r_{n+1} \in \mathbb{Z}$ takvi da je

$$r_{n-1} = r_n q_{n+1} + r_{n+1}, \quad 0 \leq r_{n+1} < r_n.$$

Kako je r_n najmanji pozitivan broj u nizu $|b|, r_1, r_2, \ldots, r_k, \ldots$, slijedi da je $r_{n+1} = 0$. Iz toga je $r_{n-1} = r_n q_{n+1}$. Iz dobivenih jednakosti, počevši od $a = bq_1 + r_1$ do $r_{n-1} = r_n q_{n+1}$ zaključuje se da parovi brojeva a i b, b i r_1, r_1 i r_2, $\ldots$, r_{n-2} i r_{n-1}, r_{n-1} i r_n imaju iste zajedničke djelitelje. Slijedi: $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n$, odnosno $(a, b) = r_n$. Dakle, svaki zajednički djelitelj od a i b je djelitelj i od $(a, b) = r_n$. S obzirom da $(a, b) \mid a$ i $(a, b) \mid b$, svaki djelitelj od (a, b) je djelitelj i od a i od b. Zaključujemo da se zajednički djelitelji od a i b podudaraju s djeliteljima od (a, b). □

U dokazu ovog teorema je zapravo opisan Euklidov algoritam, o čemu ćemo više u sljedećem potpoglavlju. Koristeći navedeni teorem dokazuje se sljedeći.

Teorem 2.1.13. *Neka su a, b cijeli brojevi. Tada je $(ma, mb) = |m|(a, b)$ za svaki cijeli broj m.*

Dokaz. Pretpostavimo $mb \neq 0$. Kao u dokazu prethodnog teorema imamo:

$$\begin{aligned} ma &= mbq_1 + mr_1, \\ mb &= mr_1q_2 + mr_2, \\ mr_1 &= mr_2q_3 + mr_3, \\ &\vdots \\ mr_{n-2} &= mr_{n-1}q_n + mr_n, \\ mr_{n-1} &= mr_nq_{n+1}. \end{aligned}$$

Prema teoremu 2.1.10 je $(ma, mb) = (mb, mr_1) = \cdots = (mr_{n-1}, mr_n)$, a iz teorema 2.1.9 proizlazi $(mr_{n-1}, mr_n) = |mr_n| = |m|r_n$. Kako je $r_n = (a, b)$, dobijemo $(ma, mb) = |m|(a, b)$. Za $mb = 0$ tvrdnja je očita. □

Primjer 2.1.14. *Neka je $a = 64, b = 40$ i $m = 3$. Tada je $(a, b) = (64, 40) = 8, (ma, mb) = (192, 120) = 24$, a $|m| \cdot (a, b) = 3 \cdot 8 = 24$.*

Teorem 2.1.15. *Neka su a i b cijeli brojevi. Ako je d cijeli broj takav da $d \mid a$ i $d \mid b$, onda je $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{|d|}$. Nadalje, brojevi $\frac{a}{(a,b)}$ i $\frac{b}{(a,b)}$ su relativno prosti.*

Dokaz. Iz prethodnog teorema imamo:

$$|d|\left(\tfrac{a}{d}, \tfrac{b}{d}\right) = \left(d \cdot \tfrac{a}{d}, d \cdot \tfrac{b}{d}\right) = (a, b).$$

Druga tvrdnja teorema dobije se za $d = (a, b)$. □

Sljedeći rezultati se odnose na relativno proste brojeve.

Teorem 2.1.16. *Neka su a, b i c cijeli brojevi. Ako je $(a, b) = 1$, onda je $(ac, b) = (c, b)$.*

Dokaz. Kako $(c, b) \mid c$, to $(c, b) \mid ac$, a kako $(c, b) \mid b$, teorem 2.1.12 povlači $(c, b) \mid (ac, b)$.

S druge strane, $(ac, b) \mid ac$ i $(ac, b) \mid bc$, pa iz teorema 2.1.12 slijedi $(ac, b) \mid (ac, bc)$. Prema teoremu 2.1.13, $(ac, bc) = |c|(a, b) = |c|$, pa $(ac, b) \mid c$. Osim toga, $(ac, b) \mid b$, pa teorem 2.1.12 povlači $(ac, b) \mid (c, b)$. Iz teorema 1.1.10 konačno slijedi $(ac, b) = (c, b)$. □

Iz ovog teorema slijedi i sljedeći rezultat.

Korolar 2.1.17. *Ako je $(a, b) = 1$ i $b \mid ac$, onda $b \mid c$.*

Dokaz. Prema prethodnom teoremu, $(ac, b) = (c, b)$. Kako, iz pretpostavke, vrijedi da $b \mid ac$, onda je $(ac, b) = |b|$, prema teoremu 2.1.9. Tada je i $(c, b) = |b|$, iz čega slijedi $b \mid c$, što je i trebalo dokazati. □

Primjer 2.1.18. *Uzmimo brojeve a, b i $c \in \mathbb{Z}$ takve da su a i c te b i c relativno prosti. Neka su to brojevi: $a = 4, b = 8$ i $c = 9$. Dakle, $(a, c) = (4, 9) = 1$ i $(b, c) = (8, 9) = 1$. Promotrimo umnožak $ab = 4 \cdot 8 = 32$. Vidimo da je $(ab, c) = (32, 9) = 1$.*

Da rezultat navedenog primjera nije slučajnost, dokazat ćemo sljedećim teoremom.

Teorem 2.1.19. *Ako je $(a, m) = (b, m) = 1$, onda je $(ab, m) = 1$.*

Dokaz. Iz teorema 2.1.4 proizlazi da postoje $x_0, y_0, x_1, y_1 \in \mathbb{Z}$ takvi da je

$$1 = ax_0 + my_0 = bx_1 + my_1.$$

Sređujući dobivamo:

$$ax_0 \cdot bx_1 = (1 - my_0)(1 - my_1).$$

Označimo sa $y_2 = y_0 + y_1 - my_0y_1$, pa je

$$ax_0 \cdot bx_1 = 1 - my_0 - my_1 + m^2y_0y_1 = 1 - my_2.$$

Tada je $ax_0 \cdot bx_1 + my_2 = 1$, pa je $(ab, m) = 1$, što je i trebalo dokazati. □

Ako je $(a, b) = 1$ i $d \mid a$, onda je $(d, b) = 1$ jer tada d i b ne mogu imati zajedničkih djelitelja. Također, $(a, b) = 1$ ako i samo ako je $(a^m, b^n) = 1, m, n \in \mathbb{Z}$. Uistinu, ako je $(a, b) = 1$, onda je i $(a \cdot a \cdots a, b \cdot b \cdots b) = 1$, i obratno.

U prvom poglavlju navedena su neka svojstva djeljivosti brojeva. Između ostalih, i za broj 6: broj je djeljiv s 6 ako i samo ako je djeljiv i s 2 i s 3. Primijetimo da su brojevi 2 i 3 relativno prosti.

Primjer 2.1.20. *Provjerimo vrijedi li navedeno svojstvo i za neke druge brojeve. Uzmimo broj* 765 *i provjerimo je li djeljiv brojem* 45 *te vrijedi li da je djeljiv s* 9 *i* 5*. Broj* 765 *je djeljiv s* 45 *jer je* $765 : 45 = 17$*, djeljiv je s* 5 *jer mu je zadnja znamenka* 5 *i djeljiv je s* 9 *jer mu je zbroj znamenaka* $(7 + 6 + 5 = 18)$ *djeljiv s* 9*. Obratno, uzmimo neki broj koji je djeljiv s* 9 *i* 5*, npr.* 405*. Ovaj broj je djeljiv s* 45 *jer je* $405 : 45 = 9$*. Možemo iz ovog primjera naslutiti da je broj djeljiv s* 45 *ako i samo ako je djeljiv i s* 9 *i s* 5*.*

Sljedeći teorem opravdava primjer.

Teorem 2.1.21. *Neka je $(a, b) = 1$. Skup svih djelitelja broja ab podudara se sa skupom $\{dd' : d \mid a,\ d' \mid b\}$. Ako je broj djelitelja od a jednak n_1, od b jednak n_2 i od ab jednak n_3, onda je $n_3 = n_1n_2$.*

Dokaz. Prvo dokazujemo da je svaki djelitelj od ab jednak umnošku djelitelja od a i b, a zatim obrnuto, da je umnožak dva proizvoljna djelitelja od a i b djelitelj od ab. Neka $d'' \mid ab$ i $(d'', a) = d$. Tada vrijedi da $\frac{d''}{d} \mid \frac{a}{d} \cdot b$ i da je $\left(\frac{d''}{d}, \frac{a}{d}\right) = 1$. Zatim iz korolara 2.1.17 slijedi da $\frac{d''}{d} \mid b$. Označimo sada $d' = \frac{d''}{d}$. Onda je $d'' = d \cdot d'$, pri čemu je d djelitelj od a, a d' djelitelj od b. Obrnuto, ako $d \mid a$ i $d' \mid b$, onda po teoremu 1.1.6 slijedi da $dd' \mid ab$.

Druga tvrdnja teorema slijedi iz činjenice da su skupovi $\{d : d \mid a\}$ i $\{d' : d' \mid b\}$ disjunktni jer je $(a, b) = 1$. □

Ovaj teorem se može i poopćiti i to na sljedeći način. Neka je $(a_i, a_j) = 1$, $i, j = 1, 2, \ldots, m, i \neq j$. Djelitelji broja $a_1 a_2 \cdots a_m$ podudaraju se s sa skupom $\{d_1 d_2 \cdots d_m : d_1 \mid a_1, d_2 \mid a_2, \ldots, d_m \mid a_m\}$. Ako je n_i broj djelitelja broja $a_i, i = 1, 2, \ldots$, onda je broj djelitelja broja $a_1 a_2 \cdots a_m$ jednak $n = n_1 n_2 \cdots n_m$. Ovo poopćenje dokazujemo matematičkom indukcijom.

Sljedeća propozicija će nam biti potrebna za dokazivanje Euklidovog algoritma.

Propozicija 2.1.22. *Neka su a, b i x cijeli brojevi. Vrijedi:* $(a, b) = (a, b + ax)$.

Dokaz. Označimo $d = (a, b), g = (a, b + ax)$. Iz teorema 2.1.4 slijedi da postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je

$$d = ax_0 + by_0,$$

odnosno

$$d = a(x_0 - xy_0) + (b + ax)y_0.$$

Sada je očito da $g \mid d$. Dokažimo da i $d \mid g$. S obzirom da $d \mid a$ i $d \mid b$, onda i $d \mid (b + ax)$. Dakle, d je zajednički djelitelj od a i $b + ax$. Sada iz teorema 2.1.12 možemo zaključiti da $d \mid g$. Dokazano je da $g \mid d$ i $d \mid g$, a brojevi d i g su pozitivni po definiciji, pa zaključujemo da je $d = g$. □

2.2 Euklidov algoritam

Teorem 2.2.1 (Euklidov algoritam)**.** *Neka su b i c* > 0 *cijeli brojevi. Pretpostavimo da je uzastopnom primjenom teorema o dijeljenju s ostatkom dobiven sljedeći niz jednakosti:*

$$\begin{aligned}
b &= cq_1 + r_1, \quad 0 < r_1 < c, \\
c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\vdots \\
r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\
r_{j-1} &= r_j q_j + 1.
\end{aligned}$$

Tada je (b, c) jednak r_j (posljednjem ostatku različitom od 0). Vrijednosti od x_0 i y_0 u $(b, c) = bx_0 + cy_0$ dobiju se izražavanjem svakog ostatka r_i kao linearne kombinacije b i c.

Dokaz. Koristeći propoziciju 2.1.22 imamo:

$$(b, c) = (b - cq_1, c) = (r_1, c) = (r_1, c - r_1q_2) = (r_1, r_2) = (r_1 - r_2q_3, r_2) = (r_3, r_2).$$

Nastavljajući ovaj postupak dobivamo: $(b, c) = (r_{j-1}, r_j) = (r_j, 0) = r_j$. Sada ćemo još dokazati da je svaki r_i linearna kombinacija od b i c, koristeći indukciju. Očito je tvrdnja točna za r_1 i r_2. Stoga, pretpostavimo da vrijedi za r_{i-1} i r_{i-2}. Kako je r_i linearna kombinacija od r_{i-1} i r_{i-2}, po pretpostavci indukcije slijedi da je i linearna kombinacija od b i c. □

Primjer 2.2.2. *Odredimo najveći zajednički djelitelj brojeva* 2574 *i* 1080 *te ga prikažimo kao linearnu kombinaciju početnih brojeva.*

$$\begin{aligned}
2574 &= 1080 \cdot 2 + 414,\\
1080 &= 414 \cdot 2 + 252,\\
414 &= 252 \cdot 1 + 162,\\
252 &= 162 \cdot 1 + 90,\\
162 &= 90 \cdot 1 + 72,\\
90 &= 72 \cdot 1 + 18,\\
72 &= 72 \cdot 4.
\end{aligned}$$

Dakle, $(2574, 1080) = 18$. *Sada prikažimo* 18 *kao linearnu kombinaciju brojeva* 2574 *i* 1080.

$$\begin{aligned}
18 &= 90 - 72 \cdot 1 = 90 - (162 - 90 \cdot 1)\\
&= 90 \cdot 2 - 162 = (252 - 162 \cdot 1) \cdot 2 - 162\\
&= 252 \cdot 2 - 162 \cdot 3 = 252 \cdot 2 - (414 - 252 \cdot 1) \cdot 3\\
&= 252 \cdot 5 - 414 \cdot 3 = (1080 - 414 \cdot 2) \cdot 5 - 414 \cdot 3\\
&= 1080 \cdot 5 - 414 \cdot 13 = 1080 \cdot 5 - (2574 - 1080 \cdot 2) \cdot 13\\
&= 1080 \cdot 31 - 2574 \cdot 13.
\end{aligned}$$

Euklidov algoritam ima istu primjenu i ako uzimamo negativne ostatke. No, uz to možemo promatrati i najmanji apsolutni ostatak. Pokažimo to sljedećim primjerom, koristeći iste početne brojeve kao i u prethodnom primjeru.

Primjer 2.2.3.

$$\begin{aligned} 2574 &= 1080 \cdot 3 - 666, \\ 1080 &= 666 \cdot 2 - 252, \\ 666 &= 252 \cdot 3 - 90, \\ 252 &= 90 \cdot 3 - 18, \\ 90 &= 18 \cdot 5. \end{aligned}$$

Dakle, $(2574, 1080) = 18$.

Primjer 2.2.4.

$$\begin{aligned} 2574 &= 1080 \cdot 2 + 414, \\ 1080 &= 414 \cdot 3 - 162, \\ 414 &= 162 \cdot 2 + 90, \\ 162 &= 90 \cdot 2 - 18, \\ 90 &= 18 \cdot 5. \end{aligned}$$

Dakle, kao i u prethodnim primjerima, $(2574, 1080) = 18$.

Vidimo da smo u oba primjera dobili isti najveći zajednički djelitelj. O tome govori sljedeći teorem.

Teorem 2.2.5. *Ako su $r_{n'}$ i $r_{n''}$ posljednji ostatci dobiveni u dva različita Euklidova algoritma, onda je $|r_{n'}| = |r_{n''}|$.*

Euklidov algoritam je postupak koji nema unaprijed strogo određen broj koraka dok ne dođemo do najvećeg zajedničkog djelitelja. To ovisi o brojevima koji su zadani na početku.

Teorem 2.2.6. *Za broj koraka j u Euklidovom algoritmu vrijedi $j < 2\log_2 c$.*

Dokaz. Promotrimo $i-$ti korak. Vrijedi da je $r_i \leq \frac{r_{i-1}}{2}$ ili $\frac{r_{i-1}}{2} < r_i < r_{i-1}$. Ako je $\frac{r_{i-1}}{2} < r_i < r_{i-1}$, onda imamo $q_{i+1} = 1$ i $r_{i+1} = r_{i-1} - r_i < \frac{r_{i-1}}{2}$. Vidimo da je u svakom slučaju $r_{i+1} < \frac{r_{i-1}}{2}$. Iz toga slijedi:

$$\begin{cases} 1 \leq r_j < \frac{r_{j-2}}{2} < \frac{r_{j-4}}{2} < \cdots < \frac{r_0}{2^{\frac{j}{2}}} \text{ ako je } j \text{ paran}, \\ 2 \leq r_{j-1} < \frac{r_{j-3}}{2} < \frac{r_{j-5}}{2} < \cdots < \frac{r_0}{2^{\frac{j-1}{2}}} \text{ ako je } j \text{ neparan}. \end{cases}$$

Dakle, u oba slučaja je $c = r_0 > 2^{\frac{j}{2}}$. Iz toga slijedi da je $j < \log_2 c$, što je i trebalo dokazati. □

U primjerima u kojima smo određivali najveći zajednički djelitelj brojeva 2574 i 1080 dobili smo broj 18. Vidimo da je broj koraka u svakom od ta tri primjera manji od $2\log_2 1080$.

2.3 Najmanji zajednički višekratnik

Definicija 2.3.1. *Neka su a i b cijeli brojevi različiti od nule. Svaki cijeli broj koji je višekratnik brojeva a i b naziva se njihovim* ***zajedničkim višekratnikom****. Najmanji pozitivan broj koji je zajednički višekratnik brojeva a i b naziva se* ***najmanji zajednički višekratnik*** *brojeva a i b i označava se* $[a, b]$.

Primjer 2.3.2. *Zajednički višekratnici brojeva* 6 *i* 8 *su* 24, 48, 72, ... *Dakle,* $[6, 8] = 24$.

Teorem 2.3.3. *Za svaka dva cijela broja a i b, $a, b \neq 0$, postoji najmanji zajednički višekratnik.*

Dokaz. Neka su a i b cijeli brojevi, različiti od nule. S obzirom da $a \mid |ab|$ i $b \mid |ab|$, postoji barem jedan zajednički višekratnik brojeva a i b i to je broj $|ab|$. Kako je najmanji zajednički višekratnik po definiciji pozitivan broj, uvijek će postojati najmanji zajednički višekratnik $[a, b] \geq |ab|$. □

Ako je c višekratnik broja a, onda je također i višekratnik broja $-a$. Iz toga slijedi:

$$[a, b] = [-a, b] = [a, -b] = [|a|, |b|].$$

Nadalje, $[a, a] = |a|$ te $[a, 1] = |a|$.

U definiciji zajedničkog višekratnika ne spominje se jesu li brojevi a i b djeljivi. Sljedeći teorem obuhvaća i takav slučaj.

Teorem 2.3.4. *Ako $a \mid b$, zajednički višekratnici brojeva a i b podudaraju se s višekratnicima broja b i vrijedi:* $[a, b] = |b|$.

Dokaz. Neka je c višekratnik od b. Kako $a \mid b$, onda je c višekratnik i od a. Time dobivamo da je c zajednički višekratnik od a i b. Dakle, zajednički višekratnici od a i b su isti kao i zajednički višekratnici od b.

Ako $a \mid b$, onda vrijedi i $a \mid |b|$. No, vrijedi i $b \mid |b|$, pa je $|b|$ zajednički višekratnik od a i b, odnosno $[a, b] \leq |b|$. S druge strane, iz prethodno dokazanog slijedi da $b \mid [a, b]$, pa je $|b| \leq [a, b]$. Slijedi, $[a, b] = |b|$. □

Primjer 2.3.5. *Dani su brojevi* 36 *i* 72. *Zajednički višekratnici ovih brojeva su* 72, 144, ... *Višekratnici broja* 72 *su također* 72, 144, . . . , *pa vidimo da su zajednički višekratnici brojeva* 36 *i* 72 *isti kao i višekratnici broja* 72. *Dakle,* $[36, 72] = 72$.

Sljedeći teorem dokazuje opću tvrdnju pokazanu primjerom 2.3.5.

Teorem 2.3.6. *Zajednički višekratnici brojeva a i b podudaraju se s višekratnicima najmanjeg zajedničkog višekratnika od a i b. Vrijedi:* $(a, b) \cdot [a, b] = |ab|$.

Dokaz. Neka je c zajednički višekratnik brojeva a i b, odnosno $a \mid c$ i $b \mid c$. Tada postoji cijeli broj k takav da $c = ak$. Kako $b \mid c$, vrijedi i da $b \mid ak$. Također, $\frac{b}{d} \mid \frac{a}{d}k$, gdje je $d = (a, b)$. Zbog teorema 2.1.15 vrijedi $\left(\frac{b}{d}, \frac{a}{d}\right) = 1$, pa iz korolara 2.1.17 slijedi $\frac{b}{d} \mid k$. Tada postoji cijeli broj t takav da je $k = \frac{b}{d}t$. Uvrstimo li ovaj izraz u $c = ak$ imamo $c = \frac{ab}{d}t$. To znači da su zajednički višekratnici dani izrazom:

$$c = \frac{ab}{d}t, \qquad t = 0, \pm 1, \pm 2, \pm 3, \ldots,$$

odnosno

$$c = \frac{|ab|}{d}t, \qquad t = 0, \pm 1, \pm 2, \pm 3, \ldots.$$

Najmanji pozitivan broj c dobije se za $t = 1$: $c = \frac{|ab|}{d}$ i time je dobiven najmanji zajednički višekratnik $[a, b]$ brojeva a i b. Dakle, $[a, b] = \frac{|ab|}{(a,b)}$, odnosno $(a, b)[a, b] = |ab|$. Ovime je dokazan drugi dio teorema.

Uvrstimo li dobivene rezultate prethodnog dijela dokaza u $c = \frac{|ab|}{d}t$, dobijemo $c = [a, b] \cdot t, \quad t = 0, \pm 1, \pm 2, \pm 3, \ldots$ Vidimo da je svaki zajednički višekratnik brojeva a i b ujedno i višekratnik njihovog najmanjeg zajedničkog višekratnika $[a, b]$, što je i trebalo dokazati. □

Primjer 2.3.7. *Najmanji zajednički višekratnik brojeva* 10 *i* 15 *je* 30*. Brojevi* 10 *i* 15 *imaju zajedničkog djelitelja, broj* 5*. Najmanji zajednički višekratnik brojeva* 2 *i* 3 *je* 6*. Brojeve* 2 *i* 3 *smo dobili dijeljenjem brojeva* 10 *i* 15 *zajedničkim djeliteljem, a onda je i broj* 30 *podijeljen istim tim djeliteljem. Odnosno,* $[10, 15] = 5 \cdot [2, 3] = 5 \cdot 6 = 30$*.*

Sljedećim teoremom dokazat će se tvrdnja ilustrirana prethodnim primjerom.

Teorem 2.3.8. *Za cijele brojeve* a, b *i* m*,* $abm \neq 0$*, vrijedi:* $[ma, mb] = |m|[a, b]$.

Dokaz. Iz teorema 2.3.6 slijedi:

$$[ma, mb] = \frac{|ma \cdot mb|}{(ma, mb)} = \frac{m^2|ab|}{|m|(a, b)} = |m|[a, b].$$

□

Teorem 2.3.9. *Ako* $m \mid a$ *i* $m \mid b$ *onda je* $\left[\frac{a}{m}, \frac{b}{m}\right] = \frac{[a,b]}{|m|}$.

Dokaz. Imamo:

$$[a, b] = \left[m \cdot \frac{a}{m}, m \cdot \frac{b}{m}\right] = |m|\left[\frac{a}{m}, \frac{b}{m}\right],$$

pa je

$$\left[\frac{a}{m}, \frac{b}{m}\right] = \frac{[a,b]}{|m|}.$$

□

Najveći zajednički djelitelj i najmanji zajednički višekratnik imaju svojstva koja su korisna prilikom vršenja računskih operacija s njima. Ta svojstva su im zajednička.

Teorem 2.3.10. *Za prirodne brojeve a, b, c i m vrijedi:*

(i) zakon idempotencije: $(a,a) = a,\ [a,a] = a$;

(ii) zakon komutacije: $(a,b) = (b,a),\ [a,b] = [b,a]$;

(iii) zakon asocijacije: $((a,b),c) = (a,(b,c)),\ [[a,b],c] = [a,[b,c]]$;

(iv) zakon distribucije: $m(a,b) = (ma,mb),\ m[a,b] = [ma,mb],\ \frac{(a,b)}{m} = \left(\frac{a}{m}, \frac{b}{m}\right),\ \frac{[a,b]}{m} = \left[\frac{a}{m}, \frac{b}{m}\right]$.

2.4 Zadatci

Zadatak 2.4.1 (Školsko/gradsko natjecanje, 2. razred srednje škole, 2020.)**.** *Odredite najveći prirodni broj n takav da* $n + 10$ *dijeli* $n^3 + 100$.

Rješenje. Kako je $n^3 + 1000$ zbroj kubova, to je $n^3 + 1000 = (n + 10)(n^2 - 10n + 100)$, tj. $\frac{n^3+1000}{n+10} = n^2 - 10n + 100$. Raspišimo početni uvjet zadataka i iskoristimo prethodni raspis. Imamo:

$$\frac{n^3 + 100}{n + 10} = \frac{n^3 + 1000 - 900}{n + 10} = n^2 - 10n + 100 - \frac{900}{n + 10}.$$

Ako je $n+10$ djelitelj od n^3+100, mora biti i djelitelj od 900. Najveći djelitelj od 900 je broj 900, pa je najveći mogući prirodni broj koji zadovoljava tvrdnju zadatka $n = 900 - 10 = 890$. □

Zadatak 2.4.2 (Školsko/gradsko natjecanje, 3. razred srednje škole, 2020.)**.** *Za prirodni broj* $n \geq 2$ *neka je* $D(n)$ *najveći prirodni djelitelj broja n različit od n. Na primjer,* $D(12) = 6$ *i* $D(13) = 1$. *Odredite najveći prirodni broj n takav da je* $D(n) = 35$.

Rješenje. Neka je $P(n)$ najmanji prirodni djelitelj od n različit od 1. Tada, po teoremu 2.3.6,vrijedi $n = P(n) \cdot D(n) = 35P(n)$. S obzirom da je 35 djelitelj od n i 5 jedan od prostih faktora broja n, onda je $P(n)$ manji od ili jednak 5, tj. 2, 3 ili 5. Najveći n dobivamo za $P(n) = 5$, tj. za $n = 35 \cdot 5$ i to je $n = 175$. □

Zadatak 2.4.3 (Školsko/gradsko natjecanje, 4. razred srednje škole, 2020.)**.** *Odredite sve prirodne brojeve n koji imaju točno* 12 *pozitivnih djelitelja* $1 = d_1 < d_2 < \cdots < d_{12} = n$ *za koje vrijedi* $d_4 = 5$ *i* $d_5^2 + 1 = d_7$.

Rješenje. Iz $d_4 = 5$ slijedi da točno jedan od brojeva $1, 2, 3, 4$ i 5 nije djelitelj broja 5. Brojevi 1 i 5 jesu djelitelji broja n. Kada broj 2 ne bi bio djelitelj broja n, onda to ne bi mogao biti ni broj 4. To znači da je i broj 2 djelitelj broja n. Promotrimo dvije mogućnosti.

Prva mogućnost je: $d_1 = 1, d_2 = 2, d_3 = 3$ i $d_4 = 5$. Očto je da je tada i 6 djelitelj broja n, pa je $d_5 = 6$. Uvjet $d_5^2 + 1 = d_7$ povlači da je $d_7 = 37$. Vidimo da n ima 4 različita prosta faktora. To znači da ima barem 16 djelitelja, što nam ne odgovara uvjetima zadatka.

Druga mogućnost je: $d_1 = 1, d_2 = 2, d_3 = 4$ i $d_4 = 5$. Tada je i broj 10 djelitelj broja n, pa je $d_5 \leq 10$. Kako 3 nije djelitelj od n, to d_5 nije ni 6 niti 9. Ako je $d_5 = 7$, onda je $d_7 = 50$, pa između d_5 i d_7 imamo više od jednog djelitelja (npr. 10 i 259), što je nemoguće: između d_5 i d_7 trebamo imati samo jednog djelitelja, a imamo i djelitelje 8,10, itd. Ako je $d_5 = 8$, onda je $d_7 = 65$, pa analogno dolazimo do kontradikcije. Ako je $d_5 = 10$, onda je $d_7 = 101$, što je prost broj. Kako je n djeljiv sa 4 i 5, onda je $d_6 = 20$. Djelitelje broja n promatrat ćemo kao umnožak jednak n, tj. $d_i \cdot d_{13-i} = n$, za $i \in \{1, 2, \ldots, 12\}$. Iz ovoga slijedi da je $d_6 \cdot d_7 = 2020$, pa provjeravamo ispunjava li $n = 2020$ uvjete zadatka. Ispišimo sve djelitelje broja 2020:

$$1, 2, 4, 5, 10, 20, 101, 202, 404, 505, 1010, 2020.$$

Dakle, $n = 2020$. □

Zadatak 2.4.4 (Županijsko natjecanje, 2. razred srednje škole, 2020.)**.** *Odredite sve uređene parove* (a, b) *prirodnih brojeva takve da je* $[a, b] - (a, b) = \frac{ab}{5}$.

Rješenje. Označimo $m = [a, b]$ i $n = (a, b)$. Po teoremu 2.3.6 vrijedi da je $mn = ab$. Imamo: $m - n = \frac{mn}{5}$, odnosno $5m - 5n = mn$. Nadalje, $25 + 5m - 5n - mn = 25$, iz čega slijedi $(5 + m)(5 - n) = 25$. Djelitelji broja 25 su $\pm 1, \pm 5, \pm 25$. Kako je m najmanji zajednički višekratnik, vrijedi $m > 0$, pa je $5 + m > 5$. Jedina mogućnost je $5 + m = 25$, tj. $m = 20$. Tada je $5 - n = 1$, odnosno $n = 4$. Dakle, $[a, b] = 20$ i $(a, b) = 4$. Očito je da su a i b nužno djeljivi s 4 te $ab = mn = 80$. Ako stavimo $a = 4k$ i $b = 4l$, tada je $kl = 5$, pa je $k = 1$, $l = 5$ ili $k = 5$, $l = 1$. Dakle, jedina moguća rješenja su $a = 4$, $b = 20$ ili $a = 20$, $b = 4$. □

Zadatak 2.4.5 (Državno natjecanje, 2. razred srednje škole, 2019.)**.** *Odredite sve parove* (m, n) *cijelih brojeva za koje vrijedi* $m^2 = n^5 + n^4 + 1$*, a broj* $m - 7n$ *dijeli* $m - 4n$.

Rješenje. Sredimo izraz $m^2 = n^5 + n^4 + 1$:

$$m^2 = n^5 + n^4 + 1 = (n^3 - n + 1)(n^2 + n + 1).$$

Odredimo najveći zajednički djelitelj izraza u zagradama:

$$\begin{aligned}
(n^3 - n + 1, n^2 + n + 1) &= (n^3 - n + 1 - n(n^2 + n + 1), n^2 + n + 1) \\
&= (-n^2 - 2n + 1, n^2 + n + 1) \\
&= (-n^2 - 2n + 1 + (n^2 + n + 1), n^2 + n + 1) \\
&= (-n + 2, n^2 + n + 1) \\
&= (-n + 2, n^2 + n + 1 + n(-n + 2)) \\
&= (-n + 2, 3n + 1) \\
&= (-n + 2, 3n + 1 + 3(-n + 2)) \\
&= (-n + 2, 7).
\end{aligned}$$

Najveći zajednički djelitelj brojeva je 1 ili 7.

Ako je najveći zajednički djelitelj 7, onda iz $m^2 = (n^3 - n + 1)(n^2 + n + 1)$ slijedi da je i m djeljiv sa 7, a iz $(-n + 2, 7)$ zaključujemo da n daje ostatak 2 pri dijeljenju sa 7, pa n nije djeljiv sa 7. Iz uvjeta zadatka imamo:

$$\frac{m - 4n}{m - 7n} = 1 + \frac{3n}{m - 7n},$$

što mora biti cijeli broj. Tada $m - 7n$ dijeli $3n$, što nije moguće jer je $m - 7n$ djeljiv sa 7, a $3n$ nije. Zaključujemo da u ovom slučaju nema rješenja.

Ako je najveći zajednički djelitelj jednak 1, onda imamo $m^2 = (n^3 - n + 1)(n^2 + n + 1)$ kao faktorizaciju potpunog kvadrata m^2 na relativno proste faktore $n^3 - n + 1$ i $n^2 + n + 1$. Kako su relativno prosti, svaki od njih je kvadrat cijelog broja. Ispitajmo kada je $n^2 + n + 1$ kvadrat cijelog broja. To će vrijediti za $n = 0$ i $n = -1$. Za sve prirodne brojeve vijedi $n^2 < n^2 + n + 1 < (n + 1)^2$, a za $n < -1$ je $(n + 1)^2 < n^2 + n + 1 < n^2$, pa su $n = 0$ i $n = -1$ jedine mogućnosti. Za $n = -1$ imamo $m^2 = 1$, odnosno $m = 1$ ili $m = -1$. No, i za $m = 1$ i $m = -1$ vrijedi da $m - 7n$ ne dijeli $m - 4n$, pa to rješenje odbacujemo. Za $n = 0$ imamo također $m = 1$ ili $m = -1$. Za oba m i $n = 0$ vrijedi da $m - 7n$ dijeli $m - 4n$. Dakle, konačna rješenja su parovi $(m, n) = (-1, 0), (m, n) = (1, 0)$. □

Poglavlje 3

Linearne diofantske jednadžbe

Linearna jednadžba s dvije nepoznanice, $ax + by = c$, u kojoj je $ab \neq 0$, ima beskonačno mnogo rješenja i naziva se **neodređenom linearnom jednadžbom**.

3.1 Linearne diofantske jednadžbe

Definicija 3.1.1. *Linearna neodređena jednadžba $ax+by = c$, s cjelobrojnim koeficijentima a, b i c i cjelobrojnim rješenjima naziva se **diofantska linearna jednadžba**. Diofantsku jednadžbu oblika $ax + by = c$ nazivamo **nehomogenom**, a jednadžba oblika $ax + by = 0$ je **pripadna homogena jednadžba**.*

Intuitivno se pitamo imaju li diofantske jednadžbe uvijek rješenja. Ilustrirat ćemo primjere takvih situacija.

Primjer 3.1.2. *Promotrimo jednadžbu $2x + 5y = 4$. Neka od cjelobrojnih rješenja su uređeni parovi $(-3, 2), (2, 0), (7, -2)$. Vidimo da rješenje diofantske jednadžbe nije nužno jedinstveno.*

Primjer 3.1.3. *Promotrimo jednadžbu $4x + 2y = 7$. Ova jednadžba je ekvivalentna jednadžbi $2(2x + y) = 7$. Vidimo da je lijeva strana jednakosti paran broj, pa je očito da ova jednadžba nema cjelobrojnih rješenja jer paran broj pomnožen bilo kojim cijelim brojem ne može biti jednak 7.*

Vidimo da diofantske jednadžbe nemaju uvijek nužno rješenja. O tome govori sljedeći teorem.

Teorem 3.1.4. *Da bi neodređena jednadžba $ax + by = c$ s cjelobrojnim koeficijentima a, b i c, $ab \neq 0$, imala cjelobrojna rješenja, nužno je i dovoljno da $(a, b) \mid c$.*

Dokaz. Dokažimo nužnost. Neka je (x_0, y_0) jedan od parova cjelobrojnih rješenja jednadžbe $ax + by = c$. Tada vrijedi: $ax_0 + by_0 = c$. Po definiciji najvećeg zajedničkog djelitelja vrijedi da $(a, b) \mid a$ i $(a, b) \mid b$. Tada iz teorema 1.1.8 slijedi da $(a, b) \mid ax_0 + by_0$, odnosno $(a, b) \mid c$.

Dokažimo dovoljnost. Pretpostavimo da $(a, b) \mid c$. Iz teorema 1.1.8 slijedi da postoje cijeli brojevi m i n takvi da je $am + bn = (a, b)$. Pomnožimo cijelu jednadžbu sa $\frac{c}{(a,b)}$ i imamo:

$$a\frac{c}{(a,b)}m + b\frac{c}{(a,b)}n = c.$$

Sada je očito da je jedno rješenje $x_0 = \frac{c}{(a,b)}m,\ y_0 = \frac{c}{(a,b)}n$. □

Primjer 3.1.5. *Zadana je jednadžba* $312x - 280y = 120$. *Odredimo najveći zajednički djelitelj brojeva* 312 *i* -280 *koristeći Euklidov algoritam.*

$$\begin{aligned} 312 &= -280 \cdot (-1) + 32, \\ -280 &= 32 \cdot (-9) + 8, \\ 32 &= 8 \cdot 4. \end{aligned}$$

Dakle, $(312, -280) = 8$. *Kako je* 120 *djeljivo sa* 8*, to postoje cjelobrojna rješenja jednadžbe. Prikažimo sada broj* 8 *kao linearnu kombinaciju brojeva* 312 *i* -280. *No, zbog* $c = 120$ *imamo:*

$$\begin{aligned} 120 &= 15 \cdot 8 = 15 \cdot (-280 - 32 \cdot (-9)) \\ &= 15 \cdot (-280 - (312 + 280 \cdot (-1)) \cdot (-9)) \\ &= 15 \cdot (-280 - 312 \cdot (-9) - 280 \cdot 9) \\ &= 15 \cdot (-280 \cdot 10 + 312 \cdot 9) \\ &= 312 \cdot 135 - 280 \cdot 150. \end{aligned}$$

Dakle, jedno cjelobrojno rješenje je par $x = 135, y = 150$.

Primjer 3.1.6. *Jednadžbe* $xy + 5y - 4y = 20$ *ili* $x^2 - xy + 4x - 4y + 6 = 0$ *su nelinearne diofantske jednadžbe.*

3.2 Metode rješavanja diofantskih jednadžbi

Diofantske jednadžbe nemaju jedinstven način rješavanja, no postoje metode koje nam olakšavaju rješavanje. Neke od metoda su: metoda umnoška, metoda količnika, metoda posljednje znamenke, metoda parnosti, metoda nejednakosti i metoda zbroja kvadrata.

Metodu umnoška primjenjujemo za rješavanje nelinearnih diofantskih jednadžbi. Cilj je zadanu jednadžbu svesti na oblik u kojem je jedna strana jednadžbe umnožak (s nepoznanicama), a druga strana cijeli broj. Zatim razmatramo sve moguće slučajeve za dobivene faktore.

Primjer 3.2.1. *Riješimo jednadžbu* $x^2 - 2xy = 5$ *metodom umnoška. Faktorizacijom dobivamo:*

$$\begin{aligned} x^2 - 2xy &= 5, \\ x(x-2y) &= 5. \end{aligned}$$

Moguće kombinacije rješenja svrstat ćemo u tablicu.

x	$x-2y$	y
1	5	-2
5	1	2
-1	-5	2
-5	-1	-2

Dakle, parovi rješenja su: $(1,-2), (5,2), (-1,2)$ *i* $(-5,-2)$.

Metodom količnika jednadžbu svodimo na oblik u kojem jednu jednadžbu izrazimo kao racionalnu funkciju pomoću druge nepoznanice, a zatim izdvajamo sve moguće slučajeve.

Primjer 3.2.2. *Riješimo jednadžbu* $xy + 4x = 9$ *metodom količnika.*

$$\begin{aligned} xy + 4x &= 9, \\ xy &= -4x + 9, \\ y &= -4 + \frac{9}{x}. \end{aligned}$$

Sve mogućnosti rješenja prikazane su u tablici.

x	$9/x$	y
1	9	5
3	3	-1
9	1	-3
-1	-9	-13
-3	-3	-7
-9	-1	-5

Dakle, parovi rješenja su: $(1,5), (3,-1), (9,-3), (-1,-13), (-3,-7)$ *i* $(-9,-5)$.

Metodom posljednje znamenke određujemo ima li jednadžba cjelobrojno rješenje tako da odredimo posljednje znamenke na lijevoj i desnoj strani jednakosti.

Primjer 3.2.3. *Jednadžba* $20x + 10y + 30z = 153$ *nema cjelobrojnih rješenja. Brojevi* $20x$, $10y$ *i* $30z$ *su djeljivi brojem* 10*, pa im je zadnja znamenka* 0*. Iz toga slijedi i da njihov zbroj ima zadnju znamenku* 0*. S druge strane, broj* 153 *završava znamenkom* 3*, stoga slijedi da jednadžba nema cjelobrojnih rješenja.*

Određujemo li u jednadžbi parnost jedne od nepoznanica koristimo metodu parnosti. Na temelju parnosti možemo zaključiti ima li jednadžba cjelobrojno rješenje ili ne.

Primjer 3.2.4. *Jednadžba* $x^2 + 12y = 1901$ *nema cjelobrojnih rješenja. Promotrimo parnost nepoznanice* x*. Ako je* x *paran, njegov kvadrat je također paran, pa je lijeva strana jednakosti parna, što ne može biti jednako* 1901*. Uzmimo da je* x *neparan. Tada je oblika* $x = 2k + 1,\ k \in \mathbb{Z}$*. Imamo:*

$$\begin{aligned}
(2k+1)^2 + 12y &= 1901,\\
4k^2 + 4k + 1 + 12y &= 1901,\\
4k^2 + 4k + 12y &= 1900,\\
4(k^2 + k + 4y) &= 1900,\\
k^2 + k + 4y &= 475,\\
k(k+1) + 4y &= 475.
\end{aligned}$$

Umnožak $k(k+1)$ *je paran, jer je to umnožak dva uzastopna cijela broja. Očito je i* $4y$ *paran broj. Iz toga slijedi da je lijeva strana jednakosti parna, a zbroj dva parna cijela broja ne može biti neparan. Dakle, ova jednadžba nema cjelobrojnih rješenja.*

Metoda zbroja kvadrata svodi se na određivanje kvadrata brojeva koji u zbroju daju cijeli broj na drugoj strani jednadžbe.

Primjer 3.2.5. *Ispišimo sva rješenja jednadžbe* $x^2 + y^2 = 2$*.*

x^2	y^2	x	y
1	1	1	1
1	1	−1	1
1	1	1	−1
1	1	−1	−1

Dakle, ova jednadžba ima četiri moguća rješenja: $(1,1), (-1,1), (1,1)$ *i* $(-1,-1)$*.*

Metoda nejednakosti često se kombinira s drugim metodama rješavanja diofantskih jednadžbi. Koristi se kako bi se smanjio skup mogućih rješenja jednadžbe. Nakon toga se raspisuju slučajevi.

Primjer 3.2.6. *Koristeći metodu nejednakosti riješimo jednadžbu $a + b + c = abc$ u skupu prirodnih brojeva. Neka je, bez smanjenja općenitosti, $a \geq b \geq c$. Tada je $a + b + c \leq 3a$. Iz $a + b + c = abc$ slijedi $bc \leq 3$. Razlikujemo slučajeve i uvrstimo dobivene vrijednosti u početnu jednadžbu.*

(I) $b = 1$, $c = 1$, *slijedi* $2 = 0$, *što je kontradikcija.*

(II) $b = 2$, $c = 1$, *slijedi* $a = 3$. *Kako je* $3 \geq 2 \geq 1$, *jedno rješenje je uređeni par* $(3, 1, 2)$.

(III) $b = 3$, $c = 1$, *slijedi* $a = 2$, *što je kontradikcija jer ne vrijedi* $2 \geq 3$.

Dakle, jedino moguće rješenje je uređeni par $(3, 1, 2)$.

3.3 Zadatci

Zadatak 3.3.1 (Školsko natjecanje, 1. razred srednje škole, 2019.)**.** *Odredi sve parove* (m, n) *cijelih brojeva za koje vrijedi* $mn + 5m + 2n = 121$.

Rješenje. Sredimo početnu jednadžbu.

$$\begin{aligned} mn + 5m + 2n &= 121, \\ mn + 5m + 2n + 10 &= 131, \\ m(n + 5) + 2(n + 5) &= 131, \\ (n + 5)(m + 2) &= 131. \end{aligned}$$

Kako je 131 prost broj, njegovi djelitelji su $\pm 1, \pm 131$. Neka je $n + 5 = \dfrac{131}{m + 2}$. Raspišimo sve mogućnosti.

$m + 2$	m	$n + 5$	n
1	-1	131	126
131	129	1	-4
-1	-3	-131	-136
-131	-133	-1	-6

Dakle, rješenja su $(m, n) = (-1, 126), (129, -4), (-3, -136), (-133, -6)$. □

Zadatak 3.3.2 (Županijsko natjecanje, 8. razred, 2002.)**.** *Na koliko načina se može točno izvagati glavicu kupusa mase* 1.67 *kg ako na raspolaganju ima samo utege masa* 20 *g i* 50 *g?*

Rješenje. Označimo sa x broj utega mase 20 g, a sa y broj utega mase 50 g. Vrijedi: $20x + 50y = 1670$, odnosno $2x + 5y = 167$. Imamo sada da je $2x = 2(83 - 2y) + 1 - y$. Lijeva strana jednakosti je paran broj. Da bi jednakost vrijedila, broj $1 - y$ također mora biti paran. Ako je $1 - y$ paran, onda je $1 - y = 2k, k \in \mathbb{Z}$, pa je $y = 1 - 2k$. Početna jednakost sada glasi: $2x = 2(81 + 5k)$, odnosno $x = 81 + 5k$. Kako je x broj utega, mora vrijediti $x \geq 0$, pa je $k \geq -16$. Analogno, $y \geq 0$ i $k \leq 0$. Dakle, imamo 17 mogućnosti za vrijednost broja k. Drugim riječima, za ovo vaganje postoji 17 načina. Zapišimo sva moguća rješenja u tablicu.

20g	50g
1	33
6	31
11	29
16	27
21	25
26	23
31	21
36	19
41	17
46	15
51	13
56	11
61	9
66	7
71	5
76	3
81	1

□

Zadatak 3.3.3 (Županijsko natjecanje, 8. razred, 2012.)**.** *Riješite jednadžbu* $x^2 - xy - 2y^2 = 27$ *u skupu cijelih brojeva.*

Rješenje. Ovaj zadatak riješit ćemo metodom umnoška. Sredimo početnu jednadžbu.

$$\begin{aligned} x^2 - xy - 2y^2 &= 27, \\ x^2 + xy - 2xy - 2y^2 &= 27, \\ x(x + y) - 2y(x + y) &= 27, \\ (x + y)(x - 2y) &= 27. \end{aligned}$$

Zapišimo sve moguće slučajeve u tablicu.

$x+y$	$x-2y$	x	y
1	27	29/3	−26/3
3	9	5	−2
9	3	7	2
27	1	55/3	26/3
−1	−27	−29/3	26/3
−3	−9	−5	2
−9	−3	−7	−2
−27	−1	−55/3	−26/3

Vidimo da su jedina moguća rješenja uređeni parovi $(5,-2),(7,2),(-5,2)$ i $(-7,-2)$. □

Zadatak 3.3.4 (Županijsko natjecanje, 1. razred srednje škole, 2001.)**.** *Postoji li cijeli broj x za koji su brojevi $\frac{14x+5}{9}$ i $\frac{17x-5}{12}$ cijeli?*

Rješenje. Treba pronaći cijeli broj x takav da je $14x+5$ djeljiv sa 9 i $17x-5$ djeljiv s 12. Sredimo početne izraze:

$$\frac{14x+5}{9} = x + \frac{5x+5}{9} = x + 5\cdot\frac{x+1}{9},$$
$$\frac{17x-5}{12} = x + \frac{5x-5}{12} = x + 5\cdot\frac{x-1}{12}.$$

Da bi oba broja bila cijela, $x+1$ mora biti djeljiv sa 9, a $x-1$ mora biti djeljiv sa 12. Kada bi to vrijedilo, tada bi i $x+1$ i $x-1$ bili djeljivi s 3, što je nemoguće zato što im je razlika 2. Dakle, takav x ne postoji. □

Zadatak 3.3.5 (Državno natjecanje, 7. razred, 1998.)**.** *U vagonu se nalazi* 1 *tona krumpira kojeg treba pretovariti u kamion. Posao obavlja jedan radnik, kojem su na raspolaganju vreće od* 60 *kg i* 80 *kg , a odjednom može prenijeti samo jednu punu vreću krumpira. Koliko kojih vreća radnik mora upotrijebiti ako posao želi obaviti s najmanjim brojem prenošenja? Prenose se samo do kraja napunjene vreće i sav krumpir mora biti pretovaren.*

Rješenje. Označimo sa x broj vreća od 60 kg, a sa y broj vreća od 80 kg. Tada je $60x+80y = 1000$, odnosno $3x+4y = 50$. Broj $2y$ i zbroj 50 djeljivi su sa 2, pa i $3x$ mora biti djeljiv sa 2. To je moguće ako je $x = 2k$, $k \in \mathbb{N}$. Sada imamo jednakost $6k+4y = 50$, tj. $3k+2y = 25$. Izrazimo y: $y = \frac{25-3k}{2} = 12-2k+\frac{1+k}{2}$. Očito je da $1+k$ mora biti paran, pa je $1+k = 2l$, $l \in \mathbb{N}$. Slijedi da je $y = 14-3l$. Kako je $y \geq 0$, to je $l \leq 4$. Ispunimo tablicu s mogućim vrijednostima.

l	1	2	3	4
x	2	6	10	14
y	11	8	5	2

Najmanji mogući zbroj $x+y$ je za $x = 2$ i $y = 11$. Dakle, posao će biti obavljen s najmanjim brojem prenošenja ako radnik prenese 2 vreće po 60 kg i 11 vreća po 80 kg. □

Zadatak 3.3.6 (Državno natjecanje, 8. razred, 1998.)**.** *Koliko ima uređenih parova troznamenkastih brojeva* (x, y) *koji su rješenja jednadžbe* $3x + 4y = 1998$.

Rješenje. Pribrojnik $4y$ je djeljiv sa 2, a zbroj mora biti 1998, pa onda i $3x$ nužno mora biti djeljiv sa 2. Neka je tada $x = 2k$, $k \in \mathbb{N}$. Početna jednadžba sada ima oblik $6k + 4y = 1998$, odnosno $3k + 2y = 999$, Analogno zaključujemo, $2y$ mora biti djeljiv sa 3, pa je $y = 3l$, $l \in \mathbb{N}$. Dakle, $3k + 6l = 999$, tj. $k + 2l = 333$. Kako su traženi brojevi troznamenkasti, to vrijedi da je $100 \leq x \leq 999$ i $100 \leq y \leq 999$. Iz dobivenih rezultata slijedi da je $k \geq 50$ i $33 \leq l \leq 141$. Zbog toga je broj uređenih parova $141 - 50 = 108$. □

Zadatak 3.3.7 (Državno natjecanje, 1. razred srednje škole, 1998.)**.** *Nađite sve prirodne brojeve* m *i* n *koji zadovoljavaju jednadžbu* $10(m + n) = mn$.

Rješenje. Sredimo dobivenu jednadžbu tako da na lijevoj strani jednakosti imamo umnožak, a na desnoj prirodan broj.

$$\begin{aligned} 10(m+n) &= mn, \\ 10m + 10n - mn &= 0, \\ mn - 10m - 10n + 100 &= 100, \\ m(n-10) - 10(n-10) &= 100, \\ (n-10)(m-10) &= 100. \end{aligned}$$

Prikažimo u tablici sve mogućnosti.

$n-10$	$m-10$	n	m
1	100	11	110
2	50	12	60
4	25	14	35
5	20	15	30
10	10	20	20
20	5	30	15
25	4	35	14
50	2	60	12
100	1	110	11

Dakle, rješenja su uređeni parovi (m, n): $(110, 11)$, $(60, 12)$, $(35, 14)$, $(30, 15)$, $(20, 20)$, $(15, 30)$, $(14, 35)$, $(12, 60)$ i $(11, 110)$. □

Poglavlje 4

Prosti djelitelji

4.1 Prosti brojevi

Broj 1 nije ni prost niti složen. Prosti brojevi mogu se naći koristeći algoritam *Eratostenovo sito*. To je algoritam kojim se konstruiraju prosti brojevi izbacivanjem višekratnika prostih brojeva. Prvih deset prostih brojeva su: $2, 3, 5, 7, 11, 13, 17, 19, 23$ i 29.

Teorem 4.1.1. *Neka je $n > 1$ prirodan broj. Najmanji njegov djelitelj, veći od 1, je prost broj.*

Dokaz. Broj pozitivnih djelitelja je konačan, pa postoji najmanji djelitelj $a > 1$ broja n. Ako je a složen broj, onda postoji djelitelj $b > 1$ broja a. Kako $b \mid a$ i $a \mid n$, po teoremu 1.1.5 slijedi da $b \mid n$, pa a nije najmanji djelitelj od n. Dakle, a je prost broj. □

Posljedica ovog teorema je da je svaki prirodan broj veći od 1 djeljiv barem jednim prostim brojem, a nekad to može biti i sam taj broj.

Teorem 4.1.2. *Prostih brojeva ima beskonačno mnogo.*

Dokaz. Neka je p prost broj. Broj $p! + 1$ nije djeljiv niti jednim prirodnim brojem $k, 2 \leq k \leq p$. Prethodni teorem tada povlači da postoji prost djelitelj q broja $p! + 1$ koji je veći od p. Tako zaključujemo da od svakog prostog broja postoji veći prost broj. Zaključujemo da ne postoji najveći prost broj, odnosno da prostih brojeva ima beskonačno mnogo. □

Teorem 4.1.3. *Za prost broj p i cijeli broj a vrijedi: $(p, a) = 1$ ili $(p, a) = p$.*

Dokaz. Po definiciji prostih brojeva, jedini djelitelji broja p su 1 i p. Ako $p \mid a$, tada po teoremu 2.1.9 vrijedi da je $(p, a) = p$. Ako $p \nmid a$, tada je jedini zajednički djelitelj od p i a jednak 1, $(p, a) = 1$. □

Ako su brojevi p i q prosti, tada je očito da im je jedini zajednički djelitelj 1, odnosno da su relativno prosti.

Teorem 4.1.4. *Neka je p prost broj te a i b cijeli brojevi. Ako $p \mid ab$, onda $p \mid a$ ili $p \mid b$.*

Dokaz. Pretpostavimo da $p \nmid a$. Tada po prethodnom teoremu slijedi da je $(p, a) = 1$. Iz korolara 2.1.17 sada imamo da $p \mid b$. □

Teorem 4.1.5. *Neka su $p, p_1, p_2, \ldots, p_n$ prosti brojevi. Ako $p \mid p_1 p_2 \cdots p_n$, tada je p jednak jednom od brojeva $p_i,\ i = 1, 2, \ldots, n$.*

Dokaz. Iz pretpostavke da $p \mid p_1 p_2 \cdots p_n$ slijedi da je $(p, p_1 p_2 \cdots p_n) = p \neq 1$. Kada bi p bio različit od svakog $p_i,\ i = 1, 2, \ldots, n$, vrijedilo bi $(p, p_i) = 1$, pa teorem 2.1.19 povlači $(p, p_1 p_2 \cdots p_n) = 1$, što je kontradikcija. Dakle, p mora biti jednak bar jednom od brojeva $p_i,\ i = 1, 2, \ldots, n$. □

Primjer 4.1.6. *Neka su $p = 7, p_1 = 3, p_2 = 5$ i $p_3 = 7$. Očito je da $7 \mid 3 \cdot 5 \cdot 7$, pa je i $p = p_3$. Vidimo da je $3 \cdot 5 \cdot 7 = 105$, odnosno da smo broj 105 dobili kao umnožak prostih brojeva. Kažemo da smo broj rastavili na **proste faktore**.*

Teorem 4.1.7. *Svaki složen broj može se jednoznačno rastaviti na proste faktore.*

Dokaz. Prvo dokažimo da za svaki složen broj n postoji konačan broj prostih faktora $p_1, p_2, \ldots, p_n$ takvih da je $a = p_1 p_2 \cdots p_n$. Dokaz ćemo provesti indukcijom. Najmanji složen broj je 4 i njegov rastav je $4 = 2 \cdot 2$. Uzmimo složen broj a' i pretpostavimo da se svaki složen broj manji od njega može rastaviti na proste faktore. Prema teoremu 4.1.1 postoji prost broj p koji dijeli a', odnosno $a' = pb$. Ako je broj b prost, onda imamo rastav broja a' na proste faktore. Ako je b složen, onda se, po pretpostavci, može rastaviti na proste faktore $b = p_1 p_2 \cdots p_k$. Sada je očito da je $a' = p p_1 p_2 \cdots p_k$, pa smo dobili rastav na proste faktore broja a', što smo trebali i dokazati.

Dokažimo sada da je rastav jedinstven. Ponovo, za rastav broja 4 tvrdnja je istinita te imamo složen broj a' s pretpostavkom da za svaki složen broj manji od a' postoji točno jedan rastav na proste faktore. Pretpostavimo suprotno, neka je $a' = p_1 p_2 \cdots p_k$ jedan rastav broja a' na proste faktore, a $a' = q_1 q_2 \cdots q_l$ drugi rastav. Uzmimo da je $b = p_2 \cdots p_k$ i $k = 2$ te imamo $a' = p_1 b$. Kako $p_1 \mid a'$, to $p_1 \mid q_1 q_2 \cdots q_l$, pa iz prethodnog teorema slijedi da je p_1 jednak barem jednom od brojeva $q_1, q_2, \ldots, q_l$. Bez smanjenja općenitosti, neka je $p_1 = q_1$. Tada je $a' = p_1 q_2 \cdots q_l$. No, kako je $a' = p_1 b$, onda je $b = q_2 \cdots q_l$. Ako je $b = p_2$, onda je b prost, pa je $b = q_2$ i stoga $p_2 = q_2$. Time smo dobili jedini rastav za a', tj. $a' = p_1 p_2$. Pretpostavimo sada da je b složen broj. Tada su, po pretpostavci, njegovi rastavi na proste faktore jednaki, pa je $k = l$ te su brojevi $p_2, p_3, \ldots, p_k$ jednaki brojevima $q_2, q_3, \ldots, q_l$. Zbog $p_1 = q_1$, zaključujemo da su i rastavi broja a' jednaki. To je i trebalo dokazati. □

Očito, ako se u rastavu na proste faktore oni ponavljaju, vrijedi $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, gdje su $p_1, p_2, \ldots, p_k$ prosti faktori, a $\alpha_1, \alpha_2, \ldots, \alpha_k$ brojevi ponavljanja prostih brojeva u rastavu.

Teorem 4.1.8. *Neka je n prirodan i složen broj. Njegov najmanji djelitelj, veći od 1, nije veći od* $\sqrt{n}$.

Dokaz. Kako je n složen broj, to postoje djelitelji d i d', veći od 1, takvi da je $n = dd'$. Bez smanjenja općenitosti, neka je $d \leq d'$. Tada je $d^2 \leq dd'$, odnosno $d^2 \leq n$. Očito je sada da je $d \leq \sqrt{n}$ i $d > 1$. □

4.2 Prosti djelitelji cijelog broja

U prošlom potpoglavlju dokazali smo neke tvrdnje vezane uz rastav brojeva na proste faktore. Pokažimo primjer.

Primjer 4.2.1. *Rastavimo brojeve* 2268 *i* 126 *na proste faktore:*

$$2268 = 2^2 \cdot 3^4 \cdot 7\ ; \qquad 126 = 2 \cdot 3^2 \cdot 7.$$

Broj 2268 *je djeljiv brojem* 126*, zato što broj* 126 *sadrži iste proste faktore, s manjim eksponentima.*

Sljedeći teorem opravdava primjer.

Teorem 4.2.2 (Kriterij djeljivosti dva broja)**.** *Neka su m i n prirodni brojevi te neka je* $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. *Tada* $n \mid m$ *ako i samo ako je* $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, *pri čemu je* $0 \leq \beta_i \leq \alpha_i,\ i = 1, 2, \ldots, k$.

Dokaz. Neka je $n = q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_l^{\gamma_l}$ rastav broja n na proste faktore. Ako $n \mid m$, onda zbog $q_i^{\gamma_i} \mid n,\ i = 1, 2, \ldots l$ vrijedi i da $q_i^{\gamma_i} \mid p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. To znači da je svaki od brojeva $q_i,\ i = 1, 2, \ldots, l$ jednak nekom od brojeva $p_j,\ j = 1, 2, \ldots, k$. Stoga je $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. S obzirom da $p_i^{\beta_i} \mid p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ i $(p_i^{\alpha_i}, p_j^{\beta_j}) = 1$, onda za $i \neq j$ slijedi da $p_i^{\beta_i} \mid p_i^{\alpha_i}$ te $\beta_i \leq \alpha_i$.

Obrnuto, ako je $0 \leq \beta_i \leq \alpha_i,\ i = 1, 2, \ldots, k$ onda $p_i^{\beta_i} \mid p_i^{\alpha_i}$, pa slijedi $n \mid m$. □

Očito je da ako $n \mid m$, onda je $\frac{m}{n} = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \cdots p_k^{\alpha_k - \beta_k}$, a djelitelji broja m su oblika $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$.

Teorem 4.2.3. *Neka je* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *rastav broja a na proste faktore. Broj njegovih djelitelja jednak je* $\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$.

Dokaz. Djelitelji broja a su oblika $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, za $a \leq \beta_i \leq \alpha_i,\ i = 1, 2, \ldots, k$. Za vrijednosti $\beta_2, \beta_3, \ldots, \beta_k$ imamo $\alpha_1 + 1$ različitih djelitelja, jer β_1 može imati vrijednosti $0, 1, 2, \ldots, \alpha_1$. Analogno, za vrijednosti $\beta_3, \beta_4, \ldots, \beta_k$ ima $\alpha_2 + 1$ različitih djelitelja, pa postoji ukupno $(\alpha_1 + 1)(\alpha_2 + 1)$ djelitelja. Indukcijom postižemo da je broj svih djelitelja od a jednak $\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$. □

Trivijalan slučaj ovog teorema je $\tau(1) = 1$, a po definiciji prostog broja p, $\tau(p) = 2$. Neka je $\sigma(a)$ zbroj svih djelitelja od a. Sljedećim teoremom dokazujemo svojstvo s relativno prostim brojevima.

Teorem 4.2.4. *Neka su a i b prirodni brojevi takvi da je $(a, b) = 1$. Vrijedi: $\sigma(ab) = \sigma(a)\sigma(b)$.*

Dokaz. Neka su $1 = a_0 < a_1 < \cdots < a_k = a$ djelitelji broja a te $1 = b_0 < b_1 < \cdots < b_l = b$ djelitelji broja b. Imamo:

$$\sigma(a) = a_0 + a_1 + \cdots + a_k = \sum_{i=0}^{k} a_i \text{ i } \sigma(b) = b_0 + b_1 + \cdots + b_l = \sum_{j=0}^{l} b_j,$$

$$\sigma(a)\sigma(b) = \sum_{i=0}^{k} a_i \cdot \sum_{j=0}^{l} b_j = \sum_{i=0}^{k} \sum_{j=0}^{l} a_i b_j = \sigma(ab).$$

□

4.3 Operacije max i min

Operacije max i min definiraju se na sljedeći način: $\max(a, b) = a$ i $\min(a, b) = b$, za realne brojeve a i b, takve da je $a \geq b$.

Teorem 4.3.1. *Za realne brojeve x, y i z vrijedi: ako je $x \geq y$ i $x \geq z$, onda je $x \geq \max(y, z)$, odnosno ako je $x \leq y$ i $x \leq z$, onda je $x \leq \min(y, z)$.*

Dokaz. Vrijedi: $\max(y, z) = y$ ili $\max(y, z) = z$. Ako je $x \geq y$ i $x \geq z$, onda je očito $x \geq \max(y, z)$. Analogno dokazujemo za operaciju min. □

Za operacije min i max vrijede sljedeća svojstva.

Teorem 4.3.2. *Ako su a, b, c i k realni brojevi, onda za operacije* min *i* max *vrijedi:*

(i) zakon idempotencije: $\max(a, a) = a,\ \min(a, a) = a$;

(ii) zakon komutacije: $\max(a, b) = \max(b, a),\ \min(a, b) = \min(b, a)$;

(iii) zakon asocijacije: $\max(\max(a,b),c) = \max(a,\max(b,c))$,
$\min(\min(a,b),c) = \min(a,\min(b,c))$;

(iv) zakon distribucije: $k\max(a,b) = \max(ka,kb),\ k \geq 0$;
$k\max(a,b) = \min(ka,kb),\ k \leq 0$;
$k\min(a,b) = \min(ka,kb),\ k \geq 0$;
$k\min(a,b) = \max(ka,kb),\ k \leq 0$;
$\min(\max(a,b),c) = \max(\min(a,c),\min(b,c))$;
$\max(\min(a,b),c) = \min(\max(a,c),\max(b,c))$.

4.4 Zadatci

Zadatak 4.4.1 (Školsko/gradsko natjecanje, 2. razred srednje škole, 2018.)**.** *Odredi sve trojke prostih brojeva* (p,q,r) *za koje vrijedi* $p^q = r - 1$.

Rješenje. Ako je $r = 2$, onda je $p^q = 1$, što nije moguće po definiciji prostih brojeva. Zaključujemo da je r prost broj veći od 2, pa je i neparan. Tada je $p^q = r - 1$ paran broj, odakle slijedi da je i broj p paran, a kako je i prost, to je $p = 2$. Za $q = 2$ rješenje je uređena trojka $(2,2,5)$. Za $q > 2$ faktorizirajmo izraz.

$$\begin{aligned} 2^q &= r - 1, \\ r &= 2^q + 1, \\ r &= (2+1)(2^{q-1} - 2^{q-2} + 2^{q-3} - \cdots + 1), \\ r &= 3(2^{q-1} - 2^{q-2} + 2^{q-3} - \cdots + 1). \end{aligned}$$

Vidimo da je r djeljiv sa 3, pa slijedi da je $r = 3$. U tom slučaju je $q = 1$, što je nemoguće. Dakle, jedino rješenje je uređena trojka $(2,2,5)$. □

Zadatak 4.4.2 (Školsko/gradsko natjecanje, 3. razred srednje škole, 2014.)**.** *Ako su* p *i* $p^2 + 8$ *prosti brojevi, dokaži da je i broj* $p^3 + 4$ *prost.*

Rješenje. Ako je $p = 2$, tada je $p^2 + 8 = 12$, što nije prost broj. Ako je $p = 3$, onda je $p^2 + 8 = 17$ prost broj te je i $p^3 + 4 = 31$ prost, pa tvrdnja vrijedi. Neka je sada $p \neq 3$. Imamo dva slučaja:

(i) Neka je $p = 3k+1, k \in \mathbb{Z}$. Vrijedi: $p^2+8 = (3k+1)^2+8 = 9k^2+6k+9 = 3(3k^2+2k+3)$, pa je $p^2 + 8$ djeljivo sa 3. Zaključujemo da $p^2 + 8$ nije prost broj.

(i) Neka je $p = 3k + 2$, $k \in \mathbb{Z}$. Sada je $p^2 + 8 = (3k + 2)^2 + 8 = 9k^2 + 12k + 12 = 3(3k^2 + 4k + 4)$, što je također djeljivo sa 3, pa ni u ovom slučaju $p^2 + 8$ nije prost broj.

Dakle, jedino je moguće da vrijedi tvrdnja za $p = 3$. □

Zadatak 4.4.3 (Školsko/gradsko natjecanje, 3. razred srednje škole, 2020.)**.** *Dani su prosti brojevi p, q, r i s takvi da je $5 < p < q < r < s < p + 10$. Dokaži da je zbroj tih četiriju brojeva djeljiv sa 60.*

Rješenje. S obzirom da su p, q, r i s prosti i veći od 5, onda su neparni. Zato moraju biti u skupu $\{p, p + 2, p + 4, p + 6, p + 8\}$. Brojevi p i $p + 6$ daju isti ostatak pri dijeljenju s 3, pa $p + 6$ nije djeljiv s 3. Također, $p + 2$ i $p + 8$ daju isti ostatak pri dijeljenju sa 3, pa onda ni oni ne mogu biti djeljivi sa 3 jer je barem jedan od njih prost. Zaključujemo da je $p + 4$ djeljiv sa 3 i nije prost. Sada znamo da je $q = p + 2, r = p + 6$ i $s = p + 8$. Zbrojimo li ih, dobivamo:

$$p + q + r + s = p + p + 2 + p + 6 + p + 8 = 4p + 16 = 4(p + 4).$$

Dobiveni zbroj je djeljiv sa 4 i sa 3. Dokažimo još da je djeljiv i sa 5. Kako su $p, p + 2, p + 4, p + 6$ i $p + 8$ uzastopni neparni brojevi, točno jedan od njih mora biti djeljiv sa 5. No, $p, p + 2, p + 6$ i $p + 8$ su prosti, pa je jedino moguće da je $p + 4$ djeljiv i sa 5. Dakle, $4(p + 4)$ djeljiv sa $3, 4$ i 5, pa je djeljiv i sa 60. □

Zadatak 4.4.4 (Županijsko natjecanje, 1. razred srednje škole, 2018.)**.** *Odredite sve cijele brojeve a za koje je $4a^2 - 24a - 5$ prost broj.*

Rješenje. Neka je $4a^2 - 24a - 45 = p$, pri čemu je p prost broj. Faktorizirajmo lijevu stranu jednakosti.

$$\begin{aligned} 4a^2 - 24a - 45 &= p, \\ 4a^2 - 30a + 6a - 45 &= p, \\ 2a(2a - 15) + 3(2a - 15) &= p, \\ (2a - 15)(2a + 3) &= p. \end{aligned}$$

Jedini djelitelji broja p su ± 1 i $\pm p$. Imamo sljedeće mogućnosti:

(i) $2a - 15 = 1$ i $2a + 3 = p$, iz čega slijedi $a = 8$ i $p = 19$;

(ii) $2a - 15 = -1$ i $2a + 3 = -p$, iz čega slijedi $a = 7$ i $p = -17$;

(iii) $2a + 3 = 1$ i $2a - 15 = p$, iz čega slijedi $a = -1$ i $p = -17$;

(iv) $2a + 3 = -1$ i $2a - 15 = -p$, iz čega slijedi $a = -2$ i $p = 19$.

Kako je $p > 0$, to su jedini cijeli brojevi a za koje je dani izraz prost broj jednaki 8 i -2. □

Zadatak 4.4.5 (Županijsko natjecanje, 2. razred srednje škole, 2015.)**.** *Odredite sve četvorke* (a, b, c, d) *prirodnih brojeva takve da je* $a^3 = b^2$, $c^5 = d^4$ *i* $a - c = 9$.

Rješenje: Brojevi a i b imaju iste proste faktore. Označimo s p zajednički prosti faktor, koji se u broju a pojavljuje s eksponentom m, a u broju b s eksponentom n. Vrijedi: $p^{3m} = p^{2n}$, iz čega slijedi da $3m = 2n$. Zaključujemo da je m paran broj. To znači da je a potpun kvadrat za svaki prost faktor p. Dakle, $a = k^2$, $k \in \mathbb{N}$. Analogno, $c = l^4$, $l \in \mathbb{N}$. Sada imamo:

$$9 = a - c = k^2 - l^4 = (k - l^2)(k + l^2).$$

Broj $k + l^2$ je očito pozitivan, pa je i $k - l^2$ pozitivan. S obzirom da su k i l prirodni brojevi, to je $k - l^2 < k + l^2$. Tada je jedina mogućnost $k + l^2 = 9$ i $k - l^2 = 1$. Rješavanjem sustava dobivamo $k = 5$ i $l = 2$. Dakle, $a = 5^2 = 25$, $b = 5^3 = 125$, $c = 2^4 = 8$ i $d = 2^5 = 32$. □

Zadatak 4.4.6 (Županijsko natjecanje, 3. razred srednje škole, 2019.)**.** *Odredi sve uređene parove* (m, n) *prirodnih brojeva za koje postoji prost broj* p *takav da vrijedi* $9^m + 3^m - 2 = 2p^n$.

Rješenje. Faktorizacijom lijeve strane jednadžbe imamo:

$$\begin{aligned} 9^m + 3^m - 2 &= 2p^n, \\ 3^{2m} - 3^m + 2 \cdot 3m - 2 &= 2p^n, \\ 3^m(3^m - 1) + 2(3^m - 1) &= 2p^n, \\ (3^m - 1)(3^m + 2) &= 2p^n. \end{aligned}$$

Kada bi lijeva strana jednakosti bila djeljiva prostim brojem p, onda bi i njihova razlika $3^m + 2 - (3^m - 1) = 3$ bila djeljiva s p, odnosno $p = 3$. No, očito je da lijeva strana nije djeljiva sa 3, pa je $3^m - 1 = 1$ ili $3^m - 1 = 2$. Uzimamo da je $3^m - 1 = 2$, pa je $3^m + 2 = p^n$. Iz $3^m - 1 = 2$ slijedi da je $m = 1$, pa je $p = 5$, a $n = 1$. □

Bibliografija

[1] A. Dujella, *Uvod u teoriju brojeva*, Matematički odsjek, Prirodoslovno - matematički fakultet, Sveučilište u Zagrebu, 2002., skripta, https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf (pristupljeno: 14.11.2019.)

[2] A. Horvatek, *Matematika na dlanu*, web-stranica, 2008., http://www.antonija-horvatek.from.hr/natjecanja-iz-matematike/zadaci-SS.htm,http://www.antonija-horvatek.from.hr/natjecanja-iz-matematike/zadaci-OS.htm (pristupljeno: 15.12.2019.)

[3] B. Dakić, *Funkcije*, Element, Zagreb, 1999.

[4] B. Pavković, B. Dakić, Ž. Hanjš, P. Mladinić, *Male teme iz matematike*, Mala matematička biblioteka, Hrvatsko matematičko društvo, Element, 1994.

[5] D. Ilišević, G. Muić, *Uvod u matematiku*, Matematički odsjek, Prirodoslovno - matematički fakultet, Sveučilište u Zagrebu, skripta, https://web.math.pmf.unizg.hr/~gmuic/predavanja/uum.pdf (pristupljeno: 12.3.2020.)

[6] M. Marić, *Diofantske jednadžbe*, web-stranica, natjecanja.math.hr, 2019., https://natjecanja.math.hr/wp-content/uploads/2019/07/Diofantske-jednadzbe-Maja-Maric-1.pdf (pristupljeno: 14.6.2020.)

[7] M. S. Popadić, *Deljivost celih brojeva*, Matematička biblioteka, Elektrotehnički fakultet Univerziteta u Beogradu, Beograd, 1959.

[8] M. Zelčić, *Diofantske jednadžbe na natjecanjima u osnovnim školama*, web-stranica, Lučko, 2016., http://www.antonija-horvatek.from.hr/natjecanja-iz-matematike/Lucko/Diofantske-jednadzbe-Zadaci-i-rjesenja-Maja-Zelcic.pdf (pristupljeno: 14.6.2020.)

[9] V. Kadum, *Funkcije "najveće cijelo" i "razlomljeni dio"*, Metodički obzori 4 (2009), 1-2

[10] V. Stošić, *Natjecanja učenika osnovnih škola*, Matkina biblioteka, Hrvatsko matematičko društvo, Zagreb, 2000.

[11] Ž. Hanjš, M. Krnić, *Matematička natjecanja 2006./2007.*, Element, Hrvatsko matematičko društvo, Zagreb, 2008.

Sažetak

U ovom radu su izloženi rezultati o djeljivosti cijelih brojeva. Preciznije, izložena su svojstva djeljivosti cijelih brojeva, svojstva prostih i relativno prostih brojeva, najvećeg zajedničkog djelitelja, najmanjeg zajedničkog višekratnika kao i metode rješavanja diofantskih jednadžbi. U radu su navedeni različiti primjeri kojima je pokazana primjena navedenih teorema koristeći konkretne brojeve. Svako poglavlje sadrži i odgovarajuće zadatke s matematičkih natjecanja.

Summary

In this thesis the results on divisibility of integers are presented. More precisely, it is on properties of divisibility of integers, on prime and relatively prime numbers, the greatest common divisor, the least common multiple and methods of solving Diophantine equations. Theorems are illustrated by applying them to various examples with concrete numbers. Each chapter is enriched with corresponding problems from mathematical competitions.

Životopis

Rođena sam 10. srpnja 1994. godine u Zagrebu. Pohađala sam Osnovnu školu Dragutina Domjanića u Svetom Ivanu Zelini te sam nakon toga, u istom gradu, upisala program opće gimnazije u Srednjoj školi Dragutina Stražimira. Srednju školu sam završila 2013. godine i odmah iste godine upisala Prirodoslovno - matematički fakultet u Zagrebu na Matematičkom odsjeku, gdje sam 2017. godine završila preddiplomski sveučilišni studij matematika, smjer nastavnički. Iste godine sam upisala diplomski studij matematika, smjer nastavnički, na istom fakultetu.