Osječki matematički list 13 (2013), 121-137

Primjene Euklidovog algoritma

Mateja Đumić * Mirela Jukić Bokun †

Sažetak

U članku pokazujemo kako se Euklidov algoritam može iskoristiti u rješavanju linearnih diofantskih jednadžbi i dobivene rezultate primjenjujemo na razne vrste zadataka. Osim toga, dovodimo u vezu Euklidov algoritam i razvoj racionalnog broja u verižni razlomak te navodimo neka od svojstava ovakvih razvoja.

Ključne riječi: *djeljivost, Euklidov algoritam, diofantska jednadžba, verižni razlomak*

Applications of the Euclidean algorithm

Abstract

In this article, we show how the Euclidean algorithm can be used for solving linear Diophantine equations and we apply the obtained results to various types of tasks. We also show that the Euclidean algorithm and expansion of a rational number to a continued fraction are closely related and we discuss some properties of those expansions.

Keywords: *divisibility, Euclidean algorithm, Diophantine equation, continued fraction*

*student Odjela za matematiku, Sveučilište u Osijeku, Gajev trg 6, HR-31 000 Osijek, email: mdjumic@mathos.hr

†Sveučilište u Osijeku, Gajev trg 6, HR-31 000 Osijek, email: mirela@mathos.hr

1 Uvod

Euklid (300 g. pr. Kr.) Značajan je što je sabrao dotadašnje matematičko znanje u zbirku poznatu kao Euklidovi elementi.

Euklidov algoritam je jedan od najstarijih algoritama. Spominje se još u Euklidovim Elementima po čemu je i dobio ime. Osnovna namjena ovog algoritma je određivanje najvećeg zajedničkog djelitelja, ali on nam, kao što ćemo vidjeti, omogućava i rješavanje linearnih diofantskih jednadžbi, te nam daje razvoj racionalnog broja u verižni razlomak.

Već je ranije u članku [9] ovog časopisa bilo riječi o Euklidovom algoritmu. Kako su tamo dokazane i najvažnije tvrdnje vezane uz sam algoritam (dokazi se mogu naći i u [5, 8]) mi ćemo u ovom članku samo podsjetiti na osnovne pojmove vezane uz njega, te ćemo naglasak staviti na posljedice ove tvrdnje i njihovu primjenu na razne vrste zadataka.

S obzirom da se teme koje se u članku obrađuju baziraju na elementarnoj teoriji brojeva i većina je tvrdnji koje dokazujemo intuitivno jasna smatramo da bi se primjeri i zadaci koje ovdje rješavamo mogli obrađivati na dodatnoj nastavi matematike i u prva tri razreda srednje škole, ali najprirodnije se uklapaju na početku četvrtog razreda srednje škole kada se prilikom obrade nastavne jedinice *Brojevni sustavi* koristi *Teorem o dijeljenju s ostatkom* na kojem je Euklidov algoritam baziran.

U članku ćemo se najprije prisjetiti osnovnih pojmova i svojstava Euklidovog algoritma te na primjerima pokazati prednosti tog algoritma. Nakon toga ćemo se baviti rješavanjem linearnih diofantskih jednadžbi i dobivene rezultate iskoristiti za rješavanje raznih vrsta zadataka. U posljednjem poglavlju otkrit ćemo vezu između Euklidovog algoritma i razvoja racionalnog broja u verižni razlomak, te navesti neka od najvažnijih svojstava ovakvih razvoja.

2 Euklidov algoritam

Ako su a, b cijeli brojevi takvi da je $a \neq 0$, onda kažemo da *a dijeli b* (odnosno da je b djeljiv s a) i pišemo $a|b$, ako postoji cijeli broj d takav da je $b = ad$. Ako b nije djeljiv s a, onda pišemo $a \nmid b$.

Teorem 2.1 (Teorem o dijeljenju s ostatkom).
Neka su a, b cijeli brojevi, $a > 0$. Tada postoje jedinstveni cijeli brojevi q i r takvi da je $b = aq + r$, $0 \leq r < a$.

Broj d nazivamo *zajednički djelitelj* cijelih brojeva a i b ako $d|a$ i $d|b$. Ako je barem jedan od brojeva a i b različit od nule, onda postoji samo konačno mnogo zajedničkih djelitelja od a i b. Najveći među njima nazivamo *najveći zajednički djelitelj* brojeva a i b i označavamo s (a, b) (ili $M(a, b)$, $NZD(a, b)$,

ili, najčešće u stranoj literaturi, $GCD(a,b)$). Ako je $(a,b) = 1$, kažemo da su a i b *relativno prosti*.

Primijetimo da vrijedi $(a,b) = (-a,b)$ i $(a,b) = (b,a)$. Stoga, bez smanjenja općenitosti, uvijek možemo tražiti (a,b) za pozitivne brojeve a,b takve da je $a \leq b$.

Euklidov algoritam. Neka su a,b cijeli brojevi, $a > 0$. Uzastopnom primjenom teorema 2.1 dobivamo niz jednakosti

$$\begin{aligned}
b &= aq_0 + r_1, & 0 < r_1 < a \\
a &= r_1q_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2q_2 + r_3, & 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_n.
\end{aligned}$$

Tada je najveći zajednički djelitelj brojeva a i b jednak r_n tj. (a,b) je jednak posljednjem ostatku različitom od nule u prethodnoj proceduri.

Uočimo da nam prethodni algoritam daje i više od najvećeg zajedničkog djelitelja. Iz prve dvije jednakosti vidimo da se r_1 pa onda i r_2 može prikazati kao linearna kombinacija od a i b. Zbog treće jednakosti se r_3 može prikazati kao linearna kombinacija od r_1 i r_2 zbog čega se onda može prikazati i kao linearna kombinacija od a i b. Primjenimo li analogan postupak zaključivanja na preostale jednakosti u Euklidovom algoritmu dobivamo da je svaki r_i kao linearna kombinacija od r_{i-1} i r_{i-2} linearna kombinacija od a i b. Specijalno, tvrdnja vrijedi i za r_n pa zaključujemo da vrijedi sljedeća tvrdnja.

Korolar 2.1. *Neka su a,b cijeli brojevi, $a > 0$. Tada postoje cijeli brojevi x_0, y_0 takvi da vrijedi $(a,b) = ax_0 + by_0$.*

Prema prethodnom korolaru slijedi da pomoću Euklidovog algoritma možemo dobiti i jedno konkretno ili takozvano partikularno rješenje jednadžbe oblika $ax + by = m$ (za $m = (a,b)$) u cijelim brojevima. Nešto više o ovom tipu jednadžbi reći ćemo u idućem poglavlju.

Primjer 1. *Euklidovim algoritmom odredite $(248, 92)$ te nađite $x, y \in \mathbb{Z}$ za koje vrijedi $(248, 92) = 248x + 92y$.*

Rješenje. Primjenom Euklidovog algoritma dobivamo

$$\begin{aligned} 248 &= 92 \cdot 2 + 64 \\ 92 &= 64 \cdot 1 + 28 \\ 64 &= 28 \cdot 2 + 8 \\ 28 &= 8 \cdot 3 + 4 \\ 8 &= 4 \cdot 2. \end{aligned}$$

Zaključujemo da je $(248, 92) = 4$. Povratne supstitucije daju

$$\begin{aligned} 4 &= 28 - 8 \cdot 3 = 28 - (64 - 28 \cdot 2) \cdot 3 = 7 \cdot 28 - 3 \cdot 64 \\ &= 7 \cdot (92 - 64) - 3 \cdot 64 = 7 \cdot 92 - 10 \cdot 64 \\ &= 7 \cdot 92 - 10 \cdot (248 - 92 \cdot 2) = 27 \cdot 92 - 10 \cdot 248. \end{aligned}$$

Stoga je traženo partikularno rješenje jednadžbe dano s $x = -10$, $y = 27$.◀

Prisjetimo se da se (a, b) može odrediti tako da se brojevi a i b rastave na faktore te se odrede zajednički faktori. Umnožak zajedničkih faktora je upravo (a, b). Iako je ova tvrdnja intuitivno jasna, napominjemo da se strogi matematički dokaz ove tvrdnje bazira na tvrdnjama koje su posljedice Euklidovog algoritma, ali mi ih ovdje nećemo navoditi (vidi npr. [8]).

Primjer 2. *Odredite* $(756500, 325992)$.

Rješenje. Kako je $756500 = 2^2 \cdot 5^3 \cdot 17 \cdot 89$, a $325992 = 2^3 \cdot 3 \cdot 17^2 \cdot 47$, zaključujemo da je $(756500, 325992) = 2^2 \cdot 17 = 68$. ◀

Jedna od najvažnijih prednosti Euklidovog algoritma je ta da pomoću njega možemo odrediti najveći zajednički djelitelj dvaju brojeva bez poznavanja njihova rastava na proste faktore što ponekad može biti, kao što ćemo vidjeti u primjeru koji slijedi, dosta težak posao.

Primjer 3. *Odredite* $(479909, 238103)$.

Rješenje. Kako je

$$\begin{aligned} 479909 &= 238103 \cdot 2 + 3703 \\ 238103 &= 3703 \cdot 64 + 1111 \\ 3703 &= 1111 \cdot 3 + 370 \\ 1111 &= 370 \cdot 3 + 1 \\ 370 &= 1 \cdot 370 \end{aligned}$$

zaključujemo da je $(479909, 238103) = 1$.

S druge strane, ako bismo željeli faktorizirati svaki od ova dva broja imali bismo puno više posla jer su ova dva broja prosta. Kako svaki složeni broj $n = m \cdot k$ ima faktor manji od $\sqrt{n}$ (kada ne bi imao, onda bi $m, k > \sqrt{n}$ pa bi $n = m \cdot k > \sqrt{n} \cdot \sqrt{n} = n$ što je kontradikcija), da dokažemo da je neki broj prost moramo pokazati da on nema prost djelitelj manji od $\sqrt{n}$. To znači, primjerice, da za faktorizaciju broja 238103 moramo provjeriti je li on djeljiv s nekim prostim brojem $< \sqrt{238103} \approx 487.958$, što bi vodilo do 93 provjere. ◀

3 Linearne diofantske jednadžbe

Polinomijalne jednadžbe s racionalnim koeficijentima kojima se traže cjelobrojna (ponekad se podrazumijevaju i racionalna) rješenja nazivaju se diofantskim jednadžbama u čast grčkog matematičara Diofanta koji ih je prvi rješavao (ne zna se pouzdano kada je Diofant djelovao, neki autori vjeruju da je djelovao oko 250. godine, dok ga drugi smještaju u rani početak prvog stoljeća).

Linearna diofantska jednadžba s dvije nepoznanice je jednadžba oblika $ax + by = m$, gdje su a, b, m cijeli brojevi i barem jedan od brojeva a, b je različit od 0. U prošlom smo poglavlju pokazali da jednadžba $ax + by = (a, b)$ uvijek ima rješenja, a idući teorem nam daje uvjete pod kojima bilo koja linearna diofantska jednadžba s dvije nepoznanice ima rješenja.

Teorem 3.1. *Linearna diofantska jednadžba $ax + by = m$ ima cjelobrojnih rješenja ako i samo ako $(a, b)|m$.*

Dokaz. Ako jednadžba $ax + by = m$ ima cjelobrojnih rješenja, onda iz $(a,b)|a$ i $(a, b)|b$ slijedi $(a, b)|ax + by$ tj. $(a, b)|m$ pa je ovaj smjer dokazan.

Pretpostavimo da $(a, b)|m$ tj. da postoji cijeli broj d takav da vrijedi $m = d \cdot (a, b)$. Prema korolaru 2.1 postoje cjelobrojni x_0, y_0 za koje vrijedi $(a, b) = ax_0 + by_0$. Množenjem ove jednakosti s d dobivamo $adx_0 + bdy_0 = m$ pa su dx_0 i dy_0 rješenja jednadžbe $ax + by = m$. □

Primjer 4. *Odredite neka cjelobrojna rješenja jednadžbe $248x + 92y = 12$, ako takva postoje.*

Rješenje. U primjeru 1 pokazali smo da je $(248, 92) = 4$. Kako $4|12$, prema prethodnom teoremu zaključujemo da jednadžba ima rješenje. Pokazali smo da je $x = -10$, $y = 27$ partikularno rješenje jednadžbe $248x + 92y = 4$ tj.

$$27 \cdot 92 - 10 \cdot 248 = 4.$$

Množenjem ove jednakosti s 3 dobijemo da je partikularno rješenje jednadžbe u ovom primjeru dano s $x = -30, y = 81$. ◀

Uočimo da $x = -30, y = 81$ nije jedino rješenje jednadžbe $248x + 92y = 12$. Lako se vidi da su i npr. $x = -7, y = 19$ rješenje ove jednadžbe. Naime, kao što ćemo vidjeti u sljedećem teoremu, ako linearna diofantska jednadžba ima barem jedno rješenje, onda ih ima beskonačno mnogo.

Teorem 3.2. *Neka je uređeni par (x_0, y_0) partikularno rješenje linearne diofantske jednadžbe $ax + by = m$ i neka je $d = (a, b)$. Tada su sva cjelobrojna rješenja ove jednadžbe dana s*

$$\begin{aligned} x &= x_0 + \frac{b}{d}t \\ y &= y_0 - \frac{a}{d}t \end{aligned}, \quad t \in \mathbb{Z}.$$

Dokaz. Neka je uređeni par (x_0, y_0) partikularno rješenje dane jednadžbe i neka je uređeni par (x, y) bilo koje drugo partikularno rješenje dane diofantske jednadžbe tj. neka vrijede sljedeće jednakosti

$$\begin{aligned} ax_0 + by_0 &= m \\ ax + by &= m. \end{aligned}$$

Oduzimanjem ovih dviju jednakosti dobivamo

$$a(x - x_0) + b(y - y_0) = 0.$$

Kako promatramo diofantsku jednadžbu, jedan od brojeva a, b mora biti različit od 0. Bez smanjenja općenitosti pretpostavimo da je $b \neq 0$. Iz prethodne jednakosti slijedi

$$y - y_0 = -\frac{a}{b}(x - x_0). \tag{1}$$

Kako je y cjelobrojan i $(a, b) = d$ postoje a', b' takvi da je $a = a'd, b = b'd$ i $(a', b') = 1$ (inače d ne bi bio najveći zajednički djelitelj od a i b). Stoga je $\frac{a}{b} = \frac{a'}{b'}$ pa iz (1) slijedi da $b' | (x - x_0)$ što znači da postoji $t \in \mathbb{Z}$ takav da vrijedi $x - x_0 = b't$. Iz jednakosti $b' = \frac{b}{d}$ sada slijedi $x = x_0 + \frac{b}{d}t$, a zbog (1) vrijedi $y = y_0 - \frac{a}{d}t$. Time je tvrdnja dokazana. □

Primjer 5. *Odredite sva cjelobrojna rješenja jednadžbe* $248x + 92y = 12$.

Rješenje. U primjeru 1 smo pokazali da je $(248, 92) = 4$, a u primjeru 4 da je $x = -30, y = 81$ partikularno rješenje dane jednadžbe. Direktnom primjenom prethodnog teorema zaključujemo da su sva rješenja ove jednadžbe dana s

$$\begin{aligned} x &= -30 + 23t \\ y &= \quad 81 - 62t \end{aligned}, \quad t \in \mathbb{Z}.$$

Točnost dobivenog rješenja se lako provjeri uvrštavanjem u polaznu jednadžbu. ◀

Uočimo da zapis beskonačnog skupa rješenja ovisi o tome koje partikularno rješenje smo odredili. Kako ovih rješenja ima beskonačno mnogo, imamo i beskonačno zapisa svih rješenja.

U nastavku ćemo riješiti nekoliko zadataka kako bismo pokazali primjenu dobivenih rezultata.

Zadatak 1. Postoji li neki prirodan broj koji pri dijeljenju s 1001 daje ostatak 23, a pri dijeljenju s brojem 1170 ostatak 42?

Rješenje. Kad bi postojao prirodan broj n s ovim svojstvom, onda bi moralo vrijediti

$$\begin{aligned} n &= 1001x + 23 \\ n &= 1170y + 42, \end{aligned}$$

tj.

$$1001x - 1170y = 19.$$

Provjerimo ima li ova diofantska jednadžba rješenja. Iz

$$\begin{aligned} 1170 &= 1001 \cdot 1 + 169 \\ 1001 &= 169 \cdot 5 + 156 \\ 169 &= 156 \cdot 1 + 13 \\ 156 &= 13 \cdot 12 \end{aligned}$$

zaključujemo da je $(1170, 1001) = 13$. Kako $13 \nmid 19$, prema teoremu 3.1 slijedi da ne postoji prirodan broj n s ovim svojstvima. ◀

Zadatak 2. Za prirodan broj n neka je $a_n = 22n + 7$, $b_n = 33n + 10$ i $d_n = (a_n, b_n)$. Dokažite da je $d_n = 1$, za svaki n.

Rješenje. Iz jednakosti

$$3(22n+7)+(-2)(33n+10)=1$$

slijedi da jednadžba $a_n x + b_n y = 1$ ima rješenja. Teorem 3.1 sada povlači da $d_n|1$. Kako je $d_n > 0$, zaključujemo da je $d_n = 1$. ◀

Zadatak 3. Ana knjigu koja košta 77 kn želi platiti kovanicama od 1, 2 i 5 kn, s tim da iskoristi dvostrukp više kovanica od 2 kn nego onih od 5 kn. Na koliko načina to može učiniti?

Rješenje. Neka je x broj kovanica po 5 kn, a y broj kovanica po 1 kn. Iz uvjeta zadatka dobivamo

$$2 \cdot 2x + 5x + y \quad = \quad 77$$

tj.

$$9x + y = 77.$$

Partikularno rješenje $x = 8$ i $y = 5$ ove jednadžbe se lako vidi pa ne moramo niti primjenjivati Euklidov algoritam. Sva cjelobrojna rješenja dana su s

$$\begin{array}{l} x = 8 + t \\ y = 5 - 9t \end{array}, \quad t \in \mathbb{Z}.$$

Iz $x > 0$ i $y \geqslant 0$ slijedi $t > -8$ i $9t \leqslant 5$ pa slijedi da je $t \in \{-7, -6, -5, -4, -3, -2, -1, 0\}$ tj. postoji 8 načina na koji Ana može platiti račun. ◀

Zadatak 4. U razredu ima između 20 i 30 učenika. Na satu tjelesnog prilikom raspoređivanja u tri kolone u dvije se nalazi jednak broj učenika, a u zadnjoj za jedan manje, a prilikom pokušaja raspoređivanja u pet kolona u četiri bi bio jednak broj, a u petoj za jedan više. Odredite broj učenika u razredu.

Rješenje. Neka je z broj učenika u razredu. Iz uvjeta zadatka slijedi

$$\begin{aligned} z &= 3x - 1 \\ z &= 5y + 1, \end{aligned}$$

odnosno

$$3x - 5y = 2.$$

Lako se iščita rješenje $x = -1$, $y = -1$ pa su sva rješenja dana s

$$\begin{array}{l} x = -1 - 5t \\ y = -1 - 3t \end{array}, \quad t \in \mathbb{Z}.$$

Iz uvjeta

$$20 < 3x - 1 < 30 \qquad 20 < 5y - 1 < 30$$

dobivamo isti uvjet na t

$$-2.26 \leqslant t \leqslant -1.6$$

Zaključujemo da je $t = -2$ pa u razredu ima $z = 3 \cdot 9 - 1 = 26$ učenika. ◀

Zadatak 5. Zbroj opsega pravilnog 15-erokuta i 17-erokuta iznosi 638. Ako je poznato da su duljine stranica cijeli brojevi, odredite te duljine.

Rješenje. Neka je x duljina stranice pravilnog 15-erokuta, a y duljina stranice pravilnog 17-erokuta. Tada imamo:

$$15x + 17y = 638.$$

Znamo da je $(17, 15) = 1$ pa rješenje postoji.

Euklidov algoritam daje

$$\begin{aligned} 17 &= 15 \cdot 1 + 2 \\ 15 &= 2 \cdot 7 + 1 \\ 2 &= 1 \cdot 2, \end{aligned}$$

pa je

$$1 = 15 - 2 \cdot 7 = 15 - 7 \cdot (17 - 15 \cdot 1) = 8 \cdot 15 - 7 \cdot 17.$$

Iz

$$8 \cdot 15 - 7 \cdot 17 \quad = \quad 1/ \cdot 638$$

slijedi

$$15 \cdot 5104 - 17 \cdot 4466 = 638.$$

Stoga je partikularno rješenje $x = 5104$, $y = -4466$, a sva rješenja su dana s

$$\begin{matrix} x = & 5104 + 17t \\ y = & -4466 - 15t \end{matrix}, \quad t \in \mathbb{Z}.$$

Kako se radi o stranicama n-terokuta znamo da je $x > 0$ i $y > 0$. Lako se pokaže da je tada $-300 \leqslant t \leqslant -298$ pa dobivamo sljedeća rješenja: $(4, 34)$, $(21, 19)$ i $(38, 4)$. ◀

Zadatak 6. Otac četvero djece kod sebe ima između 100 i 200 kn. Odlučio je svakom djetetu dati određenu svotu novca, i to na sljedeći način: prvom djetetu će dati $\frac{1}{5}$ novca kojeg ima kod sebe, drugom djetetu će dati $\frac{1}{5}$ preostale svote, trećem isto tako $\frac{1}{5}$ preostale svote, a četvrtom 30 kn. Koliki iznos otac ima kod sebe i koliki mu je iznos ostao?

Rješenje. Zapišimo raspodjelu koja je zadana u zadatku, pri čemu je x iznos koji otac ima kod sebe:

> Prvo dijete će dobiti $\frac{1}{5}x$, odnosno preostali iznos će biti $\frac{4}{5}x$. Drugo dijete će dobiti $\frac{4}{25}x$, odnosno preostali iznos će biti $\frac{21}{25}x$. Treće dijete će dobiti $\frac{21}{125}x$, a četvrto dijete će dobiti 30 kn.

Ako s y označimo iznos koji je otac dao djeci onda dobivamo jednadžbu

$$\frac{1}{5}x + \frac{4}{25}x + \frac{21}{125}x + 30 = y,$$

tj.

$$66x - 125y = -3750.$$

Euklidovim algoritmom (napravite to za vježbu) dobivamo

$$66 \cdot 36 - 125 \cdot 19 \quad = \quad 1/ \cdot (-3750),$$

odakle je

$$66 \cdot (-135000) - 125 \cdot (-71250) = -3750.$$

Sva rješenja polazne jednadžbe dana su s

$$\begin{array}{l} x = -135000 - 125t \\ y = -71250 - 66t \end{array}, \quad t \in \mathbb{Z}.$$

Prema uvjetima zadatka je $100 \leqslant x \leqslant 200$ pa su uvjeti za t dani s $-1081.6 \leqslant t \leqslant -1080.8$. Stoga je $t = -1081$. Zaključujemo da je otac imao 125 kn kod sebe, a ostalo mu je $125 - 96 = 29$ kn. ◀

Zadatak 7. Odredite sva cjelobrojna rješenja jednadžbe

$$3x - 4y + 6z = 1.$$

Rješenje. U zadatku zapravo trebamo riješiti linearnu diofantsku jednadžbu s tri nepoznanice. Promatrajmo ju u obliku $3x + 6z = 1 + 4y$. Uočimo da je $(3, 6) = 3$, odnosno lijeva strana je djeljiva s 3, pa onda i desna strana mora biti djeljiva s 3 tj. $1 + 4y$ mora biti djeljivo s 3. Stoga je $1 + 4y = 3k, k \in \mathbb{Z}$, pa dobivamo jednadžbu

$$3k - 4y = 1.$$

Partikularno rješenje ove jednadžbe je npr. $x_0 = 3, y_0 = 2$ pa je opće rješenje dano s

$$\begin{array}{l} k = 3 - 4t \\ y = 2 - 3t \end{array}, \quad t \in \mathbb{Z}.$$

Uvrštavanjem parametarskog rješenja za y u početnu jednadžbu, nakon malo sređivanja, dobivamo

$$x + 2z = 3 - 4t.$$

Jedno rješenje se relativno lako vidi, a to je $x_0 = 1$ i $z_0 = 1 - 2t$ pa je opće rješenje dano s

$$\begin{array}{l} x = 1 + 2u \\ z = 1 - 2t - u \end{array}, \quad u \in \mathbb{Z}.$$

Rješenja polazne jednadžbe su sada dana s

$$\begin{array}{l} x = 1 + 2u \\ y = 2 - 3t \\ z = 1 - 2t - u \end{array}, \quad t, u \in \mathbb{Z}.$$

◀

Zadatak 8. Koje su godine rođene osobe koje su u 1987. godini navršile onoliko godina koliki je zbroj znamenki godine njihova rođenja?

Rješenje. Neka su te osobe rođene godine $\overline{19xy}$, pri čemu su $x, y \in \{0, 1, 2, \ldots, 9\}$. Prema uvjetu zadatka vrijedi:

$$1987 - (1000 + 900 + 10x + y) = 1 + 9 + x + y,$$

odnosno:

$$11x + 2y = 77.$$

Istim postupkom kao i ranije se može pokazati da je opće rješenje ove jednadžbe dano s

$$\begin{array}{l} x = 5 + 2t \\ y = 11 - 11t \end{array}, \quad t \in \mathbb{Z}.$$

Kako x i y mogu poprimiti samo vrijednosti $0, 1, 2, \ldots, 9$, pokazuje se da naš problem ima rješenje za $t = 1$. Stoga je $x = 7$ i $y = 0$ pa su navedene osobe rođene 1970. godine.

Uočimo da osobe nisu mogle biti rođene u 19. stoljeću, jer bi tada diofantska jednadžba glasila $11x + 2y = 178$. Kako za $x, y \in \{0, 1, 2, \ldots, 9\}$ vrijedi $11x + 2y \leq 117$, ovaj slučaj ne daje rješenje. ◀

4 Verižni razlomci

Zapišemo li niz jednakosti u Euklidovom algoritmu na sljedeći način

$$\begin{aligned}
\frac{b}{a} &= q_0 + \frac{r_1}{a}, \\
\frac{a}{r_1} &= q_1 + \frac{r_2}{r_1}, \\
\frac{r_1}{r_2} &= q_2 + \frac{r_3}{r_2}, \\
&\vdots \\
\frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{r_n}{r_{n-1}}, \\
\frac{r_{n-1}}{r_n} &= q_n,
\end{aligned}$$

zaključujemo da je

$$\frac{b}{a} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots\, q_{n-1} + \cfrac{1}{q_n}}}}.$$

Ovo je razvoj broja $\frac{b}{a}$ u *verižni razlomak* koji se kraće zapisuje na sljedeći način

$$\frac{b}{a} = [q_0; q_1, q_2, \ldots, q_n].$$

Počeci verižnih razlomaka tradicionalno se vežu za vrijeme nastanka Euklidovog algoritma upravo zbog činjenice da se razvoj u verižni razlomak racionalnog broja može dobiti algebarskim manipulacijama s jednakostima u Euklidovom algoritmu, ali Euklid i njegovi prethodnici vjerojatno nisu koristili algoritam na ovaj način.

Poznato je da je indijski matematičar Aryabhata (475.–550.) koristio verižne razlomke pri određivanju rješenja linearnih diofantskih jednadžbi (o tome ćemo nešto više reći u nastavku), međutim on nije imao razvijenu opću metodu nego je verižne razlomke koristio u nekim konkretnim primjerima. Takva je primjena verižnih razlomaka trajala više od tisuću godina, a moderna teorija verižnih razlomaka počinje s radovima talijanskih matematičara Rafaela Bombellia (1526.–1572.) i Pietra Cataldia (1548.–1626.). Nakon njih je svoj doprinos razvoju teorije verižnih razlomaka dao

niz matematičara kao što su John Wallis (1616.–1703.), Christiaan Huygens (1629.–1695.), Leonard Euler (1707.–1783.), Johan Lambert (1728.–1777.), Joseph Louis Lagrange (1736.–1813.) i dr. Više o tome može se naći u [10].

Primjer 6. *Razvijte u verižni razlomak racionalni broj* $\frac{1170}{1001}$.

Rješenje. U zadatku 1 smo već primijenili Euklidov algoritam na ove brojeve pa sada samo iščitavamo

$$\frac{1170}{1001} = 1 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{12}}} = [1; 5, 1, 12].$$

◀

Zadatak 9. Razvijte u verižne razlomke racionalne brojeve $\frac{96}{67}$, $\frac{67}{96}$.

Rješenje. Kako je

$$\begin{aligned} 96 &= 67 \cdot 1 + 29 \\ 67 &= 29 \cdot 2 + 9 \\ 29 &= 9 \cdot 3 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2, \end{aligned} \tag{2}$$

dobivamo

$$\frac{96}{67} = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}} = [1; 2, 3, 4, 2].$$

Kako je $67 = 96 \cdot 0 + 67$, a ostatak algoritma je isti kao u (2), zaključujemo da je

$$\frac{67}{96} = [0; 1, 2, 3, 4, 2].$$

U ovom članku koncentrirat ćemo se na verižne razlomke racionalnih brojeva i njihova svojstva, no napominjemo da se svaki realni broj može razviti u verižni razlomak ([5]) te da se razvoj iracionalnih brojeva u verižni razlomak ne bazira na Euklidovom algoritmu.

Jedno važno svojstvo verižnih razlomaka slijedi direktno iz Euklidovog algoritma. Naime, kako Euklidov algoritam ima konačan broj koraka, razvoj racionalnog broja u verižni razlomak je konačan. S druge strane, jasno je i da se sređivanjem konačnog verižnog razlomka dobiva racionalan broj. Stoga vrijedi sljedeći teorem.

Teorem 4.1. *Razvoj u verižni razlomak realnog broja α je konačan ako i samo ako je α racionalan broj.*

Sada ćemo opisati kako se korištenjem verižnih razlomaka može odrediti rješenje linearne diofantske jednadžbe s dvije nepoznanice.

Neka je $\frac{b}{a} = [q_0; q_1, q_2, \ldots, q_n]$. Za $k \leq n$ definirajmo k-tu konvergentu ovog verižnog razlomka s

$$\frac{P_k}{Q_k} = [q_0; q_1, q_2, \ldots, q_k].$$

Metodom matematičke indukcije može se pokazati ([5]) da brojevi P_k i Q_k zadovoljavaju rekurzivne relacije

$$P_{-1} = 1, \quad P_0 = q_0, \quad P_k = q_k P_{k-1} + P_{k-2} \tag{3}$$

$$Q_{-1} = 0, \quad Q_0 = 1, \quad Q_k = q_k Q_{k-1} + Q_{k-2}. \tag{4}$$

te da je

$$Q_k P_{k-1} - P_k Q_{k-1} = (-1)^k. \tag{5}$$

Odavde slijedi da broj $d_k = (P_k, Q_k)$ ima svojstvo $d_k | 1$ pa je $d_k = 1$, tj. brojnici i nazivnici konvergenti su maksimalno skraćeni. Ako je $(a, b) = 1$, iz $\frac{b}{a} = \frac{P_n}{Q_n}$ dobivamo $b = P_n$, $a = Q_n$, a onda se za $k = n$ iz (5) dobiva jednakost

$$aP_{n-1} - bQ_{n-1} = (-1)^n. \tag{6}$$

Uočimo da iz ove jednakosti možemo iščitati partikularno rješenje jednadžbe $ax + by = 1$: ako je n paran onda je partikularno rješenje dano s $x = P_{n-1}$, $y = -Q_{n-1}$, a ako je n neparan onda je partikularno rješenje dano s $x = -P_{n-1}$, $y = Q_{n-1}$.

Primjer 7. *Koristeći verižne razlomke odredite neko cjelobrojno rješenje jednadžbe* $67x + 96y = 1$.

Rješenje. U zadatku 9 smo pokazali da je $\frac{96}{67} = [1; 2, 3, 4, 2]$ pa iz svojstva (6), jer je u ovom slučaju $n = 4$, slijedi

$$67P_3 - 96Q_3 = 1.$$

P_3 i Q_3 se relativno lako računaju korištenjem rekurzija (3) i (4):

$$\begin{aligned} P_1 &= 2\cdot 1+1=3, & Q_1 &= 2\cdot 1+0=2,\\ P_2 &= 3\cdot 3+1=10, & Q_2 &= 3\cdot 2+1=7,\\ P_3 &= 4\cdot 10+3=43, & Q_3 &= 4\cdot 7+2=30. \end{aligned}$$

Prema tome traženo partikularno rješenje je dano s $x = P_3 = 43$, $y = -Q_3 = -30$. ◀

Još jedno važno svojstvo verižnih razlomaka je da se racionalan broj α (analogna tvrdnja vrijedi i za iracionalne brojeve) može dobro aproksimirati pomoću verižnog razlomka. Ako je $\frac{P_k}{Q_k}$ konvergenta u razvoju u verižni razlomak racionalnog broja α, a $\frac{p}{q}$ bilo koji racionalni broj sa svojstvom $0 < q < Q_{k+1}$ može se pokazati ([1]) da vrijedi

$$|Q_k\alpha - P_k| \leq |q\alpha - p|.$$

Drugim riječima, konvergenta $\frac{P_k}{Q_k}$ je najbolja aproksimacija broja α s nazivnikom $< Q_{k+1}$.

Ovo svojstvo verižnih razlomaka koristio je u 17. stoljeću nizozemski matematičar i astronom Christiaan Huygens prilikom izgradnje mehanič- kog modela sunčevog sustava ([10]). Zanimljiva primjenu ovog svojstva verižnih razlomaka na problem kalendara može se naći u članku [6].

Primjer 8. *Nađite najbolje aproksimacije broja $\frac{96}{67}$ s nazivnikom manjim ili jednakim*

(i) 15 *(ii)* 30.

Rješenje. U primjeru 7 smo odredili sljedeće konvergente verižnog razlomka $\frac{96}{67} = [1;2,3,4,2]$:

$$\frac{P_2}{Q_2} = [1;2,3] = \frac{7}{10},$$
$$\frac{P_3}{Q_3} = [1;2,3,4] = \frac{43}{30}.$$

Prema spomenutoj tvrdnji slijedi da je $\frac{7}{10}$ najbolja aproksimacija broja $\frac{96}{67}$ s nazivnikom manjim od 30 (nazivnik iduće konvergente), pa onda i s nazivnikom manjim ili jednakim 15, dok je $\frac{43}{30}$ najbolja aproksimacija broja $\frac{96}{67}$ s nazivnikom manjim ili jednakim 30. ◀

Danas se verižni razlomci koriste i za rješavanje jedne vrste diofantskih jednadžbi, tzv. Pellovih jednadžbi, mogu se koristiti u faktorizaciji brojeva, imaju primjenu u kriptografiji ([7]), koriste se za određivanje racionalnih aproksimacija realnih brojeva ([1]), a imaju primjenu i u teoriji kaosa ([2]).

5 Zadaci za vježbu

Za kraj donosimo nekoliko zadataka za vježbu.

Zadatak 10. Dokažite da se razlomak $\frac{27449}{37813}$ ne može skratiti.

Zadatak 11. Odredite sva cjelobrojna rješenja jednadžbe $11200x - 1547y = 17$.

Zadatak 12. U skladištu se nalazi između 2 i 3 tone jabuka, te se one dijele u 9 trgovina. Prva trgovina dobije $\frac{1}{17}$ ukupne količine jabuka, druga $\frac{2}{13}$ ukupne količine, a preostali dio se jednako raspoređuje u preostalih 7 trgovina (svaka dobije "cijeli broj" kg jabuka) pri čemu u skladištu ostane 1 kg jabuka. Koliko se kilograma jabuka nalazi u skladištu?

Zadatak 13. (a) Razvijte u verižne razlomke brojeve $\frac{57}{37}$, $\frac{113}{151}$ i nađite im najbolje aproksimacije s nazivnikom manjim od 15.

(b) Nađite racionalne brojeve čiji su razvoji u verižni razlomak dani s $[0; 1, 2, 3, 4, 5, 6]$, $[2; 2, 2, 2, 1, 1, 1, 1]$.

Zadatak 14. Neka je $\alpha = [q_0; q_1, \ldots, q_{n-1}, q_n]$. Ako je $q_n = 1$ dokažite da je i $[q_0; q_1, \ldots, q_{n-1} + 1]$ razvoj broja α u verižni razlomak, a ako je $q_n \neq 1$ onda je i $[q_0; q_1, \ldots, q_{n-1}, q_n - 1, 1]$ razvoj broja α u verižni razlomak.

Literatura

[1] A. Baker, *A Comprehensive Course in Number Theory*, Cambridge University Press, New York, 2012.

[2] R. Corless, *Continued Fractions and Chaos*, `http://www.cecm.sfu.ca/organics/papers/corless/index.html`

[3] B. Dakić, Ž. Hanjš, P. Mladinić, B. Pavković, *Male teme iz matematike*, Element, Zagreb, 1994.

[4] B. Dakić, P. Mladinić, B. Pavković, *Elementarna teorija brojeva*, HMD - Element, Zagreb, 1994.

[5] A. Dujella, *Uvod u teoriju brojeva*, skripta, PMF-Matematički odjel, Zagreb, `http://web.math.pmf.unizg.hr/~duje/utb.html`

[6] A. Dujella, *Verižni razlomci i problem kalendara*, Matematika i škola, **2**(1999), 74–77.

[7] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[8] I. Matić, *Uvod u teoriju brojeva*, skripta, Odjel za matematiku, Osijek, `http://www.mathos.unios.hr/uutb`

[9] I. Matić, D. Ševerdija, *Grčko-kineski stil u teoriji brojeva*, Osječki matematički list **10**(2010), 43–58.

[10] C. D. Olds, *Continued Fractions*, Random House, New York, 1963.