Sveučilište u Zagrebu
Prirodoslovno–matematički fakultet
Matematički odjel

Vinko Petričević

PERIODSKI VERIŽNI RAZLOMCI

Magistarski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, srpanj 2009.

Sadržaj

Oznake

$\langle\, a_0, a_1, \ldots \,\rangle$	verižni razlomak (broj),
$[\, a_0, a_1, \ldots \,]$	regularni verižni razlomak (najčešće $a_i \in \mathbb{N}$),
$\frac{p_n}{q_n} = \langle\, a_0, a_1, \ldots, a_n \,\rangle$	n-ta konvergenta verižnog razlomka,
$\frac{p'_n}{q'_n} = \langle\, a_1, \ldots, a_n \,\rangle$	n-ta konvergenta verižnog razlomka bez a_0,
$\overline{x_m, x_{m+1}, \ldots, x_{m+n}}$	brojevi $x_m, x_{m+1}, \ldots, x_{m+n}$ se ponavljaju u nedogled,
$\mathbb{N}$	skup prirodnih brojeva,
$\mathbb{Z}$	prsten cijelih brojeva,
$\mathbb{Q}$	polje racionalnih brojeva,
$\mathbb{R}$	polje realnih brojeva,
α	realan broj, najčešće kvadratna iracionalnost,
$\square$	kvadrat racionalnog broja,
$\alpha \neq \square$	α nije potpun kvadrat, tj. ne postoji $x \in \mathbb{Q}$ takav da je $\alpha = x^2$,
$\ell\,(\alpha)$	duljina perioda kvadratne iracionalnosti α,
$\overline{\alpha}$	konjugant od α. Za $x, y \in \mathbb{Q}$, $y \neq \square$ je $\overline{x + \sqrt{y}} = x - \sqrt{y}$,
$\mathbb{N}^n$	skup svih uređenih n-torki prirodnih brojeva,
$(\frac{\cdot}{p})$	Legendreov simbol modulo p,
$p^k \parallel n$	k je najveća potencija od p koja dijeli n,
$\omega(n)$	broj prostih djelitelja prirodnog broja n,
$\tau(n)$	broj djelitelja prirodnog broja n,
$\mu(n)$	Möbiusova funkcija.

Uvod

Moderna teorija brojeva zapravo počinje radovima Fermata u sedamnaestom stoljeću. Rezultati poput:

$$\text{za neparni prosti broj } p, \qquad \exists a, b \in \mathbb{Z}, p = a^2 + b^2 \iff p \equiv 1 \pmod 4$$

doveli su do razvoja teorije kvadratnih formi. Ona je pak dovela do shvaćanja svojstva jedinstvene faktorizacije, koje je važno i prirodno kod prirodnih brojeva, ali ne mora vrijediti u polju algebarskih brojeva. U tom smislu, broj klasa je mjera koliko je to svojstvo narušeno (to jest, broj klasa 1 znači jedinstvenu faktorizaciju).

Velik je dio posla tu napravio Gauss. Njegovu teoriju binarnih kvadratnih formi Dedekind je zamijenio idealima. Već tada se znalo da razvoj u jednostavni verižni razlomak od $\sqrt{d}$ daje mnogo informacija o formama s diskriminantom d. Dakle, postoji veza između binarnih kvadratnih formi, ideala i verižnih razlomaka. Detaljan opis kvadratnih formi se može naći na mnogim mjestima, npr. u [3], [7], kao i u starim originalima [10], [5].

Gauss je smatrao da postoji beskonačno mnogo realnih kvadratnih formi s brojem klasa 1. Taj i danas nerješeni problem je motivirao Shanksa 1960-tih da u tablicama brojeva klasa traži pravilnosti, pa je otkrio familiju polja $\mathbb{Q}(\sqrt{S_n})$, $S_n = (2^n + 3)^2 - 8$, čiji broj klasa raste jako brzo.

Već u Gaussovo vrijeme je bila poznata vezu između verižnih razlomaka i binarnih kvadratnih formi, pa je Shanks taj fenomen izrazio u terminima verižnih razlomaka: period u razvoju u verižni razlomak od $\sqrt{S_n}$ je vrlo kratak.

Općenito je teško unaprijed reći kako će izgledati razvoj u verižni razlomak. Takozvana "Cohen-Lenstrina" heuristika [2] sugerira da 75% svih prostih diskriminanti ima broj klasa 1. U jeziku verižnih razlomaka, to ugrubo znači da bi duljina perioda razvoja u verižni razlomak od $\sqrt{d}$ najčešće mogla biti oko $\sqrt{d}$. Pa ipak, iako je teško predvidjeti duljinu perioda $\ell(\sqrt{d})$ od $\sqrt{d}$, postoje brojni primjeri gdje ju možemo odmah odrediti, npr.

$$\sqrt{d} = \begin{cases} [\, n, \overline{2n}\,] & \text{ako je } d = n^2 + 1, \\ [\, n, \overline{\frac{n-1}{2}, 1, 1, \frac{n-1}{2}, 2n}\,] & \text{ako je } d = n^2 + 4 \text{ i } n \equiv 1 \,(\mathrm{mod}\ 2)\,. \end{cases}$$

Schinzel je generalizirao takve primjere i dokazao da za $\Delta = b^2 - 4ac \neq 0$

brojevi $d_n = an^2 + bn + c$ imaju ograničenu duljinu perioda ako i samo ako je a kvadrat i $\Delta \mid 4\big(\operatorname{nzd}(2a, b)\big)^2$.

Nakon Shanksovog otkrića (kasnije se uspostavilo da je Nyberg zapravo prvi otkrio takve nizove), mnogi drugi matematičari su pronalazili nizove realnih kvadratnih polja s velikim brojem klasa, odnosno malim periodom. To je motiviralo Kaplanskog [14], koji ih je pokušao klasificirati i dati uvjet sličan Schinzelovom. On je nizove brojeva s malom duljinom perioda, dakle $f(x) \in \mathbb{Q}[x]$ za koje vrijedi

$$\limsup_{n\to\infty} \ell\big(\sqrt{f(n)}\big) < \infty$$

nazvao *sleepers*.

Shanksovi rezultati su generalizirani do nizova oblika:

$$d_n = \left(qrx^n + \frac{\mu(x^k - \lambda)}{q}\right)^2 + 4\mu\lambda r x^n, \qquad \text{gdje je } rq \mid x^k - \lambda, \quad \mu, \lambda \in \{-1, 1\}.$$

Kod njih je duljina perioda linearna, tj. vrijedi $\ell\left(\sqrt{d_n}\right) = an + b = \mathcal{O}(\ln d_n)$. Kod većine takvih primjera za regulator (logaritam fundamentalne jedinice) vrijedi $R(d_n) = \mathcal{O}\big(\ln^2 d_n\big)$, jer uvijek imamo bar jedan veliki parcijalni kvocijent u palindromnom dijelu razvoja. Kaplanski je takve nizove (koji su polinomijalno parametrizirani, te vrijedi $\ell\left(\sqrt{d_n}\right) = an + b$, $R(d_n) = \mathcal{O}(n^2)$) nazvao *creepers*.

Pa ipak, Williams i Buck su pronašli nizove (a kasnije su i mnogi drugi generalizirali takve nizove) kojima duljina perioda teži u beskonačnost, a u palindromnom dijelu razvoja imaju samo male parcijalne kvocijente, pa je i fundamentalna jedinica relativno mala. Kod njih je $R(d_n) = \mathcal{O}(\ln d_n)$. Takvi nizovi su nazvani *beepers* u čast van der Poortenu, koji je napravio prvu generalizaciju na njima, te tako zaradio pivo.

Yamamoto [53] je našao nizove

$$d_n = (rx^n + x - 1)^2 + 4rx^n$$

kod kojih beskonačno mnogo elemenata zadovoljava $R(d_n) \gg \ln^3 d_n$, što je najbolje do sada.

Kaplanski je brojeve kojima duljina perioda eksponencijalno raste nazvao *leapers*.

Vratimo se malo creepersima. Kaplanski ih je pokušao karakterizirati, te je nizove brojeva (d_n) za koje vrijedi:

- $d_n = A^2x^{2n} + Bx^n + C^2$, gdje su $A, B, C \in \mathbb{Q}$, $n \in \mathbb{N}$,
- $\ell\left(\sqrt{d_n}\right) = an + b$, gdje su $a, b \in \mathbb{Q}$,
- u palindromnom dijelu razvoja imamo parcijalni kvocijent reda veličine x^g, gdje je g fiksan i neovisan o n,

nazvao *kreepers*. Lako se vidi da je svaki kreeper također i creeper, no o njima se malo zna. Također se ne zna postoje li nizovi $d_n = Ax^{2n} + Bx^n + C$, $A, B, C \in \mathbb{Z}$ takvi da duljina perioda raste brže od linearnog. Oni su nazvani *jeepers*.

Kako smo vidjeli do sada, najbolji poznati rezultati su da vrijedi $\ell\left(\sqrt{d_n}\right) \geq A \ln d_n$, gdje je A neka pozitivna konstanta. Ako bi našli niz za čijih beskonačno elemenata vrijedi $\ell\left(\sqrt{d_n}\right) > A\sqrt{d_n}$, to bi povlačilo da je $h(d_n) = 1$ za beskonačno mnogo diskriminanti d_n.

U prvom poglavlju ovog magistarskog rada opisana su osnovna svojstva verižnih razlomaka, počevši od konačnih verižnih razlomaka – racionalnih brojeva, periodskih – kvadratnih iracionalnosti, čisto periodskih. Naglasak je stavljen na kvadratne iracionalnosti sa simetričnim periodom. Pokazano je da za svaku duljinu perioda postoji beskonačno mnogo brojeva s takvom duljinom, te je dana gruba ocjena duljine perioda proizvoljne kvadratne iracionalnosti.

U drugom poglavlju su opisane osnovne primjene periodskih verižnih razlomaka u teoriji brojeva, s naglaskom na Pellovu jednadžbu i određivanje fundamentalne jedinice u realnom kvadratnom polju.

U trećem poglavlju dan je kratak pregled razvoja u verižni razlomak nad funkcijskim poljima, budući da ona imaju mnoga slična svojstva s brojevima.

U četvrtom su poglavlju dani primjeri brojeva koji imaju malu duljinu perioda, dani su Schinzelovi teoremi koji ih karakteriziraju, te su objašnjene dvije metode konstrukcije niza brojeva kojem svi elementi imaju neki zadani simetrični dio. Jedna od njih koristi polinomijalne Pellove jednadžbe, pa je i o njima rečeno nekoliko riječi.

U petom poglavlju dani su primjeri nizova brojeva koji imaju velik period i kojima je bar jedan parcijalni kvocijent u palindromnom dijelu razvoja velik.

U šestom poglavlju dani su primjeri brojeva koji imaju veliku duljinu perioda, ali su im svi parcijalni kvocijenti u palindromnom razvoja dijelu mali, te je objašnjena konstrukcija nizova takvih brojeva. Ti primjeri su bitni, jer je u tom slučaju fundamentalna jedinica, pa i regulator relativno malen.

U sedmom poglavlju su poboljšane gornje ograde za duljinu perioda, te je dokazana najbolja poznata gornja ograda za duljinu perioda – Cohnov rezultat da je $\ell\big(\sqrt{d}\big) \leq \frac{7}{2\pi^2}\sqrt{d}\ln d + \mathcal{O}\big(\sqrt{d}\big)$. Na kraju je dana veza s poznatom Riemannovom slutnjom, uz koju bi za gornju ogradu duljine perioda vrijedilo

$$\ell\big(\sqrt{d}\big) = \mathcal{O}\big(\sqrt{d}\ln\ln d\big),$$

a eksperimentalni rezultati ukazuju da bolje od toga ne može vrijediti.

Na kraju bih izrazio posebnu zahvalnost svom mentoru, prof.dr.sc. Andreju Dujelli, na ukazanoj pomoći, trudu i strpljenju, kako za vrijeme izrade rada, tako i tijekom poslijediplomskog studija. Zahvaljujem također i svim članovima Seminara za teoriju brojeva i algebru, a posebno prof.dr.sc. Ivici Gusiću i prof.dr.sc. Zrinki Franušić na vrijednim savjetima i velikoj pomoći.

Poglavlje 1

Verižni razlomci

Realnom se broju na različite načine mogu pridružiti racionalni brojevi koji ga dobro aproksimiraju. Jedna od najkorisnijih metoda je verižni razlomak.

Autori koriste različite oznake, a ja ću koristiti uglavnom slične onima iz [7].

Definicija 1.1. Verižni razlomak *je izraz oblika:*

$$\alpha = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \ddots}}}, \tag{1.1}$$

gdje si a_i, b_i *proizvoljni izrazi.* Jednostavan verižni razlomak *je verižni razlomak kojem su svi* b_i *jednaki* 1.

U cijelom radu ćemo se baviti isključivo s jednostavnim verižnim razlomcima, pa ćemo riječ "jednostavan" ubuduće izostavljati. Njih je puno jednostavnije zapisivati kao $\langle\, a_0, a_1, a_2, a_3, \dots \rangle$. Izrazi a_i se zovu *parcijalni kvocijenti*, a $\alpha_i = \langle\, a_i, a_{i+1}, \dots \rangle$ *potpuni kvocijenti.*

Konačan verižni razlomak je onaj koji ima konačno mnogo parcijalnih kvocijenata, tj. $\alpha = \langle\, a_0, a_1, a_2, \dots, a_n \rangle$.

Iako izraz (1.1) ima smisla i ako su a_i realni brojevi, polinomi ili bilo kakvi izrazi, parcijalni kvocijenti su tradicionalno uglavnom prirodni brojevi, a nama će ponekad biti i polinomi.

Regularan verižni razlomak je verižni razlomak dobiven sljedećim postupkom. Neka je α proizvoljan realan broj. S $\lfloor \alpha \rfloor$ ćemo označavati najveći cijeli broj koji nije veći od α, a s $\{\alpha\}$ realan broj $\alpha - \lfloor \alpha \rfloor$. Stavimo $\alpha_0 = \alpha$,

$$a_i = \lfloor \alpha_i \rfloor, \qquad \alpha_{i+1} = \frac{1}{\alpha_i - a_i}, \qquad i = 0, 1, 2 \dots . \tag{1.2}$$

Postupak završava ako dobijemo $a_n = \alpha_n$. Tako ćemo imati $a_0 \in \mathbb{Z}$ i $a_i \in \mathbb{N}, i = 1, 2, \dots .$

Regularne verižne razlomke ćemo zapisivati sa $[\,a_0, a_1, a_2, \dots\,]$. Uočimo da je razvoj u regularni verižni razlomak jedinstven.

1.1 Osnovna svojstva

Napomena 1.2. *Navedimo neka jednostavna svojstva verižnih razlomaka:*

(i) $\langle\, a_0, a_1, \dots, a_{n-1}, a_n \,\rangle = \langle\, a_0, a_1, \dots, a_{n-1}, a_n - 1, 1 \,\rangle$,

(ii) $\langle\, a_0, \dots, a_{n-1}, a_n, 0, a_{n+2}, a_{n+3}, \dots \,\rangle = \langle\, a_0, \dots, a_{n-1}, a_n + a_{n+2}, a_{n+3}, \dots \,\rangle$,

(iii) $\dfrac{1}{\langle\, a_0, a_1, \dots, a_n \,\rangle} = \langle\, 0, a_0, a_1, \dots, a_n \,\rangle$.

Uočimo da vrijedi

$$\alpha_i = a_i + \frac{1}{\alpha_{i+1}}, \quad 0 \le i < n,$$

pa tako dobijemo

$$\alpha_0 = a_0 + \cfrac{1}{a_1 + \cfrac{\ddots}{\ddots + \cfrac{1}{\alpha_i}}}, \quad 0 < i < n,$$

odnosno

$$\alpha_0 = \langle\, a_0, a_1, \dots, a_{i-1}, \alpha_i \,\rangle = a_0 + \frac{1}{\langle\, a_1, \dots, a_{i-1}, \alpha_i \,\rangle} = \langle\, a_0, a_1, \dots, a_{i-2}, a_{i-1} + \frac{1}{\alpha_i} \,\rangle.$$

Definicija 1.3. *Za $a_0, a_1, a_2, \dots, a_i, \dots$ definirajmo*

$$\begin{array}{lll} p_{-2} = 0, & p_{-1} = 1, & p_i = a_i p_{i-1} + p_{i-2}, \\ q_{-2} = 1, & q_{-1} = 0, & q_i = a_i q_{i-1} + q_{i-2}, \end{array} \quad za\ i \in \{0, \dots, n\}.$$

Teorem 1.4. *Za proizvoljan x i a_i, uz oznake kao u prethodnoj definiciji, vrijedi*

$$\langle\, a_0, a_1, \dots, a_i, x \,\rangle = \frac{x p_i + p_{i-1}}{x q_i + q_{i-1}}.$$

Dokaz. Za $i = 0$ imamo

$$\langle\, a_0, x \,\rangle = a_0 + \frac{1}{x} = \frac{x a_0 + 1}{x} = \frac{x p_0 + p_{-1}}{x q_0 + q_{-1}}.$$

Teorem dokažimo indukcijom. Pretpostavimo da tvrdnja vrijedi za neki $i-1$, tj. za $\langle\, a_0, a_1, \ldots, a_{i-1}, x \,\rangle$. Tada je

$$\begin{aligned}\langle\, a_0, a_1, \ldots, a_i, x \,\rangle &= \langle\, a_0, a_1, \ldots, a_{i-1}, a_i + \frac{1}{x} \rangle \\ &= \frac{(a_i + \frac{1}{x})p_{i-1} + p_{i-2}}{(a_i + \frac{1}{x})q_{i-1} + q_{i-2}} \\ &= \frac{x(a_i p_{i-1} + p_{i-2}) + p_{i-1}}{x(a_i q_{i-1} + q_{i-2}) + q_{i-1}} \\ &= \frac{xp_i + p_{i-1}}{xq_i + q_{i-1}}.\end{aligned} \tag{1.3}$$

□

Korolar 1.5. *Za svaki $n \geq 0$ vrijedi $\dfrac{p_n}{q_n} = \langle\, a_0, a_1, \ldots, a_n \,\rangle$.*

Primjer 1.6. *Izračunajmo $[\,7, 6, 5, 1, 2, 3, 4\,]$.*

i	-2	-1	0	1	2	3	4	5	6
p_i	0	1	7	43	222	265	752	2521	$10\,836$
q_i	1	0	1	6	31	37	105	352	1513

Dakle, $[\,7, 6, 5, 1, 2, 3, 4\,] = \dfrac{10\,836}{1513}$.

Definicija 1.7. *Za broj $\alpha = \langle\, a_0, a_1, a_2, \ldots \,\rangle$ razlomak $\dfrac{p_i}{q_i}$ zovemo i-ta* konvergenta broja α.

Iz

$$\alpha = \frac{\alpha_i p_{i-1} + p_{i-2}}{\alpha_i q_{i-1} + q_{i-2}}$$

slijedi

$$\alpha_i = -\frac{\alpha q_{i-2} - p_{i-2}}{\alpha q_{i-1} - p_{i-1}}. \tag{1.4}$$

Lako se vidi da je ispravan i sljedeći matrični račun, kojeg ćemo označavati indeksom ${}_M$:

$$\langle\, a_0, a_1, \ldots, a_n \,\rangle_M \stackrel{\text{def}}{=} \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}. \tag{1.5}$$

Na primjer,

$$\langle\, a_0, a_1 \,\rangle_M = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_0a_1 + 1 & a_0 \\ a_1 & 1 \end{pmatrix} = \begin{pmatrix} p_1 & p_0 \\ q_1 & q_0 \end{pmatrix}.$$

Napomena 1.8. *Možemo koristiti i donjetrokutaste matrice. Lako se vidi da je ispravan i sljedeći matrični račun*

$$\begin{pmatrix} q_{n-1} & q_n \\ p_{n-1} & p_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & a_0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix},$$

ali mi ćemo koristiti gornjetrokutaste matrice, to jest (1.5)*, jer su prisutnije u literaturi.*

Teorem 1.9. *Neka je* $\langle\, a_0, a_1, a_2, \dots \rangle$*. Za* $n \geq -1$ *vrijedi da je*

$$p_{n-1}q_n - p_n q_{n-1} = (-1)^n. \tag{1.6}$$

Dokaz. Za $n = -1$ tvrdnja se provjeri direktno, a budući je s desne strane jednakosti (1.5) determinanta svake matrice jednaka -1, vrijedi:

$$p_{n-1}q_n - p_n q_{n-1} = -\det \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = (-1)^n.$$

□

Iz prethodnog teorema zaključujemo da je razlomak $\dfrac{p_n}{q_n}$ skraćen, tj. $\operatorname{nzd}(p_n, q_n) = 1$. Vidi se i da je točno jedan od brojeva $q_n p_{n-1}$ i $p_n q_{n-1}$ paran (naravno ako su $a_i \in \mathbb{Z}$). Očito vrijedi i

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}. \tag{1.7}$$

Sličnim zaključivanjem možemo dobiti za $n \geq 0$

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n \qquad \text{i} \qquad \frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}}. \tag{1.8}$$

Naime, $p_0 q_{-2} - p_{-2} q_0 = a_0$, a općenito $p_n q_{n-2} - p_{n-2} q_n = (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) = a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = (-1)^n a_n$. Dijeljenjem sa $q_{n-2} q_n$ dobije se druga formula.

Transponiranjem matrične jednakosti (1.5) dobivamo

$$\frac{p_n}{p_{n-1}} = \langle\, a_n, a_{n-1}, \dots, a_2, a_1, a_0 \,\rangle \qquad \text{i} \qquad \frac{q_n}{q_{n-1}} = \langle\, a_n, a_{n-1}, \dots, a_2, a_1 \,\rangle. \tag{1.9}$$

Često ćemo koristiti konvergente verižnog razlomka bez a_0. Označavat ćemo ih sa $\dfrac{p'_n}{q'_n} = \langle\, a_1, a_2, \dots, a_n \,\rangle$. To jest $\dfrac{p_n}{q_n} = \langle\, a_0, \dfrac{p'_n}{q'_n} \rangle$. Očito vrijedi

$$\frac{p_n}{q_n} = \frac{a_0 p'_n + q'_n}{p'_n}, \tag{1.10}$$

odnosno:

$$\frac{p'_n}{q'_n} = \frac{q_n}{p_n - a_0 q_n}. \tag{1.11}$$

Napomena 1.10. *Ponegdje u literaturi (na primjer [33]) se za* $\langle a_k, a_{k+1}, \ldots, a_{k+n} \rangle$ *koriste oznake* $\frac{p_{k,n}}{q_{k,n}}$. *Budući da takve oznake kod nekih autora označavaju i sekundarne konvergente (koje doduše nećemo koristiti u ovoj radnji), a nama treba samo razvoj bez* a_0, *mi ćemo koristiti oznaku* $\frac{p'_n}{q'_n} = \frac{p_{1,n-1}}{q_{1,n-1}}$.

1.2 Konačni verižni razlomci — racionalni brojevi i Euklidov algoritam

Vratimo se sada razvoju u verižni razlomak realnog broja α. Jasno je da ako je verižni razlomak konačan i svi a_i (racionalni) brojevi, onda je i α racionalan broj. Naime, tada je

$$\alpha = \langle a_0, a_1, a_2, \ldots, a_n \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}.$$

Vrijedi i obrat — ako je $\alpha \in \mathbb{Q}$, tada je postupak (1.2) razvoja u regularni verižni razlomak konačan. Tj. postoji $n \in \mathbb{N}_0$, $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_n \in \mathbb{N}$ takvi da je $\alpha = [a_0, a_1, \ldots, a_n]$.

Naime, neka je $\alpha = \frac{a}{b}$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $\operatorname{nzd}(a, b) = 1$. Da bi uočili da je razvoj (1.2) konačan, prisjetimo se Euklidovog algoritma i stavimo $r_0 = a$, $r_1 = b$:

$$\begin{aligned}
r_0 &= r_1 \cdot a_0 + r_2, && 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot a_1 + r_3, && 0 < r_3 < r_2,\\
r_2 &= r_3 \cdot a_2 + r_4, && 0 < r_4 < r_3,\\
&\vdots\\
r_{n-1} &= r_n \cdot a_{n-1} + r_{n+1}, && 0 < r_{n+1} < r_n,\\
r_n &= r_{n+1} \cdot a_n,
\end{aligned}$$

tj. $\alpha_i = \frac{r_i}{r_{i+1}}$, $a_i = \lfloor \alpha_i \rfloor$, $i = 0, \ldots, n$. Lako se vidi da za duljinu razvoja vrijedi $n < 2 \log_2 b$ [7, Prop 1.6]. Euklidov algoritam ima najviše koraka za dva susjedna Fibonaccijeva broja, pa se može pokazati da vrijedi i nešto bolja ocjena [8, Tm 5.3] $n \leq \left\lceil \frac{\ln(\sqrt{5}b)}{\ln\left((1+\sqrt{5})/2\right)} \right\rceil - 2 \approx 2.078 \ln b + 1.672$.

Primjer 1.11. *Razvijmo broj* $\dfrac{215}{93}$ *u verižni razlomak.*

Razvoj u regularni verižni razlomak od $\frac{215}{93}$	*Euklidov algoritam za* $(215, 93)$
$\alpha_0 = \dfrac{215}{93}, \quad a_0 = \lfloor \alpha_0 \rfloor = 2,$	$215 = 93 \cdot 2 + 29,$
$\alpha_1 = \dfrac{1}{\alpha_0 - a_0} = \dfrac{93}{29}, \quad a_1 = \lfloor \alpha_1 \rfloor = 3,$	$93 = 29 \cdot 3 + 6,$
$\alpha_2 = \dfrac{1}{\alpha_1 - a_1} = \dfrac{29}{6}, \quad a_2 = \lfloor \alpha_2 \rfloor = 4,$	$29 = 6 \cdot 4 + 5,$
$\alpha_3 = \dfrac{1}{\alpha_2 - a_2} = \dfrac{6}{5}, \quad a_3 = \lfloor \alpha_3 \rfloor = 1,$	$6 = 5 \cdot 1 + 1,$
$\alpha_4 = \dfrac{1}{\alpha_3 - a_3} = \dfrac{5}{1}, \quad a_4 = \lfloor \alpha_4 \rfloor = 5 = \alpha_4,$	$5 = 1 \cdot 5,$

pa imamo $\dfrac{215}{93} = [\,2, 3, 4, 1, 5\,]$.

Napomena 1.12. *Uočimo da je matrica* (1.5) *unimodularna (determinanta joj je* ± 1*). Vrijedi i obrat. Neka su* p*,* q*,* r *i* s *prirodni brojevi takvi da vrijedi* $ps - qr = \pm 1$ *i* $p > q, p > r$*, tada postoji* $n \in \mathbb{N}$ *i jedinstvena* $(n+1)$*-torka prirodnih brojeva* $a_0, a_1, \ldots, a_n$ *takva da vrijedi*

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} = \langle\, a_0, a_1, \ldots, a_n \,\rangle_M.$$

Dokaz. Budući da su $p, q, r, s \in \mathbb{N}$ i zbog unimodularnosti vrijedi $q > s$ i $r > s$. Označimo sa $a_0 = \left\lfloor \frac{p}{q} \right\rfloor$. Imamo

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q & s \\ p - a_0 q & r - a_0 s \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p' & r' \\ q' & s' \end{pmatrix}.$$

Desna matrica je također unimodularna (jer je $\det \left(\begin{smallmatrix} a_0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = -1$), te vrijedi

$$q = p' > r' = s, \qquad p' > q',$$

$q' \in \mathbb{N}$ (zbog načina odabira a_0) i $s' \in \mathbb{N}$ (zbog unimodularnosti). Ponovo imamo matricu istog oblika, samo s manjim brojevima, pa vidimo da taj postupak mora završiti kada (za neki n) dobijemo $a_n = \left\lfloor \dfrac{p'}{q'} \right\rfloor = \dfrac{p'}{q'}$. □

Primjer 1.13. *Promotrimo unimodularnu matricu*

$$\begin{aligned}
\begin{pmatrix} 256 & 117 \\ 35 & 16 \end{pmatrix} &= \begin{pmatrix} 7 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 35 & 16 \\ 11 & 5 \end{pmatrix} && \left\lfloor \tfrac{256}{35} \right\rfloor = 7 \\
&= \begin{pmatrix} 7 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 11 & 5 \\ 2 & 1 \end{pmatrix} && \left\lfloor \tfrac{35}{11} \right\rfloor = 3 \\
&= \begin{pmatrix} 7 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} && \left\lfloor \tfrac{11}{2} \right\rfloor = 5 \\
&= \langle\, 7, 3, 5, 2 \,\rangle_M && \left\lfloor \tfrac{2}{1} \right\rfloor = \tfrac{2}{1} = 2.
\end{aligned}$$

1.3 Beskonačni verižni razlomci

Vidjeli smo da je razvoj u jednostavni verižni razlomak realnog broja α konačan ako i samo ako je $\alpha \in \mathbb{Q}$. Dakle, za beskonačni verižni razlomak znamo da je iracionalan. Za primjene u teoriji brojeva puno veću važnost imaju beskonačni verižni razlomci. Najprije pogledajmo neke primjere.

Primjer 1.14. *Neka je* $\alpha = [\,1, 1, 1, \ldots\,]$. *Tada iz* $\alpha = 1 + \dfrac{1}{[\,1, 1, 1, \ldots\,]} = 1 + \dfrac{1}{\alpha}$ *slijedi* $\alpha^2 - \alpha - 1 = 0$, *pa iz* $\alpha \geq 1$ *dobivamo* $\alpha = \dfrac{\sqrt{5}+1}{2}$.

Konvergente $\dfrac{p_n}{q_n}$ *zadovoljavaju rekurzije*

$$\begin{aligned}
p_0 &= 1, \qquad p_1 = 2, \qquad p_n = p_{n-1} + p_{n-2}, \\
q_0 &= 1, \qquad q_1 = 1, \qquad q_n = q_{n-1} + q_{n-2}.
\end{aligned}$$

Prema tome $p_n = F_{n+2}$, $q_n = F_{n+1}$, *gdje je* (F_n) *niz Fibonaccijevih brojeva definiranih sa* $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$.

Primjer 1.15. *Razvoj broja* $e = \displaystyle\sum_{k=0}^{\infty} \frac{1}{k!} \approx 2.718281828$ *u regularni verižni razlomak. Nije teško vidjeti da je* $2.718281828 = [\,2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1\,]$. *Naslućujemo da bi moglo vrijediti:*

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

To je već dugo poznato, a dokaz se može naći npr. u [38].

Teorem 1.16. *Neka su* $a_i \in \mathbb{N}$, *za* $i > 0$. *Vrijedi:*

(i) $\dfrac{p_0}{q_0} < \dfrac{p_2}{q_2} < \dfrac{p_4}{q_4} < \ldots,$

(ii) $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \dots,$

(iii) *Za svaki i paran i j neparan, vrijedi* $\frac{p_i}{q_i} < \frac{p_j}{q_j}$.

Dokaz. Iz (1.8) za i paran vrijedi $\frac{p_{i-2}}{q_{i-2}} < \frac{p_i}{q_i}$, a za j neparan $\frac{p_{j-2}}{q_{j-2}} > \frac{p_j}{q_j}$.

Preostaje dokazati tvrdnju (iii). Neka je $i < j$. Budući je $\frac{p_i}{q_i} \leq \frac{p_{j-1}}{q_{j-1}}$, dovoljno je dokazati $\frac{p_{j-1}}{q_{j-1}} < \frac{p_j}{q_j}$. No zadnja tvrdnja je točna po (1.6). Slučaj $i > j$ se dokazuje analogno. □

Teorem 1.17. *Neka su $\frac{p_i}{q_i}$ konvergente iracionalnog broja α. Postoji $\lim_{i\to\infty}\frac{p_i}{q_i}$, te za $j \geq 0$ vrijedi da je $\frac{p_{2j}}{q_{2j}} < \lim_{i\to\infty}\frac{p_i}{q_i} < \frac{p_{2j+1}}{q_{2j+1}}$, tj.*

$$\lim_{i\to\infty}\frac{p_i}{q_i} = \alpha.$$

Dokaz. Budući je $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \dots < \frac{p_1}{q_1}$ vidimo da postoji $\lim_{i\to\infty}\frac{p_{2i}}{q_{2i}}$. Na isti način vidimo da postoji i $\lim_{i\to\infty}\frac{p_{2i+1}}{q_{2i+1}}$. Ova dva limesa su jednaka jer je $\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} = \frac{(-1)^{i-1}}{q_i q_{i-1}}$ i zbog $q_i \geq i$ je $\lim_{i\to\infty}\frac{(-1)^i}{q_i q_{i-1}} = 0$. Neka je $\beta = \lim_{i\to\infty}\frac{p_i}{q_i}$.

Iz definicije brojeva $\alpha_1, \alpha_2, \dots$ slijedi da je $\alpha = \langle\, a_0, a_1, \dots, a_i, \alpha_{i+1}\,\rangle$, gdje je $0 < \frac{1}{\alpha_{i+1}} \leq \frac{1}{a_{i+1}}$. To znači da i α leži između brojeva $\frac{p_i}{q_i}$ i $\frac{p_{i+1}}{q_{i+1}}$. To jest $|\alpha - \beta| < \frac{1}{q_i q_{i+1}}$, odnosno $\alpha = \beta$. □

Rezultati slični onome u Primjeru 1.15 postoje i za druge poznatije matematičke konstante (zainteresirani čitatelj može pogledati [15]), ali budući da za primjene u teoriji brojeva najveću važnost imaju periodski verižni razlomci, takve primjere nećemo više spominjati.

Napomena 1.18. *Na iracionalnim brojevima možemo uvesti relaciju ekvivalencije na sljedeći način: $\alpha \sim \beta$ ako postoje cijeli brojevi p, q, r, s takvi da vrijedi $ps - qr = \pm 1$ i $\alpha = \frac{p\beta + q}{r\beta + s}$. Lako se vidi da je to uistinu relacija ekvivalencije i u [33, §17] je pokazano da je $\alpha \sim \beta$ ako i samo ako počevši od nekog mjesta α i β imaju jednake razvoje u regularni verižni razlomak.*

1.4 Periodski verižni razlomci i kvadratne iracionalnosti

Definicija 1.19. *Za beskonačni verižni razlomak* $\langle a_0, a_1, a_2, \dots \rangle$ *kažemo da je* periodski *ako postoje cijeli brojevi* $h \geq 0$, $\ell \geq 1$ *takvi da je* $a_{\ell+k} = a_k$ *za sve* $k \geq h$. *U tom slučaju verižni razlomak pišemo u obliku*

$$\langle a_0, a_1, \dots, a_{h-1}, \overline{a_h, a_{h+1}, \dots, a_{h+\ell-1}} \rangle,$$

gdje "crta" iznad brojeva $a_h, \dots, a_{h+\ell-1}$ *znači da se taj blok brojeva ponavlja u nedogled. Nadalje, pretpostavljamo da je broj* ℓ *najmanji broj s gornjim svojstvom, te ga zovemo* duljina perioda.

Za periodski verižni razlomak kažemo da je čisto periodski *ako je* $h = 0$, *tj. ako nema početni blok koji se ne ponavlja.*

U Primjeru 1.14 smo imali razlomak $[1, 1, 1, \dots] = [\overline{1}]$.

Primjer 1.20. *(i) Neka je* $\beta = [3, 4, 3, 4, \dots] = [\overline{3, 4}]$. *Tada je* $\beta = 3 + \dfrac{1}{4 + \frac{1}{\beta}}$. *Sređivanjem izraza dobijemo* $\beta = \dfrac{13\beta + 3}{4\beta + 1}$, *tj.* $4\beta^2 - 12\beta - 3 = 0$, *pa zbog* $\beta > 0$, *dobivamo* $\beta = \dfrac{3 + 2\sqrt{3}}{2}$.

(ii) Neka je sada $\alpha = [2, 3, \overline{3, 4}]$. *Uočimo da je* $\alpha = [2, 3, \beta]$. *Imamo*

$$\alpha = 2 + \frac{1}{3 + \frac{1}{\beta}} = 2 + \frac{\beta}{3\beta + 1} = \frac{23 + 4\sqrt{3}}{13}.$$

Ovaj primjer ilustrira opću situaciju.

Definicija 1.21. *Za iracionalan broj* α *kažemo da je* kvadratna iracionalnost *ako je* α *korijen kvadratne jednadžbe s racionalnim (cjelobrojnim) koeficijentima i pozitivnom diskriminantom.*

Teorem 1.22 (Euler)**.** *Ako je* α *periodski verižni razlomak, tada je* α *kvadratna iracionalnost.*

Dokaz. Neka je $\alpha = [a_0, a_1, \dots, a_{h-1}, \overline{a_h, a_{h+1}, \dots, a_{h+\ell-1}}]$, te neka je neka je β čisto periodski dio od α, tj. $\beta = [\overline{a_h, a_{h+1}, \dots, a_{h+\ell-1}}] = [\overline{b_0, b_1, \dots, b_{\ell-1}}]$. Iz

$$\beta = [b_0, b_1, \dots, b_{\ell-1}, \beta],$$

slijedi

$$\beta = \frac{\beta r_{\ell-1} + r_{\ell-2}}{\beta s_{\ell-1} + s_{\ell-2}},$$

gdje je $\frac{r_i}{s_i}$ i-ta konvergenta broja β. To je kvadratna jednadžba za β s cjelobrojnim koeficijentima i pozitivnom diskriminantom. Budući da β nema konačan razvoj u verižni razlomak, β nije racionalan, pa vidimo da je kvadratna iracionalnost.

Vratimo se sada broju $\alpha = [\,a_0, a_1, \ldots, a_{h-1}, \beta\,]$. Neka su $\frac{p_i}{q_i}$ konvergente od $\alpha = [\,a_0, a_1, \ldots, a_{h-1}, \ldots\,]$. Tada vrijedi da je

$$\alpha = \frac{\beta p_{h-1} + p_{h-2}}{\beta q_{h-1} + q_{h-2}}.$$

Kako je β kvadratna iracionalnost, vidimo da je i α kvadratna iracionalnost. □

Kvadratna jednadžba $ax^2 + bx + c = 0$, gdje su $a, b, c \in \mathbb{Z}$, $a \neq 0$, kojoj diskriminanta $d = b^2 - 4ac$ nije kvadrat prirodnog broja ima dva rješenja:

$$\alpha_{1,2} = \frac{-b \pm \sqrt{d}}{2a}.$$

Kako su koeficijenti jednadžbe racionalni, rješenja ćemo označavati sa α i $\overline{\alpha}$ [1].

Primjer 1.23. *Razvijmo broj* $\alpha = \frac{4+\sqrt{37}}{7}$ *u verižni razlomak. Radi jednostavnosti uočimo prvo da je* $\lfloor\sqrt{37}\rfloor = 6$*, te stavimo* $\alpha_0 = \alpha$ *i slijedimo postupak* (1.2)

$$a_0 = \lfloor\alpha_0\rfloor = \left\lfloor\frac{4+\sqrt{37}}{7}\right\rfloor = 1,$$

$$\alpha_1 = \frac{1}{\alpha - a_0} = \frac{1}{\frac{4+\sqrt{37}}{7} - 1} = \frac{7}{\sqrt{37}-3}\cdot\frac{\sqrt{37}+3}{\sqrt{37}+3} = \frac{7(\sqrt{37}+3)}{37-3^2} = \frac{\sqrt{37}+3}{4},$$

$$a_1 = \lfloor\alpha_1\rfloor = 2,$$

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{\frac{\sqrt{37}+3}{4} - 2} = \frac{4}{\sqrt{37}-5}\cdot\frac{\sqrt{37}+5}{\sqrt{37}+5} = \frac{4(\sqrt{37}+5)}{37-5^2} = \frac{\sqrt{37}+5}{3},$$

$$a_2 = \lfloor\alpha_2\rfloor = 3,$$

$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{1}{\frac{\sqrt{37}+5}{3} - 3} = \frac{3}{\sqrt{37}-4}\cdot\frac{\sqrt{37}+4}{\sqrt{37}+4} = \frac{3(\sqrt{37}+4)}{37-4^2} = \frac{\sqrt{37}+4}{7}.$$

Kako je $\alpha_3 = \alpha_0$*, vidimo da će se postupak ponavljati u nedogled, te imamo*

$$\alpha_3 = [\,\overline{1, 2, 3}\,].$$

[1] Za $\overline{\alpha}$ kažemo da je konjugat od α u smislu Definicije 2.10.

Iz ovog primjera možemo sastaviti postupak za rastav kvadratne iracionalnosti u regularni verižni razlomak. Neka je $d \in \mathbb{N}, d \neq \square$ i $\alpha_0 = \dfrac{s_0 + \sqrt{d}}{t_0}$ kvadratna iracionalnost, tj. $s_0, t_0 \in \mathbb{Z}$, $t_0 \neq 0$ i takva da je $t_0 \mid (d - s_0^2)$. Za $i \geq 0$ imamo:

$$a_i = \lfloor \alpha_i \rfloor, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}, \quad \alpha_{i+1} = \frac{s_{i+1} + \sqrt{d}}{t_{i+1}}. \tag{1.12}$$

Propozicija 1.24. *Postupak* (1.12) *je zaista razvoj u regularni verižni razlomak proizvoljne kvadratne iracionalnosti α (tj. ekvivalentan je postupku* (1.2)*).*

Dokaz. Neka je $\alpha = \dfrac{a + \sqrt{b}}{c}$, $a, c \in \mathbb{Z}$, $b \in \mathbb{N}, b \neq \square$, $c \neq 0$ kvadratna iracionalnost. Množeći brojnik i nazivnik od α sa $|c|$ dobivamo

$$\alpha = \frac{ac + \sqrt{bc^2}}{c^2} \qquad \text{ili} \qquad \alpha = \frac{-ac + \sqrt{bc^2}}{-c^2},$$

u ovisnosti o tome da li je c pozitivan ili negativan. Stoga bez smanjenja općenitosti α možemo zapisati u obliku

$$\alpha = \frac{s_0 + \sqrt{d}}{t_0},$$

gdje su $s_0, t_0 \in \mathbb{Z}$, $t_0 \neq 0$ i takvi da $t_0 \mid (d - s_0^2)$. Iz (1.2) imamo

$$\alpha_{i+1} = \frac{1}{\alpha_i - a_i} = \frac{t_i}{s_i + \sqrt{d} - a_i t_i} = \frac{t_i}{\sqrt{d} - s_{i+1}} = \frac{t_i(\sqrt{d} + s_{i+1})}{d - s_{i+1}^2} = \frac{\sqrt{d} + s_{i+1}}{t_{i+1}},$$

pa je zaista $\alpha = [a_0, a_1, \dots]$.

Pokažimo sada matematičkom indukcijom da su $s_i, t_i \in \mathbb{Z}$ takvi da je $t_i \neq 0$ i $t_i \mid (d - s_i^2)$. Po pretpostavci to vrijedi za $i = 0$. Ako tvrdnja vrijedi za neki i, onda iz $s_{i+1} = a_i t_i - s_i$ slijedi da je broj s_{i+1} cijeli. Relacija

$$t_{i+1} = \frac{d - s_{i+1}^2}{t_i} = \frac{d - s_i^2}{t_i} + 2a_i s_i - a_i^2 t_i$$

pokazuje da je i t_{i+1} cijeli broj. Nadalje, $t_{i+1} \neq 0$, jer bi inače $d = s_{i+1}^2$ bio potpun kvadrat. Konačno, iz $t_i = \dfrac{d - s_{i+1}^2}{t_{i+1}}$ slijedi $t_{i+1} \mid (d - s_{i+1}^2)$. □

Već je Lagrange znao da je taj razvoj periodan, a mi ćemo to dokazati u sljedećem teoremu.

Teorem 1.25 (Lagrange)**.** *Neka je α kvadratna iracionalnost, tj. neka je $\alpha = \dfrac{a + \sqrt{b}}{c}$, $a, b, c \in \mathbb{Z}$, $b > 0$, $b \neq \square$ i $c \neq 0$. Tada je α periodski verižni razlomak.*

Dokaz. Neka je α_i iz postupka (1.12). Sa $\overline{\alpha_i}$ označimo konjugat od α_i, tj. $\overline{\alpha_i} = \dfrac{s_i - \sqrt{d}}{t_i}$. Budući je konjugat kvocijenta jednak kvocijentu konjugata, imamo $\overline{\alpha_0} = \dfrac{\overline{\alpha_i}p_{i-1} + p_{i-2}}{\overline{\alpha_i}q_{i-1} + q_{i-2}}$. Odavde je

$$\overline{\alpha_i} = -\frac{\overline{\alpha_0}q_{i-2} - p_{i-2}}{\overline{\alpha_0}q_{i-1} - p_{i-1}} = -\frac{q_{i-2}}{q_{i-1}}\left(\frac{\overline{\alpha_0} - \frac{p_{i-2}}{q_{i-2}}}{\overline{\alpha_0} - \frac{p_{i-1}}{q_{i-1}}}\right).$$

Kada $i \to \infty$, $\frac{p_{i-1}}{q_{i-1}}$ i $\frac{p_{i-2}}{q_{i-2}}$ teže prema α_0, a $\alpha_0 \neq \overline{\alpha_0}$, pa izraz u zagradi teži prema 1, te je zbog toga pozitivan za dovoljno veliki i, recimo za $i > k$. Za takav i vrijedi $-1 < \overline{\alpha_i} < 0$. Kako je $\alpha_i > 1$ za $i \geq 1$ imamo:

$$\alpha_i - \overline{\alpha_i} = \frac{2\sqrt{d}}{t_i} > 0 \quad \Longrightarrow \quad t_i > 0 \tag{1.13a}$$

$$\alpha_i + \overline{\alpha_i} = \frac{2s_i}{t_i} > 0 \quad \Longrightarrow \quad s_i > 0 \tag{1.13b}$$

$$\overline{\alpha_i} = \frac{s_i - \sqrt{d}}{t_i} < 0 \quad \Longrightarrow \quad s_i < \sqrt{d} \tag{1.13c}$$

$$\overline{\alpha_i} = \frac{s_i - \sqrt{d}}{t_i} > -1 \quad \Longrightarrow \quad \sqrt{d} - s_i < t_i$$

$$\alpha_i = \frac{s_i + \sqrt{d}}{t_i} > 1 \quad \Longrightarrow \quad t_i < \sqrt{d} + s_i, \tag{1.13d}$$

pa su s_i i t_i pozitivni brojevi takvi da $s_i < \sqrt{d}$ i $\sqrt{d} - s_i < t_i < \sqrt{d} + s_i$. Odavde slijedi da uređeni parovi (s_i, t_i) mogu poprimiti samo konačno mnogo vrijednosti, pa postoje prirodni brojevi k i l, takvi da je $k < l$, $s_k = s_l$ i $t_k = t_l$. Sada vidimo da je $\alpha_k = \alpha_l$, pa je

$$\alpha = [\, a_0, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{l-1}}\,],$$

što je i trebalo dokazati. □

Uočimo da u periodnom dijelu razvoja $\alpha_i = \dfrac{s_i + \sqrt{d}}{t_i} > \sqrt{d}$ povlači $s_i > \sqrt{d}(t_i - 1)$, a vrijedi i $s_i < \sqrt{d}$. Stoga je $\alpha_i > \sqrt{d}$ ako i samo ako je $t_i = 1$, pa vidimo da su $a_i < \sqrt{d}$, osim kada je $t_i = 1$, a u tom slučaju vrijedi $a_i < 2\sqrt{d}$.

Primjer 1.26. *Razvijmo broj* $\alpha = \frac{3214+\sqrt{37}}{1661}$ *u verižni razlomak. Imamo* $d = 37, s_0 = 3214, t_0 = 1661$. *Vidimo da vrijedi* $t_0 \mid (d - s_0^2)$, *pa počnimo s postup-*

kom (1.12)*:*

i	s_i	t_i	α_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 $s_3 = s_6$, $t_3 = t_6$, *pa će biti i* $\alpha_3 = \alpha_6$, *pa dobivamo* $\alpha = [\,1, 1, 15, \overline{3, 2, 1}\,]$. *Ovdje je "dovoljno veliki* i*" bio* $i > 2$, *jer je vrijedilo* $-1 < \overline{\alpha_3} < 0$, *odnosno* a_3 *je bio početak perioda.*

Uočimo da je osnovna ideja dokaza prethodnog teorema bila da za dovoljno veliki i vrijedi $-1 < \overline{\alpha_i} < 0$ (i $\alpha_i > 1$).

1.5 Reducirani brojevi i čista periodnost

Definicija 1.27. *Za kvadratnu iracionalnost* α *kažemo da je* reducirana *ako vrijedi* $\alpha > 1$ *i* $-1 < \overline{\alpha} < 0$.

Teorem 1.28 (Galois)**.** *Kvadratna iracionalnost* α *ima čisto periodski razvoj u regularni verižni razlomak ako i samo ako je reducirana.*

Dokaz. Pretpostavimo da je razvoj od α čisto periodski.

$$\alpha = [\,\overline{a_0, a_1, \ldots, a_{\ell-1}}\,],$$

$a_0, a_1, \ldots, a_{\ell-1} \in \mathbb{N}$ (zbog $a_0 = a_\ell$). Imamo $\alpha > a_0 \geq 1$. Također je

$$\alpha = [\,a_0, a_1, \ldots, a_{\ell-1}, \alpha\,] = \frac{\alpha p_{\ell-1} + p_{\ell-2}}{\alpha q_{\ell-1} + q_{l-2}}.$$

Prema tome, α zadovoljava jednadžbu

$$f(x) = x^2 q_{\ell-1} + x(q_{\ell-2} - p_{\ell-1}) - p_{\ell-2} = 0.$$

Koeficijenti su racionalni (točnije cjelobrojni), pa je drugi korijen $\overline{\alpha}$. Budući je $\alpha > 1$, dovoljno je provjeriti da $f(x)$ ima korijen između -1 i 0. To možemo provjeriti tako da pokažemo da $f(-1)$ i $f(0)$ imaju različite predznake.

$$f(0) = -p_{\ell-2} < 0 \qquad \text{i} \qquad f(-1) = (q_{\ell-1} - q_{\ell-2}) + (p_{\ell-1} - p_{\ell-2}) > 0,$$

pa vidimo da je α reducirana.

Obratno, neka je $\alpha > 1$ i $-1 < \overline{\alpha} < 0$. Stavimo $\alpha_0 = \alpha$, te definirajmo $a_i = \lfloor \alpha_i \rfloor$ i α_{i+1} rekurzivno sa $\frac{1}{\alpha_{i+1}} = \alpha_i - a_i$. Tada je

$$\frac{1}{\overline{\alpha_{i+1}}} = \overline{\left(\frac{1}{\alpha_{i+1}}\right)} = \overline{\alpha_i} - a_i. \tag{1.14}$$

Lako se vidi da za svaki $i \geq 0$ vrijedi $a_i \geq 1$. Zbog toga, ako je $\overline{\alpha_i} < 0$, onda je i $\frac{1}{\overline{\alpha_{i+1}}} < -1$, odnosno $-1 < \overline{\alpha_{i+1}} < 0$. Budući je $-1 < \overline{\alpha_0} < 0$, indukcijom slijedi da je $-1 < \overline{\alpha_i} < 0$ za sve $i \geq 0$. Sada iz (1.14) slijedi

$$0 < -\frac{1}{\overline{\alpha_{i+1}}} - a_i < 1, \qquad \text{tj. } a_i = \left\lfloor -\frac{1}{\overline{\alpha_{i+1}}} \right\rfloor.$$

Pretpostavimo da α nije čisto periodski, tj. da je oblika

$$\alpha = [\, a_0, a_1, \ldots, a_{h-1}, \overline{a_h, a_{h+1}, \ldots, a_{h+\ell-1}}\,],$$

gdje je $h \geq 1$. Tada je $a_{h-1} \neq a_{h+\ell-1}$, jer bi u protivnom period počeo jedno mjesto ranije. Svakako vrijedi $\alpha_h = \alpha_{h+\ell}$, pa je i $\overline{\alpha_h} = \overline{\alpha_{h+\ell}}$, te imamo

$$a_{h-1} = \left\lfloor -\frac{1}{\overline{\alpha_h}} \right\rfloor = \left\lfloor -\frac{1}{\overline{\alpha_{h+\ell}}} \right\rfloor = a_{h+\ell-1},$$

$$\alpha_{h-1} = a_{h-1} + \frac{1}{\alpha_h} = a_{h+\ell-1} + \frac{1}{\alpha_{h+\ell}} = \alpha_{h+\ell-1}.$$

Vidimo da vrijedi $a_{h-1} = a_{h+\ell-1}$, tj. dobili smo kontradikciju s pretpostavkom da je $h \geq 1$. □

Napomena 1.29. *Uočimo da se iz drugog dijela dokaza prethodnog teorema vidi da ako je α_0 reducirana, tj. $\alpha_0 = [\, \overline{a_0, a_1, \ldots, a_{\ell-2}, a_{\ell-1}}\,]$, tada vrijedi*

$$-\frac{1}{\overline{\alpha_0}} = [\, \overline{a_{\ell-1}, a_{\ell-2}, \ldots, a_1, a_0}\,].$$

Odnosno iz $\alpha_i = \dfrac{s_i + \sqrt{d}}{t_i}$ i $\overline{\alpha_i} = \dfrac{s_i - \sqrt{d}}{t_i}$ imamo (uz $t_{-1} = t_{\ell-1}$):

$$-\frac{1}{\overline{\alpha_i'}} = \frac{t_i}{\sqrt{d} - s_i} = \frac{t_i(\sqrt{d} + s_i)}{d - s_i^2} \overset{(1.12)}{=} \frac{\sqrt{d} + s_i}{t_{i-1}}. \tag{1.15}$$

Primjetimo da ako je α proizvoljna kvadratna iracionalnost kojoj je periodni dio $\overline{a_h, a_{h+1}, \ldots, a_{\ell-1}}$, tada je periodni dio od $\overline{\alpha}$ obrnut, tj. $\overline{a_{\ell-1}, a_{\ell-2}, \ldots, a_{h-1}, a_h}$. Na primjer:

$$\alpha = \frac{14 - \sqrt{37}}{3} = [\, 2, 1, 1, \overline{1, 3, 2}\,], \qquad \overline{\alpha} = \frac{14 + \sqrt{37}}{3} = [\, 6, \overline{1, 2, 3}\,] = [\, 6, 1, \overline{2, 3, 1}\,].$$

Napomena 1.30. *Spomenimo da ako razvoj u verižni razlomak nije regularan, kvadratna iracionalnost ne mora biti reducirana da bi dobili čisto periodski razvoj. Na primjer, vidjet ćemo u Teoremu 1.32 da za $d \in \mathbb{N}, d \neq \square$ imamo $\sqrt{d} = [\, a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}\,]$, pa vrijedi i $\sqrt{d} = \langle\, \overline{a_0, a_1, a_2, \ldots, a_2, a_1, a_0, 0}\,\rangle$.*

1.6 Palindromski periodni dio i $\sqrt{d}$, $d \in \mathbb{Q}$, $d \neq \square$

Teorem 1.31. *Neka je $d \in \mathbb{N}, d \neq \square$, te neka su $\frac{p_n}{q_n}$ pripadne konvergente od $\sqrt{d}$, te s_n, t_n kao iz (1.12). Tada za $n \geq -1$ vrijedi*

$$p_n^2 - dq_n^2 = (-1)^{n+1} t_{n+1},$$
$$p_n p_{n-1} - dq_n q_{n-1} = (-1)^n s_{n+1}.$$

Dokaz. Iz (1.12) imamo

$$\sqrt{d} = \alpha_0 = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} = \frac{(s_{n+1} + \sqrt{d}) p_n + t_{n+1} p_{n-1}}{(s_{n+1} + \sqrt{d}) q_n + t_{n+1} q_{n-1}}.$$

Budući je $\sqrt{d}$ iracionalan, odavde slijedi

$$s_{n+1} q_n + t_{n+1} q_{n-1} - p_n = 0, \qquad s_{n+1} p_n + t_{n+1} p_{n-1} - dq_n = 0.$$

Eliminirajući s_{n+1} dobijemo prvu jednakost

$$p_n^2 - dq_n^2 = (p_n q_{n-1} - p_{n-1} q_n) t_{n+1} \overset{(1.6)}{=} (-1)^{n-1} t_{n+1},$$

a eliminirajući t_{n+1} drugu

$$p_n p_{n-1} - dq_n q_{n-1} = (p_{n-1} q_n - p_n q_{n-1}) s_{n-1} \overset{(1.6)}{=} (-1)^n s_{n+1}.$$

□

Teorem 1.32. *Neka je $d \in \mathbb{Q}$, $d \neq \square$, $d > 1$. Tada razvoj u jednostavni verižni razlomak od $\sqrt{d}$ ima oblik*

$$\sqrt{d} = [\, a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0} \,],$$

tj. $a_0 = \lfloor \sqrt{d} \rfloor$, a dio razvoja od a_1 do $a_{\ell-1}$ je palindroman (centralno simetričan).

Dokaz. Promotrimo broj $\beta = \sqrt{d} + \lfloor \sqrt{d} \rfloor$. Očito je broj β reduciran, pa po Teoremu 1.28 ima čisto periodan razvoj

$$\sqrt{d} + \lfloor \sqrt{d} \rfloor = [\, \overline{b_0, b_1, \ldots, b_{\ell-1}} \,] = [\, b_0, \overline{b_1, \ldots, b_{\ell-1}, b_0} \,].$$

Razvoji od β i $\sqrt{d}$ razlikuju se samo u prvom članu, tj. $b_i = a_i$, za $i \geq 1$. Uočimo da je $b_0 = \left\lfloor \sqrt{d} + \lfloor \sqrt{d} \rfloor \right\rfloor = 2\lfloor \sqrt{d} \rfloor$. Sada je

$$\begin{aligned} \sqrt{d} = -\lfloor \sqrt{d} \rfloor + \beta &= -\lfloor \sqrt{d} \rfloor + [\, 2\lfloor \sqrt{d} \rfloor, \overline{b_1, \ldots, b_{\ell-1}, b_0} \,] \\ &= [\, \lfloor \sqrt{d} \rfloor, \overline{b_1, \ldots, b_{\ell-1}, b_0} \,]. \end{aligned} \tag{1.16}$$

Da bi dokazali centralnu simetričnost, uočimo da je $\beta = b_0 + \frac{1}{\beta_1}$, gdje je

$$\beta_1 = \frac{1}{\sqrt{d} - \lfloor \sqrt{d} \rfloor} = -\frac{1}{\overline{\beta}} = -\frac{1}{\overline{\beta_\ell}} \overset{(1.14)}{=} [\, b_{\ell-1}, -\frac{1}{\overline{\beta_{\ell-1}}}\,] = \dots$$
$$= [\, b_{\ell-1}, b_{\ell-2}, \dots, b_0, -\frac{1}{\overline{\beta}}\,] = [\, \overline{b_{\ell-1}, b_{\ell-2}, \dots, b_0}\,]. \quad (1.17)$$

Dakle, $\beta = [\, b_0, \overline{b_{\ell-1}, b_{\ell-2}, \dots, b_0}\,]$. Usporedimo li ovo s (1.16), dobivamo: $b_1 = b_{\ell-1}$, $b_2 = b_{\ell-2}$, ... □

Teorem 1.33 (Muir)**.** *Neka je* $\alpha_0 = \dfrac{\sqrt{d}}{t_0}$ *iracionalan broj, takav da* $t_0 \mid d$ *i* $t_0 < \sqrt{d}$*. Neka su* s_i, t_i *i* α_i *kao u postupku* (1.12)*. Tada su sva tri niza*

$$\begin{array}{cccccccc} & a_1, & a_2, & \dots, & a_{\ell-2}, & a_{\ell-1}, & \\ & s_1, & s_2, & \dots, & s_{\ell-2}, & s_{\ell-1}, & s_\ell, \\ t_0, & t_1, & t_2, & \dots, & t_{\ell-2}, & t_{\ell-1}, & t_\ell \end{array}$$

palindromni, tj.

$$\begin{aligned} a_i &= a_{\ell-i}, & i &= 1, 2, \dots, \ell-1, \\ s_{i+1} &= s_{\ell-i}, & i &= 0, 1, \dots, \ell-1, \\ t_i &= t_{\ell-i}\,, & i &= 0, 1, \dots, \ell. \end{aligned}$$

Dokaz. Prema Teoremu 1.32 vrijedi $\alpha_0 = [\, a_0, \overline{a_1, a_2, \dots, a_2, a_1, 2a_0}\,]$. Tada se α_i iz postupka (1.2) ponavljaju za $i \geq 1$, što ćemo označavati linijom iznad:

$$\alpha_0 = \frac{\sqrt{d}}{t_0}, \qquad \overline{\alpha_1 = \frac{s_1 + \sqrt{d}}{t_1}, \qquad \alpha_2 = \frac{s_2 + \sqrt{d}}{t_2}, \quad \dots, \quad \alpha_\ell = \frac{s_\ell + \sqrt{d}}{t_\ell}},$$

te vrijedi

$$\alpha_\ell = [\, 2a_0, \overline{a_1, a_2, \dots, a_2, a_1, 2a_0}\,] = \alpha_0 + a_0 = \frac{a_0 t_0 + \sqrt{d}}{t_0},$$

pa slijedi

$$t_\ell = t_0, \qquad s_\ell = a_0 t_0.$$

Promotrimo potpune kvocijente broja $\alpha_1 = [\, \overline{a_1, a_2, \dots, a_2, a_1, 2a_0}\,]$, koji je čisto periodan. Oni su redom:

$$\overline{\frac{s_1 + \sqrt{d}}{t_1}, \qquad \frac{s_2 + \sqrt{d}}{t_2}, \quad \dots, \quad \frac{s_\ell + \sqrt{d}}{t_\ell}}.$$

Pogledajmo i broj s inverznim periodom $[\, \overline{2a_0, a_1, a_2, \dots, a_2, a_1}\,]$ koji je također čisto periodan, pa su prema (1.15) njegovi potpuni kvocijenti (uz $t_0 = t_\ell$):

$$\overline{\frac{s_1 + \sqrt{d}}{t_0}, \qquad \frac{s_\ell + \sqrt{d}}{t_{\ell-1}}, \qquad \frac{s_{\ell-1} + \sqrt{d}}{t_{\ell-2}}, \quad \dots, \quad \frac{s_3 + \sqrt{d}}{t_2}, \quad \frac{s_2 + \sqrt{d}}{t_1}}.$$

S druge strane, to je i razvoj broja $a_0 + \alpha_0$, čiji potpuni kvocijenti su $\alpha_0 + a_0, \overline{\alpha_1, \alpha_2, \ldots, \alpha_\ell}$, pa specijalno vrijedi

$$\alpha_\ell = \frac{s_1 + \sqrt{d}}{t_0}, \quad \alpha_1 = \frac{s_\ell + \sqrt{d}}{t_{\ell-1}}, \quad \alpha_2 = \frac{s_{\ell-1} + \sqrt{d}}{t_{\ell-2}}, \quad \ldots, \quad \alpha_{\ell-1} = \frac{s_2 + \sqrt{d}}{t_1}.$$

Kako je $\alpha_i = \dfrac{s_i + \sqrt{d}}{t_i}$ imamo:

$$\begin{aligned} s_\ell &= s_1, & s_{\ell-1} &= s_2, & \ldots, & & s_1 &= s_\ell, \\ t_{\ell-1} &= t_1, & t_{\ell-2} &= t_2, & \ldots, & & t_0 &= t_\ell, \end{aligned}$$

pa slijedi tvrdnja teorema. □

Iz ove simetričnosti slijedi da ako je ℓ paran, dva uzastopna jednaka s_i-a će se pojaviti, naime $s_{\ell/2} = s_{\ell/2+1}$. Nadalje, ako je ℓ neparan, pojaviti će se dva uzastopna jednaka t_i-a, naime $t_{(\ell-1)/2} = t_{(\ell+1)/2}$.

Za praktičnu primjenu, puno je bitnija obrnuta činjenica: Dva uzastopna jednaka broja s_i ili t_i se mogu pojaviti samo na sredini primitivnog perioda.

Stoga promotrimo to malo detaljnije. Neka je α_0 kao u prethodnom teoremu. Kako je $t_0 < \sqrt{d}$, period ne može početi sa a_0, pa su svi brojevi

$$\alpha_0, \alpha_1, \ldots, \alpha_\ell \tag{1.18}$$

međusobno različiti. Po prethodnom teoremu imamo

$$\alpha_{\ell-i} = \frac{s_{\ell-i} + \sqrt{d}}{t_{\ell-i}} = \frac{s_{i+1} + \sqrt{d}}{t_i}, \qquad \text{za } i = 0, 1, \ldots, \ell - 1. \tag{1.19}$$

Ako se dogodi $s_i = s_{i+1}$, imamo

$$\alpha_{\ell-i} = \frac{s_i + \sqrt{d}}{t_i} = \alpha_i,$$

a budući su svi brojevi (1.18) različiti, slijedi $\ell - i = i$. Stoga je ℓ paran i vrijedi $i = \frac{\ell}{2}$. Nadalje, simetrični dio perioda je neparan, te na sredini imamo broj $a_{\ell/2}$.

Ako se dogodi $t_i = t_{i+1}$, imamo

$$\alpha_{\ell-i} = \frac{s_{i+1} + \sqrt{d}}{t_{i+1}} = \alpha_{i+1},$$

pa imamo $\ell - i = i + 1$. To jest, ℓ je neparan i vrijedi $i = \frac{\ell-1}{2}$. Nadalje, simetrični dio perioda je paran, te na sredini imamo dva broja $a_{(\ell-1)/2} = a_{(\ell+1)/2}$.

Upravo smo dokazali sljedeći teorem.

Teorem 1.34 (Muir)**.** *Neka je α_0 kao u Teoremu 1.33. Tada se tijekom perioda samo na jednom mjestu može dogoditi ili $s_i = s_{i+1}$ ili $t_i = t_{i+1}$.*

Napomena 1.35. *Da bi odredili period i duljinu perioda razvoja u jednostavni verižni razlomak od $\sqrt{d}$, postupak* (1.12) *možemo provesti samo do pola. Naime ako se dogodi*

(i) *$s_i = s_{i+1}$, tada znamo da je duljina perioda parna, tj. $\ell = 2i$,*

(ii) *$t_i = t_{i+1}$, tada znamo da je duljina perioda neparna, tj. $\ell = 2i + 1$.*

Primjer 1.36. *Da bismo razvili $\sqrt{\frac{11}{7}}$ u verižni razlomak, zapišimo ga u obliku*

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

Budući je sada $s_0 = 0$, $t_0 = 7$, $d = 77$, vrijedi $t_0 \mid (d - s_0^2)$. Slijedeći postupak (1.12) *dobivamo*

i	0	1	2	3	4	5	6	
s_i	0	**7**	5	*8*	*8*	5	7	7
t_i	7	**4**	13	1	13	4	7	4
a_i	1	3	1	16	1	3	2	

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

Uočimo da ako je $0 < d < 1$, a sve ostale pretpostavke Teorema 1.32 su zadovoljene, tada razvoj u jednostavni verižni razlomak od $\sqrt{d}$ ima oblik

$$[\,0, a_0, \overline{a_1, a_2, \ldots, a_{\ell-2}, a_{\ell-1}, 2a_0}\,],$$

gdje je $\sqrt{1/d} = [\,a_0, \overline{a_1, a_2, \ldots, a_{\ell-2}, a_{\ell-1}, 2a_0}\,]$.

Napomena 1.37. *Ako je period u razvoju od $\sqrt{d}$ neparan, npr. $\ell = 2r + 1$, tada prema Teoremu 1.33 vrijedi*

$$t_i = t_{2r+1-i}, \qquad \text{za } i = 0, 1, \ldots, 2r + 1,$$

pa specijalno za $i = r$ imamo

$$t_r = t_{r+1}.$$

Prema (1.12) *iz $d - s_{i+1}^2 = t_i t_{i+1}$ za $i = r$ slijedi*

$$d - s_{r+1}^2 = t_r t_{r+1} = t_{r+1}^2, \tag{1.20}$$

pa smo na taj način broj d rastavili na zbroj kvadrata.

Općenito s_{r+1} i t_{t+1} ne moraju biti relativno prosti (na primjer $\frac{\sqrt{40}}{4} = [\,1, \overline{1, 1, 2}\,]$ i $s_2 = 2, t_2 = 6$). Međutim, ako je $t_0 = 1$, tada jesu relativno prosti. Da bi to

pokazali, pretpostavimo da nisu, te neka je m proizvoljni prost broj koji ih dijeli. Iz (1.20) *vidimo da m^2 dijeli d, pa stoga m dijeli i obje strane jednakosti:*

$$p_r^2 - dq_r^2 = (-1)^{r+1}t_{r+1},$$
$$p_{r-1}^2 - dq_{r-1}^2 = (-1)^r t_r = (-1)^r t_{r+1},$$

pa m dijeli p_r i p_{r-1}. Budući su oni relativno prosti, dobili smo kontradikciju.

Konačno, uočimo još i to da broj ne mora imati neparnu duljinu perioda da bi bio zbroj kvadrata. Npr. $\sqrt{34} = [\,5, \overline{1, 4, 1, 10}\,]$ i $34 = 5^2 + 3^2$.

Vrijedi i obrat Teorema 1.32.

Teorem 1.38. *Neka je broj $\ell \in \mathbb{N}$, te neka su brojevi $a_0, a_1, \ldots, a_\ell \in \mathbb{N}$ takvi da vrijedi:*

(i) $a_\ell = 2a_0$,

(ii) $a_{\ell-i} = a_i$, *za svaki* $i = 1, 2, \ldots, \lfloor \frac{\ell-1}{2} \rfloor$.

Tada je $[\,a_0, \overline{a_1, a_2, \ldots, a_{\ell-1}, a_\ell}\,] = \sqrt{d}$, gdje je $d \in \mathbb{Q}$, $d \neq \square$, $d > 1$.

Dokaz. Neka je $\alpha = [\,a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}\,]$. Kako su $a_0, a_1 \in \mathbb{N}$ vidimo da je $\alpha > 1$. Promotrimo broj

$$\beta = a_0 + \alpha = [\,\overline{2a_0, a_1, a_2, \ldots, a_2, a_1}\,] = [\,\overline{b_0, b_1, b_2, \ldots, b_{\ell-2}, b_{\ell-1}}\,].$$

Kako je razvoj od β čisto periodski, znamo da β reducirana, te vrijedi:

$$\beta, \overline{\beta} = \frac{p_{\ell-1} - q_{\ell-2} \pm \sqrt{(p_{\ell-1} - q_{\ell-2})^2 + 4q_{\ell-1}p_{\ell-2}}}{2q_{\ell-1}},$$

gdje su $\frac{p_i}{q_i}$ konvergente broja β. Ako bi dokazali da je $a_0 = \frac{\beta + \overline{\beta}}{2}$, dokaz bi bio gotov, jer bi tada imali

$$\alpha^2 = (\beta - a_0)^2 = \left(\frac{\beta - \overline{\beta}}{2}\right)^2 = \frac{(p_{\ell-1} - q_{\ell-2})^2 + 4q_{\ell-1}p_{\ell-2}}{4q_{\ell-1}^2} \in \mathbb{Q}.$$

Očito vrijedi

$$\beta = [\,\overline{b_0, b_1, b_2, \ldots, b_{\ell-2}, b_{\ell-1}}\,] \quad \text{i} \quad -\frac{1}{\overline{\beta}} = [\,\overline{b_{\ell-1}, b_{\ell-2}, \ldots, b_2, b_1, b_0}\,],$$

tj. zbog palindromnosti imamo

$$\beta = [\,b_0, \overline{b_1, b_2, \ldots, b_2, b_1, b_0}\,] \quad \text{i} \quad -\overline{\beta} = [\,0, \overline{b_1, b_2, \ldots, b_2, b_1, b_0}\,],$$

odnosno

$$\beta = [\,b_0, \beta_1\,] \quad \text{i} \quad -\overline{\beta} = [\,0, \beta_1\,].$$

Vidimo da je $2a_0 = b_0 = \beta + \overline{\beta}$, pa je time teorem dokazan. $\square$

Napomena 1.39. *Nije teško vidjeti [17, Lemma 1] da ako su $a_0, a_1, \ldots, a_\ell$ kao u Teoremu 1.38, onda je*

$$d = \frac{w}{v}, \qquad \text{gdje je} \qquad \begin{pmatrix} w & u \\ u & v \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Primjer 1.40. *Odredimo $\alpha = [\,2, \overline{3, 5, 5, 3, 4}\,]$. Prema oznakama iz Teorema 1.38 vrijedi da je $\ell = 5$, $b_0 = 2a_0$, $b_i = a_i$ za $i = 1, 2, 3, 4$,*

i	-2	-1	0	1	2	3	4
b_i			4	3	5	5	3
p_i	0	1	4	13	69	358	1143
q_i	1	0	1	3	16	83	265

Sada imamo da je

$$\alpha^2 = \left(\frac{p_4 - q_3}{2q_4}\right)^2 + \frac{p_3}{q_4} = \left(\frac{1143 - 83}{2 \cdot 265}\right)^2 + \frac{358}{265} = \frac{1418}{265}.$$

Na drugi način (po Napomeni 1.39) imamo

i	-2	-1	0	1	2	3	4	5
a_i			2	3	5	5	3	2
p_i	0	1	2	7	37	192	613	1418
q_i	1	0	1	3	16	83	265	613

Sada je

$$\alpha^2 = \frac{p_5}{q_4} = \frac{1418}{265},$$

tj, prikažemo li ga u obliku pogodnom za algoritam (1.12)*, imamo $\alpha = \frac{\sqrt{1418 \cdot 265}}{265}$.*

Primjer 1.41. *Odredimo $\alpha = [\,6, \overline{1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12}\,]$. Očito je $\ell = 12$.*

i	0	1	2	3	4	5	6	7	8	9	10	11
b_i	12	1	3	1	1	2	6	2	1	1	3	1
p_i	12	13	51	64	115	294	1879	4052	5931	9983	35 880	45 863
q_i	1	1	4	5	9	23	147	317	464	781	2807	3588

Sada imamo

$$\alpha^2 = \left(\frac{p_{11} - q_{10}}{2q_{11}}\right)^2 + \frac{p_{10}}{q_{11}} = \left(\frac{45\,863 - 2807}{2 \cdot 3588}\right)^2 + \frac{35\,880}{3588} = 46.$$

Vidimo da je za svaki $\ell \in \mathbb{N}$ i za svaki zadani simetričan period$\in \mathbb{N}^{\ell-1}$ i $a_0 \in \mathbb{N}$ moguće naći $d \in \mathbb{Q}$ takav da je to razvoj broja $\sqrt{d}$ u verižni razlomak.

Kako smo vidjeli u primjerima, nekada dobijemo korijen racionalnog, a nekada korijen prirodnog broja. Pa bi nas moglo zanimati bi li i kako za zadani simetrični dio perioda mogli odrediti a_0 tako da to bude razvoj korijena prirodnog broja.

Teorem 1.42 (Euler, 1765)**.** *Neka su brojevi $\ell, a_0, a_1, \ldots, a_\ell, d$ kao u Teoremu 1.38. Tada je $d \in \mathbb{N}$ ako i samo ako vrijedi*

$$2a_0 \equiv (-1)^{\ell-1} p'_{\ell-2} q'_{\ell-2} \pmod{p'_{\ell-1}}, \tag{1.21}$$

gdje su $\dfrac{p'_n}{q'_n} = [\, a_1, a_2, \ldots, a_{n-1}, a_n \,]$ (tj. konvergente verižnog razlomka bez a_0 na početku).

Dokaz. Očito vrijedi:

$$p'_i = q_i \qquad \text{i} \qquad q'_i = p_i - a_0 q_i,$$

$$p_i = a_0 p'_i + q'_i \qquad \text{i} \qquad q_i = p'_i.$$

Vratimo se formuli $\alpha^2 = \left(\dfrac{p_{\ell-1} - q_{\ell-2}}{2q_{\ell-1}} \right)^2 + \dfrac{p_{\ell-2}}{q_{\ell-1}}$. Imamo:

$$\alpha^2 = \left(\frac{2a_0 p'_{\ell-1} + q'_{\ell-1} - p'_{\ell-2}}{2p'_{\ell-1}} \right)^2 + \frac{2a_0 p'_{\ell-2} + q'_{\ell-2}}{p'_{\ell-1}}.$$

Zbog palindromnosti vrijedi $p'_{\ell-2} = q'_{\ell-1}$, pa je

$$\alpha^2 = a_0^2 + \frac{2a_0 p'_{\ell-2} + q'_{\ell-2}}{p'_{\ell-1}}.$$

Da bi to bio prirodan broj, nužno je i dovoljno da vrijedi $2a_0 p'_{\ell-2} + q'_{\ell-2} \equiv 0 \pmod{p'_{\ell-1}}$, tj.

$$2a_0 p'_{\ell-2} \equiv -q'_{\ell-2} \pmod{p'_{\ell-1}}.$$

Prema Teoremu 1.9 vrijedi $p'_{\ell-2} q'_{\ell-1} \equiv (-1)^\ell \pmod{p'_{\ell-1}}$, pa zbog palindromnosti dobijemo (1.21). □

Uočimo da zbog palindromnosti vrijedi $p'_{\ell-2} = q'_{\ell-1}$, pa (1.21) možemo pisati:

$$2a_0 \equiv (-1)^{\ell-1} q'_{\ell-1} q'_{\ell-2} \pmod{p'_{\ell-1}}.$$

U izvornom obliku uvjet (1.21) glasi:

$$\exists m \in \mathbb{Z} \qquad \text{takav da} \qquad a_0 = \frac{m p'_{\ell-1} - (-1)^\ell p'_{\ell-2} q'_{\ell-2}}{2} \tag{1.22}$$

Rješenja kongruencije (1.21) ovise o broju 2 s njene lijeve strane. Imamo dakle 4 slučaja, koja ovise o parnosti brojeva $p'_{\ell-1}$ i $p'_{\ell-2} q'_{\ell-2}$:

1) ako je $p'_{\ell-1}$ paran, $p'_{\ell-2}$ će biti neparan, pa imamo dva slučaja:

   a) ako je $q'_{\ell-2}$ paran, rješenje je $a_0 \equiv (-1)^{\ell-1} p'_{\ell-2} \frac{q'_{\ell-2}}{2} \pmod{\frac{p'_{\ell-1}}{2}}$,

b) ako je $q'_{\ell-2}$ neparan, kongruencija nema rješenja,

2) ako je $p'_{\ell-1}$ neparan, imamo dva slučaja:

a) ako je $q'_{\ell-2}$ paran, onda je $a_0 \equiv (-1)^{\ell-1} p'_{\ell-2}{}^{\frac{q'_{\ell-2}}{2}} \pmod{p'_{\ell-1}}$,

b) ako je $q'_{\ell-2}$ neparan, $p'_{\ell-2} = q'_{\ell-1}$ je paran, pa je $a_0 \equiv (-1)^{\ell-1} q'_{\ell-2}{}^{\frac{p'_{\ell-2}}{2}} \pmod{p'_{\ell-1}}$.

Bit će nam korisna i formula

$$d = \alpha^2 = a_0^2 + \frac{2a_0 p'_{\ell-2} + q'_{\ell-2}}{p'_{\ell-1}} = a_0^2 + \frac{q'_\ell}{p'_{\ell-1}}.$$

Primjer 1.43. *Odredimo a_0 tako da dobijemo razvoj u jednostavni verižni razlomak korijena prirodnog broja.*

(1a) $[\, a_0, \overline{1,2,1,2a_0}\,]$. *Iz* $\ell = 4$, $\frac{p'_2}{q'_2} = \frac{3}{2}$, $\frac{p'_3}{q'_3} = \frac{4}{3}$ *slijedi da je* $a_0 \equiv -3 \cdot 1 \pmod 2 \equiv 1 \pmod 2$. *Za* $a_0 = 1$ *dobivamo* $\sqrt{3} = [\, 1, \overline{1,2,1,2}\,] = [\, 1, \overline{1,2}\,]$, *dok za npr.* $a_0 = 11$ *dobivamo* $\sqrt{138} = [\, 11, \overline{1,2,1,22}\,]$.

(1b) $[\, a_0, \overline{2,2,3,3,2,2,2a_0}\,]$. *Iz* $\ell = 7$, $\frac{p'_5}{q'_5} = \frac{129}{53}$, $\frac{p'_6}{q'_6} = \frac{314}{129}$ *slijedi da kongruencija nema rješenja, pa vidimo da se može dogoditi slučaj i da ne možemo dobiti prirodan broj — da u najboljem slučaju dobijemo korijen neke polovine.*

(2a) $[\, a_0, \overline{1,2,3,2,1,2a_0}\,]$. *Iz* $\ell = 6$, $\frac{p'_4}{q'_4} = \frac{23}{16}$, $\frac{p'_5}{q'_5} = \frac{33}{23}$ *slijedi da je* $a_0 \equiv -23 \cdot 4 \pmod{33} \equiv 14 \pmod{33}$. *Za* $a_0 = 14$ *dobivamo* $\sqrt{216} = [\, 14, \overline{1,2,3,2,1,28}\,]$, *dok za npr.* $a_0 = 47$ *dobivamo* $\sqrt{2275} = [\, 47, \overline{1,2,3,2,1,94}\,]$.

(2b) $[\, a_0, \overline{1,2,3,3,2,1,2a_0}\,]$. *Iz* $\ell = 7$, $\frac{p'_5}{q'_5} = \frac{76}{53}$, $\frac{p'_6}{q'_6} = \frac{109}{76}$ *slijedi da je* $a_0 \equiv 53 \cdot 38 \pmod{109} \equiv 52 \pmod{109}$. *Za* $a_0 = 52$ *dobivamo* $\sqrt{2777} = [\, 52, \overline{1,2,3,3,2,1,104}\,]$.

Kao što vidimo, moguća su sva četiri slučaja iz prethodnog razmatranja.

Da bi bili sigurni da za zadanu duljinu ℓ možemo konstruirati broj $d \in \mathbb{N}$ takav da je $\ell = \ell\big(\sqrt{d}\big)$, trebamo vidjeti možemo li naći brojeve $a_1, \ldots, a_{\ell-1} \in \mathbb{N}$ centralno simetrične takve da $p'_{\ell-1}$ nije paran ili $q'_{\ell-2}$ nije neparan.

Sjetimo se:

$$\begin{aligned} &p_{-2} = 0, && p_{-1} = 1, && p_n \equiv a_n p_{n-1} + p_{n-2} \,(\mathrm{mod}\, 2)\,, \\ &q_{-2} = 1, && q_{-1} = 0, && q_n \equiv a_n q_{n-1} + q_{n-2} \,(\mathrm{mod}\, 2)\,. \end{aligned}$$

Ako je a_n ili p_{n-1} paran, p_n će imati istu parnost kao i p_{n-2}, a ako su a_n i p_{n-1} neparni, p_n će imati suprotnu parnost od p_{n-2}. Isto vrijedi i za q_n.

Dakle, ako su na primjer svi a_n parni, p_n će imati istu parnost kao i q_{n-1}, pa ćemo biti ili u slučaju (1a) ili u slučaju (2b), pa vidimo da za svaki ℓ postoji $d \in \mathbb{N}$ kojem je duljina perioda ℓ. Iz konstrukcije slijedi da ih postoji čak i beskonačno mnogo. Tako smo dokazali:

Teorem 1.44. *Za svaki prirodan broj $\ell \in \mathbb{N}$ postoji beskonačno mnogo prirodnih brojeva d takvih da vrijedi $\ell(\sqrt{d}) = \ell$.* □

1.7 Duljina perioda

Prema Teoremu 1.44 za svaku duljinu perioda ℓ postoji prirodan broj d takav da je $\ell(\sqrt{d}) = \ell$. Štoviše, postoji ih beskonačno mnogo, te za svaki prirodan broj M možemo naći beskonačno mnogo prirodnih brojeva $d > M$ takvih da vrijedi $\ell(\sqrt{d}) = \ell$. Kako se čini, i najmanji broj d konstruriran postupkom kao u Teoremu 1.44 može biti jako velik. Za primjene u teoriji brojeva, puno je bitnija obrnuta ograda — za dani prirodni broj d odrediti najveću moguću duljinu perioda — budući da o tome ovisi složenost algoritama koji koriste verižne razlomke, odnosno veličina rješenja.

Vidjeli smo da svaka kvadratna iracionalnost $\alpha = \frac{s_0+\sqrt{d}}{t_0}$ ima periodan razvoj u verižni razlomak, vjerojatno s nekim početnim dijelom, pa se prirodno nameće pitanje ovisi li duljina perioda o veličini broja α, ili možda o veličini broja d.

Iz postupka (1.12) za razvoj u verižni razlomak kvadratne iracionalnosti α vidimo da su $s_k, t_k \in \mathbb{N}$ i vrijedi

$$d - s_{k+1}^2 = t_{k+1}t_k,$$

odnosno

$$d = s_{k+1}^2 + t_{k+1}t_k.$$

Imamo $0 < s_{k+1} < \sqrt{d}$ i $1 < t_{k+1} < d$, pa vidimo da uređenih parova (s_{k+1}, t_{k+1}) ima samo konačno mnogo, te će se nakon nekog mjesta početi ponavljati (kao što smo vidjeli u dokazu Teorema 1.25). Malo preciznije, iz (1.13a), (1.13b), (1.13c) i (1.13d) slijedi

$$\ell(\alpha) \leq \lfloor\sqrt{d}\rfloor\lfloor 2\sqrt{d}\rfloor < 2d.$$

Međutim, ta ocjena može biti puno bolja. Sljedeći teorem [38, §III.2] je jedno poboljšanje, a kasnije ćemo dati i neke preciznije ocjene.

Teorem 1.45. *Neka je $\alpha = \frac{s_0+\sqrt{d}}{t_0}$, gdje je $d \in \mathbb{N}$, $d \neq \square$, te prirodan broj t_0 i nenegativan cijeli broj s_0 takvi da $t_0 \mid d - s_0^2$. Tada za duljinu perioda vrijedi*

$$\ell(\alpha) = \mathcal{O}(\sqrt{d}\ln d).$$

Dokaz. Potrebno je odrediti broj parova (s, t) cijelih brojeva koji zadovoljavaju:

$$\begin{gathered} 0 < s < \sqrt{d}, \\ 0 < \sqrt{d} - s < t < \sqrt{d} + s < 2\sqrt{d}, \\ s^2 \equiv d \pmod{t}. \end{gathered}$$

Ako je $\sqrt{d} < t$, tada je zbog $t < \sqrt{d} + s < 2\sqrt{d}$ imamo

$$0 < t - \sqrt{d} < s < \sqrt{d},$$

dok $t < \sqrt{d}$, zbog $0 < \sqrt{d} - s < t < \sqrt{d}$ daje

$$0 < \sqrt{d} - t < s < \sqrt{d}.$$

U svakom slučaju za proizvoljni t, moguće vrijednosti za s su u intervalu duljine manje od t, pa moguće s-ove možemo pobrojati brojeći klase ostataka modulo t. Stoga imamo:

$$\ell(\alpha) < \sum_{0<t<2\sqrt{d}} \left(\sum_{s^2 \equiv d \pmod{t}} 1 \right),$$

$$\ell(\alpha) < \sum_{t=1}^{\lfloor 2\sqrt{d} \rfloor} \left(\sum_{s^2 \equiv d \pmod{t}} 1 \right).$$

Proučimo unutarnju sumu u tri moguća slučaja: $\operatorname{nzd}(t,d) = 1$, $1 < \operatorname{nzd}(t,d) < t$ i $\operatorname{nzd}(t,d) = t$. U prvom slučaju, pretpostavimo da $s^2 \equiv d \pmod{t}$ ima rješenja, tj. d je kvadratni ostatak modulo t. Promotrimo rastav broja t na proste faktore

$$t = 2^{k_0} \cdot p_1^{k_1} \cdots p_m^{k_m},$$

gdje su $p_1, \ldots, p_m$ različiti neparni prosti brojevi. Tada svako rješenje kongruencije $s^2 \equiv d \pmod{t}$ mora zadovoljavati i kongruencije

$$s^2 \equiv d \left(\bmod\ 2^{k_0}\right), \quad s^2 \equiv d \left(\bmod\ 2^{k_1}\right), \quad \cdots, \quad s^2 \equiv d \left(\bmod\ 2^{k_m}\right).$$

Neka je $N_i,\ i = 0, \ldots, m$ broj rješenja svake od tih kongruencija. Tada je po Kineskom teoremu o ostatcima [7, Tm. 2.7], [8, Tm. 5.4] broj rješenja polazne kongruencije točno $N_0 \cdot N_1 \cdot \cdots \cdot N_m$.

Za svaki neparan prost broj p_i rješenje od $s^2 \equiv d \pmod{p_i^{k_i}}$ je i rješenje od $s^2 \equiv d \pmod{p_i}$, a takvih je točno 2. Po Henselovoj lemi [7, Tm. 2.16], ta rješenja povlače dva rješenja modulo $p_i^{k_i}$, te je stoga $N_i = 2$ za $i = 1, \ldots, m$.

Za prosti broj 2, situacija je nešto drugačija. Neparan broj a je uvijek kvadrat modulo 2, zatim a je kvadrat modulo 2^2 ako i samo ako je $a \equiv 1 \pmod{4}$, te je a kvadrat modulo 2^{k_0} za $k_0 \geq 3$ samo ako je $a \equiv 1 \pmod{8}$. Stoga rješenje od $s^2 \equiv d \pmod{2}$ povlači dva rješenja modulo 4 i četiri rješenja modulo 2^{k_0}, za $k_0 \geq 3$. Dakle, za $\operatorname{nzd}(d,s) = 1$ imamo

$$\sum_{s^2 \equiv d \pmod{t}} 1 = 2^k \cdot 2^m,$$

gdje je m broj različitih neparnih prostih djelitelja od t, te $k = 0$ ako je $k_0 \leq 1$, $k = 1$ ako je $k_0 = 2$ i $k = 2$ ako je $k_0 \geq 3$. Budući je $2^{k+m} \leq \tau(t)$, gdje je $\tau(t)$ broj djelitelja od t, vidimo da vrijedi

$$\sum_{s^2 \equiv d \pmod{t}} 1 \leq \tau(t).$$

U drugom slučaju, kada je $1 < \operatorname{nzd}(t, d) < t$, suma ne može biti veća nego u prvom slučaju, budući je kongruencija $s^2 \equiv d \pmod{t}$ ista kao i

$$\operatorname{nzd}(t,d) \left(\frac{s}{\operatorname{nzd}(t,d)}\right)^2 \equiv \frac{d}{\operatorname{nzd}(t,d)} \pmod{\frac{t}{\operatorname{nzd}(t,d)}},$$

koja ili nema rješenja ili ih kao u prvom slučaju ima najviše $\tau\left(\frac{t}{\operatorname{nzd}(t,d)}\right)$.

Konačno, ako $t \mid d$, tada

$$\sum_{s^2 \equiv d \pmod{t}} 1 = \mathcal{O}\big(\sqrt{t}\big).$$

Budući

$$\sum_{k=1}^{n} \tau(k) \overset{\text{(Prop. 7.2)}}{=} n \ln n + \mathcal{O}(n),$$

možemo ocijeniti

$$\ell(\alpha) = \mathcal{O}\left(\sum_{t=1}^{\lfloor 2\sqrt{d} \rfloor} \tau(t)\right),$$

pa slijedi tvrdnja. □

U Tablici 1.1 su primjeri omjera $\ell(\sqrt{d})/\sqrt{d}$ iz kojih se nazire da vrijedi $\ell(\sqrt{d}) > \mathcal{O}(\sqrt{d})$, pa se čini da je dio $\ln d$ ne možemo izostaviti. Ipak, uz Riemannovu slutnju se može pokazati da vrijedi $\ell(\sqrt{d}) = \mathcal{O}(\sqrt{d} \ln \ln d)$.

d	$\ell(\sqrt{d})$	$\ell(\sqrt{d})/\sqrt{d}$	$\frac{\ell(\sqrt{d})}{\sqrt{d}\ln d}$	$\frac{\ell(\sqrt{d})}{\sqrt{d}\ln\ln d}$	d	$\ell(\sqrt{d})$	$\ell(\sqrt{d})/\sqrt{d}$	$\frac{\ell(\sqrt{d})}{\sqrt{d}\ln d}$	$\frac{\ell(\sqrt{d})}{\sqrt{d}\ln\ln d}$
2	1	0.707107	1.020139	-1.929282	1427 911	3308	2.768311	0.195340	1.044154
3	2	1.154701	1.051054	12.277801	1957 099	3898	2.786349	0.192335	1.042308
7	4	1.511858	0.776941	2.270978	2237 134	4212	2.816063	0.192608	1.049814
43	10	1.524986	0.405452	1.151160	2847 079	4784	2.835250	0.190774	1.050562
46	12	1.769303	0.462123	1.317907	5715 319	6892	2.882870	0.185290	1.050372
211	26	1.789914	0.334447	1.067048	10 393 111	9352	2.900893	0.179548	1.042612
331	34	1.868809	0.322091	1.062896	12 843 814	10 442	2.913645	0.178005	1.042318
631	48	1.910850	0.296380	1.025320	14 841 766	11 226	2.913951	0.176465	1.039158
919	60	1.979217	0.290068	1.030659	18 461 899	12 542	2.918963	0.174462	1.036094
1726	88	2.118177	0.284183	1.054506	20 289 091	13 358	2.965583	0.176254	1.050545
4846	152	2.183493	0.257308	1.021084	23 345 326	14 348	2.969555	0.175031	1.048866
7606	194	2.224455	0.248913	1.015656	28 473 454	15 876	2.975233	0.173337	1.046570
10 399	228	2.235831	0.241725	1.005064	39 803 611	19 002	3.011883	0.172113	1.052307
10 651	234	2.267361	0.244501	1.018054	40 781 911	19 396	3.037235	0.173321	1.060651
10 774	238	2.292918	0.246951	1.028958	106 347 151	31 368	3.041753	0.164577	1.042836
18 379	322	2.375171	0.241896	1.039774	115 036 366	32 688	3.047690	0.164201	1.043354
19 231	332	2.394072	0.242701	1.045939	128 303 926	35 178	3.105640	0.166345	1.061063
32 971	438	2.412171	0.231864	1.029904	138 590 299	36 578	3.107088	0.165738	1.060065
48 799	544	2.462598	0.228114	1.035085	180 628 639	41 828	3.112245	0.163699	1.056765
61 051	614	2.484975	0.225508	1.035551	274 963 789	51 973	3.134296	0.161294	1.056411
78 439	696	2.485096	0.220504	1.025987	340 193 071	57 924	3.140478	0.159861	1.054622
82 471	716	2.493230	0.220246	1.027463	394 935 451	62 610	3.150508	0.159163	1.055309
111 094	834	2.502193	0.215370	1.020234	475 477 759	68 836	3.156825	0.158001	1.054129
162 094	1016	2.523540	0.210366	1.015686	505 313 251	71 166	3.165864	0.157972	1.056075
187 366	1106	2.555111	0.210456	1.023447	612 380 869	78 530	3.173400	0.156844	1.055229
241 894	1262	2.565942	0.206993	1.019285	738 915 046	86 494	3.181916	0.155818	1.054820
257 371	1318	2.597979	0.208534	1.029969	796 549 471	90 020	3.189574	0.155621	1.056073
289 111	1400	2.603729	0.207063	1.028460	937 065 691	97 742	3.192980	0.154562	1.054445
294 694	1438	2.648947	0.210339	1.045694	1337 079 979	117 590	3.215820	0.153034	1.056037
799 621	2383	2.664906	0.196066	1.021243	1464 061 351	123 328	3.223161	0.152724	1.056953
969 406	2664	2.705711	0.196287	1.031320	1492 180 699	125 154	3.239918	0.153380	1.062134
1234 531	3030	2.727041	0.194425	1.032607	2142 594 931	150 254	3.246056	0.151083	1.058254
1365 079	3196	2.735444	0.193636	1.032996					

Tablica 1.1: Gornje ograde od $\ell(\sqrt{d})/\sqrt{d}$ za $1 < d < 2^{31}$

Poglavlje 2

Neke primjene periodskih verižnih razlomaka

Jedan od osnovnih problema u teoriji brojeva je određivanje broja klasa u kvadratnim poljima. Taj problem je prvi proučavao Gauss krajem osamnaestog stoljeća motiviran radovima Fermata, Lagrangea i drugih. Gauss je smatrao da postoji beskonačno mnogo realnih kvadratnih polja s brojem klasa 1. To je i danas neriješen problem, iako su ga mnogi matematičari pokušavali riješiti. Budući da je broj klasa obrnuto proporcionalan duljini perioda u razvoju verižnog razlomka, oni ovdje imaju veliku primjenu.

Problem je usko povezan s određivanjem grupe jedinica u realnim kvadratnim poljima. S tim problemom je pak povezano rješavanje jedne familije diofantskih jednadžbi, takozvanih Pellovskih jednadžbi.

2.1 Pellova jednadžba

Jedna od najvažnijih primjena verižnih razlomaka u teoriji brojeva je u rješavanju Pellove jednadžbe.

Definicija 2.1. *Neka je $d \in \mathbb{N}$, $d \neq \square$. Diofantska jednadžba*

$$x^2 - dy^2 = 1, \tag{2.1}$$

zove se Pellova jednadžba. *Jednadžbu oblika*

$$x^2 - dy^2 = N, \tag{2.2}$$

gdje je $N \in \mathbb{Z}$ zove se pellovska jednadžba.

Ako je $d \in \mathbb{N}$ potpun kvadrat, tada jednadžba (2.1) ima samo trivijalna rješenja. Naime iz $(x - \sqrt{d}y)(x + \sqrt{d}y) = 1$ slijedi $x - \sqrt{d}y = x + \sqrt{d}y = \pm 1$. Ako je $d \in \mathbb{Z}, d \leq 0$ jednadžba također ima samo trivijalno rješenje $(\pm 1, 0)$. Analogno

vidimo da ako je $d \leq 0$ ili ako je d potpun kvadrat, da onda jednadžba (2.2) ima najviše konačno mnogo rješenja.

Lako se vidi da je $(1, 0)$ rješenje jednadžbe (2.1). Nadalje, također se lako provjeri da ako su (x_1, y_1) i (x_2, y_2) rješenja, da su tada rješenja i $(x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1)$. Koristeći razvoj u verižni razlomak broja $\sqrt{d}$ pokazat ćemo da jednadžba (2.1) uvijek ima beskonačno mnogo rješenja. Ako jednadžba (2.2) ima jedno netrivijalno rješenje, onda ih ima beskonačno mnogo. Njome sada nećemo previše baviti, osim u slučaju $N = -1$ i $N = \pm 4$ jer nam ta rješenja daju važne informacije o grupi jedinica pripadnog kvadratnog polja. Neka svojstva te jednadžbe ćemo spomenuti u poglavlju o poboljšanju gornje ograde duljine razvoja.

Pogledajmo prvo jednadžbu (2.1).

Propozicija 2.2 (Legendre)**.** *Neka su p, q cijeli brojevi takvi da je $q \geq 1$ i*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Tada je $\dfrac{p}{q}$ neka konvergenta od α.

Dokaz. Ako je $\alpha = \dfrac{p}{q}$, tvrdnja je trivijalno zadovoljena. Pretpostavimo stoga da je $\alpha \neq \dfrac{p}{q}$. Tada možemo pisati $\alpha - \dfrac{p}{q} = \dfrac{\epsilon\vartheta}{q^2}$, gdje je $0 < \vartheta < \dfrac{1}{2}$ i $\epsilon = \pm 1$. Neka je

$$\frac{p}{q} = \langle\, b_0, b_1, \ldots, b_{n-1} \,\rangle$$

razvoj od $\dfrac{p}{q}$ u jednostavni verižni razlomak, gdje je n izabran tako da vrijedi $(-1)^{n-1} = \epsilon$ (po Napomeni 1.2 (i) to možemo uvijek postići).

Definirajmo ω sa

$$\alpha = \frac{\omega p_{n-1} + p_{n-2}}{\omega p_{q-1} + q_{n-2}},$$

tako da je $\alpha = \langle\, b_0, b_1, \ldots, b_{n-1}, \omega \,\rangle$. Vrijedi $\alpha = \dfrac{\omega p_{n-1} + p_{n-2}}{\omega q_{n-1} + q_{n-2}}$, pa imamo:

$$\begin{aligned}
\alpha - \frac{p_{n-1}}{q_{n-1}} &= \frac{\omega p_{n-1} + p_{n-2}}{\omega q_{n-1} + q_{n-2}} - \frac{p_{n-1}}{q_{n-1}} \\
&= \frac{\omega p_{n-1}q_{n-1} + p_{n-2}q_{n-1} - \omega p_{n-1}q_{n-1} - p_{n-1}q_{n-2}}{q_{n-1}(\omega q_{n-1} + q_{n-2})} \\
&= \frac{1}{q_{n-1}} \cdot \frac{(-1)^{n-1}}{\omega q_{n-1} + q_{n-2}}.
\end{aligned}$$

Sada je

$$\frac{\epsilon\vartheta}{q^2} = \alpha - \frac{p}{q} = \frac{1}{q_{n-1}} \cdot (\alpha q_{n-1} - p_{n-1}) = \frac{1}{q_{n-1}} \cdot \frac{(-1)^{n-1}}{\omega q_{n-1} + q_{n-2}},$$

pa je $\vartheta = \dfrac{q_{n-1}}{\omega q_{n-1} + q_{n-2}}$. Rješavanjem ove relacije po ω, dobivamo $\omega = \dfrac{1}{\vartheta} - \dfrac{q_{n-2}}{q_{n-1}}$. Odavde slijedi da je $\omega > 2 - 1 = 1$. Razvijmo ω u jednostavan verižni razlomak

$$\omega = [\, b_n, b_{n+1}, b_{n+2}, \dots].$$

Budući je $\omega > 1$, svi b_j $(j = n, n+1, n+2, \dots)$ su prirodni brojevi. Stoga je

$$\alpha = \langle\, b_0, b_1, \dots, b_{n-1},\ b_n, b_{n+1}, b_{n+2}, \dots \rangle$$

razvoj u jednostavni verižni razlomak od α i

$$\frac{p}{q} = \frac{p_{n-1}}{q_{n-1}} = \langle\, b_0, b_1, \dots, b_{n-1} \,\rangle$$

je konvergenta od α, što je i trebalo dokazati. □

Teorem 2.3. *Neka je $d \in \mathbb{N}$, $d \neq \square$, $\alpha_0 = \sqrt{d}$ i t_i kao u postupku (1.12), te $\ell = \ell(\sqrt{d})$. Tada je*

$$t_i = 1 \qquad \Longleftrightarrow \qquad \ell \mid i.$$

Dokaz. Neka je ℓ duljina najmanjeg perioda i β_i kao u dokazu Teorema 1.32. Imamo da je

$$\beta_i = \beta \qquad \Longleftrightarrow \qquad \ell \mid i.$$

Ako sada primijenimo postupak (1.12) na $\beta_0 = \sqrt{d} + \lfloor \sqrt{d} \rfloor$, $t_0 = 1$, $s_0 = \lfloor \sqrt{d} \rfloor$, onda za sve $j \geq 0$ vrijedi

$$\frac{s_{j\cdot\ell} + \sqrt{d}}{t_{j\cdot\ell}} = \beta_{j\cdot\ell} = \beta_0 = \frac{s_0 + \sqrt{d}}{t_0} = \lfloor \sqrt{d} \rfloor + \sqrt{d},$$

odnosno

$$s_{j\cdot\ell} - t_{j\cdot\ell} \lfloor \sqrt{d} \rfloor = (t_{j\cdot\ell} - 1)\sqrt{d},$$

pa je $t_{j\cdot\ell} = 1$ jer je $\sqrt{d}$ iracionalan. Nadalje, $t_i \neq 1$ za sve ostale vrijednosti od i. Zaista, $t_i = 1$ povlači $\beta_i = s_i + \sqrt{d}$. Međutim, β_i ima čisto periodski razvoj, pa je prema Teoremu 1.28 $-1 < s_i - \sqrt{d} < 0$. Odavde je $\sqrt{d} - 1 < s_i < \sqrt{d}$, tj. $s_i = \lfloor \sqrt{d} \rfloor$, pa je $\beta_i = \beta$, što povlači $\ell \mid i$. □

Teorem 2.4. *Neka je $d \in \mathbb{N}, d \neq \square$, te neka su $\dfrac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$. Neka je $N \in \mathbb{Z}$, $|N| < \sqrt{d}$. Tada svako pozitivno rješenje $x = u, y = v$ jednadžbe $x^2 - dy^2 = N$, takvo da je $\operatorname{nzd}(u, v) = 1$, zadovoljava $u = p_n, v = q_n$ za neki $n \in \mathbb{N}$.*

Dokaz. Neka su E i M prirodni brojevi takvi da je $\text{nzd}(E,M)=1$ i $E^2-\varrho M^2=\sigma$, gdje je $\sqrt{\varrho}$ iracionalan i $0<\sigma<\sqrt{\varrho}$. Ovdje su ϱ i σ realni brojevi, ne nužno cijeli. Tada je $\dfrac{E}{M}-\sqrt{\varrho}=\dfrac{\sigma}{M(E+M\sqrt{\varrho})}$, pa je

$$0<\frac{E}{M}-\sqrt{\varrho}<\frac{\sigma}{M(E+M\sqrt{\varrho})}=\frac{1}{M^2(\frac{E}{M\sqrt{\varrho}}+1)}<\frac{1}{2M^2}.$$

Prema Propoziciji 2.2, $\dfrac{E}{M}$ je konvergenta u razvoju od $\sqrt{\varrho}$.

Ako je $N>0$, uzmimo $\sigma=N$, $\varrho=d$, $E=u$, $M=v$, pa dobivamo tvrdnju teorema u ovom slučaju.

Ako je $N<0$, onda je $v^2-\dfrac{1}{d}u^2=-\dfrac{N}{d}$, pa možemo uzeti $\sigma=-\dfrac{N}{d}$, $\varrho=\dfrac{1}{d}$, $E=v$, $M=u$. Dobivamo da je $\frac{v}{u}$ konvergenta u razvoju od $\dfrac{1}{\sqrt{d}}$. No, ako je $\dfrac{v}{u}$ n-ta konvergenta od $\dfrac{1}{\sqrt{d}}$, onda je $\dfrac{u}{v}$ $(n-1)$-va konvergenta od $\sqrt{d}$, pa je teorem dokazan i u ovom slučaju. □

Teorem 2.5. *Sva rješenja u prirodnim brojevima jednadžbi*

$$x^2-dy^2=1 \qquad (2.3^+)$$
$$x^2-dy^2=-1 \qquad (2.3^-)$$

nalaze se među brojevima $x=p_n, y=q_n$, gdje su $\dfrac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$. Neka je $\ell=\ell(\sqrt{d})$.

(i) Ako je ℓ paran, onda jednadžba (2.3^-) nema rješenja, a sva rješenja jednadžbe (2.3^+) su dana sa $x=p_{n\cdot\ell-1}$, $y=q_{n\cdot\ell-1}$ za $n\in\mathbb{N}$.

(ii) Ako je ℓ neparan, onda su sva rješenja jednadžbe (2.3^-) dana sa $x=p_{n\cdot\ell-1}$, $y=q_{n\cdot\ell-1}$ za n neparan, a sva rješenja jednadžbe (2.3^+) su dana sa $x=p_{n\cdot\ell-1}$, $y=q_{n\cdot\ell-1}$ za n paran.

Dokaz. Teorem 2.4 kaže da rješenja jednadžbi (2.3) moraju biti konvergente od $\sqrt{d}$. Po Teoremu 1.31 imamo $p_n^2-dq_n^2=(-1)^{n+1}t_{n+1}$, pa vidimo da se rješenje može postići samo za one n za koje je $t_{n+1}=1$. Tada bi se rješenja jednadžbe (2.3^-) mogla nalaziti među parnim konvergentama, a rješenja jednadžbe (2.3^+) među neparnima.

Iz Teorema 2.3 slijedi $t_{n+1}=1$ ako i samo ako $n+1=k\cdot\ell$, $k\in\mathbb{N}$, to jest $n=k\cdot\ell-1$. Pogledajmo sljedeće slučajeve:

(i) ako je ℓ paran, (2.3^-) nema rješenja, a rješenja jednadžbe (2.3^+) dobijemo za $n = k \cdot \ell - 1, k \in \mathbb{N}$,

(ii) ako je ℓ neparan, rješenja jednadžbe (2.3^-) dobijemo za $n = (2k-1)\cdot\ell - 1, k \in \mathbb{N}$, a rješenja jednadžbe (2.3^+) dobijemo za $n = 2k \cdot \ell - 1, k \in \mathbb{N}$.

□

Teorem 2.6. *Ako je (x_1, y_1) najmanje rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$ (takozvano* fundamentalno rješenje*), onda su sva rješenja ove jednadžbe dana sa (x_n, y_n) za $n \in \mathbb{N}$, gdje su x_n i y_n prirodni brojevi definirani sa*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n. \tag{2.4}$$

Dokaz. Iz (2.4) slijedi $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, pa je

$$x_n^2 - dy_n^2 = (x_1^2 - dy_1^2)^n = 1,$$

pa vidimo da su (x_n, y_n) zaista rješenja.

Pretpostavimo sada da je (s, t) rješenje koje se ne nalazi u familiji

$$\{(x_n, y_n) : n \in \mathbb{N}\}.$$

Budući da je $x_1 + y_1\sqrt{d} > 1$ i $s + t\sqrt{d} > 1$, postoji $n \in \mathbb{N}$ takav da je

$$(x_1 + y_1\sqrt{d})^n < s + t\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}. \tag{2.5}$$

Pomnožimo li (2.5) sa $(x_1 - y_1\sqrt{d})^n$, dobivamo

$$1 < (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^n < x_1 + y_1\sqrt{d}.$$

Definiramo li $a, b \in \mathbb{Z}$ s $a + b\sqrt{d} = (s + t\sqrt{d})(y_1 - y_1\sqrt{d})^n$, imamo: $a^2 - db^2 = (s^2 - dt^2)(x_1^2 - dy_1^2)^n = 1$. Iz $a + b\sqrt{d} > 1$ slijedi $0 < a - b\sqrt{d} < 1$, pa je

$$2a = (a + b\sqrt{d}) + (a - b\sqrt{d}) > 0$$
$$2b\sqrt{d} = (a + b\sqrt{d}) - (a - b\sqrt{d}) > 0.$$

Stoga je (a, b) rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$ i $a + b\sqrt{d} < x_1 + y_1\sqrt{d}$, što je kontradikcija s pretpostavkom da je (x_1, y_1) najmanje rješenje.

□

Teorem 2.7. *Neka je (x_n, y_n) niz rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ zapisan u rastućem redoslijedu. Uzmimo da je $(x_0, y_0) = (1, 0)$. Tada vrijedi:*

$$x_{n+2} = 2x_1x_{n+1} - x_n, \quad y_{n+2} = 2x_1y_{n+1} - y_n, \qquad \text{za } n \geq 0.$$

Dokaz. Po Teoremu 2.6 vrijedi: $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$. Odavde je

$$(x_{n+1} + y_{n+1}\sqrt{d})(x_1 + y_1\sqrt{d}) = x_{n+2} + y_{n+2}\sqrt{d},$$
$$(x_{n+1} + y_{n+1}\sqrt{d})(x_1 - y_1\sqrt{d}) = x_n + y_n\sqrt{d}.$$

Sada imamo:

$$x_{n+2} = x_1x_{n+1} + dy_1y_{n+1},$$
$$x_n = x_1x_{n+1} - dy_1y_{n+1},$$

odakle zbrajanjem dobivamo $x_{n+2} = 2x_1x_{n+1} - x_n$. Analogno je

$$y_{n+2} = x_1y_{n+1} + dy_1x_{n+1},$$
$$y_n = x_1y_{n+1} - dy_1x_{n+1},$$

pa ponovo zbrajanjem dobivamo $y_{n+2} = 2x_1y_{n+1} - y_n$. □

Primjer 2.8. *Nađimo najmanja rješenja jednadžbe $x^2 - 85y^2 = \pm 1$ u prirodnim brojevima. Imamo*

$$\sqrt{85} = [\,9, \overline{4, 1, 1, 4, 18}\,].$$

Period $\ell = 5$ je neparan, pa su sva rješenja jednadžbe $x^2 - 89y^2 = -1$ dana sa (p_{10n-6}, q_{10n-6}), $n \in \mathbb{N}$, a sva rješenja jednadžbe $x^2 - 89y^2 = 1$ su (p_{10n-1}, q_{10n-1}), $n \in \mathbb{N}$. Najmanja rješenja su:

i	-1	0	1	2	3	**4**	5	6	7	8	**9**
a_i		9	4	1	1	4	18	4	1	1	4
p_i	1	9	37	46	83	**378**	6887	27 926	34 813	62 739	**285 769**
q_i	0	1	4	5	9	**41**	747	3029	3776	6805	**30 996**

Dakle,

$$378^2 - 85 \cdot 41^2 = -1, \qquad 285\,769^2 - 85 \cdot 30\,996^2 = 1.$$

Napomena 2.9. *Ako je $d \in \mathbb{N}$, $d \neq \square$, $p \mid d$, gdje je $p \equiv 3 \pmod 4$. Tada je $\ell(\sqrt{d})$ paran broj. Naime, -1 nije kvadrat modulo d, pa jednadžba $x^2 - dy^2 = -1$ nema rješenja, te po Teoremu 2.5 zaključujemo da duljina perioda ne može biti neparna.*

2.2 Kvadratna polja

Definicija 2.10. *Neka je d cijeli broj koji nije potpun kvadrat. Skup svih brojeva oblika $u + v\sqrt{d}$, $u, v \in \mathbb{Q}$, uz uobičajene operacije zbrajanja i množenja kompleksnih brojeva, čini polje, koje označavamo s $\mathbb{Q}(\sqrt{d})$ i zovemo* kvadratno polje. *Za kvadratno polje kažemo da je* realno *ako je $d > 0$, a* imaginarno *ako je $d < 0$.*

Očito je $\mathbb{Q}(\sqrt{dm^2}) = \mathbb{Q}(\sqrt{d})$ *za* $m \in \mathbb{Q}, m \neq 0$, *pa bez smanjenja općenitosti možemo pretpostaviti da je* d *kvadratno slobodan.*

Za svaki $\alpha = u + v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ *definiramo* konjugat *od* α *sa* $\overline{\alpha} = u - v\sqrt{d}$, *te* normu *od* α *sa* $|\alpha| = u^2 - dv^2 = \alpha\overline{\alpha}$.

Specijalno, polje $\mathbb{Q}\left(\sqrt{-1}\right)$ *se zove* polje Gaussovih brojeva *i uobičajeno je njegove elemente označavati u obliku* $u + iv$. *U tom slučaju je* $|\alpha| = u^2 + v^2$.

Lako se provjeri da je $\mathbb{Q}(\sqrt{d})$ stvarno polje. Na primjer, $(u + v\sqrt{d})^{-1} = \dfrac{u - v\sqrt{d}}{u^2 - dv^2}$. A u Propoziciji 2.14 ćemo vidjeti da je $|\ |$ stvarno norma.

Svaki element $\alpha \in \mathbb{Q}(\sqrt{d})$ je nultočka jedinstvenog normiranog kvadratnog polinoma s racionalnim koeficijentima (kojeg zovemo minimalni polinom od α).

Definicija 2.11. *Algebarski broj* α *je* algebarski cijeli broj *ako njegov minimalni polinom ima cjelobrojne koeficijente. Cijeli elementi u* $\mathbb{Q}(\sqrt{d})$ *čine prsten, koji označavamo sa* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Lako se vidi [7, Prop. 8.1] da su među racionalnim brojevima jedini algebarski cijeli brojevi upravo cijeli brojevi.

Teorem 2.12. *Neka je* d *kvadratno slobodan prirodan broj.*

Ako je $d \equiv 2$ *ili* $3 \pmod 4$, *onda su algebarski cijeli brojevi u* $\mathbb{Q}(\sqrt{d})$ *svi brojevi oblika* $u + v\sqrt{d}$, $u, v \in \mathbb{Z}$, *to jest* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$.

Ako je $d \equiv 1 \pmod 4$, *onda su algebarski cijeli brojevi u* $\mathbb{Q}(\sqrt{d})$ *svi brojevi oblika* $u + v\frac{1+\sqrt{d}}{2}$, $u, v \in \mathbb{Z}$. *To jest svi brojevi oblika* $u + v\sqrt{d}$, $u, v \in \mathbb{Z}$ *i* $\frac{u+v\sqrt{d}}{2}$, u, v *neparni, odnosno* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Dokaz. Neka je $\alpha = u + v\sqrt{d}$ algebarski cijeli broj u $\mathbb{Q}(\sqrt{d})$, te neka je $a = 2u, b = 2v, c = |\alpha| = u^2 - dv^2$. Tada je α nultočka polinoma $f(x) = x^2 - ax + c$. Prema tome, racionalni brojevi a i c moraju biti cijeli. Imamo $db^2 = a^2 - 4c$ i budući je d kvadratno slobodan, vidimo da je i $b \in \mathbb{Z}$.

Neka je sada $d \equiv 2$ ili $3 \pmod 4$. Iz $a^2 \equiv b^2 d \pmod 4$, $a^2 \equiv 0$ ili $1 \pmod 4$, $b^2 d \equiv 0, 2$ ili $3 \pmod 4$, slijedi da su a i b parni brojevi, pa su $u, v \in \mathbb{Z}$.

Ako je $d \equiv 1 \pmod 4$, onda iz $a^2 \equiv b^2 \pmod 4$ slijedi da su a i b iste parnosti. Stoga je broj $u - v = \frac{1}{2}(a - b)$ cijeli. Stavimo $s = u - v, t = 2v$. Tada je $s, t \in \mathbb{Z}$ i $u + v\sqrt{d} = s + t\frac{1+\sqrt{d}}{2}$. □

Definicija 2.13. Jedinica *u* $\mathbb{Q}(\sqrt{d})$ *je algebarski cijeli broj* ε *sa svojstvom da je* $\frac{1}{\varepsilon}$ *također algebarski cijeli broj.*

Propozicija 2.14. *1)* $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$,

2) $|\alpha| = 0 \iff \alpha = 0$,

3) $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \implies |\alpha| \in \mathbb{Z}$,

4) $\varepsilon \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *je jedinica* $\iff |\varepsilon| = \pm 1$.

Dokaz. 1) Neka je $\alpha = u + v\sqrt{d}, \beta = s + t\sqrt{d}$. Tada je

$$\begin{aligned}\overline{\alpha\beta} &= \overline{\left(us + vtd + (ut + vs)\sqrt{d}\right)} = us + vtd - (ut + vs)\sqrt{d} \\ &= (u - v\sqrt{d})(s - t\sqrt{d}) = \overline{\alpha} \cdot \overline{\beta}.\end{aligned}$$

Prema tome,

$$|\alpha\beta| = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta}) = |\alpha| \cdot |\beta|.$$

2) Ako je $\alpha = 0$, onda je $\overline{\alpha} = 0$ i $|\alpha| = 0$. S druge strane, ako je $|\alpha| = 0$, onda je $\alpha\overline{\alpha} = 0$, pa je $\alpha = 0$ ili $\overline{\alpha} = 0$. No, $\overline{\alpha} = 0$ povlači $\alpha = 0$.

3) Po Teoremu 2.12, α je oblika $a + b\sqrt{d}$, $a, b \in \mathbb{Z}$ kada je $d \equiv 2, 3 \pmod 4$ i oblika $a + b\frac{1+\sqrt{d}}{2}$, $a, b \in \mathbb{Z}$ kada je $d \equiv 1 \pmod 4$. U prvom slučaju se odmah vidi $|\alpha| = a^2 - db^2 \in \mathbb{Z}$, a u drugom imamo $|\alpha| = (a + b\frac{1+\sqrt{d}}{2})(a + b\frac{1-\sqrt{d}}{2}) = a^2 + ab + \frac{1-d}{4}b^2 \in \mathbb{Z}$.

4) Ako je ε jedinica, onda je $|\varepsilon| \cdot |\frac{1}{\varepsilon}| = |1| = 1$, pa budući da su $|\varepsilon|$ i $|\frac{1}{\varepsilon}|$ cijeli brojevi, slijedi da je $|\varepsilon| = \pm 1$.

Obratno, ako je $|\varepsilon| = \pm 1$, onda je $\varepsilon\overline{\varepsilon} = \pm 1$, pa je $\frac{1}{\varepsilon} = \pm\overline{\varepsilon}$ algebarski cijeli broj, što znači da je ε jedinica.

□

Budući da je algebarski cijeli broj ε jedinica ako i samo ako je $|\varepsilon| = \pm 1$, vidimo da je problem određivanja jedinica u realnom kvadratnom polju povezan s Pellovim jednadžbama. Preciznije:

- ako je $d \equiv 2$ ili $3 \pmod 4$, tada je $u + v\sqrt{d}$ jedinica u $\mathbb{Q}(\sqrt{d})$ ako i samo ako vrijedi $u^2 - dv^2 = \pm 1$,
- ako je $d \equiv 1 \pmod 4$, tada je $\frac{u+v\sqrt{d}}{2}$ jedinica u $\mathbb{Q}(\sqrt{d})$ ako i samo ako vrijedi $u^2 - dv^2 = \pm 4$.

Stoga se uz (običnu) Pellovu jednadžbu $x^2 - dy^2 = 1$ promatraju i jednadžbe $x^2 - dy^2 = -1, 4, -4$.

Uočimo da za razliku od obične Pellove jednadžbe (2.3^+), jednadžba (2.3^-) ne mora imati rješenja. Ako ima rješenja, njezino najmanje rješenje u prirodnim brojevima zovemo *fundamentalno rješenje*.

Teorem 2.15. *Pretpostavimo da jednadžba $x^2 - dy^2 = -1$ ima rješenja, te da joj je $x_1 + y_1\sqrt{d}$ fundamentalno rješenje. Tada je $(x_1 + y_1\sqrt{d})^2$ fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$. Ako definiramo $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$, tada su $x_{2n} + y_{2n}\sqrt{d}$ sva rješenja jednadžbe $x^2 - dy^2 = 1$, a $x_{2n+1} + y_{2n+1}\sqrt{d}$ sva rješenja jednadžbe $x^2 - dy^2 = -1$ u prirodnim brojevima.*

Dokaz. Imamo: $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, pa je $x_n^2 - dy_n^2 = (x_1^2 - dy_1^2)^n = (-1)^n$. Dakle, zaista je $x_{2n} + y_{2n}\sqrt{d}$ rješenje od $x^2 - dy^2 = 1$, a $x_{2n+1} + y_{2n+1}\sqrt{d}$ od $x^2 - dy^2 = -1$. Pretpostavimo da za fundamentalno rješenje $a + b\sqrt{d}$ jednadžbe (2.3^+) vrijedi

$$1 < a + b\sqrt{d} < (x_1 + y_1\sqrt{d})^2.$$

Iz $(x_1 + y_1\sqrt{d})(-x_1 + y_1\sqrt{d}) = 1$, slijedi $0 < -x_1 + y_1\sqrt{d} < 1$. Stoga je

$$-x_1 + y_1\sqrt{d} < (a + b\sqrt{d})(-x_1 + y_1\sqrt{d}) = s + t\sqrt{d} < x_1 + y_1\sqrt{d},$$

gdje je $s = -ax_1 + dby_1, t = ay_1 - bx_1$ i vrijedi $s^2 - dt^2 = -1$. Zbog $s + t\sqrt{d} > 0$ i $s - t\sqrt{d} < 0$, jasno je da je $t > 0$. Ako je $s < 0$, onda iz $-x_1 + y_1\sqrt{d} < s + t\sqrt{d}$ dobivamo $x_1 + y_1\sqrt{d} > -s + t\sqrt{d}$. Prema tome, zaključujemo da je $|s| + t\sqrt{d}$ rješenje od (2.3^-), koje je manje od fundamentalnog, što je kontradikcija.

Pretpostavimo sada da je $u + v\sqrt{d}$ neko rješenje od (2.3^-) koje nije sadržano u nizu $(x_{2n+1} + y_{2n+1}\sqrt{d})$. Tada postoji $m \in \mathbb{N}$ takav da je

$$(x_1 + y_1\sqrt{d})^{2m-1} < u + v\sqrt{d} < (x_1 + y_1\sqrt{d})^{2m+1}.$$

Množeći ove nejednakosti sa $(x_1 - y_1\sqrt{d})^{2m}$, dobivamo

$$-x_1 + y_1\sqrt{d} < \sigma + \tau\sqrt{d} < x_1 + y_1\sqrt{d},$$

gdje je $\sigma^2 - d\tau^2 = -1$. No, već smo dokazali da takvi σ i τ ne mogu postojati. □

Jednadžba

$$x^2 - dy^2 = 4 \tag{2.6}$$

$(d \in \mathbb{N}, d \neq \square)$ naravno uvijek ima rješenja u prirodnim brojevima, jer ako je (u, v) rješenje jednadžbe $x^2 - dy^2 = 1$, onda je $x = 2u, y = 2v$ rješenje jednadžbe (2.6). No, vidjet ćemo da za neke d-ove mogu postojati i neka rješenja koja se ne dobivaju na ovaj način. Potpuno analogno Teoremu 2.6, dokazuje se sljedeći teorem:

Teorem 2.16. *Sva rješenja (x_n, y_n) jednadžbe $x^2 - dy^2 = 4$ u prirodnim brojevima dana su sa*

$$\frac{x_n + y_n\sqrt{d}}{2} = \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^n, \qquad n \in \mathbb{N},$$

gdje je (x_1, y_1) fundamentalno (tj. najmanje) rješenje te jednadžbe.

Promotrimo sada slučajeve koji mogu nastupiti u ovisnosti o parnosti ili neparnosti brojeva x_1 i y_1. Jasno je da ne može biti da je y_1 neparan, a x_1 paran, pa stoga imamo tri slučaja:

- Ako su x_1, y_1 oba parni, onda su x_n, y_n također parni za svaki n i $\frac{x_1}{2} + \frac{y_1}{2}\sqrt{d}$ predstavlja fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$.
- Ako je x_1 paran, a y_1 neparan, onda $4 \mid d$, tj. $d = 4d'$. Sada je $\frac{x_1}{2} + y_1\sqrt{d'}$ fundamentalno rješenje jednadžbe $x^2 - d'y^2 = 1$.
- Ako su x_1, y_1 neparni, mora vrijediti $d \equiv dy_1^2 \equiv x_1^2 - 4 \equiv 5 \pmod 8$. Dakle, nužan uvjet da bi jednadžba $x^2 - dy^2 = 4$ imala rješenja u neparnim brojevima jest da je $d \equiv 5 \pmod 8$. Primjerice, za $d = 5, 13, 21, 29$ jednadžba (2.6) ima rješenja u neparnim brojevima. Npr. za $d = 5$, fundamentalno rješenje je $(x_1, y_1) = (3, 1)$. No uvjet $d \equiv 5 \pmod 8$ nije i dovoljan, što pokazuje primjer $d = 37$, gdje je $(x_1, y_1) = (146, 24)$, pa su sva rješenja parna.

Propozicija 2.17. *Ako jednadžba $x^2 - dy^2 = 4$ ima rješenja u neparnim brojevima i ako je $x_1 + y_1\sqrt{d}$ njezino fundamentalno rješenje, onda je*

$$\left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^3 = \frac{1}{8}(x_1^3 + 3dx_1y_1^2) + \frac{1}{8}(3x_1^2y_1 + dy_1^3)\sqrt{d}$$

fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$.

Dokaz. Budući da su x_1, y_1 neparni i $d \equiv 5 \pmod 8$, vrijedi

$$x_1^2 + 3dy_1^2 \equiv 1 + 15 \equiv 0 \pmod 8, \qquad 3x_1^2 + dy_1^2 \equiv 3 + 5 \equiv 0 \pmod 8,$$

pa su brojevi $u = \frac{1}{8}(x_1^3 + 3dx_1y_1^2)$ i $v = \frac{1}{8}(3x_1^2y_1 + dy_1^3)$ cijeli. Nadalje, $u^2 - dv^2 = \left(\frac{x_1^2 - dy_1^2}{4}\right)^3 = 1$.

Pretpostavimo da $u + v\sqrt{d}$ nije fundamentalno rješenje jednadžbe (2.3^+), te neka je $s + t\sqrt{d}$ njezino fundamentalno rješenje. To znači da je

$$1 < s + t\sqrt{d} < \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^3.$$

Uočimo da ne može biti $s + t\sqrt{d} < \dfrac{x_1 + y_1\sqrt{d}}{2}$, jer bi tada $2s + 2t\sqrt{d}$ bilo rješenje od (2.6) koje je manje od $x_1 + y_1\sqrt{d}$. Također, ne može biti $s + t\sqrt{d} = \left(\dfrac{x_1 + y_1\sqrt{d}}{2}\right)^2$,

jer broj $\dfrac{x_1^2+dy_1^2}{4}$ nije cijeli. Zato je

$$\left(\frac{x_1+y_1\sqrt{d}}{2}\right)^k < s+t\sqrt{d} < \left(\frac{x_1+y_1\sqrt{d}}{2}\right)^{k+1} \tag{2.7}$$

za $k=1$ ili $k=2$. Množeći (2.7) s $\left(\dfrac{x_1-y_1\sqrt{d}}{2}\right)^k$ dobivamo

$$1 < \frac{a+b\sqrt{d}}{2} < \frac{x_1+y_1\sqrt{d}}{2},$$

gdje je $a^2-db^2=4$, što je u kontradikciji s minimalnošću od (x_1,y_1). □

Konačno, promotrimo još i jednadžbu

$$x^2-dy^2=-4. \tag{2.8}$$

Ona ne mora imati rješenja. Ako jednadžba $x^2-dy^2=-1$ ima rješenja, onda i jednadžba (2.8) ima rješenja (u parnim brojevima). No, jednadžba (2.8) može imati i rješenja u neparnim brojevima. To je na primjer slučaj za $d=5,13,29,53$ (za $d=5$ rješenje je $(1,1)$). Ponovo je nužan uvjet za postojanje neparnih rješenja $d\equiv 5 \pmod 8$. Analogno Teoremu 2.15 se dokazuje:

Teorem 2.18. *Pretpostavimo da jednadžba $x^2-dy^2=-4$ ima rješenja, te da je $x_1+y_1\sqrt{d}$ njezino fundamentalno rješenje. Tada su sva rješenja te jednadžbe dana s*

$$\frac{x_n+y_n\sqrt{d}}{2} = \left(\frac{x_1+y_1\sqrt{d}}{2}\right)^n, \qquad n \text{ neparan.}$$

Nadalje, $\left(\dfrac{x_1+y_1\sqrt{d}}{2}\right)^2$ je fundamentalno rješenje jednadžbe $x^2-dy^2=4$.

Vratimo se sada jedinicama u realnim kvadratnim poljima i sumirajmo sve ove rezultate o jednadžbama $x^2-dy^2=\pm 1,\pm 4$. Sljedeći korolar je direktna posljedica Teorema 2.6, 2.15, 2.16 i 2.18 u kojima je dana struktura skupa svih rješenja Pellovih jednadžbi.

Korolar 2.19. *Grupa jedinica u realnom kvadratnom polju $\mathbb{Q}(\sqrt{d})$ generirana je s -1 i ε_d, gdje je $\varepsilon_d = a+b\sqrt{d}$ ili $\frac{a+b\sqrt{d}}{2}$, dok je $a+b\sqrt{d}$ fundamentalno rješenje jedne od Pellovih jednadžbi $x^2-dy^2=\pm 1,\pm 4$. Dakle, svaka se jedinica može napisati u obliku $\pm\varepsilon_d^n$, $n\in\mathbb{Z}$. Ako je $x_1+y_1\sqrt{d}$ fundamentalno rješenje Pellove jednadžbe $x^2-dy^2=1$, onda je $x_1+y_1\sqrt{d}=(a+b\sqrt{d})^k$, gdje je $k\in\{1,2,3,6\}$.*

Preciznije informacije o eksponentu k su dane u Tablici 2.2, pomoću koje k možemo odrediti iz kongruencijskih svojstava brojeva a, b i d.

Definicija 2.20. *Generator ε_d se zove* fundamentalna jedinica *kvadratnog polja $\mathbb{Q}(\sqrt{d})$, a broj $R = \ln \varepsilon_d$ zovemo* regulator.

d	$a^2 - db^2$	b	a	k	primjer
$\equiv 3 \pmod 4$	1			1	$d = 3$
$\equiv 1, 2 \pmod 4$	1	$\equiv 0 \pmod 2$		1	$d = 6$
$\equiv 1, 2 \pmod 4$	-1	$\equiv 1 \pmod 2$		2	$d = 2$
$\equiv 5 \pmod{16}$	4	$\equiv 1 \pmod 2$	$\equiv \pm 3b \pmod 8$	3	$d = 31$
$\equiv 5 \pmod{16}$	-4	$\equiv 1 \pmod 2$	$\equiv \pm b \pmod 8$	6	$d = 5$
$\equiv 13 \pmod{16}$	4	$\equiv 1 \pmod 2$	$\equiv \pm b \pmod 8$	3	$d = 45$
$\equiv 13 \pmod{16}$	-4	$\equiv 1 \pmod 2$	$\equiv \pm 3b \pmod 8$	6	$d = 13$

Tablica 2.1: Veza fundamentalnih rješenja i fundamentalnih jedinica.

2.3 Verižni razlomak od $\frac{1+\sqrt{d}}{2}$

Kao što smo vidjeli u prethodnom poglavlju, kada je $d \equiv 1 \pmod 4$, algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ su i brojevi oblika $u + v\frac{1+\sqrt{d}}{2}$, $u, v \in \mathbb{Z}$. Zato je za teoriju bitno promotriti svojstva razvoja u verižni razlomak brojeva oblika $\frac{1+\sqrt{d}}{2}$.

Promotrimo prvo malo općenitiju situaciju:

Teorem 2.21. *Neka je $d \in \mathbb{Q}$, $d \neq \square$, $d > \frac{1}{4}$. Tada razvoj u jednostavni verižni razlomak od $\sqrt{d} + \frac{1}{2}$ ima oblik*

$$\sqrt{d} + \frac{1}{2} = [\, a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0 - 1}\,],$$

tj. $a_0 = \left\lfloor \sqrt{d} + \frac{1}{2} \right\rfloor$, a dio razvoja od a_1 do $a_{\ell-1}$ je palindroman.

Dokaz. Označimo $\alpha = \sqrt{d} + \frac{1}{2}$. Kako je $d > \frac{1}{4}$, slijedi $\alpha > 1$. Promotrimo broj $\beta = \alpha + \lfloor \alpha \rfloor - 1$. Očito je $\beta > 1$ i

$$\overline{\beta} = \overline{\sqrt{d} + \frac{1}{2} + \left\lfloor \sqrt{d} + \frac{1}{2} \right\rfloor - 1} = \left\lfloor \sqrt{d} + \frac{1}{2} \right\rfloor - \frac{1}{2} - \sqrt{d}.$$

Za $x \notin \mathbb{Q}$ vrijedi $x - 1 < \lfloor x \rfloor < x$ pa dobijemo:

$$\sqrt{d} - \frac{1}{2} < \left\lfloor \sqrt{d} + \frac{1}{2} \right\rfloor < \sqrt{d} + \frac{1}{2},$$

odnosno

$$-1 < \left\lfloor \sqrt{d} + \frac{1}{2} \right\rfloor - \sqrt{d} - \frac{1}{2} < 0,$$

pa vidimo da je β reduciran ($-1 < \beta' < 0$), te mu je razvoj čisto periodan, tj.

$$\beta = [\,\overline{b_0, b_1, \ldots, b_{\ell-1}}\,] = [\,b_0, \overline{b_1, \ldots, b_{\ell-1}, b_0}\,].$$

Razvoji od β i α se razlikuju samo u prvom članu, tj. $b_0 = 2a_0 - 1$ i $b_i = a_i$, za $i \geq 1$.

Isto kao u dokazu Teorema 1.32, dobijemo $\beta = [\,b_0, \overline{b_{\ell-1}, b_{\ell-2}, \ldots, b_0}\,]$, čime je teorem dokazan. □

Potpuno analogno Napomeni 1.35, postupak za razvoj verižnog razlomka broja oblika $\sqrt{d} + \frac{1}{2}$ možemo pojednostavniti. Neka su $d, s_0, t_0 = 2s_0$ takvi da $t_0 \mid d - s_0^2$ i $s_0 < \sqrt{d}$. Tada u razvoju broja $\dfrac{\sqrt{d} + s_0}{t_0}$ nizovi a_0, s_0 i t_0 imaju istu simetriju kao u Teoremu 1.33.

Napomena 2.22. *Specijalno za $d \in \mathbb{N}, d \neq \square, d \equiv 1 \pmod 4$ i $\alpha = \frac{\sqrt{d}+1}{2}$, uz $s_0 = t_0 = 1, \alpha_0 = \dfrac{s_0 + \sqrt{d}}{2t_0}$ imamo:*

$$s_{i+1} = 2a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{4t_i}, \quad \alpha_{i+1} = \frac{s_{i+1} + \sqrt{d}}{2t_{t+1}}, \quad a_{i+1} = \left\lfloor \frac{s_{i+1} + \lfloor \sqrt{d} \rfloor}{2t_{t+1}} \right\rfloor.$$

Vrijede sljedeće simetrije:

$$\begin{aligned} a_i &= a_{\ell-i}, && i = 1, 2, \ldots, \ell - 1, && a_\ell = 2a_0 - 1, \\ s_{i+1} &= s_{\ell-i}, && i = 0, 1, \ldots, \ell - 1, \\ t_i &= t_{\ell-i}\,, && i = 0, 1, \ldots, \ell - 1. \end{aligned}$$

Ako se dogodi:

(i) $s_i = s_{i+1}$, tada znamo da je duljina perioda parna, tj. $\ell = 2i$,

(ii) $t_i = t_{i+1}$, tada znamo da je duljina perioda neparna, tj. $\ell = 2i + 1$.

Mnogi matematičari su proučavali razvoj u verižni razlomak od $\frac{1+\sqrt{d}}{2}$, a Ishii, Kaplan i K.S. Williams su u [12] uspostavili neke nejednakosti između $\ell\big(\sqrt{d}\big)$ i $\ell\big(\frac{1+\sqrt{d}}{2}\big)$. Neka je $d \in \mathbb{N}, d \neq \square, d > 16$ takav da je $d \equiv 1 \pmod 4$. Vrijede tvrdnje:

a) Ako postoje neparni brojevi x, y takvi da $x^2 - dy^2 = 4$ (nakon Teorema 2.16 smo vidjeli da je tada nužno $d \equiv 5 \pmod 8$, ali ne i dovoljno), tada

$$\ell\left(\frac{1+\sqrt{d}}{2}\right) + 4 \leq \ell\big(\sqrt{d}\big) \leq 5\ell\left(\frac{1+\sqrt{d}}{2}\right).$$

b) Ako ne postoje neparni brojevi x, y takvi da $x^2 - dy^2 = 4$, ali postoje cijeli brojevi x, y takvi da $x^2 - dy^2 = -1$, tada

$$\frac{1}{3}\ell\left(\frac{1+\sqrt{d}}{2}\right) \leq \ell\big(\sqrt{d}\big) \leq 3\ell\left(\frac{1+\sqrt{d}}{2}\right) - 4.$$

c) Ako ne postoje neparni brojevi x, y takvi da $x^2 - dy^2 = 4$, i ne postoje cijeli brojevi x, y takvi da $x^2 - dy^2 = -1$, tada

$$\frac{1}{3}\ell\left(\frac{1+\sqrt{d}}{2}\right) \leq \ell\big(\sqrt{d}\big) \leq 3\ell\left(\frac{1+\sqrt{d}}{2}\right) - 8.$$

K.S. Williams i N. Buck su u [52] pokazali da su nejednakosti najbolje moguće, tj. našli su nizove brojeva za koje se postiže jednakost. Vrijede tvrdnje:

a') Postoji beskonačno mnogo brojeva $d \in \mathbb{N}, d \neq \square, d \equiv 1 \pmod 4$ takvih da:

1) $\ell\big(\frac{1+\sqrt{d}}{2}\big) + 4 = \ell\big(\sqrt{d}\big)$,
2) $x^2 - dy^2 = 4$ je rješiva u neparnim cijelim brojevima,
3) $\ell\big(\sqrt{d}\big)$ je neograničeno.

a") Postoji beskonačno mnogo brojeva $d \in \mathbb{N}, d \neq \square, d \equiv 1 \pmod 4$ takvih da:

1) $\ell\big(\sqrt{d}\big) = 5\ell\big(\frac{1+\sqrt{d}}{2}\big)$,
2) $x^2 - dy^2 = 4$ je rješiva u neparnim cijelim brojevima,
3) $\ell\big(\sqrt{d}\big)$ je neograničeno.

b') Postoji beskonačno mnogo brojeva $d \in \mathbb{N}, d \neq \square, d \equiv 1 \pmod 4$ takvih da:

1) $\frac{1}{3}\ell\big(\frac{1+\sqrt{d}}{2}\big) = \ell\big(\sqrt{d}\big)$,
2) $x^2 - dy^2 = 4$ nije rješiva u neparnim cijelim brojevima,
2') $x^2 - dy^2 = -1$ je rješiva u cijelim brojevima,
3) $\ell\big(\sqrt{d}\big)$ je neograničeno.

b") Postoji beskonačno mnogo brojeva $d \in \mathbb{N}, d \neq \square, d \equiv 1 \pmod 4$ takvih da:

1) $\ell\big(\sqrt{d}\big) = 3\ell\big(\frac{1+\sqrt{d}}{2}\big) - 4$,
2) $x^2 - dy^2 = 4$ nije rješiva u neparnim cijelim brojevima,
2') $x^2 - dy^2 = -1$ je rješiva u cijelim brojevima,
3) $\ell\big(\sqrt{d}\big)$ je neograničeno.

c') Postoji beskonačno mnogo brojeva $d \in \mathbb{N}, d \neq \square, d \equiv 1 \pmod 4$ takvih da:

1) $\frac{1}{3}\ell\big(\frac{1+\sqrt{d}}{2}\big) = \ell\big(\sqrt{d}\big)$,
2) $x^2 - dy^2 = 4$ nije rješiva u neparnim cijelim brojevima,
2') $x^2 - dy^2 = -1$ nije rješiva u cijelim brojevima,
3) $\ell\big(\sqrt{d}\big)$ je neograničeno.

c") Postoji beskonačno mnogo brojeva $d \in \mathbb{N}, d \neq \square, d \equiv 1 \pmod 4$ takvih da:

1) $\ell\big(\sqrt{d}\big) = 3\ell\big(\frac{1+\sqrt{d}}{2}\big) - 8$,
2) $x^2 - dy^2 = 4$ nije rješiva u neparnim cijelim brojevima,
2') $x^2 - dy^2 = -1$ nije rješiva u cijelim brojevima,
3) $\ell\big(\sqrt{d}\big)$ je neograničeno.

Prethodne tvrdnje pokazane su tako da se za vrijednost d uzimaju članovi nekih specijalnih nizova. Preciznije:

a') Za $d = (2F_{6n+1} + 1)^2 + (8F_{6n} + 4)$, $n = 1, 2, \ldots$, vrijedi

$$\ell\big(\sqrt{d}\big) = 6n + 5 \qquad \text{i} \qquad \ell\left(\frac{1+\sqrt{d}}{2}\right) = 6n + 1,$$

a") Za $d = 16 \cdot 5^{2n} + 12 \cdot 5^n + 1$, $n = 1, 2, \ldots$, vrijedi

$$\ell\big(\sqrt{d}\big) = 10n + 5 \qquad \text{i} \qquad \ell\left(\frac{1+\sqrt{d}}{2}\right) = 2n + 1,$$

b') Za $d = 4 \cdot 17^{2n} + 9 \cdot 17^n + 4$, $n = 1, 2, \ldots$, vrijedi

$$\ell\big(\sqrt{d}\big) = 2n + 1 \qquad \text{i} \qquad \ell\left(\frac{1+\sqrt{d}}{2}\right) = 6n + 3,$$

b") Za $d = 9 \cdot 4^{2n} + 10 \cdot 4^n + 1$, $n = 1, 2, \ldots$, vrijedi

$$\ell\big(\sqrt{d}\big) = 6n - 1 \qquad \text{i} \qquad \ell\left(\frac{1+\sqrt{d}}{2}\right) = 2n + 1,$$

c') Za $d = 225 \cdot 61^{2n} + 155 \cdot 61^n + 25$, $n = 1, 2, \ldots$, vrijedi

$$\ell\big(\sqrt{d}\big) = 4n + 2 \qquad \text{i} \qquad \ell\left(\frac{1+\sqrt{d}}{2}\right) = 12n + 6,$$

c") Za $d = 81 \cdot 10^{2n} + 66 \cdot 10^n + 9$, $n = 1, 2, \ldots$, vrijedi

$$\ell\big(\sqrt{d}\big) = 12n - 2 \qquad \text{i} \qquad \ell\left(\frac{1+\sqrt{d}}{2}\right) = 4n + 2.$$

Pokažimo na primjer slučaj *a')*.

Primjer 2.23. *Neka je* $d(n) = (2F_{6n+1}+1)^2 + 8F_{6n} + 4$, $n \geq 1$, *gdje je* F_n *n-ti Fibonaccijev broj* ($F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$). *Tada je*

$$\ell\big(\sqrt{d}\big) = 6n+5 \qquad i \qquad \ell\left(\frac{1+\sqrt{d(n)}}{2}\right) = 6n+1.$$

Budući da je

$$F_n \equiv \begin{cases} 0 \pmod 2 & za\ n \equiv 0 \pmod 3, \\ 1 \pmod 2 & za\ n \not\equiv 0 \pmod 3, \end{cases}$$

vidimo da je $d(n) \equiv 5 \pmod 8$, *pa* $d(n)$ *ne može biti kvadrat.*

Koristeći $F_{r+t}F_s - F_rF_{s+t} = (-1)^{s-1}F_tF_{r-s}, r \geq s \geq 0, t \geq 0$, *što slijedi npr. iz Binetove formule* $F_n = \frac{1}{\sqrt{5}}\Big(\big(\frac{1+\sqrt{5}}{2}\big)^n - \big(\frac{1-\sqrt{5}}{2}\big)^n\Big)$, *indukcijom se pokaže sljedeće:*

Za $\sqrt{d}$ *imamo:*

i	s_i	t_i	a_i
0	0	1	$2F_{6n+1}+2$
k, $(1 \leq k \leq n)$	$4F_{3k}F_{6n-3k+1}$ $-2(-1)^kF_{6n-6k+1}+2$	$2F_{3k}F_{6n-3k+1}+1$	4
k, $(n+1 \leq k \leq 2n-1)$	$4F_{3k}F_{6n-3k+1}$ $-2(-1)^kF_{6k-6n-1}+2$	$2F_{3k}F_{6n-3k+1}+1$	4
$2n$	$4F_{6n} - 2F_{6n-1} + 2$	$2F_{6n}+1$	3
$2n+1$	$2F_{6n+1}+1$	4	F_{6n+1}
$2n+2$	$2F_{6n+1}-1$	$2F_{6n+2}+1$	1
$2n+k+2$, $(1 \leq k \leq n)$	$4F_{3k-1}F_{6n-3k+2}$ $-2(-1)^kF_{6n-6k+3}+2$	$2F_{3k-1}F_{6n-3k+2}+1$	4
$2n+k+2$, $(n+1 \leq k \leq 2n)$	$4F_{3k-1}F_{6n-3k+2}$ $-2(-1)^kF_{6k-6n-3}+2$	$2F_{3k-1}F_{6n-3k+2}+1$	4
$4n+3$	$2F_{6n}+2$	$2F_{6n+2}+1$	1
$4n+4$	$2F_{6n+1}-1$	4	F_{6n+1}
$4n+5$	$2F_{6n+1}+1$	$2F_{6n}+1$	3
$4n+k+6$, $(0 \leq k \leq n-1)$	$4F_{3k+1}F_{6n-3k}$ $-2(-1)^kF_{6n-6k-1}+2$	$2F_{3k+4}F_{6n-3k-3}+1$	4
$4n+k+6$, $(n \leq k \leq 2n-2)$	$4F_{3k+1}F_{6n-3k}$ $-2(-1)^kF_{6k-6n+1}+2$	$2F_{3k+4}F_{6n-3k-3}+1$	4
$6n+5$	$2F_{6n+1}+1$	1	$4F_{6n+1}+4$

pa vidimo da vrijedi $\ell\left(\sqrt{d}\right) = 6n+5$. *Nadalje, budući da imamo* $t_{4n+4} = 4$, *jednadžba* $x^2 - dy^2 = 4$ *je rješiva u neparnim cijelim brojevima.*

Za $\dfrac{1+\sqrt{d}}{2}$ *imamo:*

k	s_k	t_k	a_k
0	1	2	$F_{6n+1}+1$
$1,\ldots,6n$	$1+2F_{6n+1}-4F_{k-1}F_{6n-k+1}$	$2+4F_kF_{6n-k+1}$	1
$6n+1$	$2F_{6n+1}+1$	2	$2F_{6n+1}+1$

Vidimo da vrijedi $\ell\left(\frac{1+\sqrt{d}}{2}\right) = 6n+1$.

Ovo je bio prvi primjer razvoja u verižni razlomak od $\sqrt{d}$ *ili* $\frac{1+\sqrt{d}}{2}$ *kod kojih se pojavljuju Fibonaccijevi brojevi i njihovi kvadrati, za koje se zna točan razvoj. Takvi nizovi su kasnije nazvani beepers, a u Poglavlju 6 ćemo vidjeti poopćenje takvih primjera.*

Poglavlje 3

Funkcijska polja — razvoj u verižni razlomak nad $\mathbb{Q}((X^{-1}))$

U novije se vrijeme dosta proučavaju verižni razlomci nad funkcijskim poljima, tj. za $D \in \mathbb{Q}[X]$ verižni razlomak od $\sqrt{D}$ i $\frac{1+\sqrt{D}}{2}$ nad poljem $\kappa = \mathbb{Q}((X^{-1}))$ formalnih Laurentovih redova u X^{-1} nad $\mathbb{Q}$, jer postoje velike analogije s brojevima. $\alpha \in \kappa$ je oblika:

$$\alpha = \sum_{j=-m}^{\infty} c_j X^{-j}, \quad c_j \in \mathbb{Q},\ c_{-m} \neq 0.$$

Kada objasnimo razvoj u regularni verižni razlomak, vrijedit će sva svojstva verižnih razlomaka navedena u §1.1.

Definirajmo $\lfloor \alpha \rfloor$ kao polinomijalni dio od α, tj. $\lfloor \alpha(X) \rfloor = c_{-m}X^m + \cdots + c_{-1}X + c_0$. Regularni verižni razlomak od $\alpha(X)$, naime $\langle\, a_0(X), a_1(X), \dots \,\rangle$ [1] dobijemo istim postupkom (1.2). Imamo $\alpha_0(X) = \alpha(X)$ i

$$a_i(X) = \lfloor \alpha_i(X) \rfloor, \qquad \alpha_{i+1}(X) = \frac{1}{\alpha_i(X) - a_i(X)},\ \text{ako je } a_i(X) \neq \alpha_i(X).$$

Lako se vidi da su svi $a_i(X)$ polinomi barem prvog stupnja, te iz (1.3) slijedi:

$$\deg p_{i+1} = \deg a_{i+1} + \deg p_i \qquad \text{i} \qquad \deg q_{i+1} = \deg a_{i+1} + \deg q_i,$$

pa nam je zbog toga zgodno za $|\ |$ uzeti nearhimedsku apsolutnu vrijednost definiranu sa $|P| = e^{\deg P}$. To jest, za $\alpha \in \mathbb{Q}((X^{-1}))$ imamo

$$|\alpha| = e^{-m}.$$

Tada je $|P/Q| = e^{\deg P - \deg Q}$, za $P, Q \in \mathbb{Q}[X]$.

Razvoj u verižni razlomak ima mnoga slična svojstva kao i brojevni razvoj.

[1] Iako se radi o regularnom verižnom razlomku, koristit ćemo oznaku $\langle\ \rangle$, budući se može dogoditi da za neki $X \in \mathbb{N}$ taj razvoj brojevno nije regularan, tj. da vrijedi $a_i(X) \notin \mathbb{N}$. Također ćemo koristiti oznaku $\alpha(X)$ kada mislimo na razvoj u kojem su parcijalni kvocijenti iz $\mathbb{Q}[X]$. Općenito se takav razvoj razlikuje od razvoja kojem su koeficijenti iz $\mathbb{Z}$ — što ćemo i vidjeti na Primjerima 3.2 i 3.4 — kojeg ćemo označavati s malim x, tj. $\alpha(x)$.

Propozicija 3.1. *Neka je $f \in \mathbb{Q}((X^{-1}))$. Ako su $p(X)$ i $q(X)$ relativno prosti polinomi, tada je*

$$\deg(q(X)f(X) - p(X)) < -\deg(q(X))$$

ako i samo ako je $p(X)/q(X)$ konvergenta od $f(X)$.

Dokaz. Pogledati [31, Prop. 11]. □

Funkciju sgn definiramo kao koeficijent vodećeg koeficijenta, tj. $\operatorname{sgn}\alpha = c_{-m}$, a $\sigma(\alpha)$ kao predznak vodećeg koeficijenta.

Uočimo da ako je $\operatorname{sgn} a_0(X) > 0$, budući je $\deg a_i > 0$ ili $a_i(X) = 0$ vrijedi $\sigma(p_n(X)) = \sigma(q_n(X))$, za sve $n \geq 0$.

Primjer 3.2. *Razvijmo $\alpha(X) = \dfrac{X^4 - X^3 - 4X - 10}{X^3 - 2X^2 + 3X - 7}$ u verižni razlomak.*

$$\begin{aligned}
\alpha_0 &= X + 1 - \frac{X^2 + 3}{X^3 - 2X^2 + 3X - 7}, & a_0 &= X + 1,\\
\alpha_1 &= -\frac{X^3 - 2X^2 + 3X - 7}{X^2 + 3} = -X + 2 + \frac{1}{X^2 + 3}, & a_1 &= -X + 2,\\
\alpha_2 &= X^2 + 3, & a_2 &= X^2 + 3,
\end{aligned}$$

pa vidimo da je $\alpha(X) = \langle\, X + 1, -X + 2, X^2 + 3 \,\rangle$. Razvijmo $\alpha(x)$ u verižni razlomak za $x \geq 5$.

$$\begin{aligned}
\alpha_0 &= x + 1 - \frac{x^2 + 3}{x^3 - 2x^2 + 3x - 7}, & a_0 &= x,\\
\alpha_1 &= \frac{x^3 - 2x^2 + 3x - 7}{x^3 - 3x^2 + 3x - 10} = 1 + \frac{x^2 + 3}{x^3 - 3x^2 + 3x - 10}, & a_1 &= 1,\\
\alpha_2 &= \frac{x^3 - 3x^2 + 3x - 10}{x^2 + 3} = x - 3 - \frac{1}{x^2 + 3}, & a_2 &= x - 4,\\
\alpha_3 &= \frac{x^2 + 3}{x^2 + 2} = 1 + \frac{1}{x^2 + 2}, & a_3 &= 1,\\
\alpha_4 &= x^2 + 2, & a_4 &= x^2 + 2,
\end{aligned}$$

pa vidimo da je za $x \geq 5$ $\alpha(x) = [\, x, 1, x - 4, 1, x^2 + 2 \,]$.

Kako smo vidjeli u prethodnom primjeru, razvoj od $\alpha(X)$ nad $\mathbb{Q}[X]$ i razvoj od $\alpha(x)$ s parcijalnim kvocijentima iz $\mathbb{N}$ se mogu bitno razlikovati. S parcijalnim

kvocijentima iz $\mathbb{Z}$, razvoj od $\alpha(x)$ bi bio isti kao i $\alpha(X)$. Međutim, općenito nije tako, jer u razvoju od $\alpha(X)$ možemo dobiti i racionalne brojeve.

Kod brojeva nas uglavnom zanima duljina perioda kvadratne iracionalnosti. U analogiji s brojevnim slučajem, i ovdje bi mogli željeti odrediti duljinu perioda razvoja u verižni razlomak korijena polinoma parnog stupnja kojem je vodeći koeficijent kvadrat (ako je stupanj neparan ili vodeći koeficijent nije kvadrat, razvoj nije periodan). Na žalost, periodnost je osigurana samo ako je početno polje konačno.

Kada promatramo razvoj nad poljem karakteristike 0, parcijalni kvocijenti će tipično biti polinomi stupnja 1, ali im se najčešće koeficijenti eksponencijalno povećavaju, te razvoj najčešće nije periodan.

Pretpostavimo da je $Y^2 = f(X)$ stupnja $2(g+1)$, pa za tipični potpuni kvocijent $(Y + S_k)/T_k$ od Y vrijedi

$$\deg S_k = g + 1 \quad \text{i} \quad \deg T_k \leq g.$$

Analogno Teoremu 2.3, kraj perioda nastupa kada je $\deg a_h = g + 1$ i $\deg T_h = 0$.

Ako je razvoj periodan, u funkcijskom polju postoji netrivijalna jedinica, pa za regulator možemo uzeti stupanj fundamentalne jedinice, drugim riječima, regulator je konačan broj. Nadalje, regulator mora biti zbroj stupnjeva parcijalnih kvocijenata primitivnog perioda.

Primjer 3.3. *Za*

$$Y^2 = X^6 + 2X^2 + X + 1,$$

razvoj u verižni razlomak od Y nad $\mathbb{Q}[X]$ je

$$\Big\langle X^3, X - \frac{1}{2}, -4X - 6, \frac{-1}{16}X + \frac{1}{8}, \frac{128}{5}X + \frac{512}{25}, \frac{125}{1488}X - \frac{6025}{69192},$$
$$\frac{-3217428}{8125}X - \frac{812642742}{105625}, \frac{-1373125}{203694562323}X + \frac{20593600625}{158474369487294},$$
$$\frac{7991216816924103}{1570855000}X + \frac{279952799594094347}{77757322500}, \dots \Big\rangle \quad (3.1)$$

S druge strane, promotrimo razvoj u verižni razlomak od Y nad $\mathbb{F}_p[X]$ za različite proste brojeve p. Razvoji moraju biti periodni. Na primjer, razvoj od Y nad $\mathbb{F}_5[X]$ je

k	$a_k(X)$	$s_k(X)$	$t_k(X)$
0	X^3	0	1
1	$X+2$	X^3	$2X^2+X+1$
2	$X+4$	X^3+3X+2	$2X^2+2X+2$
3	$4X+2$	X^3+2X+1	$3X^2+X$
4	$3X^2+3X+3$	X^3+4	$4X+1$
5	$4X+2$	X^3+4	$3X^2+X$
6	$X+4$	X^3+2X+1	$2X^2+2X+2$
7	$X+2$	X^3+3X+2	$2X^2+X+1$
8	$2X^3$	X^3	1

(uočimo da $(4X+1) \mid (X^6+2X^2+X+1)$ *nad* $\mathbb{F}_5[X]$*) i vidimo da je regulator 11. Nad* $\mathbb{F}_7[X]$ *imamo,*

k	$a_k(X)$	$s_k(X)$	$t_k(X)$
0	X^3	0	1
1	$X+3$	X^3	$2X^2+X+1$
2	$3X+1$	X^3+4X+3	$3X^2+6X+6$
3	$3X+1$	X^3+6X+3	$3X^2+6X+1$
4	$6X+2$	X^3+3X+5	$5X^2+3X+4$
5	$5X+4$	X^3+6X+3	$6X^2+5X+5$
6	$2X+6$	X^3+4X+3	X^2+4X+4
7	X^3	X^3	2
8	$2X+6$	X^3	X^2+4X+4
9	$5X+4$	X^3+4X+3	$6X^2+5X+5$
10	$6X+2$	X^3+6X+3	$5X^2+3X+4$
11	$3X+1$	X^3+3X+5	$3X^2+6X+1$
12	$3X+1$	X^3+6X+3	$3X^2+6X+6$
13	$X+3$	X^3+4X+3	$2X^2+X+1$
14	$2X^3$	X^3	1

pa je ovdje regulator 9. Rezultati Yua [54] i van der Poortena [35] kažu da ako je $\sqrt{f(X)}$ *periodan nad* $\mathbb{Q}$*, tada je* $R_q q^a = R_p p^b$*, gdje je* R_i *regulator nad* $\mathbb{F}_i[X]$ *i* a*,* b *neki cijeli brojevi. Stoga, da bi* $\mathbb{Q}[X,Y]$ *imao netrivijalnu jedinicu, za njegov*

regulator bi moralo vrijediti $5^a11 = 7^b9$*, što je nemoguće, pa vidimo da razvoj* (3.1) *nije periodan.*

Prethodni primjer pokazuje koncept *kvaziperiodnosti*. Uočimo da je u posljednjoj tablici jedinica dobivena u liniji 7, ali razvoj nije potpuno periodan sve do linije 14. U stvari, razvoj je palindroman. Preciznije, ako je razvoj od $\sqrt{f(X)}$ periodan s $t_k = \kappa$ jedinicom, tada

$$\sqrt{f(X)} = \langle\, a_0(X), \overline{a_1(X), \ldots, a_h(X), \kappa a_1(X)\kappa^{-1} a_2(X), \ldots, \kappa a_h(X)}\,\rangle,$$

također je očito da u tom slučaju k mora biti neparan. Više o kvazi-periodnosti se može naći u [1] i [36].

Čak i kada je razvoj nad $\mathbb{Q}[X]$ periodan, duljina perioda se najčešće razlikuje od razvoja nad $\mathbb{N}$.

Primjer 3.4. *Razvijemo li*

$$f(x) = 9x^2 + 8x + 2$$

u verižni razlomak nad brojevima, dobijemo

$$\sqrt{f(x)} = [\, 3x + 1, \overline{2, 1, 3x, 1, 2, 2(3x + 1)}\,],$$

dok nad $\mathbb{Q}[X]$ *imamo*

$$\sqrt{f(X)} = \langle\, 3X + \tfrac{4}{3}, \overline{9(3X + \tfrac{4}{3}), 2(3X + \tfrac{4}{3})}\,\rangle.$$

Postoje i brojni drugi rezultati. Na primjer, Malyshev [21] je iz Mazurovog teorema [22][2] pokazao da za racionalne a, b, c, d, duljina perioda razvoja u verižni razlomak od

$$\sqrt{X^4 + aX^3 + bX^2 + cX + d}$$

može poprimiti samo vrijednosti $1, 2, 3, 4, 5, 6, 8, 10, 14, 18, 22$, a možda i 9 i 11.

[2]Mazurov teorem kaže da je za nesingularnu eliptičku krivulju nad $\mathbb{Q}$ torzijska podgrupa $E(\mathbb{Q})_{tors}$ grupe racionalnih točaka $E(\mathbb{Q})$ jedna od: $\mathbb{Z}/m\mathbb{Z}$, $m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ ili 12, ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$, $m = 1, 2, 3, 4$.

Poglavlje 4

Brojevi s malom duljinom perioda (sleepers)

Postojanje niza brojeva s konstantnom duljinom perioda je dugo poznato.

Primjer 4.1. *Za* $d(n) = n^2 + 1$ *vrijedi* $\ell\big(\sqrt{d(n)}\big) = 1$.

Razvijmo $\sqrt{d(n)}$ *u verižni razlomak koristeći postupak* (1.12) *uz* $d = d(n) = n^2 + 1$ *imamo* $s_0 = 0$, $t_0 = 1$ *i* $a_0 = \lfloor \sqrt{d} \rfloor = n$.

i	$s_{i+1} = a_i t_i - s_i$	$t_{i+1} = \dfrac{d - s_{i+1}^2}{t_i}$	$a_i = \left\lfloor \dfrac{s_i + a_0}{t_i} \right\rfloor$
1	$s_1 = n$	$t_1 = \dfrac{n^2 + 1 - n^2}{1} = 1$	$a_1 = \left\lfloor \dfrac{n+n}{1} \right\rfloor = 2n$
2	$s_2 = n$	$t_2 = \dfrac{n^2 + 1 - n^2}{1} = 1$	$\ldots$

pa vidimo da je $\sqrt{d(n)} = [\, n, \overline{2n}\,]$.

Lako se vidi da za $n \geq 2$ i $n \geq 3$ (respektivno) vrijedi:

$$\sqrt{n^2 - 1} = [\, n - 1, \overline{1, 2(n-1)}\,] \qquad \text{i} \qquad \sqrt{n^2 - n} = [\, n - 1, \overline{2, 2(n-1)}\,]. \tag{4.1}$$

Takvih primjera je puno. Već su u Perronovoj knjizi [33, §26] karakterizirani svi brojevi s duljinama perioda do 4.

Primjer 4.2 (Brojevi s duljinom perioda 1)**.** *U ovom slučaju vrijedi:*

$$p'_{\ell-2} = p'_{-1} = 0, \qquad p'_{\ell-1} = p'_0 = 1,$$
$$q'_{\ell-2} = q'_{-1} = 1,$$

pa koristeći (1.22) *imamo*

$$a_0 = \frac{m}{2}, \qquad d = a_0^2 + 1.$$

Vidimo da je a_0 *proizvoljan, pa su svi brojevi duljine 1 dani Primjerom 4.1.*

Primjer 4.3 (Brojevi s duljinom perioda 2)**.** *U ovom slučaju vrijedi:*

$$p'_{\ell-2} = p'_0 = 1, \qquad p'_{\ell-1} = p'_1 = a_1,$$
$$q'_{\ell-2} = q'_0 = 0,$$

pa koristeći (1.22) *imamo*

$$a_0 = \frac{ma_1}{2}, \qquad d = a_0^2 + m.$$

a_1 *mora dijeliti* $2a_0$*, pa dobijemo:*

$$\sqrt{a_0^2 + m} = [\, a_0, \overline{\tfrac{2a_0}{m}, 2a_0}\,], \qquad \text{gdje su } a_0, m \in \mathbb{N},\ m \mid 2a_0.$$

Primjer 4.4 (Brojevi s duljinom perioda 3)**.** *U ovom slučaju vrijedi:*

$$p'_{\ell-2} = p'_1 = a_1, \qquad p'_{\ell-1} = p'_2 = a_1a_2 + 1 = a_1^2 + 1,$$
$$q'_{\ell-2} = q'_1 = 1,$$

jer je period simetričan, pa je $a_1 = a_2$*. Stoga koristeći* (1.22) *imamo*

$$a_0 = \frac{m(a_1^2 + 1) + a_1}{2}, \qquad d = a_0^2 + ma_1 + 1.$$

Da bi a_0 *bio cjelobrojan,* a_1 *mora biti paran (pa stavimo* $a_1 = 2a$*) i* m *mora biti paran (stavimo* $m = 2n$*), pa dobijemo:*

$$\sqrt{\big(n(4a^2+1)+a\big)^2 + 4na + 1} = [\, n(4a^2+1) + a, \overline{2a, 2a, 2\big(n(4a^2+1)+a\big)}\,].$$

Primjer 4.5 (Brojevi s duljinom perioda 4)**.** *Krenimo od razvoja* $[\, a_0, \overline{a_1, a_2, a_1, 2a_0}\,]$*. Imamo:*

$$p'_{\ell-2} = p'_2 = a_1a_2 + 1, \qquad p'_{\ell-1} = p'_3 = a_1^2a_2 + 2a_1,$$
$$q'_{\ell-2} = q'_2 = a_2,$$

pa dobijemo:

$$a_0 = \frac{m(a_1^2a_2 + 2a_1) - (a_1a_2 + 1)a_2}{2}.$$

Da bi to bio prirodan broj, a_2 *mora biti paran; ili* a_1 *i* a_2 *neparni, a* m *paran. Tada je:*

$$\sqrt{a_0^2 + m(a_1a_2 + 1) - a_2^2} = [\, a_0, \overline{a_1, a_2, a_1, 2a_0}\,].$$

Dakako da bi mogli nastaviti ovako dalje za $\ell = 5, 6, \ldots$. Izrazi bi bili sve duži, kompliciraniji i ovisili o parnosti sve više brojeva.

U §1.6 smo vidjeli da za svaku duljinu ℓ možemo naći broj d takav da je $\ell\big(\sqrt{d}\big) = \ell$. Vrijedi i više; za svaki ℓ možemo konstruirati niz za koji vrijedi $\ell\big(\sqrt{d(n)}\big) = \ell$ za svaki $n \in \mathbb{N}$.

Primjer 4.6. *Promotrimo detaljnije Primjer 1.43 (2b):*

$$[\,a_0, \overline{1,2,3,2,1,2a_0}\,], \qquad \ell = 6, \qquad \frac{p_4'}{q_4'} = \frac{23}{16}, \qquad \frac{p_5'}{q_5'} = \frac{33}{23},$$

pa imamo $a_0 \equiv 14 \pmod{33}$ *odnosno* $a_0 = 14 + 33n$, $n = 0, 1, 2, \ldots$, *to jest*

$$a_0(n) = 33n - 19, \qquad n \in \mathbb{N}.$$

Sada iz

$$d(n) = a_0(n)^2 + \frac{2 \cdot a_0(n) \cdot 23 + 16}{33}$$

dobijemo

$$\begin{aligned} d(n) &= (33n - 19)^2 + 46n - 26 \\ &= 33^2 n^2 - 1208n + 335. \end{aligned}$$

Imamo npr. $d(1) = 216$, $d(2) = 2275$, $d(3) = 6512$, $d(4) = 12\,927, \ldots$. *Očito je:*

$$\ell\big(\sqrt{d(n)}\big) = 6, \qquad \sqrt{d(n)} = [\,a_0(n), \overline{1,2,3,2,1,2 \cdot a_0(n)}\,].$$

Uočimo da su svi prirodni brojevi koji imaju palindromni dio razvoja u verižni razlomak $(1,2,3,2,1)$ *upravo* $d(n), n \in \mathbb{N}$.

Dakle počevši od jednog broja nekog zadanog perioda, možemo konstruirati beskonačno brojeva koji imaju jednak simetrični dio perioda.

Čini se da je ovakve nizove prvi sustavno u 1960-tima proučavao Schinzel ([39], [40]). U [39] je koristeći

$$\limsup_{n\to\infty} \ell\big(\sqrt{n^2 + h}\big) < \infty \qquad \Longleftrightarrow \qquad h \mid 4n^2$$

i da je svaki kvadratni polinom biracionalno ekvivalentan sa $n^2 + h$ dokazao:

Teorem 4.7. *Neka je* $d(n) = a^2n^2 + bn + c$, *gdje su* $a \neq 0, b, c \in \mathbb{Z}$ *i* $\Delta = b^2 - 4a^2c \neq 0$. *Tada je*

$$\limsup_{n\to\infty} \ell\big(\sqrt{d(n)}\big) < \infty \qquad \Longleftrightarrow \qquad \Delta \mid 4\big(\operatorname{nzd}(2a^2, b)\big)^2.$$

Nadalje, dokazao je i

Teorem 4.8. *Neka je* $d(n) \in \mathbb{Q}[n]$ *polinom s cjelobrojnim vrijednostima kojem je vodeći koeficijent veći od nule. Ako je*

(i) $\deg d$ *neparan, ili*

(ii) vodeći koeficijent od d *nije kvadrat racionalnog broja,*

tada vrijedi:

$$\limsup_{n\to\infty} \ell\big(\sqrt{d(n)}\big) = \infty.$$

I. Kaplansky je nizove brojeva s malom duljinom perioda (kao iz Teorema 4.7) nazvao *sleepers*.

4.1 Polinomijalna Pellova jednadžba

Primjeri nizova brojeva za koje znamo razvoj u verižni razlomak daju rješenja nekih polinomijalnih Pellovih jednadžbi.

Definicija 4.9. *Neka je $D \in \mathbb{Z}[n]$. Jednadžba*

$$X(n)^2 - D(n)Y(n)^2 = 1, \qquad X, Y \in \mathbb{Z}[n] \tag{4.2}$$

se zove polinomijalna Pellova jednadžba.

Za svaki $D \in \mathbb{Z}[n]$, jednadžba očito ima trivijalno rješenje $(1, 0)$, pa ga možemo zanemariti. Međutim, nema svaka polinomijalna Pellova jednadžba netrivijalnih rješenja. Uočimo da (4.2) nema rješenja ako je $\deg D$ neparan, pa pretpostavimo da je paran. Jednadžba nema rješenja ni ako je D potpun kvadrat. Jer za $D = A^2$, imamo $1 = (X + AY)(X - AY)$, pa su jedina rješenja $(X, Y) = (\pm 1, 0)$. Stoga pretpostavimo i da $\sqrt{D}$ nije racionalna funkcija. Ni u tom slučaju rješenja ne postoje uvijek, i ne zna se neki općeniti kriterij rješivosti. Pa ipak, nešto malo se zna.

Lako se vidi da ako je (X, Y) rješenje jednadžbe (4.2), da su onda to i $(X, -Y)$ i $(-X, \pm Y)$, pa ćemo promatrati ono rješenje za koje je $\operatorname{sgn} X > 0, \operatorname{sgn} Y > 0$ (gdje je $\operatorname{sgn} A$ vodeći koeficijent polinoma A).

Nije teško vidjeti da ako je (X_1, Y_1) i (X_2, Y_2) rješenje jednadžbe (4.2) da je onda i $(X_1X_2 + DY_1Y_2, X_1Y_2 + X_2Y_1)$ također rješenje. Stoga ako imamo jedno netrivijalno rješenje, imamo ih beskonačno mnogo.

Vidi se i da ako je (X, Y) rješenje, vrijedi $\deg X = \deg Y + \frac{\deg D}{2}$, pa stupnjem rješenja možemo zvati stupanj polinoma X. Kao i kod obične Pellove jednadžbe, pokaže se da je fundamentalno rješenje (ono s najmanjim pozitivnim stupnjem) jedinstveno (do na predznak) — označimo ga sa $X_1 + Y_1\sqrt{D}$, te da su sva ostala rješenja $(X_1 + Y_1\sqrt{D})^k,\ k \in \mathbb{N}$.

Nathanson [29] je dokazao da u slučaju $D(n) = n^2 + d, d \in \mathbb{Z}$ jednadžba (4.2) ima rješenja ako i samo ako je $d = \pm 1, \pm 2$. Ramasamy [37] je našao nekoliko polinoma drugog stupnja za koje razne pellovske jednadžbe imaju rješenja, a Mc Laughlin [16] je našao rješenja za nekoliko klasa polinoma D što je dosta pogodno za nalaženje fundamentalnih jedinica u određenim klasama realnih kvadratnih polja, dok su Webb i Yokota [46] karakterizirali sve normirane polinome stupnja 2 i 4 za koje jednadžba (4.2) ima rješenja.

Teorem 4.10. *Neka je D normirani polinom parnog stupnja, to jest*

$$D = A^2 + 2C, \quad \deg C < \deg A, \quad A, C \in \mathbb{Q}[x], \tag{4.3}$$

za koji vrijedi

$$\deg C < 2 \ i \ B = A/C \in \mathbb{Q}[x]. \tag{4.4}$$

Tada je razvoj od $\sqrt{D}$ periodan.

Skica dokaza. Dokaz se temelji na tome da je svim normiranim polinomima D oblika (4.3) i (4.4), kada je $A \in \mathbb{Z}[x]$ ili $2A \in \mathbb{Z}[x]$, razvoj u verižni razlomak od $\sqrt{D}$ oblika $\langle\, A, \overline{B, 2A}\,\rangle$ ili $\langle\, A, \overline{2A}\,\rangle$, te da pokazuje da ako je $\deg C < 2$, onda mora biti $A \in \mathbb{Z}[x]$ ili $2A \in \mathbb{Z}[x]$ da bi D bio oblika (4.3). Za više detalja, pogledati [46]. □

Na taj način su dali odgovor na pitanje rješivosti Pellove jednadžbe za sve normirane polinome oblika (4.3) stupnja ≤ 4. Nathansonov rezultat (i svi normirani kvadratni polinomi) su specijalan slučaj njihovih rezultata.

Po njihovim rezultatima, svi tipovi normiranih polinoma D četvrtog stupnja za koje jednadžba (4.2) ima rješenja su ($u, v \in \mathbb{Z}$):

- $d(x) = x^4 + 2ux^3 + (u^2 + 2v)x^2 + 2uvx + v^2 \pm 1$,
- $d(x) = x^4 + 2ux^3 + (u^2 + 2v + 1)x^2 + (2uv + u)x + v^2 + v$,
- $d(x) = x^4 + 2ux^3 + (u^2 + 2v(\pm u - v))x^2 + 2(uv(\pm u - v) \pm 1)x + v^2(\pm u - v)^2 + v$,
- $d(x) = x^4 + 2ux^3 + (u^2 \pm 2v(u \mp v))x^2 + (2u(\pm v(u \mp v)) \pm 1)x + v^2(u \pm v)^2 + v$.

Primjer 4.11. $D(x) = x^4 + 8x^3 + 22x^2 + 25x + 12 = (x^2 + 4x + 3)^2 + 2\frac{x+3}{2}$. *Stoga je fundamentalno rješenje jednadžbe* $X^2 + DY^2 = 1$ *jednako* $(X, Y) = (2(x + 1)^2(x + 3) + 1, 2(x + 1))$. □

U [47] su taj rezultat proširili i na sve polinome $D = A^2 + 2C$, gdje je $pB = pA/C \in \mathbb{Z}[x]$.

Kasnije su se sličnim problemima bavili i drugi matematičari, poput Wiliamsa, Chenga, Goddarda...

Iako proučavanje rješivosti polinomijalnih Pellovih jednadžbi ima smisla samo za sebe, mi ćemo se uglavnom koncentrirati na konstruiranje nizova brojeva kod kojih razvoj u verižni razlomak ima neka interesantna svojstva.

Fiksirajmo $d \in \mathbb{N}, d \neq \square$ i promotrimo jednadžbu:

$$x^2 - dy^2 = 1. \tag{4.5}$$

Njezino fundamentalno rješenje označimo sa (B, A) [1]. Sjetimo se da vrijedi

$$(B, A) = \begin{cases} (p_{2m-1}, q_{2m-1}), & \text{ako je } \ell(\sqrt{d}) = 2m, \\ (p_{4m+1}, q_{4m+1}), & \text{ako je } \ell(\sqrt{d}) = 2m + 1. \end{cases}$$

Nadalje, znamo da jednadžba ima beskonačno mnogo rješenja i sva rješenja su neke konvergente od $\sqrt{d}$. Često ćemo fundamentalno rješenje označavati sa (B_1, A_1), a sva ostala sa (B_k, A_k).

[1] B i A označavaju brojeve, a ne polinome. Velika slova koristimo da ne uvedemo zabunu s parcijalnim kvocijentima, a u sljedećem poglavlju ćemo vidjeti da je upravo odabir slova B i A najzgodniji.

Lema 4.12. *Neka je* $d \neq \square$, $\sqrt{d} = [a_0; \overline{a_1, \cdots, a_n, 2a_0}]$. *Vrijedi:* $p_n = a_0 q_n + q_{n-1}$ $(n = \ell(\sqrt{d}) - 1)$.

Dokaz. Budući je razvoj od $\sqrt{d}$ palindroman, vrijedi:

$$\begin{pmatrix} p'_n & p'_{n-1} \\ q'_n & q'_{n-1} \end{pmatrix} = \begin{pmatrix} p'_n & q'_n \\ p'_{n-1} & q'_{n-1} \end{pmatrix}.$$

Tj. $q'_n = p'_{n-1}$. Iz (1.11) slijedi tvrdnja. □

Lema 4.13. *Ako je* $\ell(\sqrt{d}) = 2m+1$, *tada je* $B = p_{4m+1} = 2p_{2m}^2 + 1$ *i* $A = q_{4m+1} = 2p_{2m}q_{2m}$. *Nadalje,* $p_{2m} = p_m q_m + p_{m-1}q_{m-1}$ *i* $q_{2m} = q_m^2 + q_{m-1}^2$.

Dokaz. Razvoj od $\sqrt{d}$ ima oblik $[\, a_0, \overline{a_1, a_2, \ldots, a_{m-1}, a_m, a_m, a_{m-1}, \ldots, a_1, 2a_0}\,]$. Stoga je:

$$\begin{aligned} \begin{pmatrix} p_{2m} & p_{2m-1} \\ q_{2m} & q_{2m-1} \end{pmatrix} &= \begin{pmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{pmatrix} \begin{pmatrix} p'_m & q'_m \\ p'_{m-1} & q'_{m-1} \end{pmatrix} \\ &= \begin{pmatrix} p_m p'_m + p_{m-1}p'_{m-1} & \cdots \\ q_m p'_m + q_{m-1}p'_{m-1} & \cdots \end{pmatrix}. \end{aligned}$$

Iz (1.11) slijedi druga tvrdnja.

$$\begin{aligned} \begin{pmatrix} p_{4m+1} & p_{4m} \\ q_{4m+1} & q_{4m} \end{pmatrix} &= \begin{pmatrix} p_{2m} & p_{2m-1} \\ q_{2m} & q_{2m-1} \end{pmatrix} \begin{pmatrix} 2a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p'_{2m} & q'_{2m} \\ p'_{2m-1} & q'_{2m-1} \end{pmatrix} \\ &= \begin{pmatrix} p_{2m}(2a_0p'_{2m} + p'_{2m-1}) + p_{2m-1}p'_{2m} & \cdots \\ q_{2m}(2a_0p'_{2m} + p'_{2m-1}) + q_{2m-1}p'_{2m} & \cdots \end{pmatrix} \end{aligned}$$

Iz (1.11) slijedi $p_{4m+1} = p_{2m}(2a_0q_{2m}+q_{2m-1})+p_{2m-1}q_{2m} \overset{\text{(Lema 4.12)}}{=} 2p_{2m}^2 - p_{2m}q_{2m-1} + p_{2m-1}q_{2m} \overset{(1.6)}{=} 2p_{2m}^2 + 1$. Jednako se dobije i $q_{4m+1} = q_{2m}(2a_0q_{2m} + q_{2m-1}) + q_{2m-1}q_{2m} = 2p_{2m}q_{2m}$. □

Teorem 4.14. *Neka je* $\sqrt{d} = [\, a_0, \overline{a_1, \cdots, a_{\ell-1}, 2a_0}\,]$ *i* (B, A) *fundamentalno rješenje jednadžbe* (4.2). *Promotrimo polinom:* $D(n) = A^2n^2 + 2Bn + d$.

(i) Ako je ℓ *neparan,* $\sqrt{D(n)} = [\, An + a_0, \overline{a_1, \cdots, a_{\ell-1}, 2a_0, a_1, \cdots, a_{\ell-1}, 2(An + a_0)}\,]$, *za* $n \in \mathbb{N}$.

(ii) Ako je ℓ *paran,* $\sqrt{D(n)} = [\, An + a_0, \overline{a_1, \cdots, a_{\ell-1}, 2(An + a_0)}\,]$, *za* $n \in \mathbb{N}$.

Stoga je u oba slučaja $X(n) = A^2n + B$, $Y(n) = A$ *fundamentalno rješenje jednadžbe* (4.2).

Dokaz. Lako se provjeri da su ovako definirani X i Y stvarno rješenja. Ostaje utvrditi da su fundamentalna.

(i) ℓ je neparan.

$$[\,An+a_0,a_1,\ldots,a_{\ell-1},2a_0,a_1,\ldots,a_{\ell-1}\,]=[\,An+a_0,a_1,\ldots,a_{\ell-1},a_0+\frac{p_{\ell-1}}{q_{\ell-1}}\,]$$

$$\begin{aligned}
&= An+\frac{\left(a_0+\frac{p_{\ell-1}}{q_{\ell-1}}\right)p_{\ell-1}+p_{\ell-2}}{\left(a_0+\frac{p_{\ell-1}}{q_{\ell-1}}\right)q_{\ell-1}+q_{\ell-2}}\\
&= An+\frac{(a_0q_{\ell-1}+p_{\ell-1})p_{\ell-1}+p_{\ell-2}q_{\ell-1}}{(a_0q_{\ell-1}+p_{\ell-1})q_{\ell-1}+q_{\ell-2}q_{\ell-1}}\\
&= An+\frac{(2p_{\ell-1}-q_{\ell-2})p_{\ell-1}+p_{\ell-2}q_{\ell-1}}{(2p_{\ell-1}-q_{\ell-2})q_{\ell-1}+q_{\ell-2}q_{\ell-1}}\\
&= An+\frac{2p_{\ell-1}^2-1}{2p_{\ell-1}q_{\ell-1}}\\
&= An+\frac{B}{A}\\
&= \frac{A^2n+B}{A}.
\end{aligned}$$

Budući da za sve $a_i, i=1,2,\ldots\ell-1$ vrijedi $a_i<\sqrt{d}$, broj $2(An+a_0)$ je veći od svih elemenata u nizu $[\,a_1,\ldots,a_{\ell-1},2a_0,a_1,\ldots,a_{\ell-1}\,]$, pa period ne može biti kraći od ℓ. A budući je to rješenje jednadžbe (4.2), slijedi tvrdnja.

(ii) ℓ je paran.

$$[\,An+a_0,a_1,\ldots,a_{\ell-1}\,]=An+\frac{p_{\ell-1}}{q_{\ell-1}}=An+\frac{B}{A}=\frac{A^2n+B}{A},$$

pa je sve isto kao u *(i)*.

□

Primjer 4.15. *Promotrimo* $d=21$. $\sqrt{21}=[\,4,\overline{1,1,2,1,1,8}\,]$, $\ell=6$, $(B,A)=(55,12)$ *je fundamentalno rješenje jednadžbe* $x^2-21y^2=1$. *Uzmemo li*

$$D(n)=144n^2+110n+21,$$

imamo:

$$\sqrt{D(n)}=[\,12n+4,\overline{1,1,2,1,1,24n+8}\,].$$

Fundamentalno rješenje jednadžbe $X^2-DY^2=1$ *je* $(X,Y)=(144n+55,12)$. □

Teorem 4.14 nam omogućuje da nađemo fundamentalne jedinice u velikoj klasi realnih kvadratnih polja. Npr. uzevši polinom $D(n)$ iz Primjera 4.15 odmah znamo da je za $n = 1\,000\,000$ (budući je $D(n)$ kvadrano slobodan, te $\equiv 3 \pmod 4$) fundamentalna jedinica u $\mathbb{Q}(\sqrt{144000110000021})$ broj $144000055+12\sqrt{144000110000021}$.

Mc Laughlin je u [16] pokazao da slične stvari vrijede (uz dodatne pretpostavke na d) za još nekoliko klasa polinoma:

- $d(n) = (B-1)^2A^2n^2 + 2(B-1)^2n + d, \quad X = (B-1)A^4n^2 + 2(B-1)A^2n + B, \quad Y = A^3n + A,$
- $d(n) = (B+1)^2A^2n^2 + 2(B+1)^2n + d, \quad X = (B+1)A^4n^2 + 2(B+1)A^2n + B, \quad Y = A^3n + A,$
- $d(n) = (B+1)^2A^2n^2 + 2(B^2-1)n + d, \quad X = \frac{(B+1)^2}{B-1}A^4t^2 + 2(B+1)A^2n + B, \quad Y = \frac{B+1}{B-1}A^3n + A,$
- $d(n) = (B-1)^2A^6n^4 + 4(B-1)^2A^4n^3 + 6(B-1)^2A^2n^2 + 2(B-1)(2B-1)n + d.$

4.2 Konstruiranje nizova brojeva s malom duljinom perioda

Uočimo da svaki od tih slučajeva $d(n)$ daje jedan niz brojeva s malom duljinom perioda. Npr. u Primjeru 4.15 smo vidjeli da počevši od broja $d = 21$ možemo konstruirati niz brojeva kojem svi članovi imaju duljinu perioda 6 i palindromni dio perioda $1, 1, 2, 1, 1$. Koristeći Teorem 4.14 vidimo da primjere nizova s parnom duljinom perioda možemo po volji konstruirati.

S neparnim duljinama možemo postupiti analogno kao i s parnima. Za broj d kojem je duljina perioda ℓ neparna, promotrimo fundamentalno rješenje jednadžbe

$$x^2 - dy^2 = -1. \tag{4.6}$$

Ono se dobije na kraju prvog perioda, te ga označimo sa (B, A). Lako se provjeri da je $X(n) = A^2n + B, Y = A$ rješenje polinomijalne jednadžbe

$$X^2 - DY^2 = -1,$$

a analogno dokazu Teorema 4.14 se provjeri da je ono fundamentalno ($a_\ell(n) = 2(An + a_0)$ je veći od svih brojeva $a_1, \ldots, a_{\ell-1}$). Tako smo dokazali:

Korolar 4.16. *Neka je $d \in \mathbb{N}$, takav da je mu je duljina perioda ℓ neparna, $\sqrt{d} = [\, a_0, \overline{a_1, \cdots, a_{\ell-1}, 2a_0}\,]$, te neka je (B, A) fundamentalno rješenje jednadžbe (4.6). Promotrimo polinom: $D(n) = A^2n^2 + 2Bn + d$. Vrijedi:*

$$\sqrt{D(n)} = [\, An + a_0, \overline{a_1, \cdots, a_{\ell-1}, 2(An + a_0)}\,], \qquad \text{za } n \in \mathbb{N}.$$

Na taj način možemo počevši od proizvoljnog broja d kojem je duljina perioda neparna, konstruirati niz brojeva kojem svi članovi imaju jednaku duljinu i simetrični dio perioda.

Primjer 4.17. *Promotrimo* $d = 13$. $\sqrt{13} = [\,3, \overline{1, 1, 1, 1, 6}\,]$, $\ell = 5$, $(B, A) = (18, 5)$ *je fundamentalno rješenje jednadžbe* $x^2 - 13y^2 = -1$. *Uzmemo li*

$$D(n) = 25n^2 + 36n + 13,$$

imamo:

$$\sqrt{D(n)} = [\,5n + 3, \overline{1, 1, 1, 1, 10n + 6}\,].$$

Fundamentalno rješenje jednadžbe $X^2 - DY^2 = -1$ *je* $(X, Y) = (25n + 18, 10)$. □

Korolar 4.18. *Neka je* $d \in \mathbb{N}, d \neq \square$, *te neka je* $\sqrt{d} = [\,a_0, \overline{a_1, \cdots, a_{\ell-1}, 2a_0}\,]$, *i* $(B, A) = (p_{\ell-1}, q_{\ell-1})$. *Promotrimo polinom:* $D(n) = A^2n^2 + 2Bn + d$. *Vrijedi:*

$$\sqrt{D(n)} = [\,An + a_0, \overline{a_1, \cdots, a_{\ell-1}, 2(An + a_0)}\,], \qquad \text{za } n = 0, 1, 2 \ldots$$

Primjer 4.19. *Uočimo da se na ovaj način dobije isti niz* $d(n)$ *kao i konstrukcijom pokazanom u Primjeru 4.6 (ako* n *umanjimo za jedan). Krenimo od broja* $d = 216$. *Imamo*

$$\sqrt{216} = [\,14, \overline{1, 2, 3, 2, 1, 28}\,], \qquad \ell = 6.$$

$(B, A) = (p_5, q_5) = (485, 33)$, *pa za*

$$D(n) = 33^2n^2 + 2 \cdot 485n + 216$$

imamo:

$$\sqrt{D(n)} = [\,33n + 14, \overline{1, 2, 3, 2, 1, 2(33n + 14)}\,].$$

A lako se vidi i da vrijedi $d(n) = D(n - 1)$. □

Poglavlje 5

Nizovi brojeva s velikom duljinom perioda (creepers)

Iako se dugo smatralo da je Shanks [41] prvi otkrio nizove prirodnih brojeva kojima duljina perioda verižnog razlomka teži u beskonačnost, prije nekoliko godina je ustanovljeno da ih je ipak prvi otkrio norveški matematičar Nyberg [30]. Budući je članak pisan na Norveškom, nije baš bio zapažen. On je otkrio da ako je m neparan i $m \geq 3$, duljina perioda u nizu:

$$d_m(n) = \left(m^n \pm \frac{m-1}{2}\right)^2 + m, \quad n \in \mathbb{N}$$

teži u beskonačnost.

U ovom poglavlju ćemo uglavnom promatrati nizove brojeva reda veličine $\ln(d(n)) = \mathcal{O}(n)$ za koje je $\ell\big(\sqrt{d(n)}\big) = \mathcal{O}(n)$. Takvi nizovi su nazvani *creepers*.

Za razliku od sleepersa, o kojima se dosta zna, i koje je Schnitzel dobro karakterizirao, za creeperse to nije slučaj. O njima se ne zna nikakav opći rezultat ili karakterizacija. Jedino je poznato više familija takvih nizova.

5.1 Nybergov niz

Teorem 5.1. *Neka je m neparan broj veći ili jednak od 3. Tada za*

$$d_m(n) = \left(m^n - \frac{m-1}{2}\right)^2 + m, \quad n \in \mathbb{N}$$

vrijedi:

$$\ell\big(\sqrt{d_m(n)}\big) = 6n - 2$$

i

$$\sqrt{d_m(n)} = \Bigg[m^n - \frac{m-1}{2}, \overline{2m^{n-1}-1, m-1, 1,\ 2m^{n-2}-1, m^2-1, 1,\ \ldots,} \\ \overline{1,\ 1, m^n - \frac{m+1}{2}, 1,\ 1, \ldots\ , 2m^{n-1}-1,\ 2m^n-(m-1)} \Bigg].$$

Dokaz. Imamo $a_0 = \lfloor \sqrt{d_m(n)} \rfloor = m^n - \frac{m-1}{2}$, i uz $s_0 = 0, t_0 = 1$ slijedimo postupak (1.12).

$$s_1 = m^n - \frac{m-1}{2}, \qquad t_1 = m, \qquad a_1 = \Big\lfloor \frac{2m^n - m + 1}{m} \Big\rfloor = 2m^{n-1} - 1,$$

$$s_2 = m^n - \frac{m+1}{2}, \qquad t_2 = 2m^{n-1}, \qquad a_2 = \Big\lfloor m - \frac{m^{2-n}}{2} \Big\rfloor.$$

Ako je $n = 1$, imamo $a_2 = \lfloor m - \frac{m}{2} \rfloor = m - \frac{m+1}{2}$. Nadalje, dobijemo $s_3 = \frac{m+1}{2} - m^{n-1}$. Vidimo da vrijedi $s_2 = s_3$, pa po Napomeni 1.35 zaključujemo da je $\ell = 4$.

Za $n > 1$ imamo $a_2 = m - 1$, pa imamo:

$$s_3 = m^n - 2m^{n-1} + \frac{m+1}{2}, \qquad t_3 = (2m^{n-1} - m)(m-1) + 1,$$
$$a_3 = \Big\lfloor 1 + \frac{m(m-1)}{(2m^{n-1} - m)(m-1) + 1} \Big\rfloor = 1,$$

$$s_4 = m^n - m^2 + \frac{m+1}{2}, \qquad t_4 = m^2,$$
$$a_4 = \Big\lfloor 2m^{n-2} - 1 + \frac{1}{m^2} \Big\rfloor = 2m^{n-2} - 1,$$

$$s_5 = m^n - \frac{m+1}{2}, \qquad t_5 = 2m^{n-2},$$
$$a_5 = \Big\lfloor m^2 - \frac{m^{3-n}}{2} \Big\rfloor.$$

Ako je $n = 2$, imamo $a_5 = m^2 - \frac{m+1}{2}$. Nadalje, dobijemo $s_6 = m^n - m^{n-1} - m^{n-2} + \frac{m+1}{2}$. Vidimo da vrijedi $s_5 = s_6$, pa po Napomeni 1.35 zaključujemo da je $\ell = 10$. Za $n > 2$ imamo $a_5 = m^2 - 1$.

Indukcijom se lako pokaže da za $k = 0, 1, 2, \ldots, n-2$ vrijedi

$$s_{3k+1} = m^n - m^{k+1} + \frac{m+1}{2}, \qquad t_{3k+1} = m^{k+1},$$
$$a_{3k+1} = 2m^{n-k-1} - 1,$$

$$s_{3k+2} = m^n - \frac{m+1}{2}, \qquad t_{3k+2} = 2m^{n-k-1},$$

$$a_{3k+2} = 2m^{k+1} - 1,$$

$$s_{3k+3} = m^n - 2m^{n-k-1} + \frac{m+1}{2}, \quad t_{3k+3} = (2m^{n-k-1} - m)(m^{k+1} - 1) + 1,$$
$$a_{3k+3} = 1.$$

Za $k = n - 1$ imamo

$$s_{3k+2} = m^n - \frac{m+1}{2}, \qquad t_{3k+2} = 2, \qquad a_{3k+2} = m^n - \frac{m+1}{2},$$

$$s_{3k+3} = m^n - \frac{m+1}{2},$$

pa vidimo da vrijedi $s_{3k+2} = s_{3k+3}$, te ponovo zaključujemo da je $\ell = 2(3k+2) = 2(3n-1)$. Što je i trebalo dokazati. □

Primjer 5.2. *Promotrimo razvoj broja $d_5(4)$:*

$$\sqrt{d_5(4)} = \sqrt{388\,134} = \big[\,623, \overline{249, 4, 1,\ 49, 24, 1,\ 9, 124,} \\ \overline{1,\ 1, 622, 1,\ 1, 124, 9,\ 1, 24, 49,\ 1, 4, 249,\ 1246}\,\big].$$

Teorem 5.3. *Neka je m neparan broj veći ili jednak od 3. Tada za*

$$d_m(n) = \left(m^n + \frac{m-1}{2}\right)^2 + m, \quad n \in \mathbb{N}$$

vrijedi:

$$\ell\big(\sqrt{d_m(n)}\big) = 6n$$

i

$$\sqrt{d_m(n)} = \left[\, m^n + \frac{m-1}{2}, \overline{2m^{n-1}, 1,\ 2m^{n-2} - 1, 1, m^2 - 1,\ \ldots,} \right. \\ \left. \overline{1,\ 1, m^n + \frac{m-1}{2} - 1, 1,\ 1, \ldots\ , 2m^{n-1},\ 2m^n + m - 1} \,\right].$$

Dokaz. Imamo: $a_0 = \lfloor \sqrt{d_m(n)} \rfloor = m^n + \frac{m-1}{2}$, i slijedimo postupak (1.12). Imamo $s_0 = 0, t_0 = 1$ i

$$s_1 = m^n + \frac{m-1}{2}, \qquad t_1 = m,$$
$$a_1 = \left\lfloor \frac{2m^n + m - 1}{m} \right\rfloor = 2m^{n-1},$$

$$s_2 = m^n - \frac{m-1}{2}, \qquad t_2 = (2m^{n-1}-1)(m-1)+m,$$
$$a_2 = \left\lfloor 1 + \frac{1}{m-1+\frac{m}{2m^{n-1}-1}} \right\rfloor = 1,$$

$$s_3 = m^n - 2m^{n-1} + \frac{m+1}{2}, \qquad t_3 = 2m^{n-1},$$
$$a_3 = \left\lfloor m-1+\frac{m^{2-n}}{2} \right\rfloor.$$

Ako je $n = 1$, imamo $a_3 = m - 1 + \left\lfloor \frac{m}{2} \right\rfloor = m + \frac{m-3}{2}$. Nadalje, dobijemo $s_4 = 2m^n - m^{n-1} - \frac{m+1}{2}$. Vidimo da vrijedi $s_3 = s_4$, pa po Napomeni 1.35 zaključujemo da je $\ell = 6$.

Za $n > 1$ je $a_3 = m - 1$, pa imamo:

$$s_4 = m^n - \frac{m+1}{2}, \qquad t_4 = m^2,$$
$$a_4 = \left\lfloor \frac{2m^n-1}{m^2} \right\rfloor = 2m^{n-2}-1,$$

$$s_5 = m^n - m^2 + \frac{m+1}{2}, \qquad t_5 = (2m^{n-2}-1)(m^2-1)+m,$$
$$a_5 = \left\lfloor 1 + \frac{1}{m^2-1+\frac{m}{2m^{n-2}-1}} \right\rfloor = 1,$$

$$s_6 = m^n - 2m^{n-2} + \frac{m+1}{2}, \qquad t_6 = 2m^{n-2},$$
$$a_6 = \left\lfloor m^2-1+\frac{m^{3-n}}{2} \right\rfloor.$$

Ako je $n = 2$, imamo $a_6 = m^2 + \frac{m-3}{2}$. Nadalje, dobijemo $s_7 = m^n + m^{n-1} - m^{n-2} - \frac{m+1}{2}$. Vidimo da vrijedi $s_6 = s_7$, pa po Napomeni 1.35 zaključujemo da je $\ell = 12$. Za $n > 2$ imamo $a_6 = m^2 - 1$.

Indukcijom se lako pokaže da za $k = 1, 2, 3 \ldots, n-2$ vrijedi

$$s_{3k+1} = m^n - \frac{m+1}{2}, \qquad t_{3k+1} = m^{k+1},$$
$$a_{3k+1} = 2m^{n-k-1} - 1,$$

$$s_{3k+2} = m^n - m^{k+1} + \frac{m+1}{2}, \qquad t_{3k+2} = (2m^{n-k-1}-1)(m^{k+1}-1)+m,$$
$$a_{3k+2} = 1,$$

$$s_{3k+3} = m^n - 2m^{n-k-1} + \frac{m+1}{2}, \qquad t_{3k+3} = 2m^{n-k-1},$$

$$a_{3k+3} = m^{k+1} - 1.$$

Za $k = n - 1$ imamo

$$s_{3k+3} = m^n - 2 + \frac{m+1}{2}, \qquad t_{3k+3} = 2, \qquad a_{3k+3} = m^n - \frac{m-3}{2},$$

$$s_{3k+4} = m^n - 2 + \frac{m+1}{2},$$

pa vidimo da vrijedi $s_{3k+3} = s_{3k+4}$, te je ponovo $\ell = 2(3k+3) = 2 \cdot 3n$, što je i trebalo dokazati. □

Primjer 5.4. *Promotrimo razvoj broja $d_7(4)$:*

$$\sqrt{d_7(4)} = \sqrt{5\,779\,223} = \big[2404, \overline{686, 1, 6,\ \ 97, 1, 48,\ \ 13, 1, 342,}\ \overline{1, 1, 2403, 1, 1,\ \ 342, 1, 13,\ \ 48, 1, 97,\ \ 6, 1, 686,\ \ 4808}\big].$$

5.2 Neki nizovi brojeva s velikom duljinom perioda

Tijekom sedamdesetih godina prošlog stoljeća više je matematičara (L. Bernstein, M.D. Hendy, Y. Yamamoto) otkrilo neke nizove brojeva s velikom duljinom perioda. U cijelom ovom odlomku nam je $n \in \mathbb{N}$.

Williams [48] je sustavnije odredio duljinu perioda od $\sqrt{d}$ kada je d oblika:

$$d = (qA^n + \epsilon k)^2 + 2^i \eta A^n \qquad (d > 2, A > 1),$$

gdje je $A = 2^{2-i}qk + \epsilon\eta, |\epsilon| = |\eta| = 1, i = 0, 1, 2$. Na primjer, ako je $d = 3^{2n} - 3^n + 1$ ($\epsilon = -1, \eta = 1, q = k = 1, i = 0$), tada je $\ell\big(\sqrt{d}\big) = 3n + 1$.

Teorem 5.5. *Neka je $d_n = (qA^n - k)^2 + A^n$, gdje je $A = 4qk - 1$. Tada je*

$$\ell\big(\sqrt{d}\big) = 3n + 1.$$

Dokaz. Iz postupka (1.12), uz $t_{-1} = \frac{d - s_0^2}{t_0}$, imamo $t_i t_{i+1} = d - s_{i+1}^2$ i $t_{i-1}t_i = d - s_i^2$. Iz tih jednakosti dobivamo $t_i t_{i+1} + s_{i+1}^2 = t_{i-1}t_i + s_i^2$, odnosno

$$t_i(t_{i+1} - t_{i-1}) = (s_{i+1} + s_i)(s_i - s_{i+1}).$$

Iz $s_{i+1} + s_i = a_i t_i$ slijedi

$$t_{i+1} = t_{i-1} - a_i(s_{i+1} - s_i). \tag{5.1}$$

Ako za neki i dobijemo

$$s_i = qA^n - A^m + k, \qquad t_i = A^m, \qquad a_i = 2qA^{n-m} - 1,$$

tada se koristeći postupak (1.12) i (5.1), lako vidi da je

$$\begin{aligned} s_{i+1} &= qA^n - k, & t_{i+1} &= A^{n-m}, \\ a_{i+1} &= 2qA^m - 1, \\ s_{i+2} &= qA^n - A^{n-m} + k, & t_{i+2} &= 2qA^n - A^{m+1} - A^{n-m} + 2k, \\ a_{i+2} &= 1, \\ s_{i+3} &= qA^n - A^{m+1} + k, & t_{i+3} &= A^{m+1}, \\ a_{i+3} &= 2qA^{n-m-1} - 1. \end{aligned}$$

Sada, budući je $a_0 = s_1 = qA^n - k$, $t_1 = A^n$, $a_1 = 2q - 1$, indukcijom dobijemo:

$$\begin{aligned} s_{3m+1} &= qA^n - k, & t_{3m+1} &= A^{n-m}, \\ a_{3m+1} &= 2qA^m - 1, \\ s_{3m+2} &= qA^n - A^{n-m} + k, & t_{3m+2} &= 2qA^n - A^{m+1} - A^{n-m} + 2k, \\ a_{3m+2} &= 1, \\ s_{3m+3} &= qA^n - A^{m+1} + k, & t_{3m+3} &= A^{m+1}, \\ a_{3m+3} &= 2qA^{n-m-1} - 1. \end{aligned}$$

Budući da kada je $m = n$, za $i = 3m + 1$ imamo $t_i = 1$, i da je to najmanji broj s tim svojstvom, imamo $\ell\left(\sqrt{d_n}\right) = 3n + 1$. □

U istom članku je pokazano i da za $d_n = (qA^n - k)^2 - A^n$, uz $A = 4ak + 1$, vrijedi: ako je $q > 1$, onda je $\ell\left(\sqrt{d_n}\right) = 4n + 2$, dok ako je $q = 1$, imamo $\ell\left(\sqrt{d_n}\right) = 4n - 2$. Dani su i još mnogi drugi primjeri:

d	Dodatni uvjeti	$\ell\left(\sqrt{d}\right)$
$(qA^n + k)^2 + A^n,\ A = 4qk + 1$		$2n + 1$
$(qA^n - k)^2 + A^n,\ A = 4qk - 1$		$3n + 1$
$(qA^n + k)^2 - A^n,\ A = 4qk - 1$		$3n + 2$
$(qA^n - k)^2 - A^n,\ A = 4qk + 1$	$q = 1$	$4n - 2$
	$q > 1$	$4n + 2$
$(qA^n - k)^2 + 2A^n,\ A = 2qk + 1$		$4n + 2$
$(qA^n - k)^2 + 2A^n,\ A = 2qk - 1$	$q = 1$	$6n - 2$
	$q > 1$	$6n + 2$
$(qA^n + k)^2 - 2A^n,\ A = 2qk - 1$	$q = 1$	$6n$
	$q > 1$	$6n + 4$
$(qA^n - k)^2 - 2A^n,\ A = 2qk + 1$	$q = 1$	$8n - 4$
	$q = 2$	$8n$
	$q > 2$	$8n + 4$

Kada je $d = (qA^n - k)^2 + 4A^n,\ A = qk - 1$ imamo:

q	k	n	$\ell(\sqrt{d})$
$q = 1$	$k = 3$	$n \geq 2$	$5n - 9$
$q = 1$	$2 \nmid k,\ k > 3$	$n \geq 2$	$5n - 5$
$q = 1$	$k = 2$	$n \equiv 1 \pmod 3,\ n > 2$	$\frac{11(n-1)}{3}$
$q = 1$	$k = 2$	$n \not\equiv 1 \pmod 3,\ n \geq 2$	$11(n - 1)$
$q = 1$	$2 \mid k,\ k > 2$	$n \equiv 1 \pmod 3,\ n > 2$	$\frac{11(n-1)}{3}$
$q = 1$	$2 \mid k,\ k > 2$	$n \not\equiv 1 \pmod 3,\ n \geq 2$	$11(n - 7)$
$q = 2$	$2 \mid k$		$6n - 2$
$q = 2$	$2 \nmid k$		$11n - 3$
$q > 2,\ 2 \nmid q$	$2 \nmid k$		$5n - 1$
$q = 3$	$2 \mid k$	$n \equiv 1 \pmod 3$	$\frac{11n+1}{3}$
$q = 3$	$2 \mid k$	$n \not\equiv 1 \pmod 3$	$11n + 1$
$q > 3,\ 2 \nmid q$	$2 \mid k$	$n \equiv 1 \pmod 3$	$\frac{11n+1}{3}$
$q > 3,\ 2 \nmid q$	$2 \mid k$	$n \not\equiv 1 \pmod 3$	$11n + 5$
$2 \mid q,\ q > 2$	$2 \mid k$		$6n + 2$
$2 \mid q,\ q > 2$	$2 \nmid k$		$11n + 5$

Kada je $d = (qA^n + k)^2 + 4A^n,\ A = qk + 1$ imamo:

q	k	n	$\ell(\sqrt{d})$
$q = 1$	$k = 1$	$n \geq 2$	$6n - 9$
$q = 1$	$k > 1,\ 2 \nmid k$	$n \geq 4$	$4n - 5$
$q = 1$	$2 \mid k$	$n \equiv 1 \pmod 3$	$\frac{10n-7}{3}$
$q = 1$	$2 \mid k$	$n \not\equiv 1 \pmod 3$	$10n - 3$
$2 \mid q$	$2 \mid k$		$4n + 2$
$q = 2$	$2 \nmid k$		$10n + 1$
$2 \mid q,\ q > 2$	$2 \nmid k$		$10n + 5$
$2 \nmid q,\ q > 1$	$2 \nmid k$		$6n - 1$
$2 \nmid q,\ q > 1$	$2 \mid k$	$n \equiv 1 \pmod 3$	$\frac{10n+5}{3}$
$2 \nmid q,\ q > 1$	$2 \mid k$	$n \not\equiv 1 \pmod 3$	$10n + 5$

Kada je $d = (qA^n + k)^2 - 4A^n,\ A = qk - 1$ imamo:

q	k	n	$\ell(\sqrt{d})$
$q = 1$	$k = 3$	$n \geq 3$	$5(n-2)$
$q = 1$	$2 \nmid k,\ k > 3$	$n \geq 2$	$5n - 6$
$q = 1$	$k = 2$	$n \equiv 1 \pmod 3,\ n > 2$	$\frac{11n-14)}{3}$
$q = 1$	$k = 2$	$n \not\equiv 1 \pmod 3,\ n \geq 3$	$11n - 10$
$q = 1$	$2 \mid k,\ k > 2$	$n \equiv 1 \pmod 3,\ n > 2$	$\frac{11n-14}{3}$
$q = 1$	$2 \mid k,\ k > 2$	$n \not\equiv 1 \pmod 3,\ n \geq 2$	$11n - 6$
$q = 2$	$2 \mid k$		$6n$
$q = 2$	$2 \nmid k$		$11n - 2$
$q > 2,\ 2 \mid q$	$2 \mid k$		$6n + 4$
$q > 2,\ 2 \mid q$	$2 \nmid k$		$11n + 6$
$q = 3$	$2 \mid k$	$n \equiv 1 \pmod 3$	$\frac{11n-2}{3}$
$q = 3$	$2 \mid k$	$n \not\equiv 1 \pmod 3$	$11n + 2$
$q > 3,\ 2 \nmid q$	$2 \mid k$	$n \equiv 1 \pmod 3$	$\frac{11n+10}{3}$
$q > 3,\ 2 \nmid q$	$2 \mid k$	$n \not\equiv 1 \pmod 3$	$11n + 6$
$q = 3$	$2 \nmid k$		$5n - 2$
$2 \mid q,\ q > 2$	$2 \nmid k$		$5n + 2$

Kada je $d = (qA^n - k)^2 - 4A^n,\ A = qk + 1$ imamo:

q	k	n	$\ell(\sqrt{d})$
$q = 1$	$k = 1$	$n \geq 4$	$4n - 6$
$q = 1$	$2 \nmid k,\ k > 1$	$n \geq 2$	$4n - 2$
$q = 1$	$k = 2$	$n \equiv 1 \pmod 3,\ n \geq 4$	$4n - 2$
$q = 1$	$k = 2$	$n \not\equiv 1 \pmod 3,\ n \geq 3$	$12n - 14$
$q = 1$	$2 \mid k,\ k > 2$	$n \equiv 1 \pmod 3,\ n \geq 4$	$4n - 2$
$q = 1$	$2 \mid k,\ k > 2$	$n \not\equiv 1 \pmod 3,\ n \geq 3$	$12n - 6$
$q = 2$	$2 \mid k$		$8n$
$q = 2$	$2 \nmid k$	$n \geq 2$	$12n - 2$
$q = 3$	$2 \nmid k$		$4n - 2$
$q = 3$	$2 \mid k$	$n \equiv 1 \pmod 3$	$4n - 2$
$q = 3$	$2 \mid k$	$n \not\equiv 1 \pmod 3$	$12n - 2$
$q = 4$	$2 \mid k$		$8n$
$q = 4$	$2 \nmid k$		$12n + 2$

$q > 4,\ 2 \mid q$	$2 \mid k$		$8n + 4$
$q > 4,\ 2 \mid q$	$2 \nmid k$		$12n + 6$
$q > 4,\ 2 \nmid q$	$2 \nmid k$		$4n + 2$
$q > 4,\ 2 \nmid q$	$2 \nmid k$	$n \equiv 1 \pmod 3$	$4n + 2$
$q > 4,\ 2 \nmid q$	$2 \nmid k$	$n \not\equiv 1 \pmod 3$	$12n + 6$

Halter-Koch [11] je te primjere proširio brojevima oblika

$$d = (lp^k q + \lambda c)^2 + 4\mu p^k q, \quad \text{gdje su} \quad \begin{array}{c} k \geq 2, \quad l, c, q \geq 1, \quad q \mid c, \\ \lambda, \mu \in \{\pm 1\}, \quad p = cl + \lambda\mu \geq 2, \end{array} \tag{5.2}$$

kada je $d \equiv 1 \pmod 4$.

(λ, μ)	$d \equiv 1 \pmod 4$	$\ell\left(\frac{1+\sqrt{d}}{2}\right)$
$(1, 1)$	$q = 1$	$2k + 1$
	$q > 1$	$4k + 2$
$(-1, -1)$	$lcq = 1, k \geq 4$	$4k - 6$
	$q = 1, l \leq 2, lc > 1,$ i $k \geq 3$ ako je $(l, c) = (1, 2)$	$4k - 2$
	$q = 1, l \geq 3$	$4k + 2$
	$q > 1, l \leq 2$	$8k$
	$q > 1, l \geq 3$	$8k + 4$
$(1, -1)$	$lq = 1$	$3k - 2$
	$l > 1, q = 1$	$3k + 2$
	$l = 1, q > 1$	$6k$
	$l > 1, q > 1$	$6k + 4$
$(-1, 1)$	$lq = 1$	$3k - 3$
	$l > 1, q = 1$	$3k + 1$
	$l = 1, q > 1$	$6k + 2$
	$l > 1, q > 1$	$6k + 4$

Teorem 5.6. *Neka je* $d = (lp^k q + c)^2 + 4p^k q \equiv 1 \pmod 4$, $q \mid c, p = cl + 1$. *Tada je*

$$\ell\left(\frac{1+\sqrt{d}}{2}\right) = \begin{cases} 2k + 1, & za\ q = 1, \\ 4k + 2, & za\ q > 1. \end{cases}$$

Dokaz. d je oblika (5.2) uz $\mu = \lambda = 1$, $d \equiv 1 \pmod 4$, $\alpha = \frac{1+\sqrt{d}}{2}$. Tada imamo:

$$\lfloor \sqrt{d} \rfloor = \begin{cases} lp^k q + c + 1, & \text{za } l = 1, \\ lp^k q + c, & \text{za } l > 1, \end{cases}$$

$$s_0 = t_0 = 1, \qquad a_0 = \frac{lp^k q + c + 1}{2}.$$

Za $0 \leq i \leq k-1$ dobijemo:

$$\begin{aligned} s_{2i+1} &= lp^k q + c, & t_{2i+1} &= p^{k-i} q, & a_{2i+1} &= lp^i, \\ s_{2i+2} &= lp^k q - c, & t_{2i+2} &= p^{i+1}, & a_{2i+2} &= lp^{k-i-1} q, \end{aligned}$$

i za $i = k$ imamo

$$s_{2k+1} = lp^k q + c, \qquad t_{2k+1} = q, \qquad a_{2k+1} = lp^k + \left\lfloor \frac{c}{q} \right\rfloor.$$

Ako je $q = 1$ imamo $t_{2k+1} = 1$, a ako je $1 < q \mid c$ imamo $s_{2k+1} = s_{2k+2}$, pa slijedi tvrdnja teorema. □

Teorem 5.7. *Neka je* $d = (lp^k q - c)^2 - 4p^k q \equiv 1 \pmod 4$, $q \mid c, p = cl + 1$. *Tada je*

$$\ell\left(\frac{1+\sqrt{d}}{2}\right) = \begin{cases} 4k-6 & \text{za } lcq = 1, k \geq 4, \\ 4k-2 & \text{za } q = 1, l \leq 2, lc > 1, \text{ i } k \geq 3 \text{ ako je } (l,c) = (1,2), \\ 4k+2 & \text{za } q = 1, l \geq 3, \\ 8k & \text{za } q > 1, l \leq 2, \\ 8k+4 & \text{za } q > 1, l \geq 3. \end{cases}$$

Dokaz. d je oblika (5.2) uz $\mu = \lambda = -1$, $d \equiv 1 \pmod 4$, $\alpha = \frac{1+\sqrt{d}}{2}$. Neka je $k \geq 4$ ako je $lcq = 1$; i $k \geq 3$ ako je $l = 1, c = 1$. Tada imamo:

$$\lfloor \sqrt{d} \rfloor = \begin{cases} lp^k q - c - 3, & \text{za } l = 1, \\ lp^k q - c - 2, & \text{za } l = 2, \\ lp^k q - c - 1, & \text{za } l \geq 3, \end{cases}$$

$$s_0 = t_0 = 1, \qquad a_0 = \frac{lp^k q - c - 1}{2}.$$

Ako je $l \geq 3$ imamo $a_0 = \frac{lp^k q - c - 1}{2}$, pa stavimo $\delta = 2, i_0 = 0, k' = k - 1$.
Ako je $l = 2$ imamo $a_0 = \frac{2p^k q - c - 1}{2}$,

$$\begin{aligned} s_1 &= 2p^k q - c - 2, & t_1 &= p^k q - c - 1, & a_1 &= 2, \\ s_2 &= 2p^k q - 3c - 2, & t_2 &= p, & a_2 &= 2p^{k-1} q - 2, \end{aligned}$$

pa stavimo $\delta = 0, i_0 = 1$ i

$$k' = \begin{cases} k-1, & \text{za } q \geq 2, \\ k-2, & \text{za } q = 1. \end{cases}$$

Ako je $l = 1$ imamo $a_0 = \frac{2p^k q - c - 3}{2}$,

$$\begin{aligned} s_1 &= p^k q - c - 4, & t_1 &= p^k q - 2c - 4, & a_1 &= 1, \\ s_2 &= p^k q - 3c - 4, & t_2 &= p, & a_2 &= p^{k-1} q - 3, \end{aligned}$$

ako je još $c \geq 2$ stavimo $\delta = 0, i_0 = 1$ i

$$k' = \begin{cases} k-1, & \text{za } q \geq 3, \\ k-2, & \text{za } q \leq 2, \end{cases}$$

a ako je $c = 1$, pa i $p = 2, q = 1$ i $k \geq 4$

$$\begin{aligned} s_3 &= 2^k - 5, & t_3 &= 2^{k-1} - 3, & a_3 &= 2, \\ s_4 &= 2^k - 7, & t_4 &= 4, & a_4 &= 2^{k-2} - 2, \end{aligned}$$

pa stavimo $\delta = -2, i_0 = 2, k' = k - 3$.

Za $i_0 \leq i \leq k'$ dobijemo:

$$\begin{aligned} s_{4i-1+\delta} &= lp^k q - 2p^i - c, & t_{4i-1+\delta} &= lp^k q - p^{k-i} q - p^i - c, & a_{4i-1+\delta} &= 1, \\ s_{4i+\delta} &= lp^k q - 2p^{k-i} q - c, & t_{4i+\delta} &= p^{k-i} q, & a_{4i+\delta} &= lp^i - 2, \\ s_{4i+1+\delta} &= lp^k q - 2p^{k-i} q + c, & t_{4i+1+\delta} &= lp^k q - p^{k-i} q - p^{i+1} + c, & a_{4i+1+\delta} &= 1, \\ s_{4i+2+\delta} &= lp^k q - 2p^{i+1} + c, & t_{4i+2+\delta} &= p^{i+1}, & a_{4i+2+\delta} &= lp^{k-i-1} q - 2. \end{aligned}$$

Sada još samo trebamo promotriti nekoliko različitih slučajeva:

a) $clq = 1$. Imamo:

$$\begin{aligned} s_{4k-11} &= 2^{k-1} - 1, & t_{4k-11} &= 3 \cdot 2^{k-2} - 5, & a_{4k-11} &= 1, \\ s_{4k-10} &= 2^k - 9, & t_{4k-10} &= 4, & a_{4k-10} &= 2^{k-2} - 2, \\ s_{4k-9} &= 2^k - 7, & t_{4k-9} &= 2^{k-1} - 3, & a_{4k-9} &= 2, \\ s_{4k-8} &= 2^k - 5, & t_{4k-8} &= 2, & a_{4k-8} &= 2^{k-1} - 3, \\ s_{4k-7} &= 2^k - 7, & t_{4k-7} &= 2^k - 6, & a_{4k-7} &= 1, \\ s_{4k-6} &= 2^k - 5, & t_{4k-6} &= 1, & & \end{aligned}$$

pa vidimo da je $\ell(\alpha) = 4k - 6$.

b) $lq \leq 2, p \geq 3$. Imamo:

$$\begin{aligned} s_{4k-5} &= lp^k q - 2p^{k-1} - c, & t_{4k-5} &= lp^k q - p^{k-1} - pq - c, & a_{4k-5} &= 1, \\ s_{4k-4} &= lp^k q - 2pq - c, & t_{4k-4} &= pq, & a_{4k-4} &= lp^{k-1} + lq - 4. \end{aligned}$$

Kada $d \equiv 1 \pmod 4$ je $lq = 1$ ili $lq = 2, c \equiv 1 \pmod 2$ i kada $q \mid c$ je $l = 2, q = 1$.

b') $lq = 1, p \geq 3$. Imamo:

$$s_{4k-3} = p^k - 3p - 1, \qquad t_{4k-3} = p^k - 2p - 2, \qquad a_{4k-3} = 1,$$
$$s_{4k-2} = p^k - p - 3, \qquad t_{4k-2} = 1.$$

b") $l = 2, q = 1$. Imamo:

$$s_{4k-3} = 2p^k - 2p + c, \qquad t_{4k-3} = p^k - p + c, \qquad a_{4k-3} = 2,$$
$$s_{4k-2} = 2p^k - 2p + 3c, \qquad t_{4k-2} = 1.$$

c) $lq \geq 3$. Imamo:

$$s_{4k-1+\delta} = lp^k q - 2p^k - c, \quad t_{4k-1+\delta} = lp^k q - p^k - q - c, \quad a_{4k-1+\delta} = 1,$$
$$s_{4k+\delta} = lp^k q - 2q - c, \qquad t_{4k+\delta} = q, \qquad a_{4k+\delta} = lp^k - 2 - \left\lfloor \frac{c}{q} \right\rfloor.$$

Ako je $q = 1$, imamo $t_{4k+\delta} = 1$, a ako je $q > 1$ i $q \mid c$, imamo $s_{4k+\delta} = s_{4k+1+\delta}$, pa tvrdnja teorema slijedi i u ovom slučaju.

□

Teorem 5.8. *Neka je* $d = (lp^k q + c)^2 - 4p^k q \equiv 1 \pmod 4$, $q \mid c, p = cl - 1$. *Tada je*

$$\ell\left(\frac{1+\sqrt{d}}{2}\right) = \begin{cases} 3k-2 & za\ lq = 1, \\ 3k+2 & za\ l > 1, q = 1, \\ 6k & za\ l = 1, q > 1, \\ 6k+4 & za\ l > 1, q > 1. \end{cases}$$

Dokaz. d je oblika (5.2) uz $\mu = 1, \lambda = -1$, $d \equiv 1 \pmod 4$, $\alpha = \frac{1+\sqrt{d}}{2}$. Imamo:

$$\lfloor \sqrt{d} \rfloor = \begin{cases} lp^k q + c - 1, & \text{za } l \geq 2, \\ lp^k q + c - 2, & \text{za } l = 1, \end{cases}$$

$$s_0 = t_0 = 1, \qquad a_0 = \frac{lp^k q + c - 1}{2}.$$

Ako je $l = 1$ imamo

$$s_1 = p^k q + p - 1, \qquad t_1 = p, \qquad a_1 = p^{k-1} q,$$

pa stavimo $\delta = -2, i_0 = 1$.

Ako je $l \geq 2$ stavimo $i_0 = \delta = 0$.

U oba slučaja stavimo

$$k' = \begin{cases} k-2, & \text{za } lq = 1, \\ k-1, & \text{za } lq > 1, \end{cases}$$

pa za $i_0 \le i \le k'$ dobijemo:

$$\begin{aligned}
&s_{3i+1+\delta} = lp^k q - 2p^i + c, && t_{3i+1+\delta} = lp^k q - p^{k-i}q - p^i + c, && a_{3i+1+\delta} = 1,\\
&s_{3i+2+\delta} = lp^k q - 2p^{k-i}q + c, && t_{3i+2+\delta} = p^{k-i}q, && a_{3i+2+\delta} = lp^i - 1.\\
&s_{3i+3+\delta} = lp^k q - c, && t_{3i+3+\delta} = p^{i+1}, && a_{3i+3+\delta} = lp^{k-i-1}q - 1.
\end{aligned}$$

Sada još samo trebamo promotriti dva različita slučaja:

a) $lq = 1$. Imamo:

$$\begin{aligned}
&s_{3k-4} = p^k - 2p^{k-1} + p + 1, && t_{3k-4} = p^k - p^{k-1} + 1, && a_{3k-4} = 1,\\
&s_{3k-3} = p^k - p + 1, && t_{3k-3} = p, && a_{3k-3} = p^{k-1},\\
&s_{3k-2} = p^k + p - 1, && t_{3k-2} = 1.
\end{aligned}$$

b) $lq > 1$. Imamo:

$$\begin{aligned}
&s_{3k+1+\delta} = lp^k q - 2p^k + c, && t_{3k+1+\delta} = lp^k q - p^k - q + c, && a_{3k+1+\delta} = 1,\\
&s_{3k+2+\delta} = lp^k q - 2q + c, && t_{3k+2+\delta} = q.
\end{aligned}$$

Kada je $q = 1$, imamo $t_{3k+2+\delta} = 1$, a kada je $1 < q \mid c$, imamo $a_{3k+2+\delta} = lp^k - 2 + \frac{c}{q}$, pa dobijemo $s_{3k+2+\delta} = s_{3k+3+\delta}$.

□

Teorem 5.9. *Neka je* $d = (lp^k q - c)^2 - 4p^k q \equiv 1 \pmod 4$, $q \mid c, p = cl - 1$. *Tada je*

$$\ell\left(\frac{1+\sqrt{d}}{2}\right) = \begin{cases} 3k-3 & za\ lq = 1,\\ 3k+1 & za\ l > 1, q = 1,\\ 6k+2 & za\ l = 1, q > 1,\\ 6k+4 & za\ l > 1, q > 1. \end{cases}$$

Dokaz. d je oblika (5.2) uz $\mu = -1, \lambda = 1$, $d \equiv 1 \pmod 4$, $\alpha = \frac{1+\sqrt{d}}{2}$. Imamo:

$$\lfloor \sqrt{d} \rfloor = \begin{cases} lp^k q - c + 2, & \text{za } l = 1,\\ lp^k q - c + 1, & \text{za } l = 2,\\ lp^k q - c, & \text{za } l \ge 3, \end{cases}$$

$$s_0 = t_0 = 1.$$

Ako je $l = 1$ imamo $a_0 = \frac{p^k q - c + 3}{2}$ i

$$s_1 = p^k q - c + 2, \qquad t_1 = p, \qquad a_1 = p^{k-1}q - 1,$$

pa stavimo $\delta = -2, i_0 = 1$.

Ako je $l \geq 2$ imamo $a_0 = \frac{lp^k q - c + 1}{2}$ i stavimo $i_0 = \delta = 0$.

U oba slučaja stavimo

$$k' = \begin{cases} k-2, & \text{za } lq = 1, \\ k-1, & \text{za } lq > 1, \end{cases}$$

pa za $i_0 \leq i \leq k'$ dobijemo:

$$\begin{aligned} s_{3i+1+\delta} &= lp^k q - c, & t_{3i+1+\delta} &= p^{k-i} q, \\ a_{3i+1+\delta} &= lp^i - 1, \\ s_{3i+2+\delta} &= lp^k q - 2p^{k-i} q + c, & t_{3i+2+\delta} &= lp^k q - p^{k-i} q - p^{i+1} + c, \\ a_{3i+2+\delta} &= 1, \\ s_{3i+3+\delta} &= lp^k q - 2p^{i+1} + c, & t_{3i+3+\delta} &= p^{i+1}, \\ a_{3i+3+\delta} &= lp^{k-i-1} q - 1. \end{aligned}$$

Sada još samo trebamo promotriti dva slučaja:

a) $lq = 1$. Imamo:

$$\begin{aligned} s_{3k-4} &= p^k - p - 1, & t_{3k-4} &= p, & a_{3k-4} &= p^{k-1} - 1, \\ s_{3k-3} &= p^k - p + 1, & t_{3k-3} &= 1. \end{aligned}$$

b) $lq > 1$. Imamo:

$$s_{3k+1+\delta} = lp^k q - c, \qquad t_{3k+1+\delta} = q.$$

Kada je $q = 1$, imamo $t_{3k+1+\delta} = 1$, a kada je $1 < q \mid c$, imamo $a_{3k+1+\delta} = lp^k - \frac{c}{q}$, pa dobijemo $s_{3k+1+\delta} = s_{3k+2+\delta}$.

□

U istom članku je dao primjere kada je u (5.2) $d \equiv 0 \pmod 4$, tj. $c \equiv lq \equiv 0 \pmod 2$, odnosno uz $d' = \frac{d}{4}$:

$$d' = (lp^k q + \lambda c)^2 + \tau \mu p^k q, \quad \text{gdje su} \quad \begin{matrix} k \geq 2,\ l, c, q \geq 1,\ \tau \in \{1, 2\},\ \tau q \mid 2c, \\ \lambda, \mu \in \{\pm 1\}, \quad p = \frac{4}{\tau} cl + \lambda \mu \geq 2. \end{matrix} \tag{5.3}$$

(λ,μ)		$\ell(\sqrt{d'})$
$(1,1)$	$\tau q=1$	$2k+1$
	$\tau q>1$	$4k+2$
$(-1,-1)$	$lq\tau=1$	$4k-2$
	$\tau q=1, l>1$	$4k+2$
	$lq=1,\tau=2$	$8k-4$
	$\tau=l=2$	$8k$
	$l>\tau,\tau q>1$	$8k+4$
$(1,-1)$	$\tau q=1$	$3k+2$
	$l=1,\tau=2$	$6k$
	$\tau q>1,(\tau,l)\neq(2,1)$	$6k+4$
$(-1,1)$	$\tau q=1$	$3k+1$
	$l=1,\tau=2$	$6k-2$
	$\tau q>1,(\tau,l)\neq(2,1)$	$6k+2$

Teorem 5.10. *Neka je* $d=4d'$ *i* $d'=(lp^kq+c)^2+4\tau p^kq$, $\tau q \mid 2c, p=\frac{4}{\tau}cl+1$. *Tada je*

$$\ell(\sqrt{d'})=\begin{cases} 2k+1, & za\ \tau q=1,\\ 4k+2, & za\ \tau q>1,\end{cases}$$

Dokaz. d' je oblika (5.3) uz $\mu=\lambda=1$, $\alpha=\sqrt{d'}$. Tada imamo:

$$s_0=0,\qquad t_0=1,\qquad a_0=s_1=\lfloor\sqrt{d'}\rfloor=lp^kq+c.$$

Za $0\le i\le k-1$ dobijemo:

$$\begin{aligned} s_{2i+1}&=lp^kq+c, & t_{2i+1}&=\tau p^{k-i}q, & a_{2i+1}&=\frac{2}{\tau}lp^i,\\ s_{2i+2}&=lp^kq-c, & t_{2i+2}&=p^{i+1}, & a_{2i+2}&=2lp^{k-i-1}q,\end{aligned}$$

i za $i=k$ imamo

$$s_{2k+1}=lp^kq+c,\qquad t_{2k+1}=\tau q,\qquad a_{2k+1}=\frac{2}{\tau}lp^k+\left\lfloor\frac{2c}{\tau q}\right\rfloor.$$

Ako je $\tau q=1$, imamo $t_{2k+1}=1$, a ako je $1<\tau q\mid 2c$, imamo $s_{2k+1}=s_{2k+2}$, pa slijedi tvrdnja teorema. □

Teorem 5.11. *Neka je* $d = 4d'$ *i* $d' = (lp^k q - c)^2 - \tau p^k q$, $\tau q \mid 2c, p = \frac{4}{\tau}cl + 1$. *Tada je*

$$\ell\big(\sqrt{d'}\big) = \begin{cases} 4k-2 & za\ lq\tau = 1 \\ 4k+2 & za\ \tau q = 1, l > 1 \\ 8k-4 & za\ lq = 1, \tau = 2 \\ 8k & za\ \tau = l = 2 \\ 8k+4 & za\ l > \tau, \tau q > 1. \end{cases}$$

Dokaz. d' je oblika (5.3) uz $\mu = \lambda = -1$, $\alpha = \sqrt{d'}$. Tada imamo:

$$s_0 = 0, \qquad t_0 = 1,$$

$$a_0 = s_1 = \left\lfloor \sqrt{d'} \right\rfloor = \begin{cases} lp^k q - c - 2 & \text{za } \tau = 2, l = 1, \\ lp^k q - c - 1 & \text{inače.} \end{cases}$$

Ako je $\tau = 2, l = 1$ imamo:

$$\begin{array}{lll} & t_1 = 2p^k q - 4c - 4, & a_1 = 1, \\ s_2 = p^k q - 3c - 2, & t_2 = p, & a_2 = 2p^{k-1} q - 3. \end{array}$$

Ako je $\tau = l$ imamo:

$$\begin{array}{lll} & t_1 = lp^k q - 2c - 1, & a_1 = 2, \\ s_2 = lp^k q - 3c - 1, & t_2 = p, & a_2 = 2lp^{k-1} q - 2. \end{array}$$

Ako je $\tau \geq l$ stavimo $\delta = 0, i_0 = 1$ i

$$k' = \begin{cases} k-1, & \text{za } lq > 1, \\ k-2, & \text{za } lq = 1. \end{cases}$$

Ako je $\tau < l$ stavimo $\delta = 2, i_0 = 0$ i $k' = k - 1$.
U svakom od slučajeva za $i_0 \leq i \leq k'$ dobijemo:

$$\begin{aligned} s_{4i-1+\delta} &= lp^k q - p^i - c, & t_{4i-1+\delta} &= 2lp^k q - \tau p^{k-i} q - p^i - 2c, \\ a_{4i-1+\delta} &= 1, \end{aligned}$$

$$\begin{aligned} s_{4i+\delta} &= lp^k q - \tau p^{k-i} q - c, & t_{4i+\delta} &= \tau p^{k-i} q, \\ a_{4i+\delta} &= \frac{2l}{\tau} p^i - 2, \end{aligned}$$

$$\begin{aligned} s_{4i+1+\delta} &= lp^k q - \tau p^{k-i} q + c, & t_{4i+1+\delta} &= 2lp^k q - \tau p^{k-i} q - p^{i+1} + 2c, \\ a_{4i+1+\delta} &= 1, \end{aligned}$$

$$s_{4i+2+\delta} = lp^k q - p^{i+1} + c, \qquad t_{4i+2+\delta} = p^{i+1},$$
$$a_{4i+2+\delta} = 2lp^{k-i-1}q - 2.$$

Sada još samo trebamo promotriti dva slučaja:

a) $lq = 1$. Imamo:

$$s_{4k-5} = p^k - p^{k-1} - c, \qquad t_{4k-5} = 2p^k - p^{k-1} - \tau p - 2c,$$
$$a_{4k-5} = 1,$$

$$s_{4k-4} = p^k - \tau p - c, \qquad t_{4k-4} = \tau p,$$
$$a_{4k-4} = \frac{2}{\tau}p^{k-1} - 2,$$

$$s_{4k-3} = p^k - \tau p + c, \qquad t_{4k-3} = p^k - \tau p + 2c,$$
$$a_{4k-3} = 2,$$

$$s_{4k-2} = p^k - \tau p + 3c, \qquad t_{4k-2} = \tau.$$

Ako je $\tau = 1$, imamo $t_{4k-2} = 1$, a ako je $\tau = 2$, imamo $a_{4k-2} = p^k - p + c - 1$, pa dobijemo $s_{4k-2} = s_{4k-1}$.

b) $lq > 1$. Imamo:

$$s_{4k-1+\delta} = lp^k q - p^k - c, \quad t_{4k-1+\delta} = 2lp^k q - p^k - \tau q - 2c, \quad a_{4k-1+\delta} = 1,$$
$$s_{4k+\delta} = lp^k q - \tau q - c, \qquad t_{4k+\delta} = \tau q.$$

Ako je $\tau q = 1$, imamo $t_{4k+\delta} = 1$, a ako je $1 < \tau q \mid 2c$, imamo $a_{4k+\delta} = \frac{2l}{\tau}p^k - 2 - \frac{2c}{\tau q}$, pa dobijemo $s_{4k+\delta} = s_{4k+\delta+1}$.

□

Kasnije je Williams [50] tu klasu proširio brojevima oblika:

$$d = \left(\frac{\sigma}{2}\left(qra^n + \frac{\mu(a^k + \lambda)}{q}\right)\right)^2 - \sigma^2\mu\lambda a^n r,$$

gdje je $\mu, \lambda = \{-1, 1\}$, $qr \mid a^k + \lambda$, $\gcd(n, k) = 1$, $n > k \geq 1$ i

$$\sigma = \begin{cases} 1 & \text{ako } \ 2 \mid qra^n + \dfrac{\mu(a^k + \lambda)}{q}, \\ 2 & \text{ako } \ 2 \nmid qra^n + \dfrac{\mu(a^k + \lambda)}{q}. \end{cases}$$

Takvih primjera je puno, a npr. u [9] je pokazano da:

Teorem 5.12. *Za* $d_n = (12 \cdot 9^n + 1)^2 + 6 \cdot 9^n$ *vrijedi* $\ell\left(\sqrt{d_n}\right) = 4n + 6$.

Dokaz. Tvrdimo da vrijedi:

$$\begin{array}{llll} & & a_0 = 12 \cdot 9^n + 1 & \\ s_{2k+1} = 12 \cdot 9^n + 1, & t_{2k+1} = 6 \cdot 9^{n-k}, & a_{2k+1} = 4 \cdot 9^k, & \text{za } k = 0, 1, \ldots, n, \\ s_{2k} = 12 \cdot 9^n - 1, & t_{2k} = 9^k, & a_{2k} = 24 \cdot 9^{n-k}, & \text{za } k = 1, 2, \ldots, n. \end{array}$$

Budući je $(12 \cdot 9^n + 2)^2 > d_n$, imamo $a_0 = \lfloor \sqrt{d_n} \rfloor = 12 \cdot 9^n + 1$. Postupak (1.12) daje

$$s_1 = 12 \cdot 9^n + 1, \qquad t_1 = 6 \cdot 9^n, \qquad a_1 = 4.$$

Dokažimo tvrdnju indukcijom. Lako se provjeri da vrijedi za $k = 0$, pa pretpostavimo da vrijedi za $0, 1, 2, \ldots, k-1$, gdje je $k \leq n$. Tada

$$\begin{aligned} s_{2k} &= a_{2k-1}t_{2k-1} - s_{2k-1} = (4 \cdot 9^{k-1})(6 \cdot 9^{n-k+1}) - (12 \cdot 9^n + 1) = 12 \cdot 9^n - 1, \\ t_{2k} &= \frac{d_n - s_{2k-1}^2}{t_{2k-1}} = \frac{54 \cdot 9^n}{6 \cdot 9^{n-k+1}} = 9^k, \\ a_{2k} &= \left\lfloor \frac{s_{2k} + a_0}{t_{2k}} \right\rfloor = \frac{24 \cdot 9^n}{9^k} = 24 \cdot 9^{n-k}, \end{aligned}$$

i

$$\begin{aligned} s_{2k+1} &= (24 \cdot 9^{n-k}) \cdot 9^k - (12 \cdot 9^n - 1) = 12 \cdot 9^n + 1, \\ t_{2k+1} &= \frac{6 \cdot 9^n}{9^k} = 6 \cdot 9^{n-k}, \\ a_{2k+1} &= \left\lfloor \frac{24 \cdot 9^n + 2}{6 \cdot 9^{n-k}} \right\rfloor = 4 \cdot 9^k, \end{aligned}$$

što dokazuje tvrdnju.

Nadalje, imamo

$$s_{2n+2} = 12 \cdot 9^n - 1, \quad t_{2n+2} = 9^{n+1}, \quad a_{2n+2} = \left\lfloor \frac{24 \cdot 9^n}{9^{n+1}} \right\rfloor = 2,$$

$$\begin{aligned} s_{2n+3} &= 2 \cdot 9^{n+1} - (12 \cdot 9^n - 1) = 6 \cdot 9^n + 1, \\ t_{2n+3} &= \frac{d_n - s_{2n+3}^2}{t_{2n+2}} = \frac{18 \cdot 9^n (6 \cdot 9^n + 1)}{9^{n+1}} = 2(6 \cdot 9^n + 1), \\ a_{2n+3} &= \left\lfloor \frac{18 \cdot 9^n + 2}{12 \cdot 9^n + 2} \right\rfloor = 1, \end{aligned}$$

$$s_{2n+4} = 2(6 \cdot 9^n + 1) - (6 \cdot 9^n + 1) = 6 \cdot 9^n + 1,$$

$$\begin{aligned} t_{2n+4} &= \frac{18\cdot 9^n(6\cdot 9^n+1)}{2(6\cdot 9^n+1)} = 9^{n+1}, \\ a_{2n+4} &= \left\lfloor \frac{18\cdot 9^n+2}{9^{n+1}} \right\rfloor = 2. \end{aligned}$$

Budući da imamo $s_{2n+3} = s_{2n+4}$, po Napomeni 1.35 imamo $\ell\left(\sqrt{d_n}\right) = 2(2n+3) = 4n+6$. □ □

Napomena 5.13. *Mikusiński [23] je pokazao da ako je $d \in \mathbb{N}, d \neq \square$, za koji vrijedi $\ell(\sqrt{d}) \leq 2$, tada su sve Newtonove aproksimacije $R_n = \frac{1}{2}(\frac{p_n}{q_n} + \frac{dq_n}{p_n})$ konvergente od $\sqrt{d}$. Ako je R_n konvergenta od $\sqrt{d}$, tada kažemo da je R_n dobra aproksimacija. Neka $b(d)$ označava broj dobrih aproksimacija među brojevima R_n, za $n = 0, 1, \ldots, \ell(\sqrt{d}) - 1$. U [9] smo pokazali da broj $b(d)$ može biti proizvoljno velik. Nadalje, konstruirali smo nekoliko nizova koji pokazuju da za svaki $b \in \mathbb{N}$ postoji $d \in \mathbb{N}$ takav da je $b(d) = b$ i $b(d) > \frac{1}{2}\cdot \ell(\sqrt{d})$. Specijalno, za niz iz Teorema 5.12 smo pokazali da vrijedi $b(d_n) = 2n+4$, te tako dokazali smo da svaki parni broj $b \in \mathbb{N}$ postoji d_n takav da vrijedi $b(d) > \frac{1}{2}\cdot \ell(\sqrt{d})$.*

5.3 Creepers = Kreepers?

Iako se o sleepersima puno zna (već je Schnitzel dao nužan i dovoljan uvjet da bi neki niz brojeva bio sleeper), o creepersima se malo zna. Kaplanski je familije kakve smo susretali u prethodnih poglavljima (eksponencijalna funkcija polinoma) nazvao *creepers*. Kod njih je uglavnom duljina perioda jedna od nekoliko linearnih funkcija, koje ovise o ostatku pri djeljenju broja n s nekim modulom.

Kaplansky je nizove brojeva (d_n) za koje vrijedi:

- $d_n = A^2x^{2n} + Bx^n + C^2$, gdje su $A, B, C \in \mathbb{Q}$, $n \in \mathbb{N}$,
- $\ell\left(\sqrt{d_n}\right) = an + b$, gdje su $a, b \in \mathbb{Q}$,
- u palindromnom dijelu razvoja imamo parcijalni kvocijent reda veličine x^g, gdje je g fiksan i neovisan o n,

nazvao *kreepers*. Smatrao je da je creepers = kreepers. Očito je svaki kreepers ujedno i creepers. Patterson [31] je nedavno dokazao da se svaki kreeper D_n može zapisati u obliku:

$$d^2D_n = c^2\left(\left(qrx^n + (mz^2x^k - ly^2)/q\right)^2 + 4rly^2x^n\right),$$

gdje su r, l, m kvadratnoslobodni, q i r pozitivni, i vrijedi:

$$\mathrm{nzd}(rq, lymzx) = 1\ , \quad \mathrm{nzd}(ly, mz) = 1\ , \quad rly^2mz^2 \mid d^2D_n.$$

U novije se vrijeme pokazalo [13] da postoje creepersi koji nisu kreepersi, na primjer,

$$d_n = (x^{2n+2} + x^{n+2} + x^n - 1)^2 + 4x^n.$$

U [32] su Patterson i van der Poorten pokazali da za

$$d_n = (2 \cdot 2^{2n} + 2^n + 1)^2 + 4 \cdot 2^n$$

vrijedi

$$\ell\left(\frac{1+\sqrt{d_n}}{2}\right) = \begin{cases} 4n+1, & \text{za } n \text{ paran}, \\ 8n+2, & \text{za } n \text{ neparan}, \end{cases}$$

a da dani niz nije kreeper.

Poglavlje 6

Brojevi s velikom duljinom perioda i malim parcijalnim kvocijentima (beepers)

U prethodnom poglavlju smo vidjeli da postoje nizovi brojeva s velikom duljinom perioda. U svim tim primjerima su se pojavljivali veliki parcijalni kvocijenti a_i. Međutim, postoje i nizovi kod kojih su skoro svi parcijalni kvocijenti mali, a duljina perioda ipak teži u beskonačnost. Takve su nizove prvi otkrili K.S. Williams i Buck [52]. Oni su ih upotrijebili u druge svrhe, i nisu ni primjetili da su otkrili nešto novo. Kasnije se pokazalo se da su to važni primjeri, jer je kod njih fundamentalno rješenje pripadne Pellovske jednadžbe relativno malo, pa je i fundamentalna jedinica pripadnog kvadratnog polja relativno mala. Točnije, vrijedi: $R(d) = \mathcal{O}(\ln d)$.

Primjer 6.1. *Neka je* $d(n) = (2F_{6n+1} + 1)^2 + 8F_{6n} + 4$, $n \geq 1$, *gdje je* F_n *n-ti Fibonaccijev broj* ($F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$). *Tada je*

$$\ell\left(\frac{1 + \sqrt{d(n)}}{2}\right) = 6n + 1.$$

Nadalje:

i	s_i	t_i	a_i
0	1	2	$F_{6n+1} + 1$
$1, \ldots, 6n$	$1 + 2F_{6n+1} - 4F_{i-1}F_{6n-i+1}$	$2 + 4F_iF_{6n-i+1}$	1
$6n + 1$	$2F_{6n+1} + 1$	2	$2F_{6n+1} + 1$

Kasnije je van der Poorten [34] te rezultate poopćio, pa su u čast izazovu koji je riješio, za koji je zaslužio pivo, nazvani *beepers*. Kasnije su te rezultate poopćili i Mollin [25], Cheng [26], Goddard [27, 28] i mnogi drugi. Konstrukcije se uglavnom

svode na to da počevši od proizvoljno odabranog broja d konstruramo niz D_k kod kojeg razvoj u verižni razlomak svakog elementa ima k ponavljanja perioda razvoja od $\sqrt{d}$. Madden je u [20] (koristeći donjetrokutaste matrice) konstruirao nizove brojeva kod kojih sličnu stvar dobijemo, samo kombinirajući više različitih d-ova.

6.1 Konstruiranje beepersa

Promotrimo prvo jedan primjer:

Primjer 6.2. *Za $d = 14$ vrijedi $\sqrt{d} = [\,3, \overline{1, 2, 1, 6}\,] = [\,a_0, \overline{a_1, a_2, a_3, 2a_0}\,]$, duljina perioda je parna ($\ell = 4$). Označimo fundamentalno rješenje jednadžbe*

$$x^2 - 14y^2 = 1, \tag{6.1}$$

to jest, $(p_3, q_3) = (15, 4)$, sa (B_1, A_1). Po Teoremu 4.14 (ii), za polinom $D_1(n) = A_1^2 n^2 + 2B_1 n + d = 16n^2 + 30n + 14$ vrijedi:

$$\sqrt{D_1(n)} = [\,A_1 n + a_0, \overline{a_1, \ldots, a_3, 2(A_1 n + a_0)}\,] = [\,4n + 3, \overline{1, 2, 1, 8n + 6}\,].$$

Na taj način smo dobili niz brojeva u kojem svi članovi imaju isti palindromni dio, i konstantnu duljinu perioda ℓ.

Pogledajno sljedeće rješenje jednadžbe (6.1)*, ono koje se dobije iz konvergenti na kraju drugog perioda razvoja broja $\sqrt{d}$, tj. $\frac{p_7}{q_7} = [\,3,\ 1, 2, 1, 6,\ 1, 2, 1\,]$. $(B_2, A_2) = (p_7, q_7) = (449, 120)$. Primijenimo li ponovo konstrukciju iz Teorema 4.14 (ii), za polinom $D_2(n) = A_2^2 n^2 + 2B_2 n + d = 14\,400n^2 + 898n + 14$ vrijedi:*

$$\begin{aligned}\sqrt{D_2(n)} &= [\,A_2 n + a_0, \overline{a_1, \ldots, a_3, 2a_0,\ a_1, \ldots, a_3, 2(A_2 n + a_0)}\,] \\ &= [\,120n + 3, \overline{1, 2, 1, 6,\ 1, 2, 1, 240n + 6}\,].\end{aligned}$$

Na taj način smo dobili niz brojeva koji imaju isti palindromni dio, i duljinu perioda 2ℓ.

Postupak možemo nastaviti s trećim rješenjem jednadžbe (6.1)*; $(B_3, A_3) = (p_{11}, q_{11}) = (3\,596, 13\,455)$, dobili bi niz brojeva $D_3(n)$ kojem je duljina perioda 3ℓ. Pa s četvrtim, i tako dalje.*

Općenito $\ell\big(\sqrt{D_k(n)}\big) = k \cdot \ell\big(\sqrt{d}\big)$. Fiksiramo li n, na taj način smo konstruirali niz brojeva kojem duljina razvoja u verižni razlomak teži u beskonačnost, kada $k \to \infty$.

Mollin, Cheng i Goddard [27] su proširili rezultate iz Primjera 4.6 i iz Teorema 4.14 (Mc Lauglin [16]) te dobili sljedeći rezultat:

Teorem 6.3. *Neka je $d \in \mathbb{N}, d \neq \square$, takav da mu je duljina perioda ℓ parna, $\sqrt{d} = [\,a_0, \overline{a_1, \ldots, a_{\ell-1}, a_\ell}\,]$ i neka je (B, A) fundamentalno rješenje jednadžbe*

$$x^2 - dy^2 = 1.$$

Neka su

$$B_k + A_k\sqrt{d} = (B + A\sqrt{d})^k$$

sva ostala njezina rješenja. Definirajmo:

$$D_k(n) = A_k^2 n^2 + 2B_k n + d.$$

Tada je za $n \geq 0, k \geq 1$

$$\sqrt{D_k(n)} = [\, A_k \cdot n + a_0, \underbrace{\overline{a_1, \ldots, a_\ell \ \ldots\ldots \ a_1, \ldots, a_\ell}}_{k-1 \ puta}, a_1, \ldots, a_{\ell-1}, 2(A_k \cdot n + a_0)\,],$$

to jest

$$\ell\big(\sqrt{D_k(n)}\big) = k \cdot \ell\big(\sqrt{d}\big).$$

Dokaz. Isto kao kod Teorema 4.14. □

Primjer 6.4. *Vratimo se Primjeru 4.19. Uzmimo* $d = 216$, $\sqrt{d} = [\, 14, \overline{1, 2, 3, 2, 1, 28}\,]$, $\ell = 6$. *Rješenja jednadžbe*

$$B^2 - 216A^2 = 1$$

su

$$B_k + A_k\sqrt{216} = (485 + 33\sqrt{216})^k.$$

Stoga za

$$D_k(n) = A_k^2 n^2 + 2B_k n + d$$

imamo $\ell\big(\sqrt{D_k(n)}\big) = 6k$, *za* $k, n \in \mathbb{N}$. *Za* $k = 1$ *dobijemo niz iz Primjera 4.19, a za npr. k=3 imamo:*

$$B_3 + A_3\sqrt{216} = (485 + 33\sqrt{216})^3 = 456\,335\,045 + 31\,049\,667\sqrt{216},$$

pa za

$$D_3(n) = 31\,049\,667^2 n^2 + 2 \cdot 456\,335\,045 n + 216$$

imamo:

$$\sqrt{D_3(n)} = [\, A_3 \cdot n + 14, \overline{1, 2, 3, 2, 1, 28,\ 1, 2, 3, 2, 1, 28,\ 1, 2, 3, 2, 1,\ 2(A_3 \cdot n + 14)}\,].$$

Analogno kao i kod Korolara 4.18, dobije se:

Korolar 6.5. *Neka je* $d \in \mathbb{N}, d \neq \square$, *te neka je* $\sqrt{d} = [\, a_0, \overline{a_1, \cdots, a_{\ell-1}, 2a_0}\,]$, $(B, A) = (p_{\ell-1}, q_{\ell-1})$, *te neka je*

$$B_k + A_k\sqrt{d} = (B + A\sqrt{d})^k.$$

Definirajmo:

$$D_k(n) = A_k^2 n^2 + 2B_k n + d.$$

Tada je za $n \geq 0, k \geq 1$

$$\sqrt{D_k(n)} = [\, A_k \cdot n + a_0, \overline{\underbrace{a_1, \ldots, a_\ell \ \ldots\ldots \ a_1, \ldots, a_\ell}_{k-1 \ puta}, a_1, \ldots, a_{\ell-1}, 2(A_k \cdot n + a_0)}\,],$$

to jest

$$\ell\big(\sqrt{D_k(n)}\big) = k \cdot \ell\big(\sqrt{d}\big).$$

Postoje i brojne druge slične konstrukcije ovakvih primjera. Budući da su dokazi uglavnom jako slični, navesti ćemo samo rezultate i gdje se mogu naći. Uvedimo prvo neke oznake. Za $\sqrt{d} = [\, a_0, \overline{a_1, \cdots, a_{\ell-1}, 2a_0}\,]$ definirajmo:

$$w_k = \underbrace{a_1, \ldots, a_\ell,\ a_1, \ldots, a_\ell,\ \ldots\ldots,\ a_1, \ldots, a_\ell}_{k \text{ puta}},\ a_1, \ldots, a_{\ell-1},$$

Ako je ℓ paran, stavimo

$$\overrightarrow{v_k} = \underbrace{a_1, \ldots, a_\ell,\ a_1, \ldots, a_\ell,\ \ldots\ldots,\ a_1, \ldots, a_\ell}_{k \text{ puta}},\ a_1, \ldots, a_{\ell/2-1},$$

$$\overleftarrow{v_k} = a_{\ell/2-1}, \ldots, a_1,\ \underbrace{a_\ell, \ldots, a_1,\ a_\ell, \ldots, a_1,\ \ldots\ldots,\ a_\ell, \ldots, a_1}_{k \text{ puta}},$$

Teorem 6.6. *Neka je* $d \in \mathbb{N}, d \neq \square$, $k, n \in \mathbb{N}$, *i neka je* (B, A) *fundamentalno rješenje jednadžbe* $x^2 - dy^2 = 1$. *Za svaki* $k \in \mathbb{N}$ *definirajmo:*

$$B_k + A_k\sqrt{d} = (B + A\sqrt{d})^k.$$

Neka je

$$D_k(n) = (B_k - 1)^2 A_k^2 n^2 + 2(B_k - 1)^2 n + d.$$

Tada je fundamentalno rješenje jednadžbe

$$X^2 - D_k(n)Y^2 = 1$$

jednako

$$(X, Y) = \left((B_k - 1)(A_k^2 n + 1)^2 + 1, A_k^2 n + A_k\right),$$

i za

$$a_0(k, n) = (B_k - 1)A_k n + a_0$$

imamo:

a) ako je ℓ *neparan i* k *paran, tada* $d \mid (B_k - 1)$ *i:*

$$\sqrt{D_k(n)} = [\, a_0(k, n), \overline{w_{k-1}, a_0, \tfrac{2(B_k-1)A_k}{d} n, a_0, w_{k-1}, 2a_0(k, n)}\,],$$

$$\ell\big(\sqrt{D_k(n)}\big) = 2k\ell + 2,$$

b) ako su ℓ i k oba neparni, tada je

$$\sqrt{D_k(n)} = [\, a_0(k,n), \overline{w_{k-1}, 2a_0(k,n)}\,] \qquad i \qquad \ell\big(\sqrt{D_k(n)}\big) = k\ell,$$

c) ako je ℓ paran, tada vrijedi jedno od sljedećeg:

i) ako je $k = 2m+1, m \geq 0$ i $\ell/2 > 1$ neparan, tada $t_{\ell/2} \mid (B_k - 1)$ i:

$$\sqrt{D_k(n)} = [\, a_0(k,n), \overline{\overrightarrow{v_m}, \tfrac{2(B_k-1)A_k}{t_{\ell/2}}n + a_{\ell/2}, \overleftarrow{v_m}, 2a_0(k,n)}\,],$$

$$\ell\big(\sqrt{D_k(n)}\big) = k\ell,$$

i) ako je $k = 2m+1, m \geq 0$ i $\ell/2 > 1$ neparan, tada $t_{\ell/2} \mid (B_k - 1)$ i:

$$\sqrt{D_k(n)} = [\, a_0(k,n), \overline{\overrightarrow{v_m}, \tfrac{2(B_k-1)A_k}{t_{\ell/2}}n + a_{\ell/2}, \overleftarrow{v_m}, 2a_0(k,n)}\,],$$

$$\ell\big(\sqrt{D_k(n)}\big) = k\ell,$$

ii) ako je $k = 2m+1, m \geq 0$ i $\ell/2 > 1$ paran, i $a_{\ell/2}$ paran, tada $d \mid t_{\ell/2}(B_k - 1)$ i:

$$\sqrt{D_k(n)} = [\, a_0(k,n), \overline{\overrightarrow{v_m}, \tfrac{a_{\ell/2}}{2}, \tfrac{2t_{\ell/2}(B_k-1)A_k}{d}n, \tfrac{a_{\ell/2}}{2}, \overleftarrow{v_m}, 2a_0(k,n)}\,],$$

$$\ell\big(\sqrt{D_k(n)}\big) = k\ell + 2,$$

iii) ako je $k = 2m, m \in \mathbb{N}$, tada $d \mid (B_k - 1)$ i:

$$\sqrt{D_k(n)} = [\, a_0(k,n), \overline{w_{m-1}, a_0, \tfrac{2(B_k-1)A_k}{d}n, a_0, w_{m-1}, 2a_0(k,n)}\,],$$

$$\ell\big(\sqrt{D_k(n)}\big) = k\ell + 2.$$

Dokaz. Pogledati [25]. □

Mollin [25] je sličan rezultat pokazao i za niz:

$$D_k(n) = (B_k+1)^2 A_k^2 n^2 + 2(B_k+1)^2 n + d.$$

Uočimo sličnost s rezultatima iz [16], navedenim na kraju Poglavlja 4.1.

Postoje i brojni drugi primjeri, a za kraj ovoga poglavlja pokažimo kako kreirati beepers oblika $\frac{1+\sqrt{d}}{2}$.

Teorem 6.7. *Neka je $d \in \mathbb{N}, d \equiv 5 \pmod 8$. Neka je (A', B') najmanje pozitivno rješenje jednadžbe $x^2 - dy^2 = 4$ u neparnim brojevima. Stavimo $A = 2A'$ i $B = 2B'$ i za svaki $k \in \mathbb{N}$ definirajmo*

$$B_k + A_k\sqrt{d} = \frac{(B + A\sqrt{d})^k}{4^{k-1}} \qquad i \qquad \frac{1+\sqrt{d}}{2} = [\, a_0, \overline{a_1, \ldots, a_{\ell-1}, 2a_0 - 1}\,],$$

te w_k kao i ranije.

Za

$$D_k(n) = A_k^2 n^2 + 2B_k n + d,$$

fundamentalno rješenje jednadžbe $X^2 - D_k(n)Y^2 = 4$ je $(X, Y) = \left(\frac{A_k^2 n + B_k}{2}, \frac{A_k}{2}\right)$. Drugim riječima,

$$\varepsilon_{D_k(n)} = \frac{A_k^2 n + B_k + A_k\sqrt{D_k(n)}}{4}.$$

Za $a_0(k, n) = \frac{A_k}{2} n + a_0$ imamo:

a) ako je ℓ neparan

$$\frac{1+\sqrt{D_k(n)}}{2} = [\, a_0(k,n), \overline{w_{2k-1}, 2a_0(k,n) - 1}\,] \qquad i \qquad \ell\left(\frac{1+\sqrt{D_k(n)}}{2}\right) = 2k\ell,$$

b) ako je ℓ paran

$$\frac{1+\sqrt{D_k(n)}}{2} = [\, a_0(k,n), \overline{w_{k-1}, 2a_0(k,n) - 1}\,] \qquad i \qquad \ell\left(\frac{1+\sqrt{D_k(n)}}{2}\right) = k\ell.$$

Dokaz. Pogledati [26]. □

Poglavlje 7

Poboljšanje gornje ograde za duljinu perioda

Više matematičara je poboljšalo rezultate iz §1.7. Stanton, Sudler i Williams[45] su dokazali da vrijedi $\ell(\sqrt{d}) < 0.72\sqrt{d}\ln d$, a Cohn [4] je dokazao da je $\ell(\sqrt{d}) \leq \frac{7}{2\pi^2}\sqrt{d}\ln d + \mathcal{O}(\sqrt{d}) \approx 0.35\sqrt{d}\ln d + \mathcal{O}(\sqrt{d})$. U ovom poglavlju ćemo dokazati Cohnov teorem. Na kraju ćemo spomenuti vezu Riemannove slutnje i duljine perioda, jer ako je ona istinita, vrijedi $\ell(\sqrt{d}) = \mathcal{O}(\sqrt{d}\ln\ln d)$. Uvedimo prvo neke oznake.

7.1 Aritmetičke funkcije

Definicija 7.1. *Za funkciju f kažemo da je* multiplikativna *ako za svaki $m, n \in \mathbb{N}, \operatorname{nzd}(m,n) = 1$ vrijedi $f(m \cdot n) = f(m) \cdot f(n)$.*

Uočimo da ako je $f(n)$ multiplikativna funkcija, tada je i $g(n) = \sum_{d|n} f(d)$ također multiplikativna, jer imamo:

$$g(mn) = \sum_{d|m}\sum_{d'|n} f(dd') = \sum_{d|m}\sum_{d'|n} f(d)f(d') = \left(\sum_{d|m} f(d)\right)\left(\sum_{d'|n} f(d')\right) = g(m)g(n).$$

Sa $\omega(n)$ ćemo označavati broj različitih prostih djelitelja broja n. Sa $\tau(n)$ ćemo označavati broj djelitelja od n. Uočimo da vrijedi

$$\tau(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}) = \prod_{i=1}^{k}(\alpha_i + 1).$$

Propozicija 7.2. *i)*
$$\sum_{k\leq x}\frac{1}{k} = \ln x + \mathcal{O}(1),$$

ii) $$\sum_{k\le x}\tau(k) = x\ln x + \mathcal{O}(x).$$

Dokaz. *i)* $$\int_1^{\lfloor x\rfloor}\frac{1}{t}\,dt \le \sum_{k\le x}\frac{1}{k} < 1 + \int_1^x \frac{1}{t}\,dt,$$

to jest

$$\ln\lfloor x\rfloor \le \sum_{k\le x}\frac{1}{k} < 1 + \ln x,$$

odnosno

$$\sum_{k\le x}\frac{1}{k} = \ln x + \mathcal{O}(1).$$

ii)
$$\begin{aligned}\sum_{k=1}^{\lfloor x\rfloor}\tau(k) &= \sum_{k=1}^{\lfloor x\rfloor}\sum_{d\mid k}1 = \sum_{d=1}^{\lfloor x\rfloor}\sum_{m\le\frac{x}{d}}1 = \sum_{d=1}^{\lfloor x\rfloor}\Big\lfloor\frac{x}{d}\Big\rfloor = \sum_{d=1}^{\lfloor x\rfloor}\Big(\frac{x}{d}+\mathcal{O}(1)\Big)\\ &= x\ln x + \mathcal{O}(x).\end{aligned}$$

□

Sa $\mu(n)$ ćemo označavati Möbiusovu funkciju definiranu sa

$$\mu(n) = \begin{cases} 0, & \text{ako } n \text{ nije kvadratno slobodan,}\\ (-1)^k, & \text{ako je } n = p_1p_2\dots p_k, \text{ gdje su } p_i \text{ različiti prosti brojevi.}\end{cases}$$

Očito je funkcija μ multiplikativna, pa je i funkcija $\nu(n) = \sum_{d\mid n}\mu(d)$ također multiplikativna. To znači da je $\nu(1) = 1$, dok je za $n > 1$

$$\begin{aligned}\nu(n) &= \nu(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}) = \nu(p_1^{\alpha_1})\nu(p_2^{\alpha_2})\cdots\nu(p_k^{\alpha_k})\\ &= \big(\mu(1)+\mu(p_1)+\mu(p_1^2)+\cdots+\mu(p_1^{\alpha_1})\big)\cdot\cdots\\ &\qquad\cdot\big(\mu(1)+\mu(p_k)+\mu(p_k^2)+\cdots+\mu(p_k^{\alpha_k})\big)\\ &= (1-1+0+\cdots+0)\cdots(1-1+0+\cdots+0)\\ &= 0.\end{aligned}$$

Lema 7.3. *1)* $$\sum_{k=1}^{\infty}\frac{1}{k^2} = \frac{\pi^2}{6},$$

2) $$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} = \frac{6}{\pi^2}. \tag{7.1}$$

Dokaz. 1) Pokažimo najprije da za svaki $n \in \mathbb{N}$ vrijedi

$$\sum_{k=1}^{n} \operatorname{ctg}^2 \frac{k\pi}{2n+1} = \frac{n(2n-1)}{3}.$$

Iz de Moivreove formule slijedi da je

$$\cos m\alpha + i \sin m\alpha = \sin^m \alpha (\operatorname{ctg} \alpha + i)^m,$$

pa je

$$\sin(2n+1)\alpha = \sin^{2n+1} \alpha \cdot F(\operatorname{ctg}^2 \alpha),$$

gdje je

$$F(x) = \binom{2n+1}{1} x^n - \binom{2n+1}{3} x^{n-1} + \cdots + (-1)^n.$$

Ako je $\alpha = \frac{k\pi}{2n+1}$, onda je $F(\operatorname{ctg}^2 \alpha) = 0$, pa vidimo da su $\operatorname{ctg}^2 \frac{k\pi}{2n+1}$, $k = 1, \ldots, n$ upravo korijeni polinoma F. Po Viètеovim formulama je sada

$$\sum_{k=1}^{n} \operatorname{ctg}^2 \frac{k\pi}{2n+1} = \frac{\binom{2n+1}{3}}{\binom{2n+1}{1}} = \frac{n(2n-1)}{3}.$$

Iz $\sin \alpha < \alpha < \operatorname{tg} \alpha$ slijedi $\operatorname{ctg}^2 \alpha < \frac{1}{\alpha^2} < 1 + \operatorname{ctg}^2 \alpha$. Uvrstimo li ovdje $\alpha = \frac{k\pi}{2n+1}$ i sumiramo, dobivamo

$$\frac{n(2n-1)}{3} < \sum_{k=1}^{n} \frac{(2n+1)^2}{k^2\pi^2} < n + \frac{n(2n-1)}{3}.$$

Odavde je

$$\frac{\pi^2}{3} \cdot \frac{2n^2 - n}{4n^2 + 4n + 1} < \sum_{k=1}^{n} \frac{1}{k^2} < \frac{\pi^2}{3} \cdot \frac{2n^2 + 2n}{4n^2 + 4n + 1},$$

pa kada $n \to \infty$ dobivamo $\displaystyle\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$.

2) Pomnožimo izraz sa (7.1) sa $\sum_{n=1}^{\infty} \frac{1}{n^2}$. Dobivamo:

$$\left(\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} \right) \left(\sum_{n=1}^{\infty} \frac{1}{n^2} \right) = \sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{d|m} \mu(d) = \sum_{m=1}^{\infty} \frac{\nu(m)}{m^2} = 1.$$

Prema tome, imamo

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} = \frac{1}{\sum_{n=1}^{\infty} \frac{1}{n^2}} = \frac{6}{\pi^2}.$$

□

Uočimo da su $2^{\omega(n)}$ i $\tau(n)$ također multiplikativne funkcije.

Lema 7.4. *Za svaki $N \in \mathbb{N}$ vrijedi*

$$2^{\omega(N)} = \sum_{k^2|N} \tau\left(\frac{N}{k^2}\right)\mu(k).$$

Dokaz. Ako je N prost broj ili potencija prostog broja, rezultat se odmah vidi. Za ostale brojeve dokažimo indukcijom po broju različitih prostih faktora od N. Pretpostavimo da tvrdnja vrijedi za sve brojeve s najviše m prostih faktora, te neka je $N = p_0^{\alpha_0}p_1^{\alpha_1}\cdots p_m^{\alpha_m} = p_0^{\alpha_0}\cdot n$. Zbog multiplikativnosti od 2^ω, τ i μ imamo:

$$\begin{aligned}
2^{\omega(N)} &= 2^{\omega(p_0^{\alpha_0})}\cdot 2^{\omega(n)} = \sum_{i^2|p_0^{\alpha_0}} \tau\left(\frac{p_0^{\alpha_0}}{i^2}\right)\mu(i)\cdot\sum_{j^2|n}\tau\left(\frac{n}{j^2}\right)\mu(j)\\
&= \sum_{\substack{i^2|p_0^{\alpha_0}\\ j^2|n}} \tau\left(\frac{p_0^{\alpha_0}}{i^2}\right)\tau\left(\frac{n'}{j^2}\right)\mu(i)\mu(j) = \sum_{\substack{i^2|p_0^{\alpha_0}\\ j^2|n}} \tau\left(\frac{p_0^{\alpha_0}n}{i^2j^2}\right)\mu(ij)\\
&= \sum_{k^2|N}\tau\left(\frac{N}{k^2}\right)\mu(k).
\end{aligned}$$

□

Lema 7.5. *Kada $x \to \infty$ vrijedi:*

1) $S(x) \overset{\text{def}}{=} \sum_{1\le N\le x} 2^{\omega(x)} = c\cdot x\ln x + \mathcal{O}(x)$,

2) $S_2(x) \overset{\text{def}}{=} \sum_{\substack{1<N\le x\\ 2|N}} 2^{\omega(x)} = \frac{2}{3}c\cdot x\ln x + \mathcal{O}(x)$,

3) $S_2'(x) \overset{\text{def}}{=} \sum_{\substack{1\le N\le x\\ 2\nmid N}} 2^{\omega(x)} = \frac{1}{3}c\cdot x\ln x + \mathcal{O}(x)$,

4) $S_4(x) \overset{\text{def}}{=} \sum_{\substack{1<N\le x\\ 4|N}} 2^{\omega(x)} = \frac{1}{3}c\cdot x\ln x + \mathcal{O}(x)$,

5) $S_8(x) \overset{\text{def}}{=} \sum_{\substack{1<N\le x\\ 8|N}} 2^{\omega(x)} = \frac{1}{6}c\cdot x\ln x + \mathcal{O}(x)$,

6) $S_{16}(x) \overset{\text{def}}{=} \sum_{\substack{1<N\le x\\ 16|N}} 2^{\omega(x)} = \frac{1}{12} c \cdot x \ln x + \mathcal{O}(x),$

gdje je $c = \frac{6}{\pi^2}$.

Dokaz. *1)*

$$\begin{aligned} S(x) &= \sum_{1\le N\le x} 2^{\omega(x)} \overset{\text{(Lema 7.4)}}{=} \sum_{1\le N\le x} \sum_{k^2|N} \tau(\frac{N}{k^2})\mu(k) \\ &= \sum_{1\le k\le\sqrt{x}} \sum_{1\le j\le \frac{x}{i^2}} \tau(j)\mu(k) \\ &= \sum_{1\le k\le\sqrt{x}} \mu(k) \sum_{1\le j\le x/k^2} \tau(j) \\ &= \sum_{1\le k\le\sqrt{x}} \mu(k) \left\{ \frac{x}{k^2} \ln \frac{x}{k^2} + \mathcal{O}\Big(\frac{x}{k^2}\Big) \right\} \\ &= \sum_{1\le k\le\sqrt{x}} \frac{x\mu(k)\ln x}{k^2} + \mathcal{O}(x) \overset{\text{(Lema 7.3)}}{=} \frac{6}{\pi^2} \cdot x \ln x + \mathcal{O}(x) \\ &= c \cdot x \ln x + \mathcal{O}(x). \end{aligned}$$

2)

$$\begin{aligned} S_2(2x) &= \sum_{\substack{1<N\le 2x\\ 2|N}} 2^{\omega(N)} = \sum_{1\le \frac{1}{2}N\le x} 2^{\omega(2\cdot\frac{1}{2}N)} \\ &= \sum_{\substack{1<\frac{1}{2}N\le x\\ 2|\frac{1}{2}N}} 2^{\omega(2\cdot\frac{1}{2}N)} + \sum_{\substack{1\le\frac{1}{2}N\le x\\ 2\nmid\frac{1}{2}N}} 2^{\omega(2\cdot\frac{1}{2}N)} \\ &= \sum_{\substack{1<\frac{1}{2}N\le x\\ 2|\frac{1}{2}N}} 2^{\omega(\frac{N}{2})} + \sum_{\substack{1\le\frac{1}{2}N\le x\\ 2\nmid\frac{1}{2}N}} 2^{1+\omega(\frac{N}{2})} \\ &= S_2(x) + 2S_2'(x), \end{aligned}$$

pa je $S_2(2x) + S_2(x) = 2S_2(x) + 2S_2'(x) = 2S(x)$.

Pokažimo sada indukcijom da vrijedi

$$S_2(x) = 2\sum_{r=1}^{\infty} (-1)^{r-1} S(x \cdot 2^{-r}).$$

Tvrdnja je očito istinita za $x = 1$ jer obje strane iščezavaju. Pretpostavimo da je istinita za $x \leq x_0$, pa za $x \leq 2x_0$ imamo:

$$S_2(x) = 2S(\tfrac{1}{2}x) - S_2(\tfrac{1}{2}x),$$

a to je ponovo izraz traženog oblika, pa je indukcija pokazana.

Budući da za $y < 1$ vrijedi $S(y) = 0$, imamo

$$S_2(x) = 2\sum_{r=1}^{k}(-1)^{r-1}S(x \cdot 2^{-r}),$$

gdje je

$$k = \Big\lfloor \frac{\ln x}{\ln 2} \Big\rfloor.$$

Sada je po 1)

$$|S(y) - cy \ln y| < Cy,$$

za neku konstantu C i sve $y > 1$, pa imamo

$$\left| S_2(x) - 2c\sum_{r=1}^{k}(-1)^{r-1}\frac{x}{2^r}\ln\frac{x}{2^r} \right| < 2C\sum_{r=1}^{k}\frac{x}{2^r} < 2Cx,$$

odnosno

$$\left| S_2(x) - 2c\sum_{r=1}^{k}(-1)^{r-1}\frac{x}{2^r}\ln x \right| < 2Cx + 2cx\ln 2\sum_{r=1}^{k}\frac{r}{2^r} < C_1 x.$$

Naposlijetku imamo

$$\begin{aligned}\sum_{r=1}^{k}(-1)^{r-1}\frac{x}{2^r}\ln x &= \frac{1}{2}x\ln x \cdot \frac{1-(-\frac{1}{2})^k}{1-(-\frac{1}{2})} \\ &= \frac{1}{3}x\ln x\Big(1+\mathcal{O}\big(x^{-1}\big)\Big) \\ &= \frac{1}{3}x\ln x + \mathcal{O}(\ln x),\end{aligned}$$

pa slijedi tvrdnja.

3) Lako se vidi, budući je $S_2'(x) = S(x) - S_2(x)$.

4) Slijedi budući je

$$S_4(x) = \sum_{\substack{1<\frac{1}{2}N\leq\frac{x}{2} \\ 2|\frac{1}{2}N}} 2^{\omega(2\cdot\frac{N}{2})} = S_2(\frac{x}{2}).$$

5) i *6)* slijedi slično jer je $S_8(x) = S_4(\frac{x}{2})$ i $S_{16}(x) = S_8(\frac{x}{2})$.

□

7.2 Pellovska jednadžba

Definicija 7.6. *Jednadžba oblika*

$$x^2 - dy^2 = N, \tag{7.2}$$

gdje je d prirodan broj koji nije potpun kvadrat i N cijeli broj različit od nule, naziva se pellovska jednadžba.

U §2.1 smo vidjeli neke specijalne jednadžbe ovoga tipa, a ovdje će nam pomoći neki rezultati vezani uz broj rješenja takvih jednadžbi. Ona ne mora imati rješenja. No, ukoliko ima barem jedno rješenje, onda ih ima beskonačno mnogo. Označimo sa $\epsilon = u + v\sqrt{d}$ rješenje jednadžbe $x^2 - dy^2 = 1$. Ako za dani N postoji rješenje jednadžbe (7.2) (zapišimo ga sa $x_0 + y_0\sqrt{d}$), tada su rješenja i $\pm(x_0 + y_0\sqrt{d})\epsilon^n$, i taj skup zovemo *klasa rješenja*. Dana jednadžba može imati više klasa rješenja, ali je dobro znano da je broj klasa konačan. U jednoj klasi $\text{nzd}(x, y)$ je konstantan, a ako je jednak 1 kažemo da je klasa *primitivna*. Broj primitivnih klasa ćemo označavati sa $f(N; d)$. Lako se vidi da ako je $x_0 + y_0\sqrt{d}$ rješenje jednadžbe (7.2) koje nije primitivno, tj. ako je $\text{nzd}(x_0, y_0) = g$, onda je $\frac{x_0}{g} + \frac{y_0}{g}\sqrt{d}$ primitivno rješenje jednadžbe $x^2 - dy^2 = \frac{N}{g^2}$.

Za dva rješenja kažemo da su *asocirana* ako pripadaju istoj klasi. Nije teško vidjeti da su dva rješenja $x_1 + y_1\sqrt{d}$ i $x_2 + y_2\sqrt{d}$ asocirana ako i samo ako vrijedi:

$$x_1x_2 \equiv dy_1y_2 \pmod N, \qquad x_1y_2 \equiv x_2y_1 \pmod N.$$

Lema 7.7. *Ako je $x + y\sqrt{d}$ primitivno rješenje jednadžbe* (7.2)*, onda postoji cijeli broj k, $|k| \leq \frac{|N|}{2}$, sa svojstvom*

$$x_0 \equiv ky_0 \pmod N,$$
$$k^2 \equiv d \pmod N.$$

U tom slučaju kažemo da rješenje $x + y\sqrt{d}$ pripada broju k.

Dokaz. Budući da su x i y relativno prosti, to su i y_0 i N također relativno prosti. Stoga postoji $k \in \mathbb{Z}$ takav da je $ky \equiv x_0 \pmod{N}$. Broj k možemo izabrati iz bilo kojeg potpunog sustava ostataka modulo N, a tako i iz onog s najmanjim ostatcima po asolutnoj vrijednosti, koji sadrži ostatke koji su $\leq \frac{|N|}{2}$. Nadalje,

$$x^2 - dy^2 \equiv (k^2 - d)y^2 \equiv 0 \pmod{N},$$

pa je $k^2 \equiv d \pmod{N}$. □

Lema 7.8. *Dva primitivna rješenja jednadžbe* (7.2) *su asocirana ako i samo ako pripadaju istom broju.*

Dokaz. Neka su $x_1 + y_1\sqrt{d}$ i $x_2 + y_2\sqrt{d}$ dva primitivna asocirana rješenja jednadžbe (7.2). Tada postoji rješenje $u + v\sqrt{d}$ jednadžbe $x^2 - dy^2 = 1$ tako da je

$$x_2 = x_1u + dy_1v, \qquad y_2 = x_1v + y_1u.$$

Ako $x_1 + y_1\sqrt{d}$ pripada broju k, onda vrijedi

$$y_2k \equiv x_1vk + y_1uk \equiv y_1vk^2 + x_1u \equiv dy_1v + x_1u \equiv x_2 \pmod{N},$$

pa i $x_2 + y_2\sqrt{d}$ pripada broju k.

Dokažimo sada obrat. Pretpostavimo da rješenja $x_1 + y_1\sqrt{d}$ i $x_2 + y_2\sqrt{d}$ pripadaju istom broju k. Tada je

$$x_1x_2 \equiv k^2y_1y_2 \equiv dy_1y_2 \pmod{N} \qquad \text{i} \qquad x_1y_2 \equiv ky_1y_2 \equiv y_1x_2 \pmod{N},$$

pa su rješenja asocirana. □

Lema 7.9. *Za proizvoljan $N \in \mathbb{Z}$ vrijedi*

$$f(N; d) \leq 2^{\omega(|N|)},$$

a ako $2 \parallel N$ vrijedi

$$f(N; d) \leq 2^{\omega(|N|)-1}.$$

Dokaz. Uočimo da je dovoljno tvrdnju dokazati uz pretpostavku da je $\text{nzd}(N, d)$ kvadratno slobodan. Naime, ako je $\text{nzd}(N, d) = k_1^2k_2$ (k_2 kvadratno slobodan), $x^2 - dy^2 = N$ i $\text{nzd}(x, y) = 1$, tada $k_1|x$. Sada za $x_1 = \frac{x}{k_1}$, $N_1 = \frac{N}{k_1^2}$ i $d_1 = \frac{d}{k_1^2}$ vrijedi $x_1^2 - d_1y^2 = N_1$ i $\text{nzd}(x_1, y) = 1$. Vidimo da je u drugoj jednadžbi $\text{nzd}(N_1, d_1) = k_2$ kvadratno slobodan, pa ukupan broj primitivnih klasa početne jednadžbe nije veći od $2^{\omega(|N_1|)} \leq 2^{\omega(|N|)}$ općenito, ni od $2^{\omega(|N_1|)-1} \leq 2^{\omega(|N|)-1}$ ako $2 \parallel N$, budući da tada $2 \parallel N_1$. Stoga pretpostavimo da je $\text{nzd}(N, d)$ kvadratno slobodan.

Po Lemi 7.8, broj klasa je manji ili jednak broju mogućih k-ova, tj. broju rješenja kongruencije $x^2 \equiv d \pmod{N}$. Neka je $N = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_{\omega(N)}^{\alpha_{\omega(N)}}$. Po Kineskom teoremu o ostatcima, ukupan broj rješenja jednak je umnošku broja rješenja jednadžbi $x^2 \equiv d \pmod{p_i^{\alpha_i}}$. Stoga promotrimo te kongruencije.

i) Ako $p_i \mid d$, tada $p_i \mid x$. Budući da $p_i \nmid y$ (jer je klasa primitivna) i $p_i^2 \nmid d$ (jer bi u protivnom bilo i $p_i^2 \mid N$) slijedi $p_i^2 \nmid dy^2$. Pa je $\alpha_i = 1$ i $xy^{-1} \equiv 0 \pmod{p_i^{\alpha_i}}$, tj. imamo samo jedno rješenje,

ii) ako $p_i \nmid d$, tada p_i ne dijeli ni x ni y (jer bi u protivnom morao dijeliti oba, pa klasa ne bi bila primitivna). Pa je $(xy^{-1})^2 \equiv d \pmod{p_i^{\alpha_i}}$.

ii') ako je $p \neq 2$, kongruencija $(xy^{-1})^2 \equiv d \pmod{p_i}$ ima najviše dva rješenja, pa po Henselovoj lemi i kongruencija $(xy^{-1})^2 \equiv d \pmod{p_i^{\alpha_i}}$ ima najviše 2 rješenja,

ii") ako je $p_i = 2$, tada $(xy^{-1})^2 \equiv d \pmod{p_i^{\alpha_i}}$ daje:

a) ako je $\alpha_i = 1$, $(xy^{-1})^2 \equiv d \pmod 2$, to jest $xy^{-1} \equiv d \pmod{p_i^{\alpha_i}}$, tj. imamo samo jedno rješenje,

b) ako je $\alpha_i = 2$, budući je $x^2 - dy^2 \equiv 0 \pmod 4$, i x i y su neparni, slijedi $d \equiv 1 \pmod 4$, pa je $(xy^{-1})^2 \equiv 1 \pmod 4$, to jest $xy^{-1} \equiv \pm 1 \pmod 4$, tj. $xy^{-1} \equiv \pm 1 \pmod{p_i^{\alpha_i}}$, tj. imamo najviše 2 rješenja,

c) ako je $\alpha_i \geq 3$, tada je $d \equiv 1 \pmod 8$, pa $(xy^{-1})^2 \equiv d \pmod{2^{\alpha_i}}$ daje $xy^{-1} \equiv \pm a \pmod{2^{\alpha_i - 1}}$, tj. možemo imati najviše 2 rješenja modulo $2^{\alpha_i - 1}$.

Dakle, dobili smo da je xy^{-1} kongruentan najviše

$$\begin{array}{rl} 2^{\omega(N)-1} & \text{ostataka modulo } N, \text{ ako } 2 \parallel N, \\ 2^{\omega(|N|)} & \text{ostataka modulo } N, \text{ ako } 8 \nmid N, \\ 2^{\omega(|N|)} & \text{ostataka modulo } \frac{N}{2}, \text{ ako } 8 \mid N. \end{array}$$

Da bi završili dokaz, ostaje još promotriti slučaj kada $8 \mid N$. Trebamo pokazati da ako su (x_1, y_1) i (x_2, y_2) dva primitivna rješenja jednadžbe (7.2) za koja vrijedi $x_1 y_1^{-1} \equiv x_2 y_2^{-1} \pmod{\frac{N}{2}}$, da su ona u istoj klasi. Neka je

$$\begin{aligned} \frac{x_1 + y_1\sqrt{d}}{x_2 + y_2\sqrt{d}} &= \frac{(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d})}{x_2^2 - dy_2^2} = \frac{x_1x_2 - dy_1y_2}{N} + \frac{-x_1y_2 + x_2y_1}{N}\sqrt{d} \\ &= r + s\sqrt{d}. \end{aligned}$$

Lako se vidi da je s ili cijeli broj, ili polovina neparnog broja. U prvom slučaju je zbog $r^2 - ds^2 = 1$ i broj r cijeli. U drugom slučaju vrijedi $(2r)^2 = d(2s)^2 + 4$, pa budući je $2s$ neparan broj i $4 \nmid d$, i $2r$ je neparan broj, pa je $d \equiv 5 \pmod 8$. Ali to je u suprotnosti sa $x_1^2 - dy_1^2 \equiv 0 \pmod 8$, $\text{nzd}(x, y) = 1$, pa vidimo da taj slučaj ne može nastupiti.

□

Lema 7.10. *Ako jednadžba $x^2 - dy^2 = -1$ nema rješenja, tada je*

$$f(N;d) + f(-N;d) \leq \begin{cases} 2^{\omega(|N|)}, & ako\ 2 \nmid N, \\ 2^{\omega(|N|)-1}, & ako\ 2 \parallel N. \end{cases}$$

Dokaz. Po Lemi 7.9, dovoljno je dokazati da $x_1^2 - dy_1^2 = N$ i $x_2^2 - dy_2^2 = -N$ sa $x_1 y_1^{-1} \equiv x_2 y_2^{-1} \pmod{N}$ ili $\pmod{\frac{N}{2}}$ ako $8|N$ nije moguće. Jer ako bi bilo moguće, postojali bi r i s:

$$r + s\sqrt{d} = \frac{x_1 + y_1\sqrt{d}}{x_2 + y_2\sqrt{d}},$$

takvi da $r^2 - ds^2 = -1$, te su r i s ili oba cijeli brojevi ili oba polovine neparnih brojeva. Oba slučaja su nemoguća, budući da jednadžba $x^2 - dy^2 = -1$ nema rješenja (kao i u dokazu prethodne leme). □

Više of pellovskim jednadžbama može se naći u [6].

7.3 Dokaz Cohnovog teorema

Iz (1.13d) i Teorema 1.31 lako slijedi:

Lema 7.11. *Za svaki r vrijedi $|p_r^2 - dq_r^2| < 2\sqrt{d}$.*

Lema 7.12. *1) Ako jednadžba $x^2 - dy^2 = -1$ nema rješenja, tada*

$$\ell\big(\sqrt{d}\big) \leq \sum_{0<N<2\sqrt{d}} \{f(N;d) + f(-N;d)\},$$

2) Ako jednadžba $x^2 - dy^2 = -1$ ima rješenja, tada

$$\ell\big(\sqrt{d}\big) \leq \sum_{0<N<2\sqrt{d}} f(N;d).$$

Dokaz. 1) Neka je $0 \leq m < n \leq \ell\big(\sqrt{d}\big) - 1$. Tada su $p_m + q_m\sqrt{d}$ i $p_n + q_n\sqrt{d}$ rješenja nekih pellovskih jednadžbi (možda s različitim N) u različitim klasama, jer su oba manja od fundamentalnog rješenja jednadžbe $x^2 - dy^2 = 1$, koje je na kraju perioda. Ta rješenja su primitivna, jer $\operatorname{nzd}(p_r, q_r) = 1$. Po Lemi 7.11, za svaku konvergetu imamo jedno primitivno rješenje jednadžbe $x^2 - dy^2 = N$, gdje je $-2\sqrt{d} < N < 2\sqrt{d}$, tj. broj konvergenti nije veći od broj primitivnih klasa, pa vrijedi

$$\ell\big(\sqrt{d}\big) \leq \sum_{-2\sqrt{d}<N<2\sqrt{d}} f(N;d).$$

2) Ako jednadžba $x^2 - dy^2 = -1$ ima rješenja, tada vrijedi: $F(N;d) = F(-N;d)$, pa vrijede isti argumenti kao u prethodnom dijelu, uz $0 \leq m < n \leq 2\ell\big(\sqrt{d}\big) - 1$, jer je fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$ na kraju drugog perioda. □

Teorem 7.13. *Neka je $d \in \mathbb{N}$. Tada za duljinu perioda vrijedi:*

$$\ell\big(\sqrt{d}\big) \leq \frac{7}{2\pi^2}\sqrt{d}\ln d + \mathcal{O}\big(\sqrt{d}\big).$$

Dokaz. Imamo

$$\ell\big(\sqrt{d}\big) \leq \sum_{1\leq N\leq 2\sqrt{d}} 2^{\omega(N)} = c\cdot\sqrt{d}\ln d + \mathcal{O}\big(\sqrt{d}\big)$$

pa ćemo u ostatku dokaza smanjiti konstantu c. To možemo na dva načina.

Prvo: ako $2 \parallel N$, tada se gornja ograda $2^{\omega(N)}$ može prepoloviti.

Drugo: promatrati ćemo klase ostataka $d \mod 16$. U nekima za pojedine N-ove, jednadžba $x^2 - dy^2 = N$ uopće ne može imati primitivnih rješenja.

U svakom slučaju, na taj način se nije moguće riješiti svih neparnih N-ova, pa ćemo stoga uvijek imati član

$$\sum_{\substack{1\leq N\leq 2\sqrt{d}\\ 2\nmid N}} 2^{\omega(N)} = S_2'(2\sqrt{d}).$$

Promotrimo različite slučajeve:

a) $d \equiv 1 \pmod 8$. Budući da x i y ne mogu oba biti parni, $x^2 - dy^2 = N$ je ili neparan ili djeljiv s 8. Stoga je

$$\ell\big(\sqrt{d}\big) \leq S_2'(2\sqrt{d}) + S_8(2\sqrt{d}) = \frac{1}{2}c\cdot\sqrt{d}\ln d + \mathcal{O}\big(\sqrt{d}\big).$$

b) $d \equiv 5 \pmod 8$. Ako je N paran, tada $2^2 \parallel N$, pa je

$$\ell\big(\sqrt{d}\big) \leq S_2'(2\sqrt{d}) + S_4(2\sqrt{d}) - S_8(2\sqrt{d}) = \frac{1}{2}c\cdot\sqrt{d}\ln d + \mathcal{O}\big(\sqrt{d}\big).$$

c) $d \equiv 2, 3 \pmod 4$. Ako je N paran, tada $2 \parallel N$, pa je

$$\begin{aligned}\ell\big(\sqrt{d}\big) &\leq S_2'(2\sqrt{d}) + \sum_{\substack{1<N\leq 2\sqrt{d}\\ 2\parallel N}} 2^{\omega(N)-1}\\ &= S_2'(2\sqrt{d}) + \frac{1}{2}\Big(S_2(2\sqrt{d}) - S_4(2\sqrt{d})\Big)\\ &= \frac{1}{2}c\cdot\sqrt{d}\ln d + \mathcal{O}\big(\sqrt{d}\big).\end{aligned}$$

d) $d \equiv 0 \pmod 4$. U primitivnom rješenju jednadžbe $x^2 - dy^2 = N$ mora biti ili x neparan (pa je i N neparan) ili x paran i y neparan (pa $4 \mid N$). U drugom slučaju imamo $(\frac{1}{2}x)^2 - (\frac{1}{4}d)y^2 = \frac{1}{4}N$, pa dobijemo primitivno rješenje jednadžbe $X^2 - (\frac{1}{4}d)Y^2 = \frac{1}{4}N$ (Y neparan). Imamo:

ili $\frac{1}{4}d \equiv 0, 1 \pmod 4$, pa je $\frac{1}{4}N$ neparan ili djeljiv s 4,

ili $\frac{1}{4}d \equiv 2, 3 \pmod 4$, pa je $\frac{1}{4}N$ neparan ili $2 \parallel \frac{1}{4}N$.

U prvom slučaju dobijemo

$$\begin{aligned}\ell\big(\sqrt{d}\big) &\leq S_2'(2\sqrt{d}) + S_4(2\sqrt{d}) - S_8(2\sqrt{d}) + S_{16}(2\sqrt{d}) \\ &= \frac{7}{12}c \cdot \sqrt{d}\ln d + \mathcal{O}\big(\sqrt{d}\big),\end{aligned}$$

a u drugom

$$\begin{aligned}\ell\big(\sqrt{d}\big) &\leq S_2'(2\sqrt{d}) + S_4(2\sqrt{d}) - S_{16}(2\sqrt{d}) \\ &= \frac{7}{12}c \cdot \sqrt{d}\ln d + \mathcal{O}\big(\sqrt{d}\big).\end{aligned}$$

□

Napomena 7.14. *Možemo uočiti da ako $4 \nmid d$, onda se konstanta sa $\frac{7}{12}c$ može smanjiti na $\frac{1}{2}c$.*

7.4 Veza s Riemannovom slutnjom

Eksperimentalni rezultati pokazuju da gornje ograde za duljinu perioda iz prethodnog potpoglavlja nisu najbolje moguće. U Tablici 1.1 vidimo da bi moglo vrijediti: $\ell(\sqrt{d}) = \mathcal{O}(\sqrt{d}\ln\ln d)$. Slično je sugerirao i Williams [49] i brojni drugi matematičari, a slutnja (povezana s čuvenom Riemannovom slutnjom) je da vrijedi $\ell(\sqrt{d}) = \mathcal{O}(\sqrt{d}\ln\ln d)$.

Za $s \in \mathbb{C}$, takav da je $\Re s > 1$, *Riemannova zeta* funkcija je

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prost}} \left(\frac{p^s}{p^s - 1}\right).$$

Gornji red konvergira apsolutno i uniformno za $\Re s > 1$, pa je na tom skupu funkcija analitička. Pokazuje se da postoji meromorfno produljenje funkcije na $s \in \mathbb{C}$, $s \neq 1$. *Riemannova slutnja (RH)* kaže da jedine netrivijalne nultočke (trivijalne su $-2, -4, -6, \dots$) produljene funkcije leže na pravcu $\Re(s) = 1/2$.

Dirichletov karakter χ je multiplikativna funkcija za koju postoji $k \in \mathbb{N}$ takav da vrijedi $\chi(n+k) = \chi(n)$ za sve $n \in \mathbb{N}$, i $\chi(n) = 0$ ako $\operatorname{nzd}(n,k) > 1$. *Dirichletova L-funkcija* je

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Ona se ponovo može analitički produljiti na $\mathbb{C}$. *Generalizirana Riemannova slutnja (GRH)* kaže da za svaki Dirichletov karakter χ i za svaki kompleksni broj s s realnim dijelom između 0 i 1 za koji je $L(\chi, s) = 0$ vrijedi $\Re s = 1/2$. Slučaj $\chi = 1$ vodi na RH.

Neka je K polje (konačnodimenzionalno proširenje od $\mathbb{Q}$) s prstenom cijelih brojeva $\mathcal{O}_K$. Normu ideala $\mathfrak{a} \neq \mathfrak{o}$ označimo sa $N\mathfrak{a} := \#(\mathcal{O}_K/\mathfrak{a})$. *Dedekindova zeta funkcija* je

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a} \in \mathcal{O}_K \\ \mathfrak{a} \neq \mathfrak{o}}} \frac{1}{(N\mathfrak{a})^s}.$$

Analitički ju produljimo na cijeli $\mathbb{C}$. *Proširena Riemannova slutnja (ERH)* kaže da za svako polje K i svaki kompleksni broj s s realnim dijelom između 0 i 1 za koji je $\zeta_K(s) = 0$ vrijedi $\Re s = 1/2$.

Neka je $\alpha = \sqrt{d}$ i neka je ε_0 fundamentalna jedinica od $\mathbb{Q}(\sqrt{d})$. Nije teško vidjeti [51] da vrijedi

$$\varepsilon_0 = \prod_{i=1}^{\ell} \alpha_i,$$

osim ako je neki $t_k = 4$ (pogledati Teorem 1.31), a u tom slučaju mora postojati par neparnih cijelih brojeva x, y za koje vrijedi $x^2 - dy^2 = 4$, pa tada mora biti $d \equiv 5 \pmod 8$ i

$$\varepsilon_0^3 = \prod_{i=1}^{\ell} \alpha_i.$$

Sada nije teško vidjeti ($a_i \geq 1$, ili pogledati [45, (2.8)]) da vrijedi

$$\prod_{i=1}^{\ell} \alpha_i > p_{\ell-1} + q_{\ell-1} \geq F_{\ell+1} + F_\ell \geq \beta^\ell, \qquad \text{za} \qquad \beta = \tfrac{1+\sqrt{5}}{2},$$

gdje je F_n n-ti Fibonaccijev broj. Definiramo li:

$$\lambda = \begin{cases} \frac{1}{3} & \text{za } d \equiv 5 \pmod 8, \\ 1 & \text{inače,} \end{cases}$$

imamo $R > \lambda \ell \log \beta$, gdje je $R = \log \varepsilon_0$ regulator od $\mathbb{Q}(\sqrt{d})$.

Levy [18] je pokazao da za gotovo sve iracionalnosti α imamo:

$$\lim_{n\to\infty} \sqrt[n]{\alpha_1\alpha_2\alpha_3\cdots\alpha_n} = e^m,$$

gdje je $m = \frac{\pi^2}{12\ln 2} \approx 1.18656911$. Pa ako je ℓ velik, za očekivati je $R \approx \lambda\ell m$. Na primjer, za $d = 26\,437\,680\,473\,689$ imamo $R \approx 21\,737\,796.43$ (Shanks [44]), $\ell = 18\,331\,889$ (pogledati [42]), pa je $R/\ell \approx 1.185791406$.

Neka je h broj klasa od $\mathbb{Q}(\sqrt{d})$. Dobro je poznato (vidjeti na primjer [3]) da

$$2Rh = \sqrt{d}\cdot L(1,\chi_{d'}), \tag{7.3}$$

gdje je d' diskriminanta od $\mathbb{Q}(\sqrt{d})$, to jest:

$$d' = \begin{cases} d & \text{za } d \equiv 1 \pmod 4, \\ 4d & \text{inače.} \end{cases}$$

Ovdje je

$$L(1,\chi_{d'}) = \sum_{n=1}^{\infty}\left(\frac{d'}{n}\right)\frac{1}{n} = \prod_{p \text{ prost}}\left(\frac{p}{p-(d'/p)}\right), \tag{7.4}$$

gdje je $\chi_{d'}(n) = (d'/n)$ Kroneckerov simbol[1] . Littlewood [19] je pokazao da ako je proširena Riemannova hipoteza (ERH) istinita za $\chi_{d'}(n) = (d'/n)$, tada je

$$L(1,\chi_{d'}) < \big(1+o\,(1)\,\big)2e^{\gamma}\ln\ln d',$$

gdje je $\gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \ln n\right) = \int_1^{\infty}\left(\frac{1}{\lfloor x\rfloor} - \frac{1}{x}\right)dx = \lim_{x\to\infty}\left(x - \Gamma(1/x)\right) \approx 0.5772156649$ Eulerova konstanta. Nadalje, Shanks [43] je uočio da je uz istu hipotezu:

$$L_{-d}(1) = \sum_{k=1}^{\infty}\left(\frac{4d}{k}\right)\frac{1}{k} < \big(1+o\,(1)\,\big)2e^{\gamma}\ln\ln 4d.$$

[1] *Kroneckerov simbol* (d/n) je proširenje Legendreovog (Jacobijevog) simbola. Za neparan prost broj p, $(\frac{d}{p})$ je obični Legendreov simbol, a za sve $n \in \mathbb{Z}$, $(\frac{d}{n})$ je dan formulama:

$$\left(\frac{d}{0}\right) = \begin{cases} 1, & \text{za } d = \pm 1, \\ 0 & \text{inače,} \end{cases} \quad \left(\frac{d}{1}\right) = 1, \quad \left(\frac{d}{-1}\right) = \begin{cases} -1, & \text{za } d < 0, \\ 1 & \text{za } d \geq 0, \end{cases} \quad \left(\frac{d}{2}\right) = \begin{cases} 0, & \text{za } d \text{ paran,} \\ 1 & \text{za } d \equiv \pm 1 \,(\text{mod } 8)\,, \\ -1 & \text{za } d \equiv \pm 3 \,(\text{mod } 8)\,, \end{cases}$$

$$\left(\frac{d}{\pm p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}}\right) = \left(\frac{d}{\pm 1}\right)\left(\frac{d}{p_1}\right)^{\alpha_1}\left(\frac{d}{p_2}\right)^{\alpha_2}\cdots\left(\frac{d}{p_k}\right)^{\alpha_k}.$$

Iz Eulerovog produkta (7.4) imamo:

$$L_{-d}(1) = \begin{cases} \frac{1}{2}L(1,\chi_{d'}) & \text{kada je } d \equiv 1 \pmod 8, \\ \frac{3}{2}L(1,\chi_{d'}) & \text{kada je } d \equiv 5 \pmod 8, \\ L(1,\chi_{d'}) & \text{inače,} \end{cases}$$

pa je Shanksov rezultat jači od Littlewoodovog, osim u slučaju $d \equiv 1 \pmod 8$.

Ako definiramo

$$f(d) = \begin{cases} \sqrt{d}\ln\ln d & \text{kada je } d \equiv 1 \pmod 8, \\ \sqrt{d}\ln\ln 4d & \text{inače,} \end{cases}$$

imamo

$$Rh < \big(1 + o\,(1)\,\big)\lambda e^{\gamma} f(d).$$

Iz svega toga zaključujemo da je

$$G(d) \stackrel{\text{def}}{=} \frac{\ell\big(\sqrt{d}\big)}{f(d)} < K_1 + o\,(1)\,, \qquad K_1 = \frac{e^{\gamma}}{\ln\beta} \approx 3.7012232976,$$

pa čak i

$$G(d) < K_2 + o\,(1)\,, \qquad K_2 = \frac{e^{\gamma}}{m} = \frac{12e^{\gamma}\ln 2}{\pi^2} \approx 1.501027123,$$

ako je ERH istinita.

Bibliografija

[1] T.G. Berry, *On periodicity of continued fractions in hyperelliptic function fields*, Arch. Math. (Basel) **55** (1990), no. 3, 259–266.

[2] H. Cohen, H.W. Lenstra Jr, *Heuristics on class groups of number fields*, Number Theory (Noordwijkerhout 1983), Lecture Notes in Math. **1068**, Springer-Verlag, Berlin, 1984, pp. 33–62.

[3] H. Cohn, *Advanced Number Theory*, Dover Publications, Inc., New York, 1980, Reprint of "A Second Course in Number Theory".

[4] J.H.E. Cohn, *The length of the period od the simple continued fraction of* $d^{1/2}$, Pacific J. Math. **71** (1977), No. 1, 21–32.

[5] P.G.L. Dirichlet, *Lectures on number theory*, History of Mathematics, vol. 16, Amer. Math. Soc., Providence RI, 1999, Supplements by R. Dedekind. Translated from the 1863 original and with an introduction by J. Stillwell.

[6] A. Dujella, *Diofantske jednadžbe*, `http://web.math.hr/∼duje/dioph/dioph.pdf`

[7] A. Dujella, *Uvod u teoriju brojeva*, `http://web.math.hr/∼duje/utb/utblink.pdf`

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

[9] A. Dujella, V. Petričević, *Square roots with many good approximants*, Integers **5(3)** (2005), `#A6`.

[10] C.F. Gauss, *Disqusitiones Arithmeticae*, Yale Univ. Press, New Haven, Conn., 1966.

[11] F. Halter-Koch, *Einige periodische Kettenbruchentwicklungen und Grundeinheiten quadratischer Ordnungen*, Abh. Math. Sem. Univ. Hamburg **59** (1989), 157–169.

[12] N. Ishii, P. Kaplan, K.S. Williams, *On Eisenstein's problem*, Acta Arith. **54** (1990), 323-–345.

[13] M.J. Jacobson,Jr., H.C. Williams, *Solving the Pell Equation*, Springer, 2009.

[14] I. Kaplansky, *A memo on creepers*, pismo R.A. Mollinu, H.C. Williamsu i K.S. Williamsu, 23 November, 1998.

[15] A.N. Khovanskii, *The application of continued fractions and their generalizations to problems in approximation theory*, P. Noordhoff, Ltd. Groningen, 1963.

[16] J. Mc Laughlin, *Polynomial solutions to Pell's equation and fundamental units in real quadratic fields*, J. Lond. Math. Soc. (2) **67** (2003), 16–28.

[17] J. Mc Laughlin, P. Zimmer, *Some more long continued fractions, I*, Acta Arith. **127** (2007), No. 4, 365–389.

[18] P. Levy, *Sur le developpement en fraction continue d'un nombre choisi au hasard*, Compositio Math. **3** (1936), 286–303.

[19] U.E. Littlewood, *On the class-number of the corpus* $P(\sqrt{-k})$, Proc. Lond.Math.Soc. **28** (1928), 359–372.

[20] D.J. Madden, *Constructing families of long continued fractions*, Pacific J. Math. **198** (2001), No. 1, 123–147.

[21] V.A. Malyshev, *Periods of quadratic irrationalities, and torson of elliptic curves*, Algebra i Analiz, **15**, No. 4 (2003), 177–203;
Engleski prijevod, St. Petersburg Math. J. **15**, No. 4 (2004), 587-602.

[22] B. Mazur, *Rational points on modular curves*, Proc. Second Internet. Conf., Univ. Bonn, Bonn 1976, Lecture Notes in Math. **601**, Springer, Berlin (1977), 107-148.

[23] J. Mikusiński, *Sur la méthode d'approximation de Newton*, Ann. Polon. Math. **1** (1954), 184–194.

[24] R.A. Mollin, *Construction of families of long continued fraction revisited*, Acta Math. Academiae Paedagogicae Nyíregyházuensis **19** (2003), 175–181.

[25] R.A. Mollin, *Polynomials of Pellian type and continued fractions*, Serdica Math. J. **27** (2001), 317–342.

[26] R.A. Mollin, K. Cheng, *Period lengths of continued fractions involving Fibonacci numbers*, Fibonacci Quart. **42** (2004), 161–169.

[27] R.A. Mollin, K. Cheng, B. Goddard, *Pellian polynomials and period lengths of continued fractions*, JP J. Algebra Number Theory Appl. **2** (2002), 47–67.

[28] R.A. Mollin, B. Goddard *A description of continued fraction expansions of quadratic surds represented by polynomials*, J. Number Theory **107** (2004), 228–240.

[29] M.B. Nathanson, *Polynomial Pell's equations*, Proc. Amer. Math. Soc. **86** (1976), 89—92.

[30] M. Nyberg, *Culminating and almost culminating continued fractions*, Norsk. Mat. Tidsskr. **31** (1949), 95–99, (na Norveškom)

[31] R. Patterson, *Creepers: Real Quadratic Orders with Large Class Number*, Ph.D. thesis,Macquarie University, Sydney, 2003.

[32] R. Patterson, A.J. van der Poorten, *Jeepers, Creepers, ...*, in High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Alf van der Poorten and Andreas Stein eds., Fields Institute Communications **42**, Amer. Math. Soc., 2004, 305-316.

[33] O. Perron, *Die Lehre von den Kettenbrüchen I*, Dritte ed., B.G.Teubner Verlagsgesellschaft m.b.H., Stuttgart, 1954.

[34] A.J. van der Poorten, *Beer and continued fractions with periodic periods*, Number Theory (Ottawa, ON, 1996), CRM Proc. Lecture Notes, Vol. 19, Amer. Math. Soc., Providence RI, 1999, 309–314.

[35] A.J. van der Poorten, *Reduction of continued fractions of formal power series*, Continued Fractions: From Analytic Number Theory to Constructive Approximation, (Columbia, MO, 1998), Contemp. Math. **236**, Amer. Math. Soc., Providence RI, 1999, pp. 343–355.

[36] A.J. van der Poorten, X.C. Tran, *Periodic continued fractions in elliptic function fields*, Algorithmic Number Theory (Proc. Fifth International Symposium, ANTS-V, Sydney, 2002) (C. Fieker, D.R. Kohel, eds.), Lect. Notes in Comput.Sci. **2369**, Springer, 2002, pp. 390–404.

[37] A.M.S. Ramasamy, *Polynomial solutions for the Pell's equation*, Indian J. Pure Appl. Math. **25** (1994), 577—581.

[38] A.M. Rockett, P. Szüsz, *Continued Fractions*, World Scientific Publishing Co.Pte.Ltd., 1992.

[39] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, Acta Arth. **6** (1961), 393–413.

[40] A. Schinzel, *On some problems of the arithmetical theory of continued fractions II*, Acta Arth. **7** (1962), 287–298.

[41] D. Shanks, *On Gauss's class number problems*, Math. Comp. **23** (1969), 151–163.

[42] D. Shanks, *Review of UMT file: Two related quadratic surds having continued fractions with exceptionally long periods*, Math. Comp. **28** (1974), 333–334.

[43] D. Shanks, *Systematic examination of Littlewood's bounds on* $L(1,\chi)$, Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence RI, 1973, 267–283.

[44] D. Shanks, *The infrastructure of a real quadratic number field and its applications*, Proc. Number Theory Conf. (Univ. of Colorado, Boulder), (1972), 217–224.

[45] R.G. Stanton, G. Sudler, H.C. Williams, *An upper bound for the period of the simple continued fraction for* $d^{1/2}$, Pacific J. Math. **67** (1976), 525–536.

[46] W.A. Webb, H. Yokota, *Polynomial Pell's equation*, Proc. Amer. Math. Soc. **131** (2003), 993—1006.

[47] W.A. Webb, H. Yokota, *Polynomial Pell's equation–II*, J. Number Theory **106** (2004), 128—141.

[48] H.C. Williams, *A note on the period length of the continued fraction expansion of certain* $\sqrt{d}$, Util. Math. **28** (1985), 201–209.

[49] H.C. Williams, *A numerical investigation into the length of the period of the continued fraction expansion of* $\sqrt{D}$, Math. Comp. **36** (1981), 593–601.

[50] H.C. Williams, *Some generalizations of the* S_n *sequence of Shanks*, Acta Arith. **69** (1995), 199-215.

[51] H.C. Williams, J. Broere, *A computational technique for evaluating* $L(1,\chi)$ *and the class number of a real quadratic field*, Math. Comp. **30** (1976), 887–893.

[52] K.S. Williams, N. Buck, *Comparision of the lengths of the continued fractions of* $\sqrt{D}$ *and* $\frac{1+\sqrt{D}}{2}$, Proc. Amer. Math. Soc. **120** (1994), No. 4, 995–1002.

[53] Y. Yamamoto, *Real quadratic number fields with large fundamental units*, Osaka J. Math. **8** (1971), 261–270.

[54] J. Yu, *Arithmetic of hyperelliptic curves*, Lecture Notes, Arizona Winter School 1999.

Sažetak

Verižni razlomci imaju mnoge primjene u teoriji brojeva. Poznato je da je razvoj u verižni razlomak kvadratne iracionalnosti periodan, ali je teško predvidjeti duljinu razvoja proizvoljnog broja.

U ovom radu su opisana osnovna svojstva verižnih razlomaka i njihova primjena, te je opisano nekoliko familija nizova brojeva kod kojih razvoj u verižni razlomak ima neka interesantna svojstva. Dane su i metode kako konstruirati takve nizove.

Na kraju su dokazane gornje ograde za duljinu perioda, te je dana veza s poznatom Riemannovom slutnjom.

Summary

Continued fractions have many applications in number theory. It has been known that continued fraction expansion of quadratic irrational is periodic, but it is hard to predict the length of expansion of arbitrary number.

In this work the basic properties of continued fractions and their applications are studied, and few families of sequences with some interesting properties of expansion are described. It is also shown how to construct such sequences.

At the end, an upper bound for the length of expansion is proven, and connection with famous Riemann hypothesis is shown.

Životopis

Rođen sam 4. svibnja 1979. godine u Vinkovcima. Nakon osnovne škole koju sam pohađao u Starim Mikanovcima, 1997. godine završavam prirodoslovno-matematički smjer gimnazije u Vinkovcima. Dodiplomski studij matematike upisao sam iste godine na Matematičkom odjelu Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Diplomiralo sam u listopadu 2003. godine na smjeru Računarstvo. Diplomski rad pod naslovom *Kongruentni brojevi i eliptičke krivulje* izradio sam pod vodstvom prof.dr.sc. Andreja Dujelle. Nakon toga sam upisao poslijediplomski znanstveni studij matematike na Matematičkom odjelu Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu.

Od 2008. godine zaposlen sam kao znanstveni novak na Matematičkom odjelu Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Član sam Seminara za teoriju brojeva i algebru. Imam objavljena dva znanstvena rada.