Primjena linearnih formi u logaritmima na rješavanje diofantskih jednadžbi

Ilić, Marina

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Marina Ilić

PRIMJENA LINEARNIH FORMI U LOGARITMIMA NA RJEŠAVANJE DIOFANTSKIH JEDNADŽBI

Diplomski rad

Voditelj rada:
prof.dr.sc. Alan Filipin

Zagreb, studeni, 2018.

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. _____

Sadržaj

Uvod

Algebarska jednadžba dviju ili više varijabli s cjelobrojnim koeficijentima kod koje se traže cjelobrojna ili racionalna rješenja naziva se diofantska jednadžba. Diofant je prvi sustavno proučavao jednadžbe s više nepoznanica i tražio pozitivna racionalna rješenja te su po njemu takve jednadžbe dobile ime. Najznačajniji je matematičar postklasičnog razdoblja grčke matematike i posljednji veliki europski matematičar prije Fibonaccija. Najpoznatiji je po svojoj knjizi *Arithmetica* koja se sastoji od 150 algebarskih zadataka u 13 knjiga. Šest od tih 13 knjiga je sačuvano na grčkom i četiri na arapskom jeziku. Neki od Diofantovih zadataka još ni danas nisu riješeni, a kopije i prijevodi *Aritmetike* imale su velik utjecaj na mnoge matematičare koji su djelovali poslije njega.

Razlikujemo linearne i nelinearne diofantske jednadžbe, a za određivanje rješenja je potrebno pronaći efikasne metode i algoritme rješavanja. U ovom radu ćemo se baviti primjenom linearnih formi u logaritmima na rješavanje diofantskih jednadžbi. Razvoj teorije linearnih formi u logaritmima motiviran je sedmim Hilbertovim problemom, a kod primjene na rješavanje diofantskih jednadžbi želimo najprije "velika" rješenja diofantske jednadžbe pridružiti "malim" vrijednostima određene linearne forme u logaritmima. To nam daje gornju ogradu za vrijednosti linearne forme koje odgovaraju rješenjima jednadžbe. Nakon toga uspoređujemo dobivenu gornju ogradu s donjom ogradom iz Bakerove teorije te na taj način dolazimo do gornje ograde za veličinu rješenja diofantske jednadžbe. Dobivena gornja ograda je obično jako velika pa ćemo koristiti neke metode iz diofantskih aproksimacija za redukciju tih ograda. Nadalje, na primjerima simultanih pellovskih jednadžbi i Fibonaccijevog niza ćemo pokazati kako te metode funkcioniraju.

Poglavlje 1

Osnovni pojmovi i definicije

1.1 Kvadratno polje

U ovom radu bavit ćemo se Pellovim jednadžbama koje su u uskoj vezi s pronalaženjem jedinica u realnim kvadratnim poljima. Najprije ćemo definirati algebarske i transcedentne brojeve, a zatim i kvadratna polja.
Prirodan broj α je (potpun) kvadrat, ako se može zapisati u obliku n^2, $n \in \mathbb{N}$. Kažemo da je α kvadratno slobodan ako je 1 najveći kvadrat koji dijeli α.

Definicija 1.1.1. *Algebarski broj α je kompleksan broj koji je korijen polinoma $f(x)$, različitog od nulpolinoma, s racionalnim koeficijentima. Kompleksni brojevi koji nisu algebarski zovu se transcedentalni.*

Definicija 1.1.2. *Minimalni polinom p algebarskog broja α je normirani polinom najmanjeg mogućeg stupnja takav da vrijedi $p(\alpha) = 0$. Stupanj algebarskog broja je stupanj njegovog minimalnog polinoma.*

Primjer 1.1.3. *Odredimo minimalni polinom od* $x = \dfrac{10^{2/3} - 1}{\sqrt{-3}}$.

Rješenje:

Najprije zapišimo zadani broj u obliku: $\sqrt{-3}x + 1 = 10^{2/3}$. Tada imamo

$$\left(\sqrt{-3}x + 1\right)^3 = 100.$$

Kubiranjem dobivamo

$$3\sqrt{-3}x^3 + 9x^2 - 3\sqrt{-3}x + 99 = 0$$

$$\Leftrightarrow x^3 - \sqrt{-3}x^2 - x - 11\sqrt{-3} = 0.$$

Sada imamo minimalni polinom od x:

$$P(x) = \left((x^3 - x) - \sqrt{-3}(x^2 + 11)\right)\left((x^3 - x) + \sqrt{-3}(x^2 + 11)\right) = x^6 + x^4 + 67x^2 + 363.$$

Definicija 1.1.4. *Za algebarski broj α kažemo da je algebarski cijeli broj ako je α korijen nekog normiranog polinoma s cjelobrojnim koeficijentima.*

Definicija 1.1.5. *Neka je d kvadratno slobodan cijeli broj i $d \neq 1$. Kvadratno polje $\mathbb{Q}(\sqrt{d})$ je skup svih brojeva oblika $u + v\sqrt{d}, u, v \in \mathbb{Q}$, uz uobičajene operacije zbrajanja i množenja kompleksnih brojeva.*

Definicija 1.1.6. *Jedinica (ili invertibilni element) u $\mathbb{Q}(\sqrt{d})$ je algebarski cijeli broj ε sa svojstvom da je $\frac{1}{\varepsilon}$ također algebarski cijeli broj.*

Za svaki element $\alpha = u + v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ definira se norma od α kao $N(\alpha) = u^2 - dv^2$. Dakle, $N(\alpha) = \alpha\overline{\alpha}$, gdje je $\overline{\alpha} = u - v\sqrt{d}$ konjugat od α.
Za normu vrijede sljedeća svojstva:

- $N(\alpha\beta) = N(\alpha)N(\beta)$
- $N(\alpha) = 0 \Leftrightarrow \alpha = 0$
- Ako je α algebarski cijeli broj u $\mathbb{Q}(\sqrt{d})$, onda je $N(\alpha) \in \mathbb{Z}$
- Neka je γ algebarski cijeli broj u $\mathbb{Q}(\sqrt{d})$. Tada je γ jedinica ako i samo ako je $N(\gamma) = \pm 1$.

Cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ čine prsten. Prsten cijelih brojeva u kvadratnim poljima možemo opisati u ovisnosti o d:

Teorem 1.1.7. *Ako je $d \equiv 2$ ili $3 \pmod 4$, onda su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ svi brojevi oblika $u + v\sqrt{d}$, $u, v \in \mathbb{Z}$. Ako je $d \equiv 1 \pmod 4$, onda su algebarski cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ svi brojevi oblika $s + t \cdot \dfrac{1 + \sqrt{d}}{2}$, $s, t \in \mathbb{Z}$.*

Dokaz. Neka je $\alpha = u + v\sqrt{d}$ algebarski cijeli broj u $\mathbb{Q}(\sqrt{d})$ te neka je

$$a = 2u, \;\; b = 2v, \;\; c = N(\alpha) = u^2 - dv^2.$$

Tada je α nultočka polinoma $f(x) = x^2 - ax + c$. Pri tome, racionalni brojevi a i c moraju biti cijeli. Imamo $db^2 = a^2 - 4c$ i budući da je d kvadratno slobodan, vidimo da je i $b \in \mathbb{Z}$. Neka je sada $d \equiv 2$ ili $3 \pmod 4$.
Iz $a^2 \equiv b^2 d \pmod 4$, $a^2 \equiv 0$ ili $1 \pmod 4$, $b^2 d \equiv 0, 2$ ili $3 \pmod 4$, slijedi da su a i b parni brojevi pa su $u, v \in \mathbb{Z}$.
Ako je $d \equiv 1 \pmod 4$, onda iz $a^2 \equiv b^2 \pmod 4$ slijedi da su a i b iste parnosti. Stoga je broj $u - v = \frac{1}{2}(a - b)$ cijeli. Stavimo $s = u - v$ i $t = 2v$. Tada je $u + v\sqrt{d} = s + t \cdot \frac{1 + \sqrt{d}}{2}$, $s, t \in \mathbb{Z}$. □

1.2 Verižni razlomci

Kasnije ćemo pokazati kako rješenja Pellove jednadžbe možemo generirati ukoliko znamo njeno fundamentalno rješenje. Za pronalaženje fundamentalnog rješenja su nam poznate razne metode, a za jednu od metoda su nam potrebni verižni razlomci. Naime, konvergente razvoja u verižni razlomak iracionalnog broja α su jako dobre aproksimacije (iracionalnog broja α) racionalnim brojem. Stoga, navedimo osnovne činjenice o verižnim razlomcima.

Definicija 1.2.1. *Konačni verižni razlomak je izraz oblika:*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

gdje je $a_0 \in \mathbb{R}$, $a_i > 0$ *za* $1 \leqslant i \leqslant n$.

Verižni razlomak kraće zapisujemo kao $[a_0, a_1, a_2, ..., a_n]$. Za prethodni izraz kažemo da je *jednostavan verižni razlomak* ukoliko je $a_0 \in \mathbb{Z}$, a $a_1, ..., a_n \in \mathbb{N}$. Brojevi $a_0, a_1, a_2, ...$ zovu se *parcijalni kvocijenti*, a definiraju se na sljedeći način:
Neka je α proizvoljan realan broj. Stavimo: $a_0 = \lfloor \alpha \rfloor$. Ako je $a_0 \neq \alpha$, zapišimo α u obliku $\alpha = a_0 + \frac{1}{\alpha_1}$, tako da je $\alpha_1 > 1$ i stavimo da je $a_1 = \lfloor \alpha_1 \rfloor$. Ako je $a_1 \neq \alpha_1$, zapišimo α_1 u obliku $\alpha_1 = a_1 + \frac{1}{\alpha_2}$ tako da je $\alpha_2 > 1$ i stavimo da je $a_2 = \lfloor \alpha_2 \rfloor$. Ovaj algoritam možemo

nastaviti sve dok je $a_n \neq \alpha_n$ za neki n. Ako je $a_n = \alpha_n$ za neki n, onda je α racionalan broj. Dakle, razvoj u jednostavni verižni razlomak broja α je konačan ako i samo ako je α racionalan broj.

Definirajmo sada konvergente verižnog razlomka:

Definicija 1.2.2. *Verižni razlomak $c_k = [a_0, a_1, a_2, ..., a_k]$ za $0 \leqslant k \leqslant n$ se zove k-ta konvergenta od $[a_0, a_1, a_2, ..., a_n]$.*

Brojnici i nazivnici konvergenti zadovoljavaju rekurzije koje se lako dokazuju matematičkom indukcijom:

$$p_k = a_k p_{k-1} + p_{k-2}, \quad p_0 = a_0, \quad p_1 = a_0 a_1 + 1 \tag{1.1}$$

$$q_k = a_k q_{k-1} + q_{k-2}, \quad q_0 = 1, \quad q_1 = a_1. \tag{1.2}$$

Matematičkom indukcijom ćemo dokazati i sljedeći teorem koji povezuje konvergente sa susjednim indeksima. Također, dogovorno uzimamo:

$$p_{-2} = 0, \;\; p_{-1} = 1, \;\; q_{-2} = 1, \;\; q_{-1} = 0.$$

Naime, lako se provjeri da uz ovaj dogovor vrijede prethodne relacije.

Teorem 1.2.3. *Za sve $n \geqslant -1$ vrijedi: $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$*

Dokaz. 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 neki $n - 1$. Tada je:

$$q_n p_{n-1} - p_n q_{n-1} = (a_n q_{n-1} + q_{n-2})p_{n-1} - (a_n p_{n-1} + p_{n-2})q_{n-1} = -(q_{n-1}p_{n-2} - p_{n-1}q_{n-2})$$

$$= -(-1)^{n-1} = (-1)^n$$

□

Sada ćemo još pokazati da za konvergente verižnog razlomka vrijede određene nejednakosti. Za dokaz tog teorema ćemo koristiti prethodni teorem i ranije spomenute rekurzije.

Teorem 1.2.4. *Vrijede sljedeće nejednakosti:*

1. $\dfrac{p_0}{q_0} < \dfrac{p_2}{q_2} < \dfrac{p_4}{q_4} < ...$
2. $\dfrac{p_1}{q_q} > \dfrac{p_3}{q_3} > \dfrac{p_5}{q_5} > ...$
3. *Ako je n paran i m neparan, onda vrijedi:* $\dfrac{p_n}{q_n} < \dfrac{p_m}{q_m}$.

Dokaz. Iz prethodnog teorema i rekurzija slijedi:

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

Sada za n paran imamo: $\frac{p_{n-2}}{q_{n-2}} < \frac{p_n}{q_n}$, a za n neparan imamo: $\frac{p_{n-2}}{q_{n-2}} > \frac{p_n}{q_n}$.
Dokažimo jos treću tvrdnju. Neka je $n < m$. Budući da je $\frac{p_n}{q_n} \leqslant \frac{p_{m-1}}{q_{m-1}}$, dovoljno je pokazati da vrijedi $\frac{p_{m-1}}{q_{m-1}} < \frac{p_m}{q_m}$. Ova nejednakost je točna jer koristeći prethodni teorem imamo:

$$q_m p_{m-1} - p_m q_{m-1} = (-1)^m = -1 < 0.$$

Analogno se pokazuje i za slučaj $n > m$. □

Definirajmo sada i beskonačne verižne razlomke koji predstavljaju iracionalne brojeve.

Definicija 1.2.5. *Ako je α iracionalan broj, onda uvodimo oznaku*

$$\lim_{n\to\infty} [a_0, a_1, ..., a_n] = [a_o, a_1, a_2, ...].$$

Ako je $\alpha = [a_o, a_1, a_2, ...]$, onda ovaj izraz zovemo razvoj od α u beskonačni verižni razlomak.

Definicija 1.2.6. *Za beskonačni verižni razlomak $[a_o, a_1, a_2, ...]$ kažemo da je periodski ako postoje cijeli brojevi $k \geqslant 0, m \geqslant 1$ takvi da je $a_{m+n} = a_n$ za sve $n \geqslant k$. U tom slučaju verižni razlomak pišemo u obliku*

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

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

Definicija 1.2.7. *Za iracionalan broj α kažemo da je kvadratna iracionalnost ako je α korijen kvadratne jednadžbe s racionalnim koeficijentima.*

Navedimo algoritam za razvoj kvadratnih iracionalnosti u verižni razlomak:
Neka je α kvadratna iracionalnost. Prikažimo je u obliku $\frac{s_0 + \sqrt{d}}{t_0}$ gdje su $d, s_o, t_o \in \mathbb{Z}$, $t_0 \neq 0, d \neq 0, t_0 \mid (d - s_0^2)$, a t_0 i s_0 su jedinstveno određeni. Ako je $\alpha = \sqrt{d}$, onda je $s_0 = 0, t_0 = 1$. Sada parcijalne kvocijente a_i računamo rekurzivno na sljedeći način:

$$a_i = \left\lfloor \frac{s_i + a_0}{t_i} \right\rfloor, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}.$$

Primjer 1.2.8. *Razvijmo broj* $\sqrt{15}$ *u jedinstveni verižni razlomak.*

Rješenje:

$\sqrt{15} \approx 3.8729833$

$$\begin{array}{lll} s_0 = 0, & t_0 = 1, & a_0 = \lfloor \sqrt{15} \rfloor = 3, \\ s_1 = a_0 t_0 - s_0 = 3, & t_1 = \dfrac{15 - s_1^2}{t_0} = 6, & a_1 = \left\lfloor \dfrac{s_1 + a_0}{t_1} \right\rfloor = 1, \\ s_2 = 3, & t_2 = 1, & a_2 = 6, \\ s_3 = 3, & t_3 = 6. & \end{array}$$

Dakle, $(s_3, t_3) = (s_1, t_1) = (3, 6)$ i time zaustavljamo algoritam te zapisujemo:

$$\sqrt{15} = [3, \overline{1, 6}].$$

Teorem 1.2.9. *Razvoj u jednostavni verižni razlomak realnog broja* α *je periodski ako i samo ako je* α *kvadratna iracionalnost.*

Dokaz teorema možemo pogledati u [2]

Primjer 1.2.10. *Neka je* $\alpha = [\overline{3, 1, 2}]$. *Nađimo kvadratnu iracionalnost koju predstavlja* α.

Rješenje:

Imamo:

$$3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\alpha}}} = 3 + \frac{2\alpha + 1}{3\alpha + 1}.$$

Množenjem s $(3\alpha + 1)$ dobivamo kvadratnu jednadžbu $3\alpha^2 - 10\alpha - 4 = 0$.
Rješenja dobivene kvadratne jednadžbe su

$$\alpha_{1,2} = \frac{5 \pm \sqrt{37}}{3},$$

a kako je $\alpha > 0$ imamo

$$\alpha = \frac{5 + \sqrt{37}}{3}.$$

Definicija 1.2.11. *Za kvadratnu iracionalnost kažemo da je reducirana ako vrijedi* $\alpha > 1$ *i* $-1 < \overline{\alpha} < 0$.

Teorem 1.2.12. *Kvadratna iracionalnost α ima čisto periodski razvoj u jednostavni verižni razlomak ako i samo ako je reducirana.*

Dokaz. Neka je $\alpha > 1$ i $-1 < \overline{\alpha} < 0$. Stavimo $\alpha_0 = \alpha$ te definirajmo α_i rekurzivno sa $\dfrac{1}{\alpha_{i+1}} = \alpha_i - a_i$. Tada je

$$\frac{1}{\overline{\alpha_{i+1}}} = \overline{\alpha_i} - a_i. \tag{1.3}$$

Sada je $a_i \geqslant 1$ za sve $i \geqslant 0$ (zbog $\alpha > 1$). Zbog toga, ako je $\overline{\alpha_i} < 0$, onda je $\dfrac{1}{\overline{\alpha_{i+1}}} < -1$. Dakle, $-1 < \overline{\alpha_{i+1}} < 0$. Budući da je $-1 < \overline{\alpha_0} < 0$, indukcijom slijedi da je $-1 < \overline{\alpha_i} < 0$ za sve $i \geqslant 0$. Sada iz (1.3) slijedi

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

Iz Teorema 1.2.9. slijedi da postoje prirodni brojevi takvi da je $j < k$ i $\alpha_j = \alpha_k$. Sada je $\overline{\alpha_j} = \overline{\alpha_k}$ te

$$a_{j-1} = \left\lfloor -\frac{1}{\overline{\alpha_j}} \right\rfloor = \left\lfloor -\frac{1}{\overline{\alpha_k}} \right\rfloor = a_{k-1},$$

$$\alpha_{j-1} = a_{j-1} + \frac{1}{\alpha_j} = a_{k-1} + \frac{1}{\alpha_k} = \alpha_{k-1}.$$

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. $\alpha = [\overline{a_0, a_1, ..., a_{k-j}}]$.
Obrnuto, pretpostavimo da je razvoj od α čisto periodski,

$$\alpha = [\overline{a_0, a_1, ..., a_{n-1}}], \quad a_0, ..., a_{n-1} \in \mathbb{N}.$$

Imamo: $\alpha > a_0 \geqslant 1$ te

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

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 $\overline{\alpha}$. 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. Imamo:

$$f(0) = -p_{n-2} < 0,$$

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

□

Poglavlje 2

Diofantske aproksimacije

Glavni problem u teoriji diofantskih aproksimacija jest problem aproksimacije iracionalnih brojeva racionalnim. U prethodnom poglavlju smo govorili o razvoju iracionalnih brojeva u verižne razlomke pa se postavlja pitanje koliko dobro konvergente aproksimiraju iracionalan broj α. Dirichlet je dao prvi važan rezultat za problem aproksimacije iracionalnih brojeva. Također ćemo promatrati problem aproksimacije algebarskih brojeva racionalnima.

2.1 Aproksimacija iracionalnih brojeva

Za dani realni broj α s $\lfloor\alpha\rfloor$ ćemo označavati *cijeli dio* od α, a s $\{\alpha\} := \alpha - \lfloor\alpha\rfloor$ ćemo označavati *razlomljeni dio* od α koji zadovoljava $0 \leqslant \alpha < 1$.

Teorem 2.1.1 (Dirichlet, 1842.)**.** *Neka su α i Q realni brojevi i $Q > 1$. Tada postoje cijeli brojevi p, q takvi da je $1 \leqslant q < Q$ i*

$$|\alpha q - p| \leqslant \frac{1}{Q}.$$

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

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

Svi ovi brojevi leže u segmentu $[0, 1]$. Podijelimo taj segment na Q disjunktnih podintervala duljine $\frac{1}{Q}$:

$$\left[0, \frac{1}{Q}\right\rangle, \left[\frac{1}{Q}, \frac{2}{Q}\right\rangle, ..., \left[\frac{Q-1}{Q}, 1\right].$$

Prema Dirichletovom principu, barem jedan podinterval sadrži dva (ili više) od gornjih $Q+1$ brojeva. Dakle, postoje cjeli brojevi r_1, r_2, s_1, s_2 takvi da je $0 \leqslant r_i < Q$, $r_1 \neq r_2$ i da vrijedi:

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

Pretpostavimo da je $r_1 > r_2$ i stavimo $q = r_1 - r_2$, $p = s_1 - s_2$. Tada je $1 \leqslant q < 0$ i $|\alpha q - p| \leqslant \frac{1}{Q}$ čime je tvrdnja teorema dokazana za slučaj kad je Q prirodan broj.
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 $1 \leqslant q < Q'$ i $|\alpha q - p| \leqslant \frac{1}{Q'}$. Sada je $|\alpha q - p| \leqslant \frac{1}{Q}$, a $1 \leqslant q < Q'$ povlači da je $1 \leqslant q < \lfloor Q \rfloor$, odnosno $1 \leqslant q < Q$. □

Korolar 2.1.2. *Ako je α iracionalan broj, onda postoji beskonačno mnogo relativno prostih cijelih brojeva p i q takvih da je*

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

Dokaz. Tvrdnja Teorema 2.1.1. očito vrijedi i ukoliko zahtjevamo da su p i q relativno prosti. Dakle, za $Q > 1$ postoje relativno prosti brojevi p, q takvi da je $\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{Qq} < \frac{1}{q^2}$. Budući da je Q iracionalan, to je $\alpha q - p \neq 0$.
Pretpostavimo da postoji samo konačno mnogo racionalnih brojeva $\frac{p}{q}$ koji zadovoljavaju $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$. Neka su to brojevi $\frac{p_j}{q_j}$, $j = 1, .., n$. Izaberimo prirodan broj m takav da je $\frac{1}{m} < \left|\alpha q_j - p_j\right|$. Primijenimo sada Teorem 2.1.1. za $Q = m$ pa dobivamo racionalan broj koji zadovoljava $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$ i za koji vrijedi $\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{m}$. Prema tome, $\frac{p}{q}$ je različit od $\frac{p_1}{q_1}, ..., \frac{p_n}{q_n}$, što je kontradikcija. □

Sada ćemo dokazati Legendreov teorem, iz kojeg će slijediti da su sva rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ sadržana u konvergentama razvoja u verižni razlomak broja $\sqrt{d}$. Za dokaz će nam biti potrebna sljedeća lema:

Lema 2.1.3. *Neka je α iracionalan broj i neka su $c_k = \frac{p_k}{q_k}$, $k \geqslant 0$ konvergente razvoja u verižni razlomak broja α. Ako su $p, q \in \mathbb{Z}, q > 0$ i k prirodan broj tako da vrijedi:*

$$|\alpha q - p| < |\alpha q_k - p_k|,$$

onda je $q \geqslant q_{k+1}$.

Dokaz prethodne leme se nalazi u [5]

Teorem 2.1.4 (Legendre)**.** *Ako je α iracionalan broj i $\frac{p}{q}$ racionalan broj gdje je $q > 0$ i takav da vrijedi*

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

onda je $\frac{p}{q}$ konvergenta razvoja u verižni razlomak broja α.

Dokaz. Pretpostavimo suprotno, odnosno da $\frac{p}{q}$ nije konvergenta od α. Neka je k najveći prirodan broj takav da vrijedi $q \geqslant q_k$. Takav k uvijek postoji jer je $q_0 = 1$ i $\lim_{k\to\infty} q_k = \infty$. S obzirom da vrijedi $q_k \leqslant q < q_{k+1}$, i koristeći prethodnu lemu zaključujemo da vrijedi:

$$|q_k\alpha - p_k| \leqslant |q\alpha - p| = q\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q},$$

odnosno

$$q\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2qq_k}.$$

Kako je $\frac{p}{q} \neq \frac{p_k}{q_k}$ imamo $|qp_k - pq_k| \geqslant 1$ što povlači:

$$\frac{1}{qq_k} \leqslant \frac{|qp_k - pq_k|}{qq_k} = \left|\frac{p_k}{q_k} - \frac{p}{q}\right| \leqslant \left|\frac{p_k}{q_k} - \alpha\right| + \left|\alpha - \frac{p}{q}\right| < \frac{1}{2qq_k} + \frac{1}{2q^2},$$

odnosno

$$\frac{1}{2qq_k} < \frac{1}{2q^2}.$$

Iz prethodne nejednakosti slijedi da je $q_k > q$ što je kontradikcija s pretpostavkom. □

Teorem 2.1.5 (Borel)**.** *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 $\alpha = [a_0, a_1, ...]$, $\alpha_i = [a_i, a_{i+1}, ...]$, $\beta_i = \frac{q_{i-2}}{q_{i-1}}$ za $i \geqslant 1$. Imamo $\alpha = [a_0, a_1, ..., a_n, \alpha_{n+1}]$, pa je

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

Stoga je

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

Još moramo pokazati da ne postoji prirodan broj n takav da je za $i = n-1, n, n+1$ vrijedi:

$$\alpha_i + \beta_i \leqslant \sqrt{5}.$$

Pretpostavimo da je prethodna nejednakost ispunjena za $n-1, n$. Tada iz

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

slijedi

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

Stoga je $1 = \alpha_n \cdot \dfrac{1}{\alpha_n} \leqslant \left(\sqrt{5} - \beta_n\right)\left(\sqrt{5} - \dfrac{1}{\beta_n}\right)$, što je ekvivalentno sa $\beta_n^2 - \sqrt{5}\beta_n + 1 \leqslant 0$. Odavde slijedi da je $\beta_n \geqslant \dfrac{\sqrt{5}-1}{2}$. Budući da je β_n racionalan, imamo da je $\beta_n > \dfrac{\sqrt{5}-1}{2}$. Ako je nejednakost $\alpha_i + \beta_i \leqslant \sqrt{5}$ ispunjena za $i = n, n+1$, onda je $\beta_{n+1} > \dfrac{\sqrt{5}-1}{2}$. Stoga dobivamo

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

što je kontradikcija. □

Tvrdnja sljedećeg teorema slijedi direktno iz prethodnog teorema.

Teorem 2.1.6 (Hurwitz)**.** *Za svaki iracionalan broj α postoji beskonačno mnogo racionalnih brojeva $\dfrac{p}{q}$ takvih da je*

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

2.2 Aproksimacija algebarskih brojeva

Za aproksimaciju algebarskih brojeva najznačajniji su Liouvilleov i Rothov teorem. Liouville je prvi koji je dokazao egzistenciju transcendentnih brojeva.

Teorem 2.2.1 (Liouville)**.** *Neka je α realan algebarski broj stupnja d. Tada postoji konstanta $c(\alpha) > 0$ takva da za svaki racionalni broj $\frac{p}{q} \neq \alpha$, gdje je $q > 0$ vrijedi:*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}.$$

Dokaz. Dokaz ćemo podijeliti u tri dijela:

1. Neka je $g(x)$ minimalni polinom od α. Odaberimo prirodan broj m tako da polinom $P(x) = m \cdot g(x)$ ima relativno proste cjelobrojne koeficijente. To znači da je m najmanji zajednički višekratnik nazivnika koeficijenata polinoma $g(x)$, tj. ako imamo:

   $$g(x) = x^2 - \frac{1}{3}x + \frac{1}{4},$$

   tada je $m = 12$ i imamo: $P(x) = 12x^2 - 4x + 3$.

2. Bez smanjenja općenitosti možemo pretpostaviti da je $\left|\alpha - \frac{p}{q}\right| \leqslant 1$ (inače možemo staviti $c(\alpha) = 1$). Razvijemo li $P(x)$ u Taylorov red oko α, dobivamo:

   $$\left|P\left(\frac{p}{q}\right)\right| = \left|\sum_{i=1}^{d} \left(\frac{p}{q} - \alpha\right)^i \frac{1}{i!} P^{(i)}(\alpha)\right| < \frac{1}{c(\alpha)} \cdot \left|\alpha - \frac{p}{q}\right|,$$

   gdje je $c(\alpha) = \dfrac{1}{2\displaystyle\sum_{i=1}^{d} \frac{1}{i!}\left|P^{(i)}(\alpha)\right|}$.

3. Budući da je polinom $P(x)$ ireducibilan, to je $P\left(\frac{p}{q}\right) \neq 0$. Stoga je broj $q^d \left|P\left(\frac{p}{q}\right)\right|$ prirodan pa je $\left|P\left(\frac{p}{q}\right)\right| \geqslant \frac{1}{q^d}$. Usporedimo li nejednakosti dobivene u (2) i (3) dobivamo tvrdnju teorema.

□

Posljedica Liouvilleovog teorema je sljedeća: Ako je α algebarski broj stupnja $d \geqslant 2$ i $\mu > d$, onda nejednakost

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

ima konačno mnogo rješenja u racionalnim brojevima $\frac{p}{q}$.

Teorem 2.2.2 (Roth)**.** *Ako je α algebarski broj i $\delta > 0$, onda postoji samo konačno mnogo racionalnih brojeva $\frac{p}{q}$ za koje vrijedi:*

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

Ideja dokaza Rothovog teorema je modificirati korake u Liouvilleovom teoremu. Detaljan dokaz i rezultati vezani uz Rothov teorem mogu se vidjeti u [11]

Napomena 2.2.3.

- *Tvrdnja Rothovog teorema je istinita i trivijalna za $\alpha \in \mathbb{Q}\backslash\mathbb{R}$*
- *Za dani algebarski broj α stupnja $\geqslant 3$ nepoznato je postoji li konstanta $c > 0$ takva da vrijedi*

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

  za svaki racionalni broj $\frac{p}{q}$. Slutnja je da to ne vrijedi.
- *Slutnja je da vrijedi jača tvrdnja od Rothovog teorema, odnosno da*

  $$\left|\alpha - \frac{p}{q}\right| < \frac{1}{y^2 (\log y)^k},$$

  ima konačno mnogo rješenja za $k > 1$.

2.3 Baker-Davenportova redukcija

Baker-Davenportovu redukciju ćemo koristiti kod smanjivanja gornje ograde za veličinu rješenja diofantske jednadžbe. Sljedeća lema je verzija Baker-Davenportove redukcije koju ćemo mi koristiti u nastavku rada.

Lema 2.3.1. *Neka su κ, μ realni brojevi i N prirodan broj. Neka je $\frac{p}{q}$ konvergenta razvoja u verižni razlomak broja κ takva da vrijedi $q > 6N$ te neka je $\varepsilon = \|\mu q\| - N \cdot \|\kappa q\|$, gdje je sa $\|.\|$ označena udaljenost do najbližeg cijelog broja. Ako je $\varepsilon > 0$, onda nejednadžba*

$$n\kappa - m + \mu < A \cdot B^{-n},$$

gdje su $A > 0$, $B > 1$ realni brojevi, nema rješenja u prirodnim brojevima m i n takvima da vrijedi

$$\frac{\log\left(\frac{Aq}{\varepsilon}\right)}{\log B} \leqslant n \leqslant N.$$

Dokaz. Neka je $1 \leqslant n \leqslant N$. Tada vrijedi

$$n(\kappa q - p) + np - mq + \mu q < qAB^{-n},$$

odnosno

$$qAB^{-n} > |\mu q - (mq - np)| - n\|\kappa q\| \geqslant \|\kappa q\| - N\|\kappa q\| = \varepsilon,$$

iz čega zaključujemo

$$n < \frac{\log\left(\frac{Aq}{\varepsilon}\right)}{\log B}.$$

□

Napomena 2.3.2. *Uvjet $q > 6N$ u lemi je donekle proizvoljan. Naime, s jedne strane želimo biti što sigurniji da će vrijediti $\varepsilon > 0$, a s druge želimo da nam q bude što manji kako bi nova ograda bila što manja. Iz svojstva konvergenti vrijedi $\|\kappa q\| < \frac{1}{q}$ dok o $\|\kappa q\|$ općenito ne znamo ništa. Zato je razumno uzeti barem $q > 2N$, a uvjet $q > 6N$ se pokazao eksperimentalno kao dobar izbor.*
Također, ako nam uvjet $\varepsilon > 0$ nije zadovoljen, možemo pokušati uzeti sljedeću konvergentu i vidjeti hoće li nam za nju uvjet biti zadovoljen.

Poglavlje 3

Pellova jednadžba

3.1 Jednadžba $x^2 - dy^2 = 1$

Pellova jednadžba je specijalni oblik diofantske jednadžbe drugog stupnja. Interes za proučavanje Pellovih jednadžbi se javlja u 17.stoljeću među europskim matematičarima. Jednadžbe ovog tipa prvi su sustavno proučavali staroindijski matematičari. Međutim, ime je dobila po engleskom matematičaru koji nije dao značajniji doprinos u njenom rješavanju. John Pell je rođen 1611. u Southwicku, a najviše se bavio algebrom i teorijom brojeva. Njegova najpoznatija djela su: *Idea of Mathematics* (1638.), *A Refutation of Longo-montanus's Pretended Quadrature of the Circle* (1644.). U ovom poglavlju ćemo se baviti egzistencijom i strukturom rješenja Pellove jednadžbe.

Definicija 3.1.1. *Diofantska jednadžba*

$$x^2 - dy^2 = 1$$

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

Uočimo da ukoliko je d potpun kvadrat, jednadžba ima samo trivijalna rješenja $x = \pm 1, y = 0$. Naime, ako je $d = \delta^2$ i to uvrstimo u jednadžbu, dobivamo $(x-\delta y)(x+\delta y) = 1$ iz čega slijedi da je $(x - \delta y) = (x + \delta y) = \pm 1$.

Pellova jednadžba ima beskonačno mnogo rješenja u prirodnim brojevima što ćemo dokazati koristeći Dirichletov teorem iz diofantskih aproksimacija. Najprije iskažimo lemu koja će nam trebati u dokazu teorema o broju rješenja Pellove jednadžbe.

Lema 3.1.2. *Neka je d prirodan broj koji nije potpun kvadrat. Tada postoji cijeli broj k, $|k| < 1 + 2\sqrt{d}$, sa svojstvom da jednadžba*

$$x^2 - dy^2 = k$$

ima beskonačno mnogo rješenja u prirodnim brojevima.

Dokaz. Po Dirichletovom teoremu, postoji beskonačno mnogo parova prirodnih brojeva (x, y) sa svojstvom:

$$\left| \sqrt{d} - \frac{x}{y} \right| < \frac{1}{y^2},$$

odnosno

$$\left| x - y\sqrt{d} \right| < \frac{1}{y}.$$

Za svaki takav par (x, y) vrijedi:

$$\left| x + y\sqrt{d} \right| = \left| x - y\sqrt{d} + 2y\sqrt{d} \right| < \frac{1}{y} + 2y\sqrt{d} \leqslant (1 + 2\sqrt{d})y,$$

pa je

$$\left| x^2 - dy^2 \right| = \left| x - y\sqrt{d} \right| \cdot \left| x + y\sqrt{d} \right| < 1 + 2\sqrt{d}.$$

Budući da parova (x, y) s navedenim svostvom ima beskonačno, a cijelih brojeva koji su po modulu manji od $1+2\sqrt{d}$ samo konačno, postoji neki cijeli broj k, takav da je $|k| < 1+2\sqrt{d}$, za kojeg jednadžba ima beskonačno mnogo rješenja. □

Teorem 3.1.3. *Pellova jednadžba $x^2 - dy^2 = 1$ ima barem jedno rješenje u prirodnim brojevima x i y.*

Dokaz. Beskonačno mnogo rješenja jednadžbe možemo podijeliti u k^2 klasa, stavljajući rješenja (x_1, y_1) i (x_2, y_2) u istu klasu akko je $x_1 \equiv x_2 \pmod{k}$ i $y_1 \equiv y_2 \pmod{k}$. Tada neka od tih klasa sadrži barem dva različita rješenja $(x_1, y_1), (x_2, y_2)$ takva da su x_1, x_2 različiti prirodni brojevi. Definirajmo:

$$x = \frac{x_1x_2 - dy_1y_2}{k}, \quad y = \frac{x_1y_2 - x_2y_1}{k}.$$

Tvrdimo da je $x, y \in \mathbb{Z},\ y \neq 0,\ x^2 - dy^2 = 1$. Imamo sljedeće:
$x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv k \equiv 0 \pmod{k},\ x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{k}$. Stoga su $x, y \in \mathbb{Z}$. Pretpostavimo sada da je $y = 0$, tj. $x_1y_2 = x_2y_1$. Tada je

$$k = x_2^2 - dy_2^2 = x_2^2 - d \cdot \frac{x_2^2y_1^2}{x_1^2} = \frac{x_2^2}{x_1^2}\left(x_1^2 - dy_1^2\right) = \frac{x_2^2}{x_1^2} \cdot k.$$

Dakle, slijedi da je $x_1^2 = x_2^2$ što je kontradikcija s pretpostavkom da su x_1 i x_2 različiti prirodni brojevi. Konačno,

$$\begin{aligned} x^2 - dy^2 &= \frac{1}{k^2}\left[(x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - x_2y_1)^2\right] \\ &= \frac{1}{k^2}\left(x_1^2x_2^2 + d^2y_1^2y_2^2 - dx_1^2y_2^2 - dx_2^2y_1^2\right) \\ &= \frac{1}{k^2}\left(x_1^2 - dy_1^2\right)\left(x_2^2 - dy_2^2\right) = \frac{1}{k^2}\cdot k \cdot k = 1. \end{aligned}$$

□

Najmanje rješenje Pellove jednadžbe u prirodnim brojevima nazivamo *fundamentalno rješenje* i označavamo ga s (x_1, y_1) ili $x_1 + y_1\sqrt{d}$.

Teorem 3.1.4. *Pellova jednadžba $x^2 - dy^2 = 1$ ima beskonačno mnogo rješenja. Ako je (x_1, y_1) fundamentalno rješenje, onda su sva rješenja (u prirodnim brojevima) ove jednadžbe dana formulom:*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{N}.$$

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

$$x_n^2 - dy_n^2 = \left(x_1 - dy_1^2\right)^n = 1.$$

Dakle, (x_n, y_n) su zaista rješenja i ima ih beskonačno mnogo.
Pretpostavimo sada da je (s, t) rješenje koje nije oblika (x_n, y_n), $n \in \mathbb{N}$. Budući da je $x_1 + y_1\sqrt{d} > 1$ i $s + t\sqrt{d} > 1$, postoji $m \in \mathbb{N}$ takav da je

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

Pomnožimo li prethodnu nejednakost s $\left(x_1 + y_1\sqrt{d}\right)^{-m} = \left(x_1 - y_1\sqrt{d}\right)^m$, dobivamo:

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

Za $a, b \in \mathbb{Z}$ definirajmo: $a + b\sqrt{d} = \left(s + t\sqrt{d}\right)\left(x_1 - y_1\sqrt{d}\right)^m$. Tada imamo:

$$a^2 - db^2 = \left(s^2 - dt^2\right)\left(x_1^2 - dy_1^2\right)^m = 1.$$

Iz $a + b\sqrt{d} > 1$ slijedi da je $0 < a - b\sqrt{d} < 1$, odnosno $a > 0$ i $b > 0$. Stoga je (a, b) rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$ i $a + b\sqrt{d} < x_1 + y_1\sqrt{d}$ što je kontradikcija. □

U prethodnom teoremu smo koristili činjenicu iz sljedeće leme:

Lema 3.1.5. *Ako je* (x, y) *rješenje jednadžbe* $x^2 - dy^2 = 1$*, onda je* $x + y\sqrt{d} > 1$ *ako i samo ako* $x > 0$ *i* $y > 0$*.*

Dokaz. Ako vrijedi $x, y > 0$ jasno je da $x+y\sqrt{d} \geqslant 1+\sqrt{d} > 1$. Nadalje, ako je $x+y\sqrt{d} > 1$, iz $\left(x + y\sqrt{d}\right)\left(x - y\sqrt{d}\right) = 1$ dobivamo:

$$\left|x - y\sqrt{d}\right| = \frac{1}{x + y\sqrt{d}} < 1,$$

odnosno $-1 < x - y\sqrt{d} < 1$, što zajedno s $x + y\sqrt{d} > 1$ daje $x, y > 0$. □

Teorem 3.1.6. *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 redoslijedu. Uzmimo da je* $(x_0, y_0) = (1, 0)$*. Tada vrijedi:*

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

Dokaz. Vrijedi $x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n$ pa odavde slijedi:

$$\left(x_{n+1} + y_{n+1}\sqrt{d}\right)\left(x_1 + y_1\sqrt{d}\right) = x_{n+2} + y_{n+2}\sqrt{d},$$

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

Sada imamo:

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

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

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

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

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

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

Svako netrivijalno rješenje jednadžbe $x^2 - dy^2 = 1$ inducira jako dobru racionalnu aproksimaciju iracionalnog broja $\sqrt{d}$. Zaista,

$$\left|\sqrt{d} - \frac{x}{y}\right| = \frac{1}{y\left|x + y\sqrt{d}\right|} < \frac{1}{2\sqrt{d}y^2}.$$

Iz prethodne nejednakosti i Legendrovog teorema zaključujemo da za svako rješenje Pellove jednadžbe $x^2 - dy^2 = 1$ vrijedi da je $\frac{x}{y}$ neka konvergenta razvoja u verižni razlomak od $\sqrt{d}$.

Teorem 3.1.7. *Ako prirodan broj d nije potpun kvadrat, onda razvoj u jednostavni verižni razlomak od* $\sqrt{d}$ *ima oblik*

$$\sqrt{d} = [a_0, \overline{a_1, ..., a_{l-1}, 2a_0}],$$

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

Teorem 3.1.8. *Neka je l duljina perioda u razvoju od* $\sqrt{d}$.
Ako je l paran, sva rješenja od $x^2 - dy^2 = 1$ *su dana sa* $(x, y) = (p_{nl-1}, q_{nl-1})\,, \quad n \in \mathbb{N}$.
Posebno, fundamentalno rješenje je (p_{l-1}, q_{l-1}).
Ako je l neparan, sva rješenja od $x^2 - dy^2 = 1$ *su dana sa* $(x, y) = (p_{2nl-1}, q_{2nl-1})\,, \quad n \in \mathbb{N}$.
Posebno, fundamentalno rješenje je (p_{2l-1}, q_{2l-1}).

Dokaze prethodnih teorema možemo naći u [2] i [4].

Primjer 3.1.9. *Nađimo sva rješenja jednadžbe za* $x^2 - 12y^2 = 1$ *za* $1 < x < 1500$.

Rješenje:
Razvijmo najprije $\sqrt{12}$ u verižni razlomak: $\sqrt{12} \approx 3.4641016$

$$\begin{aligned}
&s_0 = 0, && t_0 = 1, && a_0 = \left\lfloor \sqrt{12} \right\rfloor = 3,\\
&s_1 = a_0 t_0 - s_0 = 3, && t_1 = \frac{12 - s_1^2}{t_0} = 3, && a_1 = \left\lfloor \frac{s_1 + a_0}{t_1} \right\rfloor = 3,\\
&s_2 = 3, && t_2 = 1, && a_2 = 6,\\
&s_3 = 3, && t_3 = 3.
\end{aligned}$$

Dakle, $(s_3, t_3) = (s_1, t_1) = (3, 3)$ i time zaustavljamo algoritam te zapisujemo:

$$\sqrt{12} = [3, \overline{2, 6}].$$

Trivijalno rješenje jednadžbe je $(x_0, y_0) = (1, 0)$. Duljina perioda je $l = 2$, tj. period je paran pa možemo odrediti fundamentalno rješenje

$$(x_1, y_1) = (p_{l-1}, q_{l-1}) = (p_1, q_1)\,.$$

Odredimo konvergente (p_1, q_1) koristeći rekurzije (1.1) i (1.2):

$$p_1 = a_0 a_1 + 1 = 6 + 1 = 7, \quad q_1 = a_1 = 2 \quad \Rightarrow \quad (x_1, y_1) = (7, 2)\,.$$

Ostala rješenja određujemo koristeći Teorem 3.1.6.

$$\begin{aligned}
x_{n+2} &= 2x_1 x_{n+1} - x_n, \qquad & y_{n+2} &= 2x_1 y_{n+1} - y_n, \quad n \geqslant 0,\\
x_2 &= 2 \cdot 7 \cdot 7 - 1 = 97, & y_2 &= 2 \cdot 7 \cdot 2 - 0 = 28,\\
x_3 &= 2 \cdot 7 \cdot 97 - 7 = 1351, & y_3 &= 2 \cdot 7 \cdot 28 - 2 = 390.
\end{aligned}$$

Dakle, imamo:

$$(x_1, y_1) = (7, 2)$$
$$(x_2, y_2) = (97, 28)$$
$$(x_3, y_3) = (1351, 390)\,.$$

3.2 Jednadžba $x^2 - dy^2 = N$

Definicija 3.2.1. *Jednadžba oblika*

$$x^2 - dy^2 = N,$$

gdje je d prirodan broj koji nije potpun kvadrat i N cijeli broj različit od 0*, naziva se pellovska jednadžba*

Pellovska jednadžba ne mora imati cjelobrojna rješenja. Međutim, ako ima barem jedno rješenje, onda ih ima beskonačno mnogo. Naime, ako je $x + y\sqrt{d}$ rješenje pellovske jednadžbe, a $u + v\sqrt{d}$ rješenje pripadne Pellove jednadžbe $x^2 - dy^2 = 1$, onda je:

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

također rješenje jednadžbe $x^2 - dy^2 = N$. To nam slijedi iz:

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

Budući da Pellova jednadžba ima beskonačno mnogo rješenja, slijedi da i pellovska jednadžba ima beskonačno rješenja (uz pretpostavku da ima barem jedno).

Definicija 3.2.2. *Za dva rješenja $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ jednadžbe $x^2 - dy^2 = N$ kažemo da su asocirana ako se jedno iz drugog može dobiti množenjem s nekim rješenjem Pellove jednadžbe.*

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

Odaberimo jedan element $x^* + y^*\sqrt{d}$ iz klase $\mathbf{K}$ i taj element nazovimo *fundamentalnim rješenjem* jednadžbe $x^2 - dy^2 = N$ u klasi $\mathbf{K}$. Biramo ga tako da y^* poprimi najmanju moguću nenegativnu vrijednost među elementima klase $\mathbf{K}$. Također, sada je i x^*

jednoznačno određen ako K nije dvoznačna. U slučaju da je $\mathbf{K}$ dvoznačna, izabiremo x^* tako da zadovolji dodatan uvjet: $x^* \geqslant 0$. Uočimo da $|x^*|$ poprima najmanju moguću vrijednost unutar klase $\mathbf{K}$.

Teorem 3.2.3. *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:*

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

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

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. Dokažimo najprije tvrdnju za $N < 0$. Definirajmo cijele brojeve x', y' sa

$$x' + y'\sqrt{d} = \left(x^* + y^*\sqrt{d}\right)\left(u - \delta v\sqrt{d}\right),$$

gdje je $\delta = 1$ ako je $x^* \geqslant 0$, 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

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

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

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

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

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

Dokaz za $N > 0$ je analogan. □

Propozicija 3.2.4. *Pretpostavimo da je $|N| < \sqrt{d}$. Ako je $x + y\sqrt{d}$ rješenje jednadžbe $x^2 - dy^2 = N$, onda je $\frac{x}{y}$ neka konvergenta razvoja u verižni razlomak od $\sqrt{d}$.*

Dokaz. Pretpostavimo najprije da je $N > 0$. Tada je $x > y\sqrt{d}$ pa je

$$0 < \frac{x}{y} - \sqrt{d} = \frac{N}{y\left(x + y\sqrt{d}\right)} < \frac{N}{2\sqrt{d}y^2} < \frac{1}{2y^2}.$$

Iz Legendrovog teorema slijedi da je $\frac{x}{y}$ neka (neparna) konvergenta od $\sqrt{d}$.
Neka je sada $N < 0$. Tada je $x < y\sqrt{d}$ pa imamo

$$0 < \frac{y}{x} - \frac{1}{\sqrt{d}} = \frac{|N|}{x\sqrt{d}\left(x + y\sqrt{d}\right)} < \frac{|N|}{2\sqrt{d}x^2} < \frac{1}{2x^2}.$$

Zaključujemo da je $\frac{y}{x}$ neka konvergenta od $\frac{1}{\sqrt{d}}$. Nadalje, ako je $\frac{y}{x}$ i-ta konvergenta od $\frac{1}{\sqrt{d}}$, onda je $\frac{x}{y}$ $(i-1)$-va konvergenta od $\sqrt{d}$. □

Primjer 3.2.5. *Riješimo jednadžbu* $x^2 - 7y^2 = -31$.

Rješenje:
Funadamentalno rješenje pripadne Pellove jednadžbe $x^2 - 7y^2 = 1$ je $8 + 3\sqrt{7}$, odnosno $(u, v) = (8, 3)$.
Za fundamentalna rješenja polazne jednadžbe vrijedi

$$0 \leqslant y^* \leqslant \frac{v}{\sqrt{2(u+\varepsilon)}}\sqrt{|N|} \leqslant \frac{3}{\sqrt{2(8-1)}}\sqrt{|-31|} \leqslant 4.4641,$$

$$|x^*| \leqslant \sqrt{\frac{1}{2}(u+\varepsilon)|N|} \leqslant \sqrt{\frac{1}{2}(8-1)|-31|} \leqslant 10.416.$$

Dakle, $y^* \leqslant 4$ i $x^* \leqslant 10$.
Provjerom za koje $y = 1, 2, 3, 4$ početna jednadžba ima rješenja, dobivamo da jednažba ima rješenja za $y = 4$:

$$x^2 = -31 + 112 = 81 \Rightarrow x = \pm 9.$$

Rješenja koja zadovoljavaju jednadžbu su $\left(9 + 4\sqrt{7}\right)$ i $\left(-9 + 4\sqrt{7}\right)$.
Sva rješenja dana su sa
$x + y\sqrt{7} = \pm\left(9 + 4\sqrt{7}\right)\left(8 + 3\sqrt{7}\right)^n$ ili $x + y\sqrt{7} = \pm\left(-9 + 4\sqrt{7}\right)\left(8 + 3\sqrt{7}\right)^n$, $n \in \mathbb{Z}$.
Imamo dva niza rješenja u prirodnim brojevima:

$$x_0 = 9,\ y_0 = 4 \Rightarrow x_1 + y_1\sqrt{7} = 156 + 59\sqrt{7} \Rightarrow x_1 = 156,\ y_1 = 59$$

$$\Rightarrow x_{n+2} = 2 \cdot 156 \cdot x_{n+1} - x_n,\quad y_{n+2} = 2 \cdot 59 \cdot y_{n+1} - y_n,$$

$$x'_0 = -9,\ y'_0 = 4 \Rightarrow x'_1 + y'_1\sqrt{7} = 12 + 5\sqrt{7} \Rightarrow x'_1 = 12,\ y'_1 = 5$$

$$\Rightarrow x'_{n+2} = 2 \cdot 12 \cdot x'_{n+1} - x'_n,\quad y'_{n+2} = 2 \cdot 5 \cdot y'_{n+1} - y'_n.$$

Poglavlje 4

Linearne forme u logaritmima

4.1 Osnovne definicije i teoremi

Definicija 4.1.1. *Linearna forma u logaritmima algebarskih brojeva je izraz oblika*

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + ... + \beta_n \log \alpha_n,$$

gdje su $\alpha_i, \ \ i = 1, ..., n \ \ i \ \ \beta_i, \ \ i = 0, ...n$ *kompleksni algebarski brojevi.*

Kod primjene linearnih formi u logaritmima na rješavanje diofantskih jednadžbi promatrat ćemo samo slučaj kad je $\beta_0 = 0$ i $\beta_i \in \mathbb{Z}, \ \ i = 1, ..., n$, a log će uvijek označavati glavnu vrijednost kompleksnog logaritma. Također, označavat ćemo $\beta_i = b_i, \ \ i = 1, ..., n$.
Najprije recimo nešto o razvoju teorije linearnih formi u logaritmima motivirane sedmim Hilbertovim problemom. Naime, jedan od najutjecajnijih matematičara 19. stoljeća (i ranog 20. stoljeća) je David Hilbert. Na Drugom međunarodnom kongresu matematičara 1900. godine u Parizu je predstavio listu neriješenih problema. Jedan od predstavljenih problema je sedmi Hilbertov problem u kojem je tražio da se dokaže: ako je α algebarski broj različit od 0 i 1 te β algebarski i iracionalan, onda je α^β transcendentan broj. Tu su tvrdnju neovisno dokazali Gelfond i Schneider 1934. godine.
Pokazali su da ako su $\alpha_1, \alpha_2 \neq 0$ algebarski brojevi takvi da su $\log \alpha_1$ i $\log \alpha_2$ linearno nezavisni nad $\mathbb{Q}$, onda je

$$\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 \neq 0,$$

za sve algebarske brojeve β_1, β_2.
Baker je 1967.godine poopćio taj rezultat i dokazao da ako su $\alpha_1, ..., \alpha_n \neq 0$ algebarski brojevi takvi da su $\log \alpha_1, ..., \log \alpha_n$ linearno nezavisni nad $\mathbb{Q}$, onda je

$$\left|\beta_0 + \beta_1 \log \alpha_1 + ... + \beta_n \log \alpha_n\right| \neq 0,$$

za sve algebarske brojeve $\beta_0, \beta_1, ..., \beta_n$ koji nisu svi jednaki nuli. Također, Baker je našao i donju ogradu za prethodni izraz.

Recimo sada nešto o visinama algebarskih brojeva. Neka je α algebarski broj stupnja d i neka je $P(x) = a_d x^d + ... + a_0$ njegov minimalni polinom s relativno prostim cjelobrojnim koeficijentima.

Definicija 4.1.2. *Apsolutna visina (ili kraće samo visina) algebarskog broja α, u oznaci $H(\alpha)$, definirana je sa*

$$H(\alpha) = \max\{|a_0|, ..., |a_d|\}.$$

Racionalne brojeve možemo shvatiti kao algebarske brojeve prvog stupnja. Stoga je visina racionalnog broja $\frac{p}{q}$ definirana sa:

$$H\left(\frac{p}{q}\right) = \max\{|p|, |q|\}.$$

Sada definirajmo i apsolutnu logaritamsku visinu:

Definicija 4.1.3. *Neka je K polje algebarskih brojeva stupnja D i neka je $\alpha \in K$ algebarski broj stupnja $d|D$. Neka je $P(x) = \sum_{k=0}^{d} a_k x^k$ njegov minimalni polinom s relativno prostim cjelobrojnim koeficijentima takav da je $a_d \neq 0$. Definiramo apsolutnu logaritamsku visinu $h(\alpha)$ algebarskog broja α sa*

$$h(\alpha) = \frac{1}{d}\left(\log(|a_d|) + \sum_{i=1}^{d} \max\{\log(|\alpha_i|, 0)\}\right),$$

gdje su α_i konjugati od α.

Također, sada imamo da je apsolutna logaritamska visina h racionalnog broja $\frac{p}{q}$ jednaka:

$$h\left(\frac{p}{q}\right) = \log\max\{|p|, |q|\}.$$

Pogledajmo na primjeru kako se računa apsolutna logaritamska visina algebarskog broja:

Primjer 4.1.4. *Neka je $\alpha = \sqrt{2}$. Stupanj algebarskog broja $\alpha = \sqrt{2}$ je 2 pa imamo:*

$$h(\alpha) = h\left(\sqrt{2}\right) = \frac{1}{2}\left(\log\left|\sqrt{2}\right| + \log\left|-\sqrt{2}\right|\right) = \frac{1}{2}\log 2.$$

Definicija 4.1.5. *Neka je K polje algebarskih brojeva stupnja D. Definiramo modificiranu visinu sa*

$$h'(\alpha_j) = \max\{Dh(\alpha_j), |\log \alpha_j|, 0.16\}, \qquad j = 1, ..., n,$$

gdje su α_j *elementi polja K različiti od* 0*.*

Nadalje, neka su $A_1, A_2, ..., A_n$ realni brojevi takvi da vrijedi:

$$A_j \geqslant h'(\alpha_j), \qquad j = 1, ..., n,$$

gdje je h' modificirana visina.

Prilikom rješavanja diofantskih jednadžbi želimo odrediti donju ogradu za linearnu formu u logaritmima.
Neka je K polje algebarskih brojeva stupnja D. Nadalje, neka su $\alpha_1, ..., \alpha_n$ elementi od K različiti od 0 i $b_1, ..., b_n \in \mathbb{Z}$. Definirajmo:

$$B = \max\{|b_1|, ..., |b_n|\},$$

$$\Lambda^* = \alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1.$$

Želimo naći donju ogradu za $|\Lambda^*|$, pretpostavljajući da je $\Lambda^* \neq 0$. S obzirom na to da se $\log(1 + x)$ asimptotski približava x kako $|x|$ teži u 0, naš problem se svodi na nalaženje donje ograde linearne forme u logaritmima:

$$\Lambda = b_1 \log \alpha_1 + ... + b_n \log \alpha_n + b_{n+1} \log(-1),$$

gdje je $b_{n+1} = 0$ ako je K realno polje, a $|b_{n+1}| \leqslant nB$ inače.
Linearne forme Λ i Λ^* su usko povezane te ćemo koristiti obje forme.
Navedimo sada teoreme koji će nam poslužiti za određivanje donje ograde.

Teorem 4.1.6 (Baker-W*ü*stholz, 1993.)**.** *Pretpostavimo da vrijedi:* $\Lambda = b_1 \log \alpha_1 + ... + b_n \log \alpha_n \neq 0$*, gdje su* α_i *algebarski brojevi, a* b_i *cjelobrojni koeficijenti. Onda je*

$$\log|\Lambda| \geqslant -18 \cdot (n+1)! n^{n+1} (32D)^{n+2} \log(2nD) h''(\alpha_1) \cdots h''(\alpha_n) \log B,$$

gdje je D stupanj proširenja polja algebarskih brojeva $\mathbb{Q}(\alpha_1, ..., \alpha_n)$*,* $B = \max\{|b_i| : i = 1, ..., n\}$*, a* $h''(\alpha) = \max\{h(\alpha), \frac{1}{D}|\log \alpha|, \frac{1}{D}\}$.

Teorem 4.1.7 (Matveev, 2001.)**.** *Pretpostavimo da vrijedi* $\Lambda^* \neq 0$*. Tada je*

$$\log|\Lambda^*| > -3 \cdot 30^{n+4} (n+1)^{5.5} D^2 A_1 \cdots A_n (1 + \log D)(1 + \log nB).$$

Nadalje, ako je K realno, vrijedi

$$\log|\Lambda^*| > -1.4 \cdot 30^{n+3} n^{4.5} D^2 A_1 \cdots A_n (1 + \log D)(1 + \log B).$$

4.2 Primjena na simultane pellovske jednadžbe

Na konferenciji u Oberwolfachu 1968. godine se pojavio problem vezan uz proširenje Diovantovih m-torki. Diofantova m-torka je skup m različitih prirodnih brojeva, takvih da je umnožak bilo koja dva njegova člana uvećan za jedan, kvadrat cijelog broja. Najpoznatija Diofantova četvorka je skup $\{1, 3, 8, 120\}$. Međutim, na konferenciji se postavilo pitanje mora li d biti jednak 120 u četvorki $\{1, 3, 8, d\}$.
Primjenom Bakerove teorije linearnih formi u logaritmima i metode redukcije, Baker i Davenport su u potpunosti riješili taj problem. Naime, problem proširenja Diofantovih m-torki vodi na rješavanje sustava simultanih pellovskih jednadžbi. Pokažimo sada kako se Baker-W*ü*stholz teorem može primijeniti na Diofantovu četvorku $\{1, 3, 8, 120\}$.

Teorem 4.2.1. *Jedini pozitivni cijeli broj d takav da su $d + 1, 3d + 1, 8d + 1$ kvadrati prirodnog broja je $d = 120$.*

Dokaz. Ako su $d + 1, 3d + 1, 8d + 1$ kvadrati prirodnog broja, možemo pisati

$$d + 1 = x^2, \quad 3d + 1 = y^2, \quad 8d + 1 = z^2, \qquad x, y, z \in \mathbb{N}.$$

Eliminacijom d iz gornjih jednakosti dobivamo

$$3x^2 - y^2 = 2,$$
$$8x^2 - z^2 = 7.$$

Dakle, dobili smo sustav simultanih pellovskih jednadžbi. U trećem poglavlju smo objasnili kako se rješavaju pellovske jednadžbe te smo govorili o broju i strukturi rješenja. Stoga dobivamo da su rješenja jednadžbi

$$y + x\sqrt{3} = \left(1 + \sqrt{3}\right)\left(2 + \sqrt{3}\right)^m,$$
$$z + x\sqrt{8} = \left(\pm 1 + \sqrt{8}\right)\left(3 + \sqrt{8}\right)^n,$$

gdje su m, n nenegativni cijeli brojevi. Neka je $x = v_m$ za neki $m \geqslant 0$ i niz (v_m) zadan rekurzivnom relacijom

$$v_0 = 1, \quad v_1 = 3, \quad v_{m+2} = 4v_{m+1} - v_m.$$

Nadalje, neka je $x = w_n^{+,-}$ za neki $n \geqslant 0$, gdje su nizovi (w_n^+) i (w_n^-) dani sa

$$w_0^+ = 1, \quad w_1^+ = 4, \quad w_{n+2^+} = 6w_{n+1}^+ - w_n^+.$$
$$w_0^- = 1, \quad w_1^- = 2, \quad w_{n+2^-} = 6w_{n+1}^- - w_n^-.$$

Dakle, problem proširenja Diofantove trojke smo sveli na rješavanje diofantske jednadžbe $v_m = w_n^{+,-}$.
Dokažimo najprije dvije leme koje će nam biti potrebne za nastavak dokaza.

Lema 4.2.2. *Ako je* $v_m = w^{+,-}, m, n > 2$, *onda*

$$0 < |\Lambda| < 7.3\left(2 + \sqrt{3}\right)^{-2m},$$

gdje je

$$\Lambda = m\log\left(2 + \sqrt{3}\right) - n\log\left(3 + 2\sqrt{2}\right) + \log\frac{2\sqrt{2}\left(1 + \sqrt{3}\right)}{\sqrt{3}\left(2\sqrt{2} \pm 1\right)}.$$

Dokaz. Izraz $v_m = w_n^{+,-}$ povlači

$$\frac{\left(1 + \sqrt{3}\right)\left(2 + \sqrt{3}\right)^m - \left(1 - \sqrt{3}\right)\left(2 - \sqrt{3}\right)^m}{2\sqrt{3}}$$

$$= \frac{\left(2\sqrt{2} \pm 1\right)\left(3 + 2\sqrt{2}\right)^n + \left(2\sqrt{2} \mp 1\right)\left(3 - 2\sqrt{2}\right)^n}{4\sqrt{2}} \tag{4.1}$$

Nadalje, vrijedi

$$v_m > \frac{\left(1 + \sqrt{3}\right)\left(2 + \sqrt{3}\right)^m}{2\sqrt{3}},$$

$$w_n^{+,-} < \frac{\left(2\sqrt{2} + 1\right)\left(3 + 2\sqrt{2}\right)^n}{2\sqrt{2}},$$

što povlači

$$\frac{\left(1 + \sqrt{3}\right)\left(2 + \sqrt{3}\right)^m}{2\sqrt{3}} < \frac{\left(2\sqrt{2} + 1\right)\left(3 + 2\sqrt{2}\right)^n}{2\sqrt{2}},$$

$$\left(3 - 2\sqrt{2}\right)^n < \frac{\sqrt{3}\left(2\sqrt{2} + 1\right)}{\sqrt{2}\left(\sqrt{3} + 1\right)}\left(2 - \sqrt{3}\right)^m < 1.7163\left(2 - \sqrt{3}\right)^m.$$

Dijeljenjem (4.1) s $\frac{2\sqrt{2} \pm 1}{4\sqrt{2}}\left(3 + 2\sqrt{2}\right)^n$, dobivamo

$$\left|\frac{2\sqrt{2\left(1 + \sqrt{3}\right)}}{\sqrt{3}\left(2\sqrt{2} \pm 1\right)} \cdot \frac{\left(2 + \sqrt{3}\right)^m}{\left(3 + 2\sqrt{2}\right)^n} - 1\right|$$

$$\leqslant \frac{2\sqrt{2} + 1}{2\sqrt{2} - 1}\left(3 - 2\sqrt{2}\right)^{2n} + \frac{2\sqrt{2}\left(\sqrt{3} - 1\right)}{\sqrt{3}\left(2\sqrt{2} - 1\right)}\left(2 - \sqrt{3}\right)^m\left(3 - 2\sqrt{2}\right)^n$$

$$< \frac{2\sqrt{2}+1}{2\sqrt{2}-1} \cdot 1.7163^2 \left(2-\sqrt{3}\right)^{2m} + \frac{2\sqrt{2}\left(\sqrt{3}-1\right)}{\sqrt{3}\left(2\sqrt{2}-1\right)} \cdot 1.7163 \left(2-\sqrt{3}\right)^{2m}$$

$$< 7.29 \left(2-\sqrt{3}\right)^{2m}.$$

Sada tvrdnja slijedi iz sljedeće leme i činjenice da je $\Lambda \neq 0$. □

Lema 4.2.3. *Neka je $a \in \mathbb{R}, a < 1$. Ako je $|x| < a$, onda vrijedi*

$$\left|\log(1+x)\right| < \frac{-\log(1-a)}{a}|x|.$$

Dokaz. Primijetimo da je funkcija $f(x) = \dfrac{\log(1+x)}{x}$ pozitivna i strogo padajuća za $|x| < 1$. Tada je ta funkcija za $|x| < a$ po vrijednosti manja od vrijednosti u točki $x = -a$. □

Vratimo se sada dokazu teorema. Promotrimo linearnu formu u tri logaritma:

$$\Lambda = m \log\left(2+\sqrt{3}\right) - n \log\left(3+2\sqrt{2}\right) + \log \frac{2\sqrt{2}\left(1+\sqrt{3}\right)}{\sqrt{3}\left(2\sqrt{2}\pm 1\right)}.$$

Možemo staviti

$$\alpha_1 = 2+\sqrt{3}, \quad \alpha_2 = 3+2\sqrt{2}, \quad \alpha_3 = \frac{2\sqrt{2}\left(1+\sqrt{3}\right)}{\sqrt{3}\left(2\sqrt{2}\pm 1\right)},$$

$$b_1 = m, \quad b_2 = -n, \quad b_3 = 1, \quad D = [\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{Q}] = 4.$$

Minimalni polinomi nad $\mathbb{Z}$ su zadani sa

$$P_{\alpha_1}(x) = x^2 - 4x + 1,$$

$$P_{\alpha_2}(x) = x^2 - 6x + 1,$$

$$P_{\alpha_3}(x) = 441x^4 - 2016x^3 + 2880x^2 - 1536x + 256.$$

Nadalje, imamo

$$h''(\alpha_1) = \frac{1}{2}\log\left(2+\sqrt{3}\right) < 0.6585,$$

$$h''(\alpha_2) = \frac{1}{2}\log\left(3+2\sqrt{2}\right) < 0.8814,$$

$$h''(\alpha_3) = \frac{1}{4}\log\left(441 \cdot \frac{2\left(4+\sqrt{2}\right)\left(3+\sqrt{3}\right)}{21} \cdot \frac{2\left(4-\sqrt{2}\right)\left(3+\sqrt{3}\right)}{21}\right) < 1.7836.$$

Primjenom Baker-W*ü*stholz teorema dobivamo donju ogradu za Λ:

$$\log|\Lambda| \geqslant -3.96 \cdot 10^{15} \log m.$$

Koristeći Lemu 4.2.2. zaključujemo da je

$$m < 6 \cdot 10^{16}.$$

Sada još moramo reducirati dobivenu gornju ogradu za m, a to ćemo učiniti pomoću Baker-Davenportove redukcije. Tada imamo sljedeće:

$$\Lambda = m \log\left(2 + \sqrt{3}\right) - n \log\left(3 + 2\sqrt{2}\right) + \log \frac{2\sqrt{2}\left(1 + \sqrt{3}\right)}{\sqrt{3}\left(2\sqrt{2} \pm 1\right)} < 7.3\left(2 + \sqrt{3}\right)^{-2m}.$$

U notaciji Leme 2.3.1. možemo zapisati

$$N = 6 \cdot 10^{16}, \quad \kappa = \frac{\alpha_1}{\alpha_2}, \quad \mu = \frac{\alpha_3}{\alpha_2},$$

$$A = \frac{7.3}{\log \alpha_2}, \quad B = \left(2 + \sqrt{3}\right)^2.$$

Sljedeći korak je pronaći konvergentu $\frac{p}{q}$ verižnog razlomka broja $\kappa = \frac{\alpha_1}{\alpha_2}$ takvu da je $q > 6N$. Pomoću programa *Mathematica* dobivamo

$$\frac{p}{q} = \frac{742265900639684111}{9935223607325971 20}.$$

Nadalje, dobivamo da je

$$||\kappa q|| N \approx 0.0187822, \quad ||\mu q|| \approx 0.00762577.$$

Nažalost,

$$\varepsilon = ||\mu q|| - ||\kappa q|| N < 0.$$

Dakle, kako bismo mogli koristiti Baker-Davenportovu redukciju, moramo naći drugu konvergentu verižnog razlomka koja zadovoljava $\varepsilon > 0$ i $q > 6N$. Takva konvergenta je

$$\frac{p}{q} = \frac{2297570640187354392}{3075296607888933649}.$$

Zaista, $\varepsilon = ||\mu q|| - ||\kappa q|| N \approx 0.296651 > 0$.
Sada dobivamo novu gornju ogradu $m = 17$. Nadalje, ponovimo li još jednom isti postupak,

dobit ćemo da je $m \leqslant 4$. To je dovoljno mala ograda da provjerimo što se događa s našim nizovima kad su indeksi mali. Dobivamo dva rješenja:

$$v_0 = w_0^{+,-} = 1,$$

što je trivijalno proširenje naše Diofantske trojke s $d = 0$ i

$$v_2 = w_2^{-} = 11,$$

što daje proširenje s $d = 120$, a to smo htjeli pokazati. □

4.3 Primjena na Fibonaccijeve brojeve

Leonardo iz Pise (poznat kao Fibonacci) je najveći europski srednjovjekovni matematičar. Promatrajući razmnožavanje zečeva u prirodi otkrio je matematički niz koji danas nosi njegovo ime. Fibonaccijev niz čine brojevi: $1, 1, 2, 3, 5, 8, 13, ...$, pri čemu se svaki sljedeći broj dobiva kao zbroj prethodna dva broja u nizu. Elementi Fibonaccijeva niza nazivaju se Fibonaccijevi brojevi. Također, Fibonaccijev niz možemo definirati rekurzivnom relacijom:

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n, \quad n \geqslant 0.$$

Rješavanjem rekurzivne relacije dobivamo karakterističnu jednadžbu:

$$f(x) = x^2 - x - 1 = (x - \alpha)(x - \beta),$$

gdje je $\alpha = \dfrac{1 + \sqrt{5}}{2}$ i $\beta = \dfrac{1 - \sqrt{5}}{2}$.
Osim toga, možemo pisati

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad n \geqslant 0.$$

U ovom poglavlju ćemo govoriti o Fibonaccijevim brojevima koji u dekadskom zapisu imaju sve znamenke jednake. Nalaženje takvih Fibonaccijevih brojeva je ekvivalentno rješavanju diofantske jednadžbe

$$F_n = \overline{dd...d}_{(10)} = d10^{m-1} + d10^{m-2} + ... + d = d\frac{10^m - 1}{10 - 1}, \quad d \in \{1, ..., 9\}. \tag{4.2}$$

Pokažimo sada na konkretnom primjeru kako koristiti linearne forme u logaritmima kod Fibonaccijevog niza.

Primjer 4.3.1. *Najveće rješenje jednadžbe* (4.2) *je* $F_{10} = 55$.

Rješenje:

Pretpostavimo da je $n > 1000$. Cilj nam je dobiti ogradu za n. Ako označimo $\alpha = \dfrac{1+\sqrt{5}}{2}$ i $\beta = \dfrac{1-\sqrt{5}}{2}$, onda (4.2) možemo zapisati

$$\frac{\alpha^n - \beta^n}{\sqrt{5}} = d10^{m-1} + d10^{m-2} + ... + d = d\frac{10^m - 1}{9},$$

što sada možemo zapisati kao

$$\left|\alpha^n - \frac{d\sqrt{5}}{9}10^m\right| = \left|\beta^n - \frac{d\sqrt{5}}{9}\right| \leqslant |\beta^n| + \left|\frac{d\sqrt{5}}{9}\right| \leqslant \alpha^{-1000} + \sqrt{5} < 2.5 \tag{4.3}$$

Nadalje, indukcijom po n se lako može pokazati da vrijedi

$$\alpha^{n-2} < F_n < \alpha^{n-1}, \quad \forall n \geqslant 3.$$

Tada je $\alpha^{n-2} < F_n < 10^m$, odnosno

$$n < \frac{\log 10}{\log \alpha}m + 2$$

i

$$10^{m-1} < F_n < \alpha^{n-1},$$

što povlači

$$n > \frac{\log 10}{\log \alpha}(m-1) + 1 = \frac{\log 10}{\log \alpha}m - \left(\frac{\log 10}{\log \alpha} - 1\right) > \frac{\log 10}{\log \alpha}m - 4.$$

Sada zaključujemo da je

$$n \in [cm - 4, cm + 2],$$

gdje je $c = \dfrac{\log 10}{\log \alpha} \approx 4.78497$. Kako je $c > 4$, vidimo da za sve $n > 1000$ vrijedi $n \geqslant m$. Definirajmo sad linearnu formu

$$\Lambda = \frac{d\sqrt{5}}{9}\alpha^{-n}10^m - 1,$$

za koju iz (4.3) zaključujemo

$$|\Lambda| < \frac{2.5}{\alpha^n} < \frac{1}{\alpha^{n-2}},$$

odnosno

$$\log|\Lambda| = \log\frac{d\sqrt{5}}{9} - n\log\alpha + m\log 10 < -(n-2)\log\alpha.$$

S druge strane, donju ogradu za $|\Lambda|$ možemo dobiti iz Teorema 4.1.7. Označimo

$$\alpha_1 = \frac{d\sqrt{5}}{9}, \quad \alpha_2 = \alpha, \quad \alpha_3 = 10,$$

$$b_1 = 1, \quad b_2 = -n, \quad b_3 = m.$$

Primjetimo da je $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}\left(\sqrt{5}\right)$ pa je u notaciji teorema $D = 2$. Odredimo $B = \max\{m, n, 1\} = \max\{m, n\}$. S obzirom da je $n > m$ imamo da je $B = n$. Također, α_2 i α_3 su algebarski cijeli brojevi. Minimalni polinom od α_1 nad $\mathbb{Z}$ je

$$P_{\alpha_1}(x) = 81x^2 - 5d^2.$$

Tada vrijedi

$$h(\alpha_1) < \frac{1}{2}\left(\log 81 + 2\log\sqrt{5}\right) = \frac{1}{2}\log 405 < 3.01,$$

$$h(\alpha_2) = \frac{1}{2}(\log\alpha + 1) < 0.75,$$

$$h(\alpha_3) = \log 10 < 2.31.$$

Tada za $A_i, \ i = 1, 2, 3$ možemo odabrati

$$A_1 = 6.02, \quad A_2 = 1.5, \quad A_3 = 4.62.$$

Sada Teorem 4.1.7. povlači

$$\log|\Lambda| > -1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 4 \cdot (1 + \log 4) \cdot 6.02 \cdot 1.5 \cdot 4.62 \cdot (1 + \log n).$$

Uspoređujući to s gornjom ogradom, dobivamo

$$n - 2 < 1.35 \cdot 10^{13}(1 + \log n),$$

odnosno $n < 4.5 \cdot 10^{15}$. Nadalje, Baker-Davenportovom redukcijom ćemo reducirati dobivenu ogradu. Stoga moramo dobiti nejednakost kao u Lemi 2.3.1. Primjetimo da je desna strana negativna u nejednakosti

$$1 - \frac{d\sqrt{5}}{9}\alpha^{-n}10^m \leqslant \frac{1}{\alpha^n}\left(\beta^n - \frac{d\sqrt{5}}{9}\right).$$

Označimo $z = \log\alpha_1 - n\log\alpha_2 + m\log\alpha_3$. Stoga dobivamo

$$-\frac{2.5}{\alpha^n} < 1 - e^z < 0.$$

Iz toga i pretpostavke $n > 1000$ dobivamo $e^z < 1.5$, odnosno

$$0 < e^z - 1 < \frac{2.5e^z}{\alpha^n} < \frac{4}{\alpha^n}.$$

Kako je $z < e^z - 1$ zaključujemo

$$0 < m\log\alpha_3 - n\log\alpha_2 + \log\alpha_1 < \frac{4}{\alpha^n},$$

što možemo zapisati

$$0 < m\left(\log\frac{\alpha_3}{\alpha_2}\right) - n + \log\frac{\alpha_1}{\alpha_2} < \frac{4}{\alpha^n\log\alpha_2} < \frac{9}{\alpha^n}.$$

Kako je

$$\left|1 - \frac{d\sqrt{5}10^m}{\alpha^n}\right| < 1,$$

imamo

$$\frac{d\sqrt{5}10^m}{\alpha^n} < 2,$$

odnosno

$$\alpha^n > \frac{d\sqrt{5}10^m}{2} > 10^m.$$

Dobili smo

$$0 < m\left(\log\frac{\alpha_3}{\alpha_2}\right) - n + \log\frac{\alpha_1}{\alpha_2} < \frac{9}{10^m},$$

što je nejednakost kakvu želimo. Iz $n < 4.5 \cdot 10^{15}$ i prethodne nejednakosti možemo zaključiti da je $m < 9.5 \cdot 10^{14}$. Primjenimo Baker-Davenportovu redukciju na prethodnu nejednakost stavljajući:

$$\kappa = \frac{\log\alpha_3}{\log\alpha_2}, \quad \mu = \frac{\log\alpha_1}{\log\alpha_2}, \quad A = 9, \quad B = 10.$$

Sada imamo

$$0 < \kappa m - n + \mu < \frac{A}{B^m},$$

gdje je $m < N := 10^{15}$. Nadalje, pomoću programa *Mathematica* dobivamo da je $q_{35} > 2 \cdot 10^{17} > 6N$, gdje je

$$\frac{p_{35}}{q_{35}} = \frac{970939497358931987}{202914354378543655}$$

konvergenta razvoja u verižni razlomak broja κ.
Za svaku od vrijednosti $d \in \{1, ..., 9\}$ računamo $\|q_{35}\mu\|$ i dobivamo minimalnu vrijednost za $d = 5$ koja iznosi 0.029.... Dakle, imamo

$$\|q_{35}\mu\| > 0.02.$$

Za $\varepsilon = 0.01 < 0.02 - 0.01 < \|q_{35}\mu\| - N\|q_{35}\kappa\|$ dobivamo

$$\frac{\log \frac{Aq_{35}}{\varepsilon}}{\log B} = 21.2313...,$$

iz čega zaključujemo da za $m \in [22, 10^{15}]$ nejednadžba

$$0 < \kappa m - n + \mu < \frac{A}{B^m},$$

nema rješenja. Dakle, $m \leqslant 21$ iz čega dobijemo da je $n \leqslant 102$ što je kontradikcija s pretpostavkom da je $n > 1000$.
Ponovno, u programu *Mathematica* provjeravamo što se događa za $n \leqslant 1000$ i na taj način dobivamo da je jedino rješenje dano s $F_{10} = 55$.

Literatura

[1] C.D.Olds, *Continued fractions*, Random House, 1963..

[2] A. Dujella, *Uvod u teoriju brojeva*, skripta, Sveučilište u Zagrebu, 2003.

[3] A. Dujella, *Diofantske jednadžbe*, skripta, Sveučilište u Zagrebu, 2006.

[4] A. Dujella, *Diofantske aproksimacije i primjene*, skripta, Sveučilište u Zagrebu, 2011.

[5] A. Filipin, *Linearne forme u logaritmima i diofantska analiza*, skripta, Sveučilište u Zagrebu, 2010.

[6] F.M.Brückler, *Povijest matematike*, Sveučilište J.J.Strossmayera, 2014.

[7] I.Tržić, *Verižni razlomci*, diplomski rad, Sveučilište J.J.Strossmayera, 2011.

[8] F. Luca, *Diophantine equations*, Universidad National Autonoma de Mexico, 2009.

[9] I. Matić, *Uvod u teoriju brojeva*, skripta, Sveučilište J.J.Strossmayera, 2014.

[10] M.Skender, *Pellove i pellovske jednadžbe*, diplomski rad, Sveučilište J.J.Strossmayera, 2012.

[11] T. Pejković, *Rothov teorem*, diplomski rad, Sveučilište u Zagrebu, 2005.

[12] A.Filipin S.Bujačić, *Linear forms in logarithms, in Diophantine Analysis: Course Notes from a Summer School (J. Steuding, Ed.)*, Birkhäuser, 2016.

Sažetak

U ovom diplomskom radu, bavimo se primjenom linearnih formi u logaritmima na rješavanje diofantskih problema. Na početku rada iskazujemo osnovne pojmove i definicije koje su nam potrebne u nastavku rada. U drugom poglavlju obrađujemo rezultate iz diofantskih aproksimacija koji se koriste u rješavanju diofantskih jednadžbi. Nadalje, u trećem poglavlju definiramo Pellovu i pellovsku jednadžbu. Također, dokazujemo niz teorema o egzistenciji i strukturi rješenja navedenih jednadžbi. U posljednjem poglavlju bavimo se linearnim formama, tj. jednom od modernih metoda rješavanja diofantskih jednadžbi. Linearna forma u logaritmima algebarskih brojeva je izraz oblika $b_1 \log \alpha_1 + ... + b_n \log \alpha_n$, gdje su α_i algebarski brojevi, a b_i cijeli brojevi. Prilikom rješavanja diofantskih jednadžbi želimo odrediti donju ogradu za linearnu formu u logaritmima. Pritom, za određivanje donje ograde koristimo Bakerovu teoriju. Na primjerima ćemo pokazati kako koristimo linearne forme u logaritmima za rješavanje simultanih pellovskih jednadžbi te kako ih primjenjujemo na Fibonaccijeve brojeve.

Summary

In this graduate thesis, we are dealing with linear forms in logarithms to solve diophantine problems. At the beginning of this thesis we present the basic concepts and definitions we need to continue the work. In the second chapter, we discuss the results of diophantic approximations used in solving diophantine equations. Furthermore, in the third chapter we define the Pell's and generalized Pell equations. We also prove a series of theorems about existence and structure of the solutions of the equations mentioned. In the last chapter, we are dealing with linear forms, one of the modern methods of solving diophantine equations. Linear form in logarithms of algebraic numbers is a form expression $b_1 \log \alpha_1 + ... + b_n \log \alpha_n$, where α_i are algebraic numbers, and b_i integers. When solving diophantine equations, we want to determine the lower fence for linear form in logarithms. In doing so, we use Baker's theory to determine the bottom fence. In the examples we will show how we use linear forms in logarithms to solve simultaneous generalized Pell equations and how we apply them to Fibonacci numbers.

Životopis

Rođena sam 13. srpnja 1991. godine u Zagrebu. Osnovnu školu sam završila 2006. godine, a zatim upisujem III. gimnaziju u Zagrebu. Nakon završetka srednje škole upisujem Preddiplomski sveučilišni studij matematike na Prirodoslovno - matematičkom fakultetu u Zagrebu. Nakon dvije godine studiranja, 2012. godine, prebacujem se na nastavnički smjer. Studij nastavljam upisom Diplomskog sveučilišnog studija.