Padeovi aproksimanti i diofantske aproksimacije

Maršić, Ivana

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Ivana Maršić

PADÉOVI APROKSIMANTI I DIOFANTSKE APROKSIMACIJE

Diplomski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, srpanj 2014.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Zahvaljujem svom mentoru prof. dr. sc. Andreju Dujelli na podršci i pomoći pri izradi ovog diplomskog rada. Također zahvaljujem svojim roditeljima i suprugu Jerku Maršiću na strpljenju, podršci i brizi. Rad posvećujem sinovima Mateju i Tinu.

Sadržaj

Uvod

U ovom radu ćemo promatrati Padéove aproksimante i diofantske aproksimacije. U prvom poglavlju dokazat ćemo da su brojevi oblika $\sqrt{d}$ te brojevi e i π iracionalni, kao i vrijednosti Tschakaloffovih funkcija. Kroz četiri dokaza otkrit ćemo pojam diofanskih aproksimacija i povezati ih s problemima iracionalnosti.
U drugom poglavlju definirat ćemo Padéove aproksimante analitičke funkcije u okolini nule, pozvat ćemo se na svojstva Gaussove hipergeometrijske funkcije, što nam dozvoljava da računamo Padéove tablice binomne funkcije $f(x) = (1-x)^{\alpha}, \alpha \in \mathbb{Z}$. Odavde dobivamo Padéove aproksimante eksponencijalne funkcije putem konfluentnih hipergeometrijskih funkcija. Na kraju drugog poglavlja, pokazat ćemo kako Padéovi aproksimanti doprinose dobroj diofantskoj aproksimaciji i rezultatima o iracionalnosti.
U trećem poglavlju, poopćit ćemo pojam racionalnih i kvadratnih brojeva defininirajući algebarske brojeve. Zatim ćemo pokazati osnovna svojstva algebarskih cijelih brojeva. Treći odjeljak trećeg poglavlja je posvećen dokazu slavnog Liouvilleovog teorema, koji ističe postojanje transcendentnih brojeva. Zapravo, Liouvilleov teorem osigurava takozvane mjere iracionalnosti za svaki algebarski broj. Proučavat ćemo ovaj pojam mnogo detaljnije u odjeljku 3.4 i pokazat da dobra diofantska aproksimacija omogućava dobijanje mjere iracionalnosti za specifične brojeve, na primjer za broj e. U odjeljku 3.5, objasnit ćemo kako poznavanje mjere iracionalnosti od $\sqrt[n]{d}$ omogućava rješavanje diofantske jednadžbe $x^n - dy^n = k$ $(n \geq 3)$. Na kraju, iskazat ćemo bez dokaza Thueov i Rothov teorem, koji poboljšavaju Liouvilleov teorem.

Poglavlje 1

Iracionalnost i diofantske aproksimacije

U ovom poglavlju, dokazat ćemo da su brojevi oblika $\sqrt{d}$, e i π iracionalni, kao i vrijednosti Tschakaloffovih funkcija. Sljedeća četiri dokaza dopuštaju nam da otkrijemo pojam diofanskih aproksimacija i da ih povežemo s problemima iracionalnosti.

1.1 Iracionalnost od $\sqrt{d}$

Teorem 1.1. *Neka je $d \in \mathbb{N}$. Pretpostavimo da d nije potpun kvadrat. Tada je $\sqrt{d}$ iracionalan.*

Dokaz. Pretpostavimo suprotno da je $\sqrt{d}$ racionalan broj. Tada je $\sqrt{d} = a/b$, gdje su a i b relativno prosti. Kvadriranjem jednakosti dobivamo $b^2 d = a^2$. Ako d nije potpun kvadrat, tada postoji prost broj p i cijeli broj k takav da je $d = p^{2k+1}\delta$, uz $p \nmid \delta$. Tada $p^{2k+1} | a^2$ i stoga $p^{k+1} | a$, pa je $a = p^{k+1}\alpha$. Otuda $b^2\delta = p\alpha^2$. Prosti broj p dijeli $b^2\delta$, ali ne dijeli δ. Stoga $p | b^2$, odakle slijedi $p | b$. Vidimo da $p | a$ i $p | b$, što je kontradikcija jer su brojevi a i b relativno prosti brojevi. Time je teorem dokazan. □

Korolar 1.2. *Ako $d \in \mathbb{N}$ nije potpun kvadrat, brojevi 1 i $\sqrt{d}$ su linearno nezavisni na $\mathbb{Q}$. Drugim riječima, ako su $p, q \in \mathbb{Q}$ i $p + q\sqrt{d} = 0$, tada je $p = q = 0$.*

Dokaz. Ako je q različit od nule, jednadžba $p + q\sqrt{d} = 0$ bi podrazumijevala da je $\sqrt{d} = -p/q \in \mathbb{Q}$, imamo kontradikciju sa teoremom 1.1. Stoga $q = 0$ i $p = 0$. □

1.2 Iracionalnost od e

Teorem 1.3. *e je iracionalan.*

Dokaz. Za svaki prirodni broj n, možemo pisati

$$e = \sum_{k=0}^{n} \frac{1}{k!} + R_n, \qquad \text{uz} \quad R_n = \sum_{k=n+1}^{+\infty} \frac{1}{k!}. \tag{1.1}$$

Jasno je da je $R_n > 0$. Štoviše,

$$R_n = \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \frac{1}{(n+3)!} + \dots$$

$$R_n = \frac{1}{(n+1)!}\left(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \frac{1}{(n+2)(n+3)(n+4)} + \dots\right)$$

$$R_n < \frac{1}{(n+1)!}\left(1 + \frac{1}{2} + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^3 + \dots\right) = \frac{2}{(n+1)!}.$$

Stoga (1.1) povlači

$$0 < n!e - n!\sum_{k=0}^{n} \frac{1}{k!} < \frac{2}{(n+1)!}. \tag{1.2}$$

Pretpostavimo suprotno, neka je $e = a/b$, gdje su a i b prirodni brojevi. Označimo $\alpha_n = n!\sum_{k=0}^{n} \frac{1}{k!}$. Tada $\alpha_n \in \mathbb{N}$ i (1.2) povlače $0 < n!a - b\alpha_n < \frac{2b}{n+1}$.

Što implicira da cijeli broj $\beta_n = n!a - b\alpha_n$ nije nula i isčezava kad n teži ka beskonačnosti. Ovo je nemoguće, jer *apsolutna vrijednost ne nul cijelog broja uvijek je veća ili jednaka* 1. Ovim je teorem dokazan. □

1.3 Iracionalnost od π

Teorem 1.4. *π je iracionalan.*

Dokaz. Neka je $P(x)$ bilo koji polinom stupnja $2n$. Stavimo

$$F(x) = P(x) - P''(x) + P^{(4)}(x) - \cdots + (-1)^n P^{(2n)}(x).$$

Uočavamo da je $P(x)\sin x = (F'(x)\sin x - F(x)\cos x)'$. Što daje *Hermitovu formulu*:

$$\int_0^\pi P(x)\sin x \mathrm{d}x = F(0) + F(\pi). \tag{1.3}$$

Pretpostavimo da je $\pi = \frac{a}{b}$, $a, b \in \mathbb{N}$, te primijenimo Hermitovu formulu s

$$P(x) = \frac{1}{n!}x^n(a - bx)^n.$$

Označimo $I_n = \int_0^\pi P(x)\sin x \,\mathrm{dx}$.
Tada $I_n > 0$ zato jer je $P(x)\sin x$ neprekidna, nenegativna i različita od nul funkcije na intervalu $[0, \pi]$. Štoviše, $x(a - bx) \leq a^2/4b$ na $[0, \pi]$, odakle $I_n \leq \frac{1}{n!}\pi\left(\frac{a^2}{4b}\right)^n$.
Stoga $\lim_{n\to+\infty} I_n = 0$.

Napomena 1.5. *Vrijedi $P(0) = P'(0) = \ldots = P^{(n-1)}(0) = 0$ te $F(0) \in \mathbb{Z}$ i $F(\pi) \in \mathbb{Z}$.*

Dokaz. Budući da je 0 višestruka nultočka kratnosti n od P, imamo $P(0) = P'(0) = \ldots = P^{(n-1)}(0) = 0$. Za $k \geq n$, konstantan član od $P^{(k)}(x)$ je $P^{(k)}(0) = \frac{k!}{n!}\binom{n}{k-n}a^{2n-k}(-b)^{k-n}$, što je jednako k-toj derivaciji člana stupnja k od $P(x)$, što je dano razvojem od $(a - bx)^n$. Budući da je $k \geq n$, $n!/k!$, odakle $P^{(k)}(0) \in \mathbb{Z}$ za svaki $k \geq n$. Stoga je $F(0) \in \mathbb{Z}$ za svaki $n \in \mathbb{N}$. Slično, $F(\pi) \in \mathbb{Z}$ i $F(0) + F(\pi)$ je cijeli broj. □

Prema tome $I_n \in \mathbb{Z}$, za svaki $n \in \mathbb{N}$. Stoga *pozitivan* niz cijelih brojeva I_n isčezava u beskonačnosti, što je nemoguće. Dakle π je iracionalan. □

1.4 Iracionalnost vrijednosti Tschakaloffove funkcije

Neka je $q \in \mathbb{C}$, $q > 1$. *Tschakaloffova funkcija* je definirana s

$$T_q(x) = \sum_{n=0}^{+\infty} \frac{x^n}{q^{\frac{n(n+1)}{2}}}, \qquad \forall x \in \mathbb{C}. \tag{1.4}$$

Ona zadovoljava funkcionalnu jednadžbu

$$T_q(qx) = 1 + xT_q(x). \tag{1.5}$$

Dokazat ćemo sljedeći rezultat.

Teorem 1.6. *Neka je $q \in \mathbb{Z}$, $|q| \geq 2$. Tada je $T_q(x)$ iracionalan za svaki $x \in \mathbb{Q}^*$.*

Trebamo sljedeću lemu, koja će također biti potrebna u proučavanju Padéovih aproksimacija.

Lema 1.7. *Neka je $\mathbb{K}$ bilo koje potpolje od $\mathbb{C}$, i neka je $f(x) = \sum_{n=0}^{+\infty} a_n x^n$, uz $a_n \in \mathbb{K}$ za svaki $n \in \mathbb{N}$ i radijus konvergencije $R > 0$. Pretpostavimo da su p, q i r tri prirodna broja koja zadovoljavaju $p < r \leq p + q + 1$. Tada postoje $P, Q \in \mathbb{K}[x]$, $Q \neq 0$, i red $g(x) = \sum_{n=0}^{+\infty} b_n x^n$, $|x| < R$, takav da je* $\deg P \leq p$, $\deg Q \leq q$ *i*

$$Q(x)f(x) + P(x) = x^r g(x). \tag{1.6}$$

Dokaz. Tražimo da su $Q(x) = \sum_{i=0}^{q} \alpha_i x^i$ i $P(x) = \sum_{i=0}^{p} \beta_i x^i$. Razvijemo $Q(x)f(x) + P(x)$ i poredamo ih prema potencijama od x. Budući da članovi stupnja $0, 1, \ldots, r-1$ trebaju iščeznuti, vidimo da α-e i β-e moraju zadovoljiti sustav

$$\begin{cases} a_0\alpha_0 + \beta_0 = 0 \\ a_0\alpha_0 + a_0\alpha_1 + \beta_1 = 0 \\ \vdots \\ a_{r-1}\alpha_0 + a_{r-2}\alpha_1 + \ldots = 0 \end{cases}$$

Ovo je sustav s $p + q + 2$ nepoznanice i r jednadžbi. Budući da je $p + q + 2 > r$, sustav ima ne-nul rješenje $(\alpha_0, \alpha_1, \ldots \alpha_q, \beta_0, \beta_1 \ldots, \beta_p)$. Ako bi svi α_i bili jednaki nula, imali bi $P \neq 0$ i $P(x) = x^r g(x)$, što je nemoguće jer je $r > p$. Stoga $Q \neq 0$ kao što smo i tvrdili. □

Sada ćemo dokazati teorem 1.6.
Neka je $x = \alpha/\beta$, $(\alpha, \beta) \in \mathbb{Z}^2$. Pretpostavimo da je $T_q(x) = \mu/\nu, (\mu, \nu) \in \mathbb{Z}^2$. Jednostavnom matematičkom indukcijom, koristeći funkcijsku jednadžbu (1.5) pokazuje se da je $T_q\left(\frac{x}{q^n}\right) = \frac{A_n}{\nu\alpha^n}$ za svaki $n \in \mathbb{N}$, gdje je $A_n \in \mathbb{Z}$.
Neka je ρ *fiksni cijeli broj*, takav da $|\alpha/q^\rho| < 1$.
Upotrebljavamo lemu 1.6 uz $\mathbb{K} = \mathbb{Q}$, $f(x) = T_q(x)$, $p = q = 2\rho$, $r = 3\rho$. Tada polinomi P i Q imaju *racionalne* koeficijente. Međutim, ako pomnožimo (1.6) sa najmanjim zajedničkim višekratnikom ovih koeficijenata, vidimo da možemo pretpostaviti da P i Q imaju *cjelobrojne* koeficijente. Dakle, možemo pisati

$$Q(x)T_q(x) + P(x) = x^{3\rho}g(x), \tag{1.7}$$

gdje su $P, Q \in \mathbb{Z}[x]$, $\deg Q \leq 2\rho$, $\deg P \leq 2\rho$, $Q \neq 0$.
Ali g nije jednak nuli; kad bi to bio slučaj, T_q bi bio racionalni razlomak zbog (1.7), i stoga je polinom jer je definiran na $\mathbb{C}$, što je nemoguće uzevši u obzir Taylorov razvoj (1.4). Stoga barem jedan Taylorov koeficijent od g nije nula. Dakle, postoji cijeli broj $\sigma \geq 0$ i funkcija h takva da je

$$Q(x)T_q(x) + P(x) = x^{3\rho+\sigma}h(x), \qquad h(0) \neq 0. \tag{1.8}$$

Zamjenimo $x = \alpha/\beta$ sa x/q^n u (1.8), pomnožimo sa $\nu\alpha^n\beta^{2\rho}q^{2\rho n}$ i označimo s B_n zajedničku vrijednost obiju strana jednadžbi

$$\begin{aligned} B_n &= \frac{\nu\alpha^{3\rho+\sigma}}{\beta^{\rho+\sigma}}\left(\frac{\alpha}{q^{\rho+\sigma}}\right)^n h\left(\frac{\alpha}{\beta q^n}\right) \\ &= \left(\beta^{2\rho}q^{2\rho n}Q\left(\frac{\alpha}{\beta q^n}\right)\right)\left(\nu\alpha^n T_q\left(\frac{\alpha}{\beta q^n}\right)\right) + \nu\alpha^n\left(\beta^{2\rho}q^{2\rho n}P\left(\frac{\alpha}{\beta q^n}\right)\right). \end{aligned} \tag{1.9}$$

Zato što su $\left(\beta^{2\rho}q^{2\rho n}P\left(\frac{\alpha}{\beta q^n}\right)\right)$, $\nu\alpha^n T_q\left(\frac{\alpha}{\beta q^n}\right)$, i $\left(\beta^{2\rho}q^{2\rho n}Q\left(\frac{\alpha}{\beta q^n}\right)\right) \in \mathbb{Z}$, vidimo da je $B_n \in \mathbb{Z}$. Štoviše, $B_n \sim \frac{\nu\alpha^{3\rho+\sigma}}{\beta^{\rho+\sigma}}\left(\frac{\alpha}{q^{\rho+\sigma}}\right)^n h(0)$, što implicira da je $\lim_{n\to+\infty} B_n = 0$ jer je $|\alpha/q^\rho| < 1$ te također $B_n \neq 0$ kao i $\alpha \neq 0$ te $h(0) \neq 0$. Ponovno, konstruirali smo niz ne nul cijelih brojeva koji isčezavaju u beskonačnosti. Time je dokazan teorem 1.6.

1.5 Diofantske aproksimacije

Konstruirati *diofantsku aproksimaciju* za zadani realni broj α znači pronaći niz racionalnih brojeva P_n/Q_n i funkciju f koja teži u beskonačnost, tako da vrijedi

$$\left|\alpha - \frac{P_n}{Q_n}\right| \leq f(Q_n), \qquad \forall n \in \mathbb{N}. \tag{1.10}$$

Napomenimo da smo dokazali iracionalnost brojeva e i $T_q(\alpha/\beta)$ koristeći diofantske aproksimacije.
Zaista, u slučaju broja e, možemo pisati (1.2) kao

$$0 < e - \frac{P_n}{Q_n} < \frac{2}{(n+1)Q_n} \leq \frac{2}{Q_n}, \tag{1.11}$$

gdje je $P_n = n! \sum_{k=0}^{n} \frac{1}{k!}$ i $Q_n = n!$.
U slučaju $T_q(\alpha, \beta)$ nije tako jasno. Moramo uočiti da je

$$T_q\left(\frac{\alpha}{\beta q^n}\right) = \frac{k_n}{\alpha^n} T_q\left(\frac{\alpha}{\beta}\right) + \frac{\ell_n}{\alpha^n},$$

gdje su $(k_n, \ell_n) \in \mathbb{Z}^2$ (indukcija pomoću (1.5)). Stoga (1.9) povlači

$$T_q\left(\frac{\alpha}{\beta}\right) + \frac{P_n}{Q_n} \leq \frac{c}{Q_n}\left(\frac{\alpha}{q^{\rho+\sigma}}\right)^n \leq \frac{c}{Q_n} \tag{1.12}$$

uz $Q_n = k_n \beta^{2\rho} q^{2\rho n} Q(\alpha/\beta q^n)$, $P_n = \alpha^n \beta^{2\rho} q^{2\rho n} P(\alpha/\beta q^n) + \ell_n Q_n/k_n$,
i $c = max_{n\in\mathbb{N}} \alpha^{3\rho+\sigma} \beta^{-\rho-\sigma} h\left(\alpha\beta^{-1} q^{-n}\right)$.
Razlika između e i $T_q(\alpha/\beta)$ je u činjenici da je diofantska aproksimacija dana jednadžbom (1.11) je eksplicitna (mogu se računati eksplicitno P_n i Q_n kao funkcije u n) dok ona dana u (1.12) nije. U zadnjem slučaju, P_n i Q_n su izražene pomoću polinoma P i Q, a lema 1.7 tvrdi *postojanje* ovih polinoma, ali ne daje način izračunavanja.
Međutim, u oba slučaja, dobivamo iracionalni rezultat, jer nakon množenja sa Q_n, produkt $Q_n f(Q_n)$ teži u beskonačnost. Kažemo da smo dobili *dobru diofantsku aproksimaciju* i možemo iskazati sljedeći rezultat.

Teorem 1.8. *Neka je $\alpha \in \mathbb{R}$. Pretpostavimo da postoji niz P_n/Q_n racionalnih brojeva koji zadovoljava*

$$\forall n \in \mathbb{N}, \qquad 0 < \left|\alpha - \frac{P_n}{Q_n}\right| \leq \frac{\varepsilon(n)}{Q_n}, \quad \text{uz } \lim_{n\to+\infty} \varepsilon(n) = 0.$$

Tada je α iracionalan.

Dokaz. Pretpostavimo da je $\alpha = a/b$, uz $a \in \mathbb{Z}$, $b \in \mathbb{Z}$. Tada

$$0 < |\alpha - p_n/q_n| \leq \varepsilon(n)/q_n \;\Rightarrow\; 0 < |aq_n - bp_n| \leq b\varepsilon(n).$$

Stoga $\lim_{n\to+\infty} |aq_n - bp_n| = 0$. Međutim, $|aq_n - bp_n| \in \mathbb{N}$, a niz pozitivnih cijelih brojeva ne može težiti ka 0, budući da nije manji od 1. Ovo dokazuje da je α iracionalan. □

Sljedeći teorem je dokazao Dirichlet (1805-1859). Pokazuje da, za dani iracionalni broj α, postoje dobre diofantske aproksimacije.

Teorem 1.9. *Neka je $\alpha \in R$. Pretpostavimo da je α iracionalan. Tada postoji beskonačan niz racionalnih brojeva P_n/Q_n koji zadovoljava*

$$0 < \left|\alpha - \frac{P_n}{Q_n}\right| \leq \frac{1}{Q_n^2}, \qquad \forall n \in \mathbb{N}.$$

Za dokaz teorema trebat će nam sljedeća lema.

Lema 1.10. *Pretpostavimo da je α iracionalan. Tada za svaki cijeli broj $Q > 1$, možemo naći $p/q \in \mathbb{Q}$ takav da $1 \leq q < Q$ i $0 < |q\alpha - p| \leq \frac{1}{Q}$.*

Dokaz Leme 1.10. Označimo sa $[\alpha]$ cijeli dio od α i promotrimo $Q+1$ brojeva
$0,\ 1,\ \alpha - [\alpha],\ 2\alpha - [\alpha],\ \ldots,\ (Q-1)\,\alpha - [(Q-1)\,\alpha]$.
Svi ovi brojevi pripradaju intervalu $[0,1]$, i svi su oblika $a\alpha + b$, a i b su cijeli brojevi, $0 \leq a \leq Q-1$. Sada ćemo koristiti *Dirichletov princip*. Dijelimo interval $[0,1]$ u Q podintervala, dakle $[0, 1/Q]$, $[1/Q, 2/Q]$, $\ldots$, $[(Q-1)/Q, 1]$. Tada barem dva od gore $Q+1$ brojeva pripadaju *istom* podintervalu (pokušajmo staviti $Q+1$ brojeva u Q intervala). Označimo ova dva broja sa $\xi_1 = a_1\alpha + b_1$ i $\xi_2 = a_2\alpha + b_2$, uz $0 \leq a_1 \leq Q-1$, $0 \leq a_2 \leq Q-1$ te $a_1 \neq a_2$ (zato što $a_1 = a_2$ implicira $a_1 = a_2 = 0$ što daje $\xi_1 = 0$ i $\xi_2 = 1$, što je nemoguće). Možemo pretpostaviti da je $a_1 > a_2$. Prema izboru ξ_1 i ξ_2, $|\xi_1 - \xi_2| = |(a_1 - a_2)\,\alpha + b_1 - b_2| \leq 1/Q$, uz $0 < a_1 - a_2 \leq Q-1$, što dokazuje lemu. □

Sada dokazujemo teorem 1.9 matematičkom indukcijom. Izaberemo proizvoljan cijeli broj $Q > 1$. Prema prethodnoj lemi možemo naći racionalni broj P_1/Q_1 takav da $0 < |\alpha - P_1/Q_1| \leq 1/QQ_1$ i $1 \leq Q_1 < Q$. Stoga $0 < |\alpha - P_1/Q_1| < 1/Q_1^2$.
Sada opet koristimo lemu odabirući Q takav da $Q^{-1} < |\alpha - P_1/Q_1|$.
Možemo pronaći racionalni broj P_2/Q_2 koji zadovoljava $1 \leq Q_2 < Q$ i $0 < |\alpha - P_2/Q_2| \leq 1/QQ_2 < 1/Q_2^2$. Štoviše,

$$\left|\frac{P_1}{Q_1} - \frac{P_2}{Q_2}\right| \geq \left\|\alpha - \frac{P_2}{Q_2}\right| - \left|\alpha - \frac{P_1}{Q_1}\right\| \neq 0$$

pošto je $|\alpha - P_1/Q_1| > 1/Q$ i $|\alpha - P_2/Q_2| \leq 1/QQ_2 \leq 1/Q$.
Indukcijom dobivamo beskonačan niz racionalnih brojeva P_n/Q_n koji zadovoljavaju $|\alpha - P_n/Q_n| < 1/Q_n^2$, što dokazuje teorem.

Napomena 1.11. *Teorem 1.9 tvrdi postojanje niza P_n/Q_n, ali ne daje način kako ga izračunati. Teorija verižnih razlomaka (formula $\left|\alpha_0 - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n^2}$) omogućit će nam eksplicitni rezultat.*

Poglavlje 2

Padéovi aproksimanti

U uvodnom odjeljku definirat ćemo Padéove aproksimante analitičke funkcije u okolini nule i dokazat ćemo lemu 2.1 koja je temeljna za diofantske aproksimacije. U drugom odjeljku pozvat ćemo se na svojstva Gaussove hipergeometrijske funkcije, što nam dozvoljava da računamo Padéove tablice binomne funkcije $f(x) = (1-x)^{\alpha}, \alpha \notin \mathbb{Z}$. Odavde dobivamo Padéove aproksimante eksponencijalne funkcije putem konfluentnih hipergeometrijskih funkcija (treći odjeljak). Na kraju, u četvrtom odjeljku pokazat ćemo kako Padéovi aproksimanti doprinose dobroj diofantskoj aproksimaciji i rezultatima o iracionalnosti.

2.1 Uvod

Definicija 2.1. *Neka je* $f(x) = \sum_{k=0}^{+\infty} a_k x^k \quad (|x| < R)$ *analitička u okolini od* 0. *Neka* $(m,n) \in \mathbb{N}^2$. *Kažemo da je uređena trojka* $(Q_m, P_n, R_{m,n})$ *je* $[m/n]$ *Padéov aproksimant od* f *ako*

(a) Q_m *i* P_n *su polinomi koji zadovoljavaju* $deg Q_m \leq m,\ deg P_n \leq n$.

(b) $R_{m,n}(x) = \sum_{k=0}^{+\infty} b_k x^k \quad (|x| < R)$ *je analitička u okolini od 0.*

(c) $Q_m(x)f(x) + P_n(x) = x^{m+n+1} R_{m,n}(x) \qquad (|x| < R)$.

Postojanje Padéovih aproksimanata ja jednostavna posljedica leme 1.7. Treba napomenuti da parcijalna suma reda n od f, $S_n(x) = \sum_{k=0}^{n} a_k x^k$, je $[0/n]$ Padeov aproksimant od f,

jer je

$$1 \cdot f(x) - S_n(x) = x^{n+1} \sum_{k=0}^{+\infty} a_{n+k+1} x^k.$$

Nadalje, ako $(Q_m, P_n, R_{m,n})$ je $[m/n]$ Padéov aproksimant od f, isto vrijedi za $(\lambda Q_m, \lambda P_n, \lambda R_{m,n})$ za svaki $\lambda \in C$.
U teoriji brojeva, uglavnom ćemo koristiti *dijagonalne* Padéove aproksimante ($n = m$). U ovom slučaju označavamo $R_{n,n} = R_n$. Sljedeći rezultat je fundamentalan.

Lema 2.2. *Neka je (Q_n, P_n, R_n) niz dijagonalnih Padéovih aproksimanata od f. Pretpostavimo da je $Q_n(0) \neq 0$ i $R_n(0) \neq 0$ za svaki $n \in \mathbb{N}$.Tada za svaki $n \in \mathbb{N}$ vrijedi*

$$\begin{vmatrix} Q_n(x) & P_n(x) \\ Q_{n+1}(x) & P_{n+1}(x) \end{vmatrix} = c_n x^{2n+1}, \text{ uz } c_n \neq 0.$$

Dokaz. Imamo da je $Q_n(x)f(x) + P_n(x) = x^{2x+1}R_n(x)$ odakle

$$\begin{vmatrix} Q_n(x) & P_n(x) \\ Q_{n+1}(x) & P_{n+1}(x) \end{vmatrix} = \begin{vmatrix} Q_n(x) & P_n(x) + Q_n(x)f(x) \\ Q_{n+1}(x) & P_{n+1}(x) + Q_{n+1}(x)f(x) \end{vmatrix}$$

$$= \begin{vmatrix} Q_n(x) & x^{2n+1}R_n(x) \\ Q_{n+1}(x) & x^{2n+3}R_{n+1}(x) \end{vmatrix} = x^{2n+1}\left(-Q_{n+1}(x)R_n(x) + x^2 Q_n(x)R_{n+1}(x)\right).$$

Stoga

$$\begin{vmatrix} Q_n(x) & P_n(x) \\ Q_{n+1}(x) & P_{n+1}(x) \end{vmatrix} = x^{2n+1}\left(-Q_{n+1}(0)R_n(0) + \sum_{k=1}^{+\infty} b_k x^k\right). \tag{2.1}$$

Sada, lijeva strana od (2.1) je *polinom* stupnja $\leq 2n + 1$, odakle $b_k = 0$ za svaki $k \geq 1$, i $c_n = -Q_{n+1}(0)R_n(0) \neq 0$. □

2.2 Gaussova hipergeometrijska funkcija i Padéovi aproksimanti binomne funkcije

Za svaki kompleksni broj a, označavamo

$$\begin{cases} (a)_0 = 1 \\ (a)_n = a(a+1)\dots(a+n-1) \qquad \text{za } n \geq 1 \end{cases} \tag{2.2}$$

te definiramo, za $|x| < 1$, *hipergeometrijsku funkciju* ${}_2F_1$ s

$${}_2F_1\left(\begin{matrix} a, b \\ c \end{matrix}\middle| x\right) = \sum_{n=1}^{+\infty} \frac{(a)_n (b)_n}{(c)_n \, n!} x^n. \tag{2.3}$$

Primjer 2.3. *Za $a = b = c = 1$, dobivamo geometrijski red:*

$$ {}_2F_1\left(\begin{matrix}1,1\\1\end{matrix}\middle| x\right) = \sum_{n=0}^{+\infty} x^n = \frac{1}{1-x}. $$

Primjer 2.4. *Za $a = -\alpha,\ b = c$, dobivamo binomni red:*

$$ {}_2F_1\left(\begin{matrix}-a,b\\b\end{matrix}\middle| x\right) = \sum_{n=0}^{+\infty} \frac{(-\alpha)(-\alpha+1)\dots(-\alpha+n-1)}{n!}\, x^n = (1-x)^{\alpha}. $$

Napomena 2.5. *Jasno je da moramo pretpostaviti da je $c \neq 0, -1, -2\dots$ u (2.3). Međutim, ako je $a \in \mathbb{Z}_-$, tada je ${}_2F_1\left(\begin{matrix}a,b\\c\end{matrix}\middle| x\right)$ polinom stupnja $-a$. U ovom slučaju, c može biti negativni cijeli broj, pod pretpostavkom da je $c < a$. Zaista, u ovom slučaju $(c)_n$ isčezava nakon $(a)_n$. Otuda, ako su a i c negativni cijeli brojevi, uz $c < a$, tada ${}_2F_1\left(\begin{matrix}a,b\\c\end{matrix}\middle| x\right)$ je polinom stupnja $-a$.*

Teorem 2.6. *Hipogeometrijska funkcija ${}_2F_1\left(\begin{matrix}a,b\\c\end{matrix}\middle| x\right)$ zadovoljava diferencijalnu jednadžbu*

$$ x(1-x)y'' + (c - (a+b+1)x)y' - aby = 0. \tag{2.4} $$

Štoviše, ako $c \notin \mathbb{Z}$, opće rješenje od (2.4) na $]0,1[$ je

$$ y = A\ {}_2F_1\left(\begin{matrix}a,b\\c\end{matrix}\middle| x\right) + Bx^{1-c}\ {}_2F_1\left(\begin{matrix}a-c+1,b-c+1\\2-c\end{matrix}\middle| x\right). \tag{2.5} $$

Teorem nećemo dokazivati.

Iz teorema 2.6 izvodimo zaključak

$$ {}_2F_1\left(\begin{matrix}a,b\\c\end{matrix}\middle| x\right)(1-x)^{a+b-c} =_2 F_1\left(\begin{matrix}c-a,c-b\\c\end{matrix}\middle| x\right). \tag{2.6} $$

Slijedeći samog Padéa (1900), upotrijebit ćemo ovu relaciju da nađemo Padéove aproksimante binomne funkcije $f(x) = (1-x)^a$.

Teorem 2.7. *Za svaki $\alpha \notin \mathbb{Z}$, $(m,n) \in \mathbb{N}^2$, $|x| < 1$,*

$$ \begin{aligned} &{}_2F_1\left(\begin{matrix}-m,-n+\alpha\\-m-n\end{matrix}\middle| x\right)(1-x)^{\alpha} - {}_2F_1\left(\begin{matrix}-n,-m-\alpha\\-m-n\end{matrix}\middle| x\right) \\ &= x^{m+n+1}\frac{(-1)^m(-m-\alpha)_{m+n+1}}{\binom{m+n}{m}(m+n+1)!}\ {}_2F_1\left(\begin{matrix}n+1-\alpha,m+1\\m+n+2\end{matrix}\middle| x\right). \end{aligned} $$

Dokaz. Neka je $\varepsilon \in \left[-\frac{1}{2}, \frac{1}{2}\right]$. U relaciji (2.6) uzimamo $a = -m$, $b = -(n+\varepsilon)+\alpha$ i $c = -m-(n+\varepsilon)$. Dobivamo

$$ {}_2F_1\left(\begin{matrix}-m, -(n+\varepsilon)+\alpha \\ -m-(n+\varepsilon)\end{matrix}\middle| x\right)(1-x)^{\alpha} = {}_2F_1\left(\begin{matrix}-(n+\varepsilon), -m-\alpha \\ -m-(n+\varepsilon)\end{matrix}\middle| x\right). \tag{2.7} $$

Hipergeometrijski red na lijevoj strani jednadžbe u (2.7) je polinom stupnja m. Kada $\varepsilon \to 0$, on teži ka ${}_2F_1\left(\begin{matrix}-m, -n+\alpha \\ -m-n\end{matrix}\middle| x\right)$.
S druge strane, hipergeometrijski red na desnoj strani se može zapisati

$$ \begin{aligned} {}_2F_1\left(\begin{matrix}-(n+\varepsilon), -m-\alpha \\ -m-(n+\varepsilon)\end{matrix}\middle| x\right) &= \sum_{k=0}^{n} \frac{(-(n+\varepsilon))_k\,(-m-\alpha)_k}{(-m-(n+\varepsilon))_k \cdot k!}x^k + \sum_{k=n+1}^{m+n} \frac{(-(n+\varepsilon))_k\,(-m-\alpha)_k}{(-m-(n+\varepsilon))_k \cdot k!}x^k \\ &+ \sum_{k=m+n+1}^{+\infty} \frac{(-(n+\varepsilon))_k\,(-m-\alpha)}{(-m-(n+\varepsilon))_k \cdot k!}x^k. \end{aligned} \tag{2.8} $$

Kada $\varepsilon \to 0$, prva suma teži ka ${}_2F_1\left(\begin{matrix}-n, -m+\alpha \\ -m-n\end{matrix}\middle| x\right)$. Nadalje, druga suma teži prema nuli, dok $(-n-\varepsilon)_k = (-n-\varepsilon)(-n-\varepsilon+1)\ldots(-n-\varepsilon+k-1)$ sadrži jedan faktor ε kada $n+1 \le k \le m+n$.
Neka $g(x)$ bude treća suma. Najprije ćemo promatrati
$(-n-\varepsilon)_k = [(-n-\varepsilon)\ldots(-\varepsilon)] \times [(-\varepsilon+1)\ldots(-\varepsilon+m)]$
$\quad \times [(-\varepsilon+m+1)\ldots(-\varepsilon+m+1+(k-m-n-1)-1)]$,
$(-m-n-\varepsilon)_k = [(-m-n-\varepsilon)\ldots(-n-1-\varepsilon)] \times [(-n-\varepsilon)\ldots(-\varepsilon)]$
$\quad \times [(-\varepsilon+1)\ldots(-\varepsilon+1+(k-m-n-1)-1)]$,
$(-m-\alpha)_k = [(-m-\alpha)\ldots(n-\alpha)]$
$\quad \times [(n+1-\alpha)\ldots(n+1-\alpha+(k-m-n-1)-1)]$,
$k! = (m+n+1)![(m+n+2)\ldots(m+n+2+(k-m-n-1)-1)]$. Ali u svakom članu od $g(x)$, možemo pojednostaviti $(-n-\varepsilon)_k$ / $(-m-n-\varepsilon)_k$ uz
$[(-\varepsilon)(-\varepsilon-1)\ldots(-\varepsilon-n)]$. Faktorizacijom i stavljanjem $h = k-m-n-1$ dobivamo

$$ g(x) = \frac{[(-\varepsilon+1)\ldots(-\varepsilon+m)] \times [(-m-\alpha)\ldots(n-\alpha)]}{[(-m-n-\varepsilon)\ldots(-n-1-\varepsilon)] \times (m+n+1)!}x^{m+n+1} \times \sum_{h=0}^{+\infty} \frac{(-\varepsilon+m+1)_h\,(n+1-\alpha)_h}{(-\varepsilon+1)_h\,(m+n+2)_h}x^h. $$

Za fiksni $|x| < 1$, niz konvergira uniformno za $\varepsilon \in \left[-\frac{1}{2}, \frac{1}{2}\right]$. Stoga imamo

$$ \lim_{\varepsilon \to 0} g(x) = \frac{m!\,(-m-\alpha)\ldots(n-\alpha)}{(-m-n)\ldots(-n-1)\cdot(m+n+1)!}x^{m+n+1} \sum_{h=0}^{+\infty} \frac{(m+1)_h (n+1-\alpha)_h}{h!(m+n+2)_h}x^h. $$

Prema tome, kada pustimo $\varepsilon \to 0$ u (2.8), dobivamo teorem 2.7. □

2.3 Konfluentne hipergeometrijske funkcije i Padéovi aproksimanti eksponencijalne funkcije

Neka je $x \in \mathbb{C}$ i neka je $b \in \mathbb{R}$, uz $b > |x|$. Tada je

$$ {}_2F_1\left(\begin{matrix}a, b\\ c\end{matrix}\middle|\frac{x}{b}\right) = \sum_{n=0}^{+\infty} \frac{(a)_n}{(c)_n}\left(1+\frac{1}{b}\right)\left(1+\frac{2}{b}\right)\ldots\left(1+\frac{n-1}{b}\right)\frac{x^n}{n!}. $$

Za fiksni x, niz konvergira uniformno za $b \in]2\,|x|\,, +\infty[$, odakle

$$ \lim_{b\to+\infty} {}_2F_1\left(\begin{matrix}a, b\\ c\end{matrix}\middle|\frac{x}{b}\right) = \sum_{n=0}^{+\infty} \frac{(a)_n}{(c)_n}\frac{x^n}{n!}. $$

Ovu cijelu funkciju zovemo *konfluentna hipergeometrijska funkcija* i označavamo je

$$ {}_1F_1\left(\begin{matrix}a\\ c\end{matrix}\middle|x\right) = \sum_{n=0}^{+\infty} \frac{(a)_n}{(c)_n}\frac{x^n}{n!}. \tag{2.9} $$

Napomena 2.8. *Općenitije, opća hipergeometrijska funkcija je definirana za $q \geq p-1$ sa*

$$ {}_pF_q\left(\begin{matrix}a_1, a_2, \ldots, a_p\\ b_1, b_2, \ldots, b_q\end{matrix}\middle|x\right) = \sum_{n=0}^{+\infty} \frac{(a_1)_n(a_2)_n\ldots(a_p)_n}{(b_1)_n(b_2)_n\ldots(b_q)_n}\frac{x^n}{n!}. \tag{2.10} $$

Ovo objašnjava zapis za ${}_1F_1$ i ${}_2F_1$.

Teorem 2.9. *Konfluentna hipergeometrijska funkcija zadovoljava diferencijalnu jednadžbu*

$$ xy'' + (c-x)y' - ay = 0. \tag{2.11} $$

Štoviše, ako $c \notin \mathbb{Z}$, opće rješenje od (2.11) na $]0, +\infty[$ je

$$ y = A\ {}_1F_1\left(\begin{matrix}a\\ c\end{matrix}\middle|x\right) + Bx^{1-c}\ {}_1F_1\left(\begin{matrix}a-c+1\\ 2-c\end{matrix}\middle|x\right). \tag{2.12} $$

Kada je a negativan cijeli broj, ${}_1F_1\left(\begin{matrix}a\\ c\end{matrix}\middle|x\right)$ je polinom koji se može koristiti za iskazivanje Padéovih aproksimacija za eksponencijalnu funkciju.

Teorem 2.10. *Za svaki $(m, n) \in \mathbb{N}^2$ i svaki $x \in \mathbb{C}$,*

$$ {}_1F_1\left(\begin{matrix}-m\\ -m-n\end{matrix}\middle|-x\right)e^x - {}_1F_1\left(\begin{matrix}-n\\ -m-n\end{matrix}\middle|x\right) = \frac{(-1)^m x^{m+n+1}}{\binom{m+n}{m}(m+n+1)!}\ {}_1F_1\left(\begin{matrix}m+1\\ n+m+2\end{matrix}\middle|x\right). $$

Dokaz. U teoremu 2.7, zamijenimo x sa $-x/\alpha$. Prvo, znamo da je $\lim_{a\to+\infty}(1+x/\alpha)^{\alpha} = e^x$. S druge strane,

$$\lim_{\alpha\to+\infty} {}_2F_1\left(\begin{matrix}-m,-n+\alpha\\-m-n\end{matrix}\middle|-\tfrac{x}{\alpha}\right)$$

$$= \lim_{\alpha\to+\infty}\sum_{k=0}^{+\infty}\frac{(-m)_k}{(-m-n)_k}\left(1-\frac{n}{\alpha}\right)\ldots\left(1-\frac{n-k+1}{\alpha}\right)\frac{(-x)^k}{k!} = {}_1F_1\left(\begin{matrix}-m\\-m-n\end{matrix}\middle|-x\right).$$

Slično $\lim_{\alpha\to+\infty} {}_2F_1\left(\begin{matrix}-n,-m-\alpha\\-m-n\end{matrix}\middle|-\tfrac{x}{\alpha}\right) = {}_1F_1\left(\begin{matrix}-n\\-m-n\end{matrix}\middle|x\right)$.

I $\lim_{\alpha\to+\infty} {}_2F_1\left(\begin{matrix}n+1-\alpha,m+1\\m+n+2\end{matrix}\middle|-\tfrac{x}{\alpha}\right) = {}_1F_1\left(\begin{matrix}m+1\\m+n+2\end{matrix}\middle|x\right)$. □

Time je teorem dokazan.

2.4 Aritmetička primjena

U ovom odjeljku dokazat ćemo sljedeći rezultat.

Teorem 2.11. *Neka je* $\mathbb{K} = \mathbb{Q}\left(i\sqrt{d}\right)$ *imaginarno kvadratno polje. Neka je* $\alpha \in \mathbb{K}^*$. *Tada* $e^{\alpha} \notin \mathbb{K}$.

Posebno, ako je $\alpha \in \mathbb{Q}^*$, tada je e^{α} iracionalan. Druga zanimljiva posljedica teorema 2.11 je sljedeći korolar.

Korolar 2.12. *Neka je* $k \in \mathbb{N}^*$. *Tada je* $\pi\sqrt{k}$ *iracionalan.*

Dokaz. Zaista, zapišimo $\sqrt{k} = m\sqrt{d}$, gdje je d kvadratno slobodan i pretpostavimo da je $\pi\sqrt{k} \in \mathbb{Q}$. Tada $\alpha = \left(\pi\sqrt{k}\right) i\sqrt{k} \in \mathbb{Q}\left(i\sqrt{d}\right)$, te stoga teorem 2.11 povlači $e^{\alpha} = e^{ik\pi} = (-1)^k \notin \mathbb{Q}\left(i\sqrt{d}\right)$, što je kontradikcija. □

Dokaz teorema 2.11 počet ćemo od dijagonalnih Padéovih aproksimanata od e^x. Dobivamo ih tako što ćemo uzeti $m = n$ u teoremu 2.10:

$$ {}_1F_1\left(\begin{matrix}-n\\-2n\end{matrix}\middle|-x\right)e^x - {}_1F_1\left(\begin{matrix}-n\\-2n\end{matrix}\middle|x\right) = \frac{(-1)^n x^{2n+1}}{\binom{2n}{n}(2n+1)!}\,{}_1F_1\left(\begin{matrix}n+1\\2n+2\end{matrix}\middle|x\right). \tag{2.13}$$

Trebamo četiri leme:

Lema 2.13. *Neka je $\mathbb{A}_{\mathbb{K}}$ prsten cijelih brojeva imaginarnog kvadratnog polja $\mathbb{K} = \mathbb{Q}(i\sqrt{d})$. Neka je $(a)_n$ niz elemenata iz $\mathbb{A}_{\mathbb{K}}$ koji zadovoljavaju $lim_{n\to+\infty} a_n = 0$. Tada je $a_n = 0$ za svaki veliki n.*

Dokaz. U $\mathbb{A}_{\mathbb{K}}$, imamo $N(a_n) = |a_n|^2 \in \mathbb{Z}$. Stoga $lim_{n\to+\infty} a_n = 0 \Rightarrow N(a_n) = 0$ i $a_n = 0$ za svaki veliki n. □

Napomena 2.14. *Lema 2.13 omogućava nam upotrebu diofantskih aproksimacija u $\mathbb{A}_{\mathbb{K}}$ kao u skupu $\mathbb{Z}$. Treba primjetiti da ovo nije moguće ako je $\mathbb{K}$ realno kvadratno polje. Na primjer, ako su P_n/Q_n konvergente razvoja u verižni razlomak od $\sqrt{2}$, tada $\left|P_n - Q_n\sqrt{2}\right| \leq 1/Q_n$, prema formuli $\left|\alpha_0 - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n^2}$, odakle $\lim_{n\to+\infty}\left(P_n - Q_n\sqrt{2}\right) = 0$. Međutim $P_n - Q_n\sqrt{2}$ nije nikad nula, jer je $\sqrt{2}$ iracionalan.*

Lema 2.15. *Za $a,\ c \in \mathbb{R},\ c > a > 0$,*

$$ {}_1F_1\left(\begin{matrix}a\\c\end{matrix}\middle| x\right) = \frac{\Gamma(c)}{\Gamma(a)\Gamma(c-a)} \int_0^1 e^{xt} t^{a-1}(1-t)^{c-a-1} dt. $$

Lemu nećemo dokazivati.

Lema 2.16. *Za $\alpha \in \mathbb{C},\ a, c \in \mathbb{R}, c > a > 0$,*

$$ \left|{}_1F_1\left(\begin{matrix}a\\c\end{matrix}\middle| \alpha\right)\right| \leq Max\left(1, e^{Re\alpha}\right) \frac{\Gamma(c)}{\Gamma(a)\Gamma(c-a)}. $$

Dokaz. Prema lemi 2.15 dobivamo $\left|{}_1F_1\left(\begin{matrix}a\\c\end{matrix}\middle| \alpha\right)\right| \leq \frac{\Gamma(c)}{\Gamma(a)\Gamma(c-a)} \int_0^1 \left|e^{\alpha t}\right| dt.$

Sada $\left|e^{\alpha t}\right| = e^{tRe\ \alpha}$. Stoga, $e^{tRe\ \alpha} \leq 1$ ako je $Re\ \alpha \leq 0$ i $e^{tRe\ \alpha} \leq e^{Re\ \alpha}$ ako je $Re\ \alpha \geq 0$. Ovim je dokazana lema. □

Lema 2.17. *Za svaki $n \in \mathbb{Z}$ i svaki $k \in \mathbb{N}$, $\quad k!|(n)_k$, odakle $k!|n(n-1)\ldots(n-k+1)$.*

Dokaz. Ako je $n = -k+1,\ -k+2, \ldots, -1,\ 0$, tada $(n)_k = 0$ pa je rezultat očit.
Ako je $n > 0$, $\frac{(n)_k}{k!} = \frac{n(n+1)\ldots(n+k-1)}{k!} = \binom{n+k-1}{k} \in \mathbb{N}$.
Ako je $n \leq -k$, $\frac{(n)_k}{k!} = (-1)^k \frac{-n(-n-1)\ldots(-n-k+1)}{k!} = (-1)^k \binom{-n}{k} \in \mathbb{Z}$.
Napokon, $n(n-1)\ldots(n-k+1) = (-1)(-n)_k$. □

Sada ćemo nastaviti dokazivati teorem 2.11.

Neka je $\alpha \in \mathbb{Q}(i\sqrt{d})$. Pišemo $\alpha = \left(a + ib\sqrt{d}\right)/\delta = \beta/\delta$, uz $(a, b, \delta) \in \mathbb{Z}^3, \beta \in \mathbb{A}_{\mathbb{K}}$. Kažemo da je δ *nazivnik* od α.
Kako je ${}_1F_1\left(\begin{matrix}-n\\-2n\end{matrix}\middle| x\right) = \sum_{k=0}^{n} \frac{(-n)_k}{(-2n)_k}\frac{x^k}{k!}$, znamo prema lemi 2.17 da su p_n i q_n definirani sa
$p_n = {}_1F_1\left(\begin{matrix}-n\\-2n\end{matrix}\middle|\alpha\right) \times D_n,\ q_n = {}_1F_1\left(\begin{matrix}-n\\-2n\end{matrix}\middle|-\alpha\right) \times D_n$, gdje je

$$D_n = (2n)(2n-1)\ldots(n+1)\delta^n = \frac{(2n)!}{n!}\delta^n, \tag{2.14}$$

pripadaju $\mathbb{A}_{\mathbb{K}}$. Zaista $\frac{(2n)!}{n!} \times \frac{(-n)_k}{(-2n)_k k!} = \frac{(2n-k)!}{k!(n-k)!}$.
Zamjenom x sa α u (2.13) i množenjem s D_n dobivamo

$$q_n e^{\alpha} - p_n = r_n = \frac{(-1)^n D_n \alpha^{2n+1}}{\binom{2n}{n}(2n+1)!}\ {}_1F_1\left(\begin{matrix}n+1\\2n+2\end{matrix}\middle|\alpha\right). \tag{2.15}$$

Kako je $\Gamma(m+1) = m!$ za svaki prirodni broj m, lema 2.16 daje

$$|r_n| \leq \mathrm{Max}\left(1, e^{Re\alpha}\right)\frac{|\delta|^n\,|\alpha|^{2n+1}}{n!}. \tag{2.16}$$

Stoga $\lim_{n\to+\infty} r_n = 0$.
Sada pretpostavimo da je $e^{\alpha} \in \mathbb{Q}(i\sqrt{d})$ tj. da je $e^{\alpha} = \gamma/\delta'$ uz $\gamma \in \mathbb{A}_{\mathbb{K}}$, $\delta' \in \mathbb{N}$. Tada (2.15) postaje $q_n\gamma - \delta' p_n = \delta' r_n$, odakle je $a_n = q_n\gamma - \delta' p_n \in \mathbb{A}_{\mathbb{K}}$. Ali $\lim_{n\to+\infty} r_n = 0 \Rightarrow \lim_{n\to+\infty} a_n = 0$ i zbog toga je $a_n = 0$ za svaki veliki n prema lemi 2.13. Otuda, za svaki n dovoljno velik, $r_n = q_n e^{\alpha} - p_n = 0$ i $r_{n+1} = q_{n+1}e^{\alpha} - p_{n+1} = 0$.

$$\text{Stoga sustav jednadžbi} \begin{cases} q_n x + p_n y = 0 \\ q_{n+1}x + p_{n+1}y = 0 \end{cases}$$

ima netrivijalno rješenje, naime $x = e^{\alpha}$, $y = -1$ i determinantu Δ_n koja je jednaka nuli. Međutim,

$$\Delta_n = \begin{vmatrix} q_n & p_n \\ q_{n+1} & p_{n+1} \end{vmatrix} = -\begin{vmatrix} D_n Q_n(\alpha) & D_n P_n(\alpha) \\ D_{n+1}Q_{n+1}(\alpha) & D_{n+1}P_{n+1}(\alpha) \end{vmatrix},$$

uz notaciju iz uvoda 2.1 za Padéove aproksimante P_n, Q_n. Sada, $\Delta_n = -D_n D_{n+1} c_n \alpha^{2n+1} \neq 0$. Ova kontradikcija dokazuje teorem 2.11.

Poglavlje 3

Algebarski brojevi i mjere iracionalnosti

U odjeljku 3.1, poopćit ćemo pojam racionalnih i kvadratnih brojeva definirajući algebarske brojeve. U odjeljku 3.2, pokazat ćemo osnovna svojstva algebarskih cijelih brojeva. Ovo je uvod u algebarsku teoriju brojeva. Odjeljak 3.3 je posvećen dokazu slavnog Liouvilleovog teorema, koji pokazuje postojanje transcendentnih (koji nisu algebarski) brojeva. Zapravo, Liouvilleov teorem osigurava mjeru iracionalnosti za svaki algebarski broj. Proučavat ćemo ovaj pojam mnogo detaljnije u odjeljku 3.4 i pokazati da dobra diofantska aproksimacija omogućava dobijanje mjere iracionalnosti za specifične brojeve, na primjer za e. U odjeljku 3.5, objasnit ćemo kako poznavanje mjere iracionalnosti od $\sqrt[n]{d}$ omogućava rješavanje diofantske jednadžbe $x^n - dy^n = k$ ($n \geq 3$). Na kraju, iskazat ćemo bez dokaza Thueov i Rothov teorem, koji poboljšavaju Liouvilleov teorem.

3.1 Algebarski brojevi

Definicija 3.1. *Neka je $\alpha \in \mathbb{C}$. Kažemo da je α algebarski ako postoji ne nul polinom $P \in \mathbb{Z}[x]$ takav da je $P(\alpha) = 0$.*

Na primjer, $\alpha = 1/\sqrt{2}$ je algebarski pošto je $2\alpha^2 - 1 = 0$ i $\beta = 1 + \sqrt[3]{5}$ je algebarski jer je $(\beta - 1)^3 - 5 = \beta^3 - 3\beta^2 + 3\beta - 6 = 0$.
Neka je α bilo koji algebarski broj, i neka je $P \in \mathbb{Z}[x]$, $P \neq 0$, takav da $P(\alpha) = 0$ i P je *najmanjeg* stupnja. Podijelimo li P s njegovim vodećim koeficijentom dobivamo *normirani* polinom $P_\alpha \in \mathbb{Q}[x]$, koji zadovoljava $P_\alpha(\alpha) = 0$, P_α najmanjeg stupnja. Takav polinom je jedinstven (primjer 3.2) i zove se *minimalni polinom od α*.

Primjer 3.2. *Pretpostavimo da algebarski broj α ima dva minimalna polinoma P_α i Q_α. Tada $P_\alpha \neq 0$, $Q_\alpha \neq 0$, $P_\alpha(\alpha) = 0$, $Q_\alpha(\alpha) = 0$ i kako P_α i Q_α imaju minimalan stupanj,*

$deg P_\alpha \leq deg Q_\alpha$ i $deg Q_\alpha \leq deg P_\alpha$, što implicira da je $deg P_\alpha = deg Q_\alpha$. Stavimo $P_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ i $Q_\alpha(x) = x^d + b_{d-1}x^{d-1} + \cdots + b_0$.
Tada $R(x) = (a_{d-1} - b_{d-1})\, x^{d-1} + \cdots + (a_0 - b_0)$ nije nula jer je $P_\alpha \neq Q_\alpha$ i $R(\alpha) = 0$ te $deg R < deg P_\alpha$. Kontradikcija.

Teorem 3.3. *Neka je $P \in \mathbb{Q}[x]$ normirani polinom koji zadovoljava $P(\alpha) = 0$. Tada je P minimalni polinom od α ako i samo ako je P ireducibilan u $\mathbb{Q}[x]$, tj. ako $P(x) = P_1(x)P_2(x)$, uz P_1 i $P_2 \in \mathbb{Q}[x]$ što povlači $P_1(x) \in \mathbb{Q}$ ili $P_2(x) \in \mathbb{Q}$.*

Primjer 3.4. *Neka je $\alpha = (a + b\sqrt{d})/c$ kvadratni iracionalni broj, što znači da su a, b, c, d racionalni cijeli brojevi i d nije kvadrat. Tada je α korijen od $P(x) = (x - \alpha)(x - \alpha^*)$ gdje je $\alpha^* = (a - b\sqrt{d})/c$ konjugat od α. Stoga je α nultočka od*

$$P(x) = x^2 - \frac{2a}{c}x + \frac{a^2 - db^2}{c^2}.$$

Ovaj polinom je ireducibilan u $\mathbb{Q}[x]$. Zaista, ako je reducibilan, možemo ga zapisati kao $P(x) = (x + r)(x + r')$, uz $r,\ r' \in \mathbb{Q}$. Stoga njegovi korijeni će biti racionalni, što nisu. Prema tome P je minimalni polinom od α.

Definicija 3.5. *Stupanj minimalnog polinoma P_α algebarskog broja α naziva se stupanj od α i zapisujemo ga s $deg(\alpha)$.*

Prema tome, ako je α racionalan, α je algebarski stupnja 1. Ako je α kvadratno iracionalan, α ja algebarski stupnja 2 (primjer 3.4).
p-ti korijen jedinice $\omega = e^{2i\pi/p}$, p prost, povezan s Fermatovom jednadžbom $x^p + y^p = z^p$ pruža drugi zanimljiv primjer. Kako bi se to proučilo, trebamo sljedeći rezultat, koji je poznat kao *Einsteinov kriterij*.

Lema 3.6. *Neka je $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, uz $a_0,\ a_1,\ \ldots,\ a_{n-1} \in \mathbb{Z}$. Neka je p prost. Pretpostavimo da p dijeli $a_0,\ a_1,\ \ldots,\ a_{n-1}$, dok p^2 ne dijeli a_0. Tada je P ireducibilan u $\mathbb{Q}[x]$.*

U dokazu koristimo sljedeću lemu.

Lema 3.7. *Neka je $P \in \mathbb{Z}[x]$. Pretpostavimo da je P ireducibilan u $\mathbb{Q}[x]$, slijedi da je P reducibilan u $\mathbb{Z}[x]$.*

Dokaz. Pretpostavimo da je $P(x) = Q(x)R(x)$, uz $Q, R \in \mathbb{Q}[x]$, $\deg Q \geq 1$, $\deg R \geq 1$. Stavimo da je $d = \deg P$ i

$$Q(x) = \frac{a}{b}x^q + \ldots, \quad R(x) = \frac{a'}{b'}x^{d-q} + \ldots\ .$$

Tada $aa'/(bb') \in \mathbb{Z}$ i zato možemo pisati $P(x) = Q_0(x)R_0(x)$, uz

$$Q_0(x) = \frac{aa'}{bb'}x^q + \ldots, \; R_0(x) = x^{d-q} + \ldots,$$

što znači da su vodeći koeficijenti od Q_0 i R_0 racionalni cijeli brojevi. Neka su $\alpha_1, \ldots, \alpha_q$ nultočke od Q_0 u $\mathbb{C}$, a $\alpha_{q+1}, \ldots, \alpha_d$ od R_0. Tada su $\alpha_1, \ldots, \alpha_q$ korijeni od $P(x)$, stoga su oni *cijeli algebarski brojevi*. Dakle, koeficijenti od $Q_0(x) = \frac{aa'}{bb'}(x-\alpha_1)\ldots(x-\alpha_q)$ su algebarski cijeli brojevi prema teoremu 3.13. Pošto su oni također racionalni, imamo da je $Q_0 \in \mathbb{Z}[x]$. Slično, $R_0 \in \mathbb{Z}[x]$. □

Dokaz Leme 3.6. Pretpostavimo da je P reducibilan u $\mathbb{Q}[x]$. Prema lemi 3.7, postoje $Q, R \in \mathbb{Z}[x]$ takvi da je $P(x) = Q(x)R(x)$ uz $\deg Q \geq 1$, $\deg R \geq 1$. Zapišimo s $\hat{n}$ klasu ostataka od n modulo p, $\hat{Q}(x) = \hat{a_0} + \hat{a_1}x + \ldots + x^q$ i $\hat{R}(x) = \hat{b_0} + \hat{b_1}x + \ldots + x^{d-q}$.
Nadalje $x^d = \hat{Q}(x)\hat{R}(x)$ u prstenu $\mathbb{F}_p[x]$ polinoma nad poljem $\mathbb{F}_p$. Ovo povlači da su $\hat{Q}(x) = x^q$, $\hat{R}(x) = x^{d-q}$. Stoga $a_0 \equiv b_0 \equiv 0 \pmod{p}$, a_0b_0 je višekratnik od p^2, imamo kontradikciju. □

Upotrijebili smo pojam algebarskih cijelih brojeva i teorem 3.13. Kao primjer, razmotrit ćemo $\beta = 1 + \sqrt[3]{5}$. Znamo da je $P(\beta) = 0$, uz $P(x) = x^3 - 3x^2 + 3x - 6$. Otuda, prema Einsteinovom kriteriju, P je ireducibilan u $\mathbb{Q}[x]$ (uzmimo $p = 3$). Stoga, P je minimalni polinom od β (teorem 3.3) i $\deg(\beta) = 3$.
Sada se vratimo na $\omega = e^{2i\pi p}$, p je prost.

Teorem 3.8. *Neka je $\omega = e^{2i\pi p}$, a p prost. Tada je ω algebarski stupnja $p-1$. Njegov minimalni polinom je $P_\omega(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.*

Definicija 3.9. *Za prosti broj p, $P_\omega(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ zovemo ciklički polinom reda p.*

Dokaz Teorema 3.7. Jasno je da

$$\omega^{p-1} + \omega^{p-2} + \cdots + \omega + 1 = (\omega^p - 1)/(\omega - 1) = 0.$$

Ostaje nam provjeriti da je P_ω ireducibilan u $\mathbb{Q}[x]$ (teorem 3.8). Ali P_ω je ireducibilan ako i samo ako je $Q(x) = P_\omega(x+1)$ ireducibilan. Imamo

$$Q(x) = ((x+1)^p - 1) \,/\, ((x+1) - 1) = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}.$$

Za $k = 1, 2, \ldots, p-1$, $p \mid \binom{p}{k}$ jer je $\binom{p}{k} = p(p-1)\ldots(p-k+1)/k!$ i p ne dijeli $k!$. Budući da je $a_0 = p$, Q je ireducibilan na $\mathbb{Q}[x]$ prema Einsteinovom kriteriju, i P_ω također. □

3.2 Algebarski cijeli brojevi

Kažemo da je α *algebarski cijeli broj* ako je algebarski i ako njegov minimalni polinom P_α ima cjelobrojne koeficijente. Drugim riječima, ako postoje $a_0, a_1, \ldots, a_{d-1} \in \mathbb{Z}$ takvi da $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 = 0$.
Na primjer, $\sqrt{2}$, $\sqrt[3]{5}$, $e^{\frac{2i\pi}{p}}$ su algebarki cijeli brojevi. Racionalni cijeli brojevi su algebarski cijeli brojevi stupnja 1. Kvadratni iracionalni cijeli brojevi su algebarski cijeli brojevi stupnja 2.

Teorem 3.10. *Neka je α algebarski broj. Tada postoji $k \in \mathbb{N}$ takav da je $\beta = k\alpha$ algebarski cijeli broj.*

Dokaz. Neka $P_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots a_0$ (uz $a_0, \ldots, a_{d-1} \in \mathbb{Q}$) bude minimalni polinom od α.
Neka je $k \in \mathbb{N}$ takav da je $ka_0 = b_0,\ ka_2 = b_1,\ \ldots,\ ka_{d-1} = b_{d-1} \in \mathbb{Z}$. Tada

$$k^d\alpha^d\ + k^{d-1}b_{d-1}\alpha^{d-1}\ + \cdots + k^{d-1}b_0 = 0.$$

Dakle, $(k\alpha)^d + b_{d-1}(k\alpha)^{d-1} + kb_{d-2}(k\alpha)^{d-2} + \cdots + k^{d-1}b_0 = 0$, i $\beta = k\alpha$ je algebarski cijeli broj. □

Najmanji prirodni broj k, takav da je $k\alpha$ algebarski cijeli broj, zovemo *nazivnik* od α i označavamo ga sa $\mathrm{den}(\alpha)$. Na primjer, ako je $\alpha = p/q$ ireducibilni racionalni broj uz $q > 0$, minimalni polinom od α je $P_\alpha(x) = x - p/q$, i $\mathrm{den}(\alpha) = q$, očekivano.
Normalno je da se zapitamo je li suma i produkt dvaju algebarskih cijelih brojeva također algebarski cijeli broj. Odgovor je pozitivan (sljedeći teorem). Kako bi se to pokazalo, trebat će nam lema, koja potječe od Newtona, o simetričnim polinomima. Kažemo da je polinom od n nepoznanica $P(x_1,\ x_2, \ldots,\ x_n)$, s koeficijentima u domeni $\mathbb{A}$, *simetričan*, ako je $P(x_{\tau(1)},\ x_{\tau(2)},\ \ldots,\ x_{\tau(n)}) = P(x_1,\ x_2, \ldots,\ x_n)$ za bilo koju permutaciju τ indeksa $1, 2, \ldots, n$ (to jest za svaku permutaciju nepoznanica $x_1,\ x_2,\ \ldots,\ x_n$). Sljedeći polinom, na primjer, je simetričan:

$$P(x_1,\ x_2, \ldots,\ x_n) = x_1^3 + x_2^3 + x_3^3 + 2x_1^2x_2^2 + 2x_1^2x_3^2 + 2x_2^2x_3^2 + 5x_1x_2x_3.$$

Lema 3.11. *Neka je $P \in \mathbb{A}[x_1,\ x_2,\ \ldots,\ x_n]$ simetričan. Neka je*

$$\begin{cases} \sigma_1 = x_1 + x_2 + \cdots + x_n = \sum_i x_i \\ \sigma_2 = \sum_{i<j} x_ix_j \\ \sigma_3 = \sum_{i<j<k} x_ix_jx_k \\ \vdots \\ \sigma_n = x_1x_2\ldots x_n \end{cases} \tag{3.1}$$

Tada $P(x_1,\ x_2,\ \ldots,\ x_n)$ možemo zapisati kao polinom od n nepoznanica $\sigma_1,\ \sigma_2,\ \ldots \sigma_n$, s koeficijentima u $\mathbb{A}$.

Dokaz. Neka je α_1 najveća potencija koja se pojavljuje uz x_1 u P. Među članovima koji sadrže $x_1^{\alpha_1}$, neka je α_2 najveća potencija koja se pojavljuje uz x_2. Među članovima koji sadrže $x_1^{\alpha_1}x_2^{\alpha_2}$, neka je α_3 najveća potencija koja se pojavljuje uz x_3, i tako dalje. Navedeni proces definira *vodeći član*, oblika $ax_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$. Zato što je P simetričan, $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$ (zaista, P isto sadrži član $ax_2^{\alpha_1}x_1^{\alpha_2}\ldots x_n^{\alpha_n}$, odakle je $\alpha_2 \leq \alpha_1$ i tako dalje).
Nadalje, uočimo da vodeći član od $\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\ldots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}$ je $x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$. Stoga, računajući $P(x_1, x_2, \ldots, x_n) - a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\ldots\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}$, eliminiramo sve članove oblika $ax_{\tau(1)}^{\alpha_1}$, $x_{\tau(2)}^{\alpha_2}$, $\ldots$, $x_{\tau(n)}^{\alpha_n}$ te lema 3.11 slijedi indukcijom. □

Napomena 3.12. *Ovaj dokaz je konstruktivan. Omogućuje transformaciju, u praksi, $P \in \mathbb{A}[x_1,\ x_2,\ \ldots,\ x_n]$ u $P \in \mathbb{A}[\sigma_1,\ \sigma_2,\ \ldots,\ \sigma_n]$.*
Na primjer, neka je $P(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3 + 2x_1^2x_2^2 + 2x_2^2x_3^2 + 2x_1^2x_3^2 + 5x_1x_2x_3$. Prvo vidimo da vodeći član odgovara $\alpha_1 = 3,\ \alpha_2 = 0,\ \alpha_3 = 0$, odakle je

$$\begin{aligned} P(x_1,\ x_2,\ x_3) - \sigma_1^3 &= P(x_1,\ x_2,\ x_3) - (x_1 + x_2 + x_3)^3 \\ &= 2x_1^2x_2^2 + 2x_2^2x_3^2 + 2x_1^2x_3^2 - 3x_1^2x_2 - 3x_1x_2^2 \\ &\quad - 3x_2^2x_3 - 3x_2x_3^2 - 3x_1^2x_3 - 3x_1x_3^2 - x_1x_2x_3. \end{aligned}$$

Novi vodeći član odgovara $\alpha_1 = 2,\ \alpha_2 = 2,\ \alpha_3 = 0$ i

$$\begin{aligned} P(x_1,\ x_2,\ x_3) - \sigma_1^3 - 2\sigma_2^2 &= P(x_1,\ x_2,\ x_3) - \sigma_1^3 - 2(x_1x_2 + x_2x_3 + x_1x_3)^2 \\ &= -4x_1^2x_2x_3 - 4x_1x_2^2x_3 - 4x_1x_2x_3^2 - 3x_1^2x_2 - 3x_1x_2^2 \\ &\quad - 3x_2^2x_3 - 3x_2x_3^2 - 3x_1^2x_3 - 3x_1x_3^2 - x_1x_2x_3. \end{aligned}$$

Sada $\alpha_1 = 2,\ \alpha_2 = 1,\ \alpha_3 = 1$, otud

$$\begin{aligned} &P(x_1,\ x_2,\ x_3) - \sigma_1^3 - 2\sigma_2^2 + 4\sigma_1\sigma_3 \\ &= -3x_1^2x_2 - 3x_1x_2^2 - 3x_2^2x_3 - 3x_2x_3^2 - 3x_1^2x_3 - 3x_1x_3^2 - x_1x_2x_3. \end{aligned}$$

Napokon, imamo $\alpha_1 = 2,\ \alpha_2 = 1,\ \alpha_3 = 0$, što povlači

$$P(x_1,\ x_2,\ x_3) - \sigma_1^3 - 2\sigma_2^2 + 4\sigma_1\sigma_3 + 3\sigma_1\sigma_2 = 8x_1x_2x_3.$$

Dakle $P(x_1,\ x_2,\ x_3) = \sigma_1^3 + 2\sigma_2^2 - 4\sigma_1\sigma_3 - 3\sigma_1\sigma_2 + 8\sigma_3$.

Teorem 3.13. *Neka su α i β dva algebarska cijela broja. Tada su $\alpha + \beta$ i $\alpha\beta$ algebarski cijeli brojevi.*

Dokaz. Neka su P_α i P_β minimalni polinomi od α i β, stupnja d, odnosno n. Neka je $x_1 = \beta$, a $x_2, \ldots, x_n$ nultočke od P_β u $\mathbb{C}$.
Znamo da $P_\beta(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \cdots + (-1)^n \sigma_n$, gdje su $\sigma_1, \sigma_2, \ldots, \sigma_n$ definirani u (3.1). Stoga $\sigma_1, \sigma_2, \ldots, \sigma_n \in \mathbb{Z}$. Jer je $x_1 = \beta$, polinom $Q(x) = P_\alpha(x - x_1)P_\alpha(x - x_2)\ldots P_\alpha(x - x_n)$ zadovoljava $Q(\alpha + \beta) = 0$. Njegovi koeficijenti su simetrični polinomi u $x_1, x_2, \ldots, x_n$, s koeficijentima u $\mathbb{Z}$. Nadalje, prema lemi 3.11, $Q \in \mathbb{Z}[x]$, što dokazuje da je $\alpha + \beta$ algebarski. □

Dokaz za umnožak $\alpha\beta$ je sličan. Samo treba zamijeniti $Q(x)$ sa

$$R(x) = (x_1 x_2 \ldots x_n)^d P_\alpha\left(\frac{x}{x_1}\right) P_\alpha\left(\frac{x}{x_2}\right) \ldots P_\alpha\left(\frac{x}{x_n}\right).$$

Korolar 3.14. *Ako su α i β algebarski brojevi, onda su $\alpha + \beta$ i $\alpha\beta$ također algebarski brojevi. Preciznije, skup $\overline{\mathbb{Q}}$ algebarskih brojeva je potpolje od $\mathbb{C}$.*

Dokaz.
1. Neka su a i b nazivnici od α i β te neka je $m = nzv(a, b)$. Tada $m\alpha = m'(a\alpha)$ i $m\beta = m''(b\alpha)$ su algebarski cijeli brojevi prema teoremu 3.13 (produkt algebarskih cijelih brojeva). Stoga $m(\alpha + \beta)$ je algebarski cijeli broj (suma algebarskih cijelih brojeva), što pokazuje da je $\alpha + \beta$ algebarski. Slično, $ab\alpha\beta$ je algebarski cijeli broj i $\alpha\beta$ je algebarski.

2. Ako su α i β algebarski brojevi, $\alpha+\beta$ i $\alpha\beta$ su također algebarski brojevi. Nadalje, $-\alpha$ je algebarski broj jer je $a_0+a_1\alpha+\cdots+a_d\alpha^d = 0 \Rightarrow\ a_0-a_1(-\alpha)+\cdots+(-1)^d a_d(-\alpha)^d = 0$.
Naposlijetku, ako je $\alpha \neq 0$, tada $1/\alpha$ je algebarski broj jer je $a_0(1/\alpha)^d + a_1(1/\alpha)^{d-1} + \cdots + a_d = 0$. Prema tome $\overline{\mathbb{Q}}$ je potpolje od $\mathbb{C}$.

□

3.3 Transcedentni brojevi i Liouvilleov teorem

Definicija 3.15. *Kompleksni broj α je transcendentan ako nije algebarski, tj. ako je $P(x) \neq 0$ za svaki $P \in \mathbb{Z}[x],\ P \neq 0$.*

Iako je jednostavno dati primjere algebarskih brojeva, daleko je od očitog izložiti transcendentne brojeve. Prvi transcendentni broj u povijesti je konstruirao Joseph Liouville (1844), koristeći sljedeći rezultat, koji je poznat kao *Liouvilleov teorem*.

Teorem 3.16. *Neka je α algebarski broj stupnja $d \geq 2$. Neka je $k \in \mathbb{N}$ takav da je $P = kP_\alpha \in \mathbb{Z}[x]$. Definiramo $C' = \max_{[\alpha-1,\,\alpha+1]} |P'(x)|$ i $C = min(1, 1/C')$. Tada, za svaki racionalni broj p/q uz $q > 0$,vrijedi*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^d} \tag{3.2}$$

Dokaz. Za svaki $p/q \in \mathbb{Q}$, broj $q^d P(p/q)$ je cijeli broj jer je $P \in \mathbb{Z}[x]$te je različit od nule jer je $\deg(\alpha) \geq 2$. Zaista, kad bi bio nula, P_α bi imao racionalni korijen, što je nemoguće zato jer je ireducibilan na $\mathbb{Q}[x]$. Stoga $\left|q^d\left(P(\alpha) - P(p/q)\right)\right| = \left|q^d P(p/q)\right| \geq 1$.

Sada, teorem srednje vrijednosti povlači $\max\limits_{[\alpha,p/q]} |P'(x)| \left|\alpha - \dfrac{p}{q}\right| \geq \dfrac{1}{q^d}$.

Ako je $|\alpha - p/q| \geq 1$, tada je očigledno $|\alpha - p/q| \geq q^{-d}$. Inače, možemo pisati $\max\limits_{[\alpha,p/q]} |P'(x)| \leq C'$ i stoga $|\alpha - p/q| \geq q^{-d}/C'$, što dokazuje Liouvilleov teorem. □

Napomena 3.17. *Liouvilleov teorem je eksplicitan. Dozvoljava nam izračunati C kada je α zadan. Na primjer, neka je $\alpha = \sqrt[3]{17}$. Tada $\alpha^3 - 17 = 0$ i $P(x) = x^3 - 17$ je minimalni polinom od α, jer je P ireducibilan na $\mathbb{Q}[x]$ prema Einsteinovom kriteriju uz $p = 17$. Nadalje,*

$$\max_{[\alpha-1,\alpha+1]} |P'(x)| = 3\left(\sqrt[3]{17} + 1\right)^2 = C',$$

odakle $C = 1/C' \geq 0.026$. Stoga, za svaki $p/q \in \mathbb{Q}$ uz $q > 0$, vrijedi

$$\left|\sqrt[3]{17} - \frac{p}{q}\right| \geq \frac{0.026}{q^3}. \tag{3.3}$$

Definicija 3.18. *Neka je $\alpha \in \mathbb{R}$ iracionalni broj. Kažemo da je α Liouvilleov broj ako, za svaki veliki $n \in \mathbb{N}$, postoji racionalni broj p/q, uz $q \geq 2$ koji zadovoljava*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}. \tag{3.4}$$

Primjer 3.19. *Slijedeći Liouvillea, promotrimo Engelov red*

$$\alpha = \sum_{k=0}^{+\infty} \frac{1}{10^{k!}}. \tag{3.5}$$

Decimalni razvoj od α je $\alpha = 1,1100010000000000000000100\ldots$. Za $n \geq 1$, imamo

$$\begin{aligned}\left|\alpha - \sum_{k=0}^{n} \frac{1}{10^{k!}}\right| = \sum_{k=0}^{+\infty} \frac{1}{10^{k!}} &\leq \frac{1}{10^{(n+1)!}}\left(1 + \frac{1}{10} + \frac{1}{10^2} + \cdots\right) \\ &\leq \frac{1}{(10^{n!})^n} \cdot \frac{1}{10^{n!}} \cdot \frac{10}{9} < \frac{1}{(10^{n!})^n}.\end{aligned}$$

Definiramo $\frac{p}{q} = \sum_{k=0}^{n} \frac{1}{10^{k!}},\ q = 10^{n!}$.

Sad je jasno da (3.4) vrijedi za $n \geq 1$ i da je α Liouvilleov broj.

Teorem 3.20. *Svaki Liouvilleov broj je transcendentan.*

Dokaz. Neka je α Liouvilleov broj. Pretpostavimo da je α algebarski broj. Tada je $d = \deg\alpha \geq 2$, jer je α iracionalan. Za svaki veliki n, postoji $p/q \in \mathbb{Q}$, uz $q \geq 2$, koji zadovoljava (3.4). Prema Liouvilleovom teoremu 3.15, $\frac{C}{q^d} \leq \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}$. Kontradikcija kada $n \to +\infty$. □

3.4 Mjere iracionalnosti

Definicija 3.21. *Neka je $\alpha \in \mathbb{R}$ iracionalni broj. Kažemo da je $\mu > 0$ mjera iracionalnosti od α ako postoji konstanta $C > 0$ takva da, za svaki racionalni p/q uz $q > 0$, vrijedi*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^\mu}. \tag{3.6}$$

Liouvilleov teorem 3.15 implicira da je d mjera iracionalnosti za svaki algebarski broj stupnja d. S druge strane, Liouvilleov broj nema mjeru iracionalnosti (primjer 3.22). Ako α ima mjeru iracionalnost, donja ograda svih mjera iracionalnosti se zove *najbolja mjera iracionalnosti* od α, u zapisu $\mu(\alpha)$. Možemo dokazati da je $\mu(\alpha) \geq 2$ (primjer 3.23). Kada je α Liouvilleov broj, uzimamo $\mu(\alpha) = +\infty$.

Primjer 3.22. *Pretpostavimo da α ima mjeru iracionalnosti μ i da je Liouvilleov broj. Za svaki n dovoljno velik, postoji $p/q \in \mathbb{Q}$ uz $q \geq 2$ i*

$$\frac{c}{q^\mu} \leq \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

Ovo povlači da je $0 < C \leq q^{\mu-n}$. Imamo kontradikciju kada $n \to +\infty$.

Primjer 3.23. *Pretpostavimo da je $\mu(\alpha) < 2$. Fiksiramo $\mu \in]\mu(\alpha), 2[$. Jer je $\mu(\alpha)$ donja ograda za sve mjere iracionalnosti od α, imamo $\left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^\mu}$, gdje je C konstanta. Uzmimo da je $p = P_n,\ q = Q_n$ gdje je P_n/Q_n n-ta konvergenta razvoja u verižni razlomak od α. Tada je*

$$\frac{C}{Q_n^\mu} \leq \left|\alpha - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n^2}.$$

Dakle, $0 < C \leq Q_n^{\mu-2}$. Ali $\mu - 2 < 0$ i $Q_n \to +\infty$, što je kontradikcija.

Teorem u nastavku omogućit će nam da nađemo mjeru iracionalnosti upotrebom niza dobrih diofantskih aproksimacija, kao što su one koje dobijemo pomoću Padéovih aproksimanata (odjeljak 2.4).

Teorem 3.24. *Neka je $\alpha \in \mathbb{R}$. Pretpostavimo da postoje konstante $a > 0$, $b > 0$, $k > 0$, $\ell \geq \frac{1}{2}$, $h \geq 1$, rastuća funkcija $g : \mathbb{N} \to \mathbb{R}_+^*$ i niz p_n/q_n diofantskih aproksimacija od α koji zadovoljavaju*

$$\forall n \in \mathbb{N}, \qquad q_n p_{n+1} - q_{n+1} p_n \neq 0, \tag{3.7}$$

$$\forall n \in \mathbb{N}, \qquad |q_n| \leq k\,(g(n))^a\,, \tag{3.8}$$

$$\forall n \in \mathbb{N}, \qquad |q_n\alpha - p_n| \leq \ell/g(n), \tag{3.9}$$

$$g(0) = 1 \; i \; \lim_{n\to+\infty} g(n) = +\infty, \tag{3.10}$$

$$\forall n \in \mathbb{N}, \qquad g(n+1) \leq b(g(n))^h. \tag{3.11}$$

Tada je α iracionalan i za svaki racionalni p/q uz $q > 0$, vrijedi

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^n}, \tag{3.12}$$

gdje je $C = \dfrac{1}{2kb^{a(h+1)}(2\ell)^{ah^2}}$ *i* $\mu = ah^2 + 1$.

Dokaz. Neka je $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ zadan. Neka je ν najmanji cijeli broj koji zadovoljava $q\ell/g(\nu) < 1/2$. Jasno je da ν postoji jer je $\lim_{n\to+\infty} g(n) = +\infty$. Pošto je $q \geq 1$, $g(0) = 1$ i $\ell \geq 1/2$, imamo $\nu \geq 1$. Zatim, $q\ell/g(\nu - 1) \geq 1/2$, odakle imamo $g(\nu - 1) \leq 2q\ell$. Iz (3.11) zaključujemo da je $g(\nu) \leq b(2q\ell)^h$. Upotrebom (3.11) opet dobivamo

$$g(\nu) < g(\nu + 1) \leq b^{h+1}(2q\ell)^{h^2}. \tag{3.13}$$

Promotrimo determinantu

$$\Delta_\nu = \begin{vmatrix} q_\nu & p_\nu \\ q_{\nu+1} & p_{\nu+1} \end{vmatrix}.$$

Iz (3.7) znamo da je $\Delta_\nu \neq 0$. Ovo znači da vektori (q_ν, p_ν) i $(q_{\nu+1}, p_{\nu+1})$ čine bazu od $\mathbb{R}^2$. Za posljedicu imamo da je barem jedna od dvije determinante

$$\begin{vmatrix} q_\nu & p_\nu \\ q & p \end{vmatrix} \text{ ili } \begin{vmatrix} q_{\nu+1} & p_{\nu+1} \\ q & p \end{vmatrix}$$

različita od nule. Neka je $m = \nu$ ili $\nu + 1$, tako da $\delta_m = \begin{vmatrix} q_m & p_m \\ q & p \end{vmatrix} \neq 0$.
Kako je $\delta_m \in \mathbb{Z}$, ovo implicira da je $|\delta_m| \geq 1$, odakle je $|pq_m - qp_m| \geq 1$. Stoga $|q(q_m\alpha - p_m) - q_m(q\alpha - p)| \geq 1$ i prema nejednakosti trokuta,

$$q\,|q_m\alpha - p_m| + |q_m|\,|q\alpha - p| \geq 1.$$

Sada, upotrijebimo (3.9) i definiciju od ν i m, pa imamo

$$q\,|q_m\alpha - p_m| \leq \frac{q\ell}{g(m)} \leq \frac{g\ell}{g(\nu)} < \frac{1}{2}, \text{ odakle } |q_m|\,|q\alpha - p| > \frac{1}{2}.$$

Nadalje, prema (3.8) i (3.13), $|q_m| \leq k(g(m))^a \leq kb^{a(h+1)}(2q\ell)^{ah^2}$ i naposlijetku dobijemo

$$|q\alpha - p| > \frac{1}{2kb^{a(h+1)}(2\ell)^{ah^2}} \frac{1}{q^{ah^2}}.$$

□

Primjer 3.25. *Izračunajmo mjeru iracionalnosti od e. Prema (2.14), (2.15), (2.16), (2.17), (2.18), znamo da*

$$\forall n \in \mathbb{N}, \qquad |q_n e - p_n| \leq \frac{e}{n!}, \tag{3.14}$$

$$p_n = \frac{(2n)!}{n!}\,{}_1F_1\left(\begin{matrix}-n\\-2n\end{matrix}\middle|1\right), \quad q_n = \frac{(2n)!}{n!}\,{}_1F_1\left(\begin{matrix}-n\\-2n\end{matrix}\middle|-1\right) \tag{3.15}$$

$$q_n p_{n+1} - p_n q_{n+1} \neq 0. \tag{3.16}$$

Primjenimo teorem 3.24 uz $g(n) = n!$, što zadovoljava (vidi primjer 3.26)

$$\forall n \in \mathbb{N}, \qquad (n+1)! \leq 3(n!)^{\frac{3}{2}}. \tag{3.17}$$

Sada pogledajmo gornju ogradu za $|q_n|$. Imamo

$$\left|{}_1F_1\left(\begin{matrix}-n\\-2n\end{matrix}\middle|-1\right)\right| \leq \sum_{k=0}^{n} \frac{n(n-1)\ldots(n-k+1)}{2n(2n-1)\ldots(2n-k+1)k!} \leq \sum_{k=0}^{n} \frac{1}{k!} \leq e,$$

i stoga $|q_n| \leq e\dfrac{(2n)!}{n!} = e\binom{2n}{n}n!$. Koristeći gornju ogradu

$$\forall n \in \mathbb{N}, \qquad \binom{2n}{n} \leq 4^n, \tag{3.18}$$

zaključujemo (primjer 3.27) da

$$\forall n \in \mathbb{N}, \qquad |q_n| \leq 30(n!)^2. \tag{3.19}$$

Sada primijenimo teorem 3.23 uz $a = 2$, $b = 3$, $k = 30$, $\ell = e$, $h = 3/2$ i vidimo da, za racionalni p/q uz $q > 0$, vrijedi

$$\left|e - \frac{p}{q}\right| \geq \frac{10^{-9}}{q^{5.5}}. \tag{3.20}$$

Zbog toga, e nije Liouvilleov broj.

Napomena 3.26. *Mjera iracionalnosti $\mu = 5.5$ ovdje dobivena je daleko od najbolje moguće. Poboljšanjem procjene (3.17) i (3.19), može se dokazati da za svaki $\varepsilon > 0$ postoji C takav da za svaki $p/q \in \mathbb{Q}$ uz $q > 0$, $|e - p/q| \geq C/q^{2+\varepsilon}$.*
Ovo znači da najbolja mjera iracionalnosti od e zadovoljava $\mu(e) \leq 2$. Međutim, najbolja mjera iracionalnosti za bilo koji realan broj α zadovoljava $\mu(e) \geq 2$ (primjer 3.23). Stoga je

$$\mu(e) = 2. \tag{3.21}$$

Primjer 3.27. *Pokazat ćemo da $n + 1 \leq 3\sqrt{n!}$ vrijedi za svaki $n \in \mathbb{N}$. Zaista, ovo vrijedi za $n = 0$. Pretpostavimo da $n + 1 \leq 3\sqrt{n!}$ vrijedi za neki $n \geq 1$, tada*

$$n + 2 \leq 3\sqrt{n!} + 1 \leq 4\sqrt{n!} \leq \frac{4}{\sqrt{n+1}}\sqrt{(n+1)!} \leq \frac{4}{\sqrt{2}}\sqrt{(n+1)!} \leq 3\sqrt{(n+1)!},$$

što dokazuje tvrdnju po principu matematičke indukcije.

Primjer 3.28. *Budući da je $(1+x)^{2n} = \sum_{k=0}^{2n}\binom{2n}{k}x^k$, imamo $\sum_{k=0}^{2n}\binom{2n}{k} = 2^{2n} = 4^n$. Kao posljedicu imamo da je $\binom{2n}{n} \leq 4^n$. Sada, jer je $|q_n| \leq e \cdot \binom{2n}{n} n!$, imamo da je $|q_n| \leq e \cdot 4^n n!$ i ostaje za dokazati da $4^n e \leq 30 \cdot n!$ vrijedi za svaki $n \in \mathbb{N}$. Ovo vrijedi za $n = 0, 1, 2, 3$. Za $n \geq 3$, imamo da je $4^{n+1}e \leq 4 \cdot 4^n \leq 4 \cdot 30 \cdot n! \leq (n+1) \cdot 30n! \leq 30(n+1)!$, što indukcijom dokazuje željeni rezultat.*

3.5 Diofantske jednadžbe i mjere iracionalnosti

Teorem 3.29. *Neka je $k \in \mathbb{Z}$, $d \in \mathbb{N}\setminus\{0,1\}$ i $n \in \mathbb{N}\setminus\{0,1,2\}$, uz $\sqrt[n]{d} \notin \mathbb{Q}$. Pretpostavimo da postoje $C > 0$ i $\mu < n$ takvi da, za svaki racionalni p/q uz $q > 0$, vrijedi*

$$\left|\sqrt[n]{d} - \frac{p}{q}\right| \geq \frac{C}{q^\mu}. \tag{3.22}$$

Tada diofantska jednadžba

$$x^n - dy^n = k \tag{3.23}$$

ima samo konačno mnogo rješenja $(x, y) \in \mathbb{Z}^2$. Preciznije, neka je (x, y) rješenje za (3.23), takvo da je $x > 0$, $y > 0$, x i y relativno prosti. Tada, ili je $y \leq 2|k|$ ili $x = P_n$, $y = Q_n$, gdje je P_n/Q_n konvergenta razvoja u verižni razlomak od $\sqrt[n]{d}$ koja zadovoljava $Q_n \leq \left(\frac{|k|}{C}\right)^{\frac{1}{n-\mu}}$.

Dokaz. Ako je n paran, možemo se ograničiti na slučaj kad je $x > 0,\ y > 0$. Ako je n neparan i ako su x i y različitih predznaka, (3.23) zapisujemo $x'^n + dy'^n = k',\ x' > 0,\ y > 0$, što ima samo konačno mnogo rješenja te ponovno samo trebamo uzeti u obzir slučaj gdje su $x > 0,\ y > 0$. Naposlijetku, možemo pretpostaviti da su x i y relativno prosti (inače bi podijelili jednadžbu s n-tom potencijom od najvećeg zajedničkog djelitelja (x, y). Uz ove pretpostavke, imamo

$$\begin{aligned}|x^n - dy^n| &= \left|x - \sqrt[n]{d}y\right|\left(x^{n-1} + x^{n-2}\sqrt[n]{d}y + \cdots + \left(\sqrt[n]{d}y\right)^{n-1}\right)\\ &\geq \left|x - \sqrt[n]{d}y\right| y^{n-1} \geq \left|x/y - \sqrt[n]{d}\right| y^n.\end{aligned}$$

Dakle, ako je (x, y) rješenje od (3.23), tada je

$$\left|\frac{x}{y} - \sqrt[n]{d}\right| \leq \frac{|k|}{y^n} = \frac{|k|}{y}\frac{1}{y^{n-1}}.$$

Prema tome, ako je $y > 2|k|,\ x/y$ je konvergenta razvoja u verižni razlomak od $\sqrt[n]{d}$. U ovom slučaju, upotrebom (3.22), vidimo da $|k|/y^n \geq C/y^\mu$, odakle je $y^{n-\mu} \leq |k|/C$. Prema pretpostavci, $n - \mu > 0$, pa stoga je $y \leq (|k|/C)^{\frac{1}{n-\mu}}$. Teorem 3.28 je time dokazan. □

Napomena 3.30. *Treba naglasiti da Liouvilleov teorem 3.16 ne omogućuje dobivanje (3.22) svaki put kad znamo poboljšanje Liouvilleovog eksponenta n. Poboljšanjem metode iz odjeljka 3.4, moguće je dobiti poboljšanje u specijalnim slučajevima. Na primjer, tablica 3.1, od Benneta iz 1997, daje eksplicitne mjere iracionalnosti za neke brojeve oblika* $\sqrt[n]{d},\ n \geq 3$.

Primjer 3.31. *Razmotrimo diofantsku jednadžbu*

$$x^3 - 6y^3 = 1. \tag{3.24}$$

Ako je $x \geq 0$ i $y \leq 0$, imamo jedno rješenje, $x = 1,\ y = 0$. Ako je $x \leq 0$ i $y \geq 0$ onda nema rješenja. Dakle, moramo riješiti jednadžbu $x^3 - 6y^3 = \pm 1$, uz $x > 0,\ y > 0,\ x$ i y su relativno prosti te se teorem 3.29 može primjeniti. Ako je $y \leq 2|k| = 2$, tada nema rješenja jer 7 i 49 nisu kubovi.
Stoga $x = P_n$ i $y = Q_n$, gdje je P_n/Q_n konvergenta razvoja u verižni razlomak od $\sqrt[3]{6}$ koja zadovoljava $Q_n \leq (1/C)^{\frac{1}{3-\mu}}$. Uporabom vrijednosti od C i μ dane u tablici 3.1, dobivamo $y = Q_n \leq 1193$.
Računamo prvi član od razvoja u verižni razlomak od $\alpha = \sqrt[3]{6}$. Prvo $\alpha^3 - 6 = 0$ i $\alpha = 1 + 1/\alpha_1$, odakle je $(1 + 1/\alpha_1)^3 - 6 = 0$, i $5\alpha_1^3 - 3\alpha_1^2 - 3\alpha_1 - 1 = 0$ što povlači da je $\alpha_1 = 1 + 1/\alpha_2$. Zamjena povlači $2\alpha_2^3 - 6\alpha_2^2 - 12\alpha_2 - 5 = 0$ i $\alpha_2 = 4 + 1/\alpha_3$. Sada α_3 zadovoljava $21\alpha_3^3 - 36\alpha_3^2 - 18\alpha_3 - 2 = 0$ i $\alpha_3 = 2 + 1/\alpha_4$ i tako dalje. Naposlijetku imamo

$\sqrt[3]{6} = [1, 1, 4, 2, 7, 3, 511, 1, 2, \ldots]$. Prve konvergente se mogu izračunati po rekurzijama $P_0 = a_0,\ P_1 = a_0a_1 + 1,\ P_n = a_nP_{n-1} + P_{n-2},\ Q_0 = 1,\ Q_1 = a_1,\ Q_n = a_nQ_{n-1} + Q_{n-2}$, pa imamo $P_0 = 1,\ Q_0 = 1,\ P_1 = 2,\ Q_1 = 1,\ P_2 = 9,\ Q_2 = 5\ P_3 = 20,\ Q_3 = 11\ P_4 = 149,\ Q_4 = 82\ P_5 = 467,\ Q_5 = 257\ P_6 = 238786,\ Q_6 = 131409$. Samo prvih šest može povlačiti rješenje od (3.24) jer je $y = Q_n \leq 1193$. Sada je jednostavno provjeriti na nijedan od parova $x = P_i,\ y = Q_i$, uz $0 \leq i \leq 5$, nije rješenje od (3.24). Dakle (3.24) nema drugo rješenje osim $x = 1,\ y = 0$.

3.6 Thueov i Rothov teorem

Mnogo je istraživanja provedeno u svrhu poboljšanja Liouvilleovog eksponenta u općem slučaju. Prvi uspjeh u ovom smjeru bio je Thueov teorem (1908):

Teorem 3.32. *Neka je α algebarski broj stupnja $d \geq 2$. Tada postoji konstanta $C > 0$ takva da za svaki $p/q \in \mathbb{Q}$ uz $q > 0$, vrijedi*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^{1+\frac{d}{2}}}.$$

Teorem 3.32 daje za $d \geq 3$ *ne eksplicitno* poboljšanje Liouvilleovog eksponenta. Zaista, konstantu C ne možemo izračunati u odnosu na α. Dokaz Thueovog teorema koristi metode teorije transcendentnih brojeva, pa to nećemo dokazivati.

Korolar 3.33. *Neka je $P(X) = a_0 + a_1X + \cdots + a_dX^d \in \mathbb{Z}[X]$ ireducibilan u $\mathbb{Q}[x]$ stupnja $d \geq 3$. Tada homogena diofantska jednadžba*

$$\sum_{i=0}^{d} a_i x^i y^{d-i} = k \tag{3.25}$$

ima samo konačno mnogo rješenja $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

Dokaz nećemo provoditi.
Općenito, nije poznato kako dobiti gornju ogradu za rješenja (x, y) u (3.25) kao funkciju od a_i-ova (suprotno teoremu 3.29). Prema tome kololar 3.33 ne daje nam metodu učinkovitog rješavanja jednadžbe (3.25).
Najbolji rezultat u diofantskim aproksimacijama algebarskih brojeva je Rothov teorem (1955):

Teorem 3.34. *Neka je α algebarski broj stupnja $d \geq 2$. Tada, za svaki $\varepsilon > 0$, postoji konstanta $C > 0$ takva da je $|\alpha - p/q| \geq C/q^{2+\varepsilon}$ za svaki racionalni broj p/q uz $q > 0$.*

Drugim riječima, najbolja mjera iracionalnosti bilo kojeg algebarskog broja α stupnja $d \geq 2$ je $\mu(\alpha) = 2$. Rothov teorem, kao i Thueov teorem nije eksplicitan.

Tablica 3.1: Eksplicitne mjere iracionalnosti $\left|\sqrt[n]{d} - p/q\right| \geq C/q^{-\mu}$

$\sqrt[n]{d}$	C	μ	$\sqrt[n]{d}$	C	μ	$\sqrt[n]{d}$	C	μ
$\sqrt[3]{2}$	0.25	2.47	$\sqrt[3]{62}$	0.04	2.50	$\sqrt[5]{18}$	0.21	4.29
$\sqrt[3]{3}$	0.39	2.76	$\sqrt[3]{63}$	0.02	2.43	$\sqrt[5]{22}$	0.14	4.91
$\sqrt[3]{5}$	0.29	2.80	$\sqrt[3]{65}$	0.02	2.43	$\sqrt[5]{28}$	0.05	3.41
$\sqrt[3]{6}$	0.01	2.35	$\sqrt[3]{66}$	0.04	2.50	$\sqrt[5]{30}$	0.02	3.04
$\sqrt[3]{7}$	0.08	2.70	$\sqrt[3]{67}$	0.06	2.56	$\sqrt[5]{31}$	0.01	2.83
$\sqrt[3]{10}$	0.15	2.45	$\sqrt[3]{68}$	0.08	2.60	$\sqrt[5]{33}$	0.01	2.82
$\sqrt[3]{11}$	0.22	2.91	$\sqrt[3]{70}$	0.12	2.68	$\sqrt[5]{34}$	0.02	3.02
$\sqrt[3]{12}$	0.28	2.95	$\sqrt[3]{76}$	0.10	2.54	$\sqrt[5]{37}$	0.05	3.48
$\sqrt[3]{13}$	0.35	2.86	$\sqrt[3]{78}$	0.03	2.60	$\sqrt[5]{39}$	0.08	2.91
$\sqrt[3]{15}$	0.19	2.54	$\sqrt[3]{83}$	0.10	2.72	$\sqrt[5]{40}$	0.09	3.90
$\sqrt[3]{17}$	0.01	2.22	$\sqrt[3]{84}$	0.37	2.92	$\sqrt[5]{42}$	0.11	4.19
$\sqrt[3]{19}$	0.02	2.30	$\sqrt[3]{90}$	0.09	2.41			
$\sqrt[3]{20}$	0.01	2.23	$\sqrt[3]{91}$	0.01	2.29	$\sqrt[7]{5}$	0.25	4.43
$\sqrt[3]{22}$	0.08	2.31				$\sqrt[7]{10}$	0.38	5.19
$\sqrt[3]{26}$	0.03	2.53	$\sqrt[4]{5}$	0.03	2.77	$\sqrt[7]{11}$	0.40	3.34
$\sqrt[3]{28}$	0.03	2.52	$\sqrt[4]{14}$	0.06	3.78	$\sqrt[7]{12}$	0.42	3.88
$\sqrt[3]{30}$	0.10	2.72	$\sqrt[4]{15}$	0.03	3.27	$\sqrt[7]{13}$	0.44	4.91
$\sqrt[3]{31}$	0.14	2.97	$\sqrt[4]{17}$	0.03	3.24	$\sqrt[7]{17}$	0.03	5.20
$\sqrt[3]{37}$	0.01	2.27	$\sqrt[4]{18}$	0.05	3.67	$\sqrt[7]{23}$	0.43	6.03
$\sqrt[3]{39}$	0.09	2.21	$\sqrt[4]{37}$	0.33	3.34	$\sqrt[7]{45}$	0.27	5.10
$\sqrt[3]{42}$	0.13	2.46	$\sqrt[4]{39}$	0.005	2.52			
$\sqrt[3]{43}$	0.01	2.32				$\sqrt[11]{48}$	0.42	5.05
$\sqrt[3]{44}$	0.22	2.87	$\sqrt[5]{3}$	0.24	3.61			
$\sqrt[3]{52}$	0.26	2.97	$\sqrt[5]{6}$	0.43	3.33	$\sqrt[13]{6}$	0.14	4.22
$\sqrt[3]{58}$	0.12	2.71	$\sqrt[5]{10}$	0.41	3.92	$\sqrt[13]{20}$	0.25	5.87
$\sqrt[3]{60}$	0.08	2.61	$\sqrt[5]{11}$	0.38	4.23			
$\sqrt[3]{61}$	0.06	2.56	$\sqrt[5]{15}$	0.28	4.27	$\sqrt[17]{50}$	0.25	6.96

Bibliografija

[1] D. Duverney, *Number Theory: An Elementary Introduction Through Diophantine Problems*, World Scientific, 2010.

[2] G. A. Baker, Jr., *Essential of Padé Approximants*, Academic Press,INC, New York,1975.

[3] A. Dujella, *Uvod u teoriju brojeva*, skripta, PMF - Matematički odjel, Zagreb

Sažetak

U ovom radu dan je uvod u temu Padéovih aproksimanata i diofantskih aproksimacija. Opisana je problematika iracionalnosti i diofantskih aproksimacija, te Padéovi aproksimanti analitičkih funkcija, čije tablice za binomne funkcije $f(x) = (1 - x)^{\alpha}, \alpha \in \mathbb{Z}$ rješavamo pomoću Gaussove hipergeometrijske funkcije. Obrađeni su pojam algebarskih brojeva te mjere iracionalnosti. Dokazan je Liouvilleov teorem.

Summary

Padé approximants and diophantine approximations

In this thesis, an introduction to the Padé approximants and diophantine approximations is given. We describe the problem of irrationality and diophantine approximation, and Padé approximants of analytical function, whose table for binomial function is computed by Gauss hypergeometric functions. The notions of algebraic numbers and irrationality measures are studied. The proof of the Liouville theorem is presented.

Životopis

Rođena sam 13.11.1984. u Šibeniku. Roditelji su mi Svetin i Marija Plavčić r. Dražić. Osnovnu školu sam pohađala u Vrpolju. Za vrijeme trajanja osnovne škole živjela sam na Vrsnom s bakom, roditeljima, dvijema sestrama Antonijom i Kristinom te bratom Ivanom. Nakon toga do 19. godine u Ražinama. Godine 2003. završila sam Gimnaziju Antuna Vrančića u Šibeniku te iste godine upisala Preddiplomski sveučilišni studij Matematike (inženjerski smjer) na Prirodoslovno-matematičkom fakultetu- Matematičkom odsjeku u Zagrebu. Godine 2007. sam se udala za Jerka Maršića i rodila nam prvog sina (Mateja). 2008. godine prebacila sam se na Preddiplomski sveučilišni studij Matematike (nastavnički smjer) kojeg sam završila 2011. godine. U međuvremenu (2010.) sam rodila i drugog sina (Tina). Diplomski sveučilišni studij Matematike (nastavnički smjer) upisala sam na Prirodoslovno-matematičkom fakultetu-Matematičkom odsjeku u Zagrebu 2011. godine i upravo ga završavam.