UNIVERZITET U BEOGRADU
MATEMATIČKI FAKULTET
BEOGRAD

Lidija Sabadoš

Verižni razlomci kvadratičnih brojeva

-master rad-

Mentor:
Prof. dr. Goran Đanković

2021, Beograd

Sadržaj

1 Uvod

Da bismo otkrili ili videli nešto neobično, tajanastveno, često mislimo da moramo otići daleko, ali da li je to zaista tako? U velikoj smo zabludi ako mislimo da je sve u našoj okolini poznato. Okruženi smo mnogim nepoznatim i neispitanim pojavama, ali tome ne posvećujemo dovoljnu pažnju.

Ovaj master rad će se baviti konačnim i beskonačnim verižnim razlomcima. Navedena su neka osnovna svojstva i definicije o verižnim razlomcima i njihovim parcijalnim konvergentima, razvoj u verižne razlomke iracionalnih brojeva, periodični verižni razlomci, kao i razvoj u verižne razlomke kvadratičnih brojeva. Zatim, cilj je da prikažem alogaritam za računanje verižnih razvoja kvadratičnih brojeva. Kao vrhunac rada ću opisati jedinice u prstenima celih kvadratičnih polja, kao i fundamentalne jedinice.

U samim počecima matematike razvija se pojam **verižnih razlomaka**. Iako su se mnogi matematičari bavili verižnim razlomcima, smatra se da najviše zasluga pripisujemo Euklidu,[1] čiji algoritam danas upotrebljavamo prilikom raspisa racionalnog broja u verižni razlomak. U njegovom algoritmu dolazimo do najvećeg zajedničkog delitelja dva prirodna broja. Kasnije su se verižni razlomci koristili za rešavanje nekih matematičkih problema, ali samo u konkretnim primerima. 19. vek je bio zlatno doba za verižne razlomke. Teorija o njima se znatno proširila.

Verižni razlomci brzo konvergiraju pa se koriste za aproksimaciju realnih brojeva razlomkom, za izračunavanje decimala broja π i drugih iracionalnih brojeva. Koristimo ih još kod rešavanja diofantskih jednačina, u kriptografiji itd. Primena verižnih razlomaka je velika. Prvi koji je uveo stepenasto zapisivanje razlomka je prvi predsednik britanske Kraljevske akademije William Brouncker[2] Prvi koji je koristio izraz **„continued fraction”** je Johm Wallis[3]. On je započeo proučavanje i generalizaciju teorije verižnih razlomaka, i tek posle njega je porastao interes za proučavanjem i razvijanjem. Indijski matematičar Aryabhata[4] je koristio verižne razlomke za rešavanje neodređenih linearnih jednačina.

[1] Euklid (oko 300. p.n.e.)- antički matematičar poznat po delima Elementi, Data, Optika... Često ga nazivamo ocem geometrije.

[2] William Brouncker (1620-1684.) - engleski matematičar

[3] Johm Wallis (1616-1703.) - engleski sveštenik i matematičar.

[4] Aryabhata (476. n.e.- 550. n.e.) - indijski matematičar i astronom, prvi iz klasičnog perioda indijske matematike i astronomije

2 Verižni razlomci

Znamo da je Arhimed[5] našao za broj π približnu vrednost 22/7. Na tu činjenicu smo navikli, videli smo u različitim knjigama, pa i ne razmišljamo o tajni koja je tu skrivena. Zašto je Arhimed uzeo baš sedmine? Zašto nije, na primer, šestine, devetine? Pitanje je veoma zanimljivo, a odgovor se zasniva na pojmu i osobinama verižnog razlomka.

Kada pišemo $\pi = 3.141592...$ zaista mislimo da je π aproksimirano racionalnim brojem $3.141592 = \frac{3141592}{1000000}$. Ova aproksimacija zahteva i veliki imenilac i veliki brojilac za tačno davanje prvih šest decimalnih mesta broja π. Možemo postići istu preciznost sa kraćim razlomkom

$$\frac{355}{113} = 3.14159292035\ldots$$

Ovu aproksimaciju sa veoma malom greškom koja iznosi samo 0.0000085% je otkrio kineski matematičar Zu Chongnzi[6] u XV veku. Teorija o verižnim razlomcima daje efikasni metod aproksimacije realnih brojeva racionalnim brojevima. Gruba aproksimacija $\eta \in \mathbb{R}$ je data najvećim celim brojem, ne većim od η. Zove se **najveći ceo deo broja** η, označavamo $\lfloor \eta \rfloor$, a za njega je karakteristično

$$\lfloor \eta \rfloor \in \mathbb{Z}, \quad 0 \le \eta - \lfloor \eta \rfloor < 1.$$

Primer 2.1 *U ovom primeru pokazujemo ilustraciju postupka:*

$$\pi = 3 + \frac{1}{\frac{1}{0.141\ldots}} = 3 + \frac{1}{7.062\ldots} = 3 + \frac{1}{7 + \frac{1}{\frac{1}{0.062\ldots}}} = 3 + \frac{1}{7 + \frac{1}{15.997\ldots}}$$

$$= 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{\frac{1}{0.997\ldots}}}} = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1.003\ldots}}} = \ldots$$

Zaokrugljivanje poslednjeg imenitelja na 1 ne menja vrednost izraza previše, i dobijamo:

$$\pi \approx 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1}}} = \frac{355}{113}$$

Niz celih brojeva 3,7,15,1,... nazivamo nizom verižnog razlomka asociranim sa π. ∎

Računanje u prethodnom primeru nam pokazuje opšti primer kako realnim brojevima dodeljujemo niz.

[5] Arhimed (287.p.n.e - 212. p.n.e.) - starogrčki matematičar, fizičar i astronom iz Sirakuze.
[6] Zu Chongnzi(429.n.e - 500. n.e.) - kineski matematičar, političar, izumitelj i pisac.

Postupak za verižne razlomke

1. $\eta \in \mathbb{R}$. Napišemo $\eta_0 := \eta$ i fiksiramo brojač $i := 0$.
2. Stavimo $a_i := \lfloor \eta_i \rfloor$. Napišemo a_i i nastavljamo.
3. Ako je $a_i = \eta_i$, završavamo.
4. Inače, stavljamo $\eta_{i+1} := \frac{1}{\eta_i - a_i}$, povećamo brojač $i := i + 1$, i vraćamo se na korak 2.

3 Konačni i beskonačni verižni razlomci

Možemo proizvoljan verižni razlomak pretvoriti u realan broj. Definišemo prvo konačan niz verižnog razlomka. Razmatramo niz $\{a_i\}$ realnih brojeva, gde su $a_i > 0,\ i \geq 1$.

Definicija 3.1 ***Konačan verižni razlomak*** *sa članovima* $a_0, a_1, \ldots, a_k$ *je izraz*

$$[a_0, a_1, \ldots, a_k] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots_{a_{k-1} + \frac{1}{a_k}}}}}$$

Kada računamo $[a_0, \ldots, a_k]$ nikada ne delimo nulom. Svaki racionalan broj se može zapisati u obliku jednostavnog konačnog verižnog razlomka sa elementima iz $\mathbb{Z}$. To zovemo razvoj broja u verižni razlomak.

Primer 3.1 *Verižnim razlomcima* (a) $[2, 1, 5, 8]$ *i* (b) $[0, 27, 12, 42]$ *odgovaraju sledeći racionalni brojevi:*

(a) $[2, 1, 5, 8] = 2 + \frac{1}{1+\frac{1}{5+\frac{1}{8}}} = 2 + \frac{1}{1+\frac{1}{\frac{41}{8}}} = 2 + \frac{1}{\frac{49}{41}} = 2 + \frac{41}{49} = \frac{139}{49}$

(b) $[0, 27, 12, 42] = \frac{1}{27+\frac{1}{12+\frac{1}{42}}} = \frac{1}{27+\frac{1}{\frac{505}{42}}} = \frac{1}{27+\frac{42}{505}} = \frac{1}{\frac{13677}{505}} = \frac{505}{13677}$ ■

Primer 3.2 *Racionalne brojeve (a)* $\frac{35}{13}$*, (b)* $\frac{126}{443}$ *predstaviti u obliku verižnog razlomka.*

(a) Da bi našli verižni razlomak za $35/13$*, više puta primenimo alogaritam deljenja:*

$$\frac{35}{13} = \frac{2 \cdot 13 + 9}{13} = 2 + \frac{9}{13} = 2 + \frac{1}{\frac{13}{9}} = 2 + \frac{1}{1 + \frac{4}{9}} = 2 + \frac{1}{1 + \frac{1}{\frac{9}{4}}} = 2 + \frac{1}{1 + \frac{1}{2+\frac{1}{4}}}$$

Dobiveni niz jednakosti možemo zapisati na sledeći način, $\frac{35}{13} = [2, 1, 2, 4]$.

(b) Na isti način nalazimo:

$$\frac{126}{443} = \frac{1}{\frac{443}{126}} = \frac{1}{3 + \frac{65}{126}} = \frac{1}{3 + \frac{1}{\frac{126}{65}}} = \frac{1}{3 + \frac{1}{1+\frac{61}{65}}} = \frac{1}{3 + \frac{1}{1+\frac{1}{\frac{65}{61}}}}$$

$$= \frac{1}{3 + \frac{1}{1+\frac{1}{1+\frac{4}{61}}}} = \frac{1}{3 + \frac{1}{1+\frac{1}{1+\frac{1}{\frac{61}{4}}}}} = \frac{1}{3 + \frac{1}{1+\frac{1}{1+\frac{1}{15+\frac{1}{4}}}}}$$

Dobili smo $\frac{126}{443} = [0, 3, 1, 1, 15, 4]$. ■

Primetimo da je zapis svakog „pravog" razlomka, razlomka kome je imenilac veći od brojioca oblika $[0, a_1, \ldots, a_n]$.

Primer 3.3 *(a) Vrednost razlomka je veća od 1.*

$$\frac{67}{29} = 2 + \frac{1}{3 + \frac{1}{4+\frac{1}{2}}}.$$

(b) Ako je vrednost razlomka manja od 1 imamo

$$\frac{29}{67} = 0 + \frac{1}{2 + \frac{1}{3+\frac{1}{4+\frac{1}{2}}}}.$$

. ■

Ako je racionalan broj $\frac{a}{b}$ negativan, onda verižne razlomke koji odgovaraju datom razlomku možemo naći na dva načina.

I način Sastoji se u tome da se prvo razloži u verižni razlomak broj $-\frac{a}{b}$, i zatim se ispred dobijenog verižnog razlomka stavi znak $-$. Tako je, na primer,

$$\frac{61}{27} = 2 + \frac{7}{27} = 2 + \frac{1}{\frac{27}{7}} = 2 + \frac{1}{3 + \frac{6}{7}} = 2 + \frac{1}{3 + \frac{1}{\frac{7}{6}}} = 2 + \frac{1}{3 + \frac{1}{1+\frac{1}{6}}}$$

Dobijamo: -[2,3,1,6].

II način Sastoji se u tome da elemenat a_0 verižnog razlomka $[a_0, a_1, a_2, \ldots, a_n]$ bude negativan, a ostali elementi $a_1, a_2, \ldots, a_n$ pozitivni. Na primer,

$$-\frac{61}{27} = -3+\frac{20}{27} = -3+\frac{1}{\frac{27}{20}} = -3+\frac{1}{1 + \frac{7}{20}} = -3+\frac{1}{1 + \frac{1}{\frac{20}{7}}} = -3+\frac{1}{1 + \frac{1}{2+\frac{6}{7}}}$$

$$= -3 + \frac{1}{1 + \frac{1}{2+\frac{1}{\frac{7}{6}}}} = -3 + \frac{1}{1 + \frac{1}{2+\frac{1}{1+\frac{1}{6}}}}$$

Dobijamo: [-3,1,2,1,6].

Definicija 3.2 *Neka je $\eta = [a_0, a_1, \ldots, a_n]$. Svaki racionalan broj za $i \leq n$, $\frac{p_i}{q_i} = [a_0, a_1, \ldots, a_i]$ zovemo **i-ta konvergenta** od η.*

Primer 3.4 *Posmatrajmo prošli primer,* 35/13. *Osim* $[2, 1, 2, 4]$ *konvergente su*

$$[2] = 2, \qquad [2, 1] = 2 + \frac{1}{1} = 3, \qquad [2, 1, 2] = 2 + \frac{1}{\frac{3}{2}} = 2 + \frac{2}{3} = \frac{8}{3}.$$

. ■

Nakon što se izračuna a_i koristeći rekurzivni razvoj broja u verižni razlomak, nije iznenađujuće da postoji rekurzivna formula za brojilac i imenilac konvergenata.

Propozicija 3.1 *Neka su nizovi* $\{p_i\}, \{q_i\}, za-2 \leq i$ *definisani sa*

$$p_{-2}=0, \quad p_{-1}=1, \qquad p_{i+1}=a_{i+1}p_i+p_{i-1},$$

$$q_{-2}=1, \quad q_{-1}=0, \qquad q_{i+1}=a_{i+1}q_i+q_{i-1},$$

Tada $[a_0,\dots,a_i]=\frac{p_i}{q_i}$.

Vrednosti p_i i q_i zavise samo od $a_0,\dots,a_i$, pošto a_j, gde je $j>i$ ne ulazi u njihovo računanje. Kada želimo da naglasimo tu činjenicu, pišemo $p_i(a_0,\dots,a_i)$ umesto p_i.

Dokaz 3.1 Dokazujemo matematičkom indukcijom.
Za $p_0=a_0$ i $q_0=1$ baza indukcije je trivijalna.
Indukcijski korak: Pretpostavimo da je jednakost tačna do $j-tog$ konvergenta bilo kog niza a_i koji zadovoljava $a_i\in\mathbb{R}, a_i>0$, za $i>1$, naročito desne strane jednakosti

$$[a_0,a_1,\dots,a_{j-1},a_j,a_{j+1}]=\left[a_0,a_1,\dots,a_{j-1},a_j+\frac{1}{a_{j+1}}\right].$$

Neka brojevi p_i,q_i budu definisani kao gore, i p_i',q_i' odgovarajući brojevi desne strane. Pošto su elementi od 0 do $j-1$ sa obe strane jednakosti jednaki, odgovarajući konvergenti su isti: $p_i=p_i'$, $q_i=q_i'$ za sve $0\leq i\leq j-1$. Tako dobijamo

$$[a_0,\dots,a_{j+1}]=\left[a_0,\dots,a_j+\frac{1}{a_{j+1}}\right]=\frac{\left(a_j+\frac{1}{a_{j+1}}\right)p_{j-1}'+p_{j-2}'}{\left(a_j+\frac{1}{a_{j+1}}\right)q_{j-1}'+q_{j-2}'}=$$

$$=\frac{\left(a_j+\frac{1}{a_{j+1}}\right)p_{j-1}+p_{j-2}}{\left(a_j+\frac{1}{a_{j+1}}\right)q_{j-1}+q_{j-2}}=\frac{a_{j+1}(a_jp_{j-1}+p_{j-2})+p_{j-1}}{a_{j+1}(a_jq_{j-1}+q_{j-2})+q_{j-1}}=$$

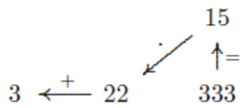
$$=\frac{a_{j+1}p_j+p_{j-1}}{a_{j+1}q_j+q_{j+1}}=\frac{p_{j+1}}{g_{j+1}}.$$

$\blacksquare$.

Primer 3.5 *Koristimo niz verižnog razlomka broja π. Prva četiri člana koja smo izračunali u primeru 2.1 ilustruju pogodan način tabelarnog prikazivanja konvergenata verižnog razlomka:*

i	-2	-1	0	1	2	3	4	5	...
a_i	-	-	3	7	15	1	292	1	...
p_i	0	1	3	22	333	335	103993	104348	...
q_i	1	0	1	7	106	113	33102	33215	...

Počinjemo tako što u kolone numerisane sa -2 i -1 upišemo $\begin{bmatrix}0\\1\end{bmatrix}$ i $\begin{bmatrix}1\\0\end{bmatrix}$ i nastavimo pisati niz verižnog razlomka do kraja. Redove popunjavamo na sledeći način:



$333 = 15 \cdot 22 + 3.$

Čitanje duž strelica daje rekurziju. Ovaj metod izračunava i p_i i q_i, jer se njihova rekurzija razlikuje samo u početnim uslovima. ■

Primer 3.6 *Razvoj broja $\frac{120}{49}$ u verižni razlomak je sledeći:*

$$\frac{120}{49} = 2 + \frac{22}{49} = 2 + \frac{1}{\frac{49}{22}} = 2 + \frac{1}{2 + \frac{5}{22}} = 2 + \frac{1}{2 + \frac{1}{\frac{22}{5}}} = 2 + \frac{1}{2 + \frac{1}{4 + \frac{2}{5}}}$$

$$= 2 + \frac{1}{2 + \frac{1}{4 + \frac{1}{\frac{5}{2}}}} = 2 + \frac{1}{2 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2}}}}$$

Imamo $[2, 2, 4, 2, 2] = [a_0, a_1, a_2, a_3, a_4]$ i kreiramo tablicu

n	-2	-1	0	1	2	3	4
a_n	-	-	2	2	4	2	2
p_n	0	1	2	5	22	49	120
q_n	1	0	1	2	9	20	49

Za svaki $k = 0, \ldots, n$, p_k dobijamo tako što a_k pomnožimo sa p_{k-1} i saberemo sa p_{k-2}. Analogno dobijamo q_k. Uočimo još da je

$$p_{-1}q_{-2} - p_{-2}q_{-1} = 1 \cdot 1 - 0 \cdot 0 = 1$$

$$p_0q_{-1} - p_{-1}q_0 = 2 \cdot 0 - 1 \cdot 1 = -1$$

$$p_1q_0 - p_0q_1 = 5 \cdot 1 - 2 \cdot 2 = 1$$

$$p_2q_1 - p_1q_2 = 22 \cdot 2 - 5 \cdot 9 = -1$$

$$\vdots$$

■

Posledica 3.1 *Konvergenti p_i/q_i zadovoljavaju sledeće:*

(a) $$p_{-2} = 0, \quad p_{-1} = 1, \qquad p_{i+1} = a_{i+1}p_i + p_{i-1},$$

$$q_{-2} = 1, \quad q_{-1} = 0, \qquad q_{i+1} = a_{i+1}q_i + q_{i-1}.$$

Ovo možemo zapisati u matričnom obliku: $M_{i+1} = M_iA_{i+1}$, *gde* $M_{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, M_i = \begin{bmatrix} p_{i-1} & p_i \\ q_{i-1} & q_i \end{bmatrix}, A_i = \begin{bmatrix} 0 & 1 \\ 1 & a_i \end{bmatrix}$.

(b) *Za sve i imamo* $p_{i-1}q_i - p_i q_{i-1} = (-1)^i$. *Specijalno kada je* $\{a_i\}$ *niz verižnog razlomka* ($a_i \in \mathbb{Z}$), *imamo* $nzd(p_i, q_i) = 1$.

(c) *Neka su* $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$, *konvergente verižnog razlomka. Tada za paran* $k \geq 0$ *i neparan* $l \geq 1$ *važi:*

$$\frac{p_k}{q_k} < \frac{p_{k+2}}{q_{k+2}},$$
$$\frac{p_{l+2}}{q_{l+2}} < \frac{p_l}{q_l},$$
$$\frac{p_k}{q_k} < \frac{p_l}{q_l}.$$

Odnosno,

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots \frac{p_{2k}}{q_{2k}} < \ldots < \frac{p_{2k+1}}{q_{2k+1}} < \ldots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

Dokaz 3.1 (a) Pomnožimo matrice.

$$M_i A_{i+1} = \begin{bmatrix} p_{i-1} & p_i \\ q_{i-1} & q_i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & a_{i+1} \end{bmatrix} = \begin{bmatrix} p_i & p_{i-1} + p_i a_{i+1} \\ q_i & q_{i-1} + q_i a_{i+1} \end{bmatrix} = \begin{bmatrix} p_i & p_{i+1} \\ q_i & q_{i+1} \end{bmatrix}$$

(b) Dokazujemo indukcijom. Prvo proverimo dva osnovna slučaja, $i = 1$ i $i = 2$. Uzimajući determinantu $M_{i+1} = M_i A_{i+1}$ dobijamo $p_i q_{i+1} - p_{i+1} q_i = -(p_{i-1} q_i - p_i q_{i-1})$, tako da (b) sledi iz baze indukcije $\det M_{-1} = -1$.

(c) Računamo

$$\frac{p_{i+2}}{q_{i+2}} - \frac{p_i}{q_i} = \frac{(-1)^i a_{i+2}}{q_i q_{i+2}}.$$

S obzirom da je $a_i > 0$ *za* $i > 0$, imamo $p_0/q_0 < p_2/q_2 < \ldots$ i $\ldots < p_3/q_3 < p_1/q_1$. Da bismo spojili dva niza nejednakosti zajedno, posmatramo

$$\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i} = \frac{p_{i+1}q_i - p_i q_{i+1}}{q_{i+1}q_i} = \frac{(-1)^i}{q_{i+1}q_i}$$

tako da $p_{2i}/q_{2i} < p_{2i+1}/q_{2i+1} < p_{2j+1}/q_{2j+1}$ za svako $i > j \geq 0$. ■

Sada se okrećemo definisanju beskonačnih verižnih razlomaka.Videli smo u primerima da konvergenti $[3, 7, 15, 1, \ldots]$ daju sve bližu i bližu aproksimaciju broja π. Ovo sugeriše definisanje beskonačnog verižnog razlomka kao limes konačnih konvergenata.

Propozicija 3.2 *Kada je* $a_0, a_1, a_2 \ldots$ *beskonačan niz verižnog razlomka, limes*

$$\lim_{i \to \infty} [a_0, a_1, \ldots, a_i]$$

postoji i iracionalan je. Označavamo sa $[a_0, a_i, \ldots]$ *i nazivamo* ***beskonačni verižni razlomak*** *sa* ***elementima*** $a_0, a_1, \ldots$ *i to je izraz oblika:*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

Dokaz 3.2 Iz posledice 3.1 (c) ovde je niz umetnutih intervala

$$\left[\frac{p_0}{q_0}, \frac{p_1}{q_1}\right] \supset \left[\frac{p_2}{q_2}, \frac{p_3}{q_3}\right] \supset \left[\frac{p_4}{q_4}, \frac{p_5}{q_5}\right] \supset \dots$$

Neka η pripada njihovom preseku, koji nije prazan. Upoređujući rastojanja od p_i/q_i do η i p_{i+1}/q_{i+1}, dobijamo procenu

$$\left|\eta - \frac{p_i}{q_i}\right| < \left|\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i}\right| = \left|\frac{(-1)^{i+1}}{q_i q_{i+1}}\right| = \frac{1}{q_i q_{i+1}}.$$

Kako je $\{q_i\}_{i\geq 0}$ rastući niz prirodnih brojeva, zaključujemo da $\eta = \lim_{i\to\infty} p_i/q_i$. Konkretno, $\eta \neq p_i/q_i$, za svako i. Ako $\eta = a/b$, $a, b \in \mathbb{Z}$, $b > 0$, tada $a/b \neq p_i/q_i$ i $|aq_i - bp_i| \geq 1$. Ovo za sve i daje:

$$\frac{1}{bq_i} \leq \left|\frac{a}{b} - \frac{p_i}{q_i}\right| < \frac{1}{q_i q_{i+1}}$$

Dakle, za sve i je $q_{i+1} < b$, i to je kontradikcija koja pokazuje da je η iracionalan broj. ■

Primetimo da svaki $a_n > 1$ možemo pisati

$$\frac{1}{a_n} = \frac{1}{(a_n - 1) + \frac{1}{1}},$$

pa $\frac{a}{b} = [a_0, a_1, a_2, \dots, a_n]$ možemo zameniti sa $\frac{a}{b} = [a_0, a_1, \dots, a_{n-1}, a_n - 1, 1]$. Znači da svaki racionalan broj ima više zapisa u obliku verižnog razlomka.
Ako je $a_n = 1$ imamo

$$\frac{1}{a_{n-1} + \frac{1}{a_n}} = \frac{1}{(a_{n-1} + 1)},$$

pa $\frac{a}{b} = [a_0, a_1, \dots, a_n]$ izgleda ovako $[a_0, a_1, a_2, \dots, a_{n-2}, a_{n-1} + 1]$.

Primer 3.7 *Posmatramo broj $\frac{19}{6}$.*

$$\frac{19}{6} = 3 + \frac{1}{6} = 3 + \frac{1}{5 + \frac{1}{1}}$$

$$\frac{19}{6} = [3, 6] = [3, 5, 1].$$

■

4 Verižni razlomci iracionalnih brojeva

Šta predstavljaju i čemu služe beskonačni verižni razlomci? Beskonačni verižni razlomci predstavljaju iracionalne brojeve.

Uspostavljamo $1-1$ vezu između iracionalnih brojeva i nizova verižnih razlomaka,

$$\mathbb{R} \setminus \mathbb{Q} \leftrightarrow \{(a_i)_{i\geq 0} : a_i \in Z, a_i > 0, i \geq 1\}$$

Lema 4.1 *Sa ranije navedenim oznakama,* $\eta_{i+1} = \frac{-q_{i-1}\eta + p_{i-1}}{q_i\eta - p_i}$.

Dokaz 4.1 Pomoću jednakosti koju imamo za konvergente, imamo:

$$\eta = [a_0, a_1, \ldots, a_i, \eta_{i+1}] = \frac{\eta_{i+1}p_i + p_{i-1}}{\eta_{i+1}q_i + q_{i-1}}.$$

Poslednju jednakost dobijamo iz rekurzije

$$p_{-2} = 0, \quad p_{-1} = 1, \qquad p_{i+1} = a_{i+1}p_i + p_{i-1},$$

$$q_{-2} = 1, \quad q_{-1} = 0, \qquad q_{i+1} = a_{i+1}q_i + q_{i-1},$$

sa $a_{i+1} = \eta_{i+1}$. Rešavajući za η_{i+1} dokazujemo lemu. ∎

Moramo da procenimo koliko su približni njegovi konvergenti.

Lema 4.2 *Za* $\eta \in \mathbb{R} \setminus \mathbb{Q}$ *imamo procenu greške:*

$$\frac{1}{q_i(q_i + q_{i+1})} < \left|\eta - \frac{p_i}{q_i}\right| < \frac{1}{q_i q_{i+1}}.$$

Dokaz 4.2 Iz izraza $\eta = [a_0, a_1, \ldots, a_i, \eta_{i+1}] = \frac{\eta_{i+1}p_i + p_{i-1}}{\eta_{i+1}q_i + q_{i-1}}$ dobija se tačna formula za grešku aproksimirajući η sa p_i/q_i:

$$\left|\eta - \frac{p_i}{q_i}\right| = \left|\frac{\eta_{i+1}p_i + p_{i-1}}{\eta_{i+1}q_i + q_{i-1}} - \frac{p_i}{q_i}\right| = \left|\frac{p_{i-1}q_i - p_i q_{i-1}}{q_i(\eta_{i+1}q_i + q_{i-1})}\right| =$$

$$= \frac{1}{q_i(\eta_{i+1}q_i + q_{i-1})}.$$

Ovo pretvaramo u korisniju procenu koristeći $a_{i+1} < \eta_{i+1} < a_{i+1} + 1$:

$$q_{i+1} = a_{i+1}q_i + q_{i-1} < \eta_{i+1}q_i + q_{i-1} < (a_{i+1} + 1)q_i + q_{i-1} = q_{i+1} + q_i$$

Kombinacija ova dva dokazuje lemu. ∎

5 Periodični verižni razlomci

U produžetku opisujemo verižni razlomak kvadratičnog broja. Rezultati su neophodni za pronalaženje jedinica u realnom kvadratičnom polju.

Definicija 5.1 *Beskonačni verižni razlomak* $[a_0, a_1, a_2, \ldots]$ *je* ***periodičan*** *ako postoje* $l \in \mathbb{N}, r \in \mathbb{Z}_{\geq 0}$ *takvi da* $a_k = a_{k+l}$ *za sve* $k \geq r$. *Ako možemo da uzmemo* $r = 0$, *tj. ako nema dela koji se ne ponavlja, kažemo da je verižni razlomak* ***čisto periodični****.*

Periodični verižni razlomak izgleda ovako:

$$[b_0, \ldots, b_{r-1}, c_0, \ldots c_{l-1}, c_0, \ldots, c_{l-1}, \ldots].$$

Najkraći deo koji se ponavlja nazivamo **period**, a l **dužinu perioda** verižnog razlomka. Periodični verižni razlomak skraćujemo stavljanjem crtice iznad perioda i to pišemo na sledeći način:

$$[b_0, \ldots, b_{r-1}, \overline{c_0, \ldots, c_{l-1}}].$$

A čisto periodični razlomak pišemo: $[\overline{c_0, \ldots, c_{l-1}}]$.

Primer 5.1 *Nađimo verižni razlomak za* $\sqrt{3}$. *Možemo pisati:*

$$\sqrt{3} = 1 + (\sqrt{3} - 1) = 1 + \frac{2}{\sqrt{3}+1} = 1 + \frac{1}{\frac{\sqrt{3}+1}{2}} = 1 + \frac{1}{1 + \frac{\sqrt{3}-1}{2}} =$$

$$= 1 + \frac{1}{1 + \frac{1}{1+\sqrt{3}}} = 1 + \frac{1}{1 + \frac{1}{2+(\sqrt{3}-1)}}.$$

Situacija se periodično ponavlja, i zato je $\sqrt{3} = [1, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, \ldots] = [1, \overline{1, 2}]$. *U ovom primeru je period dužine 2.* ■

Naime, može se pokazati da se svaki broj oblika $\sqrt{n} \in \mathbb{N}$ može raspisati u beskonačan periodičan verižni razlomak. J. L. Lagrange[7] je dokazao da se svaki drugi broj oblika $r\sqrt{d} + q$, gde su $d, q, r \in \mathbb{N}$ (d nije potpun kvadrat) može prikazivati u obliku beskonačnog periodičnog verižnog razlomka.

Definicija 5.2 ***Potpuni kvadrat*** *je broj koji predstavlja kvadrat nekog prirodnog broja.*

Primer 5.2 *9 je potpuni kvadrat jer je* $9 = 3^2$, *dok* 8 *nije.*

[7]Joseph-Louis Lagrange (1736.-1813.)- veliki francuski matematičar

Definicija 5.3 *Neka je D ceo broj koji nije potpun kvadrat. Skup svih brojeva oblika $a+b\sqrt{D}$, $a,b \in \mathbb{Q}$ uz uobičajene operacije sabiranja i množenja kompleksih brojeva, čini polje, koje označavamo sa $\mathbb{Q}[\sqrt{D}]$ i zovemo* ***kvadratično polje****. Tj.*

$$\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\},$$

Ako je $D < 0$ polje $\mathbb{Q}[\sqrt{D}]$ je ***imaginarno kvadratično polje****, a* ***realno kvadratično polje*** *je ako je $D > 0$.*

Kažemo da je D bez kvadrata ako nije deljiv bilo kojim potpunim kvadratom osim 1, tj. D je proizvod različitih prostih brojeva. Kada radimo u $\mathbb{Q}[\sqrt{D}]$, često nam je od velike pomoći da predpostavimo da je D bez kvadrata. Ovo ne gubi na opštosti: ako $D' = n^2D$, tada $a+b\sqrt{D'} = a+bn\sqrt{D}$, tako da $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$.

Definicija 5.4 ***Kvadratični broj*** *je iracionalan element kvadratičnog polja. Drugim rečim, to je broj oblika*

$$\frac{x + y\sqrt{z}}{w}$$

gde su x, y, z celi brojevi, $y, w \neq 0$, i z nije potpun kvadrat.

Teorema 5.1 *Verižni razlomak $\eta \in \mathbb{R} \setminus \mathbb{Q}$ je periodičan* ***ako i samo ako*** *je η kvadratični broj.*

Dokaz 5.1 Pre dokaza teoreme ćemo uraditi jedan primer.

Primer 5.3 *Izračunajmo vrednost periodičnog verižnog razlomka:*

(a) $\eta = [3, 1, \overline{2, 5}] = [3, 1, 2, 5, 2, 5, \ldots]$. Čisto periodični deo $\eta_2 = [2, 5, 2, 5, \ldots]$ se ne menja kada uklonimo prva dva elementa:

$$\eta_2 = [2, 5, 2, 5, \ldots] = [2, 5, \eta_2] = 2 + \frac{1}{5 + \frac{1}{\eta_2}} = \frac{11\eta_2 + 2}{5\eta_2 + 1}.$$

Dobijamo kvadratnu jednačinu $5\eta_2^2 - 10\eta_2 - 2 = 0$. Rešenja su:

$$\eta_{1,2} = \frac{10 \pm \sqrt{100 + 40}}{10} = \frac{5 \pm \sqrt{35}}{5}.$$

Onda računamo:

$$\eta = [3, 1, \eta_2] = 3 + \frac{1}{1 + \frac{1}{\eta_2}} = 3 + \frac{1}{1 + \frac{5}{5+\sqrt{35}}} = \frac{42 + \sqrt{35}}{13}.$$

(b) $\eta = [1, 8, 1, 8, \ldots] = [\overline{1, 8}]$. *Vidimo da je ovaj verižni razlomak čisto periodičan, jer nema dela koji se ne ponavlja. Tada je* $\eta = 1 + \frac{1}{8+\frac{1}{\eta}}$. *Kada desnu stranu napišemo kao razlomak imamo*

$$\eta = \frac{9\eta + 1}{8\eta + 1},$$

tj. dobijamo kvadratnu jednačinu $8\eta^2 - 8\eta - 1 = 0$. *Rešenja ove jednačine su*

$$\eta_{1,2} = \frac{2 \pm \sqrt{6}}{4}.$$

S obzirom da je $\eta > 0$, *sledi* $\eta = \frac{2+\sqrt{6}}{4}$. ■

Propozicija 5.1 *Ako je verižni razlomak* η *periodičan, tada je* η *kvadratični broj.*

Dokaz 5.1 Dokaz je neposredna generalizacija predhodnog izračunavanja. Razmatramo dva slučaja:

(a) Ako je $\eta = [\overline{c_0, \ldots, c_{l-1}}]$ čisto periodičan, tada

$$\eta = [c_0, \ldots, c_{l-1}, \eta] = \frac{\eta p_{l-1} + p_{l-2}}{\eta q_{l-1} + q_{l-2}}.$$

Iz predhodnog reda se dobija kvadratna jednačina:

$$q_{l-1}\eta^2 + (q_{l-2} - p_{l-1})\eta - p_{l-2} = 0.$$

(b) Neka je $\eta = [b_0, \ldots, b_{r-1}, \zeta]$, gde je ζ čisto periodični deo. Stavljajući $[b_0, \ldots, b_i] = h_i/k_i$ nalazimo

$$\eta = \frac{\zeta h_{r-1} + h_{r-2}}{\zeta k_{r-1} + k_{r-2}} \in \mathbb{Q}[\zeta]$$

jer je $\mathbb{Q}[\zeta]$ prema (a) kvadratično polje. Dakle, i η je kvadratični broj. ■

Primer 5.4 *Kao zagrevanje za dokazivanje da je verižni razlomak kvadratičnih brojeva periodičan, razmotrićemo sledeće:*

$$\eta = \frac{6 + \sqrt{10}}{2} = 4 + \frac{\sqrt{10} - 2}{2} = 4 + \frac{1}{\frac{2}{\sqrt{10}-2}} = 4 + \frac{1}{\frac{2+\sqrt{10}}{3}}$$

$$
\begin{aligned}
&= 4 + \cfrac{1}{1 + \frac{\sqrt{10}-1}{3}} = 4 + \cfrac{1}{1 + \frac{1}{\frac{3}{\sqrt{10}-1}}} = 4 + \cfrac{1}{1 + \frac{1}{\frac{1+\sqrt{10}}{3}}} \\
&= 4 + \cfrac{1}{1 + \frac{1}{1+\frac{\sqrt{10}-2}{3}}} = 4 + \cfrac{1}{1 + \frac{1}{1+\frac{1}{\frac{3}{\sqrt{10}-2}}}} = 4 + \cfrac{1}{1 + \frac{1}{1+\frac{1}{\frac{2+\sqrt{10}}{2}}}} \\
&= 4 + \cfrac{1}{1 + \frac{1}{1+\frac{1}{2+\frac{\sqrt{10}-2}{2}}}} = 4 + \cfrac{1}{1 + \frac{1}{1+\frac{1}{2+\frac{1}{\frac{2}{\sqrt{10}-2}}}}} = 4 + \cfrac{1}{1 + \frac{1}{1+\frac{1}{2+\frac{1}{\frac{2+\sqrt{10}}{3}}}}}.
\end{aligned}
$$

Svaki red se sastoji od tri izraza koji zajedno čine iteraciju procedure razvoja broja u verižni razlomak. Cela radnja se odvija u imenitelju poslednjeg $1/\ldots$ razlomka predhodnog reda. U prvi izraz zapisujemo $\eta_i = a_i + (\eta_i - a_i)$, dok u drugom okrenemo razlomljeni deo i na taj način dobijemo

$$\eta_i = a_i + \frac{1}{\frac{1}{\eta_i - a_i}} = a_i + \frac{1}{\eta_{i+1}}.$$

Treći izraz su isključivo kvadratični brojevi. Racionalizujemo imenilac η_{i+1}. Čitamo η_i kao imenilac poslednjeg $1/\ldots$ razlomka u $i-tom$ redu:

$$\eta_1 = \frac{2+\sqrt{10}}{3}, \quad \eta_2 = \frac{1+\sqrt{10}}{3}, \quad \eta_3 = \frac{2+\sqrt{10}}{2}, \quad \eta_4 = \frac{2+\sqrt{10}}{3}.$$

S obzirom da je $\eta_4 = \eta_1$, i a_i i η_{i+1} zavise samo od η_i vidimo da je $\eta_5 = \eta_2$. Generalno je $\eta_{i+3} = \eta_i$ i $a_{i+3} = a_i$ za $i \geq 1$, pa je

$$\frac{6+\sqrt{10}}{2} = [4, \overline{1, 1, 2}].$$

■

Svi η_i u primeru su oblika $\eta_i = (m_i + \sqrt{10})/v_i$ za $m_i, v_i \in \mathbb{Z}$. $\sqrt{10}$ je donekle proizvoljan. Ostali elementi $\mathbb{Q}[\sqrt{10}]$ se mogu koristiti umesto toga, a najprirodnije je da se koristi samo η. Zaista, $\sqrt{10} = 2\eta - 6$, tako da

$$\eta_1 = \frac{-4+2\eta}{3}, \quad \eta_2 = \frac{-5+2\eta}{3}, \quad \eta_3 = \frac{-4+2\eta}{2}, \quad \eta_4 = \frac{-4+2\eta}{3}.$$

Kvadratični broj η zadovoljava $e\eta^2 - f\eta + g = 0$, $e, f, g \in \mathbb{Z}$. Izaberemo ono što je veće, ili $\eta_O = e\eta$ ili $e\overline{\eta}$. Tada je η_O koren polinoma $P(x) = x^2 - fx + eg$.

Propozicija 5.2 *Ako je $\eta \in \mathbb{R}$ kvadratični broj, tada je verižni razlomak broja η periodičan.*

Dokaz 5.2 Konstruisanjem eksplicitne rekurzije prvo ćemo pronaći $m_i, v_i \in \mathbb{Z}$ tako da zadovoljava

$$\eta_i = \frac{m_i + n_O}{v_i}, i \geq 0.$$

Tada ćemo pokazati da su m_i i v_i ograničeni nezavisno od i. Pošto su celi brojevi, postoji samo konačno mnogo različitih parova (m_i, v_i). Za neke $i \neq j$ moramo imati $m_i = m_j$ i $v_i = v_j$, pa zato imamo i $\eta_i = \eta_j$. Periodičnost će zatim uslediti kao u prošlom primeru.

Rekurzija za (m_i, v_i): Zamenimo $\eta_i = \frac{m_i+\eta_O}{v_i}$ u formulu $\eta_{i+1} = \frac{1}{\eta_i - a_i}$:

$$\begin{aligned}\eta_{i+1} &= \frac{1}{\frac{m_i+\eta_O}{v_i} - a_i} = \frac{v_i}{(m_i - a_i v_i) + \eta_O} \cdot \frac{m_i - a_i v_i + \overline{\eta}_O}{m_i - a_i v_i + \overline{\eta}_O} \\ &= \frac{v_i(m_i - a_i v_i + \overline{\eta}_O)}{P(a_i v_i - m_i)} = \frac{a_i v_i - m_i - f + \eta_O}{-\frac{P(a_i v_i - m_i)}{v_i}}.\end{aligned}$$

Ovo sugeriše stavljanje $m_{i+1} = a_i v_i - m_i - f$ i $v_{i+1} = -P(a_i v_i - m_i)/v_i = -P(m_{i+1} + f)/v_i$. Koristeći identitet $P(x + f) = P(-x)$ dobijamo konačan oblik željene rekurzije:

$$m_{i+1} = a_i v_i - m_i - f, \quad v_{i+1} = -\frac{P(-m_{i+1})}{v_i}.$$

Pošto su koreni $P(x)$ iracionalni, $v_i v_{i-1} = P(-m_i) \neq 0$. Indukcijom $v_i \neq 0$ i v_{i+1} je dobro definisano. Konačno, potreban nam je početni uslov:

$$\text{ako } \eta_O = e\eta, \text{ uzimamo } m_0 = 0, v_0 = e;$$

$$\text{ako } \eta_O = e\overline{\eta} = f - e\eta, \text{ uzimamo } m_0 = -f, v_0 = -e$$

U oba slučaja $\eta = (m_0 + \eta_O)/v_0$ i $P(-m_0) \equiv 0 \pmod{v_0}$.

Dokazujemo da su m_i i v_i celi brojevi: Predhodni identiteti su slučajevi $i = 0$ iskaza:

$$m_i, v_i \in \mathbb{Z} \quad i \quad P(-m_i) \equiv 0 \pmod{v_i},$$

što dokazujemo indukcijom. Iz gornje rekurzije, tj. iz $m_{i+1} = a_i v_i - m_i - f$, $v_{i+1} = -\frac{P(-m_{i+1})}{v_i}$ se jasno vidi da $m_{i+1} \in \mathbb{Z}$. Dalje,

$$P(-m_{i+1}) = P(a_i v_i - m_i) \equiv P(-m_i) \equiv 0 \pmod{v_i},$$

poslednja jednakost je induktivan korak. Dakle, $v_{i+1} = -P(-m_{i+1})/v_i \in \mathbb{Z}$, i $P(-m_{i+1}) = -v_i v_{i+1} \equiv 0 \pmod{v_{i+1}}$.

Ograničavanje m_i i v_i: Pokazujemo da je $v_i > 0$ za $i \geq 1$. Primenom konjugacija na izraz η_i u polju $\mathbb{Q}[\eta]$ iz leme 4.1 dobijamo

$$\overline{\eta}_i = \frac{-q_{i-2}\overline{\eta} + p_{i-2}}{q_{i-1}\overline{\eta} - p_{i-1}} = -\frac{q_{i-2}}{q_{i-1}} \cdot \frac{\overline{\eta} - \frac{p_{i-2}}{q_{i-2}}}{\overline{\eta} - \frac{p_{i-1}}{q_{i-1}}} < 0.$$

Da bismo opravdali nejednakost moramo imati na umu da je prvi faktor uvek negativan, dok je drugi za dovoljno veliko i blizu 1 . Zapravo, i njegov imenilac i brojilac se približavaju $\overline{\eta} - \lim_{i\to\infty} p_i/q_i = \overline{\eta} - \eta \neq 0$. S druge strane, $\eta_i > 0$, $i \leq 1$, i

$$0 < \eta_i - \overline{\eta}_i = \frac{m_i + \eta_O}{v_i} - \frac{m_i + \overline{\eta}_O}{v_i} = \frac{\eta_O - \overline{\eta}_O}{v_i}.$$

Tu naša predpostavka $\eta_O > \overline{\eta}_O$ omogućava zaključak da je $v_i > 0$ za sve $i \geq 1$ (v_0 može biti i negativno). Sledi željena veza:

$$0 < v_i \leq v_i v_{i+1} = -P(-m_{i+1}) \leq -\min P(x).$$

Ovaj lanac nejednačina daje $P(-m_i) < 0$, tako da se m_i nalazi između dva korena $P(x)$:

$$-\eta_O < m_i < -\overline{\eta}_O$$

■

Za aritmetičku primenu korisno je koeficient v_i povezati sa normom polja.

Propozicija 5.3 *Za ceo algebarski broj η i $i \geq 0$, imamo*

$$v_{i+1} = (-1)^{i+1} N(p_i - q_i\eta).$$

Dokaz 5.3 Kako je $\eta = \eta_O$ algebarski ceo broj, možemo naći $f, g \in \mathbb{Z}$ za koje $\eta^2 - f\eta + g = 0$, tako da $n + \overline{\eta} = f$ i $\eta\overline{\eta} = g$. Iz leme 4.1

$$\begin{aligned}
\eta_{i+1} &= \frac{-q_{i-1}\eta + p_{i-1}}{q_i\eta - p_i} = \frac{-q_{i-1}\eta + p_{i-1}}{q_i\eta - p_i} \cdot \frac{q_i\overline{\eta} - p_i}{q_i\overline{\eta} - p_i} = \\
&= \frac{(-p_i p_{i-1} - g q_i q_{i-1}) + p_{i-1} q_i \overline{\eta} + p_i q_{i-1}\eta}{N(p_i - q_i\eta)} \\
&= \frac{(-p_i p_{i-1} - g q_i q_{i-1} + f p_{i-1} q_i) + (-p_{i-1} q_i + p_i q_{i-1})\eta}{N(p_i - q_i\eta)} \\
&= \frac{(-p_i p_{i-1} - g q_i q_{i-1} + f p_{i-1} q_i) + (-1)^{i-1}\eta}{-p_i p_{i-1} - g q_i q_{i-1}} \\
&= \frac{(-1)^i(-p_i p_{i-1} - g q_i q_{i-1} + f p_{i-1} q_i) + \eta}{(-1)^{i+1} N(p_i - q_i\eta)}
\end{aligned}$$

Kada dobijeno uporedimo sa $\eta_{i+1} = (m_{i+1} + \eta)/v_{i+1}$ vidimo da je tvrđenje dokazano. Takođe $m_{i+1} = (-1)^i(p_i p_{i-1} + g q_i q_{i-1} - f p_{i-1} q_i)$. ■

Teorema 5.2 *Neka je a kvadratični broj, koji na osnovu ranije dokazane teoreme ima periodični verižni razlomak . Taj periodični razlomak je čisto periodični* ***ako i samo ako*** *je* $\eta > 1$ *i* $-1 < \overline{\eta} < 0$.

Dokaz 5.2 Označimo sa l dužinu perioda η. Prvo predpostavimo da je η čisto periodičan. Dokazali smo da ako je verižni razlomak periodičan, da je η kvadratičan broj, pa su zato η i $\overline{\eta}$ koreni polinoma $f(x) = q_{l-1}x^2 + (q_{l-2} - p_{l-1})x - p_{l-2}$. Pošto je $\{a_i\}$ niz verižnog razlomka, $1 \leq a_l = a_0 = p_0 < \eta$. Zatim, pored $q_i > 0$ rekurzija za sve $i \geq 0$ pokazuje $p_i > 0$, što je uvek tačno.

Nejednačina $-1 < \overline{\eta} < 0$ važi ako i samo ako $f(x)$ ima nulu u intervalu $(-1, 0)$. Da bi to pokazali, dovoljno je da pokažemo da su $f(-1)$ i $f(0)$ suprotnog znaka. Zaista,

$$\begin{aligned} f(-1) &= q_{-1} - q_{l-2} + p_{l-1} - p_{l-2} \\ &= a_{l-1}q_{l-2} + q_{l-3} - q_{l-2} + a_{l-1}p_{l-2} + p_{l-3} - p_{l-2} \\ &= (a_{l-1} - 1)(q_{l-2} + p_{l-2}) + q_{l-3} + p_{l-3} > 0, \\ f(0) &= -p_{l-2} < 0. \end{aligned}$$

Obratno, predpostavimo da $\eta > 1$ i $-1 < \overline{\eta} < 0$. To je granični slučaj $i = 0$ $\eta_i > 1$, $-1 < \overline{\eta}_i < 0$. Prva nejednačina je tačna za sve $i > 0$, pošto je $\eta_i > \lfloor \eta_i \rfloor = a_i \geq 1$. Da bismo dokazali drugu nejednačinu moramo induktivno da argumentujemo. Ako je $\overline{\eta}_i < 0$, tada $\overline{\eta}_i - a_i < -a_i \leq -1$ dakle $-1 < 1/(\overline{\eta}_i - a_i) = \overline{\eta}_{i+1} < 0$

Prepišemo nejednakost $-1 < \overline{\eta}_i < 0$ kao $0 < -\overline{\eta}_i = -1/\overline{\eta}_{i+1} - a_i < 1$, tako da je $a_i = \lfloor 1/\overline{\eta}_{i+1} \rfloor$. S obzirom da je a kvadratični broj, znamo $\eta_k = \eta_{k+l}$ za dovoljno veliko k. Iz

$$a_{k-1} = \left\lfloor -\frac{1}{\overline{\eta}_k} \right\rfloor = \left\lfloor -\frac{1}{\overline{\eta}_{k+l}} \right\rfloor = a_{k+l-1}$$

zaključujemo da je $\eta_{k-1} = a_{k-1} + 1/\eta_k = a_{k+l-1} + 1/\eta_{k+l} = \eta_{k+l-1}$. Smanjujemo indeks sve dok ne dobijemo da je $\eta_0 = \eta_l$: η čisto periodičan. ■

Primer 5.5 *Uzmemo* $D \in \mathbb{N}$*, gde* D *nije savršen kvadrat. Posmatrajmo* $\lfloor\sqrt{D}\rfloor + \sqrt{D} > \lfloor\sqrt{D}\rfloor \geq 1$, *i* $0 < \sqrt{D} - \lfloor\sqrt{D}\rfloor < 1$ *po definiciji* $\lfloor\sqrt{D}\rfloor$. *Dakle,* $\lfloor\sqrt{D}\rfloor + \sqrt{D}$ *zadovoljava uslov predhodne teoreme i verižni razlomak je čisto periodičan:*

$$\sqrt{D} + \lfloor\sqrt{D}\rfloor = [2\lfloor\sqrt{D}\rfloor, a_1, \ldots, a_{l-1}, 2\lfloor\sqrt{D}\rfloor, \ldots].$$

Ako oduzmemo ceo broj $\lfloor\sqrt{D}\rfloor$ *promeni se samo prvi element u verižnom razlomku , i imamo*

$$\sqrt{D} = [\lfloor\sqrt{D}\rfloor, \overline{a_1, \ldots 2\lfloor\sqrt{D}\rfloor}].$$

■.

6 Računanje kvadratičnih verižnih razlomaka

Propozicija 6.1 *Bilo koji kvadratični broj oblika* $\eta = (m_0 + \sqrt{d})/v_0$, *za neke* $d, m_0, v_0 \in \mathbb{Z}$ *tako da zadovoljava* $v_0 | m_0^2 - d$. *Stavimo* $v_{-1} = (m_0^2 - d)/v_0$. *Nizovi* $\{m_i\}$ *i* $\{v_i\}$ *su definisani rekurzivno sa:*

$$m_{i+1} = a_i v_i - m_i, \quad v_{i+1} = v_{v-1} + a_i(m_i - m_{i+1})$$

i zadovoljavaju sledeća svojstva za $i \geq 1$*:*

(a) $\eta_i = (m_i + \sqrt{d})/v_i$*;*

(b) $m_i, v_i \in \mathbb{Z}$ *i* $v_i | m_i^2 - d$*;*

(c) $0 < v_i \leq d$ *i* $-\sqrt{d} < m_i < \sqrt{d}$.

Dokaz 6.1 Dokaz ide isto kao dokaz propozicije 5.2, samo zamenimo η_O sa $\sqrt{d}$. Treba napomenuti da ne zahtevamo da d bude kvadrat, i da v_0 može biti negativan. Na primer, $(1-\sqrt{2})/3$ mora biti prepisan kao $(-3+\sqrt{18})/(-9)$ da bi se osiguralo da je $v_{-1} \in \mathbb{Z}$. Da bismo pronašli m_0, v_0 i d pratimo sledeći primer.

Početni uslov garantuje da iz rekurzije dobijamo $m_i, v_i \in \mathbb{Z}$. Ono što je možda manje očigledno je da je u rekurziji $m_{i+1} = a_i v_i - m_i - f, v_{i+1} = -\frac{P(-m_{i+1})}{v_i}$ za v_i sa $P(x)$ zamenjeno $x^2 - d$. Zapravo, počevši od

$$m_{i+1} = a_i v_i - m_i - f, \; v_{i+1} = -\frac{P(-m_{i+1})}{v_i}$$

nalazimo

$$v_{i+1} = -\frac{m_{i+1}^2 - d}{v_i} = -\frac{(a_i v_i - m_i)^2 - d}{v_i} = 2a_i m_i - a_i^2 v_i - \frac{m_i^2 - d}{v_i}$$
$$= a_i(m_i + m_i - a_i v_i) + v_{i-1} = v_{i-1} + a_i(m_i - m_{i+1}).$$

■

Propozicija 6.2 *Za sve* $i \geq 1$ *imamo* $a_i = \lfloor (m_i + \lfloor \sqrt{d} \rfloor)/v_i \rfloor$. *Pored toga* $a_0 = \lfloor (m_0 + \lfloor \sqrt{d} \rfloor)/v_0 \rfloor$ *ili* $\lfloor (m_0 + \lfloor \sqrt{d} \rfloor)/v_0 \rfloor - 1$. *Druga mogućnost javlja se ako i samo ako* $v_0 < 0$ *i* $v_0 \mid m + \lfloor \sqrt{d} \rfloor$.

Dokaz 6.2 Predpostavimo da je $i \geq 1$. Iz prethodne propozicije pod (c) imamo $a_i v_i - m_i = m_{i+i} \leq \lfloor \sqrt{d} \rfloor$. Deljenjem sa $v_i > 0$ dobijamo:

$$a_i \leq \frac{m_i + \lfloor \sqrt{d} \rfloor}{v_i} < \frac{m_i + \sqrt{d}}{v_i} < a_i + 1.$$

Ovo samo znači $a_i = \lfloor (m_i + \lfloor \sqrt{d} \rfloor)/v_i \rfloor$. ■

Zbog praktičnosti iz dokaza predhodne propozicije izdvajamo algoritam za pronalaženje verižnog razlomka kvadratičnog broja η:

ALGORITAM ZA PRONALAŽENJE VERIŽNOG RAZLOMKA KVADRATIČNIH BROJEVA

1. $\eta \in \mathbb{R}$ je kvadratični broj . Stavimo $\eta_0 := \eta = (m_0 + \sqrt{d})/v_0$, tako da $v_0 \mid d - m_0^2$, (kao u sledećem primeru). Stavimo $v_{-1} := (d - m_0^2)/v_0,\ s := \lfloor\sqrt{d}\rfloor$, i postavimo brojač $i := 0$.

2. Ako je $(m_i, v_i) = (m_r, v_r)$, za neko $0 \leq r < i$ završavamo i pišemo:
$$\eta = [a_0, \ldots, a_{r-1}, \overline{a_r, \ldots, a_{i-1}}].$$

3. U suprotnom računamo sledećim redosledom:
$$\begin{aligned} a &:= \lfloor (m_i + s)/v_i \rfloor \\ a_i &:= \begin{cases} a - 1 & \text{ako } i = 0, v_0 < 0 \ \ i \ \ v_0 \mid m_0 + s \\ a & \text{inače} \end{cases} \\ m_{i+1} &:= a_i v_i - m_i \\ v_{i+1} &:= v_{i-1} + a_i(m_i - m_{i+1}). \end{aligned}$$

   Povećajmo brojač i za 1 i vratimo se na korak 2.

Primer 6.1 *Da bi se pronašao verižni razlomak broja $\sqrt{223}$, stavimo $d = 223$, $m_0 = 0,\ v_0 = 1,\ s = 14$ i popunimo sledeću tabelu koristeći algoritam, pazeći na periodičnost:*

i	-1	0	1	2	3	4	5
a_i	-	14	1	13	1	28	1
m_i	-	0	14	13	13	14	14
v_i	223	1	27	2	27	1	27

Kako su $m_5 = m_1$ i $v_5 = v_1$, dobijamo $\sqrt{223} = [14, \overline{1, 13, 1, 28}]$.

Zanimljiv dodatak se krije u ovoj tabeli. Označimo sa p_i/q_i i-ti konvergent broja $\sqrt{223}$. Tada su p_i i q_i strogo rastući nizovi celih brojeva. Međutim, na osnovu propozicije 5.3 , jedine moguće vrednosti za $N(p_i - q_i\sqrt{223}) = (-1)^{i+1}v_{i+1}$ su $1, -27$ i 2. ■

Primer 6.2 *Razvijmo broj* $\eta = \frac{3214+\sqrt{37}}{1661}$ *u verižni razlomak. Imamo* $d = \sqrt{37}$, $m_0 = 3214, v_0 = 1661$. *Vidimo da vredi* $v_0 | m_0^2 - d$ *i počinjemo s postupkom.*

i	m_i	v_i	η_i	a_i
0	3214	1661	$\frac{3214+\sqrt{37}}{1661}$	1
1	-1553	-1452	$\frac{-1553+\sqrt{37}}{-1452}$	1
2	101	7	$\frac{101+\sqrt{37}}{7}$	15
3	4	3	$\frac{4+\sqrt{37}}{3}$	3
4	5	4	$\frac{5+\sqrt{37}}{4}$	2
5	3	7	$\frac{3+\sqrt{37}}{7}$	1
6	4	3		

Vidimo da je $m_3 = m_6$, $v_3 = v_6$, *pa će biti i* $\eta_3 = \eta_6$, *i dobijamo* $\eta = [1, 1, 15, \overline{3, 2, 1}]$. *U ovom primeru nam je dovoljno bilo* $i > 2$, *odnosno* a_3 *je početak perioda.* ■

Primer 6.3 *Da bismo razvili* $\sqrt{\frac{11}{7}}$ *u verižni razlomak, zapišimo ga u obliku*

$$\sqrt{\frac{11}{7}} = \frac{0 + \sqrt{77}}{7}.$$

Sada je $m_0 = 0, v_0 = 7, d = 77$ *i imamo* $v_0 | m_0^2 - d$. *Dobijamo*

i	0	1	2	3	4	5	6	
m_i	0	7	5	8	8	5	7	7
v_0	7	4	13	1	13	4	7	4
a_i	1	3	1	16	1	3	2	

odnosno $\sqrt{\frac{11}{7}} = [1, \overline{3, 1, 16, 1, 3, 2}]$. ■

7 Aproksimacija konvergenata

Već smo nagovestili da je realan broj efikasno aproksimiran članovima verižnog razlomka. Sada ćemo tu tvrdnju precizirati. Koristićemo jednostavno zapažanje da za $a, p \in \mathbb{Z}$ i $b, q \in \mathbb{N}$,

$$\frac{a}{b} \neq \frac{p}{q} \quad \text{implicira} \left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq},$$

$aq - bp$ je ceo broj različit od nule. Pretpostavimo da je $\eta = [a_0, a_1, \ldots]$ iracionalan, sa konvergentima p_i/q_i.

Propozicija 7.1 *Neka je* $a, b \in \mathbb{Z}$, $b > 0$ *i* $\text{nzd}(a, b) = 1$. *Ako je* $\left|\eta - \frac{a}{b}\right| < \left|\eta - \frac{p_i}{q_i}\right|$ *tada* $b > q_i$.

Jasno nam je da ako želimo da poboljšamo aproksimaciju η datu konvergentima potreban nam je razlomak sa što većim imeniocem.

Dokaz 7.1 Zbog jednostavnosti pretpostavimo da je i neparan, pa je tako

$$p_{i+1}/q_{i+1} < \eta < p_i/q_i.$$

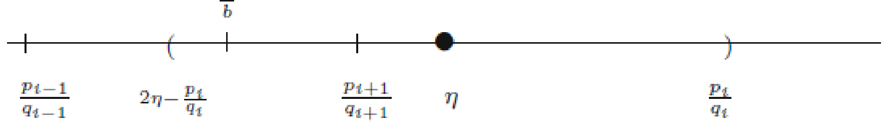
Paran slučaj je sličan, nejednakosti su obrnute.
Po pretpostavci , a/b je u intervalu centriranom sa η, sa jednom krajnjom tačkom p_i/q_i. Uzimamo u obzir samo slučaj $a/b \in (2\eta - p_i/q_i, \eta)$. Budući da se stalno približava η, p_{i+1}/q_{i+1} je u istom intervalu a to vidimo i na slici dole.

Prema tome, dužina $(2\eta - p_i/q_i, \eta)$ je veća od udaljenosti između p_{i+1}/q_{i+1} i a/b. To nam daje drugu nejednakost

$$\frac{1}{bq_{i+1}} \leq \left|\frac{a}{b} - \frac{p_{i+1}}{q_{i+1}}\right| < \left|\eta - \frac{p_i}{q_i}\right| < \frac{1}{q_i q_{i+1}}.$$

Zaključujemo da je $b > q_i$. ■

Kako možemo znati da li je razlomak konvergent broja η? Sledeća propozicija nam daje dovoljan uslov.



Propozicija 7.2 *Za* $a, b \in \mathbb{Z},\ b > 0$ *i* $\mathrm{nzd}(a, b) = 1$.

$$\left|\eta - \frac{a}{b}\right| < \frac{1}{2b^2} \text{ implicira } \ a = p_i,\ b = q_i,\ \text{za neko } \ i \geq 0.$$

Dokaz 7.2 Dokazaćemo kontradikcijom.

Ako $a/b \neq p_k/q_k$ za sve k, postoji jedinstveno i tako da je a/b između p_{i-1}/q_{i-1} i p_{i+1}/q_{i+1}. Pretpostavljamo da je i neparno, a paran slučaj ide analogno. Situacija je prikazana na gornjoj slici. ali, za razliku od prethodnog dokaza, a/b može biti sa obe strane $2\eta - p_i/q_i$.

Imamo sledeći lanac nejednakosti, od kojih je poslednji očigledan sa slike :

$$\left|\eta - \frac{p_i}{q_i}\right| < \frac{1}{q_i q_{i+1}} = \frac{b}{q_i} \cdot \frac{1}{b q_{i+1}} \leq \frac{b}{q_i} \left|\frac{p_{i+1}}{q_{i+1}} - \frac{a}{b}\right| < \frac{b}{q_i} \left|\eta - \frac{a}{b}\right|.$$

Kada ovo iskombinujemo sa nejednakošću trougla, dobijamo:

$$\frac{1}{bq_i} \leq \left|\frac{a}{b} - \frac{p_i}{q_i}\right| \leq \left|\eta - \frac{a}{b}\right| + \left|\eta - \frac{p_i}{q_i}\right| < \left|\eta - \frac{a}{b}\right| \left(1 + \frac{b}{q_i}\right)$$

Tek sada primenjujemo predpostavku $|\eta - \frac{a}{b}| < \frac{1}{2b^2}$:

$$\frac{1}{bq_i} < \left|\eta - \frac{a}{b}\right| \left(1 + \frac{b}{q_i}\right) < \frac{1}{2b^2} \cdot \frac{q_i + b}{q_i}$$

Tako da $b < q_i$.

S druge strane, a/b leži u intervalu $(p_{i-1}/q_{i-1}, \eta)$. Sličnim zaključivanjem kao u prethodnoj propoziciji, tj. u

$$\frac{1}{bq_{i+1}} \leq \left|\frac{a}{b} - \frac{p_{i+1}}{q_{i+1}}\right| < \left|\eta - \frac{p_i}{q_i}\right| < \frac{1}{q_i q_{i+1}}$$

dobijamo $q_i < b$. Ta kontradikcija pokazuje da je a/b konvergent. ■

Sledeća posledica je ključna za našu primenu verižnih razlomaka realnih kvadratičnih polja.

Posledica 7.1 *Neka je* $P(x) = x^2 - fx + g$ *polinom sa koeficientima iz* $\mathbb{Z}$*, i diskriminanta* $D = f^2 - 4g > 0$*. Pretpostavimo da koreni polinoma zadovoljavaju* $\eta > 0 > \overline{\eta}$*, i neka su* p_i/q_i *konvergenti verižnog razlomka broja* η*. Za uzajamno proste* $a, b \in \mathbb{N}$ *važi sledeća implikacija:*

$$\text{Ako } |a^2 - fab + gb^2| < \frac{\sqrt{D}}{2},\ \text{tada } a = p_i,\ b = q_i, \text{za neko } i > 0.$$

Dokaz 7.1 Deljenjem sa b^2 dobijamo:

$$\left|P\left(\frac{a}{b}\right)\right| = \left|\left(\frac{a}{b}\right)^2 - f\left(\frac{a}{b}\right) + g\right| < \frac{\sqrt{D}}{2b^2}.$$

Razlikujemo dva slučaja:

<u>*SLUČAJ 1:*</u> $\eta < a/b$. Pošto je $P'(\eta) = \sqrt{D} > 0$ i pošto je parabola $y = P(x)$ iznad tangente na η, imamo da je $0 < P'(\eta)(x - \eta) < P(x)$ kada $\eta < x$. Stavljajući $x = a/b$ i deljenjem sa $P'(\eta)$, dobijamo:

$$\left|\frac{a}{b} - \eta\right| = \frac{a}{b} - \eta < \frac{P(a/b)}{\sqrt{D}} = \frac{|P(a/b)|}{\sqrt{D}} = \frac{\sqrt{D}/2b^2}{\sqrt{D}} = \frac{1}{2b^2},$$

tako da $a = p_i,\ b = q_i$ za neko i (sledi iz predhodne propozicije).

<u>*SLUČAJ 2:*</u> $0 < a/b < \eta$. Prema našoj predpostavci $\eta > 0 > \overline{\eta}$, polinom $Q(x) = -x^2 P(1/x) = -gx^2 + fx - 1$ ima korene $1/\eta > 0 > 1/\overline{\eta}$ i zadovoljava $Q'(1/\eta) = \sqrt{D} > 0$. Štaviše, njegov vodeći koeficient $-g = -\eta\overline{\eta}$ je pozitivan pa $Q(x)$ i $P(x)$ imaju ista svojstva. Ako je $0 < x < \eta$, tada $1/\eta < 1/x$, i dobijamo isto kao u slučaju 1

$$\left|\frac{1}{x} - \frac{1}{\eta}\right| < \frac{Q(1/x)}{\sqrt{D}} = \frac{-P(x)}{x^2\sqrt{D}} = \frac{|P(x)|}{x^2\sqrt{D}},$$

poslednju jednakost dobijamo jer je $P(x) < 0$ za $0 < x < \eta$. Za $x = a/b$ ovo postaje

$$\left|\frac{b}{a} - \frac{1}{\eta}\right| < \frac{|P(a/b)|}{(a^2/b^2)\sqrt{D}} < \frac{\sqrt{D}/2b^2}{(a^2/b^2)\sqrt{D}} = \frac{1}{2a^2}.$$

Opet na osnovu predhodne propozicije b/a je konvergent $1/\eta$. Videli smo u primeru 3.4 da je $b/a = q_i/p_i$ za neko proizvoljno i. ∎

8 Grupa jedinica realnih kvadratičnih polja

U aritmetici na koju smo navikli radimo sa racionalnim brojevima iz skupa $\mathbb{Q}$ i celim brojevima iz skupa $\mathbb{Z}$. Osim što je savršeno intuitivna, ovakva aritmetika ima veoma poželjna svojstva: poredak, dobro definisanu deljivost, proste brojeve, jedinstveno razlaganje na proste činioce.

Međutim, moć aritmetike nad $\mathbb{Q}$ je ograničena. Zato nam je ponekad potrebno da radimo sa drugim skupovima. Da bismo mogli da govorimo o aritmetici, nije neophodno da radimo u skupu $\mathbb{Q}$ ili $\mathbb{Z}_p$. To može biti bilo koji skup u kome možemo da sabiramo, oduzimamo, množimo i delimo. Drugim rečima, taj skup može da bude bilo koje polje.

Definicija 8.1 *Prsten F je polje ako je svaki ne nula elemenat invertibilan, tj. $F^\times = F \setminus 0$.*

Ovde će fokus biti polje oblika $\mathbb{Q}[\sqrt{D}]$.

Kvadratični brojevi su imaginarni ako $z < 0$, a realni ako $z > 0$.

Definicija 8.2 *Neka je $\alpha \in \mathbb{Q}[\sqrt{D}]$. **Konjugat** od $\alpha = a+b\sqrt{D}$ je $\overline{\alpha} = a-b\sqrt{D}$. **Trag** i **normu** definišemo pomoću*

$$\mathrm{Tr}\alpha = \alpha + \overline{\alpha}, \qquad \mathrm{N}\alpha = \alpha\overline{\alpha}$$

Definicija 8.3 ***Prsten celih** kvadratičnog polja $\mathbb{Q}[\sqrt{D}]$ je*

$$\begin{aligned} O &= \{\alpha \in \mathbb{Q}[\sqrt{D}] : \alpha^2 - t\alpha + n = 0 \text{ za neko } t, n \in \mathbb{Z}\} \\ &= \{\alpha \in \mathbb{Q}[\sqrt{D}] : \mathrm{Tr}\alpha, \mathrm{N}\alpha \in \mathbb{Z}\}. \end{aligned}$$

Teorema 8.1 *Pretpostavimo da je $D \in \mathbb{Z}$ bez kvadrata. Skup celih u $\mathbb{Q}[\sqrt{D}]$ je prsten dat sa $O = \mathbb{Z} + \mathbb{Z}\delta_0 = \mathbb{Z}[\delta_0]$, gde*

$$\delta_0 = \begin{cases} \sqrt{D} & \text{za } D \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & \text{za } D \equiv 1 \pmod 4 \end{cases}$$

Dokaz 8.1 U oba slučaja δ_0 je u O, jer zadovoljava moničnu jednačinu sa koeficientima u $\mathbb{Z}$, naime $x^2 - D = 0$ ili $x^2 - x + (1-D)/4 = 0$. Poslednja jednakost ima koeficijent iz $\mathbb{Z}$ samo kada $D \equiv 1 \pmod 4$. Lako je uočiti da je $\mathbb{Z}+\mathbb{Z}\delta_0 \subseteq O$, a mi se fokusiramo na dokazivanje obrnute inkluzije.

Uzmimo $\alpha = a + b\sqrt{D} \in O$. Iz gornje definicije to znači da su $\mathrm{Tr}\alpha = 2a$ i $\mathrm{N}\alpha = a^2 - b^2 D$ oba iz $\mathbb{Z}$. Stavimo $a = r/2, b = m/n$ za neke $r, m, n \in \mathbb{Z}$ tako da nzd$(m,n) = 1$. Tada $4m^2D = n^2(r^2 - 4\mathrm{N}\alpha)$, tako da $n^2|4m^2D$, i činjenica je $n^2 \mid 4D$ jer je nzd$(m,n) = 1$. Da je p neparan prosti faktor n, imali bi $p^2 \mid D$, a to je kontradikcija sa time da je D bezkvadratni. Dakle, n mora biti jednak stepenu 2. Pošto 4 ne deli D, $n^2 \mid 4D$ imlicira $n^2 \mid 8$, dakle $n = 1$ ili 2. U oba slučaja $b = s/2$ za neko $s \in \mathbb{Z}$.

Pošto $a^2 - b^2D \in \mathbb{Z}$, imamo $r^2 \equiv s^2D \pmod 4$. Razmatramo dva slučaja:

(a) Ako $D \not\equiv 1 \pmod 4$, svaki par (r,s) zadovoljava $r^2 \equiv s^2 \equiv 0 \pmod 4$. Ovo implicira da su r i s čak i celi brojevi, pa su a i b u $\mathbb{Z}$ i $O \subseteq \mathbb{Z} + \mathbb{Z}\sqrt{D}$.

(b) Ako $D \equiv 1 \pmod 4$ tada $r^2 \equiv s^2D \equiv s^2 \pmod 4$, što implicira $r \equiv s \pmod 2$. Zapisujući $r = s + 2k$ za $k \in \mathbb{Z}$ to vidimo

$$\alpha = a + b\sqrt{D} = \frac{r + s\sqrt{D}}{2} = \frac{s + 2k + s\sqrt{D}}{2} = k + s\frac{1+\sqrt{D}}{2}.$$

Tako je $O \subseteq \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{D}}{2}$. ■

Definicija 8.4 ***Diskriminanta*** $\alpha \in O$ *je* $\mathrm{disc}\alpha = (\mathrm{Tr}\alpha)^2 - 4\mathrm{N}\alpha$.

Definicija 8.5 *Stavimo* $D_F = \mathrm{disc}O = \mathrm{disc}\delta_0$ *i nazovimo* ***diskriminanta polja*** $F = \mathbb{Q}[\sqrt{D}]$.

U sledećoj tabeli sumiramo osnovne informacije o O:

D mod 4	δ_0, gde $O = \mathbb{Z}[\delta_0]$	jednačina za δ_0	$D_F = \mathrm{disc}O$
2,3	$\sqrt{D}$	$\delta_0^2 - D = 0$	4D
1	$\frac{1+\sqrt{D}}{2}$	$\delta_0^2 - \delta_0 + \frac{1-D}{4} = 0$	D

Napomene:

1. Uvek možemo napisati $F = \mathbb{Q}[\sqrt{D_F}]$.
2. Ako ne želimo da pravimo razliku između ta dva slučaja koja imamo u gornjoj tabeli, umesto δ_0 možemo koristiti malo komplikovanije

$$\delta_1 = \frac{D_F + \sqrt{D_F}}{2}, \text{ za koje } \delta_1^2 - D_F\delta_1 + \frac{D_F^2 - D_F}{4} = 0.$$

   Tada je $O = \mathbb{Z}[\delta_1]$ bez obzira na vrednost D mod 4.
3. Kada pokazujemo opšte teoreme o O nije nas briga za konkretni izbor δ , $O = \mathbb{Z}[\delta]$. Bilo koji δ sa pravom diskriminantom odgovara. Stoga, popravljamo sledeći zapis: U ostatku rada, F označava kvadratično polje sa diskriminantom D_F i prstenom celih $O = \mathbb{Z}[\delta]$. Takvo δ mora da zadovolji $\delta^2 - t\delta + n = 0$ za neke $t, n \in \mathbb{Z}$ sa $D_F = t^2 - 4n$.

Do sada smo na verižne razlomke gledali kao na alat za približavanje realnim brojevima. Ali, oni imaju jednu neočekivanu upotrebu: određivanje grupe jedinica u prstenu celih $O = \mathbb{Z}[\delta]$ realnog kvadratičnog polja F.

Propozicija 8.1 *Postoji tačno jedan broj Δ takav da $O = \mathbb{Z}[\Delta]$ i verižni razlomak Δ je čisto periodičan:* $\Delta > 1$ i $-1 < \overline{\Delta} < 0$.

Dokaz 8.1 Nakon moguće zamene δ i $\overline{\delta}$ možemo pretpostaviti da $\delta > \overline{\delta}$. Bilo koji δ', $O = \mathbb{Z}[\delta']$ mora biti oblika $\delta' = a \pm \delta$ za neko $a \in \mathbb{Z}$. Pretpostavimo da je δ' čisto periodično, što po teoremi 5.2 znači da

$$a \pm \delta > 1 \text{ i } -1 < a \pm \overline{\delta} < 0$$

Konkretno, $\pm\delta > -a > \pm\overline{\delta}$ pa zbog $\delta > \overline{\delta}$ znak mora da bude plus, tj. $\overline{\delta} = a + \delta$. Druga nejednakost tada daje $a + 1 > -\overline{\delta} > a$, drugim rečima, $a = \lfloor -\overline{\delta} \rfloor$.

Ako postoji periodično δ' , mora biti $\Delta = \lfloor -\overline{\delta} \rfloor + \delta$. Ostaje da se proveri $\Delta > 1$. Najmanja moguća diskriminanta realnog kvadratičnog polja $D_{\mathbb{Q}[\sqrt{5}]} = 5$. Tada $2 < \sqrt{D_F} = \delta - \overline{\delta} < \delta + \lfloor -\overline{\delta} \rfloor + 1$, odakle $1 < \lfloor -\overline{\delta} \rfloor + \delta = \Delta$. ■

Za ostatak ovog odeljka popravljamo uobičajene zapise u referenci na Δ. Dakle, t i n su definisani sa $\Delta^2 - t\Delta + n = 0$, dok su a_i, p_i, q_i i Δ_i veličine povezane sa verižnim razlomkom Δ. Pošto je Δ algebarski ceo broj, $\Delta_O = \Delta$. Kao u dokazu propozicije 5.2. stavljamo

$$\Delta_i = \frac{m_i + \Delta}{v_i} \text{ sa } v_i, m_i \in \mathbb{Z} \text{ i } v_i \mid m_i^2 + tm_i + n.$$

Sa l označavamo dužinu perioda Δ, i nazivamo **dužina perioda F**.

Propozicija 8.2 *Za $i > 0$, $v_i = 1$ ako i samo ako je i sadržalac l.*

Dokaz 8.2 Predpostavimo da je $v_i = 1$ pa je $\Delta_i = m_i + \Delta$. Kako su Δ i Δ_i čisto periodični, iz teoreme 5.2 imamo $-1 < \overline{\Delta} < 0$ i $-1 < m_i + \overline{\Delta} < 0$. S obzirom da je $m_i \in \mathbb{Z}$, ovo je jedino moguće ako je $m_i = 0$. Tada je $\Delta_i = \Delta$ i i je sadržalac dužine perioda.

Obratno, ako $i = lk$ za neko k, imamo $\Delta = \Delta_{lk} = (m_{lk} + \Delta)/v_{lk}$. Upoređivanjem koeficienata dobijamo $v_{lk} = 1$. ■

Definicija 8.6 ***Fundamentalna jedinica*** *O (ili F) je jedinica $\varepsilon_F \in O^\times$ koja ispunjava sledeće uslove:*

(a) Za bilo koje $\varepsilon \in O^\times$, $\varepsilon = \pm\varepsilon_F^k$ za neko $k \in \mathbb{Z}$, i

(b) $\varepsilon_F > 1$

Uslov (a) znači da $O^\times = \pm\langle\varepsilon_F\rangle$. Ovde je $\langle\varepsilon_F\rangle$ multiplikativna beskonačna ciklična grupa generisana sa ε_F.

Uslov (b) garantuje da ako ε_F postoji, on je jedinstven. Sledeća teorema pokazuje kako konstruisati.

Teorema 8.2 *Neka $O = \mathbb{Z}[\delta]$ tako da $\delta > \overline{\delta}$. Neka su $p_i^{'}/q_i^{'}$ konvergenti δ, i neka je l dužina perioda F.*

Stavimo $\varepsilon_1 = p_{l-1}^{'} - q_{l-1}^{'}\delta$. Bilo koja jedinica $\varepsilon \in O^\times$ je oblika $\varepsilon = \pm\varepsilon_1^k$ za neko $k \in \mathbb{Z}$. Fundamentalna jedinica ε_F je tada $\pm\varepsilon_1$ ili $\pm\overline{\varepsilon}_1$, šta god je veće od 1.

Dokaz 8.2 Prema propoziciji 5.3, ε_1 je jedinica. Kako je $\delta > \overline{\delta}$, postoji $a \in \mathbb{Z}$ takav da je $\delta = \Delta + a$. Iz primera imamo da su konvergenti δ i Δ povezani sa $p_i^{'} = aq_i + p_i$ i $q_i^{'} = q_i$. Izračunavamo

$$\varepsilon_1 = p_{l-1}^{'} - q_{l-1}^{'}\delta = p_{l-1} + aq_{l-1} - q_{l-1}\delta = p_{l-1} - q_{l-1}(\delta - a)$$
$$= p_{l-1} - q_{l-1}\Delta.$$

Bez umanjenja opštosti, predpostavimo da je $\delta = \Delta$.

Jedinica ε je jednaka stepenu ε_1 do na znak ako je istinito za $-\varepsilon$, ili za $\overline{\varepsilon} = \pm\varepsilon^{-1}$ To nam omogućava da se ograničimo na slučaj $\varepsilon = a - b\Delta$ za $a, b \in \mathbb{Z}_{\geq 0}$. Zapravo, ako je $a < 0$ onda zamenimo ε sa $-\varepsilon$. Zatim, ako je $b < 0$ zamenimo ε sa $\overline{\varepsilon} = a - b\overline{\Delta} = (a - bt) - (-b)\Delta$. Pošto je Δ čisto periodičan, $t > 0$ i $a - bt$ je i dalje pozitivno.

Pošto je $D_F \geq D_{\mathbb{Q}[\sqrt{5}]} = 5$, imamo

$$|a^2 - tab + nb^2| = |N(a - b\Delta)| = 1 < \sqrt{5}/2 \leq \sqrt{D_F}/2.$$

Zaključujemo iz posledice 7.1. da je $a = p_i, b = q_i$ za neko $i > 0$. Propozicija 5.3 nam onda daje

$$v_{i+1} = (-1)^{i+1}N(p_i - q_i\Delta) = (-1)^{i+1}N_\varepsilon = \pm 1.$$

Kako je $v_{i+1} > 0$ pomoću dokaza iz propozicije 5.2 zaključujemo da je $v_{i+1} = 1$ i iz propozicije 8.2 da je $i + 1 = kl$ sadržalac perioda.

Pokazali smo da svaki $a - b\Delta \in O^\times,\ a, b \in \mathbb{Z}_{\geq 0}$ mora biti oblika

$$\varepsilon_k = p_{lk-1} - q_{kl-1}\Delta, \text{ za neko } k \geq 0.$$

Da bi se dokazala teorema dovoljno je potvrditi da je $\varepsilon_{k+1}/\varepsilon_k = \varepsilon_1$. Iz leme 4.1

$$-\Delta_{i+1} = \frac{p_{i-1} - q_{i-1}\Delta}{p_i - q_i\Delta}.$$

Formiramo teleskopski proizvod:

$$(-1)^l \Delta_{i+1}\Delta_{i+2}\cdots\Delta_{i+l} = \frac{p_{i-1} - q_{i-1}\Delta}{p_i - q_i\Delta} \cdot \frac{p_-iq_i\Delta}{p_{i+1} - q_{i+1}\Delta} \cdots \frac{p_{i+l+2} - q_{i+l-2}}{p_{i+l-1} - q_{i+l-1}\Delta}$$
$$= \frac{p_{i-1} - q_{i-1}\Delta}{p_{i+l-1} - q_{i+l-1}\Delta}.$$

Kada $i = kl$, dobijamo

$$(-1)^l \Delta_{kl+1}\Delta_{kl+2}\cdots\Delta_{(k+1)l} = \frac{p_{kl-1} - q_{kl-1}\Delta}{p_{(k+1)l-1} - q_{(k+1)l-1}\Delta} = \frac{\varepsilon_k}{\varepsilon_{k+1}}.$$

Kada je $k = 0$ ovo zauzvrat postaje

$$(-1)^l \Delta_1\Delta_2\cdots\Delta_l = \frac{p_{-1} - q_{-1}\Delta}{p_{l-1} - q_{l-1}\Delta} = \frac{1}{p_{l-1} - q_{l-1}\Delta} = \frac{1}{\varepsilon_1}.$$

Periodičnost podrazumeva $\Delta_{kl+1}\Delta_{kl+2}\cdots\Delta_{(k+1)l} = \Delta_1\Delta_2\ldots\Delta_l$. Stoga imamo, $\varepsilon_k/\varepsilon_{k+1} = 1/\varepsilon_1$. ■

Primer 8.1 *Predhodnu teoremu pokazujemo pronalaženjem fundamentalne jedinice* $\mathbb{Z}[\sqrt{223}]$. *Izračunavamo konvergente verižnog razlomka koje smo našli u primeru 6.1* $\sqrt{223} = [14, \overline{1, 13, 1, 28}]$. *Dovoljno je ići do kraja perioda:*

i	-2	-1	0	1	2	3	4	...
a_i	-	-	14	1	13	1	28	...
p_i	0	1	14	15	209	224	6481	...
q_i	1	0	1	1	14	15	434	...

Predhodna teorema nam to pokazuje, $\mathbb{Z}[223]^\times$ *je generisano sa* $\varepsilon_1 = p_3 - q_3\sqrt{223} = 224 - 15\sqrt{223} = 0.0022\ldots$. *Fundamentalna jedinica mora biti veća od 1, pa je dobijamo kao* $\overline{\varepsilon}_1$:

$$\varepsilon_{\mathbb{Q}[\sqrt{223}]} = p_3 + q_3\sqrt{223} = 224 + 15\sqrt{223}.$$

■

9 Zanimljivosti verižnih razlomaka

9.1 Računanje kalendarske godine

Jedna od zanimljivih primena verižnog razlomka je u računanju kalendarske godine. Trajanje jedne sunčane godine eksperimentalna je veličina, samim tim nema smisla da proučujemo taj broj kao racionalan ili iracionalan. Zamenićemo taj broj približnom vrednošću.

$$\alpha = \ 365 + \frac{5h\ 48min\ 46s}{1dan} \ = \ 365 + \frac{20926s}{86400s} \ = \ 365\frac{10463}{43200}$$

Kao što vidimo, broj α je racionalan pa je njegov razvoj u verižni razlomak konačan. Sada primenimo Euklidov algoritam na brojeve 43200 i 10463, i dobijamo:

$$\begin{aligned} 43200 &= 10463 \ \cdot \ 4 + 1348 \\ 10463 &= 1348 \cdot 7 + 1027 \\ 1348 &= 1027 \cdot 1 + 321 \\ 1027 &= 321 \cdot 3 + 64 \\ 321 &= 64 \cdot 5 + 1 \\ 64 &= 1 \cdot 64 \end{aligned}$$

Imamo da je $\alpha = [365, 4, 7, 1, 3, 5, 64]$, i da su konvergente broja $\alpha - 365$

$$\frac{1}{4}, \frac{7}{29}, \frac{8}{33}, \frac{31}{128}, \frac{163}{673}, \frac{10463}{43200}.$$

Svaki od gore navedenih konvergenti nam daje jedno rešenje problema kalendara. Tako je, npr kod prve konvergente prosečno trajanje godine $365\frac{1}{4}$ dana. To nam znači da je svaka četvrta godina prestupna. Uopšteno gledajući imenilac konvergenti nam daje dužinu ciklusa, a brojilac broj prestupnih godina u svakom ciklusu. Vidimo da peta i šesta konvergenta daju nepraktično rešenje stoga uopšteno razmatramo kalendare koje nam daju prve četiri konvergente. Julijanski kalendar je upravo naša prva konvergenta, dok kod četvrte konvergente je najmanja greška kod računanja.

9.2 Broj e

U matematici i njenim primenama veoma značajno mesto ima broj $e = 2,718281828\ldots$ osnova prirodnih logaritma. Interesantan je verižni razlomak koji odgovara tom broju:

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{2}{3 + \cfrac{3}{4 + \cfrac{4}{5 + \cfrac{5}{6 + \ddots}}}}}}$$

Verižnim razlomcima se bavio i Ojler [8], pa je tako možda i prvi dokazao da se svaki racionalan broj može zapisati u obliku konačnog verižnog razlomka. Autor je sledećih neobičnih jednakosti:

$$e - 1 = 1 + \cfrac{2}{2 + \cfrac{3}{3 + \cfrac{4}{4 + \cfrac{5}{5 + \ldots}}}}$$

$$\frac{1}{e+2} = 1 + \cfrac{1}{2 + \cfrac{2}{3 + \cfrac{3}{4 + \cfrac{4}{5 + \cfrac{5}{6 + \ldots}}}}}$$

Ovi razlomci nisu standardni verižni razlomci, jer im brojilac nije jednak jedinici. Vredi i

$$\sqrt{e} = [1, 1, 1, 1, 5, 1, 1, 9, 1, 1, 13, 1, 1, 17, 1, 1, \ldots],$$

i jednakost

$$e - 1 = [1, 1, 1, 2, 1, 1, 4, 1, 1, 6, \ldots].$$

Primer: Naći nekoliko približnih vrednosti broja e koristeći odgovarajući verižni razlomak. Redom nalazimo

$$e = 2;$$
$$e = 2 + \frac{1}{1} = 3;$$
$$e = 2 + \frac{1}{1 + \frac{1}{2}} = \frac{8}{3} = 2,66\ldots = 2,(6);$$
$$e = 2 + \frac{1}{1 + \frac{1}{2 + \frac{2}{3}}} = \frac{30}{11} = 2,7272\ldots = 2,(72);$$

[8] Leonhard Euler (1707-1783.) - švajcarski matematičar i fizičar. Ojler je došao do velikih otkrića u potpuno različitim oblastima kao što su matematička analiza i teorija grafova. Uveo je u upotrebu veliki broj termina koji se koriste u savremenoj matematici i unapredio matematičku notaciju.

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{2}{3 + \frac{3}{4}}}} = \frac{144}{53} = 2,71698113\ldots;$$

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{2}{3 + \cfrac{3}{4 + \frac{4}{5}}}}} = \frac{840}{309} = \frac{280}{103} = 2,71844660\ldots;$$

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{2}{3 + \cfrac{3}{4 + \cfrac{4}{5 + \frac{5}{6}}}}}} = \frac{5760}{2119} = 2,71826333\ldots;$$

i tako dalje. Dakle, imamo

$$2 < \frac{8}{3} < \frac{144}{53} < \frac{5760}{2119} < \ldots < e < \ldots < \frac{280}{103} < \frac{30}{11} < 3.$$

.

9.3 Verižni razlomci i Fibonačijev niz

Fibonačijev niz $1, 1, 2, 3, 5, 8, 13, 21, 34, 55\ldots$ definisan je formulom

$$F_n = F_{n-1} + F_{n-2} \qquad F_0 = 1, F_1 = 1.$$

Količnik dvaju uzastopnih članova ovog niza preko verižnog razlomka izgleda ovako:

$$\frac{13}{8} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{1}}}}} = [1, 1, 1, 1, 1, 1].$$

Kada posmatramo opšti slučaj, biće

$$\frac{F_{n+1}}{F_n} = 1 + \frac{F_{n-1}}{F_n} = a + \cfrac{1}{\frac{F_n}{F_{n-1}}} = 1 + \cfrac{1}{1 + \cfrac{1}{\frac{F_{n-1}}{F_{n-2}}}}$$

i situacija se dalje ponavlja, pa imamo $\frac{F_{n+1}}{F_n} = \Big[1, \underbrace{1, 1, \ldots, 1}_{n}\Big]$.

10 Zaključak

Verižni razlomci imaju mnoge primene u teoriji brojeva. Poznato je da je razvoj u verižni razlomak kvadratne iracionalnosti periodičan, ali je zaista teško predvideti kolika je dužina perioda razvoja proizvoljnog broja.

Čovek je kao razlomak, čiji je brojilac ono što on jeste, a imenilac ono što misli o sebi. Što je imenilac veći, razlomak je manji ." Lav Tolstoj[9]

* * *

Veliku zahvalnost dugujem mentoru, dr Goranu Đankoviću, na pruženom znanju, požrtvovanosti, korisnim savetima i svesrdnoj pomoći. Na kraju želim da se zahvalim mojim roditeljima, sestri i prijateljima na ljubavi, podršci i strpljenju koju mi pružaju.

[9]Lav Tolstoj (1828 - 1910.) - ruski pisac. Njegova dva najveća dela su Ana Karenjina i Rat i mir

Literatura

[1] Mak Trifković, *Algebraic Theory of Quadratic Numbers*, Department of Math and Statistics, University of Victoria, 2013

[2] Vinko Petričević, *Periodski verižni razlomci*, Magistarski rad, PMF - matematički odjel, Sveučilište u Zagrebu, Zagreb, 2009.
https://web.math.pmf.unizg.hr/ vpetrice/radovi/Magistarski.pdf

[3] Andrej Dujella, *Uvod u teoriju brojeva*, matematički odjel, Sveučilište u Zagrebu
https://web.math.pmf.unizg.hr/ duje/utb/utblink.pdf

[4] Ivana Tržić *Verižni razlomci,*, Diplomski rad, Sveučilište J.J. Strossmayera, Osijek, 2011,
http://www.mathos.unios.hr/ mdjumic/uploads/diplomski/TR%C5%BE01.pdf

[5] C.D.Olds, *Continued Fractions*, The Mathematical Association of America, 1963.
http://www.ms.uky.edu/ sohum/ma330/files/Continued%20Fractions.pdf

[6] Andrea Vranić *Beskonačni verižni razlomci*, Završni rad, Sveučilište J. J. Strossmayera u Osijeku, Odjel za matematiku, Osijek 2020.
http://www.mathos.unios.hr/ mdjumic/uploads/diplomski/VRA10.pdf

[7] WOLFRAM Demonstrations Project
https://demonstrations.wolfram.com/ContinuedFractions/

Biografija

Lidija Sabadoš rođena je 18.03.1994. godine u Vrbasu. Odrasla je u Ruskom Krsturu, gde je završila osnovnu školu ,,Petro Kuzmjak" 2009. godine i opšti smer gimnazije ,,Petro Kuzmjak" 2013. godine na rusinskom jeziku. Nosilac Vukove diplome, a po završetku srednje škole upisuje osnovne akademske studije matematike na Prirodno-matematičkom fakultetu u Novom Sadu. Diplomirala je u oktobru 2019. godine i stekla zvanje Diplomirani profesor matematike. Obrazovanje je nastavila na Matematičkom fakultetu u Beogradu, gde u oktobru 2019. godine upisuje master studije, teorijska matematika i primene. Zaključno sa julom 2020. godine ispolagala je sve ispite na master studijama i time stekla uslov za odbranu master rada.

Od 2020. godine, radi kao profesor matematike u srednjoj tehničkoj školi ,,Mihajlo Pupin" u Kuli.

Beograd, 2021.

Lidija Sabadoš