Diofantske aproksimacije i primjene

Andrej Dujella

Poslijediplomski kolegij 2011/2012

Sadržaj

1 Aproksimacija iracionalnih brojeva racionalnima **2**
- 1.1 Dirichletov teorem . . . 2
- 1.2 Fareyevi nizovi . . . 4
- 1.3 Verižni razlomci . . . 11
- 1.4 Verižni razlomci i aproksimacija iracionalnih brojeva racionalnima 16
- 1.5 Ekvivalentni brojevi . . . 24
- 1.6 Periodski verižni razlomci . . . 28
- 1.7 Pellova i pellovska jednadžba . . . 34

2 Simultane aproksimacije **40**
- 2.1 Dirichletov teorem o simultanim aproksimacijama . . . 40
- 2.2 Teoremi Blichfeldta i Minkowskog . . . 41
- 2.3 LLL algoritam . . . 46

3 Primjena diofantskih aproksimacija u kriptografiji **54**
- 3.1 Vrlo kratki uvod u kriptografiju . . . 54
- 3.2 RSA kriptosustav . . . 55
- 3.3 Wienerov napad na RSA kriptosustav . . . 57
- 3.4 Napadi na RSA koji koriste LLL algoritam . . . 60
- 3.5 Coppersmithov teorem . . . 62

4 Aproksimacija algebarskih brojeva **66**
- 4.1 Liouvilleov teorem . . . 66
- 4.2 Rothov teorem . . . 68
- 4.3 Thueova jednadžba . . . 71
- 4.4 Tzanakisova metoda za kvartične Thueove jednadžbe i nejednadžbe 74

5 Aproksimacija algebarskim brojevima **79**
- 5.1 Aproksimacija kvadratnim iracionalnostima . . . 79
- 5.2 Separacija korijena polinoma . . . 84

Poglavlje 1

Aproksimacija iracionalnih brojeva racionalnima

1.1 Dirichletov teorem

Za dani realni broj α, sa $\lfloor\alpha\rfloor$ označavat ćemo cjelobrojni dio od α ("pod" od α), tj. najveći cijeli broj $\leq \alpha$, a sa $\{\alpha\} = \alpha - \lfloor\alpha\rfloor$ razlomljeni dio od α. Nadalje, sa $\|\alpha\|$ označavat ćemo udaljenost od α do najbližeg cijelog broja, tj. $\|\alpha\| = \min(\{\alpha\}, 1 - \{\alpha\})$. Očito je $0 \leq \{\alpha\} < 1$ i $0 \leq \|\alpha\| \leq \frac{1}{2}$.

Teorem 1.1 (Dirichlet (1842))**.** *Neka su α i Q realni brojevi i $Q > 1$. Tada postoje cijeli brojevi p, q takvi da je $1 \leq q < Q$ i $\|\alpha q\| = |\alpha q - p| \leq \frac{1}{Q}$.*

Dokaz: Pretpostavimo najprije da je Q prirodan broj. Promotrimo sljedećih $Q + 1$ brojeva:

$$0, 1, \{\alpha\}, \{2\alpha\}, \ldots, \{(Q-1)\alpha\}.$$

Svi ovi brojevi leže u segmentu $[0, 1]$ i imaju oblik $r\alpha - s$, za neke cijele brojeve r i s ($0 = 0 \cdot \alpha - 0$, $1 = 0 \cdot \alpha - (-1)$, $\{i\alpha\} = i\alpha - \lfloor i\alpha\rfloor$). Podijelimo segment $[0, 1]$ na Q disjunktnih podintervala duljine $\frac{1}{Q}$:

$$[0, \frac{1}{Q}\rangle,\ [\frac{1}{Q}, \frac{2}{Q}\rangle,\ [\frac{2}{Q}, \frac{3}{Q}\rangle,\ \ldots,\ [\frac{Q-1}{Q}, 1].$$

Prema Dirichletovom principu, barem jedan podinterval sadrži dva (ili više) od gornjih $Q + 1$ brojeva. Uočimo da ta dva broja ne mogu biti 0 i 1. Stoga postoje cijeli brojevi r_1, r_2, s_1, s_2 takvi da je $0 \leq r_i < Q$, $i = 1, 2$, $r_1 \neq r_2$ i da vrijedi

$$|(r_1\alpha - s_1) - (r_2\alpha - s_2)| \leq \frac{1}{Q}.$$

Možemo pretpostaviti da je $r_1 > r_2$. Stavimo: $q = r_1 - r_2$, $p = s_1 - s_2$. Tada je $1 \leq q < Q$ i $|\alpha q - p| \leq \frac{1}{Q}$, čime je tvrdnja teorema dokazana u slučaju $Q \in \mathbb{N}$.

Pretpostavimo sada da Q nije prirodan broj. Neka je $Q' = \lfloor Q \rfloor + 1$. Prema prije dokazanom, postoje cijeli brojevi p, q takvi da je $1 \leq q < Q'$ i $|\alpha q - p| \leq \frac{1}{Q'}$. No sada je $|\alpha q - p| < \frac{1}{Q}$, a $1 \leq q < Q'$ povlači da je $1 \leq q \leq \lfloor Q \rfloor$, odnosno $1 \leq q < Q$. □

Korolar 1.1. *Ako je α iracionalan broj, onda postoji beskonačno mnogo parova p, q relativno prostih cijelih brojeva takvih da je*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{1.1}$$

Dokaz: Tvrdnja Teorema 1.1 očito vrijedi i ukoliko zahtjevamo da su p i q relativno prosti (uvjeti na p i q će ostati zadovoljeni i nakon što ih podijelimo s njihovih zajedničkim faktorom). Dakle, za $Q > 1$ postoje relativno prosti cijeli brojevi p, q takvi da je $|\alpha - \frac{p}{q}| \leq \frac{1}{Qq} < \frac{1}{q^2}$. Budući da je α iracionalan, to je $\alpha q - p \neq 0$.

Pretpostavimo da postoji samo konačno mnogo racionalanih brojeva $\frac{p}{q}$ koji zadovoljavaju (1.1). Neka su to brojevi $\frac{p_j}{q_j}$, $j = 1, \ldots, n$. Izaberimo prirodan broj m tako da je $\frac{1}{m} < |\alpha q_j - p_j|$ za sve $j = 1, \ldots, n$. Primijenimo sada Teorem 1.1 uz $Q = m$, pa dobivamo racionalan broj $\frac{p}{q}$ koji zadovoljava (1.1) i za koji vrijedi $|\alpha q - p| \leq \frac{1}{m}$. Prema tome, $\frac{p}{q}$ je različit od $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$, što je kontradikcija. □

Napomena 1.1. Tvrdnja Korolara 1.1 ne vrijedi ako je α racionalan. Zaista, neka je $\alpha = \frac{u}{v}$. Ako je $\frac{p}{q} \neq \alpha$, onda je

$$|\alpha - \frac{p}{q}| = |\frac{u}{v} - \frac{p}{q}| = |\frac{uq - vp}{vq}| \geq \frac{1}{vq}, \tag{1.2}$$

pa (1.1) povlači da je $q < v$. To znači da (1.1) može biti zadovoljeno samo za konačno parova p, q relativno prostih cijelih brojeva.

Primjer 1.1. *Dokažimo da je broj $e = \sum_{i=0}^{\infty} \frac{1}{i!}$ iracionalan.*

Rješenje: Pretpostavimo da je $e = \frac{u}{v}$ racionalan broj. Uzmimo prirodan broj $n > v$, te definirajmo $\frac{p}{q} = \sum_{i=0}^{n} \frac{1}{i!}$, gdje je $q = n!$. Tada je prema (1.2)

$$\begin{aligned} \frac{1}{v} \leq q|e - \frac{p}{q}| &= n! \sum_{j=1}^{\infty} \frac{1}{(n+j)!} < n! \sum_{k=0}^{\infty} \frac{1}{(n+1)!} \cdot \frac{1}{(n+1)^k} \\ &\leq \frac{1}{n+1} \cdot \frac{1}{1 - \frac{1}{n+1}} = \frac{1}{n}, \end{aligned}$$

što je u kontradikciji s pretpostavkom da je $n > v$. ♢

1.2 Fareyevi nizovi

Definicija 1.1. *Neka je $n \in \mathbb{N}$.* Fareyev niz $\mathcal{F}_n$ *reda n je niz svih racionalnih brojeva $\frac{h}{k}$, gdje su h i k cijeli brojevi takvi da je $0 \leq h \leq k \leq n$ i $\operatorname{nzd}(h,k) = 1$, zapisanih u rastućem redosljedu.*

Npr. niz $\mathcal{F}_5$ izgleda ovako:

$$0,\ \frac{1}{5},\ \frac{1}{4},\ \frac{1}{3},\ \frac{2}{5},\ \frac{1}{2},\ \frac{3}{5},\ \frac{2}{3},\ \frac{3}{4},\ \frac{4}{5},\ 1.$$

Broj elemenata u nizu $\mathcal{F}_n$ je jednak $1+\varphi(1)+\varphi(2)+\cdots+\varphi(n)$, gdje je φ Eulerova funkcija, tj. $\varphi(n)$ je broj brojeva u nizu $1, 2, \ldots, n$ koji su relativno prosti s n. Može se pokazati da je ova suma asimptotski jednaka $\frac{3}{\pi^2}n^2$.

Teorem 1.2. *Ako su $\frac{h}{k}$ i $\frac{h'}{k'}$ dva uzastopna elementa Fareyevog niza $\mathcal{F}_n$, onda je $h'k - hk' = 1$.*

Lema 1.1. *Neka su $X = (x_1, x_2)$ i $Y = (y_1, y_2)$ cjelobrojne točke u ravnini, takve da $O = (0,0)$, X i Y ne leže na istom pravcu. Pretpostavimo da zatvoreni trokut $\mathcal{T}$ s vrhovima O, X, Y ne sadrži niti jednu cjelobrojnu točku, osim svojih vrhova. Tada je*

$$|x_1y_2 - x_2y_1| = 1.$$

Dokaz: Neka je $\mathcal{P}$ paralelogram s vrhovima $O, X, Y, X+Y$. Tada $\mathcal{P}$ ne sadrži niti jednu cjelobrojnu točku, osim svojih vrhova. Zaista, pretpostavimo da je Z cjelobrojna točka u $\mathcal{P}$. Budući da $Z \notin \mathcal{T}$, to je $X+Y-Z \in \mathcal{T}$. Stoga je $X+Y-Z = O$, X ili Y, pa je $Z = X+Y$, Y ili X, što je i trebalo pokazati.

Proizvoljnu cjelobrojnu točku R možemo zapisati u obliku $R = \lambda X + \mu Y$ s realnim koeficijentima λ, μ, zato što O, X, Y nisu kolinearne. Sada je $R = R' + R''$, gdje je

$$R' = \lfloor\lambda\rfloor X + \lfloor\mu\rfloor Y \quad \text{i} \quad R'' = \{\lambda\}X + \{\mu\}Y.$$

Budući da su R i R' cjelobrojne, to je i R'' cjelobrojna. Također je $R'' \in \mathcal{P}$ ($\mathcal{P}$ je upravo skup svih točaka oblika $\alpha X + \beta Y$, $0 \leq \alpha, \beta \leq 1$). Kako je $R'' \neq X, Y, X+Y$, zaključujemo da je $R'' = O$. Prema tome, $R = \lambda X + \mu Y$, gdje su $\lambda, \mu \in \mathbb{Z}$.

Posebno je

$$\begin{aligned}(1,0) &= \lambda X + \mu Y = (\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2),\\ (0,1) &= \lambda' X + \mu' Y = (\lambda' x_1 + \mu' y_1, \lambda' x_2 + \mu' y_2)\end{aligned}$$

za neke $\lambda, \mu, \lambda', \mu' \in \mathbb{Z}$. Odavde slijedi da je

$$1 = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = \begin{vmatrix} \lambda & \mu \\ \lambda' & \mu' \end{vmatrix} \cdot \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix},$$

pa je $\begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} = \pm 1$, što se i tvrdilo. □

Dokaz Teorema 1.2: Neka je $X = (h, k)$, $Y = (h', k')$. Tada točke O, X, Y nisu kolinearne budući da je $\text{nzd}(h, k) = \text{nzd}(h', k') = 1$ i $X \neq Y$. Označimo s $\mathcal{T}$ trokut s vrhovima O, X, Y. Tada $\mathcal{T}$ ne sadrži niti jednu cjelobrojnu točku, osim O, X, Y. Zaista, ako bi postojala takva točka (h'', k''), onda bi također postojala i takva točka koja zadovoljava i dodatni zahtjev $\text{nzd}(h'', k'') = 1$. Tada bi vrijedilo

$$(h'', k'') = \lambda(h, k) + \mu(h', k'), \quad \text{uz} \quad \lambda, \mu \geq 0,\ 0 < \lambda + \mu \leq 1,\ (\lambda, \mu) \neq (1, 0), (0, 1).$$

Ovo povlači da je $k'' \leq \lambda n + \mu n \leq n$, pa $\frac{h''}{k''}$ pripada nizu $\mathcal{F}_n$. Nadalje, jer je $\text{nzd}(h, k) = \text{nzd}(h', k') = 1$, imamo da je $\lambda > 0$, $\mu > 0$, što povlači da je $\frac{h}{k} < \frac{h''}{k''} < \frac{h'}{k'}$. Dakle, dobili smo kontradikciju s pretpostavkom da su $\frac{h}{k}$ i $\frac{h'}{k'}$ uzastopni elementi niza $\mathcal{F}_n$.

Prema tome, zadovoljene su sve pretpostavke Leme 1.1, pa zaključujemo da je $|h'k - hk'| = 1$, a budući da je $\frac{h}{k} < \frac{h'}{k'}$, dobivamo konačno $h'k - hk' = 1$. □

Korolar 1.2. *Ako su $\frac{h}{k}$, $\frac{h''}{k''}$, $\frac{h'}{k'}$ tri uzastopna elementa niza $\mathcal{F}_n$, onda je*

$$\frac{h''}{k''} = \frac{h + h'}{k + k'}.$$

Dokaz: Prema Teoremu 1.2 je $h''k - hk'' = 1$ i $h'k'' - h''k' = 1$. Oduzimanjem dobivamo $h''(k + k') - k''(h + h') = 0$, odnosno $\frac{h''}{k''} = \frac{h+h'}{k+k'}$. □

Lema 1.2. *Neka su $\frac{h}{k}$, $\frac{h'}{k'}$ dva uzastopna elementa niza $\mathcal{F}_n$. Stavimo $h'' = h + h'$, $k'' = k + k'$ (uočimo da $\frac{h''}{k''} \notin \mathcal{F}_n$). Tada za svaki realan broj α, takav da je $\frac{h}{k} \leq \alpha \leq \frac{h'}{k'}$, vrijedi barem jedna od sljedeće tri nejednakosti:*

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{\sqrt{5}k^2}, \quad \left|\alpha - \frac{h''}{k''}\right| < \frac{1}{\sqrt{5}k''^2}, \quad \left|\alpha - \frac{h'}{k'}\right| < \frac{1}{\sqrt{5}k'^2}. \tag{1.3}$$

Dokaz: Bez smanjenja općenitosti možemo pretpostaviti da je $\alpha \geq \frac{h''}{k''}$. Naime, u protivnom zamijenimo α sa $1 - \alpha$, $\frac{h}{k}$ sa $1 - \frac{h}{k}$, itd. Ako niti jedna od nejednakosti u (1.3) nije ispunjena, onda je

$$\alpha - \frac{h}{k} \geq \frac{1}{\sqrt{5}k^2}, \quad \alpha - \frac{h''}{k''} \geq \frac{1}{\sqrt{5}k''^2}, \quad \frac{h'}{k'} - \alpha \geq \frac{1}{\sqrt{5}k'^2}.$$

Zbrajanjem prve i treće nejednakosti dobivamo

$$\frac{h'}{k'} - \frac{h}{k} = \frac{1}{kk'} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{k^2} + \frac{1}{k'^2}\right),$$

dok zbrajanjem druge i treće nejednakosti dobivamo

$$\frac{h'}{k'} - \frac{h''}{k''} = \frac{h'(k + k') - k'(h + h')}{k'k''} = \frac{1}{k'k''} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{k'^2} + \frac{1}{k''^2}\right).$$

Prema tome, $\sqrt{5}kk' \geq k^2+k'^2$ i $\sqrt{5}k'k'' \geq k'^2+k''^2$, tako da je $\sqrt{5}k'(k+k'') \geq k^2+2k'^2+k''^2$ i stoga $\sqrt{5}k'(2k+k') \geq 2k^2+3k'^2+2kk'$. Odavde slijedi da je

$$0 \geq \frac{1}{2}(2k-(\sqrt{5}-1)k')^2,$$

što je nemoguće budući da su k i k' prirodni brojevi. □

Lema 1.3. *Neka je α iracionalan broj i r prirodan broj. Tada postoji $n_0 \in \mathbb{N}$ takav da za sve $n \geq n_0$ dva susjedna elementa od $\mathcal{F}_n$ između kojih se nalazi α imaju nazivnike veće od r.*

Dokaz: Neka su $m_1, m_2, \ldots, m_r$ cijeli brojevi koji su najbliži brojevima $\alpha, 2\alpha, \ldots, r\alpha$, tj. $m_j = \lfloor j\alpha + \frac{1}{2} \rfloor$, $j = 1, \ldots, r$. Odaberimo n_0 tako da je

$$\frac{1}{n_0} < \left|\alpha - \frac{m_j}{j}\right|,$$

za sve $j = 1, \ldots, r$. Ako je $q \in \mathbb{Z}$, tada za svaki $j = 1, \ldots, r$ vrijedi:

$$|j\alpha - m_j| \leq |j\alpha - q| \Rightarrow \left|\alpha - \frac{m_j}{j}\right| \leq \left|\alpha - \frac{q}{j}\right| \Rightarrow \frac{1}{n_0} < \left|\alpha - \frac{q}{j}\right|. \qquad (1.4)$$

Neka je $n \geq n_0$, te neka su $\frac{h}{k}$ i $\frac{h'}{k'}$ susjedni elementi od $\mathcal{F}_n$ takvi da je $\frac{h}{k} < \alpha < \frac{h'}{k'}$. Udaljenost susjednih elemenata od $\mathcal{F}_n$ je $\leq \frac{1}{n}$, pa vrijedi

$$\left|\alpha - \frac{h}{k}\right| < \left|\frac{h'}{k'} - \frac{h}{k}\right| \leq \frac{1}{n}, \quad \left|\alpha - \frac{h'}{k'}\right| < \left|\frac{h}{k} - \frac{h'}{k'}\right| \leq \frac{1}{n}.$$

Usporedimo li ovo s (1.4), zaključujemo da je $k > r$ i $k' > r$, što je i trebalo dokazati. □

Lema 1.4. *Neka je α iracionalan broj koji je korijen polinoma*

$$P(X) = aX^2 + bX + c, \quad a \neq 0,$$

s cjelobrojnim koeficijentima i diskriminantom $D = b^2 - 4ac > 0$. Tada za $A > \sqrt{D}$ nejednadžba $|\alpha - \frac{p}{q}| < \frac{1}{Aq^2}$ ima samo konačno mnogo rješenja.

Dokaz: Zapišimo $P(X)$ u obliku $P(X) = a(X-\alpha)(X-\alpha')$. Tada je $D = a^2(\alpha-\alpha')^2$. Ako je $|\alpha - \frac{p}{q}| < \frac{1}{Aq^2}$, onda imamo:

$$\frac{1}{q^2} \leq \left|P(\frac{p}{q})\right| = \left|\alpha - \frac{p}{q}\right| \cdot \left|a(\alpha' - \frac{p}{q})\right| < \frac{1}{Aq^2}\left|a((\alpha'-\alpha) + (\alpha - \frac{p}{q}))\right| < \frac{\sqrt{D}}{Aq^2} + \frac{|a|}{A^2q^4}.$$

Odavde je, zbog $A > \sqrt{D}$,

$$q^2 < \frac{|a|}{A^2(1 - \frac{\sqrt{D}}{A})},$$

što očito ima samo konačno mnogo rješenja. □

Teorem 1.3 (Hurwitz (1891))**.**

(i) Za svaki iracionalan broj α postoji beskonačno mnogo različitih racionalnih brojeva $\frac{p}{q}$ takvih da je

$$|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}\,. \tag{1.5}$$

(ii) Tvrdnja (i) ne vrijedi ako se $\sqrt{5}$ zamijeni s bilo kojom konstantom $A > \sqrt{5}$.

Dokaz:

(i) Možemo pretpostaviti da je $0 < \alpha < 1$. Ako su $\frac{h}{k}$ i $\frac{h'}{k'}$ uzastopni elementi u Fareyevom nizu $\mathcal{F}_n$ takvi da je $\frac{h}{k} < \alpha < \frac{h'}{k'}$ i ako je $h'' = h + h'$, $k'' = k + k'$, onda prema Lemi 1.2 barem jedan od brojeva $\frac{h}{k}$, $\frac{h'}{k'}$, $\frac{h''}{k''}$ zadovoljava (1.5).

Pretpostavimo sada da nejednadžba (1.5) ima samo konačno mnogo rješenja $\frac{p}{q}$ i neka je r najveći nazivnik koji se pojavljuje u tim rješenjima. Tada Lema 1.3 osigurava da, za dovoljno veliki n, susjedni elementi $\frac{h}{k}$ i $\frac{h'}{k'}$ niza $\mathcal{F}_n$ između kojih se nalazi α imaju nazivnike veće od r. Postoji rješenje $\frac{p}{q}$ od (1.5) koje je jedan od brojeva $\frac{h}{k}$, $\frac{h'}{k'}$, $\frac{h''}{k''}$. Razlomci $\frac{h}{k}$ i $\frac{h'}{k'}$ su skraćeni po definiciji Fareyevih nizova, a $\frac{h+h'}{k+k'}$ je također skraćen jer je $h'(k + k') - k'(h + h') = h'k - hk' = 1$. Dakle, ovo rješenje ima nazivnik veći od r, što je kontradikcija.

(ii) Tvdnja (ii) slijedi iz Leme 1.4 za $\alpha = \frac{\sqrt{5}-1}{2}$, budući da je tada $P(X) = X^2 + X - 1$ i $D = 5$.

□

Nejednakost (1.5) može se zapisati u obliku

$$-\frac{1}{\sqrt{5}q^2} < \alpha - \frac{p}{q} < \frac{1}{\sqrt{5}q^2}\,,$$

tako da je interval u kojem se nalaze brojevi $\frac{p}{q}$ simetričan u odnosu na α.

Teorem 1.4 (Segre (1945), Niven (1962))**.** *Neka je α iracionalan broj i $\tau \geq 0$. Tada postoji beskonačno mnogo racionalnih brojeva $\frac{p}{q}$ takvih da je*

$$-\frac{1}{\sqrt{1+4\tau}q^2} < \alpha - \frac{p}{q} < \frac{\tau}{\sqrt{1+4\tau}q^2}\,. \tag{1.6}$$

Nadalje, tvrdnja vrijedi i ako se u (1.6) $\alpha - \frac{p}{q}$ zamijeni s $\frac{p}{q} - \alpha$.

Za $\tau = 1$ dobivamo upravo Hurwitzov teorem. Primijetimo također da drugi dio teorema slijedi primjenom prvog dijela na broj $-\alpha$.

Lema 1.5. *Neka je α iracionalan broj i $\tau \geq 0$. Neka su $\frac{a}{b}$ i $\frac{c}{d}$ racionalni brojevi s pozitivnim nazivnicima takvi da je $bc - ad = 1$ i*

$$\frac{a}{b} < \frac{a+c}{b+d} < \alpha < \frac{c}{d}.$$

Tada barem jedan od brojeva $\frac{a}{b}$, $\frac{a+c}{b+d}$, $\frac{c}{d}$ zadovoljava relaciju (1.6).

Dokaz: Neka je $\lambda = \frac{1}{\sqrt{1+4\tau}}$, $\mu = \frac{\tau}{\sqrt{1+4\tau}}$. Tada je $0 < \lambda \leq 1$ i $\mu = \frac{1-\lambda^2}{4\lambda}$. Pretpostavimo da tvrdnja leme ne vrijedi. Tada je

$$\alpha - \frac{p}{q} \geq \frac{\mu}{b^2}, \quad \alpha - \frac{a+c}{b+d} \geq \frac{\mu}{(b+d)^2}, \quad \frac{c}{d} - \alpha \geq \frac{\lambda}{d^2}. \tag{1.7}$$

Zbrajanjem prve i treće, te druge i treće nejednakosti, dobivamo

$$\frac{c}{d} - \frac{a}{b} = \frac{1}{bd} \geq \frac{\mu}{b^2} + \frac{\lambda}{d^2}, \quad \frac{c}{d} - \frac{a+c}{b+d} = \frac{1}{d(b+d)} \geq \frac{\mu}{(b+d)^2} + \frac{\lambda}{d^2},$$

odnosno

$$\lambda b^2 - bd + \mu d^2 \leq 0, \quad \lambda(b+d)^2 - d(b+d) + \mu d^2 \leq 0. \tag{1.8}$$

Zbrajanjem ovih dviju nejednakosti dobivamo

$$2\lambda b^2 + (2\lambda - 2)bd + (\lambda + 2\mu - 1)d^2 \leq 0. \tag{1.9}$$

Ova kvadratna forma u b i d ima diskriminantu

$$D = 4(\lambda-1)^2 - 8\lambda(\lambda + 2\mu - 1) = -4(\lambda^2 + 4\lambda\mu - 1) = 0.$$

Odavde slijedi da (1.9) možemo zapisati u obliku

$$\frac{1}{2\lambda}(2\lambda b + (\lambda - 1)d)^2 \leq 0.$$

Budući da u posljednjoj relaciji mora vrijediti jednakost, zaključujemo da jednakost mora vrijediti i u relacijama (1.9), (1.8) i (1.7). Nadalje, vidimo da je $2\lambda b + (\lambda - 1)d = 0$, što povlači da je broj $\lambda = \frac{d}{d+2b}$ racionalan. No, sada relacija $\frac{c}{d} - \alpha = \frac{\lambda}{d^2}$ povlači da je i α racionalan, što je kontradikcija. □

Dokaz Teorema 1.4: Neka su $\frac{a_1}{b_1}$ i $\frac{c_1}{d_1}$ dva susjedna elementa Fareyevog niza $\mathcal{F}_n$ između kojih se nalazi α. Tada je po Teoremu 1.2 $b_1c_1 - a_1d_1 = 1$. Ako vrijedi

$$\frac{a_1}{b_1} < \frac{a_1+c_1}{b_1+d_1} < \alpha < \frac{c_1}{d_1},$$

onda primijenimo Lemu 1.5 na racionalne brojeve $\frac{a_1}{b_1}$ i $\frac{c_1}{d_1}$, te dobivamo jedno rješenje od (1.6). Ako je pak

$$\frac{a_1}{b_1} < \alpha < \frac{a_1 + c_1}{b_1 + d_1} < \frac{c_1}{d_1},$$

označimo s j prirodan broj takav da je

$$\frac{a_1}{b_1} < \frac{(j+1)a_1 + c_1}{(j+1)b_1 + d_1} < \alpha < \frac{ja_1 + c_1}{jb_1 + d_1}.$$

Takav j se sigurno može naći jer je $\lim_{j\to\infty} \frac{ja_1+c_1}{jb_1+d_1} = \frac{a_1}{b_1}$. Sada možemo primijeniti Lemu 1.5 na racionalne brojeve $\frac{a_1}{b_1}$ i $\frac{ja_1+c_1}{jb_1+d_1}$. Uvjet $bc - ad = 1$ iz leme je zadovoljen budući da je

$$b_1(ja_1 + c_1) - a_1(jb_1 + d_1) = b_1c_1 - a_1d_1 = 1.$$

Tako smo i u ovom slučaju dobili jedno rješenje od (1.6).

Neka je $\frac{h_1}{k_1}$ jedno rješenje od (1.6). Prema Lemi 1.3, odaberimo n tako velik da dva susjedna elementa od $\mathcal{F}_n$ između kojih se nalazi α imaju nazivnike veće od k_1. Neka su $\frac{a_2}{b_2}$ i $\frac{c_2}{d_2}$ elementi niza $\mathcal{F}_n$ takvi da je

$$\frac{a_2}{b_2} < \alpha < \frac{c_2}{d_2}.$$

Sada na njih ponovimo prethodno razmatranje. Dakle, ako je

$$\frac{a_2}{b_2} < \frac{a_2 + c_2}{b_2 + d_2} < \alpha < \frac{c_2}{d_2},$$

onda primijenimo Lemu 1.5 direktno. U protivnom, izaberemo j tako da vrijedi

$$\frac{a_2}{b_2} < \frac{(j+1)a_2 + c_2}{(j+1)b_2 + d_2} < \alpha < \frac{ja_2 + c_2}{jb_2 + d_2}.$$

U jednom ili drugom slučaju, dobivamo rješenje $\frac{h_2}{k_2}$ od (1.6), gdje je k_2 jedan od brojeva:

$$b_2,\ d_2,\ b_2 + d_2,\ jb_2 + d_2,\ (j+1)b_2 + d_2.$$

Lako se vidi da su svi razlomci u prethodnim nejednakostima skraćeni. Npr.

$$b_2(ja_2 + c_2) - a_2(jb_2 + d_2) = b_2c_2 - a_2d_2 = 1$$

povlači da je $\mathrm{nzd}(ja_2 + c_2, jb_2 + d_2) = 1$. Prema tome, rješenje $\frac{h_2}{k_2}$ od (1.6) je različito od $\frac{h_1}{k_1}$. Budući da ovaj proces možemo nastaviti neograničeno, teorem je dokazan. □

Za $\tau = 0$ u Segreovom teoremu dobivamo

Korolar 1.3. *Neka je α iracionalan broj. Tada postoji beskonačno mnogo racionalnih brojeva $\frac{p}{q}$ takvih da je*

$$-\frac{1}{q^2} < \alpha - \frac{p}{q} < 0,$$

te beskonačno mnogo racionalnih brojeva $\frac{p}{q}$ takvih da je

$$0 < \alpha - \frac{p}{q} < \frac{1}{q^2}.$$

1.3 Verižni razlomci

Definirat ćemo polinome $p_0, q_0, p_1, q_1, p_2, q_2, \ldots$, takve da su p_n, q_n polinomi u varijablama $a_0, a_1, \ldots, a_n$. Najprije definiramo $p_0 = a_0$, $q_0 = 1$. Zatim, pretpostavimo da su $p_0, q_0, \ldots, p_{n-1}, q_{n-1}$ već definirani. Uz oznake $p'_k = p_k(a_1, a_2, \ldots, a_{k+1})$, $q'_k = q_k(a_1, a_2, \ldots, a_{k+1})$, definiramo

$$p_n = a_0 p'_{n-1} + q'_{n-1}, \quad q_n = p'_{n-1}.$$

Sada je $\frac{p_n}{q_n}$ racionalna funkcija od $a_0, a_1, \ldots, a_n$, i pisat ćemo

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n].$$

Specijalno je $[a_0] = \frac{p_0}{q_0} = a_0$. Za $n > 0$ imamo

$$[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n} = \frac{a_0 p'_{n-1} + q'_{n-1}}{p'_{n-1}} = a_0 + \frac{1}{p'_{n-1}/q'_{n-1}} = a_0 + \frac{1}{[a_1, \ldots, a_n]}.$$

Ponavljanjem ovog postupka, dobivamo

$$[a_0, a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}. \tag{1.10}$$

Racionalne funkcije ovog oblika nazivaju se *verižni ili neprekidni razlomci.*

Lema 1.6. *Za $n \geq 2$ vrijedi*

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}.$$

Dokaz: Za $n = 2$ tvrdnja se provjerava direktno. Pretpostavimo da je $n > 2$ i da tvrdnja vrijedi za $n - 1$. Tada je

$$p'_{n-1} = a_n p'_{n-2} + p'_{n-3}, \quad q'_{n-1} = a_n q'_{n-2} + q'_{n-3},$$

pa dobivamo

$$\begin{aligned} p_n &= a_0(a_n p'_{n-2} + p'_{n-3}) + (a_n q'_{n-2} + q'_{n-3}) \\ &= a_n(a_0 p'_{n-2} + q'_{n-2}) + (a_0 p'_{n-3} + q'_{n-3}) = a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n p'_{n-2} + p_{n-3} = a_n q_{n-1} + q_{n-2}. \end{aligned}$$

□

Dogovorno uzimamo da je $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, $q_{-1} = 0$. Lako se provjerava da uz ovaj dogovor Lema 1.6 vrijedi za sve $n \geq 0$.

Lema 1.7. *Za $k = 1, \ldots, n$, neka je $r_k = [a_k, a_{k+1}, \ldots, a_n]$. Tada je*

$$[a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_{k-1}, [a_k, a_{k+1}, \ldots, a_n]] = \frac{p_{k-1}r_k + p_{k-2}}{q_{k-1}r_k + q_{k-2}}.$$

Dokaz: Druga jednakost slijedi direktno iz Leme 1.6. Prvu jednakost ćemo dokazati indukcijom po k. Za $k = 1$ tvrdnja leme je točna budući da je

$$[a_0, a_1, \ldots, a_n] = a_0 + \frac{1}{[a_1, \ldots, a_n]} = [a_0, [a_1, \ldots, a_n]].$$

Pretpostavimo sada da tvrdnja leme vrijedi da $k-1$, gdje je $1 < k \leq n$. Tada je

$$\begin{aligned}[a_0, a_1, \ldots, a_n] &= a_0 + \frac{1}{[a_1, \ldots, a_n]} = a_0 + \frac{1}{[a_1, \ldots, a_{k-1}, [a_k, \ldots, a_n]]} \\ &= [a_0, a_1, \ldots, a_{k-1}, [a_k, \ldots, a_n]].\end{aligned}$$

□

Lema 1.8. *Za $n \geq -1$ vrijedi: $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$.*

Dokaz: Lemu dokazujemo indukcijom. Za $n = -1$ imamo: $q_{-1}p_{-2} - p_{-1}q_{-2} = 0 \cdot 0 - 1 \cdot 1 = (-1)^{-1}$. Pretpostavimo da tvrdnja vrijedi za $n-1$. Tada je

$$\begin{aligned}q_n p_{n-1} - p_n q_{n-1} &= (a_n q_{n-1} + q_{n-2})p_{n-1} - (a_n p_{n-1} + p_{n-2})q_{n-1} \\ &= -(q_{n-1}p_{n-2} - p_{n-1}q_{n-2}) = -(-1)^{n-1} = (-1)^n.\end{aligned}$$

□

Lema 1.9. *Za $n \geq 0$ vrijedi: $q_n p_{n-2} - p_n q_{n-2} = (-1)^{n-1} a_n$.*

Dokaz: Iz Lema 1.6 i 1.8 slijedi

$$\begin{aligned}q_n p_{n-2} - p_n q_{n-2} &= (a_n q_{n-1} + q_{n-2})p_{n-2} - (a_n p_{n-1} + p_{n-2})q_{n-2} \\ &= a_n(q_{n-1}p_{n-2} - p_{n-1}q_{n-2}) = (-1)^{n-1}a_n.\end{aligned}$$

□

Lema 1.10. *Neka je $\alpha = [a_0, a_1, \ldots, a_{n+1}]$. Tada je*

$$q_n \alpha - p_n = \frac{(-1)^n}{a_{n+1}q_n + q_{n-1}}.$$

Dokaz: Prema Lemama 1.6 i 1.8 je

$$q_n \alpha - p_n = q_n \frac{p_{n+1}}{q_{n+1}} - p_n = \frac{-(q_{n+1}p_n - p_{n+1}q_n)}{q_{n+1}} = \frac{(-1)^n}{a_{n+1}q_n + q_{n-1}}.$$

□

Lema 1.11. *Za $n \geq 1$ vrijedi*

$$\frac{q_n}{q_{n-1}} = [a_n, a_{n-1}, \ldots, a_1].$$

Dokaz: Lemu ćemo dokazati indukcijom. Za $n = 1$ imamo $\frac{q_1}{q_0} = \frac{a_1}{1} = [a_1]$. Pretpostavimo da tvrdnja vrijedi za $n - 1$. Tada je

$$\begin{aligned}\frac{q_n}{q_{n-1}} &= \frac{a_n q_{n-1} + q_{n-2}}{q_{n-1}} = a_n + \frac{1}{q_{n-1}/q_{n-2}} = a_n + \frac{1}{[a_{n-1}, \ldots, a_1]} \\ &= [a_n, a_{n-1}, \ldots, a_1].\end{aligned}$$

□

Lema 1.12. *Neka su $a_0, a_1, a_2, \ldots$ realni brojevi, te neka su $a_1, a_2, \ldots$ pozitivni. Tada vrijedi*

1) $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots$,

2) $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \cdots$,

3) Ako je n paran, a m neparan, onda je $\frac{p_n}{q_n} < \frac{p_m}{q_m}$.

Dokaz: Prema Lemi 1.9 je

$$\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} = \frac{(-1)^{n-1} a_n}{q_n q_{n-2}}.$$

Primijenimo li ovo za n paran, $n \geq 2$, dobivamo $\frac{p_{n-2}}{q_{n-2}} < \frac{p_n}{q_n}$, a za n neparan, $n \geq 3$, dobivamo $\frac{p_{n-2}}{q_{n-2}} > \frac{p_n}{q_n}$.

Preostaje dokazati tvrdnju 3). Neka je $n < m$. Budući da je $\frac{p_n}{q_n} \leq \frac{p_{m-1}}{q_{m-1}}$, dovoljno je dokazati da je $\frac{p_{m-1}}{q_{m-1}} < \frac{p_m}{q_m}$. No, zadnja nejednakost je točna jer je, po Lemi 1.8, $q_m p_{m-1} - p_m q_{m-1} = (-1)^m = -1 < 0$. Slučaj $n > m$ se dokazuje sasvim analogno. □

Lema 1.13. *Neka je a_0 cijeli broj, te $a_1, \ldots, a_n$ prirodni brojevi. Tada je $[a_0, a_1, \ldots, a_n]$ racionalan broj. Obrnuto, za dani racionalan broj $\frac{u}{v}$ postoji $n \geq 0$ i brojevi $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_n \in \mathbb{N}$ tako da je*

$$\frac{u}{v} = [a_0, a_1, \ldots, a_n]. \tag{1.11}$$

Nadalje, ako je $\frac{u}{v} \geq 1$, onda je $a_0 \geq 1$.

Dokaz: Treba dokazati samo drugi dio leme. Bez smanjenja općenitosti možemo pretpostaviti da je $v > 0$ i $\mathrm{nzd}(u, v) = 1$. Dokaz provodimo indukcijom po v. Ako je $v = 1$, onda je $\frac{u}{v}$ cijeli broj, pa imamo $\frac{u}{v} = [a_0]$ uz $a_0 = \frac{u}{v}$. Pretpostavimo sada da je $v > 1$. Tada postoje cijeli brojevi q, r takvi da je $u = vq + r$, $1 \leq r < v$. Po pretpostavci indukcije, $\frac{v}{r}$ možemo zapisati kao

verižni razlomak, recimo $\frac{v}{r} = [a_1, \ldots, a_n]$. Budući da je $\frac{v}{r} > 1$, to su brojevi $a_1, \ldots, a_n$ prirodni. Stoga je

$$\frac{u}{v} = q + \frac{1}{v/r} = q + \frac{1}{[a_1, \ldots, a_n]} = [q, a_1, \ldots, a_n]$$

i (1.11) vrijedi uz $a_0 = q$. Jasno je da ako je $\frac{u}{v} \geq 1$, onda je $a_0 = q \geq 1$, čime je dokaz dovršen. □

Definicija 1.2. *Ako je a_0 cijeli broj, $a_1, \ldots, a_n$ prirodni brojevi, te ako je $r = [a_0, a_1, \ldots, a_n]$, onda ovaj izraz zovemo razvoj broja r u* konačni jednostavni verižni (neprekidni) razlomak*; $\frac{p_i}{q_i}$ je i-ta* konvergenta *od r, a_i je i-ti* parcijalni kvocijent *od r, a $r_i = [a_i, a_{i+1}, \ldots, a_n]$ je i-ti* potpuni kvocijent *od r.*

Uočimo da je razlomak $\frac{p_i}{q_i}$ skraćen (tj. $\text{nzd}(p_i, q_i) = 1$), prema Lemi 1.8.

Lema 1.14.

(i) Ako je r cijeli broj, onda postoje točno dva razvoja od r u jednostavni verižni razlomak: $r = [r]$ i $r = [r-1, 1]$.

(ii) Ako je r racionalan broj, ali nije cijeli, onda r ima točno dva razvoja u jednostavni verižni razlomak: jedan je oblika $[a_0, a_1, \ldots, a_n]$ uz $a_n \geq 2$, a drugi je oblika $[a_0, a_1, \ldots, a_{n-1}, a_n - 1, 1]$.

Dokaz: U oba slučaja, r je racionalan broj, pa po Lemi 1.13 ima razvoj u jednostavni verižni razlomak

$$r = [a_0, a_1, \ldots, a_n],$$

gdje je a_0 cijeli, a $a_1, \ldots, a_n$ prirodni brojevi.

Pretpostavimo da je r cijeli broj. Ako je $n = 0$, onda je $r = [a_0] = a_0$, pa je $r = [r]$. Ako je $n > 0$, onda je

$$r = a_0 + \frac{1}{[a_1, \ldots, a_n]}$$

i $[a_1, \ldots, a_n] \geq 1$. Budući da je $r - a_0 \in \mathbb{Z}$, to je $[a_1, \ldots, a_n] = 1$. Budući da je $a_1 \geq 1$, zaključujemo da je $n = 1$ i $a_1 = 1$. Tada je $a_0 = r - 1$ i $r = [r-1, 1]$, pa smo dokazali (i).

Pretpostavimo sada da je $r = \frac{u}{v}$, $\text{nzd}(u, v) = 1$ i $v > 0$. Tvrdnju (ii) ćemo dokazati indukcijom po v. Slučaj $v = 1$ je dokazan u (i). Ako je $v > 1$, onda je a_0 u razvoju od $\frac{u}{v}$ jednoznačno određen: to je cjelobrojni dio od $\frac{u}{v}$. Imamo:

$$\frac{u}{v} = a_0 + \frac{u_1}{v},$$

gdje je $\alpha_1 = \frac{v}{u_1}$ ima nazivnik manji od v. Stoga, po pretpostavci indukcije, α_1 ima točno dva razvoja u jednostavni verižni razlomak: oblika $[a_1, \ldots, a_{n-1}, a_n]$ uz $a_n \geq 2$ i $[a_1, \ldots, a_{n-1}, a_n - 1, 1]$. Odavde direktno slijedi tvrdnja (ii). □

Neka je $\frac{u}{v}$ racionalan broj, $\text{nzd}(u, v) = 1$ i $u > v > 0$. Primijenimo na njega Euklidov algoritam:

$$u = vq_1 + r_1, \ v = r_1q_2 + r_2, \ \cdots, \ r_{j-1} = r_jq_{j+1}.$$

Tada je

$$\frac{u}{v} = q_1 + \frac{1}{\frac{c}{r_1}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}} = \cdots = [q_1, q_2, \ldots, q_{j+1}].$$

Primjer 1.2. *Razvijmo broj* $\frac{141}{100}$ *u jednostavni verižni razlomak.*

Rješenje:

$$\begin{aligned} 141 &= 100 \cdot 1 + 41 \\ 100 &= 41 \cdot 2 + 18 \\ 41 &= 18 \cdot 2 + 5 \\ 18 &= 5 \cdot 3 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2. \end{aligned}$$

Odavde je $\frac{141}{100} = [1, 2, 2, 3, 1, 1, 2]$. ♢

Lema 1.15. *Neka je* a_0 *cijeli broj, te* $a_1, a_2, \ldots$ *prirodni brojevi. Tada limes* $\lim_{n\to\infty} \frac{p_n}{q_n}$ *postoji i iracionalan je. Obrnuto, ako je* α *iracionalan, onda postoje jedinstveni cijeli brojevi* a_0, $a_1 \geq 1$, $a_2 \geq 1, \ldots$ *takvi da je* $\alpha = \lim_{n\to\infty} \frac{p_n}{q_n}$.

Dokaz: Budući je $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_1}{q_1}$, to $\lim\limits_{\substack{n \to \infty \\ n \text{ paran}}} \frac{p_n}{q_n}$ postoji. Iz sličnog razloga postoji i $\lim\limits_{\substack{n \to \infty \\ n \text{ neparan}}} \frac{p_n}{q_n}$ Ali ova dva limesa su jednaka jer je $\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_{n-1}q_n}$ i zbog $q_n \geq n$ je $\lim_{n\to\infty} \frac{(-1)^n}{q_{n-1}q_n} = 0$. Neka je $\alpha = \lim_{n\to\infty} \frac{p_n}{q_n}$. Budući da α leži između brojeva $\frac{p_n}{q_n}$ i $\frac{p_{n+1}}{q_{n+1}}$, imamo

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_{n+1}q_n} < \frac{1}{q_n^2}.$$

Kako su p_n i q_n relativno prosti, zaključujemo da postoji beskonačno mnogo različitih racionalnih brojeva $\frac{p}{q}$ takvih da je $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$. Sada iz Napomene 1.1 slijedi da je α iracionalan.

Dokažimo sada obrat. Neka je α iracionalan broj. Neka je $a_0 = \lfloor \alpha \rfloor$ i definirajmo α_1 sa $\alpha = a_0 + \frac{1}{\alpha_1}$. Tada je α_1 također iracionalan i $\alpha_1 > 1$. Nastavljamo ovaj postupak te za $k \geq 1$ definiramo $a_k = \lfloor \alpha_k \rfloor$ i $\alpha_k = a_k + \frac{1}{\alpha_{k+1}}$. Tada je $a_k \geq 1$, $\alpha_{k+1} > 1$ i α_{k+1} je iracionalan. Sada ćemo pokazati da je

$$\alpha = [a_0, a_1, a_2, \ldots].$$

Za svaki $n \geq 0$ imamo $\alpha = [a_0, a_1, \ldots, a_n, \alpha_{n+1}]$. Prema Lemi 1.10 je

$$|q_n \alpha - p_n| = \frac{1}{\alpha_{n+1} q_n + q_{n-1}},$$

pa je

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}. \tag{1.12}$$

Ovo povlači da je $\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$.

Preostaje pokazati da su cijeli brojevi a_0, $a_1 \geq 1$, $a_2 \geq 1, \ldots$ jedinstveni. Imamo:

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

Odavde je $0 \leq \alpha - a_0 < 1$, pa je $a_0 = \lfloor \alpha \rfloor$ i stoga je a_0 jedinstven. Zato je i $\alpha_1 = [a_1, a_2, \ldots]$ jedinstveno određen sa α. Sada je $a_1 = \lfloor \alpha_1 \rfloor$ pa je i a_1 jedinstven, itd. □

Primjer 1.3. Neka je $\alpha = [1, 1, 1, \ldots]$. Tada iz $\alpha = 1 + \frac{1}{[1,1,1,\ldots]} = 1 + \frac{1}{\alpha}$ slijedi $\alpha^2 - \alpha - 1 = 0$, pa iz $\alpha \geq 1$ dobivamo $\alpha = \frac{\sqrt{5}+1}{2}$.

Konvergente $\frac{p_n}{q_n}$ zadovoljavaju rekurzije

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

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

1.4 Verižni razlomci i aproksimacija iracionalnih brojeva racionalnima

Neka je α iracionalan broj. Prema formuli (1.12) svaka konvergenta od α zadovoljava nejednakost

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

Teorem 1.5 (Vahlen (1895))**.** *Neka su $\frac{p_{n-1}}{q_{n-1}}$ i $\frac{p_n}{q_n}$ dvije uzastopne konvergente od α. Tada barem jedna od njih zadovoljava nejednakost*

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

Dokaz: Brojevi $\alpha - \frac{p_n}{q_n}$, $\alpha - \frac{p_{n-1}}{q_{n-1}}$ imaju suprotni predznak, pa je

$$\left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_n q_{n-1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n-1}^2}$$

(jer je $2ab < a^2 + b^2$ za $a \neq b$). Prema tome, vrijedi

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \quad \text{ili} \quad \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q_{n-1}^2}.$$

□

Teorem 1.6 (Borel (1903))**.** *Neka su* $\frac{p_{n-2}}{q_{n-2}}$, $\frac{p_{n-1}}{q_{n-1}}$, $\frac{p_n}{q_n}$ *tri uzastopne konvergente od* α*. Tada barem jedna od njih zadovoljava nejednakost*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Dokaz: Stavimo $\alpha = [a_0, a_1, \dots]$, $\alpha_i = [a_i, a_{i+1}, \dots]$ i $\beta_i = \frac{q_{i-2}}{q_{i-1}}$ za $i \geq 1$. Iz Leme 1.10 imamo

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})}. \tag{1.13}$$

Da bi dovršili dokaz, moramo pokazati da ne postoji prirodan broj n takav da za $i = n-1, n, n+1$ vrijedi

$$\alpha_i + \beta_i \leq \sqrt{5}. \tag{1.14}$$

Pretpostavimo da je (1.14) ispunjeno za $i = n-1, n$. Tada iz

$$\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}, \quad \frac{1}{\beta_n} = \frac{q_{n-1}}{q_{n-2}} = a_{n-1} + \frac{q_{n-3}}{q_{n-2}} = a_{n-1} + \beta_{n-1}$$

slijedi

$$\frac{1}{\alpha_n} + \frac{1}{\beta_n} = \alpha_{n-1} + \beta_{n-1} \leq \sqrt{5}.$$

Stoga je $1 = \alpha_n \cdot \frac{1}{\alpha_n} \leq (\sqrt{5} - \beta_n)(\sqrt{5} - \frac{1}{\beta_n})$, što je ekvivalentno sa $\beta_n^2 - \sqrt{5}\beta_n + 1 \leq 0$. Odavde slijedi da je $\beta_n \geq \frac{\sqrt{5}-1}{2}$, odnosno, budući je β_n racionalan, $\beta_n > \frac{\sqrt{5}-1}{2}$.

Ako bi (1.14) također bilo ispunjeno za $i = n, n+1$, onda bi bilo $\beta_{n+1} > \frac{\sqrt{5}-1}{2}$, pa bi dobili da je

$$1 \leq a_n = \frac{q_n}{q_{n-1}} - \frac{q_{n-2}}{q_{n-1}} = \frac{1}{\beta_{n+1}} - \beta_n < \frac{2}{\sqrt{5}-1} - \frac{\sqrt{5}-1}{2} = 1,$$

što je kontradikcija. □

Teorem 1.7 (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 $\frac{p}{q}$ neka konvergenta od α.

Dokaz: Možemo pretpostaviti da je $\alpha \neq \frac{p}{q}$; inače je tvrdnja trivijalno zadovoljena. Tada možemo pisati $\alpha - \frac{p}{q} = \frac{\varepsilon\vartheta}{q^2}$, gdje je $0 < \vartheta < \frac{1}{2}$ i $\varepsilon = \pm 1$. Prema Lemi 1.14, postoji razvoj od $\frac{p}{q}$ u jednostavni verižni razlomak

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

gdje je n izabran tako da vrijedi $(-1)^{n-1} = \varepsilon$.

Definirajmo ω sa

$$\alpha = \frac{\omega p_{n-1} + p_{n-2}}{\omega q_{n-1} + q_{n-2}}, \tag{1.15}$$

tako da je $\alpha = [b_0, b_1 \ldots, b_{n-1}, \omega]$. Uočimo da je (1.15) ekvivalentno sa $(\alpha q_{n-1} - p_{n-1})\omega = p_{n-2} - \alpha q_{n-2}$. Možemo pretpostaviti da je $\alpha q_{n-1} - p_{n-1} \neq 0$ jer je inače $\alpha = \frac{p_{n-1}}{q_{n-1}} = \frac{p}{q}$.

Sada je, iz Leme 1.10,

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

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

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

Budući je $\omega > 1$, svi b_j $(j = n, n+1, \ldots)$ su prirodni brojevi. Koristeći Lemu 1.7 i prelazeći na limes ako je potrebno, dobivamo

$$\begin{aligned} \alpha &= [b_0, b_1, \ldots, b_{n-1}, [b_n, b_{n+1}, \ldots]] \\ &= [b_0, b_1, \ldots, b_{n-1}, b_n, b_{n+1}, \ldots]. \end{aligned}$$

Ovo je razvoj u jednostavni verižni razlomak od α i

$$\frac{p}{q} = \frac{p_{n-1}}{q_{n-1}} = [b_0, b_1, \ldots, b_{n-1}]$$

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

Lema 1.16. *Pretpostavimo da α ima razvoj u verižni razlomak oblika*

$$\alpha = [a_0, a_1, \ldots, a_N, 1, 1, 1, \ldots].$$

Tada je $\lim_{n\to\infty} q_n^2 \left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{\sqrt{5}}$.

Dokaz: Uz oznake iz dokaza Teorema 1.6, imamo:

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})}.$$

Ovdje je, za n dovoljno velik, $\alpha_{n+1} = [1, 1, 1, \dots] = \frac{\sqrt{5}+1}{2}$ i, prema Lemi l36,

$$\frac{1}{\beta_{n+1}} = \frac{q_n}{q_{n-1}} = [a_n, a_{n-1}, \dots, a_1] = [\underbrace{1, 1, \dots, 1}_{n-N}, a_N, \dots, a_1].$$

Budući da su $[\underbrace{1, 1, \dots, 1}_{n-N-1}]$ i $\underbrace{1, 1, \dots, 1}_{n-N}]$ susjedne konvergente od $\frac{1}{\beta_{n+1}}$, to se $\frac{1}{\beta_{n+1}}$ nalazi između njih. Stoga je $\lim_{n\to\infty} \frac{1}{\beta_{n+1}} = [1, 1, 1, \dots] = \frac{\sqrt{5}+1}{2}$. Prema tome,

$$\lim_{n\to\infty} \beta_{n+1} = \left(\frac{\sqrt{5}+1}{2}\right)^{-1} = \frac{\sqrt{5}-1}{2} \quad \text{i} \quad \lim_{n\to\infty} (\alpha_{n+1} + \beta_{n+1}) = \sqrt{5}.$$

□

Drugi dokaz Hurwitzovog teorema 1.3: Tvrdnja (i) slijedi direktno iz Teorema 1.6, dok tvrdnja (ii) slijedi iz Teorema 1.7 i Leme 1.16. Naime, ako iracionalan broj α ima oblik iz Leme 1.16, onda se po Teoremu 1.7 sva rješenja nejednadžbe $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$, gdje je $A > \sqrt{5}$, nalaze među konvergentama od α, a po Lemi 1.16 ovu nejednadžbu zadovoljava samo konačno mnogo konvergenti od α. □

Teorem 1.8 (Worley (1981), Dujella (2004))**.** *Neka je α proizvoljan realan broj, te c pozitivan realan broj. Ako racionalan broj $\frac{p}{q}$ zadovoljava nejednakost*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}, \tag{1.16}$$

onda je

$$\frac{p}{q} = \frac{rp_{k+1} \pm sp_k}{rq_{k+1} \pm sq_k},$$

za neki $k \geq -1$ i nenegativne cijele brojeve r, s takve da je $rs < 2c$ (i neki izbor predznaka).

Dokaz: Pretpostavit ćemo da je $\alpha < \frac{p}{q}$. U slučaju $\alpha > \frac{p}{q}$, dokaz je analogan. Također ćemo pretpostaviti da je α iracionalan (za α racionalan potrebna je mala modifikacija dokaza). Neka je k najveći neparan broj takav da je

$$\alpha < \frac{p}{q} \leq \frac{p_k}{q_k}.$$

(Ako je $\frac{p}{q} > \frac{p_1}{q_1}$, onda uzimamo $k = -1$.) Definirajmo brojeve r i s s

$$p = rp_{k+1} + sp_k,$$
$$q = rq_{k+1} + sq_k.$$

Prema Lemi 1.8, determinanta ovog sustava je ± 1, pa su r, s cijeli brojevi, a kako je $\frac{p_{k+1}}{q_{k+1}} < \frac{p}{q} \leq \frac{p_k}{q_k}$, vrijedi $r \geq 0$ i $s > 0$.

Zbog maksimalnosti od k, imamo

$$\left|\frac{p_{k+2}}{q_{k+2}} - \frac{p}{q}\right| < \left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}.$$

Nadalje,

$$\begin{aligned}\left|\frac{p_{k+2}}{q_{k+2}} - \frac{p}{q}\right| &= \frac{(a_{k+2}q_{k+1} + q_k)(rp_{k+1} + sp_k) - (a_{k+2}p_{k+1} + p_k)(rq_{k+1} + sq_k)}{qq_{k+2}} \\ &= \frac{sa_{k+2} - r}{qq_{k+2}}.\end{aligned}$$

Stoga je

$$q(sa_{k+2} - r) < cq_{k+2} = \frac{c}{s}((sa_{k+2} - r)q_{k+1} + q),$$

tj.

$$(sa_{k+2} - r)(q - \frac{c}{s}q_{k+1}) < \frac{c}{s}\,q.$$

Dalje imamo

$$\frac{1}{sa_{k+2} - r} > \frac{q - \frac{c}{s}q_{k+1}}{\frac{c}{s}q} = \frac{s}{c} - \frac{1}{r + \frac{sq_k}{q_{k+1}}} \geq \frac{s}{c} - \frac{1}{r}.$$

Tako smo dobili nejednakost (kvadratnu nejednadžbu po r):

$$r^2 - sra_{k+2} + ca_{k+2} > 0. \tag{1.17}$$

Razlikujemo sada dva slučaja:

1) $s^2a_{k+2} \geq 4c$

   Uz ovu pretpostavku je $s^4a_{k+2}^2 - 4cs^2a_{k+2} \geq (s^2a_{k+2} - 4c)^2$, pa za rješenje nejednadžbe (1.17) vrijedi da je

   $$r < \frac{1}{2s}\left(s^2a_{k+2} - \sqrt{s^4a_{k+2}^2 - 4cs^2a_{k+2}}\right) \leq \frac{2c}{s},$$

   ili

   $$r > \frac{1}{2s}\left(s^2a_{k+2} + \sqrt{s^4a_{k+2}^2 - 4cs^2a_{k+2}}\right) \geq \frac{1}{s}(s^2a_{k+2} - 2c).$$

   Prva mogućnost povlači $rs < 2c$. Ako je nastupila druga mogućnost, uvodimo supstituciju $t = sa_{k+2} - r$. Broj t je prirodan i vrijedi

   $$\begin{aligned}p &= rp_{k+1} + sp_k = (sa_{k+2} - t)p_{k+1} + sp_k = sp_{k+2} - tp_{k+1}, \\ q &= sq_{k+2} - tq_{k+1}\end{aligned}$$

   i $st = s^2a_{k+2} - rs < 2c$.

2) $s^2 a_{k+2} < 4c$

Ako je $r < \frac{1}{2} s a_{k+2}$, onda $rs < \frac{1}{2} s^2 a_{k+2} < 2c$. Ako je $\frac{1}{2} s a_{k+2} \leq r < s a_{k+2}$, onda ponovo definiramo $t = s a_{k+2} - r$ i vrijedi $st \leq \frac{1}{2} s^2 a_{k+2} < 2c$.

□

Stavimo li $c = 1$ u Teorem 1.8, dobivamo sljedeći rezultat.

Korolar 1.4 (Fatou (1904), Grace (1918)). *Neka su p, q cijeli brojevi takvi da je $q \geq 1$ i*

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

Tada postoji $n \geq 0$ tako da je

$$\frac{p}{q} = \frac{p_n}{q_n} \quad ili \quad \frac{p_n - p_{n-1}}{q_n - q_{n-1}} \quad ili \quad \frac{p_n + p_{n-1}}{q_n + q_{n-1}}.$$

Teorem 1.9 (Lagrange (1770)). *Neka je α iracionalan broj, te $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots$ konvergente od α. Tada vrijedi:*

(i) $|\alpha q_0 - p_0| > |\alpha q_1 - p_1| > |\alpha q_2 - p_2| > \cdots$

(ii) Ako je $n \geq 1$ i $1 \leq q \leq q_n$, te ako je $(p, q) \neq (p_{n-1}, q_{n-1}), (p_n, q_n)$, onda je $|\alpha q - p| > |\alpha q_{n-1} - p_{n-1}|$.

Dokaz: Po Lemi 1.10 je

$$|\alpha q_n - p_n| = \frac{1}{\alpha_{n+1} q_n + q_{n-1}} < \frac{1}{q_n + q_{n-1}},$$
$$|\alpha q_{n-1} - p_{n-1}| = \frac{1}{\alpha_n q_{n-1} + q_{n-2}} > \frac{1}{(a_n + 1) q_{n-1} + q_{n-2}} = \frac{1}{q_{n-1} + q_n},$$

čime je dokazana tvrdnja (i).

Da bi dokazali (ii), definirajmo brojeve μ, ν pomoću jednadžbi

$$\mu p_n + \nu p_{n-1} = p,$$
$$\mu q_n + \nu q_{n-1} = q.$$

Matrica ovog sustava ima determinantu ± 1, pa su brojevi μ, ν cijeli brojevi. Ako je $\nu = 0$, onda je $p = \mu p_n$, $q = \mu q_n$, a to je nemoguće jer je $0 < q \leq q_n$ i $(p, q) \neq (p_n, q_n)$. Ako je $\mu = 0$, onda je $p = \nu p_{n-1}$, $q = \nu q_{n-1}$. Budući da je $(p, q) \neq (p_{n-1}, q_{n-1})$, to je $\nu \geq 2$ i zato je

$$|\alpha q - p| \geq 2 |\alpha q_{n-1} - p_{n-1}| > |\alpha q_{n-1} - p_{n-1}|.$$

Ako su $\mu \neq 0$, $\nu \neq 0$, onda zbog $1 \leq q \leq q_n$, μ i ν imaju suprotne predznake, pa brojevi $\mu(\alpha q_n - p_n)$ i $\nu(\alpha q_{n-1} - p_{n-1})$ imaju iste predznake. Stoga je

$$|\alpha q - p| = |\mu(\alpha q_n - p_n)| + |\nu(\alpha q_{n-1} - p_{n-1})|,$$

pa je, zbog $\mu\nu \neq 0$, $|\alpha q - p| > |\alpha q_{n-1} - p_{n-1}|$. □

Definicija 1.3. *Razlomke oblika* $\frac{p_{n,r}}{q_{n,r}} = \frac{rp_{n+1}+p_n}{rq_{n+1}+q_n}$, $r = 1, 2, \ldots, a_{n+2}-1$, $n \geq -1$, *nazivamo* sekundarne konvergente *verižnog razlomka* $[a_0, a_1, \ldots]$.

Uočimo: $\frac{p_{n,0}}{q_{n,0}} = \frac{p_n}{q_n}$, $\frac{p_{n,a_{n+2}}}{q_{n,a_{n+2}}} = \frac{p_{n+2}}{q_{n+2}}$.

Lema 1.17. *Za n paran vrijedi*

$$\frac{p_n}{q_n} < \cdots < \frac{p_{n,r}}{q_{n,r}} < \frac{p_{n,r+1}}{q_{n,r+1}} < \cdots < \frac{p_{n+2}}{q_{n+2}},$$

dok za n neparan vrijedi

$$\frac{p_n}{q_n} > \cdots > \frac{p_{n,r}}{q_{n,r}} > \frac{p_{n,r+1}}{q_{n,r+1}} > \cdots > \frac{p_{n+2}}{q_{n+2}}.$$

Nadalje, za svaki prirodan broj n vrijedi

$$q_{n,r+1}p_{n,r} - p_{n,r+1}q_{n,r} = (-1)^{n+1}. \tag{1.18}$$

Dokaz: Dovoljno je dokazati relaciju (1.18). Imamo:

$$\begin{aligned} &q_{n,r+1}p_{n,r} - p_{n,r+1}q_{n,r} \\ &\quad = [(r+1)q_{n+1}+q_n](rp_{n+1}+p_n) - [(r+1)p_{n+1}+p_n](rq_{n+1}+q_n) \\ &\quad = q_{n+1}p_n - p_{n+1}q_n = (-1)^{n+1}. \end{aligned}$$

□

Reći ćemo da je racionalan broj $\frac{a}{b}$, $b > 0$, *dobra aproksimacija* iracionalnog broja α ako vrijedi

$$\left|\alpha - \frac{a}{b}\right| = \min\left\{\left|\alpha - \frac{x}{y}\right| : x, y \in \mathbb{Z},\ 0 < y \leq b\right\}.$$

Teorem 1.10. *Svaka dobra aproksimacija od* α *je ili konvergenta ili sekundarna konvergenta od* α.

Dokaz: Neka je $\frac{a}{b}$ dobra aproksimacija od α koja nije ni konvergenta ni sekundarna konvergenta od α. Bez smanjenja općenitosti možemo pretpostaviti da je $\frac{a}{b} > \alpha$. Tada postoje uzastopne (obične ili sekundarne) konvergente $\frac{P}{Q}$ i $\frac{P'}{Q'}$ od α takve da je

$$\alpha < \frac{P}{Q} < \frac{a}{b} < \frac{P'}{Q'} \quad \text{i} \quad P'Q - PQ' = 1.$$

Sada je

$$\frac{1}{Q'b} \leq \frac{P'}{Q'} - \frac{a}{b} < \frac{P'}{Q'} - \frac{P}{Q} = \frac{1}{Q'Q}.$$

Dakle, dobili smo da je $Q < b$ i $\left|\alpha - \frac{P}{Q}\right| < \left|\alpha - \frac{a}{b}\right|$, što je kontradikcija. □

Primjer 1.4. *Pokažimo primjerom da ne mora svaka sekundarna konvergenta biti dobra aproksimacija.*

Rješenje: Neka je $\alpha = [1, 2, 2, 2, \dots]$. Tada je $\frac{1}{\alpha-1} = \alpha + 1$, pa je stoga $\alpha = \sqrt{2}$. Konvergente od α su: 1, $\frac{3}{2}$, $\frac{7}{5}$, $\frac{17}{12}$, $\dots$, a sekundarne konvergente: $\frac{4}{3}$, $\frac{10}{7}$, $\frac{24}{17}$, $\dots$. Međutim, $\left|\sqrt{2} - \frac{7}{5}\right| \approx 0.0142$, $\left|\sqrt{2} - \frac{10}{7}\right| \approx 0.0144$, pa $\frac{10}{7}$ nije dobra aproksimacija broja $\sqrt{2}$. ♢

Definicija 1.4. *Za iracionalan broj α kažemo da je* slabo aproksimabilan *ako postoji konstanta $c = c(\alpha) > 0$ takva da je*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^2}$$

za svaki racionalan broj $\frac{p}{q}$. (Iz Hurwitzovog teorema slijedi da konstanta c mora zadovoljavati $0 < c < \frac{1}{\sqrt{5}}$.)

Teorem 1.11. *Iracionalan broj α je slabo aproksimabilan ako i samo ako su mu parcijalni kvocijenti u razvoju u jednostavni verižni razlomak omeđeni.*

Dokaz: Iz dokaza Teorema 1.6 i Leme 1.11, slijedi

$$\begin{aligned}\left|\alpha - \frac{p_n}{q_n}\right| &= \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})} \\ &= \frac{1}{q_n^2([a_{n+1}, a_{n+2}, \dots] + [0, a_n, a_{n-1}, \dots, a_1])},\end{aligned} \tag{1.19}$$

pa je

$$\frac{1}{q_n^2(a_{n+1} + 2)} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2 a_{n+1}}. \tag{1.20}$$

Ako $\frac{p}{q}$ nije konvergenta od α, onda je, prema Teoremu 1.7, $|\alpha - \frac{p}{q}| > \frac{1}{2q^2}$. Ako su parcijalni kvocijenti od α omeđeni, tj. ako postoji $K > 0$ takav da je $a_n \leq K$ za sve $n \geq 0$, onda je

$$\left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{q_n^2(K + 2)}.$$

Dakle, za svaki racionalan broj $\frac{p}{q}$ vrijedi $|\alpha - \frac{p}{q}| > \frac{c}{q^2}$, gdje je $c = \min(\frac{1}{K+2}, \frac{1}{2}) = \frac{1}{K+2}$, što znači da je α slabo aproksimabilan.

Obrnuto, pretpostavimo da je α slabo aproksimabilan. To znači da postoji $c > 0$ takav da je $|\alpha - \frac{p}{q}| > \frac{c}{q^2}$ za svaki racionalan broj $\frac{p}{q}$. Sada (1.20) povlači da je $a_{n+1} < \frac{1}{c}$ za svaki $n \geq 0$, što znači da su parcijalni kvocijenti od α omeđeni. □

Korolar 1.5. *Postoji neprebrojivo mnogo slabo aproksimabilnih i neprebrojivo mnogo realnih brojeva koji nisu slabo aproksimabilni.*

Dokaz: Prema Teoremu 1.11, svi realni brojevi oblika $\alpha = [a_0, a_1, \ldots]$, gdje je $a_n \in \{1, 2\}$ za $n \geq 0$, su slabo aproksimabilni, i ima ih neprebrojivo mnogo.

Svi realni brojevi oblika $\alpha = [a_0, a_1, \ldots]$, gdje je $a_n = n + b_n$, $b_n \in \{0, 1\}$ za $n \geq 0$, nisu slabo aproksimabilni, i ima ih neprebrojivo mnogo. □

1.5 Ekvivalentni brojevi

Definicija 1.5. *Kažemo da su iracionalni brojevi α i β* ekvivalentni *ako postoje cijeli brojevi a, b, c, d takvi da je $ad - bc = \pm 1$ i*

$$\beta = \frac{a\alpha + b}{c\alpha + d}.$$

Lako se provjeri da je ovo zaista relacija ekvivalencije. Oznaka je $\alpha \cong \beta$.

Teorem 1.12 (Serret (1878))**.** *Neka su $\alpha = [a_0, a_1, a_2, \ldots]$ i $\beta = [b_0, b_1, b_2, \ldots]$ iracionalni brojevi. Tada su α i β ekvivalentni ako i samo ako postoje cijeli brojevi k i l takvi da je $a_{k+n} = b_{l+n}$ za sve $n \geq 0$.*

Lema 1.18. *Neka su a, b, c, d cijeli brojevi i*

$$\beta = \frac{a\alpha + b}{c\alpha + d}, \quad ad - bc = \pm 1, \quad \alpha > 1, \quad c > d > 0,$$

onda su $\frac{b}{d}$ i $\frac{a}{c}$ dvije uzastopne konvergente od β, recimo $\frac{p_{n-2}}{q_{n-2}}$ i $\frac{p_{n-1}}{q_{n-1}}$, te vrijedi $\alpha = \beta_n$.

Dokaz Leme 1.18: Prikažimo $\frac{a}{c}$ kao konačni jednostavni verižni razlomak

$$\frac{a}{c} = [a_0, a_1, \ldots, a_{n-1}] = \frac{p_{n-1}}{q_{n-1}}.$$

Budući da su a i c relativno prosti, imamo: $a = p_{n-1}$, $c = q_{n-1}$. Izaberimo n tako da vrijedi

$$p_{n-1}q_{n-2} - q_{n-1}p_{n-2} = \varepsilon,$$

gdje je $\varepsilon = ad - bc$. Iz $ad - bc = p_{n-1}d - q_{n-1}b = \varepsilon$ dobivamo

$$p_{n-1}(d - q_{n-2}) = q_{n-1}(b - p_{n-2}).$$

Budući da je $\text{nzd}(p_{n-1}, q_{n-1}) = 1$, slijedi da $q_{n-1} | (d - q_{n-2})$. Međutim, $q_{n-2} \leq q_{n-1}$ i $d < q_{n-1}$, pa je $|d - q_{n-2}| < q_{n-1}$. Stoga je $d - q_{n-2} = 0$. Odavde je i $b - p_{n-2} = 0$. Dakle, dobili smo da je

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

To znači da je $\beta = [a_0, a_1, \ldots, a_{n-1}, \alpha]$. Budući da je $\alpha > 1$, vidimo da je $\alpha = \beta_n$, te da su $\frac{b}{d} = \frac{p_{n-2}}{q_{n-2}}$ i $\frac{a}{c} = \frac{p_{n-1}}{q_{n-1}}$ susjedne konvergente od β. □

Dokaz Teorema 1.12: Pretpostavimo da postoje cijeli brojevi k i l takvi da je $a_{k+n} = b_{l+n}$ za sve $n \geq 0$. Drugim riječima, $\alpha = [a_0, a_1, \ldots, a_{k-1}, \alpha_k]$, $\beta = [b_0, b_1, \ldots, b_{l-1}, \beta_l]$ i $\alpha_k = \beta_l$. Po Lemama 1.7 i 1.8 je $\alpha \cong \alpha_k$ i $\beta \cong \beta_l$, pa je i $\alpha \cong \beta$.

Pretpostavimo sada da su α i β ekvivalentni, tj. $\beta = \frac{a\alpha+b}{c\alpha+d}$, $ad-bc = \pm 1$. Bez smanjenja općenitosti možemo pretpostaviti da je $c\alpha + d > 0$ (inače zamijenimo a, b, c, d sa $-a, -b, -c, -d$). Za $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, uvedimo oznaku: $\sigma\alpha = \frac{a\alpha+b}{c\alpha+d}$. Lako se provjerava da vrijedi $\sigma(\tau\alpha) = (\sigma\tau)\alpha$. Neka je $\sigma_{n-1} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}$. Tada je $\alpha = \sigma_{n-1}\alpha_n$, pa je $\beta = \sigma\sigma_{n-1}\alpha_n$. Vrijedi:

$$\sigma\sigma_{n-1} = \begin{pmatrix} ap_{n-1} + bq_{n-1} & ap_{n-2} + bq_{n-2} \\ cp_{n-1} + dq_{n-1} & cp_{n-2} + dq_{n-2} \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

Imamo:

$$cp_{n-1} + dq_{n-1} = q_{n-1}\left(c\frac{p_{n-1}}{q_{n-1}} + d\right) = c',$$
$$cp_{n-2} + dq_{n-2} = q_{n-2}\left(c\frac{p_{n-2}}{q_{n-2}} + d\right) = d'.$$

Budući da je $c\alpha + d > 0$ i $\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$, zaključujemo da su za dovoljno veliki n brojevi c' i d' pozitivni. Nadalje, $a'd' - b'c' = \det(\sigma) \cdot \det(\sigma_{n-1}) = \pm 1$. Odaberimo parnost od n tako da je $c' > d'$ (ako je $c \geq 0$, biramo n paran, a ako je $c < 0$, biramo n neparan). Sada su zadovoljene sve pretpostavke Leme 1.18, pa zaključujemo da je $\alpha_n = \beta_m$ za neki m, što je i trebalo dokazati. □

Definicija 1.6. Markovljeva konstanta $M(\alpha)$ *je supremum skupa svih realnih brojeva* λ *takvih da nejednadžba*

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

ima beskonačno mnogo rješenja $\frac{p}{q}$.

Teorem 1.13 (Hurwitz (1891))**.**

(i) Ako je $\alpha \cong \alpha'$*, onda je* $M(\alpha) = M(\alpha')$.

(ii) Ako je $\alpha = \frac{1+\sqrt{5}}{2}$*, onda je* $M(\alpha) = \sqrt{5}$.

(iii) Ako je α *iracionalan i* $\alpha \ncong \frac{1+\sqrt{5}}{2}$*, onda je* $M(\alpha) \geq \sqrt{8}$.

(iv) Ako je $\alpha \cong \sqrt{2}$*, onda je* $M(\alpha) = \sqrt{8}$.

Dokaz:

(i) Iz $|\alpha - \frac{p_n}{q_n}| = \frac{1}{q_n^2(\alpha_{n+1}+\beta_{n+1})}$, zaključujemo da je

$$M(\alpha) = \limsup(\alpha_{n+1} + \beta_{n+1}).$$

Prema Lemi 1.11 je $\beta_{n+1} = \frac{q_{n-1}}{q_n} = \frac{1}{q_n/q_{n-1}} = [0, a_n, a_{n-1}, \ldots, a_1]$. Dakle,

$$M(\alpha) = \limsup([a_{n+1}, a_{n+2}, \ldots] + [0, a_n, a_{n-1}, \ldots, a_1]). \tag{1.21}$$

Ako je $\alpha \cong \alpha'$, onda postoji $l \geq 0$ sa svojstvom da je $a_n = a'_{n+l}$ za dovoljno velike n. Tada je $\alpha_{n+1} = \alpha'_{n+l+1}$. Također, β_{n+1} i β'_{n+l+1} imaju iste početne parcijalne kvocijente, pa je za n dovoljno velik njihova razlika po volji mala. Dakle,

$$\lim_{n\to\infty}((\alpha_{n+1} + \beta_{n+1}) - (\alpha'_{n+l+1} + \beta_{n+l+1})) = 0,$$

pa je $M(\alpha) = M(\alpha')$.

(ii)

$$M(\frac{1+\sqrt{5}}{2}) = \lim_{n\to\infty}([1,1,\ldots]+[0,\underbrace{1,1,\ldots,1}_{n}]) = \frac{1+\sqrt{5}}{2}+\frac{\sqrt{5}-1}{2} = \sqrt{5}.$$

(iii) Iz $\alpha \ncong \frac{1+\sqrt{5}}{2}$ imamo da je $a_k \geq 2$ za beskonačno mnogo indeksa k. Ako je $a_k \geq 3$ za beskonačno mnogo k-ova, onda iz (1.21) slijedi da je $M(\alpha) \geq 3 > \sqrt{8}$. Dakle, dovoljno je promatrati one α za koje je $a_k \in \{1, 2\}$ za dovoljno velike k-ove.

Ako među a_k-ovima postoji beskonačno mnogo jednica i beskonačno mnogo dvojki, onda postoji beskonačno mnogo indeksa k takvih da je $a_k = 1$ i $a_{k+1} = 2$. No, tada je

$$[a_{k+1}, a_{k+2}, \ldots] \geq 2 + \frac{1}{a_{k+2} + \frac{1}{a_{k+3}}} \geq 2 + \frac{1}{2 + \frac{1}{1}} = \frac{7}{3},$$

$$[0, a_k, \ldots, a_1] \geq \frac{1}{1 + \frac{1}{a_{k-1}}} \geq \frac{1}{1 + \frac{1}{1}} = \frac{1}{2},$$

pa je $M(\alpha) \geq \frac{7}{3} + \frac{1}{2} = \frac{17}{6} = 2.833\cdots > \sqrt{8}$.

Preostao je slučaj kada je $a_k = 2$ za sve dovoljno velike k-ove. Tada je

$$\alpha \cong [1, 2, 2, 2, \ldots] = \sqrt{2},$$

pa je

$$M(\alpha) = \lim_{n\to\infty}([2,2,\ldots] + [0,\underbrace{2,2,\ldots,2}_{n}]) = (\sqrt{2}+1) + (\sqrt{2}-1) = \sqrt{8},$$

čije je dokazano i (iii) i (iv).

□

Brojevi $\sqrt{5}$ i $\sqrt{8}$ predstavljaju prva dva člana niza $\mu_1 = \sqrt{5} < \mu_2 = \sqrt{8} < \mu_3 = \frac{\sqrt{221}}{5} < \mu_4 = \frac{\sqrt{1517}}{13} < \dots$ čiji je limes jednak 3, a za koje je Markov (1879) dokazao da su jedine vrijednosti od $M(\alpha)$ koje su manje od 3. Svakom od μ_i-ova odgovara skupo brojeva koji su ekvivalentni korijenu neke kvadratne jednadžbe. Mi ovaj rezultat nećemo dokazivati. Pokazat ćemo, međutim, da je struktura skupa svih α za koje je $M(\alpha) = 3$ bitno drugačija.

Teorem 1.14 (Markov (1879))**.** *Postoji neprebrojivo mnogo realnih brojeva α takvih da je $M(\alpha) = 3$, te da nikoja dva među njima nisu ekvivalentna.*

Dokaz: Neka je $r_1, r_2, \dots$ strogo rastući niz prirodnih brojeva i neka je

$$\alpha = [\underbrace{1, 1, \dots, 1}_{r_1}, 2, 2, \underbrace{1, 1, \dots, 1}_{r_2}, 2, 2, \underbrace{1, 1, \dots, 1}_{r_3}, 2, 2, \dots]. \tag{1.22}$$

Ako odaberemo k tako da je $a_{k+1} = 1$, onda je $\alpha_{k+1} + \beta_{k+1} < 2 + 1 = 3$. Ako k prolazi nizom indeksa takvih da je $a_{k+1} = a_{k+2} = 2$, onda, zbog $\lim_i r_i = \infty$, imamo:

$$\lim_k(\alpha_{k+1}+\beta_{k+1}) = [2, 2, 1, 1, \dots]+[0, 1, 1, \dots]) = 2+\frac{1}{2+\frac{\sqrt{5}-1}{2}}+\frac{\sqrt{5}-1}{2} = 3.$$

Konačno, ako k prolazi skupom indeksa za koje je $a_k = a_{k+1} = 2$, onda je

$$\lim_k(\alpha_{k+1}+\beta_{k+1}) = [2, 1, 1, \dots]+[0, 2, 1, 1, \dots]) = 2+\frac{\sqrt{5}-1}{2}+\frac{1}{2+\frac{\sqrt{5}-1}{2}} = 3.$$

Dakle, $M(\alpha) = \limsup(\alpha_{k+1} + \beta_{k+1}) = 3$.

Da bi dovršili dokaz, moramo još pokazati da je skup međusobno neekvivalentnih brojeva α definiranih s (1.22) neprebrojiv. Brojevi α i α' su ekvivalentni ako i samo ako im se pripadni nizovi $r_1, r_2, \dots$ i $r'_1, r'_2, \dots$ podudaraju od nekog mjesta nadalje. Za takve nizove ćemo reći da su ekvivalentni. Pretpostavimo da neekvivalentnih nizova ima prebrojivo mnogo, recimo da su to $R_1, R_2, \dots$, gdje R_i predstavlja niz $r_{i_1} < r_{i_2} < \dots$. Možemo pretpostaviti da je $R_1 = (1, 2, 3, \dots)$. Za $i > 1$, R_i nije ekvivalentan R_1, pa postoji beskonačno mnogo prirodnih brojeva koji nisu sadržani u R_i.

Za $i > 1$ sa $S_i = (s_{i_k})$ označimo niz koji je komplementaran nizu R_i. Znamo da je svaki S_i beskonačan. Sada ćemo definirati niz T na sljedeći način. Najprije izaberemo $t_1 \in S_2$, a zatim izaberemo $t_2, t_3, \dots$ tako da vrijedi

$$\begin{aligned}
t_1 \in S_2, &\quad t_1 < t_2 \in S_3, \\
1 + t_2 < t_3 \in S_2, &\quad t_3 < t_4 \in S_3, \quad t_4 < t_5 \in S_4, \\
1 + t_5 < t_6 \in S_2, &\quad t_6 < t_7 \in S_3, \quad t_7 < t_8 \in S_4, \quad t_8 < t_9 \in S_5, \\
&\vdots
\end{aligned}$$

Očito je T rastući niz prirodnih brojeva. Za svaki $k \geq 2$, beskonačno mnogo članova niza T je sadržano u S_k, pa stoga nije sadržano u R_k. Prema tome, T nije ekvivalentan niti jednom od $R_2, R_3, \ldots$. Budući da svaki od elemenata $t_3, t_6, t_{10}, \ldots$ od T koji pripada S_2 premašuje svog prethodnika za barem 2, zaključujemo da T nije ekvivalentan niti sa R_1. Dakle, T nije ekvivalentan niti jednom R_k, što je u suprotnosti s pretpostavkom da niz (R_k) sadrži po jedan element iz svake klase ekvivalencije. □

Iz prethodnog teorema direktno slijedi

Korolar 1.6. *Postoje transcendentni brojevi α za koje je $M(\alpha) = 3$.*

Vidjet ćemo kasnije da Liouvilleov teorem povlači da je svaki realan broj koji se može dovoljno dobro aproksimirati racionalnim brojevima nužno transcendentan. Međutim, Korolar 1.6 pokazuje da postoje transcendentni brojevi čije su racionalne aproksimacije skoro najgore moguće, u svjetlu Hurwitzovog teorema.

1.6 Periodski verižni razlomci

Definicija 1.7. *Za beskonačni verižni razlomak $[a_0, a_1, a_2, \ldots]$ kažemo da je* periodski *ako postoje cijeli brojevi $k \geq 0$, $m \geq 1$ takvi da je $a_{m+n} = a_n$ za sve $n \geq k$. U tom slučaju verižni razlomak pišemo u obliku*

$$[a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+m-1}}],$$

gdje "crta" iznad brojeva $a_k, \ldots, a_{k+m-1}$ znači da se taj blok brojeva ponavlja u nedogled.

Primjer 1.5. *(i) Neka je $\beta = [2, 3, 2, 3, \ldots] = [\overline{2, 3}]$. Tada je $\beta = 2 + \frac{1}{3+\frac{1}{\beta}}$. To daje kvadratnu jednadžbu za β: $3\beta^2 - 6\beta - 2 = 0$, pa zbog $\beta > 0$, dobivamo da je $\beta = \frac{3+\sqrt{15}}{3}$.*

(ii) Neka je sada $\alpha = [4, 1, \overline{2, 3}]$. Imamo:

$$\alpha = 1 + \frac{1}{1 + \frac{1}{\beta}} = 4 + \frac{\beta}{\beta + 1} = \frac{29 + \sqrt{15}}{7}.$$

Ova dva primjera ilustriraju opću situaciju.

Definicija 1.8. *Za iracionalan broj α kažemo da je* kvadratna iracionalnost *ako je α korijen kvadratne jednadžbe s racionalnim koeficijentima (drugim riječima, α je algebarski broj stupnja 2).*

Teorem 1.15 (Euler (1737), Lagrange (1770))**.** *Razvoj u jednostavni verižni razlomak realnog broja α je periodski ako i samo ako je α kvadratna iracionalnost.*

Dokaz: Neka je $\alpha = [b_0, b_1, \ldots, b_{k-1}, \overline{a_0, a_1, \ldots, a_{m-1}}]$, te neka je $\beta = [\overline{a_0, a_1, \ldots, a_{m-1}}]$, tj. neka je β čisto periodski dio od α. Primjenom Leme 1.7 na verižni razlomak $\beta = [a_0, a_1, \ldots, a_{m-1}, \beta]$, dobivamo da je

$$\beta = \frac{\beta p_{m-1} + p_{m-2}}{\beta q_{m-1} + q_{m-2}},$$

a to je kvadratna jednadžba za β (s cjelobrojnim koeficijentima). Budući je, prema Lemi 1.15, β iracionalan, to je β kvadratna iracionalnost.

Zapišimo α pomoću β:

$$\alpha = \frac{\beta p + p'}{\beta q + q'}, \tag{1.23}$$

gdje su $\frac{p}{q}$ i $\frac{p'}{q'}$ zadnje dvije konvergente od $[b_0, b_1, \ldots, b_{k-1}]$. Međutim, β ima oblik $\frac{a+\sqrt{b}}{c}$, pa iz (1.23) slijedi da i α ima isti oblik. Budući da α nije racionalan, prvi dio teorema je dokazan.

Dokažimo sada obrat. Neka je α kvadratna iracionalnost, tj. neka je $\alpha = \frac{a+\sqrt{b}}{c}$, $a, b, c, \in \mathbb{Z}$, $b > 0$, $c \neq 0$ i b nije potpun kvadrat. Množeći brojnik i nazivnik od α sa $|c|$, dobivamo

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

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

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

gdje su $d, s_0, t_0 \in \mathbb{Z}$, $t_0 \neq 0$, d nije potpun kvadrat i $t_0 | (d - s_0^2)$.

Sada ćemo opisati razvoj $[a_0, a_1, \ldots]$ u jednostavni verižni razlomak od α. Neka je $\alpha_0 = \alpha$, te neka je

$$a_i = \lfloor \alpha_i \rfloor, \quad \alpha_i = \frac{s_i + \sqrt{d}}{t_i}, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}. \tag{1.24}$$

Imamo:

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

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

Pokažimo sada matematičkom indukcijom da su s_i, t_i cijeli brojevi takvi da je $t_i \neq 0$ i $t_i | (d - s_i^2)$. 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 $t_i = \frac{d - s_{i+1}^2}{t_{i+1}}$ slijedi da $t_{i+1} | (d - s_{i+1}^2)$.

Sa α_i' označimo konjugat od α_i, tj. $\alpha_i' = \frac{s_i - \sqrt{d}}{t_i}$. Budući da je konjugat kvocijenta jednak kvocijentu konjugata, imamo: $\alpha_0' = \frac{\alpha_n' p_{n-1} + p_{n-2}}{\alpha_n' q_{n-1} + q_{n-2}}$. Odavde je

$$\alpha_n' = -\frac{q_{n-2}}{q_{n-1}} \Big(\frac{\alpha_0' - \frac{p_{n-2}}{q_{n-2}}}{\alpha_0' - \frac{p_{n-1}}{q_{n-1}}} \Big).$$

Kad n teži u ∞, $\frac{p_{n-1}}{q_{n-1}}$ i $\frac{p_{n-2}}{q_{n-2}}$ teže prema α_0, a $\alpha_0 \neq \alpha_0'$. Stoga izraz u zagradi teži prema 1, pa je zbog toga pozitivan za dovoljno velike n, recimo za $n > N$. Sada je za $n > N$ broj α_n' negativan. No, α_n je pozitivan za $n \geq 1$, pa je $\alpha_n - \alpha_n' = \frac{2\sqrt{d}}{t_n} > 0$. Dakle, $t_n > 0$ za $n > N$. Nadalje, za $n > N$ imamo:

$$0 > \alpha_n \alpha_n' = \frac{s_n^2 - d}{t_n^2} \implies |s_n| < \sqrt{d},$$

dok iz $\alpha_n > 1$ i upravo dokazanog slijedi

$$t_n < s_n + \sqrt{d} < 2\sqrt{d}.$$

Odavde slijedi da uređeni parovi (s_n, t_n) mogu poprimiti samo konačno mnogo vrijednosti, pa postoje prirodni brojevi j, k, $j < k$, takvi da je $s_j = s_k$, $t_j = t_k$. Sada (1.24) povlači da je $\alpha_j = \alpha_k$, pa je

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

što je i trebalo dokazati. □

Napomena 1.2. Uočimo da vrijedi

$$a_i = \left\lfloor \frac{s_i + \sqrt{d}}{t_i} \right\rfloor = \left\lfloor \frac{s_i + \lfloor \sqrt{d} \rfloor}{t_i} \right\rfloor.$$

Zaista, neka je $\left\lfloor \frac{s_i + \lfloor \sqrt{d} \rfloor}{t_i} \right\rfloor = u$. Tada je $s_i + \lfloor \sqrt{d} \rfloor = t_i u + v$, za $0 \leq v \leq t - 1$. Zato je $u < \frac{s_i + \sqrt{d}}{t_i} < \frac{s_i + \lfloor \sqrt{d} \rfloor + 1}{t_i} \leq u + 1$, pa je $\left\lfloor \frac{s_i + \sqrt{d}}{t_i} \right\rfloor = u$. Prema tome, algoritam (1.24) zapravo radi samo s cijelim brojevima (i ne zahtjeva preciznu aproksimaciju za $\sqrt{d}$).

Definicija 1.9. *Za kvadratnu iracionalnost α kažemo da je* reducirana *ako je $\alpha > 1$ i $-1 < \alpha' < 0$, gdje je α' konjugat od α.*

Teorem 1.16. *Kvadratna iracionalnost α ima čisto periodski razvoj u jednostavni verižni razlomak ako i samo ako je reducirana.*

Dokaz: Neka je $\alpha > 1$ i $-1 < \alpha' < 0$. Stavimo $\alpha_0 = \alpha$, te definirajmo α_i sa $\frac{1}{\alpha_{i+1}} = \alpha_i - a_i$. Tada je

$$\frac{1}{\alpha_{i+1}} = \alpha_i' - a_i. \tag{1.25}$$

Po pretpostavci je $-1 < \alpha_0' < 0$. Indukcijom slijedi da je $-1 < \alpha_i' < 0$ za sve $i \geq 0$. Zaista, vrijedi $a_i \geq 1$ za sve $i \geq 0$ (čak i za $i = 0$ zbog $\alpha > 1$), pa $\alpha_i' < 0$ povlači da je $\frac{1}{\alpha_{i+1}'} < -1$, odnosno $-1 < \alpha_{i+1}' < 0$.

Sada iz (1.25) slijedi

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

Iz Teorema 1.15 slijedi da postoje prirodni brojevi takvi da je $j < k$ i $\alpha_j = \alpha_k$. Sada je $\alpha_j' = \alpha_k'$, te

$$a_{j-1} = \left\lfloor -\frac{1}{\alpha_j'} \right\rfloor = \lfloor -\frac{1}{\alpha_k'} \rfloor = a_{k-1},$$
$$\alpha_{j-1} = a_{j-1} + \frac{1}{\alpha_j} = a_{k-1} + \frac{1}{\alpha_k} = \alpha_{k-1}.$$

Dakle, $\alpha_j = \alpha_k$ povlači da je $\alpha_{j-1} = \alpha_{k-1}$. Primijenimo li ovu implikaciju j puta, dobivamo $\alpha_0 = \alpha_{k-j}$, tj. $\alpha = [\overline{a_0, a_1, \ldots, a_{k-j-1}}]$.

Obrnuto, pretpostavimo da je razvoj od α čisto periodski, $\alpha = [\overline{a_0, a_1 \ldots, a_{n-1}}]$, $a_0, a_1, \ldots, a_{n-1} \in \mathbb{N}$ (zbog $a_0 = a_n$). Imamo: $\alpha > a_0 \geq 1$. Također je

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

Prema tome, α zadovoljava jednadžbu

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

Ova kvadratna jednadžba ima dva korijena, α i α'. Budući da je $\alpha > 1$, dovoljno je provjeriti da $f(x)$ ima korijen između -1 i 0. To ćemo provjeriti tako da pokažemo da $f(-1)$ i $f(0)$ imaju različite predznake. Najprije je $f(0) = -p_{n-2} < 0$, a potom

$$f(-1) = q_{n-1} - q_{n-2} + p_{n-1} - p_{n-2} > 0.$$

□

Teorem 1.17. *Ako prirodan broj d nije potpun kvadrat, onda razvoj u jednostavni verižni razlomak od $\sqrt{d}$ ima oblik*

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

gdje je $a_0 = \lfloor \sqrt{d} \rfloor$, a $a_1, \ldots, a_{r-1}$ su centralno simetrični, tj. $a_1 = a_{r-1}$, $a_2 = a_{r-2}$, ...

Dokaz: Promotrimo broj $\beta = \sqrt{d} + \lfloor\sqrt{d}\rfloor$. Očito je broj β reduciran, pa po Teoremu 1.16 ima čisto periodičan razvoj

$$\sqrt{d} + \lfloor\sqrt{d}\rfloor = [\overline{b_0, b_1, \ldots, b_{r-1}}] = [b_0, \overline{b_1, \ldots, b_{r-1}, b_0}]. \tag{1.26}$$

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

$$\begin{aligned}\sqrt{d} &= -\lfloor\sqrt{d}\rfloor + \beta = -\lfloor\sqrt{d}\rfloor + [2\lfloor\sqrt{d}\rfloor, \overline{b_1, \ldots, b_{r-1}, b_0}] \\ &= [\lfloor\sqrt{d}\rfloor, \overline{b_1, \ldots, b_{r-1}, b_0}] \\ &= [a_0, \overline{a_1, \ldots, a_{r-1}, 2a_0}].\end{aligned}$$

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

$$\begin{aligned}\beta_1 &= (\sqrt{d} - \lfloor\sqrt{d}\rfloor)^{-1} = -\frac{1}{\beta'} = -\frac{1}{\beta'_r} = (\text{zbog } 1.25) = [b_{r-1}, -\frac{1}{\beta'_{r-1}}] = \cdots \\ &= [b_{r-1}, b_{r-2}, \ldots, b_0, -\frac{1}{\beta'}] = [\overline{b_{r-1}, b_{r-2}, \ldots, b_0}].\end{aligned}$$

Dakle, $\beta = [b_0, \overline{b_{r-1}, b_{r-2}, \ldots, b_0}]$. Usporedimo li ovo s (1.26), dobivamo: $b_1 = b_{r-1}$, $b_2 = b_{r-2}$, $\ldots$. □

Primjer 1.6. *Neka je d prirodan broj. Dokažimo da vrijedi:*

$$\sqrt{d^2+1} = [d, \overline{2d}].$$

Rješenje: Imamo:

$$\begin{aligned}&s_0 = 0,\ t_0 = 1,\ a_0 = d, \\ &s_1 = a_0t_0 - s_0 = d,\ t_1 = \frac{d^2+1-d^2}{1} = 1,\ a_1 = \left\lfloor \frac{d + \lfloor\sqrt{d^2+1}\rfloor}{1} \right\rfloor = 2d, \\ &s_2 = d,\ t_2 = 1.\end{aligned}$$

Dakle, $(s_1, t_1) = (s_2, t_2)$, pa je $\sqrt{d^2+1} = [d, \overline{2d}]$. ♢

Podsjetimo se Worleyevog teorema 1.8, koji kaže da sve racionalne aproksimacije p/q realnog broja α koje zadovoljavaju nejednakost $\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}$ imaju oblik

$$\frac{p}{q} = \frac{rp_{k+1} \pm sp_k}{rq_{k+1} \pm sq_k},$$

za neki $k \geq -1$ i nenegativne cijele brojeve r, s takve da je $rs < 2c$. Pokazat ćemo sada da je ovaj rezultat najbolji mogući u smislu da se uvjet $rs < 2c$ ne može zamijeniti uvjetom $rs < Ac$ za niti jednu konstantu $A < 2$.

Teorem 1.18 (Dujella-Ibrahimpašić (2008))**.** *Za svaki $\varepsilon > 0$ postoji prirodan broj c, realan broj α i racionalan broj $\frac{a}{b}$, tako da vrijedi*

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2},$$

a $\frac{a}{b}$ se ne može prikazati u obliku $\frac{a}{b} = \frac{rp_{k+1} \pm sp_k}{rq_{k+1} \pm sq_k}$, za $k \geq -1$ i nenegativne cijele brojeve r i s takve da je $rs < (2-\varepsilon)c$.

Dokaz: Uzmimo prirodan broj c takav da je $c > \frac{1}{\varepsilon}$. Nadalje, uzmimo $\alpha = \sqrt{4c^2+1}$ i $\frac{a}{b} = 2c + \frac{1}{2c-1} = \frac{2c(2c-1)+1}{2c-1}$. Prema Primjeru 1.6 je

$$\alpha = [2c, \overline{4c}] > 2c + \frac{1}{4c + \frac{1}{4c}} = 2c + \frac{4c}{16c^2+1}.$$

Stoga je

$$\begin{aligned} b^2\left|\alpha - \frac{a}{b}\right| = b^2\left(\frac{a}{b} - \alpha\right) &< \left(\frac{1}{2c-1} - \frac{4c}{16c^2+1}\right)(2c-1)^2 \\ &= \frac{(8c^2+4c+1)(2c-1)}{16c^2+1} = c - \frac{3c+1}{16c^2+1} < c. \end{aligned}$$

Dakle, $\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2}$.

Tvrdimo da se $\frac{a}{b}$ ne može prikazati u obliku $\frac{a}{b} = \frac{rp_{k+1} \pm sp_k}{rq_{k+1} \pm sq_k}$, za $k \geq -1$ i nenegativne cijele brojeve r i s takve da je $rs < (2-\varepsilon)c$.

Ako je $k = -1$, tada iz

$$\begin{aligned} a &= rp_0 + sp_{-1} = 2cr + s, \\ b &= rq_0 + sq_{-1} = r, \end{aligned}$$

slijedi $r = 2c-1$, $s = 1$, $t = sa_1 - r = 2c+1$, i stoga je $rs = 2c-1 > 2c - c\varepsilon = (2-\varepsilon)c$, dok je $st = 2c+1 > 2c$.

Ako je $k \geq 0$, onda iz $s = -bp_{k+1} + aq_{k+1}$ i $\frac{a}{b} > \frac{p_1}{q_1}$ slijedi da je $s \geq \left|\frac{a}{b} - \frac{p_1}{q_1}\right| bq_1 = 2c+1$, i stoga je $rs \geq 2c+1 > 2c$ i $st \geq 2c+1 > 2c$. □

1.7 Pellova i pellovska jednadžba

Definicija 1.10. *Diofantska jednadžba*

$$x^2 - dy^2 = 1, \tag{1.27}$$

gdje je $d \in \mathbb{N}$ *i* d *nije potpun kvadrat, naziva se* Pellova jednadžba. *Jednadžbu oblika*

$$x^2 - dy^2 = N, \tag{1.28}$$

gdje je d *kao gore i* $N \in \mathbb{N}$, *zovemo* pellovska jednadžba.

Ako je $d < 0$, onda očito jednadžbe (1.27) i (1.28) imaju samo konačno mnogo rješenja (jednadžba (1.27) ima samo trivijalna rješenja $(x, y) = (\pm 1, 0)$). Ako je d potpun kvadrat, recimo $d = a^2$, onda jednadžba (1.28) postaje $(x - ay)(x + ay) = N$, pa ponovo imamo samo konačno mnogo rješenja koja odgovaraju faktorizacijama od N. U slučaju kada je d prirodan broj koji nije kvadrat, pokazat ćemo, koristeći razvoj u verižni razlomak broja $\sqrt{d}$, da Pellova jednadžba (1.27) uvijek ima beskonačno mnogo rješenja.

Teorem 1.19. *Neka je* d *prirodan broj koji nije potpun kvadrat. Tada je*

$$p_n^2 - dq_n^2 = (-1)^{n+1} t_{n+1}, \quad \text{za sve } n \geq -1.$$

Nadalje, $t_i = 1$ *ako i samo ako* $r | i$, *gdje* r *označava duljinu najmanjeg perioda u razvoju od* $\sqrt{d}$.

Dokaz: Iz (1.24) 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 da je $\sqrt{d}$ iracionalan, odavde slijedi

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

Eliminirajući s_{n+1}, dobivamo

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

Neka je, kao u dokazu Teorema 1.17, $\beta = \sqrt{d} + \lfloor \sqrt{d} \rfloor$. Iz (1.24), za sve $i \geq 1$ imamo $\beta_i = \alpha_i = \frac{s_i + \sqrt{d}}{t_i}$. Stoga je $t_i = 1$ ako i samo ako je $\beta_i = s_i + \sqrt{d}$. Međutim, β_i ima čisto periodski razvoj, pa je, po Teoremu 1.16, $-1 < s_i - \sqrt{d} < 0$. Odavde je $\sqrt{d} - 1 < s_i < \sqrt{d}$, tj. $s_i = \lfloor \sqrt{d} \rfloor$, pa je $\beta_i = \beta$, a budući da je r duljina najmanjeg perioda, ovo je ekvivalentno sa $r | i$. □

Korolar 1.7. *Ako je r duljina perioda u razvoju od $\sqrt{d}$, onda je*

$$p_{nr-1}^2 - dq_{nr-1}^2 = (-1)^{nr}.$$

Teorem 1.20. *Neka je d prirodan broj koji nije potpun kvadrat, te neka su $\frac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$. Neka je N cijeli broj, $|N| < \sqrt{d}$. 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 $\operatorname{nzd}(E, M) = 1$ 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 $\frac{E}{M} - \sqrt{\varrho} = \frac{\sigma}{M(E+M\sqrt{\varrho})}$ pa je

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

Po Teoremu 1.7, $\frac{E}{M}$ 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 $v^2 - \frac{1}{d}u^2 = -\frac{N}{d}$, pa možemo uzeti $\sigma = -\frac{N}{d}$, $\varrho = \frac{1}{d}$, $E = v$, $M = u$. Dobivamo da je $\frac{v}{u}$ konvergenta u razvoju od $\frac{1}{\sqrt{d}}$. No, ako je $\frac{v}{u}$ n-ta konvergenta od $\frac{1}{\sqrt{d}}$, onda je $\frac{u}{v}$ $(n-1)$-va konvergenta od $\sqrt{d}$, pa je teorem dokazan i u ovom slučaju. □

Iz Teorema 1.19 i 1.20 direktno slijedi sljedeći teorem koji karakterizira rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ i "negativne Pellove jednadžbe" $x^2 - dy^2 = -1$ (te daje uvjet uz koji ova druga ima rješenja).

Teorem 1.21. *Sva rješenja u prirodnim brojevima jednadžbi $x^2 - dy^2 = \pm 1$ nalaze se među $x = p_n$, $y = q_n$, gdje su $\frac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$. Neka je r duljina perioda u razvoju od $\sqrt{d}$.*

Ako je r paran, onda jednadžba $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja od $x^2 - dy^2 = 1$ su dana sa $x = p_{nr-1}$, $y = q_{nr-1}$ za $n \in \mathbb{N}$. Posebno, najmanje rješenje Pellove jednadžbe $x^2 - dy^2 = 1$ je $(x_1, y_1) = (p_{r-1}, q_{r-1})$.

Ako je r neparan, onda su sva rješenja jednadžbe $x^2 - dy^2 = -1$ dana sa $x = p_{nr-1}$, $y = q_{nr-1}$ za n neparan, dok su sva rješenja jednadžbe $x^2 - dy^2 = 1$ dana sa $x = p_{nr-1}$, $y = q_{nr-1}$ za n paran. Posebno, najmanje rješenje Pellove jednadžbe $x^2 - dy^2 = 1$ je $(x_1, y_1) = (p_{2r-1}, q_{2r-1})$.

□

Teorem 1.22. *Ako je (x_1, y_1) najmanje rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$, 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*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n. \tag{1.29}$$

Dokaz: Najprije provjerimo da su (x_n, y_n) zaista rješenja. Budući da je konjugat produkta jednak produktu konjugata, iz (1.29) slijedi $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, pa je

$$x_n^2 - dy_n^2 = (x_n - y_n\sqrt{d})(x_n + y_n\sqrt{d}) = (x_1^2 - dy_1^2)^n = 1.$$

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 $s + t\sqrt{d} > 1$, to postoji $m \in \mathbb{N}$ takav da je

$$(x_1 + y_1\sqrt{d})^m < s + t\sqrt{d} < (x_1 + y_1\sqrt{d})^{m+1}. \tag{1.30}$$

Pomnožimo li (1.30) sa $(x_1 - y_1\sqrt{d})^m = (x_1 + y_1\sqrt{d})^{-m}$, dobivamo

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

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

$$\begin{aligned} 2a &= (a + b\sqrt{d}) + (a - b\sqrt{d}) > 0, \\ 2b\sqrt{d} &= (a + b\sqrt{d}) - (a - b\sqrt{d}) > 0. \end{aligned}$$

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. □

Teorem 1.23. *Neka je (x_n, y_n), $n \in \mathbb{N}$ niz svih rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ u prirodnim brojevima, zapisan u rastućem redosljedu. Uzmimo da je $(x_0, y_0) = (1, 0)$. Tada vrijedi:*

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

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

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

Sada imamo:

$$\begin{aligned} x_{n+2} &= x_1x_{n+1} + dy_1y_{n+1}, \\ x_n &= x_1x_{n+1} - dy_1y_{n+1}, \end{aligned}$$

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

$$\begin{aligned} y_{n+2} &= x_1y_{n+1} + y_1x_{n+1}, \\ y_n &= x_1y_{n+1} - y_1x_{n+1}, \end{aligned}$$

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

Pellovska jednadžba

$$x^2 - dy^2 = N, \tag{1.31}$$

gdje je d prirodan broj koji nije potpun kvadrat i N cijeli broj različit od 0, ne mora imati cjelobrojnih rješenja (vidjeli smo to već u slučaju $N = -1$). No, ukoliko ima barem jedno rješenje, onda ih ima beskonačno mnogo. Zaista, ako je $x + y\sqrt{d}$ rješenje jednadžbe 1.31, a $u + v\sqrt{d}$ rješenje pripadne Pellove jednadžbe $x^2 - dy^2 = 1$, onda je

$$(x + y\sqrt{d})(u + v\sqrt{d}) = (ux + dvy) + (uy + vx)\sqrt{d} \tag{1.32}$$

također rješenje jednadžbe (1.31), jer je

$$(ux + dvy)^2 - d(uy + vx)^2 = (x^2 - dy^2)(u^2 - dv^2) = N \cdot 1 = N.$$

Budući da Pellova jednadžba ima beskonačno mnogo rješenja, to iz (1.32) slijedi da i jednadžba (1.31) ima beskonačno rješenja (uz pretpostavku da ima barem jedno).

Za dva rješenja $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ jednadžbe (1.31) kažemo da su *asocirana* ako se jedno iz drugog može dobiti množenjem s nekim rješenjem Pellove jednadžbe kao u formuli (1.32). Lako se provjerava da je na ovaj način uvedena relacija ekvivalencije na skupu svih rješenja jednadžbe (1.31) (podsjetimo se da je $(u+v\sqrt{d})^{-1} = u - v\sqrt{d}$, što povlači simetričnost). Reći ćemo da međusobno asocirana rješenja tvore jednu *klasu rješenja*. Nije teško za vidjeti da su $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ asocirani ako i samo ako vrijedi

$$xx' \equiv dyy' \pmod{N}, \quad xy' \equiv x'y \pmod{N}.$$

Neka je $\mathbf{K}$ jedna klasa rješenja, te neka su njeni elementi $x_i + y_i\sqrt{d}$, $i = 1, 2, 3, \ldots$. Tada klasu koja se sastoji od rješenja $x_i - y_i\sqrt{d}$ označavamo s $\bar{\mathbf{K}}$ i kažemo da je *konjugirana* klasi $\mathbf{K}$. Ako vrijedi da je $\mathbf{K} = \bar{\mathbf{K}}$, onda kažemo da je klasa $\mathbf{K}$ *dvoznačna*.

Među svim elementima klase $\mathbf{K}$ odabrat ćemo jedan, $x^* + y^*\sqrt{d}$, kojeg ćemo zvati *fundamentalno rješenje jednadžbe* $x^2 - dy^2 = N$ *u klasi* $\mathbf{K}$. Biramo ga tako da y^* poprimi najmanju moguću nenegativnu vrijednost među svim elementima $x + y\sqrt{d}$ u klasi $\mathbf{K}$. Ovim je zahtjevom i x^* jednoznačno određen, osim u slučaju kada je $\mathbf{K}$ dvoznačna. Ako je $\mathbf{K}$ dvoznačna, onda izabiremo x^* tako da zadovolji i dodatni uvjet da je $x^* \geq 0$. Uočimo da $|x^*|$ poprima najmanju moguću vrijednost unutar klase $\mathbf{K}$.

Teorem 1.24. *Neka je* $u + v\sqrt{d}$ *fundamentalno rješenje jednadžbe* $x^2 - dy^2 = 1$. *Tada za svako fundamentalno rješenje* $x^* + y^*\sqrt{d}$ *jednadžbe* $x^2 - dy^2 = N$ *vrijede nejednakosti:*

$$0 \leq y^* \leq \frac{v}{\sqrt{2(u+\varepsilon)}}\sqrt{|N|},$$

$$|x^*| \leq \sqrt{\frac{1}{2}(u+\varepsilon)|N|},$$

gdje je $\varepsilon = 1$ *ako je* $N > 0$, *a* $\varepsilon = -1$ *ako je* $N < 0$. *Posebno, fundamentalnih rješenja (pa i klasa rješenja) ima konačno mnogo.*

Dokaz: Dokazat ćemo tvrdnju za $N < 0$. Dokaz za $N > 0$ je analogan. Definirajmo cijele brojeve x', y' sa $x' + y'\sqrt{d} = (x^* + y^*\sqrt{d})(u - \delta v\sqrt{d})$, gdje je $\delta = 1$ ako je $x^* \geq 0$, a $\delta = -1$ ako je $x^* < 0$. Tada $x' + y'\sqrt{d}$ pripada istoj klasi kao i $x^* + y^*\sqrt{d}$, pa zbog minimalnosti od y^* zaključujemo da je

$$y' = uy^* - \delta v x^* \geq y^*,$$

što povlači $v|x^*| \leq (u-1)y^*$. Kvadriranjem dobivamo

$$v^2(dy^{*2} + N) \leq (u^2 - 2u + 1)y^{*2},$$

tj. $y^{*2}(2u-2) \leq |N| \cdot v^2$, pa dobivamo traženu nejednakost za y^*. Sada je

$$x^{*2} = dy^{*2} + N \leq \frac{-dNv^2}{2u-2} + N = \frac{-N(u^2-2u+1)}{2u-2} = \frac{|N| \cdot (u-1)}{2}.$$

□

Prema Teorem 1.20, rješivost jednadžbe $x^2 - dy^2 = N$ u relativno prostim cijelim brojevima x, y, ako je $|N| < \sqrt{d}$, možemo ustanoviti tako da $\sqrt{d}$ razvijemo u verižni razlomak, te provjerimo zadovoljava li neka od prvih $2r$ konvergenti relaciju

$$p_i^2 - dq_i^2 = (-1)^{i+1}t_{i+1} = N.$$

Ako $|N|$ nije puno veći od $\sqrt{d}$ (npr. $|N| < 4\sqrt{d}$), onda možemo koristiti Worleyev teorem 1.8 umjesto Legendreovog teorema. Pritom koristimo relaciju

$$(rp_i \pm sp_{i-1})^2 - d(rq_i \pm sq_{i-1})^2 = (-1)^{i+1}(r^2 t_{i+1} - s^2 t_i \mp 2rss_{i+1}), \quad (1.33)$$

koja je analogon formule iz Teorema 1.19.

Za rješenje $x_0 + y_0\sqrt{d}$ kažemo da je *primitivno* ako su x_0 i y_0 relativno prosti. Ako je $\text{nzd}(x_0, y_0) = g$, onda je $\frac{x_0}{g} + \frac{y_0}{g}\sqrt{d}$ primitivno rješenje jednadžbe $x^2 - dy^2 = \frac{N}{g^2}$.

Primjer 1.7. *Neka je* k *prirodan broj. Odrediti sve prirodne brojeve* N *takve da je* $N < 4k$ *i da jednadžba*

$$x^2 - (k^2+1)y^2 = N$$

ima primitivno rješenje.

Rješenje: Imamo da je

$$0 < \frac{x}{y} - \sqrt{k^2+1} < \frac{N}{2\sqrt{k^2+1}y^2} < \frac{2k}{\sqrt{k^2+1}y^2} < \frac{2}{y^2}.$$

Po Teoremu 1.19, brojevi x i y imaju oblik $x = rp_i \pm sp_{i-1}$, $y = rq_i \pm sq_{i-1}$, gdje je $rs < 4$. Iz Primjera 1.6 znamo da broj $\sqrt{k^2+1}$ ima vrlo jednostavan razvoj u verižni razlomak:

$$\sqrt{k^2+1} = [k; \overline{2k}].$$

Nadalje, $s_i = k$, $t_i = 1$ za svaki $i \geq 1$. Zato je u formulu (1.33) dovoljno uvrstiti $i = 1$, te $(r, s) = (1, 0), (1, 1), (1, 2), (2, 1), (1, 3), (3, 1)$. Dobivaju se sljedeće vrijednosti od N koje zadovoljavaju uvjet $0 < N < 4k$:

$$N = 1,\ 2k,\ 4k-3 \quad (\text{za svaki } k \in \mathbb{N}),$$

te još dodatno $N = 10$ za $k = 3$ (što je jednako $6k - 8$). ♢

Poglavlje 2

Simultane aproksimacije

2.1 Dirichletov teorem o simultanim aproksimacijama

Teorem 2.1. *Neka su $\alpha_1, \ldots, \alpha_n$ realni brojevi, te $Q > 1$ prirodan broj. Tada postoje cijeli brojevi $q, p_1, \ldots, p_n$ takvi da je*

$$1 \leq q < Q^n, \quad i \quad |\alpha_i q - p_i| \leq \frac{1}{Q}, \ i = 1, \ldots, n. \tag{2.1}$$

Korolar 2.1. *Pretpostavimo da je barem jedan od brojeva $\alpha_1, \ldots, \alpha_n$ iracionalan. Tada postoji beskonačno mnogo m-torki $\frac{p_1}{q}, \ldots, \frac{p_n}{q}$ sa svojstvom*

$$|\alpha_i - \frac{p_i}{q}| < \frac{1}{q^{1+1/n}}, \quad i = 1, \ldots, n. \tag{2.2}$$

Dokaz Korolara 2.1: U Teoremu 2.1 možemo dodatno zahtijevati da je $\text{nzd}(q, p_1, \ldots, p_n) = 1$. Očito je da nejednakosti (2.1) povlače nejednakost (2.2).

Neka je, recimo, α_1 iracionalan. Tada je $|\alpha_1 q - p_1| \neq 0$. Zato, za fiksne $q, p_1, \ldots, p_n$, nejednakosti (2.1) mogu vrijediti samo za $Q \leq Q_0 = \frac{1}{|\alpha_1 q - p_1|}$. Prema tome, kad $Q \to \infty$, dobivamo beskonačno mnogo različitih rješenja. □

Teorem 2.2. *Neka su dani $\alpha_1, \ldots, \alpha_n$ i Q kao u Teoremu 2.1. Tada postoje cijeli brojevi $q_1, \cdots, q_n, p$ takvi da je*

$$1 \leq \max(|q_1|, \ldots, |q_n|) < Q^{1/n} \quad i \quad |\alpha_1 q_1 + \cdots + \alpha_n q_n - p| \leq \frac{1}{Q}. \tag{2.3}$$

Korolar 2.2. *Pretpostavimo da su $1, \alpha_1, \cdots, \alpha_n$ linearno nezavisni nad $\mathbb{Q}$. Tada postoji beskonačno mnogo $(n+1)$-torki relativno prostih brojeva $(q_1, \ldots, q_n, p)$ sa svojstvom*

$$q = \max(|q_1|, \ldots, |q_n|) > 0 \quad i \quad |\alpha_1 q_1 + \cdots + \alpha_n q_n - p| < \frac{1}{q^n}. \tag{2.4}$$

Dokaz Korolara 2.2: Očito je da (2.3) povlači (2.4). Zbog linearne nezavisnosti, uvijek vrijedi $|\alpha_1 q_1 + \cdots + \alpha_n q_n - p| \neq 0$. Zbog toga, za fiksne $q_1, \ldots, q_n, p$, nejednakost (2.3) vrijedi samo za $Q \leq Q_0 = \frac{1}{|\alpha_1 q_1 + \cdots + \alpha_n q_n - p|}$. Prema tome, kad $Q \to \infty$, dobivamo beskonačno mnogo različitih rješenja. □

Teorem 2.3 (Dirichlet (1842))**.** *Neka su α_{ij} $(i = 1, \ldots, n;\ j = 1, \ldots, m)$ realni brojevi, $Q > 1$ prirodan broj. Tada postoje cijeli brojevi $q_1, \ldots, q_m$, $p_1, \ldots, p_n$ takvi da je*

$$1 \leq \max(|q_1|, \ldots, |q_n|) < Q^{n/m},$$
$$|\alpha_{i1} q_1 + \cdots + \alpha_{im} q_m - p_i| \leq \frac{1}{Q}, \quad i = 1, \ldots, n. \tag{2.5}$$

Napomena 2.1. Pretpostavka da je Q prirodan broj nije nužna, kao što ćemo pokazati u sljedećem odjeljku. Teoremi 2.1 i 2.2 su specijalni slučajevi Teorema 2.3 (dobivaju se za $n = 1$, odnosno $m = 1$).

Dokaz Teorema 2.3: Promotrimo točke

$$(\{\alpha_{11} x_1 + \cdots + \alpha_{1m} x_m\}, \ldots, \{\alpha_{n1} x_1 + \cdots + \alpha_{nm} x_m\}),$$

gdje su x_j, $j = 1 \ldots, m$, cijeli brojevi koji zadovoljavaju uvjet $0 \leq x_j < Q^{n/m}$. Postoji barem Q^n takvih točaka i svaka od njih leži u zatvorenoj jediničnoj kocki $I^n = \{(t_1, \ldots, t_n) : 0 \leq t_k \leq 1,\ k = 1, \ldots, n\}$. Također je i $(1, 1, \ldots, 1) \in I^n$, pa zajedno s ovom točkom promatramo barem $Q^n + 1$ točaka iz I^n.

Podijelimo I^n na Q^n u parovima disjunktnih potkocaka čiji su bridovi duljine $\frac{1}{Q}$. (Dakle, potkocke sadrže neke od svojih strana ili bridova, a neke ne.) Po Dirichletovom principu, dvije od promatranih točaka nalaze se u istoj potkocki. Recimo da su to točke

$$(\alpha_{11} x_1 + \cdots + \alpha_{1m} x_m - y_1, \ldots, \alpha_{n1} x_1 + \cdots + \alpha_{nm} x_m - y_n),$$

$$(\alpha_{11} x'_1 + \cdots + \alpha_{1m} x'_m - y'_1, \ldots, \alpha_{n1} x'_1 + \cdots + \alpha_{nm} x'_m - y'_n).$$

Ovdje je $(x_1, \ldots, x_m) \neq (x'_1, \ldots, x'_m)$. Stavimo $q_j = x_j - x'_j$ za $j = 1, \ldots, m$, te $p_i = y_i - y'_i$ za $i = 1, \ldots, n$. Tada je (2.5) očito zadovoljeno. □

2.2 Teoremi Blichfeldta i Minkowskog

U daljnjem će nam E^n označavati realni n-dimenzionalni euklidski prostor, čije ćemo točke označavati sa $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$, itd. S U ćemo označavati jedinični interval $[0, 1\rangle$, a s U^n jediničnu kocku koja se sastoji od svih točaka $x = (x_1, \ldots, x_n)$ takvih da je $x_k \in U$ za $k = 1, \ldots, n$. S I^n ćemo označavati zatvarač od U^n (tj. zatvorenu jediničnu kocku).

Za $x = (x_1, \ldots, x_n) \in E^n$ definiramo

$$\|x\| = \max(|x_1|, \ldots, |x_n|).$$

Ako su svi x_k cijeli brojevi, reći ćemo da je x *cjelobrojna točka*.

Neka je $S \subseteq E^n$. Ako je $x \in E^n$, sa $S + x$ označit ćemo *translaciju* od S za x, tj. skup svih točaka oblika $s + x = (s_1 + x_1, \ldots, s_n + x_n)$ za $s \in S$. Ako je $\lambda \in \mathbb{R}$, tada λS označava skup svih točaka oblika $\lambda s = (\lambda s_1, \ldots, \lambda s_n)$ za $s \in S$.

Teorem 2.4 (Blichfeldt (1914))**.** *Neka je $\mathcal{P}$ diskretan skup u E^n (tj. skup bez gomilišta), invarijantan s obzirom na translacije za cjelobrojne točke, te s točno N točaka u U^n. Neka je $\mathcal{R} \subseteq E^n$ izmjeriv skup mjere (volumena) $\mu(\mathcal{R}) > 0$. Tada postoji točka x u U^n takva da $\mathcal{R} + x$ sadrži barem $N\mu(\mathcal{R})$ točaka od $\mathcal{P}$. Štoviše, ako je $\mathcal{R}$ kompaktan, onda postoji translacija od $\mathcal{R}$ koja sadrži više od $N\mu(\mathcal{R})$ točaka od $\mathcal{P}$.*

Dokaz: Označimo s $\nu(S)$ broj točaka od $\mathcal{P}$ koje leže u skupu S. Skup $\mathcal{P}$ ima N točaka u U^n, recimo da su to točke $p^1, \ldots, p^N$. Označimo sa $\nu_i(S)$, $i = 1, \ldots, n$, broj točaka oblika $p^i + g$ (gdje je g cjelobrojna točka) koje leže u S. Budući da je $\mathcal{P}$ invarijantan s obzirom na translacije za cjelobrojne točke, imamo:

$$\nu(S) = \sum_{i=1}^{N} \nu_i(S). \tag{2.6}$$

Za svaki $i = 1, \ldots, n$ vrijedi

$$\nu_i(\mathcal{R} + x) = \sum_g \chi(p^i + g - x),$$

gdje je χ karakteristična funkcija skupa $\mathcal{R}$, a sumira se po svim cjelobrojnim točkama $g \in E^n$. Sada imamo:

$$\mu(\mathcal{R}) = \int_{E^n} \chi(z)dz = \int_{E^n} \chi(p^i - z)dz = \int_{U^n} (\sum_g (\chi(p^i + g - x))dx = \int_{U^n} \nu_i(\mathcal{R} + x)dx.$$

Iz (2.6) slijedi da je $\int_{U^n} \nu(\mathcal{R} + x)dx = N\mu(\mathcal{R})$. Stoga je $\nu(\mathcal{R} + x) \geq N\mu(\mathcal{R})$ za neki $x \in U^n$.

Neka je sada $\mathcal{R}$ kompaktan. Tada nemamo što dokazivati ukoliko $N\mu(\mathcal{R})$ nije prirodan broj. Pa neka je $N\mu(\mathcal{R}) = \nu_0$ prirodan broj. Iz prvog dijela dokaza slijedi da za svaki prirodan broj k postoji točka $x^k \in U^n$ takva da za skup

$$S_k = (1 + \frac{1}{k})\mathcal{R} + x^k$$

vrijedi $\nu(S_k) \geq \nu_0 + 1$. Budući da točke x^k leže u kompaktnom skupu I^n, to niz $(x_k)_{k=1}^{\infty}$ ima konvergentan podniz $(x^{k_j})_{j=1}^{\infty}$. Neka je $\lim_j x^{k_j} = x^0$.

Zbog kompaktnosti od $\mathcal{R}$ i I^n, familija skupova S_{k_j} je uniformno omeđena, tj. postoji $\lambda \in \mathbb{R}$ takav da je $S_{k_j} \subseteq \lambda[-1,1]^n$ za sve j. Neka je sada $v^j \in \mathcal{P} \cap S_{k_j}$. Tada niz $(v^j)_{j=1}^{\infty}$ ima konvergentan podniz, pa jer je $\mathcal{P}$ diskretan, taj podniz je stacionaran počevši od nekog mjesta. Odavde i iz $\nu(S_{k_j}) \geq \nu_0 + 1$ zaključujemo da postoji $\nu_0 + 1$ točaka $u^1, \ldots, u^{\nu_0+1}$ koje leže u beskonačno mnogo skupova S_{k_j}. Naime, pokazali smo već da postoji u^1 koji je element beskonačno mnogo skupova S_{k_j}. Primijenimo li isto razmatranje na skupove $\mathcal{P} \cap (S_{k_j} \setminus \{u^1\})$, dobivamo točku u^2, itd.

Dokažimo sada da je $u^i \in \mathcal{R} + x^0$ za $i = 1, \ldots, \nu_0 + 1$. Pretpostavimo suprotno, tj. $u^i \notin \mathcal{R} + x^0$ za neki i. Zbog kompaktnosti od $\mathcal{R} + x^0$ je $d_\infty(u^i, \mathcal{R} + x^0) = \varepsilon > 0$. S druge strane, postoji $j_0 \in \mathbb{N}$ takav da je za sve $j \geq j_0$, $\|x^{k_j} - x^0\| < \frac{\varepsilon}{2}$ i $\frac{1}{k_j} \max_{r \in \mathcal{R}} \|r\| < \frac{\varepsilon}{2}$. Također, postoji $l \geq j_0$ takav da je $u^i \in S_{k_l}$. Neka je $r \in \mathcal{R}$ takav da je $u^i = (1 + \frac{1}{k_l})r + x^{k_l}$. Tada je

$$d_\infty(u^i, \mathcal{R} + x^0) \leq \|u^i - r - x^0\| = \|\frac{r}{k_l} + x^{k_l} - x^0\| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Kontradikcija.

Dakle, $u^1, \ldots, u^{\nu_0+1} \in \mathcal{R} + x^0$, što znači da je

$$\nu(\mathcal{R} + x^0) \geq \nu_0 + 1 > N\mu(\mathcal{R}),$$

pa je dokaz gotov ukoliko je $x^0 \in U^n$. Ako $x^0 \notin U^n$, onda zamijenimo x^0 točkom u U^n koja se dobije iz nje translacijom za cjelobrojnu točku. □

Napomena 2.2. Pomoću Teorema 2.4 možemo dokazati da tvrdnja Teorema 2.3 vrijedi za sve realne brojeve $Q > 1$. Naime, promotrimo točke

$$(\alpha_{11}x_1 + \cdots + \alpha_{1m}x_m, \ldots, \alpha_{n1}x_1 + \cdots + \alpha_{nm}x_m),$$

gdje su x_j, $j = 1, \ldots, m$, cijeli brojevi koji zadovoljavaju uvjet $0 \leq x_j < Q^{n/m}$. Neka je $\mathcal{P}$ skup svih takvih točaka zajedno sa svim njihovim translacijama za cjelobrojne točke. Uočimo da broj N točaka iz $\mathcal{P}$ koje leže u U^n zadovoljava $N \geq Q^n$. Neka je $\mathcal{R}$ kocka $\{(t_1, \ldots, t_n) : 0 \leq t_k \leq \frac{1}{Q}\}$. Tada je skup $\mathcal{R}$ kompaktan i $\mu(\mathcal{R}) = \frac{1}{Q^n}$. Teorem 2.4 povlači da postoji translacija $\mathcal{R} + x$ za koju vrijedi $\nu(\mathcal{R} + x) > N\mu(\mathcal{R}) \geq 1$, tj. $\nu(\mathcal{R} + x) \geq 2$. Dalje dokaz ide isto kao u gore navedenom dokazu Teorema 2.3.

Teorem 2.5 (Teorem Minkowskog o konveksnom tijelu (1896))**.** *Neka je $\mathcal{R}$ konveksan skup u E^n, simetričan s obzirom na ishodište i omeđen, te neka $\mathcal{R}$ ima volumen $\mu(\mathcal{R})$. Pretpostavimo da je $\mu(\mathcal{R}) > 2^n$ ili da je $\mathcal{R}$ kompaktan i $\mu(\mathcal{R}) \geq 2^n$. Tada $\mathcal{R}$ sadrži cjelobrojnu točku različitu od ishodišta.*

Napomena 2.3. Ako promotrimo kocku $\mathcal{R} = \{(x_1, \ldots, x_n) : |x_i| < 1\}$ za koju je $\mu(\mathcal{R}) = 2^n$, vidimo da je tvrdnja Teorema 2.5 najbolja moguća

Dokaz Teorema 2.5: Imamo da je $\mu(\frac{1}{2}\mathcal{R}) > 1$ ili je $\mathcal{R}$ kompaktan i $\mu(\frac{1}{2}\mathcal{R}) \geq 1$. U svakom slučaju, primjenjujemo Teorem 2.4 na skupove $\frac{1}{2}\mathcal{R}$ i $\mathcal{P}$, gdje je $\mathcal{P}$ skup svih cjelobrojnih točaka u E^n. Zaključujemo da postoji translacija $\frac{1}{2}\mathcal{R}+x$ koja sadrži barem dvije različite cjelobrojne točke, recimo g^1 i g^2.

Dakle, $g^1 - x \in \frac{1}{2}\mathcal{R}$ i $g^2 - x \in \frac{1}{2}\mathcal{R}$. Zbog simetrije je i $x - g^2 \in \frac{1}{2}\mathcal{R}$. Stoga možemo staviti da je $g^1 - x = \frac{1}{2}x^1$, $x - g^2 = \frac{1}{2}x^2$, gdje su $x^1, x^2 \in \mathcal{R}$. Skup $\mathcal{R}$ je konveksan, pa je $g = g^1 - g^2 = \frac{1}{2}x^1 + \frac{1}{2}x^2 \in \mathcal{R}$. Prema tome, točka g zadovoljava uvjet teorema. □

Teorem 2.6 (Teorem Minkowskog o linearnim formama)**.** *Neka su β_{ij}, $1 \leq i, j \leq n$, realni brojevi takvi da je determinanta matrice (β_{ij}) jednaka ± 1, te neka su $A_1, \ldots, A_n$ pozitivni brojevi sa svojstvom $A_1 A_2 \cdots A_n = 1$. Tada postoji cjelobrojna točka $x = (x_1, \ldots, x_n) \neq O$, takva da je*

$$|\beta_{i1}x_1 + \cdots + \beta_{in}x_n| < A_i, \quad i = 1, \ldots, n-1, \tag{2.7}$$

$$|\beta_{n1}x_1 + \cdots + \beta_{nn}x_n| \leq A_n. \tag{2.8}$$

Dokaz: Uvedimo oznake

$$L_i(x) = \beta_{i1}x_1 + \cdots + \beta_{in}x_n, \quad L_i'(x) = \frac{1}{A_i}L_i(x), \quad i = 1, \ldots, n.$$

Tada (2.7) i (2.8) možemo zapisati kao

$$|L_i'(x)| < 1, \quad i = 1, \ldots, n-1,$$
$$|L_n'(x)| \leq 1.$$

Determinanta od $L_1', \ldots, L_n'$ je opet jednaka $\det(\beta_{ij}) = \pm 1$ (zbog $A_1 \cdots A_n = 1$), pa bez smanjenja općenitosti možemo od početka pretpostaviti da je $A_1 = \cdots = A_n = 1$.

Osnovna ideja dokaza je sljedeća. Promotrimo skup $\mathcal{R} = \{x \in E^n : |L_i(x)| \leq 1, i = 1, \ldots, n\}$. Neka je $V^n = \{(x_1, \ldots, x_n) : |x_i| \leq 1\}$, te neka je $B : E^n \to E^n$ linearni operator čija je matrica u kanonskom paru baza jednaka (β_{ij}). Tada je $B^{-1}(V^n) = \mathcal{R}$. Dakle, $\mathcal{R}$ je dobiven iz V^n pomoću linearnog operatora čija je determinanta jednaka ± 1. Prema tome, $\mathcal{R}$ je simetričan zatvoren paralelepiped volumena 2^n.

Po Teoremu Minkowskog o konveksnom tijelu, postoji cjelobrojna točka $x \neq O$ u ovom paralelepipedu.

Da bi dobili strogu nejednakost u prvih $n-1$ nejednakosti, napravit ćemo sljedeću modifikaciju. Za svaki $\varepsilon > 0$, sustav nejednadžbi

$$|L_i(x)| < 1,\ i = 1, \ldots, n-1, \quad |L_i(x)| < 1 + \varepsilon$$

definira simetričan paralelepiped Π_ε volumena $2^n(1+\varepsilon) > 2^n$. Po Teoremu 2.5, postoji cjelobrojna točka $x_\varepsilon \neq O$ u Π_ε. Neka je $\varepsilon_k = \frac{1}{k}$, $k \in \mathbb{N}$. Pomoću

niza (ε_k) dobivamo niz $(x_{\varepsilon_k})_{k=1}^{\infty}$ cjelobrojnih točaka različitih od ishodišta, $x_{\varepsilon_k} \in \Pi_{\varepsilon_k}$. Familija svih paralelepipeda Π_{ε_k} je uniformno omeđena, pa postoji cjelobrojna točka $x \neq O$ takva da je $x = x_{\varepsilon_k}$ za beskonačno mnogo k-ova. Stoga je $x \in \Pi_{\varepsilon_k}$ za beskonačno mnogo k-ova, pa x zadovoljava (2.7) i (2.8). □

Drugi dokaz Teorema 2.3: Stavimo $l = m + n$ i promotrimo sljedećih l linearnih formi u $x = (x_1, \ldots, x_n)$:

$$\begin{aligned} L_i(x) &= x_i, \quad i = 1, \ldots, m, \\ L_{m+j}(x) &= \alpha_{j1}x_1 + \cdots \alpha_{jm}x_m - x_{m+j}, \quad j = 1, \ldots, n. \end{aligned}$$

Njihova determinanta je

$$\begin{vmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ & \vdots & & & & \vdots & \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ \alpha_{11} & \cdots & & \alpha_{1m} & -1 & 0 \cdots & 0 \\ & \vdots & & & & \vdots & \\ \alpha_{n1} & \cdots & & \alpha_{nm} & 0 & \cdots 0 & -1 \end{vmatrix} = \pm 1.$$

Neka je $Q > 1$ realan broj (ne nužno prirodan). Po Teoremu 2.6 postoji cjelobrojna točka $x \neq O$ takva da je

$$\begin{aligned} |L_i(x)| &< Q^{n/m}, \quad i = 1, \ldots, m, \\ |L_{m+j}(x)| &\leq Q^{-1}, \quad j = 1, \ldots, n, \end{aligned}$$

jer je $(Q^{n/m})^m \cdot (Q^{-1})^n = 1$.

Stavimo $q_i = x_i$, $i = 1, \ldots, m$, te $p_j = x_{m+j}$, $j = 1, \ldots, n$. Tada je

$$q = \max(|q_1|, \ldots, |q_m|) < Q^{n/m}$$

i

$$|\alpha_{j1}q_1 + \cdots + \alpha_{jm}q_m - p_j| \leq \frac{1}{Q}, \quad j = 1, \ldots, m.$$

Preostaje pokazati da je $q \geq 1$. U protivnom bi bilo $q_i = 0$ za $i = 1, \ldots, m$, te stoga $|p_j| \leq \frac{1}{Q} < 1$ za $j = 1, \ldots, n$. Ali to znači da su svi $p_j = 0$, pa je $x = O$. Kontradikcija. □

2.3 LLL algoritam

Iako su Dirichletovi teoremi o simultanim aproksimacijama direktna poopćenja (običnog) Dirichletovog teorema za $n = 1$, kada je u pitanju efektivna algoritamska realizacija pronalaženja racionalnih brojeva čiju egzistenciju garantiraju ti teoremi, postoji bitna razlika između slučajeva $n = 1$ i $n \geq 2$. Naime, u slučaju $n = 1$, kao što smo već vidjeli, racionalne aproksimacije sa željenim svojstvom možemo dobiti pomoću verižnih razlomaka. U slučaju $n \geq 2$, situacija je u tom pogledu složenija. Postoje različita poopćenja verižnih razlomaka, odnosno njihovih svojstava, na više dimenzije. Mi ćemo obraditi jednu, vjerojatno najpoznatiju, i za brojne primjene najvažniju, a to je tzv. LLL algoritam. On će nam efikasno (u polinomijalnom vremenu) dati racionalne aproksimacije slične kvalitete kao one koje garantiraju Dirichletovi teoremi (pojavit će se neki dodatni faktori u odnosu na kvalitetu optimalnih aproksimacija koje daje teorija).

LLL algoritam je povezan s problemom nalaženja najkraćeg nenul vektora u rešetki.

Definicija 2.1. *Neka je n prirodan broj te neka su $b_1, \ldots, b_n$ linearno nezavisni vektori u $\mathbb{R}^n$.* Rešetka *($\mathbb{Z}$-modul) L razapeta ovim vektorima je skup svih njihovih cjelobrojnih linearnih kombinacija:*

$$L = \left\{ \sum_{i=1}^{n} x_i \cdot b_i \,:\, x_i \in \mathbb{Z} \right\}.$$

Kaže se da je $B = \{b_1, \ldots, b_n\}$ baza rešetke *L.*

Npr. u $\mathbb{R}^2$, ako je $b_1 = (1, 0)$, $b_2 = (0, 1)$, onda je L rešetka svih točaka u ravnini s cjelobrojnim koordinatama.

S B ćemo označavati i matricu čiji su stupci vektori $b_1, \ldots, b_n$. Determinanta rešetke L se definira sa $\Delta(L) = |\det(B)|$. Ova definicija je dobra, jer je baza rešetke jedinstvena do na množenje zdesna s matricama iz $GL_n(\mathbb{Z})$, tj. matricama s cjelobrojnim koeficijentima i determinantnom ± 1.

Sa $\langle\, , \,\rangle$ ćemo označavati standardni skalarni produkt u $\mathbb{R}^n$. Primijetimo da kvadrat euklidske norme vektora $v = \sum_{i=1}^{n} x_i \cdot b_i$ inducira kvadratnu formu

$$\|v\|^2 = v^\tau v = x^\tau B^\tau B x = Q(x).$$

Budući da je rešetka diskretan skup, dobro je definiran pojam duljine najkraćeg nenul vektora rešetke. Iz Teorema Minkowskog o konveksnom tijelu slijedi da ako je C kompaktan, konveksan skup, simetričan s obzirom na ishodište, te ako je $\mu(C) \geq 2^n \Delta(L)$, onda C sadrži nenul vektor iz L (primijenimo Teorem 2.5 na skup $B^{-1}(C)$). Ako sada za C uzmemo n-dimenzionalnu kuglu, dobivamo gornju ocjenu za duljinu najkraćeg nenul vektora u rešetki.

Propozicija 2.1. *Postoji konstanta γ_n takva da vrijedi*

$$\min_{v\in L\setminus\{0\}} \|v\| \leq \sqrt{\gamma_n}\Delta(L)^{1/n}.$$

Optimalne vrijednosti od γ_n su poznate za $n \leq 8$. Primjerice, $\gamma_1 = 1$, $\gamma_2 = \frac{4}{3}$, $\gamma_3 = 2$.

Jedna rešetka može imati više različitih baza, pa se pitamo možemo li izabati bazu koja bi imala neko dodatno dobro svojstvo. Jasno je da B predstavlja bazu vektorskog prostora $\mathbb{R}^n$. Znamo da Gram-Schmidtovim postupkom možemo dobiti ortogonalnu bazu za isti vektorski prostor ($b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*$, $i = 1, \ldots, n$, gdje je $\mu_{ij} = \frac{\langle b_i, b_j^*\rangle}{\langle b_j^*, b_j^*\rangle}$). No, ta nova baza ne mora razapinjati istu rešetku kao polazna baza B, jer koeficijenti μ_{ij} ne moraju biti cijeli brojevi. Općenito, rešetka ni ne mora imati ortogonalnu bazu. A. K. Lenstra, H. W. Lenstra i L. Lovász uveli su *pojam LLL-reducirane baze*, koja ima svojstva:

1) $|\mu_{i,j}| \leq \frac{1}{2}$, $1 \leq j < i \leq n$;

2) $\|b_i^*\|^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)\|b_{i-1}^*\|^2$.

Prvi uvjet se može interpretirati tako da se kaže da je LLL-reducirana baza "skoro ortogonalna", dok drugi uvjet govori da niz normi vektora $\|b_i^*\|$ "skoro raste". Dodatno važno svojstvo LLL-reducirane baze je da je prvi vektor u toj bazi vrlo kratak, tj. ima malu normu. Može se dokazati da uvijek vrijedi da je $\|b_1\| \leq 2^{(n-1)/2}\|x\|$, za sve ne-nul vektore $x \in L$, no, u praksi se vrlo često događa da je $\|b_1\|$ upravo najkraći ne-nul vektor iz L. To ćemo precizirati u sljedećoj lemi.

Lema 2.1. *Neka je $\{b_1, \ldots, b_n\}$ LLL-reducirana baza, te $\{b_1^*, \ldots, b_n^*\}$ pripadna Gram-Schmidtova baza. Tada vrijedi:*

1) $\|b_j\|^2 \leq 2^{i-1}\|b_i^*\|^2$, $1 \leq j \leq i \leq n$;

2) $\Delta(L) \leq \prod_{i=1}^n \|b_i\| \leq 2^{n(n-1)/4}\Delta(L)$;

3) $\|b_1\| \leq 2^{(n-1)/4}\left(\Delta(L)\right)^{1/n}$;

4) Za svaki $x \in L$, $x \neq 0$, vrijedi $\|b_1\|^2 \leq c_1\|x\|^2$, gdje je

$$c_1 = \max\left\{\frac{\|b_1\|^2}{\|b_i^*\|^2} \,:\, 1 \leq i \leq n\right\} \leq 2^{n-1}.$$

5) Za vektor $y \notin L$ definiramo $\sigma = B^{-1}y$, gdje je B matrica čiji su stupci $b_1, \ldots, b_n$. Neka je i_0 najveći indeks takav da $\sigma_{i_0} \notin \mathbb{Z}$, te $\|\sigma_{i_0}\|$ udaljenost od σ_{i_0} do najbližeg cijelog broja. Tada za svaki $x \in L$ vrijedi

$$\|x - y\|^2 \geq c_1^{-1}\|\sigma_{i_0}\|^2\|b_1\|^2.$$

Dokaz: 1) Iz definicije LLL-reducirane baze slijedi

$$\|b_i^*\|^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)\|b_{i-1}^*\|^2 \geq \frac{1}{2}\|b_{i-1}^*\|^2$$

za $i = 1, 2, \ldots, n$. Odavde indukcijom slijedi $\|b_j^*\|^2 \leq 2^{i-j}\|b_i^*\|^2$ za $1 \leq j \leq i \leq n$. Sada iz definicije Gram-Schmidtove baze dobivamo

$$\begin{aligned}\|b_i\|^2 &= \|b_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 \|b_j^*\|^2 \leq \left(1 + \sum_{j=1}^{i-j} 2^{i-j-2}\right) \|b_i^*\|^2 \\ &= \left(1 + \frac{1}{4}(2^i - 2)\right) \|b_i^*\|^2 \leq 2^{i-1}\|b_i^*\|^2.\end{aligned}$$

Dakle, za $1 \leq j \leq i \leq n$ vrijedi

$$\|b_j\|^2 \leq 2^{j-1}\|b_j^*\|^2 \leq 2^{j-1+i-j}\|b_i^*\|^2 = 2^{i-1}\|b_i^*\|^2.$$

2) Iz ortogonalnosti vektora b_i^* slijedi

$$\Delta(L) = |\det(b_1^*, \ldots, b_n^*)| = \prod_{i=1}^{n} \|b_i^*\|.$$

Iz tvrdnje 1) i nejednakosti $\|b_i^*\| \leq \|b_i\|$ dobivamo

$$\Delta(L) \leq \prod_{i=1}^{n} \|b_i\| \leq \prod_{i=1}^{n} 2^{(i-1)/2}\|b_i^*\| \leq 2^{n(n-1)/4} \prod_{i=1}^{n} \|b_i^*\| = 2^{n(n-1)/4}\Delta(L).$$

3) Uvrstimo $j = 1$ u tvrdnju 1) i uzmimo produkt po svim mogućim i-ovima, pa dobivamo

$$\|b_i\|^{2n} \leq \prod_{i=1}^{n} 2^{i-1}\|b_i^*\|^2 \leq 2^{n(n-1)/2}\Delta(L)^2,$$

otkud direktno slijedi tvrdnja 3).

4) Neka je

$$x = \sum_{i=1}^{n} r_i b_i = \sum_{i=1}^{n} r_i' b_i^*, \quad r_i \in \mathbb{Z},\ r_i' \in \mathbb{R}.$$

Neka je i_0 najveći indeks za kojega je $r_{i_0} \neq 0$. Budući da $b_1, \ldots, b_i$ razapinju isti vektorski prostor kao $b_1^*, \ldots, b_i^*$, za sve i, te da je b_{i+1}^* projekcija od b_{i+1} na ortogonalni komplement tog prostora, zaključujemo da je $r_{i_0}' = r_{i_0}$. Stoga imamo

$$\|x\|^2 = \sum_{i=1}^{n} r_i'^2 \|b_i^*\|^2 \geq {r_{i_0}'}^2 \|b_{i_0}^*\|^2 \geq \|b_{i_0}^*\|^2 \geq c_1^{-1}\|b_1\|^2.$$

5) Neka je

$$x = \sum_{i=1}^{n} r_i b_i = \sum_{i=1}^{n} r'_i b^*_i, \quad y = \sum_{i=1}^{n} \sigma_i b_i = \sum_{i=1}^{n} \sigma'_i b^*_i.$$

Ako je i_1 najveći indeks takav da je $r_{i_1} \neq \sigma_{i_1}$, onda je $r_{i_1} - \sigma_{i_1} = r'_{i_1} - \sigma'_{i_1}$, pa imamo

$$\|x - y\|^2 \geq |r_{i_1} - \sigma_{i_1}|^2 \|b^*_i\|^2 \geq |r_{i_1} - \sigma_{i_1}|^2 c_1^{-1} \|b_1\|^2.$$

Ako je $i_1 < i_0$, onda vrijedi $\sigma_{i_0} = r_{i_0} \in \mathbb{Z}$, što je kontradikcija. Ako je $i_1 = i_0$, onda imamo $|r_{i_1} - \sigma_{i_1}| = |r_{i_0} - \sigma_{i_0}| \geq \|\sigma_{i_0}\|$, te dobivamo traženu nejednakost. Konačno, ako je $i_1 > i_0$, onda je $\sigma_{i_1} \in \mathbb{Z}$, pa iz $\sigma_{i_1} \neq r_{i_1}$ i $\|\sigma_{i_0}\| \leq \frac{1}{2}$, dobivamo $|r_{i_1} - \sigma_{i_1}| \geq 1 \geq \|\sigma_{i_0}\|$. □

U svom članku iz 1982. godine, A. K. Lenstra, H. W. Lenstra i L. Lovász prikazali su polinomijalni algoritam za konstrukciju LLL-reducirane baze iz proizvoljne baze rešetke (po njima nazvan *LLL algoritam*). Algoritam je ubrzo našao brojne primjene, npr. u faktorizaciji polinoma s racionalnim koeficijentima, kriptoanalizi RSA kriptosustava s malim javnim ili tajnim eksponentom, problemu ruksaka, te diofantskim aproksimacijama i diofantskim jednadžbama.

Prikazat ćemo de Wegerovu varijantu LLL-algoritma iz 1989. godine, koja koristi samo cjelobrojnu aritmetiku (ukoliko su ulazni podaci cjelobrojni), te izbjegava probleme vezane uz numeričku stabilnost algoritma. Za $i = 1, \ldots, n$, uvedimo oznaku

$$D_i = \det(\langle b_j, b_l \rangle_{1 \leq j,l \leq i}) = \prod_{j=1}^{i} \langle b^*_j, b^*_j \rangle.$$

Tada je $c_i = D_{i-1} b^*_i \in \mathbb{Z}^n$, $\lambda_{ij} = D_j \mu_{ij} \in \mathbb{Z}$.

Algoritam INIT: (nalazi Gram-Schmidtovu bazu)

$D_0 = 1$
for $i = 1$ to n do
    $c_i = b_i$
    for $j = 1$ to $i - 1$ do
        $\lambda_{ij} = \langle b_j, c_j \rangle$
        $c_i = (D_j c_i - \lambda_{ij} c_j)/D_{j-1}$
    $D_i = \langle c_i, c_i \rangle / D_{i-1}$

Algoritam MI-LAMBDA: (postiže da $|\mu_{kl}| \leq \frac{1}{2}$)

if $(2|\lambda_{kl}| > D_l)$ then
    $r = [\lambda_{kl}/D_l]$
    $b_k = b_k - rb_l$
    for $j = 1$ to $l-1$ do
        $\lambda_{kj} = \lambda_{kj} - r\lambda_{lj}$
    $\lambda_{kl} = \lambda_{kl} - rD_l$

Algoritam ZAMIJENI: (zamjenjuje b_k i b_{k-1}, te pripadne podatke)

zamijeni vektore b_{k-1} i b_k
for $j = 1$ to $k-2$ do
    zamijeni $\lambda_{k-1,j}$ i $\lambda_{k,j}$
for $i = k+1$ to n do
    $t = \lambda_{i,k-1}$
    $\lambda_{i,k-1} = (\lambda_{i,k-1}\lambda_{k,k-1} + \lambda_{i,k}D_{k-2})/D_{k-1}$
    $\lambda_{i,k} = (tD_k - \lambda_{i,k}\lambda_{k,k-1})/D_{k-1}$
$D_{k-1} = (D_{k-2}D_k + \lambda_{k,k-1}^2)/D_{k-1}$

LLL-algoritam (de Wegerova varijanta):

primijeni algoritam INIT na matricu B
$k = 2$
while $(k \leq n)$ do
    primijeni algoritam MI-LAMBDA za $l = k-1$
    if $(4D_{k-2}D_k < (3D_{k-1}^2 - 4\lambda_{k,k-1}^2)$ then
        primijeni algoritam ZAMIJENI
        if $k > 2$ then $k = k-1$
    else
        for $l = k-1$ to 1 do
            primijeni algoritam MI-LAMBDA
        $k = k+1$

U programskom paketu PARI je LLL-algoritam implementiran pomoću funkcije `qflll`(x), koja kao rezultat vraća transformacijsku matricu T takvu da je xT LLL-reducirana baza rešetke generirane stupcima matrice x. Naredbe za nalaženje LLL-reducirane baze postoje i u drugim programskim paketima (npr. `lattice` u Maplu ili `LatticeReduce` u Mathematici).

Prije nego što prijeđemo na primjene rešetki na simultane diofantske aproksimacije u više dimenzija, pogledajmo možemo li dobro poznati nam

problem aproksimacije jednog iracionalnog broja racionalnima interpretirati u terminima rešetki. Znamo da se dobre racionalne aproksimacije iracionalnog broja α mogu biti pomoću konvergenti $\frac{p_i}{q_i}$ verižnog razlomka od $\alpha = [a_0, a_1, a_2, \ldots]$. Konvergente zadovoljavaju rekurzije

$$p_{i+1} = a_i p_i + p_{i-1}, \quad q_{i+1} = a_i q_i + q_{i-1}.$$

Uvedemo li oznaku

$$M(i) = \begin{pmatrix} q_i & q_{i+1} \\ p_i & p_{i+1} \end{pmatrix}, \tag{2.9}$$

rekurzije možemo matrično zapisati kao

$$M(i) = M(i-1) \cdot \begin{pmatrix} 0 & 1 \\ 1 & a_i \end{pmatrix}, \tag{2.10}$$

uz $M(-1) = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Matrice $M(i)$ imaju determinantu ± 1, tj. $M(i) \in GL_n(\mathbb{Z})$. Neka je C pozitivan realan broj. Označimo sa $L_C(\alpha)$ rešetku generiranu stupcima matrice $\begin{pmatrix} 1 & 0 \\ -C\alpha & C \end{pmatrix}$. Vrijedi

$$\begin{pmatrix} 1 & 0 \\ -C\alpha & C \end{pmatrix} M(i) = \begin{pmatrix} q_i & q_{i+1} \\ C(p_i - q_i\alpha) & C(p_{i+1} - q_{i+1}\alpha) \end{pmatrix}.$$

Prisjetimo se da je $|p_i - q_i\alpha| < \frac{1}{q_i}$. Ako sada izaberemo $C \approx q_i^2$, onda vidimo da je prvi stupac u zadnjoj matrici vektor $(q_i, C(p_i - q_i\alpha))^\tau$ iz rešetke $L_C(\alpha)$ koji je bitno kraći od vektora polazne baze te rešetke. Nadalje, q_i je prva komponenta tog kratkog vektora.

Propozicija 2.2. *Neka su α i $C > 0$ realni brojevi. Ako je $(u, C(\alpha u - w))^\tau$, $u > 0$, najkraći vektor u rešetki $L_C(\alpha)$, onda je u nazivnik neke konvergente verižnog razlomka od α, te vrijedi $u \leq \frac{2}{\sqrt{3}}\sqrt{C}$.*

Dokaz: Pretpostavimo suprotno, te neka je n najveći indeks sa svojstvom da je $q_n < u$. Tada iz svojstva najboljih aproksimacija (Teorem 1.9) slijedi $|\alpha q_n - p_n| < |u\alpha - w|$. Odavde je

$$q_n^2 + C^2(\alpha q_n - p_n)^2 < u^2 + C^2(\alpha u - w)^2,$$

što je u suprotnosti s minimalnošću od $(u, C(\alpha u - w))^\tau$.

Budući da je $\Delta(L_C(\alpha)) = C$, iz Propozicije 2.1 i $\gamma_2 = \frac{4}{3}$ slijedi da je $u \leq \frac{2}{\sqrt{3}}\sqrt{C}$. □

Zaključujemo da se LLL algoritam može iskoristiti da dobivanje dobrih racionalnih aproksimacija. Za razliku od algoritma verižnog razlomka koji nam daje cijeli niz dobrih aproksimacija, ovdje za fiksni C dobivamo jednu

dobru aproksimaciju, pa za dobivanje više dobrih aproksimacija treba varirati C.

Sada ćemo ovu ideju primijeniti na problem simultanih diofantskih aproksimacija.

Teorem 2.7. *Neka su $\alpha_1, \ldots, \alpha_n$ realni brojevi, te $Q > 1$ prirodan broj. Postoji polinomijalni algoritam koji pronalazi cijele brojeve $q, p_1, \ldots, p_n$ takve da je*

$$1 \le q \le 2^{n/4} Q^n, \quad i \quad |\alpha_i q - p_i| \le \frac{\sqrt{5} \cdot 2^{(n-4)/4}}{Q}, \ i = 1, \ldots, n. \tag{2.11}$$

Dokaz: Za realan broj x, sa $\lfloor x \rceil$ ćemo označavati najbliži cijeli broj broju x. Neka je $C = Q^{n+1}$. Promotrimo matricu

$$B = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ -\lfloor C\alpha_1 \rceil & C & 0 & \cdots & 0 \\ -\lfloor C\alpha_2 \rceil & 0 & C & \cdots & 0 \\ \vdots & 0 & 0 & \ddots & \vdots \\ -\lfloor C\alpha_n \rceil & 0 & 0 & \cdots & C \end{pmatrix},$$

te rešetku L generiranu njezinim stupcima. Dimenzija rešetke je $n+1$, a volumen C^n. Prema Lemi 2.1.3), LLL algoritam nalazi vektor $r = (q, p_1, \ldots, p_n)^\tau$ iz $\mathbb{Z}^{n+1}$, takav da je $v = Br$ vektor iz L čija je norma

$$\le \Lambda := 2^{n/4} \cdot C^{n/(n+1)} = 2^{n/4} Q^n.$$

Komponente vektora v su $v_1 = q$, $v_{i+1} = Cp_i - q\lfloor C\alpha_i \rceil$, $i = 1, \ldots, n$. Vrijedi

$$q^2 + \sum_{i=1}^{n} (Cp_i - q\lfloor C\alpha_i \rceil)^2 \le \Lambda^2.$$

Dakle, $q \le \Lambda$ i $\max_{1 \le i \le n} |Cp_i - q\lfloor C\alpha_i \rceil| \le \Lambda$. Budući da je $|Cp_i - q\lfloor C\alpha_i \rceil| \ge C|p_i - q\alpha_i| - q/2$, dobivamo

$$|p_i - q\alpha_i| \le C^{-1}(|Cp_i - q\lfloor C\alpha_i \rceil| + q/2).$$

Konačno, iskoristimo još ovu jednostavnu činjenicu: za realne brojeve x, y vrijedi

$$2x + y \le \sqrt{5(x^2 + y^2)}. \tag{2.12}$$

Zaista, kvadriranjem dobivamo $(x - 2y)^2 \ge 0$, što je očito točno. Primijenimo li (2.12) na $x = |Cp_i - q\lfloor C\alpha_i \rceil|$, $y = q$, dobivamo

$$|p_i - q\alpha_i| \le C^{-1} \cdot \sqrt{5(|Cp_i - q\lfloor C\alpha_i \rceil|^2 + q^2)}/2 \le \frac{\sqrt{5}}{2C}\Lambda = \frac{\sqrt{5}}{2} 2^{n/4} Q^{-1}.$$

□

Primjer 2.1. Neka je $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt{3}$, $\alpha_3 = \sqrt{5}$. Uzmimo $Q = 1000$, te primijenimo algoritam iz Teorema 2.7. Formiramo matricu B kao u dokazu teorema, te pomoću PARI-ja izračunamo `qflll`(B). Iz prvog stupca ove matrice pročitamo brojeve $q = 118452669$, $p_1 = 167517371$, $p_2 = 205166041$, $p_3 = 264868220$. Provjerom dobivamo da je $q < 1.2 \cdot Q^3$, $|q\sqrt{2} - p_1| < 0.91 \cdot Q^{-1}$, $|q\sqrt{3} - p_2| < 0.14 \cdot Q^{-1}$, $|q\sqrt{5} - p_3| < 0.29 \cdot Q^{-1}$,

$$\max\left(\left|\sqrt{2} - \frac{p_1}{q}\right|, \left|\sqrt{3} - \frac{p_2}{q}\right|, \left|\sqrt{5} - \frac{p_3}{q}\right|\right) < q^{-4/3}.$$

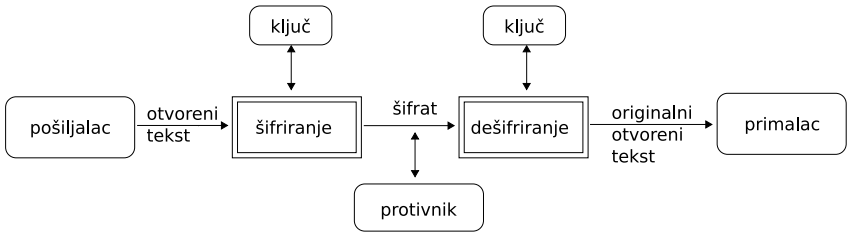
Dakle, dobivene simultane racionalne aproksimacije su čak i bolje nego što Teorem 2.7 garantira, te zadovoljavaju nejednakost (2.2) iz korolara Dirichletovog teorema o simultanim aproksimacijama bez ikakvih dodatnih faktora.

Poglavlje 3

Primjena diofantskih aproksimacija u kriptografiji

3.1 Vrlo kratki uvod u kriptografiju

Kako uspostaviti sigurnu komunikaciju preko nesigurnog komunikacijskog kanala? Metode za rješavanje ovog problema proučava znanstvena disciplina koja se zove kriptografija. Osnovni zadatak kriptografije je omogućavanje komunikacije dvaju osoba (zovemo ih *pošiljalac* i *primalac* - u kriptografskoj literaturi za njih su rezervirana imena *Alice* i *Bob*) na takav način da treća osoba (njihov *protivnik* - u literaturi se najčešće zove *Eva* ili *Oskar*), koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke. Poruku koju pošiljalac želi poslati primaocu zovemo *otvoreni tekst*. Pošiljalac transformira otvoreni tekst koristeći unaprijed dogovoreni *ključ* K. Taj se postupak zove *šifriranje*, a dobiveni rezultat *šifrat*. Nakon toga pošiljalac pošalje šifrat preko nekog komunikacijskog kanala. Protivnik prisluškujući može saznati sadržaj šifrata, ali kako ne zna ključ, ne može odrediti otvoreni tekst. Za razliku od njega, primalac zna ključ kojim je šifrirana poruka, pa može *dešifrirati* šifrat i odrediti otvoreni tekst.



shema simetrične kriptografije

Definicija 3.1. Kriptosustav *je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, *gdje je* $\mathcal{P}$ *konačan skup svih otvorenih tekstova,* $\mathcal{C}$ *konačan skup svih šifrata,* $\mathcal{K}$ *konačan skup svih mogućih ključeva,* $\mathcal{E}$ *skup svih funkcija šifriranja i* $\mathcal{D}$ *skup*

svih funkcija dešifriranja. Za svaki $K \in \mathcal{K}$ *postoji* $e_k \in \mathcal{E}$ *i odgovarajući* $d_K \in \mathcal{D}$. *Pritom su* $e_K : \mathcal{P} \to \mathcal{C}$ *i* $d_K : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki* $x \in \mathcal{P}$.

Shema koju smo gore opisali predstavlja tzv. *simetrični kriptosustav*. Funkcije koje se koriste za šifriranje e_K i dešifriranje d_K ovise o ključu K kojeg Alice i Bob moraju tajno razmjeniti prije same komunikacije. Kako njima nije dostupan siguran komunikacijski kanal, ovo može biti veliki problem.

Diffie i Hellman su 1976. godine predložuli protokol za razmjenu ključeva, zasnovan na činjenici da je u nekim grupama potenciranje puno jednostavnije od logaritmiranja (*problem diskretnog logaritma*). Diffie i Hellman se smatraju začetnicima *kriptografije javnog ključa*. Ideja javnog ključa se sastoji u tome da se konstruiraju kriptosustavi kod kojih bi iz poznavanja funkcije šifriranja e_K bilo praktički nemoguće (u nekom razumnom vremenu) izračunati funkciju dešifriranja d_K. Tada bi funkcija e_K mogla biti javna.

Dakle, u kriptosustavu s javnim ključem svaki korisnik K ima dva ključa: javni e_K i tajni d_K. Ako Alice želji poslati Bobu poruku x, onda je ona šifrira pomoću Bobovog javnog ključa e_B, tj. pošalje Bobu šifrat $y = e_B(x)$. Bob dešifrira šifrat koristeći svoj tajni ključ d_B, $d_B(y) = d_B(e_B(x)) = x$.

Uočimo da Bob mora posjedovati neku dodatnu informaciju (tzv. *trap-door* - skriveni ulaz) o funkciji e_B, da bi samo on mogao izračunati njezin inverz d_B, dok je svima drugima (a posebno Evi) to nemoguće. Takve funkcije čiji je inverz teško izračunati bez poznavanja nekog dodatnog podatka zovu se *osobne jednosmjerne funkcije*.

3.2 RSA kriptosustav

Najpoznatiji kriptosustav s javnim ključem je RSA kriptosustav iz 1977. godine, nazvan po svojim tvorcima Ronaldu Rivestu, Adi Shamiru i Leonardu Adlemanu.

Njegova sigurnost je zasnovana na prvenstveno na teškoći faktorizacije velikih prirodnih brojeva. Parametri RSA kriptosustava su modul n koji je produkt dva velika prosta broja p i q, te eksponenti e i d koji se koriste za šifriranje i dešifriranje.

Definicija RSA kriptosustava:
Neka je $n = pq$, gdje su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$, te

$$\mathcal{K} = \{(n, p, q, d, e) : n = pq,\ de \equiv 1 \pmod{\varphi(n)}\}.$$

Za $K \in \mathcal{K}$ definiramo

$$e_K(x) = x^e \bmod n, \qquad d_K(y) = y^d \bmod n.$$

Vrijednosti n i e su javne, a vrijednosti p, q i d su tajne, tj. (n, e) je javni, a (p, q, d) je tajni (privatni) ključ.

Ovdje je $\varphi(n) = (p-1)(q-1) = n - p - q + 1$ Eulerova funkcija. Iz njezinog svojstva da je $a^{\varphi(n)} \equiv 1 \pmod{n}$ za $\text{nzd}(a, n) = 1$, slijedi da su funkcije e_K i d_K jedna drugoj inverzne. U standardnoj verziji RSA, još dodatno pretpostavljamo da p i q imaju približno jednaki broj bitova (to se naziva i balansirani RSA), te da je $e < n$.

Sigurnost RSA kriptosustava leži u pretpostavci da je funkcija $e_K(x) = x^e \bmod n$ jednosmjerna. Dodatni podatak ("trapdoor") koji omogućava dešifriranje je poznavanje faktorizacije $n = pq$. Zaista, onaj tko zna faktorizaciju broja n, taj može izračunati $\varphi(n) = (p-1)(q-1)$, te potom dobiti eksponent d rješavajući linearnu kongruenciju $de \equiv 1 \pmod{\varphi(n)}$ (pomoću proširenog Euklidova algoritma). No, otvoreno je pitanje je li razbijanje RSA kriptosustava, tj. određivanje x iz poznavanja $x^e \bmod n$, ekvivalentno faktorizaciji od n. Metodama faktorizacije se nećemo baviti u ovom kolegiju, pa recimo samo da trenutno najbrži algoritmi za faktorizaciju trebaju

$$e^{O((\log n)^{1/3}(\log\log n)^{2/3})}$$

operacija, tako da su brojevi od preko 250 znamenaka zasad sigurni od ovog napada.

Recimo sada nešto malo preciznije o izboru parametara za RSA:

1. Tajno izaberemo dva velika prosta broja p i q slične veličine (recimo oko 512 bitova). Najprije generiramo slučajan prirodan broj m sa željenim brojem bitova, pa zatim pomoću nekog testa prostosti (npr. Miller-Rabinovog) tražimo prvi prost broj veći ili jednak m.

   Treba paziti da $n = pq$ bude otporan na metode faktorizacije koje su vrlo efikasne za brojeve specijalnog oblika. Tako bi brojevi $p \pm 1$ i $q \pm 1$ trebali imati barem jedan veliki prosti faktor, jer postoje efikasne metode za faktorizaciju brojeva koji imaju prosti faktor p takav da je jedan od brojeva $p-1$, $p+1$ "gladak", tj. ima samo male proste faktore. Također, p i q ne smiju biti jako blizu jedan drugome, jer ih se onda može naći koristeći činjenicu da su približno jednaki $\sqrt{n}$.

2. Izračunamo $n = pq$ i $\varphi(n) = (p-1)(q-1) = n - p - q + 1$.

3. Izaberemo broj e takav da je $\text{nzd}(e, \varphi(n)) = 1$, te pomoću proširenog Euklidova algoritma izračunamo d takav da je $de \equiv 1 \pmod{\varphi(n)}$. Obično se uzima da je $e < \varphi(n)$. Broj e se može izabrati slučajno, a ima smisla izabrati ga i što manjim, tako da bi šifriranje $x^e \bmod n$ (tzv. modularno potenciranje) bilo što brže. Broj operacija u šifriranju ovisi o veličini broja e, te o broju jedinica u binarnom zapisu od e. Stoga je dugo vremena $e = 3$ bio popularan izbor. No, vidjet ćemo da izbor

vrlo malog eksponenta e predstavlja opasnost za sigurnost, te se danas preporuča izbor $e = 2^{16} + 1 = 65537$.

4. Stavimo ključ za šifriranje (n, e) u javni direktorij.

Za efikasnost RSA kriptosustava, važna je činjenica da se modularno potenciranje može izvesti vrlo efikasno. Navedimo ovdje osnovnu metodu za računanje $e_K(x) = x^e \bmod n$, metodu "kvadriraj i množi" (ili "binarne ljestve"). Najprije e prikažemo u bazi 2:

$$e = 2^{s-1} \cdot e_{s-1} + \cdots + 2 \cdot e_1 + e_0,$$

a potom primijenimo sljedeći algoritam:

Kvadriraj i množi:

$y = 1$
for $(s - 1 \geq i \geq 0)$ {
  $y = y^2 \bmod n$
  if $(e_i = 1)$ then $y = y \cdot x \bmod n$ }

Očito je ukupan broj množenja $\leq 2s$, pa je ukupan broj operacija $O(\log e \cdot \log^2 n)$. To znači da je ovaj algoritam polinomijalan.

3.3 Wienerov napad na RSA kriptosustav

Budući da je broj operacija za modularno potenciranje linearan u broju bitova eksponenta, na prvi pogled čini se kao dobra ideja pokušati izabrati parametre RSA kripotsustava tako da jedan od eksponenata e ili d bude mali. To bi moglo smanjiti vrijeme potrebno za šifriranje, odnosno dešifriranje, što bi posebno moglo biti od interesa u situacijama kad postoji veliki nesrazmjer u snazi dvaju uređaja koji sudjeluju u komunikaciji, kao što je npr. slučaj kad "pametna kartica" komunicira s centralnim računalom. U toj situaciji bismo možda poželjeli kartici dodijeliti mali tajni eksponent, a računalu mali javni eksponent, da bismo minimizirali onaj dio računanja koje treba provesti kartica. Međutim, vidjet ćemo da takav izbor eksponenata ipak nije dobar. Sljedeći teorem M. Wienera iz 1990. godine pokazuje da u slučaju izbora relativno malog tajnog eksponenta d (u odnosu na n) postoji efikasan algoritam za razbijanje RSA šifre.

Teorem 3.1. *Neka je $n = pq$ i $p < q < 2p$, te neka je $e < \varphi(n)$ i $d < \frac{1}{3}n^{0.25}$. Tada postoji polinomijalni algoritam koji iz poznavanja n i e izračunava d.*

Dokaz: Iz $ed \equiv 1 \pmod{\varphi(n)}$ slijedi da postoji prirodan broj k takav da je $ed - k\varphi(n) = 1$. Odavde je

$$\left| \frac{e}{\varphi(n)} - \frac{k}{d} \right| = \frac{1}{d\varphi(n)}. \tag{3.1}$$

Dakle, $\frac{k}{d}$ je dobra aproksimacija od $\frac{e}{\varphi(n)}$. Međutim, mi ne znamo $\varphi(n)$. Stoga ćemo $\varphi(n)$ aproksimirati s n. Iz $\varphi(n) = n - p - q + 1$ i $p + q - 1 < 3\sqrt{n}$ slijedi $|n - \varphi(n)| < 3\sqrt{n}$. Zamijenimo $\varphi(n)$ s n u (3.1), pa dobivamo:

$$\left|\frac{e}{n} - \frac{k}{d}\right| = \left|\frac{ed - k\varphi(n) - kn + k\varphi(n)}{nd}\right| = \left|\frac{1 - k(n - \varphi(n))}{nd}\right| \leq \frac{3k\sqrt{n}}{nd} = \frac{3k}{d\sqrt{n}}.$$

Sada je $k\varphi(n) = ed - 1 < ed$, pa iz $e < \varphi(n)$ (to je standardna pretpostavka u RSA kriptosustavu), slijedi $k < d < \frac{1}{3}n^{0.25}$, te dobivamo

$$\left|\frac{e}{n} - \frac{k}{d}\right| \leq \frac{1}{d\sqrt[4]{n}} < \frac{1}{2d^2}. \tag{3.2}$$

Iz Legenderovog teorema (Teorem 1.7) slijedi da relacija (3.2) povlači da je k/d neka konvergenta razvoja u verižni razlomak od e/n. Iz rekurzije za nazivnike konvergenti $\frac{p_k}{q_k}$ verižnog razlomka, slijedi da je $q_k \geq F_k$, gdje je F_k k-ti Fibonaccijev broj, što znači da nazivnici konvergenti rastu eksponencijano. U našem slučaju dakle slijedi da ima $O(\log n)$ konvergenti od $\frac{e}{n}$. Jedna od njih je $\frac{k}{d}$. Dakle, izračunamo sve konvergente od $\frac{e}{n}$ i testiramo koja od njih zadovoljava uvjet $(x^e)^d \equiv x \pmod{n}$ za slučajno odabran broj x. To daje polinomijalni algoritam za otkrivanje tajnog ključa d.

Drugi način za testiranje točnosti pretpostavke da je neka konkretna konvergenta jednaka $\frac{k}{d}$, jest da se, uz tu pretpostavku, izračuna $\varphi(n) = (p-1)(q-1) = (ed-1)/k$. Tada se može izračunati $\frac{p+q}{2}$ iz identiteta

$$\frac{pq - (p-1)(q-1) + 1}{2} = \frac{p+q}{2},$$

te $\frac{q-p}{2}$ iz identiteta $(\frac{p+q}{2})^2 - pq = (\frac{q-p}{2})^2$. Ako se na ovaj način dobije da su brojevi $\frac{p+q}{2}$ i $\frac{q-p}{2}$ cijeli, onda zaključujemo da je promatrana konvergenta stvarno jednaka $\frac{k}{d}$. Tada iz $\frac{p+q}{2}$ i $\frac{q-p}{2}$ možemo lako dobiti i faktorizaciju modula $n = pq$. □

Primjer 3.1. Pretpostavimo da su u RSA kriptosustavu zadani modul

$$n = 7978886869909,$$

javni eksponent

$$e = 3594320245477,$$

te da je poznato da tajni eksponent d zadovoljava $d < \frac{1}{3}n^{0.25} < 561$. Da bismo primijenili Wienerov napad, računamo razvoj broja $\frac{e}{n}$ u verižni razlomak. Dobivamo:

$$[0, 2, 4, 1, 1, 4, 1, 2, 31, 21, 1, 3, 1, 16, 3, 1, 114, 10, 1, 4, 5, 1, 2].$$

Potom računamo pripadne konvergente:

$$0, \frac{1}{2}, \frac{4}{9}, \frac{5}{11}, \frac{9}{20}, \frac{41}{91}, \frac{50}{111}, \frac{141}{313}, \frac{4421}{9814}, \ldots .$$

Konačno, provjeravamo koji od nazivnika 2, 9, 11, 20, 91, 111, 313 zadovoljava kongruenciju $(x^e)^d \equiv x \pmod{n}$ za npr. $x = 2$. Tako dobivamo da je tajni eksponent $d = 313$. ♢

U ovom primjeru smo vidjeli da je prava konvergenta bila upravo zadnja koja je zadovoljavala uvjet za veličinu nazivnika. To nam sugerira da možda uopće nije nužno testirati sve konvergente u zadanom rasponu, već da bi moglo biti moguće karakterizirati pravu konvergentu. Zaista, to se može napraviti preciznijom ocjenom za $\varphi(n)$. Uz razumnu pretpostavku da je $n > 10^8$, dobije se da je $\frac{k}{d}$ jedinstvena konvergenta koja zadovoljava nejednakost

$$\frac{2e}{n\sqrt{n}} < \frac{k}{d} - \frac{e}{n} < \frac{2.122\, e}{n\sqrt{n}}.$$

Verheul i van Tilborg (1997), te Dujella (2004) prikazali su dvije varijante Wienerova napada na RSA u kojem je tajni ključ veći od $\sqrt[4]{n}$. Neka je $d = D\sqrt[4]{n}$. Ako D nije jako velik, onda možemo pokušati $\frac{k}{d}$ prikazati u obliku $\frac{rp_{m+1} \pm sp_m}{rq_{m+1} \pm sq_m}$, gdje su r, s nenegativni cijeli brojevi i $\frac{p_m}{q_m}$ konvergenta verižnog razlomka od $\frac{e}{n}$. Koristeći poopćenje Legendreova teorema (Worleyev teorem 1.8), Dujella je dao ocjene za broj parova (r, s) koje treba ispitati u najlošijem slučaju. Te su ocjene ugrubo $O(D^2)$, dakle eksponencijalne u D. Preciznije, broj mogućih parova (r, s) u Verheul - van Tilborgovom napadu je $O(D^2A^2)$, gdje je $A = \max\{a_i : i = m+1, m+2, m+3\}$, dok je u Dujellinoj varijanti $O(D^2 \log A)$ (a_i su parcijalni kvocijenti u razvoju u verižni razlomak).

Ilustirat ćemo tu varijantu Wienerovog napada na sljedećem primjeru.

Primjer 3.2. Neka je $n = 7978886869909$, $e = 4603830998027$, i pretpostavimo da je $d < 10000000$. Razvoj u verižni razlomak broja $\frac{e}{n}$ je

$$[0, 1, 1, 2, 1, 2, 1, 18, 10, 1, 3, 3, 1, 6, 57, 2, 1, 2, 14, 7, 1, 2, 1, 4, 6, 2],$$

a prvih nekoliko konvergenti je

$$0,\ 1,\ \frac{1}{2},\ \frac{3}{5},\ \frac{4}{7},\ \frac{11}{19},\ \frac{15}{26},\ \frac{281}{487},\ \frac{2825}{4896},\ \ldots .$$

Tražimo dvije susjedne neparne konvergente između kojih se nalazi $\frac{e}{n} + \frac{2.122e}{n\sqrt{n}}$. Dobivamo:

$$\frac{281}{487} < \frac{e}{n} + \frac{2.122e}{n\sqrt{n}} < \frac{11}{19}.$$

Sada tajni eksponent d tražimo među brojevima nekog od oblika $26r + 19s$ ili $487s - 26t$ ili $4896r' + 487s'$. Primjenjujući kriterij za testiranje kandidata za razlomak $\frac{k}{d}$ opisan u dokazu Teorema 3.1, nalazimo da je $d = 5936963$, što se dobiva za $s = 12195$, $t = 77$. ♢

Vremenska složenost ovog napad može poboljšati primjenom metode "susret u sredini" (*meet-in-the-middle*) za testiranje kandidata (Dujella, 2009). Želimo testirati je li

$$2^{e(rq_{m+1}+sq_m)} \equiv 2 \pmod{n}.$$

Primijetimo da je indeks m skoro fiksiran. Naime, ako je m' najveći neparan prirodan broj takav da je

$$\frac{p_{m'}}{q_{m'}} > \frac{e}{n} + \frac{2.122e}{n\sqrt{n}},$$

onda je $m \in \{m', m'+1, m'+2\}$.

Uvedimo oznake:

$$2^{eq_{m+1}} \bmod n = a, \quad (2^{eq_m})^{-1} \bmod n = b.$$

Tada zapravo možemo testirati kongruenciju

$$a^r \equiv 2b^s \pmod{n}.$$

To možemo napraviti tako da izračunamo $a^r \bmod n$ za sve r, sortiramo rezultate, a potom računamo $2b^s \bmod n$ redom za svaki s i provjeravamo pojavljuje li se rezultat u prethodno dobivenoj sortiranoj listi. Na ovaj način broj koraka u testiranju postaje ugrubo (broj mogućnosti za r) + (broj mogućnosti za s). Preciznije, vremenska složenost faze testiranja smanjuje sa $O(D^2)$ na $O(D \log D)$ (uz prostornu (memorijsku) složenost $O(D)$). Ovaj napad radi efikasno za vrijednosti od D do 2^{30}, tj. za $d < 2^{30} n^{0.25}$.

3.4 Napadi na RSA koji koriste LLL algoritam

Postoje i napadi koji, umjesto verižnih razlomaka, koriste Coppersmithovu metodu za nalaženje rješenja polinomijalnih kongruencija. Naime, radi se o sljedećem problemu. Neka je zadan polinom $f(x) \in \mathbb{Z}[x]$ stupnja d i neka je poznato da postoji "malo" rješenje kongruencije $f(x) \equiv 0 \pmod{N}$, tj. rješenje x_0 za koje vrijedi $|x_0| < N^{1/d}$. Pitanje je možemo li efikasno naći x_0. Coppersmith je pokazao da je odgovor na ovo pitanje potvrdan. Osnovna ideja je konstruirati novi polinom $h(x) = h_0 + h_1 x + \cdots h_n x^n \in \mathbb{Z}[x]$ za kojeg će također vrijediti $h(x_0) \equiv 0 \pmod{N}$, ali koji će imati male koeficijente. Preciznije, traži se da "norma" $\|h(x)\| := \left(\sum_{i=0}^{n} h_i^2\right)^{1/2}$ bude mala. Tada se može iskoristiti sljedeća jednostavna činjenica: ako za prirodan broj X vrijedi

$$\|h(xX)\| < \frac{N}{\sqrt{n+1}}$$

i $|x_0| < X$ zadovoljava kongruenciju $h(x_0) \equiv 0 \pmod{N}$, onda je x_0 nultočka polinoma h, tj. vrijedi ne samo kongruencija, već i jednakost $h(x_0) = 0$.

Polinom $h(x)$ s traženim svojstvom može se naći pomoću LLL algoritma. Naime, koeficijenti polinoma $h(x)$ mogu se dobiti kao komponente prvog vektora LLL-reducirane baze određene rešetke koja se dobije pomoću koeficijenata polaznog polinoma $f(x)$.

Boneh i Durfee su opisali jedan napad na RSA ovakvog tipa koji je primjenjiv u slučaju da je $d < n^{0.292}$. Slično kao kod Weinerova napada, kreće se od jednakosti $ed - k\varphi(n) = 1$, koja se može zapisati i kao

$$ed - k(n + 1 - p - q) = 1.$$

Stavimo $s = p + q$, $a = n + 1$. Sada je nalaženje malog tajnog eksponenta d, recimo $d < n^{\delta}$, ekvivalentno nalaženju malih rješenja k i s kongruencije

$$f(k, s) = k(s - a) \equiv 1 \pmod{e}.$$

Zaista, za k i e imamo sljedeće ocjene:

$$|s| < 3\sqrt{n} \approx e^{0.5}, \quad |k| < \frac{de}{\varphi(n)} \approx e^{\delta}.$$

Dakle, situacija je slična kao kod gore navedenog Coppersmithova rezultata, samo što se ovdje radi o polinomu od dvije varijable, pa se Coppersmithov teorem ne može direktno primijeniti da bi se strogo dokazala korektnost ovog napada. Ipak, pokazalo se da on u praksi radi sasvim zadovoljavajuće.

Savjet je da se izbjegava slučaj kada je $d < \sqrt{n}$, jer je poznato da su svi ovi gore spomenuti napadi sasvim neprimjenjivi ako je $d > \sqrt{n}$.

Također postoje i napadi na RSA uz pretpostavku da je eksponent e mali, pa bi i to trebalo izbjegavati. U ranijim implementacijama RSA kriptosustava, često se uzimalo $e = 3$, da bi se minimiziralo vrijeme potrebno za šifriranje. Pokazat ćemo zašto taj izbor za e nije dobar.

Pretpostavimo da imamo tri korisnika s različitim vrijednostima javnog modula n_1, n_2, n_3, te pretpostavimo da svi oni koriste isti javni eksponent $e = 3$. Nadalje, pretpostavimo da im netko želi poslati identičnu poruku m. Tada njihov protivnik može doznati sljedeće šifrate:

$$c_1 \equiv m^3 \pmod{n_1}, \quad c_2 \equiv m^3 \pmod{n_2}, \quad c_3 \equiv m^3 \pmod{n_3}.$$

Nakon toga, on može, koristeći Kineski teorem o ostatcima naći rješenje sustava linearnih kongruencija

$$x \equiv c_1 \pmod{n_1}, \quad x \equiv c_2 \pmod{n_2}, \quad x \equiv c_3 \pmod{n_3}.$$

Na taj način, dobit će broj x sa svojstvom $x \equiv m^3 \pmod{n_1 n_2 n_3}$. No, kako je $m^3 < n_1 n_2 n_3$, zapravo vrijedi jednakost $x = m^3$, pa protivnik može izračunati originalnu poruku m tako na nađe treći korijen iz x.

Upravo opisani napad može se izbjeći tako da se porukama prije šifriranja doda neki "slučajni dodatak" (engl. random pad). Na taj način, nikad nećemo različitim primateljima slati potpuno identične poruke. No, postoje napadi (zasnovani na gore spomenutu Coppersmithovu rezultatu i LLL algoritmu) koji pokazuju da ni u tom slučaju RSA kriptosustav s vrlo malim eksponentom e nije siguran. Prikazat ćemo sada Hastadov napad (1985).

Pretpostavimo da je, prije šifriranja, na početku svake poruke dodan neki podatak ovisan o korisniku. Npr.

$$c_i = (i \cdot 2^h + m)^e \bmod n_i, \;\; i = 1, \ldots, k.$$

Dakle, imamo k polinoma $g_i(x) = (i \cdot 2^h + x)^e - c_i$, te tražimo m sa svojstvom da je

$$g_i(m) \equiv 0 \pmod{n_i}.$$

Neka je $n = n_1 n_2 \cdots n_k$. Pomoću Kineskog teorema o ostacima možemo naći t_i tako da je

$$g(x) = \sum_{i=1}^{k} t_i g_i(x) \;\text{ i }\; g(m) \equiv 0 \pmod{n}$$

($t_i \equiv 1 \pmod{n_i}$, $t_i \equiv 0 \pmod{n_j}$ za $j \neq i$). Polinom g je normiran i stupnja e. Ako je $k > e$, tj. imamo više korisnika (presretnutih šifrata) nego što je javni eksponent, onda je $m < \min_i n_i < n^{1/k} < n^{1/e}$, pa se m može efikasno naći primjenom gore navedenog Coppersmithovog rezultata.

Može se preporučiti uporaba eksponenta $e = 65537$, koji je dovoljno velik da bi onemogućio sve poznate napade na RSA s malim eksponentom, a prednost mu je vrlo brzo šifriranje jer ima malo jedinica u binarnom zapisu. Naime, $65537 = 2^{16} + 1$.

3.5 Coppersmithov teorem

Recimo sada nešto malo više o Coppersmithovom rezultatu korištenom u napadima opisanim u prethodnom potpoglavlju.

Neka je N veliki složen broj s nepoznatom faktorizacijom. Nadalje, neka je f (normirani) polinom

$$f(x) = f_0 + f_1 x + \cdots + f_{d-1} x^{d-1} + x^d$$

s cjelobrojnim koeficijentima stupnja d, za kojeg je poznato da postoji "malo" rješenje kongruencije $f(x) \equiv 0 \pmod{N}$, tj. rješenje x_0 za koje vrijedi $|x_0| < N^{1/d}$. Ovdje pretpostavka da je polinom f normiran nije gubitak općenitosti, jer ga inače možemo pomnoziti s inverzom modulo N od vodećeg koeficijenta (a ukoliko inverz ne postoji, onda smo našli netrivijalni faktor od N).

Želimo (efikasno) naći x_0. Kao što smo već spomenuli, osnovna ideja je konstruirati novi polinom $h(x) = h_0 + h_1 x + \cdots h_n x^n \in \mathbb{Z}[x]$ za kojeg će također vrijediti $h(x_0) \equiv 0 \pmod{N}$, ali koji će imati male koeficijente. Tada se kongruencija modulo N može zamijeniti običnom jednakošću, te problem riješiti nalaženje cjelobrojnih nultočaka polinoma h.

Lema 3.1. *Neka je $h(x) = h_0 + h_1 x + \cdots h_n x^n \in \mathbb{Z}$ polinom stupnja n, te neka su X i N prirodni brojevi. Pretpostavimo da vrijedi*

$$\|h(xX)\| < \frac{N}{\sqrt{n+1}}.$$

Tada ako $|x_0| < X$ zadovoljava kongruenciju $h(x_0) \equiv 0 \pmod{N}$, onda je $h(x_0) = 0$.

Dokaz: Iz nejednakosti trokuta, te nejednakosti aritmetičke i kvadratne sredine, imamo:

$$\begin{aligned} |h(x_0)| &\leq |h_0| + |h_1|X + \cdots + |h_n|X^n \\ &\leq \sqrt{n+1} \cdot \sqrt{h_0^2 + h_1^2 X^2 + \cdots + h_n^2 X^{2n}} \\ &= \sqrt{n+1} \cdot \|h(xX)\| < \sqrt{n+1} \cdot \frac{N}{\sqrt{n+1}} = N. \end{aligned}$$

Sada iz $h(x_0) \equiv 0 \pmod{N}$ i $|h(x_0)| < N$ slijedi da je $h(x_0) = 0$. □

Vratimo se sada na polazni polinom f i kongruenciju $f(x_0) \equiv 0 \pmod{N}$. Iz ove konkruencije slijedi da je i $f(x_0)^k \equiv 0 \pmod{N^k}$ za svaki $k \geq 1$. Nadalje, ako za dani prirodni broj m definiramo polinome

$$g_{u,v}(x) = N^{m-v} x^u f(x)^v,$$

onda za sve $0 \leq u < d$ i $0 \leq v \leq m$ vrijedi

$$g_{u,v}(x_0) \equiv 0 \pmod{N^m}.$$

Sada ćemo traženi polinom h tražiti u obliku

$$h(x) = \sum_{u=0}^{d-1} \sum_{v=0}^{m} a_{u,v} g_{u,v}(x),$$

gdje su $a_{u,v} \in \mathbb{Z}$.

Dakle, želimo naći cijele brojeve $a_{u,v}$ tako da dobiveni polinom h zadovoljava nejednakost

$$\|h(xX)\| \leq \frac{N^m}{\sqrt{d(m+1)}}.$$

Ovaj je problem može shvatiti kao problem nalaženja malog vektora u odgovarajućoj rešetki, i stoga ga se može riješiti pomoću LLL algoritma. Ilustrirat ćemo to na primjeru polinoma malog stupnja ($d = 2$).

Zadan je polinom

$$f(x) = x^2 + ax + b$$

i želimo naći (mali) x_0 takav da je $f(x_0) \equiv 0 \pmod{N}$. Uzmimo $m = 2$, te konstruirajmo polinome $g_{u,v}$ na gore opisani način:

$$\begin{aligned}
g_{0,0}(xX) &= N^2, \\
g_{1,0}(xX) &= XN^2x, \\
g_{0,1}(xX) &= bN + aXNx + NX^2x^2, \\
g_{1,1}(xX) &= bNXx + aNX^2x^2 + NX^3x^3, \\
g_{0,2}(xX) &= b^2 + 2abXx + (a^2 + 2b)X^2x^2 + 2aX^3x^3 + X^4x^4, \\
g_{1,2}(xX) &= b^2Xx + 2abX^2x^2 + (a^2 + 2b)X^3x^3 + 2aX^4x^4 + X^5x^5.
\end{aligned}$$

Cilj nam je naći linearnu kombinaciju ovih šest polinoma tako da dobiveni polinom ima male koeficijente. Drugim riječima, tražimo kratki vektor u rešetki generiranoj stupcima sljedeće matrice, u kojoj redci odgovaraju potencijama od x, a stupci polinomima $g_{u,v}$:

$$A = \begin{pmatrix}
N^2 & 0 & bN & 0 & b^2 & 0 \\
0 & XN^2 & abX & bNX & 2abX & Xb^2 \\
0 & 0 & NX^2 & aNX^2 & (a^2+2b)X^2 & 2abX^2 \\
0 & 0 & 0 & NX^3 & 2aX^3 & (a^2+2b)X^3 \\
0 & 0 & 0 & 0 & X^4 & 2aX^4 \\
0 & 0 & 0 & 0 & 0 & X^5
\end{pmatrix}.$$

Determinanta ove matrice je $\det(A) = N^6X^{15}$. Primjenom LLL algoritma na rešetku generiranu stupcima matrice A, dobivamo LLL bazu za tu rešetku. Po Lemi 2.1.3), prvi vektor b_1 te zadovoljava

$$\|b_1\| \leq 2^{5/4} \det(A)^{1/6} = 2^{5/4} NX^{5/2}.$$

Prema tome, polinom

$$h(x) = b_1^{(1)} g_{0,0}(x) + b_1^{(2)} g_{1,0}(x) + \cdots + b_1^{(6)} g_{1,2}(x)$$

zadovoljava

$$\|h(xX)\| \leq 2^{5/4} NX^{5/2}.$$

Sada možemo primijeniti Lemu 3.1 ako je zadovoljen uvjet

$$2^{5/4} NX^{5/2} < N^2/\sqrt{6},$$

tj.

$$X < \frac{N^{0.4}}{6^{0.2} \cdot 2^{0.5}}.$$

Za dovoljno veliki N, to znači da ćemo moći naći rješenje x_0 kongruencije $f(x_0) \equiv 0 \pmod{N}$ ako je

$$|x_0| \leq N^{0.39}.$$

Analogna tehnika se može primijeniti i na polinome proizvoljnog stupnja d. Postoje različiti izbori pripadnih rešetki (obično rešetke veće dimenzije daju bolje ekponente). Ovdje navodimo originalni Coppersmithov teorem koji za dobivanje eksponenta $1/d - \epsilon$ koristi rešetku dimenzije $d(2m-1)$, gdje je $m \geq \max(\frac{d-1+\epsilon d}{\epsilon d^2}, \frac{7}{d})$.

Teorem 3.2 (Coppersmith (1997))**.** *Neka je $f(x) \in \mathbb{Z}[x]$ normirani polinom stupnja d, te neka je N prirodan broj. Ako postoji rješenje kongruencije $f(x_0) \equiv 0 \pmod{N}$ koje zadovoljava nejednakost $|x_0| \leq N^{1/d-\epsilon}$, tada postoji algoritam koji pronalazi x_0, a čija je složenost polinomijalna u $\log N$ i $1/\epsilon$ (za fiksirani d).*

Poglavlje 4

Aproksimacija algebarskih brojeva

4.1 Liouvilleov teorem

Definicija 4.1. *Kompleksan broj α naziva se* algebarski broj *ako postoji polinom $Q(x)$ s racionalnim koeficijentima, različit od nulpolinoma, takav da je $Q(\alpha) = 0$. Kompleksan broj se zove* transcendentan *ako nije algebarski.*

Teorem 4.1. *Za svaki algebarski broj α postoji jedinstveni polinom*

$$P(x) = a_d x^d + \cdots + a_0$$

sa sljedećim svojstvima

1) $P(x) \in \mathbb{Z}[x]$*;*

2) $a_d > 0$ *i* $\operatorname{nzd}(a_0, a_1, \ldots, a_d) = 1$*;*

3) $P(\alpha) = 0$*;*

4) ako je $P_0(x) \in \mathbb{Q}[x]$ *takav da je* $P_0(\alpha) = 0$*, onda* $P(x) | P_0(x)$*;*

5) $P(x)$ *je ireducibilan nad* $\mathbb{Q}$*.*

Dokaz: Neka je $\mathcal{M}$ skup svih ne-nulpolinoma iz $\mathbb{Q}[x]$ čiji je α korijen. Skup svih prirodnih brojeva koji su stupnjevi nekog polinoma iz $\mathcal{M}$ je neprazan, pa sadrži minimalni element. Neka je taj minimalni element d. Dakle, postoji $P_1(x) \in \mathbb{Q}[x]$, $\operatorname{st} P_1 = d$ i $P_1(\alpha) = d$. Pomnožimo li $P_1(x)$ s najmanjim zajedničkim višekratnikom nazivnika njegovih koeficijenata, dobivamo polinom $P_2(x)$ s cjelobrojnim koeficijentima. Podijelimo $P_2(x)$ s najvećeim zajedničkim djeljiteljem njegovih koeficijenata i pomnožimo ga s -1 ako mu je vodeći koeficijent negativan. Na taj način smo dobili polinom $P(x)$ za kojeg tvrdimo da zadovoljava uvjete teorema. Prva tri svojstva su očito zadovoljena.

Neka je $P_0 \in \mathbb{Q}$ takav da je $P_0(\alpha) = 0$. Podijelimo polinom $P_0(x)$ s $P(x)$. Dobivamo

$$P_0(x) = P(x)S(x) + R(x), \quad S(x), R(x) \in \mathbb{Q}[x], \quad \operatorname{st} R(x) \leq d - 1.$$

Kako je $P_0(\alpha) = P(\alpha) = 0$, to je i $R(\alpha) = 0$, pa zbog minimalnosti od d, polinom $R(x)$ mora biti nulpolinom. Dakle, $P(x)|P_0(x)$ i svojstvo 4) je dokazano.

Pokažimo da je $P(x)$ ireducibilan nad $\mathbb{Q}$. U protivnom bi bilo $P(x) = Q_1(x)Q_2(x)$, gdje je $1 \leq \operatorname{st} Q_i \leq d - 1$, pa bi imali $Q_1(\alpha) = 0$ ili $Q_2(\alpha) = 0$, protivno pretpostavci o minimalnosti stupnja od $P(x)$.

Konačno, pokažimo jedinstvenost od $P(x)$. Neka je $T(x) \in \mathbb{Q}[x]$ polinom koji zadovoljava svojstva 1) – 5). Tada polinom $U(x)$ takav da je $T(x) = P(x)U(x)$. No, ireducibilnost od $T(x)$ povlači da je $U(x)$ konstanta, dok iz svojstva 2) slijedi da je $U(x) = 1$, pa je $T(x) = P(x)$. □

Definicija 4.2. Minimalni polinom *algebarskog broja α je polinom $P(x)$ opisan u Teoremu 4.1.* Stupanj *algebarskog broja je stupanj njegovog minimalnog polinoma.*

Napomena 4.1. Često se minimalnim polinomom od α naziva i polinom $g(x) = \frac{1}{a_d}P(x)$, dakle ireducibilni normirani polinom s racionalnim koeficijentima takav da je $g(\alpha) = 0$.

Teorem 4.2 (Liouville (1844))**.** *Neka je α realan algebarski broj stupnja d. Tada postoji konstanta $c(\alpha) > 0$ tako da vrijedi*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$$

za sve racionalne brojeve $\frac{p}{q}$, gdje je $q > 0$ i $\frac{p}{q} \neq \alpha$.

Dokaz: Neka je $P(x)$ minimalni polinom od α. Bez smanjenja općenitosti možemo pretpostaviti da je $|\alpha - \frac{p}{q}| \leq 1$ (inače možemo staviti $c(\alpha) = 1$). Razvijemo li $P(x)$ u Taylorov red oko α, dobivamo:

$$\left|P(\frac{p}{q})\right| = \left|\sum_{i=1}^{d}(\frac{p}{q} - \alpha)^i \frac{1}{i!}P^{(i)}(\alpha)\right| < \frac{1}{c(\alpha)} \cdot \left|\alpha - \frac{p}{q}\right|, \tag{4.1}$$

gdje je $c(\alpha) = \frac{1}{2\sum_{i=1}^{d}\frac{1}{i!}|P^{(i)}(\alpha)|}$.

Budući da je polinom $P(x)$ ireducibilan, to je $P(\frac{p}{q}) \neq 0$. Stoga je broj $q^d\left|P(\frac{p}{q})\right|$ prirodan, pa je $\left|P(\frac{p}{q})\right| \geq \frac{1}{q^d}$. Usporedimo li ovo sa (4.1), dobivamo tvrdnju teorema. □

Primjer 4.1. *Broj $\alpha = \sum_{n=1}^{\infty} 2^{-n!}$ je transcendentan.*

Rješenje: Stavimo $q(k) = 2^{k!}$, $p(k) = 2^{k!} \sum_{n=1}^{k} 2^{-n!}$. Tada je

$$\left|\alpha - \frac{p(k)}{q(k)}\right| = \sum_{n=k+1}^{\infty} 2^{-n!} < 2^{-(k+1)!} + 2^{-(k+1)!-1} + 2^{-(k+1)!-2} + \cdots$$
$$= 2 \cdot 2^{-(k+1)!} = \frac{2}{(q(k))^{k+1}}.$$

Odavde slijedi da za svaki prirodan broj d i svaki $c > 0$ postoji $k_0 \in \mathbb{N}$ takav da za sve $k \geq k_0$ vrijedi

$$\left|\alpha - \frac{p(k)}{q(k)}\right| < \frac{c}{(q(k))^d}.$$

Po Liouvilleovom teoremu, α ne može biti algebarski broj stupnja d za niti jedan d, pa je stoga α transcendentan. ♢

4.2 Rothov teorem

Neka je α realan algebarski broj stupnja $d \geq 2$. Liouvilleov teorem povlači da nejednadžba

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\mu}} \tag{4.2}$$

ima samo konačno mnogo racionalnih rješenja $\frac{p}{q}$ ako je $\mu > d$.

Thue (1909) je dokazao da (4.2) ima samo konačno mnogo rješenja ako je $\mu > \frac{d}{2}+1$, Siegel (1921) je dokazao da ista tvrdnja vrijedi ako je $\mu > 2\sqrt{d}$, kok su Dyson (1947) i Geljfond (1948) dakazali tvrdnju za $\mu > \sqrt{2d}$. Konačno je Roth (1955) dokazao za nejednažba (4.2) ima samo konačno mnogo rješenja ako je $\mu > 2$. Za taj rezultat Roth je 1958. godine nagrađen Fieldsovom medaljom.

Teorem 4.3 (Roth (1955))**.** *Neka je α realan algebarski broj stupnja $d \geq 2$. Tada za svaki $\delta > 0$ nejednadžba*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}} \tag{4.3}$$

ima samo konačno mnogo rješenja u racionalnim brojevima $\frac{p}{q}$.

Napomena 4.2. *(i)* Tvrdnja Teorema 4.3 je točna i trivijalna za $\alpha \in \mathbb{C} \setminus \mathbb{R}$.

(ii) Po Dirichletovom teoremu, eksponent 2 u (4.3) je najbolji mogući. Ako je stupanj od α jednak 2, onda je $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^2}$ po Liouvilleovom teoremu, što povlači tvrdnju Rothovog teorema u ovom slučaju. Primijetimo da isti zaključak slijedi već iz Leme 1.4.

(iii) Nije poznat niti jedan algebarski broj α stupnja ≥ 3 za kojeg vrijedi $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^2}$, tj. koji je slabo aproksimabilan.

(iv) Lang (1965) je postavio slutnju da za svaki algebarski broj α stupnja ≥ 3 nejednadžba

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2(\log q)^\beta}$$

ima samo konačno mnogo rješenja ako je $\beta > 1$.

Ideja dokaza Rothovog teorema (a i prethodnih poboljšanja Liouvilleovog teorema) je da se pokuša modificirati osnovne korake u dokazu Liouvilleovog teorema. U Liovilleovom teoremu kreće se od minimalnog polinoma od α. U svom poboljšanju Liouvilleovog teorema, Thue je koristio polinom oblika $x_2Q(x_1) - P(x_1)$, Siegel je koristio općeniji polinom $P(x_1, x_2)$ u dvije varijable, dok je Roth koristio polinom $P(x_1, \ldots, x_m)$ u više varijabli. Glavna poteškoća u ovakvom pristupu nastupa dok provjere zadnjeg koraka iz dokaza Liouvilleovog teorema. Dok polinoma u jednom varijabli, zaključak da je $P(\frac{p}{q}) \neq 0$ bio je sasvim jednostavan. No, kod polinoma u više varijabli, skup rješenja jednadžbe $P(x_1, \ldots, x_m) = 0$ je neka algebarska mnogostrukost u $\mathbb{R}^m$ i vrlo je teško pokazati da je $P(\frac{p}{q}, \ldots, \frac{p}{q}) \neq 0$. Ta se poteškoća pokušava riješiti korištenjem m-torki $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$ različitih racionalnih aproksimacija i pokušava se dokazati da je $P(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}) \neq 0$. Pokazuje da se nazivnici $q_1 < q_2 < \cdots < q_m$ moraju brzo rasti. Primjerice, u slučaju $m = 2$, trebaju nam dvije dobre aproksimacije $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$ od α takve da je q_2 puno veći od q_1. To je razlog zbog čega jedna dobra aproksimacija ne daje nikakvu konradikciju, te je Rothov teorem, kao i sva ostala poboljšanja Liouvilleovog teorema dobivena ovom metodom, "neefektivan", u smislu da ne daje nikakvu ogradu za veličinu nazivnika q u dobrim aproksimacijama.

Definicija 4.3. *Za algebarski broj α kažemo da je* algebarski cijeli broj *ako je α korijen nekog normiranog polinoma s cjelobrojnim koeficijentima.*

Iz Gaussove leme, koja kaže da ako su $f(x) \in \mathbb{Z}[x]$, $g(x), h(x) \in \mathbb{Q}[x]$ normirani polinomi i $f(x) = g(x)h(x)$, onda su $g(x), h(x) \in \mathbb{Z}[x]$, slijedi da je minimalni polinom algebarskog cijelog broja normiran.

Ako je α algebarski broj stupnja d koji zadovoljava jednadžbu $a_d x^d + \cdots + a_0 = 0$, onda je $\beta = a_d\alpha$ algebarski cijeli broj stupnja d. Pretpostavimo da nejednadžba $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}}$ ima beskonačno mnogo rješenja. Tada i nejednadžba $\left|\beta - a_d\frac{p}{q}\right| < \frac{a_d}{q^{2+\delta}}$ ima beskonačno mnogo rješenja takvih da je $q^{\delta/2} > a_d$, pa dobivamo da nejednadžba $\left|\beta - \frac{a_d p}{q}\right| < \frac{1}{q^{2+\delta/2}}$ ima beskonačno mnogo rješenja. Stoga je dovoljno dokazati Rothov teorem za algebarske cijele brojeve.

Feljdman (1971) je, koristeći Bakerovu metodu linearnih formu u logaritmima algebarskih brojeva, dokazao "efektivno" poboljšanje Liouvilleovog teorema, naime rezultat tipa

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^{d-c_1(\alpha)}},$$

gdje su $c(\alpha) > 0$ i $c_1(\alpha) > 0$ eksplicitne konstante. Međutim, konstanta $c_1(\alpha)$ dobivena tom metodom je obično vrlo mala, tako da je eksponent $d - c_1(\alpha)$ veći od eksponenta $\frac{d}{2} + 1$ iz Thueovog teorema.

4.3 Thueova jednadžba

Neka je

$$F(x,y) = a_0x^n + a_1x^{n-1}y + \cdots + a_ny^n$$

binarna forma s cjelobrojnim koeficijentima, ireducibilna nad $\mathbb{Q}$, stupnja $n \geq 3$. Primijetimo da forma F ne može biti ireducibilna nad $\mathbb{C}$. Naime,

$$F(x,1) = a_0(x-\theta_1)\cdots(x-\theta_n),$$

gdje su $\theta_1, \ldots, \theta_n$ algebarski brojevi stupnja n, pa je

$$F(x,y) = y^nF(\frac{x}{y},1) = a_0(x-\theta_1y)\cdots(x-\theta_ny).$$

No, ireducibilnost nad $\mathbb{Q}$ povlači da $F(x,1)$ nema višestrukih korijena, tj. da su θ_i-ovi međusobno različiti.

Neka je $m \neq 0$ cijeli broj. Diofantsku jednadžbu oblika $F(x,y) = m$ zovemo *Thueova jednadžba*. Godine 1909. Thue je dokazao da takva jednadžba ima samo konačno mnogo rješenja, koristeći svoj, ranije spomenuti, rezultat iz diofantskih aproksimacija. Dokažimo najprije jednostavan specijalni slučaj tog rezultata.

Teorem 4.4. *Ako jednadžba $F(x,1) = 0$ nema realnih rješenja, tada jednadžba $F(x,y) = m$ ima samo konačno mnogo rješenja. Preciznije, sva rješenja zadovoljavaju nejednakost*

$$|y| \leq \frac{|m|}{\min_{1\leq i\leq n}|Im\,(\theta_i)|},$$

gdje smo sa θ_i označili korijene polinoma $F(x,1)$.

Dokaz: Pretpostavimo da je (x,y) rješenje jednadžbe $F(x,y) = m$ i uzmimo θ_k tako da je $|x-\theta_ky| = \min_{1\leq i\leq n}|x-\theta_iy|$. Tada je jasno da vrijedi $|y|\cdot|\mathrm{Im}\,(\theta_k)| = |\mathrm{Im}\,(\theta_ky)| \leq |x-\theta_ky| \leq |m|$, pa dobivamo tvrdnju teorema. □

Teorem 4.5 (Thue)**.** *Thueova jednadžba ima samo konačno mnogo cjelobrojnih rješenja.*

Dokaz: Neka je $F(x,y) = m$. Uz gore uvedene oznake, možemo pisati

$$a_0(x-\theta_1y)\cdots(x-\theta_ny) = m. \tag{4.4}$$

Možemo pretpostaviti da je $y \neq 0$, jer za $y = 0$ imamo najviše dva rješenja. Podijelimo (4.4) sa y^n i uzmimo apsolutne vrijednosti, pa dobivamo

$$|a_0|\cdot\left|\theta_1-\frac{x}{y}\right|\cdots\left|\theta_n-\frac{x}{y}\right| = \left|\frac{m}{y^n}\right|. \tag{4.5}$$

Kao i u dokazu prethodnog teorema, uzmimo θ_k tako da je

$$|x - \theta_k y| = \min_{1 \le i \le n} |x - \theta_i y|,$$

tj.

$$\left|\theta_k - \frac{x}{y}\right| = \min_{1 \le i \le n} \left|\theta_i - \frac{x}{y}\right|.$$

Neka je $\gamma = \frac{1}{2} \min_{i \neq j} |\theta_i - \theta_j| > 0$. Za y dovoljno velik, obje strane od (4.5) se mogu učiniti po volji male. Posebno to onda vrijedi i za najmanji faktor na lijevoj strani, tj. $|\theta_k - \frac{x}{y}|$. Dakle, postoji $y_0 > 0$ tako da za $y \ge y_0$ vrijedi $|\theta_k - \frac{x}{y}| < \gamma$. Za $i \neq k$ imamo:

$$|\theta_i - \frac{x}{y}| \ge |\theta_i - \theta_k| - |\theta_k - \frac{x}{y}| \ge 2\gamma - \gamma = \gamma.$$

Stoga iz (4.5) slijedi

$$\left|\theta_k - \frac{x}{y}\right| \le \left|\frac{m}{a_0 y^n \gamma^{n-1}}\right| = \frac{c}{|y|^n}. \tag{4.6}$$

Budući da je $n \ge 3$, Rothov teorem (u stvari već i Thueov, ali ne i Liouvilleov) povlači da nejednadžba (4.6) ima samo konačno mnogo rješenja, što je i trebalo dokazati. □

Napomena 4.3. Iz teorije linearnih diofantskih jednadžbi i Pellovih jednadžbi znamo da tvrdnja Teorema 4.5 ne vrijedi ako je stupanj $n = 1$ ili $n = 2$. S druge strane, tvrdnja Teorema 4.5 vrijedi ukoliko se pretpostavka da je polinom ireducibilan nad $\mathbb{Q}$ zamijeni s pretpostavkom da polinom $F(x, 1)$ ima barem tri različita (kompleksna) korijena.

Zaista, pretpostavimo da je polinom $F(x, y)$ reducibilan nad $\mathbb{Q}$. Ako F ima barem dva različita ireducibilna faktora F_1 i F_2, onda dobivamo konačno mnogo sustava diofantskih jednadžbi $F_1(x, y) = m_1$, $F_2(x, y) = m_2$. Svaki od tih sustava ima konačno mnogo (kompleksnih) rješenja (po Bezoutovom teoremu broj rješenja nije veći od produkta stupnjeva od F_1 i F_2). Ostaje razmotriti slučaj $F(x, y) = aG(x, y)^k$, gdje je polinom G ireducibilan nad $\mathbb{Q}$. Ako je $\deg G \ge 3$, onda iz Teorema 4.5 slijedi da jednadžba $F(x, y) = m$ ima konačno mnogo rješenja. Dakle, jedini slučajevi kada jednadžba $F(x, y) = m$, gdje je F binarna forma, može imati beskonačno mnogo rješenja su slučajevi kada je

$$F(x, y) = a(bx + cy)^n \quad \text{ili} \quad F(x, y) = a(bx^2 + cxy + dy^2)^{n/2},$$

a to su upravo slučajevi kada $F(x, 1)$ ima manje od tri različita korijena.

Primjer 4.2. *Naći sva cjelobrojna rješenja jednadžbe*

$$x^5 - x^4 y - 4x^3 y^2 + 2x^2 y^3 + 4xy^4 + y^5 = 1.$$

Rješenje: Vrijedi

$$x^5 - x^4y - 4x^3y^2 + 2x^2y^3 + 4xy^4 + y^5 = (x^3 - 3xy^2 - y^3)(x^2 - xy - y^2),$$

pa se rješavanje dane jednadžbe svodi na rješavanje dvaju sustava diofantskih jednadžbi

$$x^3 - 3xy^2 - y^3 = 1, \qquad x^2 - xy - y^2 = 1; \tag{4.7}$$

$$x^3 - 3xy^2 - y^3 = -1, \qquad x^2 - xy - y^2 = -1. \tag{4.8}$$

Jedan od načina za rješavanje sustava polinomijalnih jednadžbi je pomoću tzv. *rezultante* polinoma. Rezultanta polinoma $f(X) = a_0X^l + \cdots + a_l$ i $g(X) = b_0X^m + \cdots + b_m$ nad poljem k, u oznaci $\mathrm{Res}(f, g)$ ili $\mathrm{Res}(f, g, X)$, je $(l + m) \times (l + m)$ determinanta

$$\begin{vmatrix}
a_0 & & & & b_0 & & & \\
a_1 & a_0 & & & b_1 & b_0 & & \\
a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\
\vdots & a_2 & \ddots & a_0 & \vdots & b_2 & \ddots & b_0 \\
a_l & \vdots & \ddots & a_1 & b_m & \vdots & \ddots & b_1 \\
 & a_l & & a_2 & & b_m & & b_2 \\
 & & \ddots & \vdots & & & \ddots & \vdots \\
 & & & a_l & & & & b_m
\end{vmatrix}$$

(na praznim mjestima su nule). Važna svojstva rezultante su:

- $\mathrm{Res}(f, g) = 0$ ako i samo ako f i g imaju zajednički faktor u $k[X]$;
- postoje polinomi A i B iz $k[X]$ takvi da vrijedi $Af + Bg = \mathrm{Res}(f, g)$.

Ako su $f, g \in k[x, y]$, onda ovo posljednje svojstvo povlači da za svako rješenje sustava $f(x, y) = 0$, $g(x, y) = 0$ vrijedi $\mathrm{Res}(f, g, x) = 0$ i $\mathrm{Res}(f, g, y) = 0$. U slučaju sustava (4.7), dobivamo jednadžbu

$$\mathrm{Res}(x^3 - 3xy^2 - y^3 - 1, x^2 - xy - y^2 - 1, x) =$$
$$\begin{vmatrix}
1 & 0 & 1 & 0 & 0 \\
0 & 1 & -y & 1 & 0 \\
-3y^2 & 0 & -y^2 - 1 & -y & 1 \\
-y^3 - 1 & -3y^2 & 0 & -y^2 - 1 & -y \\
0 & -y^3 - 1 & 0 & 0 & -y^2 - 1
\end{vmatrix} = -y^6 + y^3 + 3y^2 - 3y = 0,$$

čija su jedina cjelobrojna rješenja $y = 0$ i $y = 1$. Za sustav (4.8), dobivamo jednadžbu

$$\mathrm{Res}(x^3 - 3xy^2 - y^3 + 1, x^2 - xy - y^2 + 1, x) = -y^6 - y^3 + 3y^2 - 3y + 2 = 0,$$

čije je jedino cjelobrojno rješenje $y = 1$. Sada se lako provjeri da su sva rješenja polazne jednadžbe $(x, y) = (1, 0), (2, 1)$ i $(0, 1)$. ♢

4.4 Tzanakisova metoda za kvartične Thueove jednadžbe i nejednadžbe

Problem nalaženja svih cjelobrojnih rješenja Thueove jednadžbe je od interesa sam za sebe, ali također i zbog toga što se drugi važni diofantski problemi, poput nalaženja cjelobrojnih točaka na eliptičkim krivuljama, mogu svesti na taj problem. Poznati opći algoritmi za rješavanje Thueovih jednadžbi zahtjevaju poznavanje netrivijalnih podataka o prstenu cijelih brojeva polja $\mathbb{Q}(\theta_i)$ (fundamentalne jedinice, faktorizacija). To može predstavljati veliki problem, pogotovo kod rješavanja parametarske familije takvih jednadžbi.

Godine 1993. Tzanakis je pokazao kako se jedna dosta široka klasa Thueovih jednadžbi 4. stupnja može svesti na problem rješavanja sustava pellovskih jednadžbi. To je slučaj kada je $\mathbb{Q}(\theta_i)$ kompozit od dva realna kvadratna polja, tj. $\mathbb{Q}(\theta_i) = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Metoda je posebno korisna kod rješavanja Thueovih nejednadžbi $|f(x, y)| \leq m$, jer iz poznavanja verižnog razlomka od $\sqrt{d_1}$ i $\sqrt{d_2}$, korištenjem rezultata iz diofantskih aproksimacija (primjerice Worleyevog teorema), možemo eliminirati one $|\mu| \leq m$ za koje jednadžba $f(x, y) = \mu$ nema rješenja.

Promotrimo kvartičnu Thueovu jednadžbu

$$f(x, y) = m, \tag{4.9}$$

gdje je

$$f(x, y) = a_0x^4 + 4a_1x^3y + 6a_2x^2y^2 + 4a_3xy^3 + a_4y^4 \in \mathbb{Z}[x, y], \;\; a_0 > 0.$$

Ovoj jednadžbi pridružujemo kubnu jednadžbu

$$4\rho^3 - g_2\rho - g_3 = 0 \tag{4.10}$$

čiji su korijeni suprotni korijenima kubne rezolvente jednadžbe $f(x, 1) = 0$. Ovdje je $g_2 = a_0a_4 - 4a_1a_3 + 3a_2^2 \in \frac{1}{12}\mathbb{Z}$,

$$g_3 = \begin{vmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{vmatrix} \in \frac{1}{432}\mathbb{Z}\,.$$

Da bi promatrano kvartično polje imalo željeni oblik, nužno je i dovoljno da kubna jednadžba (4.10) ima tri racionalna korijena ρ_1, ρ_2, ρ_3, te da je

$$\frac{a_1^2}{a_0} - a_2 \geq \max\{\rho_1, \rho_2, \rho_3\}. \tag{4.11}$$

Za polinom $f(x,y)$, definiramo njegovu invarijantu četvrtog stupnja $H(x,y)$ i invarijantu šestog stupnja $G(x,y)$ na sljedeći način:

$$H(x,y)=-\frac{1}{144}\begin{vmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial y^2} \end{vmatrix} \in \frac{1}{48}\mathbb{Z}[x,y]\,,$$

$$G(x,y)=-\frac{1}{8}\begin{vmatrix} \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} \\ \frac{\partial H}{\partial x} & \frac{\partial H}{\partial y} \end{vmatrix} \in \frac{1}{96}\mathbb{Z}[x,y]\,.$$

Tada vrijedi $4H^3 - g_2 H f^2 - g_3 f^3 = G^2$. Ako stavimo $H = \frac{1}{48}H_0$, $G = \frac{1}{96}G_0$, $\rho_i = \frac{1}{12}r_i$, $i = 1,2,3$, onda su $H_0, G_0 \in \mathbb{Z}[x,y]$, $r_i \in \mathbb{Z}$, $i = 1,2,3$, te

$$(H_0 - 4r_1 f)(H_0 - 4r_2 f)(H_0 - 4r_3 f) = 3G_0^2.$$

Postoje kvadratno slobodni prirodni brojevi k_1, k_2, k_3 i kvadratne forme G_1, G_2, $G_3 \in \mathbb{Z}[x,y]$ tako da je

$$H_0 - 4r_i f = k_i G_i^2, \quad i = 1,2,3$$

i $k_1k_2k_3(G_1G_2G_3)^2 = 3G_0^2$. Ako je $(x,y) \in \mathbb{Z}\times\mathbb{Z}$ rješenje jednadžbe (4.9), onda eliminacijom H_0 dobivamo

$$k_2G_2^2 - k_1G_1^2 = 4(r_1 - r_2)m, \tag{4.12}$$
$$k_3G_3^2 - k_1G_1^2 = 4(r_1 - r_3)m. \tag{4.13}$$

Na ovaj se način rješavanje Thueove jednadžbe (4.9) svelo na rješavanje sustava pellovskih jednadžbi (4.12) i (4.13) s jednom zajedničkom nepoznanicom.

Ilustrirat ćemo Tzanakisovu metodu na familiji Thueovih jednadžbi i nejednadžbi iz članaka Dujelle i Jadrijević (2002, 2004). Neka je

$$f(x,y) = x^4 - 4cx^3y + (6c+2)x^2y^2 + 4cxy^3 + y^4\,.$$

Tada je

$$g_2 = \frac{1}{3}(21c^2 + 6c + 4),$$
$$g_3 = -\frac{1}{27}(81c^3 + 99c^2 - 18c - 8),$$

$$\rho_1 = \frac{1}{2}c + \frac{2}{3}, \quad \rho_2 = c - \frac{1}{3}, \quad \rho_3 = -\frac{3}{2}c - \frac{1}{3}.$$

Očito je da je uvjet (4.11) zadovoljen.

Nadalje, dobivamo

$$\begin{aligned} H_0 - 4r_1 f &= 24(c-2)(2c+1)(x^2+y^2)^2, \\ H_0 - 4r_2 f &= 48c(c-2)(x^2+xy-y^2)^2, \\ H_0 - 4r_3 f &= 24c(2c+1)(-x^2+4xy+y^2)^2. \end{aligned}$$

Stoga možemo staviti $k_1 = 6(c-2)(2c+1)$, $k_2 = 3c(c-2)$, $k_3 = 6c(2c+1)$, $G_1 = 2(x^2+y^2)$, $G_2 = 4(x^2+xy-y^2)$, $G_3 = 2(-x^2+4xy+y^2)$. Uvrstimo li ovo u (4.12) i (4.13), dobivamo

$$cG_2^2 - (4c+2)G_1^2 = -8m, \tag{4.14}$$

$$cG_3^2 - (c-2)G_1^2 = 8m. \tag{4.15}$$

Neka je

$$U = \frac{G_1}{2} = x^2+y^2, \quad V = \frac{G_2}{4} = x^2+xy-y^2, \quad Z = \frac{G_3}{2} = -x^2+4xy+y^2.$$

Tada iz (4.14) i (4.15) dobivamo sustav pellovskih jednadžbi

$$(2c+1)U^2 - 2cV^2 = m, \tag{4.16}$$

$$(c-2)U^2 - cZ^2 = -2m. \tag{4.17}$$

U slučaju kada je $m = 1$, može se pokazati da su sva rješenja od (4.16) dana sa $U = v_m$, gdje je

$$v_0 = 1, \quad v_1 = 8c+1, \quad v_{m+2} = (8c+2)v_{m+1} - v_m, \quad m \geq 0, \tag{4.18}$$

a sva rješenja od (4.17) sa $U = w_n$, gdje je

$$w_0 = 1, \quad w_1 = 2c-1, \quad w_{n+2} = (2c-2)w_{n+1} - w_n, \quad n \geq 0. \tag{4.19}$$

Dakle, rješavanje Thueove jednadžbe $f(x,y) = 1$ svodi se na nalaženje presjeka nizova v_m i w_n. Korištenjem standardnih metoda za rješavanje takvog problema, Dujella i Jadrijević su pokazali da je jedino rješenje $m = n = 0$, tj. $(x,y) = (\pm 1, 0), (0, \pm 1)$.

Promotrimo sada Thueovu nejednadžbu

$$|f(x,y)| < 6c-2. \tag{4.20}$$

Prema gore pokazanom, njezino rješavanje se svodi na rješavanje sustava pellovskih jednadžbi (4.16) i (4.17), gdje je $|m| < 6c-2$. Dokazat ćemo sljedeći rezultat.

Teorem 4.6. *Neka je $c \geq 5$ prirodan broj. Sva rješenja Thueove nejednažbe*

$$|x^4 - 4cx^3y + (6c+2)x^2y^2 + 4cxy^3 + y^4| < 6c-2$$

u relativno prostim cijelim brojevima x i y su $(x,y) = (\pm 1, 0), (0, \pm 1), (\pm 1, \mp 2), (\pm 2, \pm 1)$.

Budući da je $f(a,b) = f(-a,-b) = f(b,-a) = f(-b,a)$, dovoljno je naći rješenja u nenegativnim cijelim brojevima, i tvrdimo da su jedina takva rješenja $(x,y) = (1,0)$, $(0,1)$ i $(2,1)$. Budući da je $f(1,0) = f(0,1) = 1$, $f(2,1) = 25$, vidimo da to zaista jesu rjesenja od (4.20) za $c \geq 5$. Slučaj $m = 1$ smo već razmotrili, pa se sada pitamo za koje još m-ove, $|m| < 6c-2$, jednadžba 4.16 ima rješenja. Iz

$$(2c+1)U^2 - 2cV^2 = m,$$

slijedi

$$\begin{aligned}\left|\sqrt{\frac{2c+1}{2c}} - \frac{V}{U}\right| &= \left|\frac{2c+1}{2c} - \frac{V^2}{U^2}\right| \cdot \left|\sqrt{\frac{2c+1}{2c}} + \frac{V}{U}\right|^{-1} \\ &< \frac{|m|}{2cU^2} \cdot \frac{1}{2} < \frac{2}{U^2}.\end{aligned}$$

Pretpostavimo da su U i V relativno prosti. Iz Worleyevog teorema (Teorem 1.8) znamo da V/U ima oblik $(rp_n \pm sp_{n-1})/(rq_n \pm sq_{n-1})$ za $rs < 4$, gdje je p_n/q_n n-ta konvergenta verižnog razlomka od

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

Iskoristimo formulu

$$(2c+1)(rq_n \pm sq_{n-1})^2 - 2c(rp_n \pm sp_{n-1})^2 = (-1)^n(r^2t_{n+1} - s^2t_n \mp 2rss_{n+1}),$$

koja je analogon formule (1.33), gdje su (s_n), (t_n) nizovi koji se dobiju primjenom algoritma za razvoj u verižni razmlomak kvadratne iracionalnosti $\sqrt{\frac{2c+1}{2c}} = \frac{\sqrt{2c(2c+1)}}{2c}$, tj. $s_n = 2c$, $t_{2n} = 2c$, $t_{2n+1} = 1$. Dobivamo da su jedini m-ovi, $|m| < 6c-2$, za koje jednadžba 4.16 ima rješenja $m = 1, -2c, 2c+1, -6c+1$. Preciznije, rješenja su $(U,V) = (q_{2n}, p_{2n})$ ako je $m = 1$; $(U,V) = (q_{2n+1}, p_{2n+1})$ ako je $m = -2c$; $(U,V) = (q_{2n+1} + q_{2n}, p_{2n+1} + p_{2n})$ ako je $m = 2c+1$.

Sve ovo smo dobili promatranjem samo jednadžbe (4.16). Promotrimo sada sustav (4.16) i (4.17). Tvrdimo da on nema rješenja za $m = -2c$ i $2c+1$. Niz q_n zadovoljavaju rekurzije

$$\begin{aligned}q_{2n} &= 2q_{2n-1} + q_{2n-2}, \\ q_{2n+1} &= 4cq_{2n} + q_{2n-1},\end{aligned}$$

te

$$\begin{aligned}q_{2n} &= (8c+2)q_{2n-2} - q_{2n-4}, \\ q_{2n+1} &= (8c+2)q_{2n-1} - q_{2n-3}.\end{aligned}$$

Analogne rekurzije zadovoljava niz p_n.

Neka je $m = -2c$. Tada je $U = q_{2n+1}$ za neki $n \geq 0$. Budući da je $q_1 = 4c$, $q_3 = 32c^2 + 8c$, zaključujemo da je U djeljiv sa $4c$, recimo $U = 4cU_1$. Tada je $Z = 2Z_1$ i jednažba (4.17) postaje

$$Z_1^2 - 4c(c-2)U_1^2 = -1,$$

što je očito nemoguće modulo 4.

Neka je sada $m = 2c + 1$. Tada je $V = p_{2n+1} + p_{2n}$. Budući da je $p_1 + p_0 = 2(2c + 1)$ i $p_3 + p_2 = 4(2c + 1)(4c + 1)$, zaključujemo da je $V = 2(2c + 1)V_1$. Uvrstimo li ovo u sustav (4.16) i (4.17), dobivamo

$$Z^2 - 8(c-2)(2c+1)V_1^2 = 5,$$

što je nemoguće modulo 8.

Na ovaj način smo dokazali Teorem 4.6 u slučaju kada su U i V relativno prosti. Pretpostavimo sada da je $d = \gcd(U, V) > 1$. Neka je $U = dU_1$, $V = dV_1$. Tada su U_1 i V_1 relativno prosti i zadovoljavaju

$$(2c+1)U_1^2 - 2cV_1^2 = \frac{m}{d^2}.$$

Budući da je $|m/d^2| \leq (6c-2)/4 < 2c$, prema gore pokazanom, mora vrijediti da je $m/d^2 = 1$, tj. $m = d^2$. Iz

$$4V^2 + Z^2 = 5U^2$$

slijedi da $d|Z$, recimo $Z = dZ_1$. Dakle, dobili smo trojku (U_1, V_1, Z_1) koja zadovoljava sustav $(2c + 1)U_1^2 - 2cV_1^2 = 1$, $(c - 2)U_1^2 - cZ_1^2 = -2$. No, to je upravo sustav (4.16), (4.17) za $m = 1$, za koji znamo da su mu jedina rješenja $(U_1, V_1, Z_1) = (\pm 1, \pm 1, \pm 1)$. Dakle, $(U, V, Z) = (\pm d, \pm d, \pm d)$, tj.

$$x^2 + y^2 = d, \tag{4.21}$$

$$x^2 + xy - y^2 = \pm d, \tag{4.22}$$

$$-x^2 + 4xy + y^2 = \pm d. \tag{4.23}$$

Pretpostavili smo da su x i y nenegativni, pa imamo predznak + u (4.22) i (4.23). Sada (4.21) i (4.22) povlače $xy = 2y^2$ pa, jer su x i y relativno prosti, dobivamo da je $(x, y) = (2, 1)$.

Poglavlje 5

Aproksimacija algebarskim brojevima

5.1 Aproksimacija kvadratnim iracionalnostima

Osnovni problem o diofantskim aproksimacijama jest problem aproksimacije realnog broja pomoću racionalnim brojeva. Racionalne brojeve možemo shvatiti kao algebarske brojeva prvog stupnja. Stoga je prirodno promatrati generalizaciju ovog osnovnog problema u kojoj se racionalni brojevi zamjenjuju algebarskim brojevima stupnja $\leq k$, za dani prirodni broj k.

Ako je α algebarski broj n-tog stupnja, onda on zadovoljava jednadžbu $P(\alpha) = 0$, gdje je $P(x) = a_n X^n + \cdots + a_0$ polinom n-tog stupnja s relativno prostim cjelobrojnim koeficijentima. *Apsolutna visina*, ili kraće samo *visina*, od α je definirana sa

$$H(\alpha) = \|P\| = \max(|a_0|, \ldots, |a_n|).$$

Sljedeća slutnja (Schmidt (1980) je generalizacija Dirichletovog teorema o diofantskim aproksimacijama:

Slutnja: *Neka je α realan broj koji nije algenarski broj stupnja $\leq k$. Tada postoji beskonačno mnogo realnih algebarskih brojeva β stupnja $\leq k$ sa svojstvom*

$$|\alpha - \beta| < \frac{c(k, \alpha)}{H(\beta)^{k+1}}.$$

Slutnja je točna za $k = 1$ po Dirichletovom teorema, a poznato je da je točna i za $k = 2$, dok je za $k \geq 3$ pitanje njezine točnosti i dalje otvoreno.

Teorem 5.1 (Davenport i Schmidt (1967))**.** *Za svaki realan broj α koji nije niti racionalan niti kvadratna iracionalnost, postoji beskonačno mnogo brojeva β koji su ili racionalni ili su kvadratne iracionalnosti, takvih da je*

$$|\alpha - \beta| < c(\alpha) H(\beta)^{-3}.$$

Ovaj teorem čemo dokazati malo kasnije. Što se tiče općeg slučaja, tj. proizvoljnog k, navest ćemo bez dokaza sljedeći rezultat.

Teorem 5.2 (Wirsing (1961))**.** *Za svaki realan broj α koji nije algebarski broj stupnja $\leq k$, postoji beskonačno mnogo algebarskih brojeva β stupnja $\leq k$ takvih da je*

$$|\alpha - \beta| < c(k, \alpha) H(\beta)^{-(k+3)/2}.$$

Neka je $x = (x_1, x_2, x_3)$, $\|x\| = \max(|x_1|, |x_2|, |x_3|)$, te $L(x) = \alpha x_1 + \beta x_2 + \gamma x_3$ linearna forma. Iz Teorema Minkowskog (Teoremi 2.5 i 2.6) slijedi da postoji beskonačno mnogo cjelobrojnih točaka $x \neq O$ sa svojstvom

$$|L(x)| \ll \|x\|^{-2},$$

gdje konstanta u $\ll$ ovisi o L. Za dokaz Teorema 5.1, trebat će sam sljedeći, nešto jači rezultat.

Teorem 5.3. *Neka su L i P nezavisne linearne forme. Tada postoji beskonačno mnogo cjelobrojnih točaka $x = (x_1, x_2, x_3) \neq O$ sa svojstvom*

$$|L(x)| \ll \|x\|^{-4} |P(x)|^2, \tag{5.1}$$

gdje konstanta u $\ll$ ovisi o L i P.

Dokaz: Možemo pretpostaviti da je $L(x) \neq 0$ za cjelobrojne točke $x \neq O$. Izaberimo linearnu formu F takvu da su F, L, P nezavisne. Stavimo

$$\langle x \rangle = \max(|F(x)|, |L(x)|, |P(x)|). \tag{5.2}$$

Za realan broj t, promotrimo konačan skup cjelobrojnih $x \neq O$ koje zadovoljavaju $\langle x \rangle \leq t$. Za velike t-ove ovaj skup je neprazan i zbog naše pretpostavke na L, vrijednosti od L u točakama tog skupa su različite. Odaberimo jedinstvenu točku x u tom skupu za koju je $|L(x)|$ minimalno i prvi element $\neq 0$ u trojki $F(x)$, $L(x)$, $P(x)$ je pozitivan. Nazovimo tu točku minimalnom točkom koja odgovara t. Očito je da ako je x minimalna točka koja odrgovara t, onda je ta točka minimalna za sve t-ove iz nekog intervala $t^* \leq t < t^{**}$. Postoji niz realnih brojeva $t_1 < t_2 < \cdots$ koji teži u beskonačno, i niz točaka $x^1, x^2, \ldots$, takvih da je x^i minimalna točka koja odgovara svim t-ovima u intervalu $t_i \leq t < t_{i+1}$, ali niti jednom drugom t-u. Jasno je da je $\langle x^i \rangle = t_i$. Uvedimo oznake $F_i = F(x^i)$, $L_i = L(x^i)$, $P_i = P(x^i)$. Očito je $|L_1| > |L_2| > \cdots$. Iz konstrukcije nizova t_i i x^i slijedi da ne postoji cjelobrojna točka $x \neq O$ takva da je

$$\langle x \rangle < t_{i+1}, \quad |L(x)| < |L_i|. \tag{5.3}$$

Nejednadžbe (5.3) definiraju simetričan konveksan skup volumena $\ll t_{i+1}^2 |L_i|$, tako da po teoremu Minkowskog o konveksnom tijelu imamo $t_{i+1}^2 |L_i| \ll 1$, tj.

$$|L_i| \ll t_{i+1}^{-2}. \tag{5.4}$$

Tvrdnja teorema bit će dokazana ako pokažemo da je $|L_i| \ll t_i^{-4} P_i^2$ za beskonačno mnogo i-ova. Pretpostavimo suprotno, tj. da je

$$P_i^2 = o(|L_i| t_i^4). \tag{5.5}$$

Tada iz (5.4) i (5.5) dobivamo

$$|P_i| = o(t_i^2 t_{i+1}^{-1}) = o(t_i). \tag{5.6}$$

Budući da $L_i \to 0$ i $\langle x^i \rangle = \max(|F_i|, |L_i|, |P_i|)$, zaključujemo da je $F_i = t_i$.

Za točku $y = x^{i+1} - x^i$ vrijedi $0 < F(y) < t_{i+1}$. Budući da je $|L(y)| \ll 1$ i $|P(y)| \le |P_{i+1}| + |P_i| = o(t_{i+1})$, imamo da je $\langle y \rangle < t_{i+1}$ ako je i dovoljno velik. Budući da (5.3) nema rješenje različito od O, mora vrijediti

$$|L_{i+1} - L_i| = |L(y)| \ge |L_i|.$$

Odavde je

$$L_i L_{i+1} < 0. \tag{5.7}$$

Lema 5.1. *Neka je i dovoljno velik, te*

$$|P_{i+1}| \le \frac{1}{2} t_i. \tag{5.8}$$

Tada je $x^{i+1} = v x^i + x^{i-1}$, gdje je v prirodan broj.

Dokaz: Definirajmo cijele brojeve u, v sa

$$u = \lfloor |L_{i-1}/L_i| \rfloor, \quad v = \lfloor t_{i+1}/t_i \rfloor,$$

te cjelobrojne točke y i z sa

$$y = x^{i+1} - v x^i, \quad z = x^{i-1} + u x^i.$$

Točke x^i i x^{i+1} su nezavisne, pa je $y \ne O$. Analogno je $z \ne O$.

Imamo $0 \le F(y) < t_i$, dok iz (5.4) slijedi $|L(y)| < \frac{3}{4} t_i$ ako je i dovoljno velik. Konačno, iz (5.6) i (5.8) slijedi

$$|P(y)| \le |P_{i+1}| + t_{i+1} t_i^{-1} |P_i| \le \frac{1}{2} t_i + o(t_{i+1} t_i^{-1} t_i^2 t_{i+1}^{-1}) < \frac{3}{4} t_i$$

za i dovoljno velik. Stoga je $\langle y \rangle < t_i$, pa budući da (5.3) nema ne-nul rješenja, mora vrijediti $|L(y)| \ge |L_{i-1}|$. Dakle, $|L_{i-1}| \le |L_{i+1}| + v|L_i|$, pa je $u \le v + |L_{i+1}/L_i| < v + 1$, tj. $u \le v$.

Vratimo li se na z, dobivamo

$$|L(z)| = |L_{i-1}| - u|L_i| < |L_i|, \tag{5.9}$$

budući da prema (5.7) L_{i-1} i L_i imaju različite predznake. Pošto (5.3) nema ne-nul rješenja, to je $\langle z \rangle \ge t_{i+1}$. Budući da je $|L(z)| = o(t_{i+1})$ i $|P(z)| \le$

$|P_{i-1}|+u|P_i| \le |P_{i-1}|+v|P_i| = o(t_{i+1})$, mora vrijediti $|F(z)| \ge t_{i+1}$. Odavde je

$$t_{i-1} + ut_i \ge t_{i+1},$$

pa je $v < u+1$, tj. $v \le u$. Dakle, dokazali smo da je $u = v$.

Promotrimo sada točku

$$w = x^{i+1} - vx^i - x^{i-1} = y - x^{i-1} = x^{i+1} - z. \tag{5.10}$$

Iz izraza $y - x^{i-1}$, onoga što već znamo o y, te iz (5.6), dobivamo $|L(w)|, |P(w)| < t_i$ ako je i dovoljno velik. Iz $0 \le F(y) < t_i$, dobivamo $|F(w)| < t_i$, tako da je

$$\langle w \rangle < t_i < t_{i+1}.$$

Također, iz izraza $x^{i+1} - z$, imajući u vidu da $L(z)$ ima isti predznak kao L_{i-1} i isti predznak kao L_{i+1}, dobivamo

$$|L(w)| \le \max(|L_{i+1}|, |L(z)|) < |L_i|.$$

Dakle, w zadovoljava (5.3), pa je $w = O$. □

Završetak dokaza Teorema 5.3: Pretpostavimo da (5.8) vrijedi za neki veliki i. Tada zbog Leme 5.1 imamo

$$\begin{aligned} |t_iL_{i+1} - t_{i+1}L_i| &= |t_{i-1}L_i - t_iL_{i-1}|, \\ |P_iL_{i+1} - P_{i+1}L_i| &= |P_{i-1}L_i - P_iL_{i-1}|. \end{aligned}$$

Pretpostavimo sada da (5.8) vrijedi da sve i, $h < i < k$. Tada je

$$|t_hL_{h+1} - t_{h+1}L_h| = |t_{k-1}L_k - t_kL_{k-1}| \tag{5.11}$$

i

$$|P_hL_{h+1} - P_{h+1}L_h| = |P_{k-1}L_k - P_kL_{k-1}|,$$

te

$$|P_{h+1}L_h| \le |P_hL_{h+1}| + |P_{k-1}L_k| + |P_kL_{k-1}|. \tag{5.12}$$

Ove relacije su trivijalno zadovoljene u slučaju $k = h+1$.

Lijeva strana od (5.11) je $|L(t_hx^{h+1} - t_{h+1}x^h)|$ i to nije 0. Ali prema (5.4) desna strana od (5.11) teži prema 0 kada $k \to \infty$. Prema tome, (5.8) ne može biti zadovoljeno za sve velike i, pa postoji beskonačno mnogo i-ova za koje (5.8) ne vrijedi.

Pretpostavimo da (5.8) vrijedi za sve i, $h < i < k$, ali ne za $i = h$ i $i = k$. Tada je $|P_{h+1}| > \frac{1}{2}t_h$ i prema (5.12), (5.5) i (5.6) imamo

$$\begin{aligned} \tfrac{1}{2}t_h|L_h| &\le |P_hL_{h+1}| + |P_{k-1}L_k| + |P_kL_{k-1}| \\ &= o(t_h|L_{h+1}| + |L_{k-1}|^{1/2}t_{k-1}^2|L_k| + |L_k|^{1/2}t_k^2|L_{k-1}|). \end{aligned}$$

Budući da je $|L_{h+1}| < |L_h|$ i $|L_k| < |L_{k-1}$, ovo daje

$$t_h|L_h| = o(t_k^2|L_k|^{1/2}|L_{k-1}|),$$

što zbog $|L_{k-1}| \leq |L_h|$ i (5.4) dalje povlači

$$t_h|L_h|^{1/2} = o(t_k^2|L_k|^{1/2}|L_{k-1}|^{1/2}) = o(t_k|L_k|^{1/2}).$$

Posebno, ako je h, pa onda i k, velik, imamo da je

$$t_k|L_k|^{1/2} > 2t_h|L_h|^{1/2}.$$

Međutim, ovo je nemoguće budući da generira beskonačni niz vrijednosti od j za koje $t_j|L_j|^{1/2}$ raste u ∞, dok s druge strane znamo iz (5.4) da je taj niz omeđen. □

Dokaz Teorema 5.1: Stavimo u Teoremu 5.3

$$L(x) = \alpha^2 x_1 + \alpha x_2 + x_3, \quad P(x) = 2\alpha x_1 + x_2.$$

Za dani x koji zadovoljava (5.1), polinom

$$B(t) = x_1 t^2 + x_2 t + x_3$$

zadovoljava

$$|B(\alpha) \ll \|x\|^{-4}|P(x)|^2 \ll \|x\|^{-3}|P(x)| \ll \|x\|^{-3}|B'(\alpha)|. \tag{5.13}$$

Sada je ili $\deg B = 1$ ili $\deg B = 2$. Ako je $\deg B = 1$, onda $B(t)$ ima racionalni korijen β sa svojstvom

$$0 = B(\beta) = B(\alpha) + (\beta - \alpha)B'(\alpha),$$

pa je

$$|\alpha - \beta| = |B(\alpha)/B'(\alpha)| \ll \|x\|^{-3} \ll \|B\|^{-3} \ll H(\beta)^{-3}.$$

Ako je $\deg B = 2$, onda korijen β od $B(t)$ zadovoljava

$$0 = B(\beta) = B(\alpha) + (\beta - \alpha)B'(\alpha) + \frac{1}{2}(\beta - \alpha)B''(\alpha).$$

Rješavajući ovu kvadratnu jednadžbu po $\beta - \alpha$, vidimo iz (5.13) da su korijeni β realni, te da za jedan od korijena β vrijedi

$$\begin{aligned} |\beta - \alpha| &= |-B'(\alpha) + \sqrt{B'(\alpha)^2 - 2B(\alpha)B''(\alpha)}|/|B''(\alpha)| \\ &= |2B(\alpha)|/|B'(\alpha) + \sqrt{B'(\alpha)^2 - 2B(\alpha)B''(\alpha)}| \\ &\ll |B(\alpha)/B'(\alpha)| \ll \|x\|^{-3} \ll \|B\|^{-3} \ll H(\beta)^{-3}. \end{aligned}$$

5.2 Separacija korijena polinoma

Neka je $P(x) = a_n x^n + \cdots + a_0$ polinom s cjelobrojnim koeficijentima. Pitamo se koliko bliski mogu biti njegovi različiti korijeni. Budući da složenost polinoma $P(X)$ obično mjerimo njegovom visinom

$$H(P) = \|P\| = \max(|a_0|, \ldots, |a_n|),$$

prirodno je usporediti udaljenost među različitim korijenima od $P(X)$ s visinom $H(P)$. Važan rezultat u tom smjeru je dobio Mahler 1964. godine kada je dokazao da je $|\alpha - \beta| \gg H(P)^{-n+1}$, za svaka dva različita korijena α, β polinoma $P(X)$ stupnja n s cjelobrojnim koeficijentima. Konstanta koja se podrazumijeva u $\gg$ je efektivna i ovisi o stupnju n danog polinoma.

Veza ovog problema s problemima i rezultatima diofantskih aproksimacija dolazi od toga što su korijena α, β polinoma $P(x)$ algebarski brojevi. I mi u ovom problemu razmatramo jednu varijantnu problema koliko se dobro jedan algebarski broj može aproksimirati drugim algebarskim brojem. Ako je još dodatno polinom P normiran, onda su promatrani korijeni α, β algebarski cijeli brojevi.

Pored (obične, naivne) visine $H(P)$ polinoma, postoje i druge definicije visine polinoma (pa onda i visine algebarskog broja). Npr. za polinom $P(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n)$, se definira veličina

$$M(P) = |a_n| \prod_{i=1}^{n} \max\{1, |\alpha_i|\},$$

koja se naziva *Mahlerova mjera* polinoma P, dok se *logaritamska Weilova visina* definira sa $h(P) = \frac{1}{n} \ln M(P)$. Vrijedi sljedeća nejednakost između naivne visine i Mahlerove mjere:

$$M(P) \leq \sqrt{n+1} H(P). \tag{5.14}$$

Ona je posljedica Jensenove formule

$$\ln \max\{1, |\alpha|\} = \int_0^1 \ln |e^{2\pi i t} - \alpha| dt.$$

Sada ćemo dokazati prije spomenuti Mahlerov rezultat

Teorem 5.4. *Neka je $P(x)$ polinom stupnja $n \geq 2$ s cjelobrojnim koeficijentima i različitim korijenima. Za svaka dva različita korijena α, β polinoma $P(x)$ vrijedi nejednakost*

$$|\alpha - \beta| > \sqrt{3}(n+1)^{-(2n+1)/2} \max\{1, |\alpha|, |\beta|\} H(P)^{-n+1}.$$

Dokaz: Neka je

$$P(x) = a_n x^n + \cdots + a_0 = a_n(x-\alpha_1)\cdots(x-\alpha_n).$$

Možemo pretpostaviti da je $|\alpha| \geq |\beta|$, te uzmimo da je $\alpha_1 = \alpha$, $\alpha_2 = \beta$. Budući da polinom $P(x)$ ima različite korijene (separabilan je), njegova diskriminanta

$$\mathrm{Disc}(P) = a_n^{2n-2} \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2$$

je cijeli broj različit od nule. Diskriminata $\mathrm{Disc}(P)$ se može zapisati i pomoću determinante Vandermondeove matrice

$$V = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ & & \cdots & & \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$

Vrijedi da je $\det(V) = \prod_{1\leq i<j\leq n}(\alpha_j - \alpha_i)$, pa je $\mathrm{Disc}(P) = \pm a_n^{2n-2}(\det(V))^2$. Vrijednost determinante V se neće promijeniti ako prvi redak zamijenimo s razlikom prvog i drugog redka. U novoj matrici, elementi prvog redka su $\alpha^j - \beta^j$. Prijemijeno sada na tu novu matricu Hadamardovu nejednakost, koja kaže da apsolutna vrijednost determinante nije veća od produkta duljina vektora stupaca matrice. Dakle, imamo

$$\begin{aligned} |\mathrm{Disc}(P)| &\leq |a_n|^{2n-2} \left(\textstyle\sum_{j=1}^{n-1} |\alpha^j - \beta^j|^2\right) \cdot \prod_{i=2}^{n}(1 + |\alpha_i|^2 + \cdots + |\alpha_i|^{2n-2}) \\ &\leq |a_n|^{2n-2}|\alpha-\beta|^2 \left(\textstyle\sum_{j=1}^{n-1} |\alpha^{j-1} + \alpha^{j-2}\beta + \cdots + \beta^{j-1}|^2\right) \\ &\qquad \cdot n^{n-1} \textstyle\prod_{i=2}^{n} \max\{1, |\alpha_i|\}^{2n-2} \\ &\leq |\alpha-\beta|^2 n^{n-1} M(P)^{2n-2} \max\{1,|\alpha|\}^{-2} \cdot (1 + 2^2 + 3^2 + \cdots (n-1)^2). \end{aligned}$$

Sada iz $1+2^2+\cdots(n-1)^2 = \frac{n(n-1)(2n-1)}{6} < \frac{n^3}{3}$, $|\mathrm{Disc}(P)| \geq 1$ i nejednakosti (5.14) dobivamo tvrdnju teorema. □

Za polinom $P(x)$ stupnja $n \geq 2$ s cjelobrojnim koeficijentima i različitim korijenima $\alpha_1, \ldots, \alpha_n$, definiramo

$$\mathrm{sep}(P) = \min_{1\leq i<j\leq n} |\alpha_i - \alpha_j|$$

te eksponent separacije $e(P)$ sa

$$\mathrm{sep}(P) = H(P)^{-e(P)}.$$

Nadalje, za fiksirani $n \geq 2$, stavimo

$$e(n) := \limsup_{\deg(P)=n, H(P)\to+\infty} e(P),$$

$$e_{\text{irr}}(n) := \limsup_{\deg(P)=n, H(P)\to+\infty} e(P),$$

gdje se u zadnjem slučaju limes superior uzima po svim ireducibilnim cjelobrojnim polinomimam $P(x)$ stupnja n.

Mahlerov teorem pokazuje da je $e(n) \leq n-1$ za sve n. Točne vrijednosti za $e(n)$ i $e_{\text{irr}}(n)$ su poznate samo za $n = 2$ i $n = 3$, s time da je slučaj $n = 2$ trivijalan, dok je slučaj $n = 3$ znanost složeniji. Vrijedi $e_{\text{irr}}(2) = e(2) = 1$, te $e_{\text{irr}}(3) = e(3) = 2$.

U slučaju $n = 2$ je $P(x) = ax^2 + bx + c$, $\text{Disc}(P) = b^2 - 4ac$, $\text{sep}(P) = \sqrt{|\text{Disc}(P)|}/a$. Ako uzmemo npr. $a = k^2 + k - 1$, $b = 2k + 1$, $c = 1$, onda je $\text{Disc}(P) = 5$, pa je $\text{sep}(P) \ll H(P)^{-1}$.

Godine 1982., Mignotte je dao familiju polinoma $X^n - 2(aX - 1)^2$, za proizvoljne cijele brojeve $n \geq 3$ i $a \geq 2$ s vrlo dobrim separacijskim svojstvima (koeficijent 2 osigurava ireducibilnost polinoma prema Eisensteinovom kriteriju). Naime, ovi polinomi imaju dva korijena jako bliska a^{-1}. Naime, iz $P(a^{-1} + \varepsilon) \approx a^{-n} - 2a^2\varepsilon^2$, vidimo da $P(x)$ ima korijene približno jednake

$$a^{-1} \pm a^{(-n-2)/2}/\sqrt{2}.$$

Budući da je $H(P) = 2a^2$, pustimo li a u beskonačno, dobivamo $\text{sep}(P) \ll H(P)^{-(n+2)/4}$, tj.

$$e(n) \geq e_{\text{irr}}(n) \geq (n+2)/4.$$

U međuvremenu je bilo nekoliko poboljšanja Mignotteovog rezultata, no pitanje koji je eksponent najbolji mogući i dalje je otvoreno.

Primjer 5.1. Neka je α algebarski broj trećeg stupnja, te $Q(x)$ njegov minimalni polinom. Prema Davenport-Schmidtovom teoremu (Teorem 5.1) postoji beskonačno mnogo algebarskih brojeva β stupnja ≤ 2 sa svojstvom da je $|\alpha - \beta| \ll H(\beta)^{-3}$. Neka je $R(x)$ minimalni polinom od β. Promotrimo polinom $P(x) = Q(x)R(x)$. On ima korijene α i β, te vrijedi $H(P) \ll H(R) = H(\beta)$ (jer je α fiksan). Možemo pretpostaviti da je stupnja od $P(x)$ jednak 5 (po pretrebi ga pomnočzimo s linearnim faktorom). Stoga zaključujemo da je $e(5) \geq 3$.

Primjer 5.2 (Bugeaud & Dujella, 2011)**.** Za $a \geq 1$, korijeni polinoma

$$P_{4,a}(x) = (20a^4 - 2)x^4 + (16a^5 + 4a)x^3 + (16a^6 + 4a^2)x^2 + 8a^3x + 1,$$

su približno jednaki

$$\begin{aligned}
r_1 &= -1/4a^{-3} - 1/32a^{-7} - 1/256a^{-13} + \ldots,\\
r_2 &= -1/4a^{-3} - 1/32a^{-7} + 1/256a^{-13} + \ldots,\\
r_3 &= -2/5a + 11/100a^{-3} + 69/4000a^{-7} + 4/5a\,i + \ldots,\\
r_4 &= -2/5a + 11/100a^{-3} + 69/4000a^{-7} - 4/5a\,i + \ldots.
\end{aligned}$$

Vrijedi: $H(P_{4,a}) = O(a^6)$, $\operatorname{sep}(P_{4,a}) = |r_1 - r_2| = O(a^{-13})$. Nadalje, primjenom Eisensteinovog kriterija na recipročni polinom $x^4 P_{4,a}(1/x)$, zaključujemo da je polinom $P(x)$ ireducibilan. Pa kad pustimo a u beskonačno, dobivamo $e(4) \geq e_{\text{irr}}(4) \geq 13/6$.

Familije polinoma iz prethodnog primjera mogu se poopćiti na proizvoljni stupanj (u konstrukciji polinoma $P_{n,a}$ koriste se Catalanovi brojevi). Tako su Bugeaud i Dujella dokazali sljedeću nejednakost

$$e_{\text{irr}}(n) \geq \frac{d}{2} + \frac{d-2}{4(d-1)}.$$