Euklidov algoritam i primjene

Rengel, Maja

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Maja Rengel

Euklidov algoritam i primjene

Završni rad

Osijek, 2020.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Maja Rengel

Euklidov algoritam i primjene

Završni rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2020.

Sažetak

U ovom završnom radu bavit ćemo se promatranjem Euklidova algoritma i nekih njegovih primjena. Najprije ćemo uvesti pojmove i neke važne tvrdnje vezane uz djeljivost, doći do algoritma te pokazati primjenu na traženje najvećeg zajedničkog djelitelja danih brojeva. Nakon toga ćemo promatrati primjenu algoritma na još neke strukture.

U prvom ćemo se poglavlju baviti detaljnijim proučavanjem najvećih zajedničkih djelitelja dvaju brojeva nakon čega slijedi uvođenje Euklidova algoritma i primjena na iste. Nadalje ćemo uvesti pojam linearnih diferencijalnih jednadžbi, proširiti algoritam i pokazati njegovu primjenu na rješavanje istih. Naposlijetku, proučavat ćemo razvoj realnih brojeva u jednostavne verižne razlomke uz pomoć Euklidova algoritma te ćemo pokazati još jedan način rješavanja linearnih diofantskih jednadžbi pomoću Euklidova algoritma.

Ključne riječi

djeljivost, Euklidov algoritam, najveći zajednički djelitelj, linearne diofantske jednadže, jednostavni verižni razlomci.

The Euclidean algorithm and its applications

Summary

In this final paper, we will focus to the Euclidean algorithm and its applications. Firstly, we will introduce definitions and some important claims connected to divisibility, come to the algorithm, and show how to apply it to find the largest common divisor of a given number. After that, we will observe an application of the algorithm to few other structures.

In the first chapter, we will observe the largest common divisor of two numbers and follow it with the introduction of the Euclidean algorithm and its applications. Furthermore, we will introduce the linear diophantine equations, expand the algorithm and show how to apply it in their solving. Finally, we will consider numbers in the form of the simple continued fractions expression by using the Euclidean algorithm. Moreover, we will show one more method of solving linear diophantine equations with the help of the Euclidean algorithm.

Key words

divisibility, the Euclidean algorithm, greatest common divisor, linear diophantine equation, simple continued fractions.

Sadržaj

Uvod **i**

1 Euklidov algoritam **1**

1.1 Najveći zajednički djelitelj 1

1.2 Euklidov algoritam 4

1.3 Primjena Euklidova algoritma 5

2 Linearne diofantske jednadžbe **7**

2.1 Osnovni pojmovi linearnih diofantskih jednadžbi 7

2.2 Primjeri linearnih diofantskih jednadžbi 11

3 Verižni razlomci **14**

Literatura **19**

Uvod

Euklid (oko 330. pr. Kr. - 275. pr. Kr.) je najistaknutiji starogrčki matematičar o čijem životu se ne zna mnogo. Njegovo najznačajnije djelo je knjiga *Elementi* koja je, uz Bibliju, jedna od najprevođenijih knjiga na svijetu. *Elementi* se sastoje od 13 knjiga u kojima je Euklid obradio planimetriju, stereometriju te aritmetiku i teoriju brojeva u geometrijskom obliku. Tako je u $VII.$ i $X.$ knjizi opisao izuzetno efikasan način traženja najvećeg zajedničkog djelitelja dvaju brojeva kojeg danas nazivamo *Euklidov algoritam*. Napomenimo kako neki otkriće tog algoritma pripisuju Pitagorejcima. Poznato je, također, da su isti taj algoritam koristili indijski i kineski matematičari u 5. stoljeću.
Euklidov algoritam ima puno teorijskih i praktičnih primjena. Osim što ga koristimo za traženje najvećeg zajedničkog djelitelja dvaju brojeva, također ga koristimo i kod kraćenja razlomaka do neskrativog oblika. Primjena algoritma može se pronaći i kod rješavanja linearnih diofantskih jednadžbi, kod razvoja broja u verižni razlomak te kod pronalaženja najbolje racionalne aproksimacije realnog broja. Nadalje, Euklidov algoritam koristimo kao osnovu u dokazivanju nekih teorema u teoriji brojeva i u kriptografiji.
U originalu, algoritam je osmišljen samo za prirodne brojeve i geometrijske duljine (realni brojevi), ali u 19. stoljeću algoritam je generaliziran na sve ostale tipove brojeva kao što su Gaussovi cijeli brojevi te polinomi jedne varijable. To je dovelo do modernih algebarskih struktura poput Euklidovih domena.

Slika 1: Euklid

1 Euklidov algoritam

Problem traženja najvećeg zajedničkog djelitelja dvaju brojeva često može biti mukotrpan posao. Htjeli bismo, dakle, uvesti efikasan način njegova traženja. Tu će nam uvelike pomoći naslovni algoritam čija se primjena temelji na pronalasku tog djelitelja.

1.1 Najveći zajednički djelitelj

Najprije ćemo upoznati osnovne pojmove i tvrdnje koje ćemo, nadalje, često koristiti i koje će nam omogućiti uvođenje Euklidova algoritma.

Definicija 1. *Neka su a i b cijeli brojevi i $a \neq 0$. Kažemo da a **dijeli** b, odnosno da je b **djeljiv s** a ukoliko postoji cijeli broj c takav da je $b = a \cdot c$. Oznaka koju koristimo je $a \mid b$. Ukoliko takav c ne postoji, kažemo da a ne dijeli b (ili da b nije djeljiv s a) te označavamo s $a \nmid b$. Nadalje, ukoliko a dijeli b, kažemo da je b **višekratnik** od a te da je a **djelitelj** od b.*

Znamo da skup cijelih brojeva nije zatvoren s obzirom na operaciju dijeljenja, odnosno nije uvijek moguće podijeliti dva broja tako da rezultat bude cijeli broj. Primjerice, $14 : 3 \approx 4.67$. Kako $4.67 \notin \mathbb{Z}$, onda $3 \nmid 14$. Idući teorem proširuje shvaćanje dijeljenja kao takvog te nam predstavlja jedan korak u Euklidovom algoritmu.

Teorem 1 (Teorem o dijeljenju s ostatkom, vidjeti [1, Teorem 2.2.])**.** *Neka je $a \in \mathbb{Z}$ i $b \in \mathbb{N}$. Tada postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da je $a = b \cdot q + r$ pri čemu je $0 \leq r < b$.*

Dokaz. Označimo: $S = \{s : s = a - b \cdot k \ , \ k \in \mathbb{Z} \text{ i } s \geq 0\}$. Uočimo kako je S neprazan skup jer se u njemu nalazi element $a - b \cdot (-|a|) = a + b|a| \geq 0$. Dakle, skup S ima najmanji nenegativan element kojeg ćemo označiti s r. Kako je $r \in S$, očito postoji neki $q \in \mathbb{Z}$ za kojeg vrijedi da je $a - b \cdot q = r$, odnosno $a = b \cdot q + r$.

Nadalje, pokažimo uvjet $0 \leq r < b$. Uvjet $0 \leq r$ je očito zadovoljen samim time što je $r \in S$. Pretpostavimo sada da je $r \geq b$. Tada je $r - b \geq 0$. Uvrštavanjem dobivamo $a - b \cdot q - b = a - b \cdot (q + 1) \geq 0$ pa je očito taj element iz S. Dobili smo postojanje elementa iz S koji je manji od r, tj. $r - b < r$ što je u kontradikciji s minimalnošću elementa r. Dakle, pretpostavka $r \geq b$ nije točna i vrijedi $0 \leq r < b$.

Preostalo je pokazati jedinstvenost elemenata r i q. Pretpostavimo da uz par r i q postoji još jedan par brojeva r_1 i q_1 koji također zadovoljava $a = b \cdot q_1 + r_1$. Ako bismo pretpostavili da je $r < r_1$ dobili bismo $0 < r - r_1 < b$, odnosno $0 < a - b \cdot q - (a - b \cdot q_1) < b$ što je $0 < b \cdot (q_1 - q) < b$, a to nije moguće jer je $b \cdot (q_1 - q) > b$. Dakle, došli smo do kontradikcije. Sličnim razmatranjem dobili bismo da r ne može biti veći od r_1 te zaključujemo da je $r = r_1$ što nam dalje daje jednakost $q = q_1$. □

Napomena 1. *Broj q iz Teorema 1 nazivamo **kvocijent**, a r **ostatak** pri dijeljenju a s b. Stoga, a je djeljiv s b onda i samo onda ako je ostatak r jednak 0.*

Primjer 1.

a) Jasno je da je $14 = 7 \cdot 2$ *pa očito* $7 \mid 14$*. Uočimo kako je ostatak* $r = 0$ *što je bilo i za očekivati prema prethodnoj napomeni. Kvocijent pri dijeljenju broja* 14 *s brojem* 7 *je* $q = 2$*.*

b) Ako je $a = 49$*,* a $b = 8$*, prema prethodnom teoremu imamo* $49 = 8 \cdot 6 + 1$*, gdje je kvocijent* $q = 6$*,* a *ostatak* $r = 1$*.*

Pogledajmo sada skup S (konačan ili beskonačan) čiji su elementi cijeli brojevi koji nisu svi jednaki 0. Svaki cijeli broj d koji dijeli svaki element skupa S naziva se *zajednički djelitelj* elemenata skupa S. Kako svaki zajednički djelitelj dijeli svaki element u S, to znači da on dijeli neki $a_0 \in S$ te $|d| \leq |a_0|$. Iz toga nadalje slijedi da je skup svih zajedničkih djelitelja konačan pa među njima postoji najveći.

Definicija 2. *Neka su* $b_0, b_1, \ldots, b_n$ *cijeli brojevi koji nisu svi jednaki 0.* ***Najveći zajednički djelitelj*** *danih brojeva je najveći (po apsolutnoj vrijednosti) cijeli broj* d *za kojeg vrijedi:* $d \mid b_i$*, za svaki* $i \in \{1, 2, \ldots, n\}$ *i označavamo ga s* $(b_0, b_1, \ldots, b_n)$*.*

U literaturi možemo pronaći i druge oznake za najveći zajednički djelitelj brojeva. Neke od njih su $NZD(b_0, b_1, \ldots, b_n)$, $M(b_0, b_1, \ldots, b_n)$ te $GCD(b_0, b_1, \ldots, b_n)$.

Napomenimo kako ćemo mi u ovom radu promatrati najveći zajednički djelitelj dvaju brojeva pa ćemo, sukladno tome, pretežito koristiti oznaku (a, b).

Uočimo kako za najveći zajednički djelitelj dvaju cijelih brojeva a i b vrijedi:

$$(a, b) = (b, a) \text{ i } (a, -b) = (a, b)$$

$$(a, b) \geq 0 \text{ te } (a, 0) = a.$$

Napomenimo kako $(0, 0)$ nije definiran jer nula ima beskonačno mnogo djelitelja (ponekad se uzima $(0, 0) = 0$).

Primjerice, znamo kako je $(6, 9) = 3$. Očito je $(9, 6)$ također jednak 3, a isto tako je i $(-6, 9) = (6, -9) = (-6, -9) = 3$.

Definicija 3. *Kažemo da su cijeli brojevi* $a_0, a_1, \ldots, a_n$ ***relativno prosti*** *ukoliko je njihov najveći zajednički djelitelj jednak jedan, tj.* $(a_0, a_1, \ldots, a_n) = 1$*.*

Idući teorem će nam dati jednu važnu jednakost koju ćemo koristiti kroz gotovo cijeli rad, a njega kao takvog ćemo koristit u dokazu tvrdnje koja prethodi Euklidovom algoritmu.

Teorem 2 (vidjeti [4, Theorem 4])**.** *Neka su* a *i* b *cijeli brojevi takvi da je barem jedan od njih različit od nule. Tada je njihov najveći zajednički djelitelj najmanji pozitivan cijeli broj koji se može napisati kao suma višekratnika brojeva* a *i* b*, odnosno*

$$(a, b) = min\{a \cdot x + b \cdot y : x, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

Dokaz. Kako a i b nisu istovremeno jednaki 0, uočimo da možemo zapisati $|a| = (\pm 1)\cdot a + 0\cdot b$ ili $|b| = 0\cdot a + (\pm 1)\cdot b$. Tada je očito barem jedan od ta dva pozitivna broja element skupa $\{a\cdot x + b\cdot y : x, y \in \mathbb{Z}\} \cap \mathbb{N}$. Najmanji element toga skupa označimo s l. Dakle, l možemo prikazati kao

$$l = a\cdot x + b\cdot y,$$

gdje su x i y neki cijeli brojevi. Pokažimo da je $l = (a, b)$.
Podijelimo li a s l prema Teoremu 1 imamo $a = l\cdot q + r$, $0 \leq r < l$, odnosno

$$r = a - l\cdot q = a - a\cdot x\cdot q - b\cdot y\cdot q = a\cdot(1 - x\cdot q) + b\cdot(-y\cdot q).$$

Dakle, dobiveni pozitivan r je također suma višekratnika od a i b. Kako je $r < l$, očito je $r = 0$, odnosno $l \,|\, a$. Na sličan se način dobije $l \,|\, b$. Pretpostavimo da je $d = (a, b)$. Tada je $l \leq d$. S druge strane, kako je d zajednički djelitelj od a i b, očito $d \,|\, a$ i $d \,|\, b$ pa $d \,|\, l$. Dakle, $d \leq l$. Pokazali smo da je tada $d = l$, odnosno da je $l = (a, b)$. □

Vrijedi i poopćenje ovog teorema za cijele brojeve $a_1, a_2, \ldots, a_n$ (vidjeti [4], str. 10).

Napomena 2. *Iz prethodnog teorema slijedi da za sve cijele brojeve a i b postoje cijeli brojevi x i y takvi da je*

$$a\cdot x + b\cdot y = (a, b) \in \mathbb{N}.$$

Navedeni izraz naziva se ***Bezoutov identitet****. Specijalno, $(a, b) = 1$ ako i samo ako postoje $x, y \in \mathbb{Z}$ takvi da je $a\cdot x + b\cdot y = 1$. Osim toga, ukoliko se d može prikazati kao $d = a\cdot x + b\cdot y$, onda $(a, b) \,|\, d$.*

Primjer 2. *Neka je $a = 9$ i $b = 6$. Već smo ranije komentirali kako je $(9, 6) = 3$. Uočimo kako je $9\cdot 1 + 6\cdot(-1) = 9 - 6 = 3$, dakle pronašli smo cijele brojeve $x = 1$ i $y = -1$ koji zadovoljavaju gore navedeni identitet.*

Iduća propozicija nam predstavlja neka korisna svojstva najvećeg zajedničkog djelitelja koja ćemo, kao i ostala svojstva, prešutno koristiti u radu.

Propozicija 1 (vidjeti [1, Propozicije 2.4 i 2.5])**.** *Neka su a, b i c cijeli brojevi. Tada vrijedi sljedeće:*

a) Ako je $(a, b) = (c, b) = 1$, onda je $(a\cdot c, b) = 1$.

b) Ako $c \,|\, a\cdot b$ i $(b, c) = 1$, onda $c \,|\, a$.

c) Ako $a \,|\, b$ i $a \,|\, c$, onda $a \,|\, (b, c)$.

Dokaz. Dokaz ove propozicije može se pronaći u [1]. □

1.2 Euklidov algoritam

Problem efikasnog pronalaska najvećeg zajedničkog djelitelja dvaju brojeva, čime se bavi Euklidov algoritam, usko je povezan s problemom pronalaska cijelih brojeva x i y koji zadovoljavaju jednakost $a \cdot x + b \cdot y = (a, b)$, a čiju smo egzistenciju pokazali u Teoremu 2. Najprije ćemo dokazati tvrdnju koja će nam direktno pomoći u dokazivanju naslovnog algoritma.

Propozicija 2 (vidjeti [1, Propozicija 2.6])**.** *Neka su a, b i c cijeli brojevi. Tada vrijedi*

$$(a, b) = (a, b + a \cdot x).$$

Dokaz. Neka je $d = (a, b)$ te neka je $e = (a, a \cdot x + b)$. Prema Teoremu 2 postoje cijeli brojevi y i z takvi da je $d = a \cdot y + b \cdot z$. Dodamo li jednadžbi $\pm a \cdot x \cdot z$ dobivamo

$$d = a \cdot y - a \cdot x \cdot z + b \cdot z + a \cdot x \cdot z = a \cdot (y - x \cdot z) + (b + a \cdot x) \cdot z.$$

Očito je desna strana jednakosti djeljiva s e pa slijedi $e \mid d$. Pokažimo još da $d \mid e$. Znamo da $d \mid a$ i $d \mid b$ pa $d \mid (a \cdot x + b)$. Dakle, iz $d \mid a$ i $d \mid (a \cdot x + b)$ slijedi $d \mid (a, a \cdot x + b)$, odnosno $d \mid e$. Kako su $d, e \in \mathbb{N}$ dobivamo $d = e$. □

Napokon, nakon što smo definirali i dokazali sve potrebno, možemo iskazati i dokazati Euklidov algoritam.

Teorem 3 (Euklidov algoritam, vidjeti [3, 1.2 Euklidov algoritam])**.** *Neka su a i b cijeli brojevi. Pretpostavimo da je uzastopnom primjenom Teorema o dijeljenju s ostatkom dobiven sljedeći niz jednakosti:*

$$\begin{aligned}
b &= a \cdot q_1 + r_1, & 0 < r_1 < a \\
a &= q_2 \cdot r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= q_3 \cdot r_2 + r_3, & 0 < r_3 < r_2 \\
&\dots & \dots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} \cdot r_n.
\end{aligned}$$

Postupak završava kada dobijemo ostatak jednak nuli. Tada je $(b, a) = r_j$, odnosno jednak je posljednjem ostatku različitom od nule.

Dokaz. Potrebno je pokazati $(b, a) = r_j$.
Primjenjujući Propoziciju 2, redom dobivamo:

$$\begin{aligned}
(b, a) &= (b - a \cdot q_1, a) = (r_1, a) = (r_1, a - q_2 \cdot r_1) = (r_1, r_2) = (r_1 - q_3 \cdot r_2, r_2) \\
&= (r_3, r_2) = \dots = (r_{j-1}, r_j) = (r_{j-1} - q_{j+1} \cdot r_j, r_j) = (0, r_j) = r_j.
\end{aligned}$$

□

Napomena 3. *Uočimo da je postupak ovog algoritma konačan jer je $0 < r_j < r_{j-1} < \dots < < r_3 < r_2 < r_1 < a$.*

1.3 Primjena Euklidova algoritma

Prvenstveno se primjena algoritma temelji na traženju najvećeg zajedničkog djelitelja dvaju brojeva. Pogledajmo neke primjere.

Primjer 3. *Odredimo* $(68952, 514420)$.
Kako je

$$68952 = 2^3 \cdot 3 \cdot 13^2 \cdot 17$$
$$514420 = 2^2 \cdot 5 \cdot 17^2 \cdot 89,$$

očito je $(68952, 514420) = 2^2 \cdot 17 = 68$ *jer je to najveći broj koji dijeli oba dana broja.*

Glavna prednost Euklidova algoritma je što možemo pronaći najveći zajednički djelitelj dvaju brojeva iako ne znamo njihov rastav na proste faktore, a što ponekad može biti jako teško za odrediti.

Primjer 4. *Odredimo sada* $(68952, 514420)$ *pomoću Euklidova algoritma.*

$$514420 = 68952 \cdot 7 + 31756$$
$$68952 = 31756 \cdot 2 + 5440$$
$$31756 = 5440 \cdot 5 + 4556$$
$$5440 = 4556 \cdot 1 + 884$$
$$4556 = 884 \cdot 5 + 136$$
$$884 = 136 \cdot 6 + 68$$
$$136 = 68 \cdot 2.$$

Znamo kako je najveći zajednički djelitelj dvaju brojeva jednak posljednjem ostatku različitom od nule pa je, kako smo već ranije i izračunali, $(68952, 514420) = 68$. *Uočimo kako je ovaj postupak traženja najvećeg zajedničkog djelitelja bio jednostavniji za provesti nego postupak u prethodnom primjeru.*

Primjer 5. *Izračunajmo* $(56941, 867253)$.

$$867253 = 56941 \cdot 15 + 13138$$
$$56941 = 13138 \cdot 4 + 4389$$
$$13138 = 4389 \cdot 2 + 4360$$
$$4389 = 4360 \cdot 1 + 29$$
$$4360 = 29 \cdot 150 + 10$$
$$29 = 10 \cdot 2 + 9$$
$$10 = 9 \cdot 1 + 1$$
$$9 = 1 \cdot 9.$$

Slijedi da je $(56941, 867253) = 1$*, odnosno da su ta dva broja relativno prosta.*

Primijetimo, kada bismo htjeli riješiti ovaj primjer faktorizacijom, naišli bismo na poveće teškoće s obzirom da su oba ova broja prosta. Znamo da svaki složen broj $a = b \cdot c$ *ima faktor koji je manji ili jednak* $\sqrt{a}$*. Uzmemo li, primjerice,* 56941 *to bi značilo da taj broj trebamo pokušati podijeliti sa svim prostim brojevima manjim ili jednakim* $\sqrt{56941} \approx 238.623$*. Kako postoji* 51 *prosti broj manji od* 238 *to nam kaže da bismo morali napraviti najmanje toliko provjera da bismo utvrdili da je dani broj prost.*

Primjer 6. *Odredimo* $(92, 64)$ *te ga prikažimo kao linearnu kombinaciju višekratnika od* 92 *i* 64*.*
Koristeći direktno Euklidov algortam, redom dobivamo sljedeće jednakosti:

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

Dobivamo da je $(92, 64) = 4$*. Prikažimo ga kao linearnu kombinaciju tih brojeva.*

$$\begin{aligned} 4 &= 28 - 8 \cdot 3 = 28 - (64 - 28 \cdot 2) \cdot 3 = 28 - 64 \cdot 3 + 28 \cdot 6 = 28 \cdot 7 - 64 \cdot 3 \\ &= (92 - 64 \cdot 1) \cdot 7 - 64 \cdot 3 = 92 \cdot 7 - 64 \cdot 7 - 64 \cdot 3 = 92 \cdot 7 - 64 \cdot 10. \end{aligned}$$

Primjer 7. *Maksimalno skratimo razlomak* $\frac{155614}{104714}$*.*
Najprije primjenom Euklidova algoritma pronađimo $(155614, 104714)$*. Dobivamo:*

$$\begin{aligned} 155614 &= 104714 \cdot 1 + 50900 \\ 104714 &= 50900 \cdot 2 + 2914 \\ 50900 &= 2914 \cdot 17 + 1362 \\ 2914 &= 1362 \cdot 2 + 190 \\ 1362 &= 190 \cdot 7 + 32 \\ 190 &= 32 \cdot 5 + 30 \\ 32 &= 30 \cdot 1 + 2 \\ 30 &= 2 \cdot 15. \end{aligned}$$

Dakle, $(155614, 104714) = 2$*, tj.* 2 *dijeli oba broja pa prema definicji znamo da postoje brojevi* m_1 *i* m_2 *takvi da je*

$$\begin{aligned} 155614 &= 2 \cdot m_1 \Rightarrow m_1 = 77807 \\ 104714 &= 2 \cdot m_2 \Rightarrow m_2 = 52357. \end{aligned}$$

Supstitucijom dobivamo

$$\frac{155614}{104714} = \frac{\cancel{2} \cdot 77807}{\cancel{2} \cdot 52357} = \frac{77807}{52357}.$$

Provedbom Euklidova algoritma na brojeve 77807 *i* 52357 *dobivamo da su oni prosti, tj.* $(77807, 52357) = 1$ *odakle možemo zaključiti da je dani razlomak maksimalno skraćen.*

2 Linearne diofantske jednadžbe

Primjena Euklidova algoritma može se proširiti i na druge strukture. Prvenstveno ćemo definirati linearne diofantske jednadžbe te osnovne pojmove vezane uz njih. Pokazat ćemo neke tvrdnje o njihovim rješenjima te ćemo pokazati kako rješavati takve jednadžbe pomoću Euklidova algoritma.

2.1 Osnovni pojmovi linearnih diofantskih jednadžbi

Pogledajmo najprije što je to linearna diofantska jednadžba te nakon toga pogledajmo način kako ju povezati s Euklidovim algoritmom.

Definicija 4. *Neka je m prirodan broj te neka su a_1, a_2, ..., a_n cijeli brojevi takvi da je barem jedan od njih različit od nule. Jednadžba oblika $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n = m$ naziva se* ***linearna diofantska jednadža****.*

Uočimo kako je oblik linerane diofantske jednadže za $n = 2$ identičan Bezoutovom identitetu kojim smo se bavili u prethodnom poglavlju: $a \cdot x + b \cdot y = (a, b)$. Naime, brojeve x i y iz tog identiteta možemo efikasno izračunati primjenom Euklidova algoritma i izražavanjem svakog ostatka kao linearne kombinacije brojeva a i b. Na taj način dobivamo jedno rješenje linearne diofantske jednadžbe u kojoj su nepoznanice x i y i njega često nazivamo *partikularnim rješenjem* te jednadžbe.

Primjerice, vratimo li se kratko na Primjer 6, vidjet ćemo primjenu gore opisanog postupka, dakle u tom primjeru pripadno partikularno rješenje je $x = 7$ i $y = -10$.

Kao i kod drugih tipova jednadžbi, i kod linearnih diofantskih će nas zanimati pitanje egzistencije i jedinstvenosti njihovog rješenja. Sljedeći teorem daje nam nužan i dovoljan uvjet za rješivost linearnih diofantskih jednadžbi oblika $a \cdot x + b \cdot y = m$.

Teorem 4 (vidjeti [4, 2.2 The Diophantine equation, Theorem 1])**.** *Neka su a, b i m cijeli brojevi. Linearna diofantska jednadžba*

$$a \cdot x + b \cdot y = m \tag{1}$$

ima cjelobrojna rješenja ako i samo ako $(a, b) \mid m$.

Dokaz. Neka je $d = (a, b)$. Pretpostavimo da postoje x i y, cjelobrojna rješenja dane jednadžbe (1). Tada iz

$$a \cdot x + b \cdot y = m$$

imamo: kako $d \mid a$ i $d \mid b$, tada on dijeli cijelu lijevu stranu izraza, tj. $d \mid (a \cdot x + b \cdot y)$ pa zbog znaka jednakosti dijeli i desnu stranu, odnosno $d \mid m$.
S druge strane, pretpostavimo da $d \mid m$, tada po definiciji postoji cijeli broj k takav da je $m = d \cdot k$. Prema Teoremu 2 postoje cijeli brojevi p i q takvi da je $a \cdot p + b \cdot q = (a, b) = d$. Pomnožimo li ovu jednakost s k, dobivamo

$$a \cdot (p \cdot k) + b \cdot (q \cdot k) = d \cdot k = m.$$

Dakle, jedno cjelobrojno rješenje jednadžbe je $x = p \cdot k$ i $y = q \cdot k$. □

Proučimo neke primjere koji će nam uprizoriti način na koji koristimo prethodni teorem.

Primjer 8. *Ispitajmo ima li jednadžba* $12 \cdot x + 24 \cdot y = 16$ *cjelobrojna rješenja.*

Provedimo Euklidov algoritam kako bismo pronašli $(12, 24)$.

$$12 = 24 \cdot 0 + 12$$
$$24 = 12 \cdot 2.$$

Dakle, $(12, 24) = 12$. *Prema Teoremu 4 preostaje nam provjeriti dijeli li* $(12, 24)$ *broj* 16. *Očito,* $12 \nmid 16$ *pa nisu zadovoljeni uvjeti navedenog teorema. Prema tome, dana jednadžba nema cjelobrojnih rješenja.*

Primjer 9. *Provjerimo može li se jednadžba* $7 \cdot x + 3 \cdot y = 29$ *riješiti u skupu cijelih brojeva.*

Uvidimo kako su 7 *i* 3 *relativno prosti jer je* $(7, 3) = 1$. *Kako* $1 \mid 29$, *prema Teoremu 4 slijedi da jednadžba ima cjelobrojnih rješenja, odnsno da se može riješiti u skupu cijelih brojeva.*

Pokazali smo pod kojim uvjetom jednadžba (1) ima rješenja pa proučimo način na koji bismo ta rješenja mogli izračunati.

Napomena 4. *Rješenja linearne diofantske jednadžbe* $a \cdot x + b \cdot y = (a, b)$ *mogu se dobiti na sljedeći način. Ako je*

$$\begin{aligned} r_{-1} &= a, \quad r_0 = b, \quad r_i = r_{i-2} - q_i \cdot r_{i-1} \\ x_{-1} &= 1, \quad x_0 = 0, \quad x_i = x_{i-2} - q_i \cdot x_{i-1} \\ y_{-1} &= 0, \quad x_1 = 1, \quad y_i = y_{i-2} - q_i \cdot y_{i-1}, \end{aligned}$$

onda je $a \cdot x_i + b \cdot y_i = r_i$, *gdje je* $i \in \{-1, 0, 1, \ldots, j, j+1\}$, *a* j *je indeks posljednjeg nenul ostatka dobivenog primjenom Euklidovog algoritma na* a *i* b.
Tvrdnja je očito zadovoljena za $i = -1$ *te* $i = 0$. *Dokaz bi, nadalje, išao indukcijom jer bi obje strane jednakosti zadovoljavale istu rekurziju.*
Specijalno, vrijedi

$$a \cdot x_j + b \cdot y_j = (a, b) = r_j.$$

Svaki r_i *i* q_i *iz ove napomene dobiveni su primjenom postupka iz Euklidova algoritma.*

Kako bismo olakšali računanje rješenja linearnih diofantskih jednadžbi na način predstavljen u ovoj napomeni, koristit ćemo se tablicom koju prikazujemo u nastavku.

i	-1	0	1	2	$\cdots$	$j+1$	$\cdots$
q_i			q_1	q_2	$\cdots$	q_{j+1}	$\cdots$
x_i	$x_{-1} = 1$	$x_0 = 0$	$x_1 = 1 - q_1 \cdot 0$	$x_2 = 0 - q_2 \cdot x_1$	$\cdots$	$x_{j+1} = x_{j-1} - q_{j+1} \cdot x_j$	$\cdots$
y_i	$y_{-1} = 0$	$y_0 = 1$	$y_1 = 0 - q_1 \cdot 1$	$y_2 = 1 - q_2 \cdot y_1$	$\cdots$	$y_{j+1} = y_{j-1} - q_{j+1} \cdot y_j$	$\cdots$

Tablica 1: Prikaz postupka računanja rješenja linearne diofantske jednadžbe

Usmjerimo na nekoliko kratkih primjera u kojima ćemo vidjeti izravno korištenje postupka iz Napomene 4 i Euklidova algoritma u rješavanju linearnih diofantskih jednadžbi s dva člana.

Primjer 10. *Riješimo sljedeću jednadžbu:* $44 \cdot x + 216 \cdot y = (44, 216)$ *u skupu* $\mathbb{Z}$.

Provedimo najprije algoritam kako bismo izračunali $(44, 216)$.

$$\begin{aligned} 44 &= 216 \cdot 0 + 44 \\ 216 &= 44 \cdot 4 + 40 \\ 44 &= 40 \cdot 1 + 4 \\ 40 &= 4 \cdot 10. \end{aligned}$$

Dobivamo da je $(44, 216) = 4$. *Sada riješimo jednadžbu* $44 \cdot x + 216 \cdot y = 4$ *pomoću postupka iz Napomene 4. Ona očito ima cjelobrojna rješenja po Teoremu 4.*

i	-1	0	1	2	3
q_i			0	4	1
x_i	1	0	1	-4	5
y_i	0	1	0	1	-1

Iz prethodne tablice lako iščitamo x_3 *i* y_3 *te ih uvrstimo u polaznu jednadžbu. Imamo*

$$44 \cdot 5 + 216 \cdot (-1) = 4.$$

Dakle, $x = 5$ *i* $y = -1$ *je rješenje polazne jednadžbe.*

Verzija naslovnog algoritma koja ne računa samo najveći zajednički djelitelj brojeva, već i rješenja x i y jednadžbe $a \cdot x + b \cdot y = (a,\ b)$ naziva se **prošireni Euklidov algoritam**.

Primjer 11. *Pronađimo cijele brojeve* x *i* y *takve da je* $181 \cdot x + 94 \cdot y = 9$.

Izračunajmo $(181, 94)$.

$$\begin{aligned} 181 &= 94 \cdot 1 + 87 \\ 94 &= 87 \cdot 1 + 7 \\ 87 &= 7 \cdot 12 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3. \end{aligned}$$

Provedimo postupak iz Napomene 4 kako bismo pronašli rješenje jednadžbe

$$181 \cdot x_1 + 94 \cdot y_1 = (181, 94) = 1. \tag{2}$$

i	-1	0	1	2	3	4
q_i			1	1	12	2
x_i	1	0	1	-1	13	-27
y_i	0	1	-1	2	-25	52

Imamo $181 \cdot (-27) + 94 \cdot 52 = 1$*, odnosno jedno rješenje jednadžbe (2) je* $x_1 = -27$ *i* $y_1 = 52$*. Nadalje, kako* $(181, 94) = 1 \mid 9$ *slijedi da polazna jednadžba ima cjelobrojna rješenja, prema Teoremu 4. Njih ćemo dobiti tako što ćemo rješenja jednadžbe (2) pomnožiti s konstantom 9 (jer polaznu jednadžbu možemo dobiti iz jednadžbe (2) množenjem s tom konstantom, a u tom slučaju je* $x = x_1 \cdot 9$ *i* $y = y_1 \cdot 9$*). Rješenje polazne jednadžbe je*

$$\begin{aligned} x &= x_1 \cdot 9 = -27 \cdot 9 = -243 \\ y &= y_1 \cdot 9 = 52 \cdot 9 = 468. \end{aligned}$$

Zaista,

$$\begin{aligned} &181 \cdot x_1 + 94 \cdot y_1 = 1 \qquad / \cdot 9 \\ &181 \cdot (x_1 \cdot 9) + 94 \cdot (y_1 \cdot 9) = 9 \\ &181 \cdot (-243) + 94 \cdot 468 = 9. \end{aligned}$$

Kao što smo već spomenuli, kod jednadžbi nas zanima što više informacija o njihovim rješenjima. Iz gornjih primjera bi se moglo naslutiti kako dobivena rješenja linearne diofantske jednadžbe nisu jedinstvena, odnosno da postoji više rješenja koja bi zadovoljavala jednadžbu. Dosad smo pokazali postojanje cjelobrojnih rješenja, pokažimo sada u kojem su obliku rješenja dana i koliko ih ima.

Teorem 5 (vidjeti [1, Teorem 10.1])**.** *Neka su* a*,* b *i* m *cijeli brojevi te neka je* $d = (a, b)$*. Tada jednadžba*

$$a \cdot x + b \cdot y = m \tag{3}$$

ima beskonačno mnogo cjelobrojnih rješenja ako $d \mid m$*. Ako je uređeni par* (x_0, y_0) *jedno (partikularno) rješenje jednadžbe (3), onda su sva rješenja dana u obliku* $x = x_0 + \frac{b}{d} \cdot k$ *i* $y = y_0 - \frac{a}{d} \cdot k$*, gdje je* $k \in \mathbb{Z}$*.*

Dokaz. Pretpostavimo da $d \mid m$. Tada, prema definiciji djeljivosti, postoji cijeli broj l takav da je $m = d \cdot l$. Nadalje, prema Teoremu 2 postoje cijeli brojevi x_1 i y_1 takvi da je

$$d = a \cdot x_1 + b \cdot y_1.$$

Množenjem s l slijedi $a \cdot x_1 + b \cdot y_1 = d \cdot l = m$ pa je uređeni par $(x, y) = (x_1 \cdot l, y_1 \cdot l)$ jedno rješenje jednadžbe (3).
Neka je uređeni par (x_0, y_0) jedno rješenje od (3), odnosno neka je $a \cdot x_0 + b \cdot y_0 = m$. Neka je i uređeni par (x, y) rješenje te jednadžbe, tj. neka je $a \cdot x + b \cdot y = m$. Tada iz

$$a \cdot x + b \cdot y = m = a \cdot x_0 + b \cdot y_0$$

dobivamo $a \cdot (x - x_0) = b \cdot (y_0 - y)$, odnosno

$$\frac{a}{d} \cdot (x - x_0) = \frac{b}{d} \cdot (y_0 - y). \tag{4}$$

Kako je $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, iz jednakosti (4) slijedi da $\frac{b}{d} \mid (x - x_0)$, tj. postoji $k \in \mathbb{Z}$ takav da je $x - x_0 = \frac{b}{d} \cdot k$. Uvršatavnjem tog izraza u jednakost (4) dobivamo

$$\frac{a}{d} \cdot \frac{b}{d} \cdot k = \frac{b}{d} \cdot (y_0 - y) \iff (y_0 - y) = \frac{a}{d} \cdot k.$$

Dakle, sva rješenja jednadžbe (3) dana su sa $x = x_0 + \frac{b}{d} \cdot k$ i $y = y_0 - \frac{b}{d} \cdot k$, gdje je $k \in \mathbb{Z}$ i ima ih beskonačno mnogo. □

2.2 Primjeri linearnih diofantskih jednadžbi

Ponajprije ćemo promotriti neke "teorijske" primjere nakon čega ćemo preći na primjere primjenjive u svakodnevnom životu.

Primjer 12. *Riješimo jednadžbu* $194 \cdot x + 288 \cdot y = 8$ *u skupu cijelih brojeva.*

Ponajprije Euklidovim algoritmom pronađimo $(194, 288)$.

$$\begin{aligned} 194 &= 288 \cdot 0 + 194 \\ 288 &= 194 \cdot 1 + 94 \\ 194 &= 94 \cdot 2 + 6 \\ 94 &= 6 \cdot 15 + 4 \\ 6 &= 4 \cdot 1 + 2 \\ 4 &= 2 \cdot 2. \end{aligned}$$

Dakle, $(194, 288) = 2$. *Kako* $2 \mid 8$ *to prema Teoremu 5 ova jednadžba ima beskonačno mnogo rješenja. Izračunajmo ih. Provedimo postupak iz Napomene 4 za jednadžbu* $194 \cdot x + 288 \cdot y = 2$.

i	-1	0	1	2	3	4	5
q_i			0	1	2	15	1
x_i	1	0	1	-1	3	-46	49
y_i	0	1	0	1	-2	31	-33

Stoga, kako je $194 \cdot 49 + 288 \cdot (-33) = 2$, *množenjem s konstantom* 4 *dobivamo*

$$\begin{aligned} 194 \cdot 49 \cdot 4 + 288 \cdot (-33) \cdot 4 &= 2 \cdot 4 \\ 194 \cdot 196 + 288 \cdot (-132) &= 8. \end{aligned}$$

Partikularno rješenje polazne jednadžbe je uređeni par $(x, y) = (196, -132)$. *Sva rješenja, prema Teoremu 5, dana su s:*

$$x = 196 + 144 \cdot k, \quad y = -132 - 97 \cdot k, \quad k \in \mathbb{Z}.$$

Točnost dobivenog rješenja se lako provjeri uvrštavanjem u jednadžbu.

Primjer 13. *Za prijevoz paprike koriste se vreće od* 35 *i* 50 *kilograma. Odredimo koliko je kojih vreća potrebno da bismo prevezli* 800 *kg paprike.*

Označimo s x količinu vreća od 35 kg, a s y količinu vreća od 50 kg. Pripadna jednadžba je tada sljedećeg oblika.

$$35 \cdot x + 50 \cdot y = 800. \tag{5}$$

Uočimo kako je to baš dvočlana linearna diofantska jednadžba. Riješimo je pomoću već poznatog postupka.

$$\begin{aligned} 35 &= 50 \cdot 0 + 35 \\ 50 &= 35 \cdot 1 + 15 \\ 35 &= 15 \cdot 2 + 5 \\ 15 &= 5 \cdot 3. \end{aligned}$$

Dakle, $(35, 50) = 5$. Izračunajmo rješenja jednadžbe $35 \cdot x + 50 \cdot y = 5$ te iz njih izrazimo rješenja jednadžbe (5) koja postoje prema Teoremu 5 jer $5 \mid 800$.

i	-1	0	1	2	3
q_i			0	1	2
x_i	1	0	1	-1	3
y_i	0	1	0	1	-2

Dakle, kako je $35 \cdot 3 + 50 \cdot (-2) = 5$ to je $35 \cdot 480 + 50 \cdot (-320) = 800$ pa su pripadna rješenja dane jednadžbe (5) dana s:

$$x = 480 + 10 \cdot k, \quad y = -320 - 7 \cdot k, \quad k \in \mathbb{Z}.$$

Nas zanimaju samo rješenja u kojima su i x i y veći ili jednaki od 0. Očito je x pozitivan za svaki pozitivan k dok je y za takve k negativan. Nadalje, x će biti pozitivan (ili 0) i za $-48 \leq k \leq 0$ dok je y pozitivan za svaki $k \leq -46$. Dakle, pozitivna rješenja našeg problema su x i y za $k \in \{-46, -47, -48\}$, tj. rješenja jednadžbe (5) su uređeni parovi $(20, 2)$, $(10, 9)$ i $(0, 16)$.
Zaključujemo kako je za prijevoz 800 kg paprike potrebno koristiti ili 20 vreća od 35 kg i dvije vreće od 50 kg ili 10 vreća od 35 kg i 9 vreća od 50 kg ili samo 16 vreća od 50 kg.

Primjer 14. *Pronađimo sve prirodne brojeve koji pri dijeljenju sa 7 daju ostatak 2, a pri dijeljenju s 19 ostatak 5.*

Neka je x broj koji zadovoljava uvjete zadatka. Prema Teoremu 1 znamo da postoje cijeli brojevi k i l za koje vrijedi $x = 7 \cdot k + 2$ i $x = 19 \cdot l + 5$. Izjednačavanjem dobivamo

$$\begin{aligned} 7 \cdot k + 2 &= 19 \cdot l + 5 \\ 7 \cdot k - 19 \cdot l &= 3 \\ 7 \cdot k + 19 \cdot (-l) &= 3. \end{aligned}$$

Supstitucijom $m = -l$ dobivamo linearnu diofantsku jednadžbu:

$$7 \cdot k + 19 \cdot m = 3. \tag{6}$$

Provedimo Euklidov algoritam za brojeve 7 *i* 19*:*

$$\begin{aligned} 7 &= 19 \cdot 0 + 7 \\ 19 &= 7 \cdot 2 + 5 \\ 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2. \end{aligned}$$

Slijedi $(7, 19) = 1$*. Rješenja jednadžbe* $7 \cdot k + 19 \cdot m = 1$ *iščitamo iz sljedeće tablice:*

i	-1	0	1	2	3	4
q_i			0	2	1	2
x_i	1	0	1	-2	3	-8
y_i	0	1	0	1	-1	3

.

Imamo $7 \cdot (-8) + 19 \cdot 3 = 1$ *pa je* $7 \cdot (-24) + 19 \cdot 9 = 3$*. Sva rješenja jednadžbe (6) dana su sa:*

$$k = -24 + 19 \cdot t, \quad m = 9 - 7 \cdot t, \quad t \in \mathbb{Z}.$$

Napomenimo da za izračunavanje prirodnih brojeva koji imaju svojstva zadana u ovom primjeru moramo uvrštavati l*, a ne* m*. Vraćanjem supstitucije, imamo:* $m = -9 + 7 \cdot t,\ t \in \mathbb{Z}$*. Očito, za svaki* $t \geq 2$ *dobivamo prirodne brojeve sa zadanim svojstvima. Neki od njih su:* $100, 233, 366, 499, 632, \ldots$

Primjer 15. *Izračunajmo na koliko načina je moguće* 211 *litara mlijeka raspodijeliti u posude ukupne zapremnine* 9 *odnosno* 15 *litara.*

Označimo s x *broj posuda u koju stane* 9*, a s* y *broj posuda u koju stane* 15 *litara mlijeka. Tada se dani problem svodi na rješavanje sljedeće jednadžbe*

$$9 \cdot x + 15 \cdot y = 211.$$

Provedbom Euklidova algoritma, kao u primjerima gore, dobivamo $(9, 15) = 3$*. Kako* $3 \nmid 211$*, prema Teoremu 4, ova jednadžba nema rješenje.*
Zaključujemo kako ne postoji niti jedan način raspodijele svih 211 *litara mlijeka u posude danih zapremnina.*

3 Verižni razlomci

U ovom poglavlju prezentirat ćemo razvoj racionalnih brojeva u verižni razlomak pomoću Euklidova algoritma. Napomenimo kako je u verižni razlomak moguće razviti sve realne brojeve, no pri razvoju iracionalnih brojeva u verižni razlomak ne koristimo Euklidov algoritam.
Najprije ćemo uvesti definiciju verižnog razlomka te pogledati postupak razvijanja nekog broja u takav razlomak.

Definicija 5. *Izraz oblika*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_m}}}},$$

gdje je svaki a_i, za $i \geq 2$ kompleksan broj različit od nule naziva se ***konačan verižni razlomak****. Ako su svi a_i, osim eventualno a_1, prirodni brojevi onda se izraz naziva* ***konačan jednostavan verižni razlomak****.*

Pogledajmo, nadalje, teorem koji nam daje postupak za razvoj racionalnog broja u konačan jednostavan verižni razlomak.

Teorem 6 (vidjeti [4, 12.3 Finite continued fractions, Theorem 2])**.** *Svaki se racionalan broj može razviti u konačan jednostavan verižni razlomak.*

Dokaz. Neka je $\alpha = \frac{a}{b}$. Pretpostavimo da je $b > 0$. Primjenom Euklidova algoritma na brojeve a i b dobivamo sljedeće jednakosti:

$$\begin{aligned}
a &= b \cdot a_0 + b_0, && 0 < b_0 < b \\
b &= b_0 \cdot a_1 + b_1, && 0 < b_1 < b_0 \\
b_0 &= b_1 \cdot a_2 + b_2, && 0 < b_2 < b_1 \\
&\dots && \dots \\
b_{m-3} &= b_{m-2} \cdot a_{m-1} + b_{m-1}, && 0 < b_{m-1} < b_{m-2} \\
b_{m-2} &= b_{m-1} \cdot a_m.
\end{aligned}$$

Kako su svi b_i, $i \in \{0, 1, 2, \dots, m-1\}$ prirodni brojevi to slijedi da su brojevi $a_1, a_2, \dots, a_m$ pozitivni cijeli brojevi, tj. prirodni brojevi.

Zapisivanjem gornjih jednakosti na drugačiji, dobivamo

$$\begin{aligned}
\frac{a}{b} &= a_0 + \frac{b_0}{b} \\
\frac{b}{b_0} &= a_1 + \frac{b_1}{b_0} \\
\frac{b_0}{b_1} &= a_2 + \frac{b_2}{b_1} \\
&\vdots \\
\frac{b_{m-3}}{b_{m-2}} &= a_{m-1} + \frac{b_{m-1}}{b_{m-2}} \\
\frac{b_{m-2}}{b_{m-1}} &= a_m.
\end{aligned}$$

Višestrukom primjenom supstitucije slijedi

$$\begin{aligned}
\alpha = \frac{a}{b} = a_0 + \frac{b_0}{b} = a_0 + \frac{1}{\frac{b}{b_0}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{b_0}{b_1}}} \\
= \cdots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_m}}}.
\end{aligned} \tag{7}$$

Dakle, prikazali smo proizvoljan racionalan broj kao verižni razlomak pa slijedi da se svaki racionalan broj može zapisati u takvom obliku. □

Napomena 5. *Racionalan broj* $\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_m}}}$ *iz prethodnog teorema zapisujemo i u obliku* $\alpha = [a_0, a_1, a_2, \ldots, a_m]$ *i kažemo da je to* ***razvoj broja*** α ***u jednostavan verižni razlomak*** *.Napomenimo još jednom kako nam ovaj dokaz daje razvoj broja u verižni razlomak koristeći baš Euklidov algoritam.*

Pogledajmo jedan kratak primjer u kojem ćemo upotrijebiti postupak opisan u dokazu prethodnog teorema.

Primjer 16. *Razvijmo broj* $\frac{39}{31}$ *u verižni razlomak.*

Provedimo Euklidov algoritam nad brojevima 39 *i* 31*.*

$$\begin{aligned}
39 &= 31 \cdot 1 + 8 \\
31 &= 8 \cdot 3 + 7 \\
8 &= 7 \cdot 1 + 1 \\
7 &= 1 \cdot 7.
\end{aligned}$$

Sukladno oznakama iz Teorema 6 imamo $n = 3$ te

$$a_0 = 1$$
$$a_1 = 3$$
$$a_2 = 1$$
$$a_3 = 7.$$

Uvrstimo te oznake u krajnji izraz jednakosti (7) u dokazu Teorema 6 kako bismo provjerili dobivamo li zaista traženi broj $\frac{39}{31}$.

$$1 + \frac{1}{3 + \frac{1}{1+\frac{1}{7}}} = 1 + \frac{1}{3 + \frac{7}{8}} = 1 + \frac{8}{31} = \frac{39}{31}.$$

Prema prethodnoj napomeni, dobiveni razvoj možemo kraće pisati u obliku

$$\frac{39}{31} = [1, 3, 1, 7].$$

Prirodno je zapitati se je li takav rastav racionalnog broja jedinstven. Proučimo teorem koji će nam opisati koliko različitih razvoja u konačan jednostavan verižni razlomak ima svaki racionalan broj.

Teorem 7 (vidjeti [1, Lema 8.21])**.** *Svaki se racionalan broj koji nije cijeli može razviti u konačan jednostavan verižni razlomak na točno dva načina. Jedan je $[a_0, a_1, \ldots, a_{m-1}, a_m]$, a drugi $[a_0, a_1, \ldots, a_{m-1} - 1, 1]$, uz $m \geq 2$.*

Dokaz. Neka je $\alpha = \frac{r}{s}$, $s > 0$ i $(r, s) = 1$ te neka je dan razvoj broja α u konačan jednostavan verižni razlomak, $\alpha = [a_0, a_1, \ldots, a_m]$. Tvrdnju ćemo dokazati indukcijom po s.
Ukoliko je $s = 1$, tada je α cijeli broj. Ako je $m = 0$, onda je $\alpha = [a_0] = a_0$ pa je $\alpha = [\alpha]$. Ako je $m > 0$, onda imamo

$$\alpha = a_0 + \frac{1}{[a_1, a_2, \ldots, a_m]}$$

i $[a_1, a_2, \ldots, a_m] \geq 1$. Kako je $\alpha - a_o$ cijeli broj, to slijedi da je $[a_1, a_2, \ldots, a_m] = 1$. S obzirom da je $a_1 \geq 1$, slijedi da je $m = 1$ i $a_1 = 1$. Dobivamo $a_0 = \alpha - 1$ i $\alpha = [\alpha - 1, 1]$.
Ako je $s > 1$, onda imamo $\frac{r}{s} = a_0 + \frac{r_0}{s}$, gdje $\alpha_1 = \frac{s}{r_0}$ ima nazivnik manji od s. Prema pretpostavci indukcije, α_1 ima točno dva razvoja u jednostavan verižni razlomak, jedan oblika $[a_0, a_1, \ldots, a_{m-1} - 1, 1]$ i drugi oblika $[a_0, a_1, \ldots, a_m]$. □

Primjer 17. *Razvoj broja $\frac{39}{31}$ u verižni razlomak, prema prethodnom primjeru, dan je s*

$$\frac{39}{31} = [1, 3, 1, 7].$$

Prema Teoremu 7 dan razvoj može se zapisati i na sljedeći način $\frac{39}{31} = [1, 3, 1, 6, 1]$. Provjerimo uvrštavanjem

$$1 + \frac{1}{3 + \frac{1}{1+\frac{1}{6+\frac{1}{1}}}} = 1 + \frac{1}{3 + \frac{1}{1+\frac{1}{7}}} = 1 + \frac{1}{3 + \frac{1}{\frac{8}{7}}} = 1 + \frac{1}{3 + \frac{7}{8}} = 1 + \frac{1}{\frac{31}{8}} = 1 + \frac{8}{31} = \frac{39}{31}.$$

Dakle, pronašli smo dva različita razvoja broja $\frac{39}{31}$ u konačan jednostavan verižni razlomak.

Uvedimo sada definiciju pojma m-te konvergente koji ćemo koristiti kod rješavanja primjera vezanih uz linearne diofantske jednadžbe.

Definicija 6. *Neka je dan razvoj racionalnog broja α u konačan jednostavan verižni razlomak. Racionalan broj $\frac{p_m}{q_m} = [a_0, a_1, a_2, \ldots, a_m]$ nazivamo* ***m-ta konvergenta*** *u razvoju broja α u konačan jednostavan verižni razlomak.*

Napomena 6. *Metodom matematičke indukcije može se pokazati da brojevi p_m i q_m zadovoljavaju sljedeće rekurzivne relacije, za $m \geq 2$*

$$\begin{aligned} p_{-1} &= 1, \qquad p_0 = a_0, \qquad p_k = a_k \cdot p_{k-1} + p_{k-2} \\ q_{-1} &= 0, \qquad q_0 = 1, \qquad q_k = a_k \cdot q_{k-1} + q_{k-2} \end{aligned}$$

te da vrijedi

$$q_k \cdot p_{k-1} - p_k \cdot q_{k-1} = (-1)^k, \tag{8}$$

za svaki $k \geq 1$. Slijedi da najveći zajednički djelitelj $(p_k, q_k) = c_k$ dijeli 1 pa je $c_k = 1$, odnosno brojnici i nazivnici konvergenti su maksimalno skraćeni.

Prethodno navedena jednadžba (8) veoma sliči dvočlanoj linearnoj diofantskoj jednadžbi. Kako se Euklidov algoritam koristi i kod rješavanja takvih jednadžbi i kod razvoja broja u verižni razlomak, prirodno je zapitati se možemo li linearne diofantske jednadžbe rješavati i uz pomoć verižnih razlomaka.

Napomena 7. *Opišimo najprije na koji se način može dobiti rješenje linearne diofantske jednadžbe s dvije nepoznanice primjenom verižnih razlomaka.*
Ako je $(a, b) = 1$, iz $\frac{b}{a} = \frac{p_n}{q_n}$ dobivamo $b = p_n$ i $a = q_n$ te se za $k = n$ iz jednakosti (8) iz Napomene 6 dobiva sljedeća jednakost

$$a \cdot p_{n-1} - b \cdot q_{n-1} = (-1)^n. \tag{9}$$

Primjer 18. *Odredimo cjelobrojno rješenje linearne diofantske jednadžbe $93 \cdot x + 67 \cdot y = 17$ koristeći verižne razlomke.*
Provedimo Euklidov algoritam kako bismo pronašli najveći zajednički djelitelj $(93, 67)$

$$\begin{aligned} 93 &= 67 \cdot 1 + 26 \\ 67 &= 26 \cdot 2 + 15 \\ 26 &= 15 \cdot 1 + 11 \\ 15 &= 11 \cdot 1 + 4 \\ 11 &= 4 \cdot 2 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3. \end{aligned}$$

Dobili smo $(93, 67) = 1$*, tj. ta su dva broja relativno prosta. Kako* $1 \mid 17$ *znamo da postoje cjelobrojna rješenja dane jednadžbe.*
Razvoj broja $\frac{93}{67}$ *u konačan jednostavan verižni razlomak dan je sljedećim izrazom*

$$\frac{93}{67} = [1, 2, 1, 1, 2, 1, 3].$$

Tada je $n = 6$*. Kako je* $(93, 67) = 1$*, prema jednakosti (9) dobivamo*

$$93 \cdot p_5 - 67 \cdot q_5 = (-1)^5 = -1. \tag{10}$$

Pronađimo petu konvergentu broja $\frac{93}{67}$ *kako bismo dobili rješenje jednadžbe (10).*

$$\begin{aligned}\frac{p_5}{q_5} = [1, 2, 1, 1, 2, 1] &= 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}}}} = 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}}} \\ &= 1 + \frac{1}{2 + \frac{1}{1 + \frac{3}{4}}} = 1 + \frac{1}{2 + \frac{4}{7}} = 1 + \frac{1}{2 + \frac{4}{7}} = 1 + \frac{7}{18} = \frac{25}{18}.\end{aligned}$$

Kako je $p_5 = 18$ *i* $q_5 = 25$*, očito je*

$$93 \cdot 18 - 67 \cdot 25 = -1.$$

Množenjem prethodne jednakosti s -17 *dobivamo*

$$93 \cdot (-306) + 67 \cdot 425 = 17$$

pa vidimo kako je jedno rješenje polazne jednadžbe uređeni par $(-306, 425)$.

Dodatni primjeri i zadatci vezani uz primjene Euklidova algoritma mogu se pronaći u [2].

Literatura

[1] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[2] M. Đumić, M. Jukić Bokun, *Primjene Euklidovog algoritma*, Osječki matematički list **13**(2013), 121-137.

[3] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište Josipa Jurja Strossmayera u Osijeku, Osijek, 2015.

[4] J. E. Shockley, *Introduction to number theory*, Holt, Rinehart and Winston, INC., New York, 1967.