ACTA MATHEMATICA SPALATENSIA
Series didactica
Vol.7 (2024) 31–48
https://doi.org/10.32817/amssd.7.3

Zaprimljen: 29. listopada 2023.
Prihvaćen: 6. siječnja 2024.

Racionalna rekonstrukcija

Dragana Blagojević, Ivan Matić

Sažetak

Racionalan broj ima ili konačan ili beskonačan periodičan decimalni zapis. U radu ćemo predstaviti postupak kojim možemo, koristeći metode teorije brojeva, rekonstruirati racionalan broj koji ima beskonačan periodičan decimalni zapis iz poznavanja gornje ograde na njegov nazivnik i dovoljno mnogo prvih znamenaka u njegovom decimalnom zapisu, ali bez nužnog poznavanja čitavog dijela koji se periodično ponavlja.

Ključni pojmovi: racionalni brojevi, periodičan decimalni zapis, prošireni Euklidov algoritam

Abstract

It is well-known that a rational number has either a finite or a repeating decimal representation. We present a procedure, based on the number theory methods, which allows one the reconstruct a rational number having a repeating decimal representation from an upper bound on its denominator and a certain number of repeating digits, but not necessarily all of them.

Keywords: rational numbers, periodic decimal notation, extended Euclidean algorithm

1. Uvod

Decimalni brojevi pogodni su za izražavanje različitih veličina kakve svakodnevno pronalazimo u našem okruženju. Mnogi od njih predstavljaju vrijednosti koje se mogu izraziti i pomoću racionalnih brojeva, poput

$0.5 = \frac{1}{2}$, $4.125 = \frac{33}{8}$, $8.99 = \frac{899}{100}$, ali decimalni su zapisi prihvatljiviji u praktičnoj upotrebi. Također možemo ponekad sresti i aproksimacije, odnosno zaokruživanja, racionalnih brojeva pomoću decimalnih zapisa, u obliku poput 0.334 za $\frac{1}{3} = 0.\overline{3}$, pri čemu crtom iznad znamenke 3 označavamo njeno periodično ponavljanje. Učenici se po prvi put susreću s razlomcima i decimalnim zapisima pojedinih razlomaka u petom razredu, čime su lagano odškrinuta vrata koja vode u široki svijet decimalnih zapisa realnih brojeva.

Općenito, decimalni zapis realnog broja može biti konačan, beskonačan periodičan ili beskonačan neperiodičan. U ovom ćemo se radu posebno posvetiti decimalnim zapisima racionalnih brojeva pa ćemo najprije opisati njihovu karakterizaciju.

Propozicija 1. *Ako realan broj z ima konačan ili beskonačan periodičan decimalni zapis, tada je z racionalan broj.*

Dokaz. Pretpostavimo najprije da z ima konačan zapis oblika $z = z'.z_1 z_2 \ldots z_k$, pri čemu je $z_i \in \{0, 1, \ldots, 9\}$. Tada je

$$z = \frac{z' \cdot 10^k + z_1 \cdot 10^{k-1} + \cdots + z_k}{10^k}$$

pa je z racionalan broj.

Napomena 1. *Primijetimo da racionalan broj $z = \frac{s}{t}$, pri čemu s i t nemaju zajedničkog djelitelja većeg od 1, može imati konačan decimalni zapis jedino ako je t oblika $2^i \cdot 5^j$, za nenegativne cijele brojeve i, j.*

Neka sada z ima beskonačan periodičan decimalni zapis oblika

$$z = z'.z_1 \ldots z_k \overline{z_{k+1} \ldots z_{k+p}}$$

pri čemu je $z_i \in \{0, 1, \ldots, 9\}$ te je s $\overline{z_{k+1} \ldots z_{k+p}}$ označen dio koji se periodično ponavlja. Tada je

$$\begin{aligned}
z &= \frac{z' \cdot 10^k + z_1 \cdot 10^{k-1} + \cdots + z_k}{10^k} \\
&+ \sum_{i \geq 1} \frac{z_{k+1} \cdot 10^{p-1} + z_{k+2} \cdot 10^{p-2} + \cdots + z_{k+p}}{10^{k+i \cdot p}} \\
&= \frac{z' \cdot 10^k + z_1 \cdot 10^{k-1} + \cdots + z_k}{10^k} \\
&+ \frac{z_{k+1} \cdot 10^{p-1} + z_{k+2} \cdot 10^{p-2} + \cdots + z_{k+p}}{10^k} \sum_{i \geq 1} \frac{1}{10^{i \cdot p}} \\
&= \frac{z' \cdot 10^k + z_1 \cdot 10^{k-1} + \cdots + z_k}{10^k} \\
&+ \frac{z_{k+1} \cdot 10^{p-1} + z_{k+2} \cdot 10^{p-2} + \cdots + z_{k+p}}{10^k} \cdot \frac{\frac{1}{10^p}}{1 - \frac{1}{10^p}},
\end{aligned}$$

što je racionalan broj. □

Primjer 1. *Broj* 4.35 *možemo zapisati u obliku* $4.35 = \frac{435}{100}$, *dok broj* $4.3\overline{56}$ *možemo zapisati u obliku*

$$4.3\overline{56} = \frac{43}{10} + \sum_{i \geq 1} \frac{56}{10^{1+2i}} = \frac{43}{10} + \frac{56}{10} \cdot \sum_{i \geq 1} \frac{1}{10^{2i}} = \frac{43}{10} + \frac{56}{10} \cdot \frac{\frac{1}{100}}{1 - \frac{1}{100}} = \frac{43}{10} + \frac{56}{990}.$$

Provjerimo sada i obrat rezultata iskazanog propozicijom 1, odnosno pogledajmo što možemo reći o decimalnom zapisu racionalnog broja. Pri tome ćemo se koristiti klasičnim načinom određivanja decimalnog zapisa znamenku po znamenku. Radi se o postupku koji je baziran na jednom od fundamentalnih rezultata teorije brojeva, koji navodimo u nastavku te čiji se dokaz može naći u [2, poglavlje 1] ili u [3, poglavlje 1].

Teorem 2 (Teorem o dijeljenju s ostatkom)**.** *Neka je* a *cijeli broj i* b *prirodan broj. Tada postoje jedinstveni cijeli brojevi* q *i* r *takvi da je* $0 \leq r < b$ *i*

$$a = qb + r.$$

Također vrijedi $q = \lfloor \frac{a}{b} \rfloor$, *pri čemu je s* $\lfloor x \rfloor$ *označen najveći cijeli broj koji nije veći od* x.

Navedimo i jednu direktnu posljedicu prethodnog teorema.

Korolar 3. *Neka je* a *cijeli broj i* b *prirodan broj. Za* $r = a - \lfloor \frac{a}{b} \rfloor b$ *vrijedi* $0 \leq r < b$.

Pokažimo sada kako primjenom Teorema o dijeljenju s ostatkom odrediti oblik decimalnog zapisa racionalnog broja.

Propozicija 4. *Racionalan broj ima ili konačan ili beskonačan periodičan decimalni zapis.*

Dokaz. Neka je $z = \frac{a}{b}$. Ako je $a = 0$, tada je i $z = 0$, dok za $a < 0$ decimalni zapis od $\frac{a}{b}$ možemo dobiti kao decimalni zapis broja $-\frac{-a}{b}$ pa možemo pretpostaviti da su a i b prirodni brojevi. Neka je $z' = \lfloor \frac{a}{b} \rfloor$ te označimo sa z_i i-tu znamenku nakon decimalne točke u decimalnom zapisu broja z. Tada je

$$a = z'b + r_1$$

pri čemu je $0 \leq r_1 < b$. Ako je $r_1 = 0$, tada je z cijeli broj pa ima konačan decimalni zapis. U suprotnom, koristeći Teorem o dijeljenju s ostatkom, z_1 dobivamo kao cjelobrojni kvocijent pri dijeljenju $10 \cdot r_1$ s b, odnosno

$$10 \cdot r_1 = z_1 b + r_2,$$

gdje je $0 \leq r_2 < b$, i nastavljamo na isti način:

$$\begin{aligned} 10 \cdot r_2 &= z_2 b + r_3 \\ 10 \cdot r_3 &= z_3 b + r_4 \\ &\vdots \\ 10 \cdot r_i &= z_i b + r_{i+1} \\ &\vdots \end{aligned}$$

gdje je $0 \leq r_i < b$ za svaki i. Ako postoji k takav da je $r_{k+1} = 0$, postupak staje i dobivamo konačan decimalni zapis oblika

$$z = z'.z_1 z_2 \ldots z_k,$$

pri čemu za $j \leq k$ vrijedi $r_j \neq 0$. U suprotnom, zbog $0 \leq r_i < b$ za svaki i, slijedi da postoji j, $j > i$, takav da je $r_{i+1} = r_{j+1}$. Uzmemo li najmanji takav j, dobivamo beskonačan periodičan decimalni zapis oblika

$$z = z'.z_1 z_2 \ldots z_i \overline{z_{i+1} \ldots z_j}.$$

□

Pogledajmo postupak opisan u dokazu propozicije 4 na jednom primjeru.

Primjer 2. *Neka je* $z = \frac{39}{11}$. *Tada imamo*

$$\begin{aligned} 39 &= 3 \cdot 11 + 6 \\ 60 &= 5 \cdot 11 + 5 \\ 50 &= 4 \cdot 11 + 6 \end{aligned}$$

pa je $\frac{39}{11} = 3.\overline{54}$.

Pokazali smo da su racionalni brojevi upravo oni realni brojevi čiji je decimalni zapis ili konačan ili beskonačan periodičan. Ako su nam poznate sve znamenke u slučaju konačnog decimalnog zapisa, nije teško odrediti odgovarajući racionalan broj. Također, ukoliko se radi o beskonačnom periodičnom decimalnom zapisu te su nam poznate i sve znamenke dijela koji se periodički ponavlja i sve znamenke koje se pojavljuju prije tog dijela, odgovarajući racionalan broj možemo rekonstruirati na način prikazan u dokazu propozicije 1.

Možda donekle i neočekivano, pokazat ćemo kako u slučaju beskonačnog periodičnog zapisa odgovarajući racionalan broj $\frac{a}{b}$ možemo rekonstruirati i iz poznavanja gornje ograde na nazivnik b te poznavanja dovoljno mnogo znamenaka koje se pojavljuju u decimalnom zapisu, ali često bez nužnog poznavanja čitavog dijela koji se periodično ponavlja.

Takav postupak poznat je pod nazivom *racionalna rekonstrukcija* te ćemo prikazati kako se on može provesti korištenjem rezultata elementarne teorije brojeva.

2. Prošireni Euklidov algoritam

Najstarijim poznatim algoritmom u matematici smatra se Euklidov algoritam. Njegova je osnovna namjena određivanje najvećeg zajedničkog djelitelja prirodnih brojeva a i b, koji obično označavamo s (a, b). Radi se o postupku utemeljenom na uzastopnoj primjeni Teorema o dijeljenju s ostatkom, odnosno teorema 2, o kojem se neki detalji mogu pronaći u [1, potpoglavlje 1.2] i u [4].

U nastavku ovog poglavlja opisat ćemo proširenu varijantu Euklidova algoritma, koja će nam biti posebno važna za rekonstrukciju racionalnog broja iz nepotpunog decimalnog zapisa. Jedna od posebnih primjena postupka koji ćemo opisati jest određivanje prikaza najvećeg zajedničkog djelitelja prirodnih brojeva a i b u obliku njihove linearne kombinacije s cjelobrojnim koeficijentima.

Propozicija 5 (Prošireni Euklidov algoritam)**.** *Neka su a i b prirodni brojevi takvi da je $a \geq b$. Definiramo $r_0 := a$ i $r_1 := b$. Neka su uzastopnom primjenom Teorema o dijeljenju s ostatkom dobivene iduće jednakosti:*

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\vdots \\ r_{m-2} &= r_{m-1} q_{m-1} + r_m \\ r_{m-1} &= r_m q_m, \end{aligned}$$

pri čemu je $r_1 > r_2 > \cdots > r_m > 0$. *Tada je* $(a,b) = r_m$. *Neka je* $r_{m+1} = 0$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$ *i, za* $i \in \{2,\dots,m\}$,

$$s_{i+1} = s_{i-1} - s_i q_i, t_{i+1} = t_{i-1} - t_i q_i.$$

Tada imamo:

(i) *za* $i \in \{0,1,\dots,m+1\}$ *je* $as_i + bt_i = r_i$, *posebno* $as_m + bt_m = (a,b)$;

(ii) *za* $i \in \{0,1,\dots,m\}$ *je* $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$;

(iii) *za* $i \in \{0,1,\dots,m+1\}$ *je* $(s_i,t_i) = 1$;

(iv) *za* $i \in \{0,1,\dots,m\}$ *je* $t_i \cdot t_{i+1} \leq 0$ *i* $|t_i| \leq |t_{i+1}|$. *Za* $i \in \{1,2,\dots,m\}$ *je* $s_i \cdot s_{i+1} \leq 0$ *i* $|s_i| \leq |s_{i+1}|$;

(v) *za* $i \in \{1,2,\dots,m+1\}$ *je* $r_{i-1}|t_i| \leq a$ *i* $r_{i-1}|s_i| \leq b$;

(vi) *za* $i \in \{1,2,\dots,m+1\}$ *je* $|t_i| \leq a$ *i* $|s_i| \leq b$. *Ako je* $m \geq 3$, *tada je* $|t_m| \leq \frac{a}{2}$ *i* $|s_m| \leq \frac{b}{2}$.

Dokaz. Dokaz da je $(a,b) = r_m$ može se pronaći u [3, poglavlje 1]. Dokažimo tvrdnju (i) koristeći matematičku indukciju po i. Za $i \in \{0,1\}$ tvrdnja slijedi iz definicije od s_0, s_1, t_0 i t_1. Neka je sada $i \geq 2$ te pretpostavimo da za $j \in \{0,1,\dots,i-1\}$ vrijedi $as_j + bt_j = r_j$. Tada je

$$\begin{aligned}
as_i + bt_i &= a(s_{i-2} - s_{i-1}q_{i-1}) + b(t_{i-2} - t_{i-1}q_{i-1}) \\
&= (as_{i-2} + bt_{i-2}) - (as_{i-1} + bt_{i-1})q_{i-1} \\
&= r_{i-2} - r_{i-1}q_{i-1} \\
&= r_i
\end{aligned}$$

pa tvrdnja vrijedi za svaki $i \in \{0,1,\dots,m+1\}$.

I tvrdnju (ii) dokazat ćemo koristeći matematičku indukciju po i. Za $i = 0$ imamo $s_0 t_1 - t_0 s_1 = 1 \cdot 1 - 0 \cdot 0 = 1 = (-1)^0$. Neka je $i \geq 1$ te pretpostavimo da tvrdnja vrijedi za $i-1$, tj. da je $s_{i-1}t_i - t_{i-1}s_i = (-1)^{i-1}$. Tada je

$$\begin{aligned}
s_i t_{i+1} - t_i s_{i+1} &= s_i(t_{i-1} - t_i q_i) - t_i(s_{i-1} - s_i q_i) \\
&= s_i t_{i-1} - s_{i-1} t_i \\
&= -(s_{i-1}t_i - t_{i-1}s_i) \\
&= -(-1)^{i-1} = (-1)^i
\end{aligned}$$

pa tvrdnja vrijedi za svaki $i \in \{0,1,\dots,m+1\}$.

Neka je $i \in \{0,\dots,m+1\}$. Prema tvrdnji (ii), svaki je zajednički djelitelj brojeva s_i i t_i ujedno i djelitelj od $(-1)^i$ pa je $(s_i,t_i) = 1$, čime je dokazana tvrdnja (iii).

I u dokazu tvrdnje (iv) koristit ćemo matematičku indukciju. Vrijedi $t_0 \cdot t_1 = 0$ i $|t_0| \leq |t_1|$. Neka je $i \in \{1, 2, \ldots, m\}$ te pretpostavimo da je $t_{i-1} \cdot t_i \leq 0$. Ako je $t_i < 0$, tada je $t_{i-1} \geq 0$ te iz $t_{i+1} = t_{i-1} - t_i q_i$ i $q_i > 0$ slijedi da je $t_{i+1} > 0$. Isto tako, ako je $t_i > 0$, tada iz $t_{i-1} \leq 0$ i $t_{i+1} = t_{i-1} - t_i q_i$ slijedi $t_{i+1} < 0$. Prema tome, $t_i \cdot t_{i+1} \leq 0$.

Kako su t_{i-1} i $t_i q_i$ suprotnih predznaka, vrijedi

$$|t_{i+1}| = |t_{i-1} - t_i q_i| = |t_{i-1}| + |t_i q_i| = |t_{i-1}| + |t_i| q_i \geq |t_i|.$$

Na potpuno isti način pokazuje se da je $s_i \cdot s_{i+1} \leq 0$ te $|s_i| \leq |s_{i+1}|$ za $i \in \{1, 2, \ldots, m\}$.

Dokažimo sada tvrdnju (v). Neka je $i \in \{1, 2, \ldots, m\}$. Iz tvrdnje (i) slijedi

$$as_{i-1} + bt_{i-1} = r_{i-1} \tag{1}$$
$$as_i + bt_i = r_i. \tag{2}$$

Pomnožimo li (1) s t_i, a (2) s t_{i-1}, dobivamo

$$\begin{aligned} as_{i-1}t_i + bt_{i-1}t_i &= r_{i-1}t_i \\ as_i t_{i-1} + bt_{i-1}t_i &= r_i t_{i-1}, \end{aligned}$$

odakle slijedi

$$a(s_{i-1}t_i - s_i t_{i-1}) = r_{i-1}t_i - r_i t_{i-1}$$

pa je

$$|a| \cdot |(s_{i-1}t_i - s_i t_{i-1})| = |r_{i-1}t_i - r_i t_{i-1}|.$$

Iz $a \geq 1$ i tvrdnje (ii) dobivamo

$$a = |r_{i-1}t_i - r_i t_{i-1}|.$$

Kako su, prema (iv), t_i i t_{i-1} suprotnih predznaka te $r_i \geq 0$, $r_{i-1} \geq 0$, vrijedi

$$|r_{i-1}t_i - r_i t_{i-1}| = |r_{i-1}t_i| + |r_i t_{i-1}| = r_{i-1}|t_i| + r_i|t_{i-1}| \geq r_{i-1}|t_i|,$$

čime je dokazano $a \geq r_{i-1}|t_i|$.

Tvrdnja $b \geq r_{i-1}|s_i|$ dokazuje se na sličan način množeći jednakost (1) sa s_i i jednakost (2) sa s_{i-1}.

Preostaje dokazati tvrdnju (vi). Kako je $r_{i-1} \geq 1$ za $i \in \{1, 2, \ldots, m+1\}$, iz tvrdnje (v) slijedi $a \geq |t_i|$ i $b \geq |s_i|$. Ako je $m \geq 3$, tada iz $1 \leq r_m < r_{m-1}$ slijedi $r_{m-1} \geq 2$ te iz tvrdnje (v) dobivamo $a \geq 2|t_m|$ i $b \geq 2|s_m|$, odnosno $|t_m| \leq \frac{a}{2}$ i $|s_m| \leq \frac{b}{2}$. $\square$

Primjer 3. *Odredimo brojeve r_i, q_i, s_i, t_i koristeći prošireni Euklidov algoritam za $a = 100000$ i $b = 51655$.*

Rješenje. Najprije uzastopnom primjenom Teorema o dijeljenju s ostatkom dobivamo iduće jednakosti:

$$\begin{aligned}
100000 &= 51655 \cdot 1 + 48345 \\
51655 &= 48345 \cdot 1 + 3310 \\
48345 &= 3310 \cdot 14 + 2005 \\
3310 &= 2005 \cdot 1 + 1305 \\
2005 &= 1305 \cdot 1 + 700 \\
1305 &= 700 \cdot 1 + 605 \\
700 &= 605 \cdot 1 + 95 \\
605 &= 95 \cdot 6 + 35 \\
95 &= 35 \cdot 2 + 25 \\
35 &= 25 \cdot 1 + 10 \\
25 &= 10 \cdot 2 + 5 \\
10 &= 5 \cdot 2,
\end{aligned}$$

iz kojih slijedi da je $m = 12$, dok r_i, za $i \in \{0, 1, \ldots, 12\}$ i q_i za $i \in \{1, 2, \ldots, 12\}$ navodimo u tablici 1.

i	0	1	2	3	4	5	6	7	8	9	10	11	12
r_i	100000	51655	48345	3310	2005	1305	700	605	95	35	25	10	5
q_i		1	1	14	1	1	1	1	6	2	1	2	2

Tablica 1. Brojevi r_i, q_i.

Koristeći tablicu 1, uvrštavanjem u propoziciju 5, dobivamo s_i, t_i za $i \in \{0, 1, \ldots, 12\}$:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13
s_i	1	0	1	-1	15	-16	31	-47	78	-515	1108	-1623	4354	-10331
t_i	0	1	-1	2	-29	31	-60	91	-151	997	-2145	3142	-8429	20000

Tablica 2. Brojevi s_i, t_i.

3. Racionalna rekonstrukcija

Počnimo s rezultatom koji nam, pod odgovarajućim uvjetima, osigurava jednakost dvaju racionalnih brojeva.

Propozicija 6. *Neka su n, b, r^* i t^* cijeli brojevi takvi da je $r^* \geq 0$, $t^* > 0$ i $n > 2r^*t^*$. Ako su r, t, r' i t' cijeli brojevi takvi da je $|r| \leq r^*$, $0 < |t| \leq t^*$, $|r'| \leq r^*$, $0 < |t'| \leq t^*$ te n dijeli i $r - bt$ i $r' - bt'$, tada je $\frac{r}{t} = \frac{r'}{t'}$, odnosno $rt' - r't = 0$.*

Dokaz. Kako n dijeli $r - bt$, postoji cijeli broj x takav da je $r - bt = nx$. Također, kako n dijeli $r' - bt'$, postoji i cijeli broj y takav da je $r' - bt' = ny$. Zato je

$$n(xt' - yt) = nxt' - nyt = rt' - btt' - (r't - bt't) = rt' - r't$$

pa n dijeli i $rt' - r't$. S druge strane, imamo

$$|rt' - r't| \leq |rt'| + |r't| = |r||t'| + |r'||t| \leq r^*t^* + r^*t^* = 2r^*t^* < n.$$

Prema tome, $rt' - r't$ je višekratnik od n koji je po apsolutnoj vrijednosti manji od n pa je $rt' - r't = 0$, odnosno $rt' = r't$, odakle slijedi $\frac{r}{t} = \frac{r'}{t'}$. □

Napomena 2. *Za cijele brojeve n, b, r^* i t^* takve da je $0 < r^* \leq n < r^*t^*$ nam Thueova lema ([5, teorem 2.33]) osigurava postojanje cijelih brojeva r i t takvih da je $|r| \leq r^*$, $0 < |t| \leq t^*$ i da n dijeli $r - bt$. Prethodna nam propozicija, uz dodatni uvjet $n > 2r^*t^*$, osigurava i jedinstvenost kvocijenta $\frac{r}{t}$.*

Idući rezultat predstavlja ključni korak za rekonstrukciju racionalnog broja koji ima beskonačan periodičan decimalni zapis bez nužnog poznavanja čitavoga dijela koji se periodično ponavlja te uz poznavanje gornje ograde na nazivnik tog broja. Teorem koji ćemo iskazati i dokazati zato ponekad i nazivamo Teorem o racionalnoj rekonstrukciji ili samo Racionalna rekonstrukcija, a baziran je na Proširenom Euklidovu algoritmu.

Teorem 7 (Racionalna rekonstrukcija)**.** *Neka su n, b, r^* i t^* cijeli brojevi takvi da je $0 \leq b < n$, $0 \leq r^* < n$ i $0 < t^*$. Neka je $r_0 := n$ i $r_1 := b$ te neka su uzastopnom primjenom Teorema o dijeljenju s ostatkom dobivene jednakosti*

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 \\
r_1 &= r_2 q_2 + r_3 \\
&\vdots \\
r_{m-2} &= r_{m-1} q_{m-1} + r_m \\
r_{m-1} &= r_m q_m,
\end{aligned}$$

pri čemu je $r_1 > r_2 > \cdots > r_m > 0$. Neka je $r_{m+1} = 0$ te neka su $s_0, s_1, \ldots, s_{m+1}$ i $t_0, t_1, \ldots, t_{m+1}$ kao u iskazu propozicije 5. Označimo s

j najmanji $i \in \{0, 1, \ldots, m+1\}$ takav da je $r_i \le r^*$ te stavimo $r' := r_j$, $s' := s_j$ i $t' := t_j$. Pretpostavimo da postoje cijeli brojevi r, s, t takvi da je $r = ns + bt$, $|r| \le r^*$ i $0 < |t| \le t^*$. Tada vrijedi:

(i) $0 < |t'| \le t^*$;

(ii) *ako je $n > 2r^*t^*$, tada postoji cijeli broj q, $q \neq 0$, takav da je $r = r'q$, $s = s'q$ i $t = t'q$.*

Dokaz. Kako je $r_0 = n > r^* \ge 0 = r_{m+1}$, slijedi da je j dobro definiran, odnosno da postoji j kao u iskazu teorema. Također, vrijedi $j \ge 1$, $0 \le r_j \le r^* < r_{j-1}$ i $0 < |t_j|$. Iz pretpostavke teorema i dijela (i) propozicije 5 dobivamo

$$r = ns + bt \tag{3}$$

$$r_{j-1} = ns_{j-1} + bt_{j-1} \tag{4}$$

$$r_j = ns_j + bt_j. \tag{5}$$

Primijetimo da n dijeli i $r - bt$ i $r_j - bt_j$, jer je $r - bt = ns$ i $r_j - bt_j = ns_j$.

Neka je

$$x = s_j t_{j-1} - s_{j-1} t_j$$

$$y = \frac{t_{j-1}s - s_{j-1}t}{x}$$

$$z = \frac{s_j t - t_j s}{x}.$$

Prema dijelu (ii) propozicije 5 vrijedi $x \in \{1, -1\}$ pa su y i z cijeli brojevi. Može se provjeriti da vrijedi

$$s_j y + s_{j-1} z = s \tag{6}$$

$$t_j y + t_{j-1} z = t. \tag{7}$$

Promotrit ćemo odvojeno tri slučaja.

- Ako je $z = 0$, slijedi $t_j y = t$ pa je, zbog $t \neq 0$, $|t'| = |t_j| \le |t| \le t^*$.

- Ako je $yz < 0$, tada y i z imaju suprotne predznake, jednako kao i t_{j-1} i t_j, prema dijelu (iv) propozicije 5. No, tada $t_j y$ i $t_{j-1} z$ imaju jednake predznake pa je

$$t^* \ge |t| = |t_j y + t_{j-1} z| = |t_j y| + |t_{j-1} z| \ge |t_j y| = |t_j||y| \ge |t_j| = |t'|.$$

- Ako je $z \neq 0$ i $yz \geq 0$, množenjem jednakosti (6) s n dobivamo $ns_jy + ns_{j-1}z = ns$, dok množenjem jednakosti (7) s b dobivamo $bt_jy + bt_{j-1}z = bt$. Zbrajanjem dobivenih jednakosti slijedi redom

$$ns_jy + ns_{j-1}z + bt_jy + bt_{j-1}z = ns + bt$$
$$(ns_j + bt_j)y + (ns_{j-1} + bt_{j-1})z = ns + bt$$

pa, koristeći jednakosti (3), (4) i (5), dobivamo

$$r_jy + r_{j-1}z = r.$$

Kako iz pretpostavke $yz \geq 0$ slijedi da y i z imaju isti predznak, dobivamo $|r| = |r_jy + r_{j-1}z| = |r_jy| + |r_{j-1}z|$ pa, zbog $z \neq 0$, slijedi $|r| \geq |r_{j-1}|$. Iz $r^* \geq |r|$ slijedi $r^* \geq r_{j-1}$, što nije moguće. Prema tome, slučaj $z \neq 0$ i $yz \geq 0$ nije moguć.

Pokazali smo da je $t^* \geq |t'| > 0$ u slučaju $z = 0$ i u slučaju $yz < 0$. Također, pokazali smo i da su to jedini mogući slučajevi, čime je dokazan prvi dio teorema.

Pretpostavimo sada da vrijedi i $n > 2r^*t^*$. Iz pretpostavki teorema znamo da je $t^* \geq |t| > 0$ i $r^* \geq |r|$. Kako smo vidjeli da n dijeli i $r - bt$ i $r_j - bt_j$ te da je $r^* \geq |r'| = |r_j|$ i $t^* \geq |t_j| > 0$, ispunjene su pretpostavke propozicije 6. Zato je

$$rt_j - r_jt = 0. \tag{8}$$

Množenjem jednakosti (5) s t dobivamo

$$ns_jt + bt_jt = r_jt, \tag{9}$$

dok množenjem jednakosti (3) s t_j dobivamo

$$nst_j + bt_jt = rt_j. \tag{10}$$

Oduzimanjem jednakosti (9) od jednakosti (10) dobivamo

$$ns_jt - nst_j = r_jt - rt_j,$$

odnosno, zbog jednakosti (8),

$$n(s_jt - st_j) = 0.$$

Zato je

$$s_jt - st_j = 0. \tag{11}$$

Prema tome, $s_jt = st_j$ pa t_j dijeli s_jt. Kako je, prema dijelu (*iii*) propozicije 5, $(s_j, t_j) = 1$, slijedi da t_j dijeli t, odnosno postoji q takav da je $t = qt_j$, pa je $q \neq 0$ jer je $t \neq 0$.

Uvrstimo li $t = qt_j$ u jednakost (8), dobivamo $rt_j - r_j qt_j = 0$, odnosno $(r - r_j q)t_j = 0$ pa je $r - r_j q = 0$, odnosno $r = qr_j$.

Uvrstimo li $t = qt_j$ u jednakost (11), na isti način dobivamo i $s = qs_j$, čime je teorem dokazan. $\square$

Neka je zadan racionalan broj $z = \frac{s}{t}$, pri čemu su s i t prirodni brojevi takvi da je $s < t$. Pretpostavimo da z ima beskonačan periodičan decimalni zapis i neka je $z = 0.z_1 z_2 z_3 \ldots$, pri čemu je $z_i \in \{0, 1, \ldots, 9\}$ za svaki i. Pokazat ćemo da iz poznavanja dovoljnog broja znamenaka z_i možemo odrediti z bez nužnog poznavanja čitavog dijela koji se periodično ponavlja, ali uz još jedan potreban podatak.

Pretpostavimo da nam je poznato prvih k znamenaka nakon decimalne točke u decimalnom zapisu broja z, odnosno da znamo $z_1, z_2, \ldots, z_k$. Moguće je da se decimalni zapisi različitih racionalnih brojeva podudaraju u prvih nekoliko znamenaka, kao na primjer

$$\frac{1235}{7913} = 0.15607\ldots, \quad \frac{1235}{7911} = 0.15611\ldots$$

pa nam ne može svaki prirodan broj k biti dobar kako bismo mogli tvrditi da iz poznavanja $z_1, z_2, \ldots, z_k$ možemo odrediti $z = 0.z_1 z_2 \ldots$ U nastavku ćemo pokazati kako je dovoljno da k zadovoljava nejednakost $10^k > 2d^2$, pri čemu je d prirodan broj za koji vrijedi $t \leq d$.

Teorem 8. *Neka je $z = \frac{s}{t} = 0.z_1 z_2 \ldots$ racionalan broj koji ima beskonačan periodičan zapis. Neka su d i k prirodni brojevi za koji vrijedi $t \leq d$ i $10^k > 2d^2$. Definiramo $n = 10^k$ i*

$$b = z_1 \cdot 10^{k-1} + z_2 \cdot 10^{k-2} + \cdots + z_{k-1} \cdot 10 + z_k.$$

Neka je $r^* = t^* = d$, $r_0 = n$, $r_1 = b$ te neka su uzastopnom primjenom Teorema o dijeljenju s ostatkom dobivene jednakosti

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\vdots \\ r_{m-2} &= r_{m-1} q_{m-1} + r_m \\ r_{m-1} &= r_m q_m, \end{aligned}$$

pri čemu je $r_1 > r_2 > \cdots > r_m > 0$. Neka je $r_{m+1} = 0$, neka su s_i, t_i za $i \in \{0, 1, \ldots, m+1\}$ kao u iskazu propozicije 5 te j, r', s' i t' kao u iskazu teorema 7. Tada je

$$z = \frac{s}{t} = -\frac{s'}{t'}$$

i razlomak $\frac{s'}{t'}$ *je potpuno skraćen.*

Dokaz. Iz $n = 10^k$ i $10^k > 2d^2$ slijedi $n > d^2 \geq r^*$. Očito je i $t^* = d > 0$. Kako je

$$b = \lfloor z_1 z_2 \dots z_k . z_{k+1} z_{k+2} \dots \rfloor = \lfloor 10^k z \rfloor = \lfloor nz \rfloor = \left\lfloor \frac{ns}{t} \right\rfloor$$

iz korolara 3 slijedi da za

$$r = ns - \left\lfloor \frac{ns}{t} \right\rfloor t = ns - bt$$

odnosno

$$r = ns + b(-t)$$

vrijedi $0 \leq r < t$. Kako je $t \leq d = t^* = r^*$, slijedi $|r| \leq r^*$ i $0 < |-t| \leq t^*$ pa cijeli brojevi r, s i $-t$ ispunjavaju uvjete teorema 7. Iz $n = 10^k > 2d^2 > 2r^* t^*$ slijedi da postoji cijeli broj q, $q \neq 0$, takav da je $s = s'q$ i $-t = t'q$. Zato je

$$z = \frac{s}{t} = \frac{s'q}{-t'q} = -\frac{s'}{t'}.$$

Kako je $s' = s_j$ i $t' = t_j$, iz dijela (iii) propozicije 5 dobivamo $(s', t') = 1$ pa je razlomak $\frac{s'}{t'}$ potpuno skraćen. $\square$

Primjer 4. *Pogledajmo rezultat iskazan u prethodnom teoremu na primjeru racionalnog broja* $\frac{78}{151}$.

Rješenje. Kako 151 nije djeljiv niti s 2 niti s 5, dani racionalan broj ima beskonačan periodičan decimalni zapis. Imamo $z = \frac{78}{151}$ i $s = 78$, $t = 151$ pa možemo uzeti da je $d = 200$. Kako bi k bio što manji, uzmimo da je 10^k najmanja potencija broja 10 koja je veća od $2d^2 = 80000$, dakle $10^k = 100000$ i $k = 5$. Sada trebamo odrediti prvih pet znamenaka koje se u decimalnom zapisu broja z nalaze nakon decimalne točke. Koristeći postupak opisan u dokazu propozicije 4, dobivamo $z_1 = 5$, $z_2 = 1$, $z_3 = 6$, $z_4 = 5$ i $z_5 = 5$. Prema tome, decimalni zapis broja $z = \frac{78}{151}$ počinje s 0.51655.

Sada je $n = 100000$ i $b = 51655$. Također je i $r^* = 200$. Prošireni Euklidov algoritam za ovaj slučaj je proveden u primjeru 3 te je $m = 12$ i $r_{13} = 0$. Iz tablice 1 možemo očitati da je najmanji $i \in \{0, 1, \dots, 13\}$ takav da je $r_i \leq r^* = 200$ jednak 8. Sada nam trebaju s_8 i t_8, koji se nalaze u tablici 2. Dobivamo $s' = 78$ i $t' = -151$ pa je, zaista,

$$z = \frac{78}{151} = \frac{s}{t} = -\frac{s'}{t'} = -\frac{78}{-151}.$$

Napomenimo kako vrijedi

$$\frac{78}{151} = 0.\overline{5165562913907284768211920529801324503311258278145695364238410596026490066 22}.$$

Napomena 3. *Opisani postupak može se koristiti i za rekonstrukciju racionalnih brojeva koji imaju konačan decimalni zapis, no u konkretnim se slučajevima to često pokazuje beskorisnim. Osnovni je razlog tome broj znamenaka koje trebamo poznavati kako bismo proveli rekonstrukciju. Preciznije, ako je primjerice* $\frac{a}{b} = 0.z_1z_2\ldots z_n$ *konačan decimalni zapis racionalnog broja* $\frac{a}{b}$ *i* $d > b$*, u praksi se često događa da je najmanji prirodan broj* k *za koji vrijedi* $10^k > 2d^2$ *veći od* n *pa nam je potrebno poznavanje više znamenaka nego što ih se u decimalnom zapisu pojavljuje.*

U takvoj se situaciji konačan decimalni zapis može pretvoriti u beskonačan periodičan zapis te $\frac{a}{b} = 0.z_1z_2\ldots z_n$*, zbog* $z_n \geq 1$*, zapisati u obliku*

$$\frac{a}{b} = 0.z_1z_2\ldots z_{n-1}(z_n-1)\overline{9},$$

kao, na primjer,

$$\frac{1}{50} = 0.02 = 0.01\overline{9}.$$

Iako bismo tada uvijek mogli odrediti potrebnih k *znamenaka, one bi automatski uključivale i poznavanje čitavog dijela koji se periodično ponavlja pa postupak racionalne rekonstrukcije ne daje konkretnu prednost. Iz tog smo se razloga u teoremu 8 odlučili ograničiti na racionalne brojeve koji nemaju konačan decimalni zapis.*

Pogledajmo i jedan primjer koji je računski jednostavniji od primjera 4.

Primjer 5. *Neka je* $z = \frac{5}{14}$*. Odredimo decimalni zapis racionalnog broja* z *koristeći standardni pristup opisan u dokazu propozicije 4, a zatim rekonstruirajmo racionalan broj* z *koristeći prvih nekoliko znamenaka u decimalnom zapisu i pristup opisan teoremom 8.*

Rješenje. Kako je razlomak $\frac{5}{14}$ potpuno skraćen i 14 nije oblika $2^i \cdot 5^j$ za nenegativne cijele brojeve i, j, decimalni je zapis ovog razlomka beskonačan i periodičan. Koristeći postupak opisan u dokazu propozicije 4, dobivamo

$$\frac{5}{14} = 0.3\overline{571428}.$$

Možemo uzeti $d = r^* = 15$. Tada je $2d^2 = 450$ te iz $10^k > 2d^2$ slijedi da možemo uzeti $k = 3$. Prema tome, za rekonstrukciju su nam potrebne samo prve tri znamenke nakon decimalne točke: $3, 5, 7$. Primjenom Euklidova algoritma na brojeve $n = 1000$ i $b = 357$ dobivamo

$$\begin{aligned}1000 &= 357 \cdot 2 + 286\\ 357 &= 286 \cdot 1 + 71\\ 286 &= 71 \cdot 4 + 2\\ 71 &= 2 \cdot 35 + 1\\ 2 &= 1 \cdot 2.\end{aligned}$$

Zato je $m = 5$ te imamo

i	0	1	2	3	4	5
r_i	1000	357	286	71	2	1
q_i		2	1	4	35	2

Tablica 3. Brojevi r_i, q_i.

Dodatno je i $r_6 = 0$. Najmanji $i \in \{0, 1, \ldots, 6\}$ takav da je $r_i \leq r^* = 15$ jednak je 4. Zato trebamo odrediti s_4 i t_4. Koristeći tablicu 3 i propoziciju 5 redom imamo

$$\begin{gathered}s_0 = 1, s_1 = 0, s_2 = 1, s_3 = -1, s_4 = 5,\\ t_0 = 0, t_1 = 1, t_2 = -2, t_3 = 3, t_4 = -14\end{gathered}$$

pa je, zaista, $z = -\frac{s_4}{t_4} = -\frac{5}{-14} = \frac{5}{14}$.

Iako je decimalni zapis broja $z = \frac{5}{14}$ potpuno određen s prvih 7 znamenaka nakon decimalne točke, pokazali smo da z možemo rekonstruirati poznavajući gornju ogradu na nazivnik ovog razlomka i samo prve 3 znamenke nakon decimalne točke.

Ako je $z = \frac{s}{t}$ pozitivan racionalan broj koji ima beskonačan periodičan decimalni zapis te je $s \geq t$, možemo zapisati s u obliku $s = at + b$, pri čemu je $0 \leq b < t$. Dobivamo

$$z = \frac{s}{t} = \frac{at + b}{t} = a + \frac{b}{t}$$

i $a = \lfloor z \rfloor$. Sada možemo, iz poznavanja $\lfloor z \rfloor$ i dovoljnog broja prvih znamenaka nakon decimalne točke, rekonstruirati racionalan broj z.

Ilustrirajmo i ovaj postupak jednim primjerom.

Primjer 6. *Marko kaže Darku: ,,Zamisli pozitivan racionalan broj* $\frac{s}{t}$ *koji ima beskonačan periodičan decimalni zapis. Dovoljno je da razlomak* $\frac{s}{t}$ *bude potpuno skraćen i da* t *ima prost djelitelj različit od* 2 *i* 5*". ,,U redu, zamislio sam!" kaže Darko. ,,Sad mi reci neki prirodan broj koji je veći od* t*", nastavi Marko. ,,Evo, na primjer,* 300*", odgovori Darko nakon kraćeg razmišljanja. ,,U redu, ako mi kažeš početak decimalnog zapisa broja* $\frac{s}{t}$*, koji sadrži prvih* 6 *znamenaka nakon decimalne točke, reći ću ti koji broj si zamislio", nastavi Marko. ,,Ako ti tako kažeš. Početak je* 1.653284*, ali ne vidim kako ti to pomaže", zbunjeno će Darko. Kako će Marko odrediti broj koji je Darko zamislio?*

Rješenje. Kako je $\lfloor \frac{s}{t} \rfloor = 1$, imamo $\frac{s}{t} = 1 + \frac{s'}{t}$ pri čemu je $s' < t$ i decimalni zapis broja $\frac{s'}{t}$ počinje s 0.653284. Koristeći postupak opisan teoremom 8, Marko određuje $\frac{s'}{t}$. Iz $d = 300$, Marko je izračunao $2d^2 = 180000$ te odmah zaključio da može uzeti $k = 6$. Sada je $n = 1000000$ i $b = 653284$. Euklidov algoritam primijenjen na ove brojeve daje

$$\begin{aligned}
1000000 &= 653284 \cdot 1 + 346716\\
653284 &= 346716 \cdot 1 + 306568\\
346716 &= 306568 \cdot 1 + 40148\\
306568 &= 40148 \cdot 7 + 25532\\
40148 &= 25532 \cdot 1 + 14616\\
25532 &= 14616 \cdot 1 + 10916\\
14616 &= 10916 \cdot 1 + 3700\\
10916 &= 3700 \cdot 2 + 3516\\
3700 &= 3516 \cdot 1 + 184\\
3516 &= 184 \cdot 19 + 20\\
184 &= 20 \cdot 9 + 4\\
20 &= 4 \cdot 5,
\end{aligned}$$

odakle je

i	0	1	2	3	4	5
r_i	1000000	653284	346716	306568	40148	25532
q_i		1	1	1	7	1

Tablica 4.

Sada je $m = 12$ i najmanji $i \in \{0, 1, \ldots, 13\}$ takav da je $r_i \leq r^* = 300$ jest 10. Prema tome, tražimo s_{10} i t_{10}. Iz tablice 5 i propozicije 5 redom

i	6	7	8	9	10	11	12
r_i	14616	10916	3700	3516	184	20	4
q_i	1	1	2	1	19	9	5

Tablica 5. Brojevi r_i, q_i.

dobivamo

$$s_0 = 1, s_1 = 0, s_2 = 1, s_3 = -1, s_4 = 2, s_5 = -15, s_6 = 17, s_7 = -32,$$
$$s_8 = 49, s_9 = -130, s_{10} = 179,$$
$$t_0 = 0, t_1 = 1, t_2 = -1, t_3 = 2, t_4 = -3, t_5 = 23, t_6 = -26, t_7 = 49,$$
$$t_8 = -75, t_9 = 199, t_{10} = -274.$$

Sada je $\frac{s'}{t} = -\frac{179}{-274} = \frac{179}{274}$, odakle je

$$\frac{s}{t} = 1 + \frac{s'}{t} = 1 + \frac{179}{274} = \frac{453}{274}.$$

Darko je zamislio broj $\frac{453}{274}$. Napomenimo kako vrijedi

$$\frac{453}{274} = 1.6\overline{53284671}.$$

Literatura

[1] D. Blagojević, *Euklidov algoritam*, Diplomski rad, Fakultet primijenjene matematike i informatike, Sveučilište u Osijeku, 2023.

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

[3] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište u Osijeku, 2014.

[4] I. Matić, D. Ševerdija, *Grčko-kineski stil u teoriji brojeva*, Osječki matematički list, 10(2010), 43-57

[5] V. Shoup, *A computational introduction to number theory and algebra*, Cambridge University Press, Cambridge, 2009.

Dragana Blagojević
Fakultet primijenjene matematike i informatike, Sveučilište J. J. Strossmayera u Osijeku

E-mail: dblagoje@mathos.hr

Ivan Matić
Fakultet primijenjene matematike i informatike, Sveučilište J. J. Strossmayera u Osijeku
E-mail: imatic@mathos.hr