

Linearne forme u logaritmima i diofantska analiza

Alan Filipin

24. veljače 2010.

Sadržaj

1	Pellovske jednadžbe	5
1.1	Jednadžbe $x^2 - dy^2 = \pm 1, \pm 4$	5
1.2	Verižni razlomci	15
1.3	Jednadžba $x^2 - dy^2 = N$	21
2	Metode i algoritmi iz diofantskih aproksimacija	27
2.1	Liouvilleov i Rothov teorem	27
2.2	Hipergeometrijska metoda. Simultane diofantske aproksimacije	32
2.3	LLL-algoritam	38
2.4	Baker-Davenportova redukcija	50
3	Linearne forme u logaritmima	53
3.1	Uvod	53
3.2	Primjena linearnih formi na diofantske jednadžbe i probleme	56
3.2.1	Donja ograda za $ 2^m - 3^n $	57
3.2.2	Donje ograde za trag od α^n	62
3.2.3	Čiste potencije u binarno rekurzivnim nizovima	64
3.2.4	Najveći prosti faktori članova rekurzivnih nizova	68
3.2.5	Najveći prosti faktori u vrijednostima cjelobrojnih polinoma	69
3.2.6	Diofantska jednadžba $ax^n - by^n = c$	70
3.2.7	Catalanova jednadžba	71
3.2.8	Sustavi simultanih pellovskih jednadžbi	73
3.2.9	Thueove jednadžbe	76

Poglavlje 1

Pellovske jednadžbe

1.1 Jednadžbe $x^2 - dy^2 = \pm 1, \pm 4$

Diofantska jednadžba oblika

$$x^2 - dy^2 = 1, \tag{1.1}$$

gdje je d prirodan broj koji nije potpun kvadrat, naziva se Pellova jednadžba. Slučaj kad je d potpun kvadrat nećemo razmatrati jer je tada očito da jednadžba (1.1) ima samo trivijalno rješenje $x = \pm 1, y = 0$. Ova jednadžba je dobila ime po engleskom matematičaru Johnu Pellu, kojem je Euler pogrešno pripisao zasluge za njeno rješavanje. Neke pojedine jednadžbe ovog tipa nalaze se u tekstovima starogrčkih matematičara (Arhimed, Diofant), ali prvi su ih sustavno proučavali srednjovjekovni indijski matematičari (Brahmagupta). Od europskih matematičara, metode za rješavanje Pellovih jednadžbi dali su Brouncker, Fermat, Euler i Lagrange, koji je prvi dao i striktan dokaz korektnosti predložene metode.

Navedimo prvo nekoliko primjera gdje se pojavljuje Pellova jednadžba. Promotrimo problem nalaženja prirodnih brojeva koji su u isto vrijeme i trokutasti i kvadrati. Prisjetimo se da su trokutasti brojevi definirani sa $T_n = \frac{n(n+1)}{2}$. Znači tražimo prirodne brojeve x tako da je $\frac{x(x+1)}{2} = y^2$ za neki cijeli broj y . Tada dobivamo $4x^2 + 4x = 8y^2$, odnosno

$$(2x + 1)^2 - 8y^2 = 1, \tag{1.2}$$

što je Pellova jednadžba sa $d = 8$. Najmanji pozitivan $x \neq 1$ koji zadovoljava

(1.2) je $x = 8$, što nam daje trokutasti broj 36 koji je ujedno i kvadrat. Uskoro ćemo pokazati da postoji beskonačno mnogo takvih brojeva.

Drugi primjer je traženje cjelobrojnih (primitivnih) Pitagorinih trojki, čije se duljine kateta razlikuju za 1. Znamo da su stranice takvog trokuta dane sa $m^2 - n^2$ i $2mn$ za m i n prirodne brojeve. Tada moramo naći m i n za koje vrijedi

$$m^2 - n^2 - 2mn = \pm 1.$$

To možemo zapisati

$$(m - n)^2 - 2n^2 = \pm 1,$$

što je primjer Pellove jednadžbe s $d = 2$. Jedno od rješenja te jednadžbe je $m - n = 3$, $n = 2$, što nam daje trokut sa stranicama 20, 21 i 29.

Sada ćemo pokazati da jednadžba (1.1) uvijek ima netrivialno ($y \neq 0$) rješenje. Prvo nam treba jedna jednostavna lema.

Lema 1.1 (Dirichlet) *Neka je s prirodan broj. Tada uvijek postoje cijeli brojevi x i y tako da vrijedi*

$$|x - y\sqrt{d}| < \frac{1}{s} \leq \frac{1}{|y|}.$$

Dokaz. Za svaki cijeli broj y tako da je $0 \leq y \leq s$, definiramo $x = \lceil y\sqrt{d} \rceil$. Tada za svaki takav par (x, y) vrijedi

$$0 < x - y\sqrt{d} < 1.$$

Ako podijelimo segment $[0, 1]$ na s disjunktnih podintervala širine $\frac{1}{s}$, zaključujemo po Dirichletovom principu da dva od $s+1$ parova (x, y) , recimo (x_1, y_1) i (x_2, y_2) , zadovoljavaju da $x_1 - y_1\sqrt{d}$ i $x_2 - y_2\sqrt{d}$ leže u istom podintervalu. Kako je $y_1 \neq y_2$, vidimo da su i $x_1 - y_1\sqrt{d}$ i $x_2 - y_2\sqrt{d}$ različiti i

$$-\frac{1}{s} < x_1 - y_1\sqrt{d} - (x_2 - y_2\sqrt{d}) < \frac{1}{s},$$

odnosno

$$|x_1 - x_2 - (y_1 - y_2)\sqrt{d}| < \frac{1}{s}.$$

Također kako je $|y_1 - y_2| \leq s$, dobivamo

$$|x_1 - x_2 - (y_1 - y_2)\sqrt{d}| < \frac{1}{s} \leq \frac{1}{|y_1 - y_2|}.$$

■

Korolar 1.1 Postoji beskonačno mnogo parova cijelih brojeva (x, y) tako da je

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

Dokaz. Pretpostavimo suprotno, da postoji samo konačan skup S takvih parova (x, y) . Tada postoji minimalan prirodan broj M tako da je

$$\frac{1}{M} < \min\{|x - y\sqrt{d}| : (x, y) \in S\}.$$

Sada po lemi (za $s = M$) postoje cijeli brojevi x' i y' tako da je

$$|x' - y'\sqrt{d}| < \frac{1}{M} \leq \frac{1}{|y'|}.$$

Kako je $|x' - y'\sqrt{d}| < \frac{1}{|y'|}$, imamo $(x', y') \in S$. No s druge strane dobivamo

$$|x' - y'\sqrt{d}| < \frac{1}{M} < \min\{|x - y\sqrt{d}| : (x, y) \in S\},$$

što je kontradikcija. ■

Teorem 1.1 Pellova jednadžba $x^2 - dy^2 = 1$ ima barem jedno netrivialno rješenje.

Dokaz. Označimo sa S beskonačan skup svih parova cijelih brojeva (x, y) tako da je

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

Tada za sve $(x, y) \in S$ vrijedi

$$\begin{aligned} |x^2 - dy^2| &= |x - y\sqrt{d}||x + y\sqrt{d}| < \frac{1}{|y|} (|x - y\sqrt{d}| + |2y\sqrt{d}|) < \\ &< \frac{1}{|y|} \left(\frac{1}{|y|} + 2|y|\sqrt{d} \right) = \frac{1}{y^2} + 2\sqrt{d} \leq 1 + 2\sqrt{d}. \end{aligned}$$

Kako je $1 + 2\sqrt{d}$ fiksirano, ponovo po Dirchletovom principu, postoji beskonačno mnogo parova $(x, y) \in S$ tako da je

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

za neki fiksni $k \in \mathbb{Z}$ za koji vrijedi $|k| < 1 + 2\sqrt{d}$. Tada također postoji beskonačno mnogo takvih parova čije su vrijednosti x i y jednake modulo k . Neka su (x_1, y_1) i (x_2, y_2) dva takva para za koje vrijedi $x_1 \not\equiv \pm x_2$ i $y_1 \not\equiv \pm y_2$. Tada se lako provjeri da vrijedi

$$(x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - x_2y_1)^2 = k^2. \quad (1.3)$$

Sada iz $x_1y_2 - x_2y_1 \equiv 0 \pmod{k}$, zaključujemo da je i $x_1x_2 - dy_1y_2 \equiv 0 \pmod{k}$. Pa ako podijelimo (1.3) s k dobivamo

$$\left(\frac{x_1x_2 - dy_1y_2}{k}\right)^2 - d\left(\frac{x_1y_2 - x_2y_1}{k}\right)^2 = 1,$$

što nam daje netrivialno rješenje jednadžbe (1.1) ako je $x_1y_2 - x_2y_1 \neq 0$. No ako je $x_1y_2 - x_2y_1 = 0$, tada je $x_1x_2 - dy_1y_2 = \pm k$, a ove dvije jednakosti istovremeno mogu biti zadovoljene samo ako je $x_1 = \pm x_2$ i $y_1 = \pm y_2$, što smo uzeli da ne vrijedi. ■

Najmanje rješenje (x, y) u prirodnim brojevima Pellove jednadžbe (1.1), nazivamo njeno fundamentalno rješenje i označavamo ga s (x_1, y_1) ili $x_1 + y_1\sqrt{d}$.

Dokažimo sada da jednadžba (1.1) ima beskonačno mnogo rješenja.

Lema 1.2 *Ako je (x, y) rješenje jednadžbe (1.1), onda je $x + y\sqrt{d} > 1$ ako i samo ako vrijedi $x > 0, y > 0$.*

Dokaz. Ako vrijedi $x, y > 0$, jasno je $x + y\sqrt{d} \geq 1 + \sqrt{d} > 1$. S druge strane ako je $x + y\sqrt{d} > 1$, iz $(x + y\sqrt{d})(x - y\sqrt{d}) = 1$, dobivamo

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

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

Teorem 1.2 *Pellova jednadžba $x^2 - dy^2 = 1$ ima beskonačno mnogo rješenja. Ako je (x_1, y_1) njeno fundamentalno rješenje, onda su sve rješenja (u prirodnim brojevima) ove jednadžbe dana formulom*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{N}, \quad (1.4)$$

odnosno

$$x_n = x_1^n + \binom{n}{2} dx_1^{n-2}y_1^2 + \binom{n}{4} d^2x_1^{n-4}y_1^4 + \dots,$$

$$y_n = nx_1^{n-1}y_1 + \binom{n}{3} dx_1^{n-3}y_1^3 + \binom{n}{5} d^2x_1^{n-5}y_1^5 + \dots$$

Dokaz. Iz (1.4) dobivamo $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, pa imamo

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

Odnosno zaključujemo da su (x_n, y_n) doista rješenja naše Pellove jednadžbe i da ih ima beskonačno mnogo.

Pretpostavimo sada da postoji neko rješenje (s, t) u prirodnim brojevima koje nije oblika (x_n, y_n) za $n \in \mathbb{N}$. Tada postoji $m \in \mathbb{N}$ takav da vrijedi

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

Odnosno koristeći $(x_1 - y_1\sqrt{d})^m = (x_1 + y_1\sqrt{d})^{-m}$ dobivamo

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

Definirajmo sad $a, b \in \mathbb{Z}$ sa $a + b\sqrt{d} = (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m$. Tada je

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

Nadalje iz $a + b\sqrt{d} > 1$ zaključujemo po prethodnoj lemi da je $a, b > 0$. Sada smo dobili da je (a, b) rješenje jednažbe $x^2 - dy^2 = 1$ u prirodnim brojevima za koje vrijedi $a + b\sqrt{d} < x_1 + y_1\sqrt{d}$, što je kontradikcija. ■

Napomena 1.1 Iz (1.4) se lako dobiju rekurzije za nizove (x_n) i (y_n) . Naime vrijedi

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

gdje je (x_1, y_1) fundamentalno rješenje jednadžbe (1.1), a $(x_0, y_0) = (1, 0)$ njeno trivijalno rješenje.

Sada vidimo kako možemo dobiti sva rješenja jednadžbe (1.1) ako znamo njeno fundamentalno rješenje. No prethodni teoremi nam ne govore kako to rješenje naći. Vidjet ćemo da to nije sasvim jednostavan problem. Recimo kad

bi uvrštavajući redom prirodne brojeve htjeli naći najmanji x za koji jednadžba $x^2 - 1621y^2 = 1$ ima rješenje, prošlo bi dosta vremena prije nego bi taj x našli. U ovom slučaju takav x ima 76 znamenaka. No prije nego prijedemo na metode za nalaženje fundamentalnog rješenja, pozabavit ćemo se i ostalim jednadžbama iz naslova ovog odjeljka. Te jednadžbe se isto često nazivaju Pellove jednadžbe.

Za razliku od Pellove jednadžbe (1.1), jednadžba

$$x^2 - dy^2 = -1 \quad (1.5)$$

ne mora imati rješenja u cijelim brojevima. Nužan uvjet da jednadžba (1.5) ima rješenje je da d nema prostih djeljitelja oblika $p = 4k + 3$. Naime -1 mora biti kvadratni ostatak modulo d . No taj uvjet nije i dovoljan. Jedan od kriterija za rješivost ove jednadžbe je duljina perioda u razvoju u verižni razlomak broja \sqrt{d} , što ćemo uskoro vidjeti. Ako jednadžba (1.5) ima rješenja, onda njeno najmanje rješenje u prirodnim brojevima zovemo fundamentalno rješenje. Tada vrijedi sljedeći teorem.

Teorem 1.3 *Pretpostavimo da jednadžba $x^2 - dy^2 = -1$ ima rješenja i neka je $x_1 + y_1\sqrt{d}$ njeno fundamentalno rješenje. Tada je $(x_1 + y_1\sqrt{d})^2$ fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$. Nadalje ako definiramo $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$, tada su $x_{2n} + y_{2n}\sqrt{d}$ sva rješenja jednadžbe $x^2 - dy^2 = 1$, a $x_{2n+1} + y_{2n+1}\sqrt{d}$ sva rješenja jednadžbe $x^2 - dy^2 = -1$ u prirodnim brojevima.*

Dokaz. Kako je $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, imamo

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

pa je zaista $x_{2n} + y_{2n}\sqrt{d}$ rješenje jednadžbe (1.1), a $x_{2n+1} + y_{2n+1}\sqrt{d}$ rješenje jednadžbe (1.5). Pokažimo sada da je $(x_1 + y_1\sqrt{d})^2$ fundamentalno rješenje jednadžbe (1.1). Pretpostavimo suprotno, da za fundamentalno rješenje $a + b\sqrt{d}$ vrijedi

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

Tada iz $(x_1 + y_1\sqrt{d})(-x_1 + y_1\sqrt{d}) = 1$ zaključujemo $0 < -x_1 + y_1\sqrt{d} < 1$, pa imamo

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

Nadalje vrijedi $s^2 - dt^2 = -1$. Iz $s + t\sqrt{d} > 0$ i $s - t\sqrt{d} < 0$, zaključujemo $t > 0$. Ako je $s > 0$ onda dobivamo rješenje jednadžbe (1.5) u prirodnim brojevima za koje vrijedi $s + t\sqrt{d} < x_1 + y_1\sqrt{d}$ što je kontradikcija. Ukoliko je pak $s < 0$, tada iz $-x_1 + y_1\sqrt{d} < s + t\sqrt{d}$, zaključujemo $-s + t\sqrt{d} < x_1 + y_1\sqrt{d}$, pa je $|s| + t\sqrt{d}$ rješenje jednadžbe (1.5) u prirodnim brojevima koje je manje od fundamentalnog što je opet kontradikcija.

Ostalo je pokazati da su sva rješenja od (1.5) sadržana u nizu $(x_{2n+1} + y_{2n+1}\sqrt{d})$. Pretpostavimo suprotno, da postoji neko rješenje $u + v\sqrt{d}$ u prirodnim brojevima od (1.5) koje nije u tom nizu. Tada postoji $m \in \mathbb{N}$ takav da je

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

Ako ove nejednakosti pomnožimo s $(x_1 - y_1\sqrt{d})^{2m}$, dobivamo

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

gdje vrijedi $\sigma^2 - d\tau^2 = -1$. No malo prije smo pokazali da takvi σ i τ na postoje. ■

Primjer 1.1 *Jednadžba $x^2 - 40y^2 = -1$ nema rješenja. Naime, fundamentalno rješenje jednadžbe $x^2 - 40y^2 = 1$ dano je sa $19 + 3\sqrt{40}$. Kad bi jednadžba $x^2 - 40y^2 = -1$ imala rješenje onda bi za njeno fundamentalno rješenje $x + y\sqrt{40}$ vrijedilo $(x + y\sqrt{40})^2 = 19 + 3\sqrt{40}$, odnosno sustav jednadžbi*

$$x^2 + 40y^2 = 19, 2xy = 3$$

bi imao rješenje u prirodnim brojevima što je očito nemoguće.

Također je poznato da neki specijalni oblici broja d impliciraju rješivost jednadžbe (1.5).

Propozicija 1.1 *Ako je p prost broj i $p \equiv 1 \pmod{4}$, onda jednadžba $x^2 - py^2 = -1$ ima rješenja.*

Propozicija 1.2 *Ako je p prost broj i $p \equiv 5 \pmod{8}$, onda jednadžba $x^2 - 2py^2 = -1$ ima rješenja.*

Propozicija 1.3 *Ako je su p i q prosti brojevi i $p, q \equiv 5 \pmod{8}$, onda jednadžba $x^2 - 2pqy^2 = -1$ ima rješenja.*

Propozicija 1.4 *Ako je su p i q različiti prosti brojevi za koje vrijedi $p, q \equiv 1 \pmod{4}$ i $\left(\frac{p}{q}\right) = -1$ onda jednačba $x^2 - pqy^2 = -1$ ima rješenja, gdje je sa $(-)$ označen Legendreov simbol.*

Promotrimo sada jednačbu

$$x^2 - dy^2 = 4, \quad (1.6)$$

gdje je d prirodan broj koji nije potpun kvadrat. Odmah je jasno da ova jednačba uvijek ima rješenja u prirodnim brojevima. Naime, ako je (x, y) rješenje jednačbe $x^2 - dy^2 = 1$, onda je $(2x, 2y)$ rješenje jednačbe (1.6). No za neke d -ove postoje i rješenja koja se ne dobivaju na ovaj način. Sljedeći teorem se dokazuje potpuno analogno Teoremu 1.2.

Teorem 1.4 *Sva rješenja jednačbe $x^2 - dy^2 = 4$ u prirodnim brojevima dana su sa*

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

gdje je (x_1, y_1) fundamentalno, odnosno najmanje rješenje te jednačbe.

Promotrimo sada što se događa u ovisnosti o parnosti brojeva x_1 i y_1 . Kako je odmah jasno da ne može biti da je x_1 neparan, a y_1 paran, preostalo je razmotriti tri slučaja.

Prvo, ako su x_1 i y_1 oba parni, onda su x_n i y_n parni za svaki $n \in \mathbb{N}$ i $\frac{x_1}{2} + \frac{y_1}{2}\sqrt{d}$ je fundamentalno rješenje jednačbe $x^2 - dy^2 = 1$.

Ako je x_1 paran, a y_1 neparan, vidimo da je $d \equiv 0 \pmod{4}$, odnosno $d = 4d'$. U tom slučaju je $\frac{x_1}{2} + y_1\sqrt{d'}$ fundamentalno rješenje jednačbe $x^2 - d'y^2 = 1$.

Ukoliko su pak x_1 i y_1 neparni, nemamo odmah direktnu vezu s Pellovom jednačbom. No u tom slučaju vrijedi

$$d \equiv dy_1^2 \equiv x_1^2 - 4 \equiv 5 \pmod{8}.$$

Znači nužan uvjet da bi jednačba $x^2 - dy^2 = 4$ imala rješenja u neparnim brojevima jest $d \equiv 5 \pmod{8}$. No to nije i dovoljan uvjet, jer na primjer za $d = 37$ dobivamo da je fundamentalno rješenje od $x^2 - 37y^2 = 4$ jednako $(146, 24)$, a onda su sva rješenja parna.

Propozicija 1.5 Ako jednačba $x^2 - dy^2 = 4$ ima rješenja u neparnim brojevima i ako je $x_1 + y_1\sqrt{d}$ njeno fundamentalno rješenje, onda je

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

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

Dokaz. Kako su x_1 i y_1 neparni, vrijedi $d \equiv 5 \pmod{8}$. Tada je

$$x_1^2 + 3dy_1^2 \equiv 1 + 15 \equiv 0 \pmod{8}, \quad 3x_1^2 + dy_1^2 \equiv 3 + 5 \equiv 0 \pmod{8}.$$

No onda su brojevi $u_1 = \frac{1}{8}(x_1^3 + 3dx_1y_1^2)$ i $v_1 = \frac{1}{8}(3x_1^2y_1 + dy_1^3)$ cijeli i vrijedi $u_1^2 - dv_1^2 = \left(\frac{x_1^2 - dy_1^2}{4}\right)^3 = 1$. Pretpostavimo sada da $u_1 + v_1\sqrt{d}$ nije fundamentalno rješenje jednačbe $x^2 - dy^2 = 1$ te neka je $s_1 + t_1\sqrt{d}$ njeno fundamentalno rješenje. Tada vrijedi

$$1 < s_1 + t_1\sqrt{d} < \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^3.$$

Kad bi vrijedilo $s_1 + t_1\sqrt{d} < \frac{x_1 + y_1\sqrt{d}}{2}$ dobili bi rješenje $2s_1 + 2t_1\sqrt{d}$ jednačbe (1.6) koje je manje od $x_1 + y_1\sqrt{d}$. Također ne može vrijediti $s_1 + t_1\sqrt{d} = \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^2$, jer broj $\frac{x_1^2 + dy_1^2}{4}$ nije cijeli. Pa zaključujemo da je

$$\left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^i < s_1 + t_1\sqrt{d} < \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^{i+1},$$

za $i = 1$ ili $i = 2$. Sada množeći ove nejednakosti sa $\left(\frac{x_1 - y_1\sqrt{d}}{2}\right)^i$ dobivamo

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

gdje vrijedi $a^2 - db^2 = 4$, što je u kontradikciji s minimalnošću od $x_1 + y_1\sqrt{d}$. ■

Primjer 1.2 Fundamentalno rješenje jednačbe

$$x^2 - 5y^2 = 4$$

dano je sa $3 + \sqrt{5}$, pa je fundamentalno rješenje jednačbe

$$x^2 - 5y^2 = 1$$

dano sa $\left(\frac{3 + \sqrt{5}}{2}\right)^3 = 9 + 4\sqrt{5}$.

I na kraju dolazimo do jednadžbe

$$x^2 - dy^2 = -4. \quad (1.7)$$

Ta jednadžba ne mora imati rješenja. Ako pak jednadžba $x^2 - dy^2 = -1$ ima rješenja, onda i jednadžba (1.7) ima rješenja u parnim brojevima. No ova jednadžba može imati rješenja i u neparnim brojevima, npr. za slučaj $d = 5$ imamo rješenje $(x, y) = (1, 1)$. Nužan uvjet za postojanje rješenja u neparnim brojevima je ponovo $d \equiv 5 \pmod{8}$. Sljedeći teorem se dokazuje potpuno analogno kao teorem 1.3.

Teorem 1.5 *Pretpostavimo da jednadžba $x^2 - dy^2 = -4$ ima rješenja. Neka je nadalje $x_1 + y_1\sqrt{d}$ njeno fundamentalno rješenje. Tada su sva rješenja te jednadžbe dana sa*

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

za $n \in \mathbb{N}$ i n neparan. Nadalje, fundamentalno rješenje jednadžbe $x^2 - dy^2 = 4$ dano je sa $\frac{x_2 + y_2\sqrt{d}}{2} = \left(\frac{x_1 + y_1\sqrt{d}}{2} \right)^2$.

Prije nego prijedemo na metode za traženje fundamentalnog rješenja, spomenimo da su upravo spomenute Pellove jednadžbe u uskoj vezi s pronalaženjem jedinica u realnim kvadratnim poljima.

Neka je d cijeli broj koji nije potpun kvadrat. Tada skup svih brojeva oblika $u + v\sqrt{d}$, $u, v \in \mathbb{Q}$, uz uobičajene operacije zbrajanja i množenja kompleksnih brojeva, čini polje koje zovemo kvadratno polje i označavamo ga s $\mathbb{Q}(\sqrt{d})$. Kako je $\mathbb{Q}(\sqrt{dm^2}) = \mathbb{Q}(\sqrt{d})$, za $m \in \mathbb{Q}$ i $m \neq 0$, možemo pretpostaviti da je d kvadratno slobodan. Za svaki element $\alpha \in \mathbb{Q}(\sqrt{d})$ postoji jedinstveni normiran polinom minimalnog stupnja s racionalnim koeficijentima koji poništava α . Taj polinom zovemo minimalan polinom od α . Ukoliko su koeficijenti tog polinoma cjelobrojni, onda kažemo da je α cijeli broj. Cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ čine prsten koji označavamo s $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Prsten cijelih brojeva u kvadratnim poljima možemo opisati u ovisnosti o d . Naime, ukoliko je $d \equiv 2, 3 \pmod{4}$, onda je

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \left\{ u + v\sqrt{d} : u, v \in \mathbb{Z} \right\} = \mathbb{Z}[\sqrt{d}].$$

Ukoliko je pak $d \equiv 1 \pmod{4}$, onda je

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \left\{ \frac{u + v\sqrt{d}}{2} : u, v \in \mathbb{Z}, u \equiv v \pmod{2} \right\} = \mathbb{Z} \left[\frac{1 + \sqrt{d}}{2} \right].$$

Invertibilne elemente prstena $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ zovemo jedinice polja $\mathbb{Q}(\sqrt{d})$. Nadalje normu elementa $\alpha = u + v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ definiramo kao

$$N(\alpha) = (u + v\sqrt{d})(u - v\sqrt{d}) = u^2 - dv^2.$$

Za normu vrijede sljedeća svojstva:

- $N(\alpha\beta) = N(\alpha)N(\beta)$
- $N(\alpha) = 0 \Leftrightarrow \alpha = 0$
- $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \Leftrightarrow N(\alpha) \in \mathbb{Z}$
- $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ je jedinica $\Leftrightarrow N(\alpha) = \pm 1$

Sada je jasno da je problem pronalaženja jedinica u realnim kvadratnim poljima ($d > 0$) doista usko povezan s Pellovim jednažbama. Naime vrijedi sljedeće:

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

1.2 Verižni razlomci

Do sada smo pokazali kako možemo generirati sva rješenja Pellove jednažbe $x^2 - dy^2 = 1$ ukoliko znamo njeno fundamentalno rješenje. Također smo na primjeru vidjeli da nam treba efikasnija metoda za nalaženje fundamentalnog rješenja od uvrštavanja redom $y = 1, 2, 3, \dots$. Za jednu od tih metoda će nam trebati verižni (neprekidni) razlomci. Naime, konvergente razvoja u verižni razlomak iracionalnog broja α su jako dobre aproksimacije od α racionalnim brojem, a u ovom odjeljku ćemo dovesti u vezu to svojstvo s rješenjima Pellove jednažbe. Navedimo sada neke osnovne činjenice o verižnim razlomcima.

Definicija 1.1 (i) *Konačni verižni razlomak je izraz oblika*

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}},$$

gdje je $a_0 \in \mathbb{R}$ i $a_i > 0$ za $1 \leq i \leq n$. Za ovaj izraz ćemo koristiti oznaku $[a_0; a_1, \dots, a_n]$.

(ii) *Verižni razlomak se zove jednostavan ako vrijedi $a_0, \dots, a_n \in \mathbb{Z}$.*

(iii) *Verižni razlomak $c_k = [a_0; a_1, \dots, a_k]$ za $0 \leq k \leq n$ se zove k -ta konvergenta od $[a_0; a_1, \dots, a_n]$.*

Očito je svaki jednostavan konačan verižni razlomak racionalan broj. A vrijedi i obratno, svaki racionalan broj možemo zapisati kao jednostavan konačan verižni razlomak koristeći Euklidov algoritam. Nadalje, definirajmo za svaki (konačan) verižni razlomak $[a_0; a_1, \dots, a_n]$ brojeve p_0, p_1, \dots, p_n i q_0, q_1, \dots, q_n sa

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

$$q_0 = 1, q_1 = a_1, q_k = a_k q_{k-1} + q_{k-2},$$

za $k = 2, \dots, n$. Tada vrijedi sljedeća propozicija koju možemo dokazati indukcijom.

Propozicija 1.6 *Uz prijašnje oznake imamo*

$$(i) \quad c_k = \frac{p_k}{q_k},$$

$$(ii) \quad p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}, \text{ za } k \geq 1,$$

$$(iii) \quad c_k - c_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}, \text{ za } 1 \leq k \leq n,$$

$$(iv) \quad c_k - c_{k-2} = \frac{(-1)^k a_k}{q_k q_{k-2}}, \text{ za } 2 \leq k \leq n.$$

Propozicija nam kaže da je $c_k < c_{k-2}$ za $k \geq 3$ i k neparan, dok je $c_k > c_{k-2}$ ukoliko je $k \geq 2$ paran. Nadalje vrijedi

$$c_{2m} - c_{2m-1} = \frac{(-1)^{2m-1}}{q_{2m} q_{2m-1}} < 0,$$

pa zaključujemo

$$c_1 > c_3 > c_5 > \dots > c_6 > c_4 > c_2 > c_0.$$

Sada možemo definirati i beskonačni verižni razlomak.

Stvarno, ukoliko je $(a_n)_{n \geq 0}$ niz cijelih brojeva tako da je $a_n > 0$ za $n \geq 1$, definirajući $c_k = [a_0; a_1, \dots, a_k]$, možemo zaključiti:

- Niz $(c_{2n+1})_{n \geq 0}$ je padajući i ograničen, odnosno konvergentan.
- Niz $(c_{2n})_{n \geq 0}$ je rastući i ograničen, odnosno konvergentan.
- Niz $(c_{2n} - c_{2n+1})$ teži u nulu.

Odnosno iz ovoga možemo zaključiti da je niz $(c_n)_{n \geq 0}$ konvergentan pa je korektna sljedeća definicija.

Definicija 1.2 Neka je $(a_n)_{n \geq 0}$ niz cijelih brojeva tako da je $a_n > 0$ za $n \geq 1$. Beskonačan verižni razlomak definiramo kao limes konačnog verižnog razlomka, odnosno

$$[a_0; a_1, a_2, \dots] = \lim_{n \rightarrow \infty} c_n.$$

Lako se vidi da beskonačni verižni razlomci uvijek predstavljaju iracionalne brojeve. S druge strane, svaki iracionalan broj α može se razviti u beskonačan verižni razlomak o čemu nam govori sljedeća propozicija.

Propozicija 1.7 Neka je $\alpha = \alpha_0 \in \mathbb{R} \setminus \mathbb{Q}$ i neka je niz $(a_n)_{n \geq 0}$ definiran na sljedeći način

$$a_k = \lfloor \alpha_k \rfloor, \quad \alpha_{k+1} = \frac{1}{\alpha_k - a_k}, \quad k \geq 0.$$

Tada je $\alpha = [a_0; a_1, a_2, \dots]$.

Sada ćemo dokazati Legendreov teorem, iz kojeg će odmah slijediti da su sva rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ sadržana u konvergentama razvoja u verižni razlomak broja \sqrt{d} . Prvo nam treba jedna lema.

Lema 1.3 Neka je α iracionalan broj i neka su $c_k = \frac{p_k}{q_k}$ za $k \geq 0$ konvergente razvoja u verižni razlomak broja α . Ako su $p, q \in \mathbb{Z}$ tako da je $q > 0$ i k prirodan broj tako da vrijedi

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

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

Dokaz. Pretpostavimo suprotno da vrijedi $1 \leq q < q_{k+1}$. Tada nam sustav jednadžbi

$$p_k x + p_{k+1} y = p,$$

$$q_k x + q_{k+1} y = q,$$

daje

$$(p_{k+1} q_k - p_k q_{k+1}) x = q p_{k+1} - p q_{k+1}, \quad (p_k q_{k+1} - p_{k+1} q_k) y = q p_k - p q_k.$$

Odnosno vrijedi

$$x = (-1)^k (q p_{k+1} - p q_{k+1}), \quad y = (-1)^k (p q_k - q p_k).$$

Pokažimo sada da je $xy < 0$. Kad bi bilo $x = 0$, imali bi $\frac{p}{q} = \frac{p_{k+1}}{q_{k+1}}$, pa koristeći da su p_{k+1} i q_{k+1} relativno prosti dobivamo kontradikciju s $q < q_{k+1}$. Ako je pak $y = 0$, imamo $p = p_k x$, $q = q_k x$, odnosno

$$|q\alpha - p| = |x| |q_k \alpha - p_k| \geq |q_k \alpha - p_k|,$$

što je opet kontradikcija. Znači $xy \neq 0$.

Pretpostavimo sada da je $y < 0$. Tada iz $q_k x = q - q_{k+1} y$ zaključujemo $x > 0$. A ako je pak $y > 0$, zaključujemo $q_k x = q - q_{k+1} y < 0$, odnosno $x < 0$. Sad smo pokazali da su x i y različitog predznaka. Nadalje znamo da u ovisnosti o parnosti broja k vrijedi

$$\frac{p_k}{q_k} < \alpha < \frac{p_{k+1}}{q_{k+1}}$$

ili

$$\frac{p_{k+1}}{q_{k+1}} < \alpha < \frac{p_k}{q_k}.$$

Što nam u oba slučaja daje da su $q_k \alpha - p_k$ i $q_{k+1} \alpha - p_{k+1}$ različitog predznaka, odnosno da su $x(q_k \alpha - p_k)$ i $y(q_{k+1} \alpha - p_{k+1})$ istog predznaka. No tada vrijedi

$$\begin{aligned} |q\alpha - p| &= |(q_k x + q_{k+1} y)\alpha - (p_k x + p_{k+1} y)| = \\ &= |x(q_k \alpha - p_k) + y(q_{k+1} \alpha - p_{k+1})| = |x| |q_k \alpha - p_k| + |y| |q_{k+1} \alpha - p_{k+1}| > \\ &> |x| |q_k \alpha - p_k| \geq |q_k \alpha - p_k|, \end{aligned}$$

što nam daje željenu kontradikciju. ■

Teorem 1.6 (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, da $\frac{p}{q}$ nije konvergenta od α . I neka je k najveći prirodan broj takav da vrijedi $q \geq q_k$. Takav k uvijek postoji jer je $q_0 = 1$ i

$$\lim_{k \rightarrow \infty} q_k = \infty.$$

Kako je $q_k \leq q < q_{k+1}$ po prethodnoj lemi zaključujemo

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

odnosno

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

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

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

odnosno

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

što povlači $q_k > q$, a to je u kontradikciji s $q \geq q_k$. ■

Napomena 1.2 Sada je jasno da su sva rješenja u prirodnim brojevima jednadžbi $x^2 - dy^2 = \pm 1$ sadržana u konvergentama razvoja u verižni razlomak broja \sqrt{d} . Naime, očito je da za rješenje (x, y) jednadžbe $x^2 - dy^2 = \pm 1$ vrijedi $x > y$. Nadalje imamo

$$|x - y\sqrt{d}||x + y\sqrt{d}| = 1,$$

odnosno

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

pa dobivamo

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

Prisjetimo se sada da je \sqrt{d} kvadratna iracionalnost (iracionalan broj koji je korijen kvadratnog polinoma s cjelobrojnim koeficijentima). Tada mu je razvoj u verižni razlomak periodičan. Štoviše, kako je broj $[\sqrt{d}] + \sqrt{d}$ reduciran (veći je od 1, a konjugat $[\sqrt{d}] - \sqrt{d}$ mu je iz intervala $\langle -1, 0 \rangle$), razvoj mu je čisto periodičan. Odnosno \sqrt{d} ima razvoj oblika

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \dots, a_{l-1}, 2a_0}],$$

gdje je $a_0 = [\sqrt{d}]$ te vrijedi $a_1 = a_{l-1}, a_2 = a_{l-2}, \dots$.

Za razvoj kvadratnih iracionalnosti u verižni razlomak koristimo sljedeći algoritam. Ukoliko je α kvadratna iracionalnost, zapišemo je u obliku $\alpha = \frac{s_0 + \sqrt{d}}{t_0}$, gdje su $d, s_0, t_0 \in \mathbb{Z}$, $t_0 \neq 0$, d nije potpun kvadrat i $t_0 | (d - s_0^2)$. To je uvijek moguće napraviti. U našem slučaju kako je $\alpha = \sqrt{d}$, dobivamo $s_0 = 0, t_0 = 1$. Sada brojeve a_i računamo rekurzivno na sljedeći način:

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

Može se pokazati da za dovoljno velike indekse i vrijedi

$$0 < s_i < \sqrt{d}, \quad 0 < t_i < s_i + \sqrt{d} < 2\sqrt{d},$$

što povlači da su nizovi (s_i) i (t_i) ograničeni. Tako se i pokazuje da razvoj mora biti periodičan jer moraju postojati različiti indeksi j i k takvi da je $(s_j, t_j) = (s_k, t_k)$. Iz ovoga možemo dobiti i ocjenu za duljinu perioda u razvoju od \sqrt{d} . Naime iz ovog direktno dobivamo ocjenu $l(\sqrt{d}) < \sqrt{d} \cdot 2\sqrt{d} = 2d$. Preciznijom analizom odnosa između brojeva s_i i t_i , može se dobiti ocjena oblika $l(\sqrt{d}) = O(\sqrt{d} \log d)$, a slutnja je da vrijedi $l(\sqrt{d}) = O(\sqrt{d} \log \log d)$.

Nadalje, za iracionalan broj $\alpha = \sqrt{d}$ u notaciji propozicije 1.7. imamo $\alpha_k = \frac{s_k + \sqrt{d}}{t_k}$, pa ako u jednakosti

$$\sqrt{d} = \frac{\frac{s_{n+1} + \sqrt{d}}{t_{n+1}} p_n + p_{n-1}}{\frac{s_{n+1} + \sqrt{d}}{t_{n+1}} q_n + q_{n-1}},$$

izjednačimo racionalne i iracionalne dijelove, dobivamo

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

ukoliko još dodatno definiramo $p_{-1} = 1, q_{-1} = 0$. Sada možemo zaključiti da rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ odgovaraju onim n -ovima za koje je

$(-1)^{n+1}t_{n+1} = 1$. Lako se pokaže da je $t_i = 1$ ako i samo ako $l|i$, pa vrijedi sljedeći teorem.

Teorem 1.7 *Neka je l duljina perioda u razvoju u verižni razlomak broja \sqrt{d} .*

Ako je l paran, onda jednačba $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja od $x^2 - dy^2 = 1$ su dana sa $(x, y) = (p_{nl-1}, q_{nl-1})$, $n \in \mathbb{N}$. Specijalno, fundamentalno rješenje je dano sa (p_{l-1}, q_{l-1}) .

Ako je l neparan, onda su sve rješenja jednačbe $x^2 - dy^2 = -1$ dana sa $(x, y) = (p_{(2n-1)l-1}, q_{(2n-1)l-1})$, a sva rješenja jednačbe $x^2 - dy^2 = 1$ su dana sa $(x, y) = (p_{2nl-1}, q_{2nl-1})$, $n \in \mathbb{N}$. Specijalno, fundamentalno rješenje od $x^2 - dy^2 = 1$ je dano sa (p_{2l-1}, q_{2l-1}) .

Primjer 1.3 *Nađimo fundamentalno rješenje jednačbe*

$$x^2 - 71y^2 = 1.$$

Koristeći upravo opisani algoritam, dobivamo razvoj u verižni razlomak

$$\sqrt{71} = [8; \overline{2, 2, 1, 7, 1, 2, 2, 16}].$$

Za duljinu perioda dobivamo $l = 8$ pa i iz toga (osim što je $71 \equiv 3 \pmod{4}$) možemo zaključiti da jednačba $x^2 - 71y^2 = -1$ nema rješenja. Dok je fundamentalno rješenje jednačbe $x^2 - 71y^2 = 1$ dano sa $(x, y) = (p_7, q_7) = (3480, 413)$.

1.3 Jednačba $x^2 - dy^2 = N$

Neka je d prirodan broj koji nije potpun kvadrat. Tada jednačbu

$$x^2 - dy^2 = N, \tag{1.8}$$

gdje je $N \neq 0$ cijeli broj zovemo pellovska jednačba. Očito, takva jednačba ne mora biti rješiva, ali ako je $x + y\sqrt{d}$ njeno rješenje, a $u + v\sqrt{d}$ bilo koje rješenje jednačbe $x^2 - dy^2 = 1$, onda je i

$$(x + y\sqrt{d})(u + v\sqrt{d}) = xu + yvd + (yu + xv)\sqrt{d}$$

rješenje jednačbe (1.8). Za to rješenje kažemo da je asociirano s rješenjem $x + y\sqrt{d}$. Skup svih međusobno asociiranih rješenja tvore jednu klasu rješenja.

Nije teško odrediti pripadaju li dva rješenja $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ istoj klasi. Naime te rješenja su asocirana ako i samo ako vrijedi

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

Ako se klasa rješenja \mathbf{K} sastoji od rješenja $x_i + y_i\sqrt{d}$, $i = 1, 2, 3, \dots$, onda rješenja $x_i - y_i\sqrt{d}$, $i = 1, 2, 3, \dots$ tvore isto jednu klasu rješenja, koju označavamo s $\overline{\mathbf{K}}$. Za tu klasu kažemo da je konjugirana klasi \mathbf{K} . Konjugirane klase su općenito različite, ali mogu se u nekim slučajevima podudarati, pa ako je $\mathbf{K} = \overline{\mathbf{K}}$, kažemo da je klasa \mathbf{K} dvoznačna.

Među svim rješenjima $x + y\sqrt{d}$ u danoj klasi \mathbf{K} sada ćemo izabrati jedno $x^* + y^*\sqrt{d}$ na sljedeći način. Neka y^* bude najmanja nenegativna vrijednost od y što se pojavljuje u klasi \mathbf{K} . Ukoliko \mathbf{K} nije dvoznačna, time je jedinstveno određen i broj x^* . Ako je pak \mathbf{K} dvoznačna, x^* je jednoznačno određen ukoliko tražimo $x^* \geq 0$. Ovako izabrano rješenje $x^* + y^*\sqrt{d}$ zovemo fundamentalno rješenje jednadžbe $x^2 - dy^2 = N$.

Pretpostavimo sada da je $N > 0$. Tada vrijedi sljedeći teorem.

Teorem 1.8 *Neka je $u + v\sqrt{d}$ fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$. Tada za svako fundamentalno rješenje $x^* + y^*\sqrt{d}$ jednadžbe $x^2 - dy^2 = N$, vrijede nejednakosti*

$$0 \leq y^* \leq \frac{v}{\sqrt{2(u+1)}} \cdot \sqrt{N},$$

$$0 < |x^*| \leq \sqrt{\frac{1}{2}(u+1)N}.$$

Dokaz. Primjetimo da ako su ove nejednakosti točne za klasu \mathbf{K} , onda su točne i za konjugiranu klasu $\overline{\mathbf{K}}$, pa možemo pretpostaviti da je x^* pozitivan. Očito vrijedi

$$x^*u - dy^*v = x^*u - \sqrt{(x^{*2} - N)(u^2 - 1)} > 0.$$

Promotrimo sada rješenje

$$(x^* + y^*\sqrt{d})(u - v\sqrt{d}) = x^*u - dy^*v + (ux^* - vy^*)\sqrt{d},$$

koje pripada istoj klasi kao i $x^* + y^*\sqrt{d}$. Kako je $x^* + y^*\sqrt{d}$ fundamentalno rješenje te klase i kako je $x^*u - dy^*v > 0$ mora vrijediti

$$x^*u - dy^*v \geq x^*.$$

To nadalje povlači

$$x^{*2}(u-1)^2 \geq d^2 y^{*2} v^2 = (x^{*2} - N)(u^2 - 1),$$

odnosno

$$\frac{u-1}{u+1} \geq 1 - \frac{N}{x^{*2}}$$

i konačno

$$x^{*2} \leq \frac{1}{2}(u+1)N.$$

Iz ove ocjene, odmah dobivamo i ocjenu za y^* . ■

Ukoliko je $N < 0$, potpuno analogno dokazuje se sljedeći teorem.

Teorem 1.9 *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*

$$0 < y^* \leq \frac{v}{\sqrt{2(u-1)}} \cdot \sqrt{|N|},$$

$$0 \leq |x^*| \leq \sqrt{\frac{1}{2}(u-1)|N|}.$$

Spomenimo da ako znamo fundamentalno rješenje $x^* + y^*\sqrt{d}$ jednadžbe (1.8) koje pripada klasi \mathbb{K} , onda su sva rješenja u toj klasi dana sa

$$x_n + y_n\sqrt{d} = \pm(x^* + y^*\sqrt{d})(u + v\sqrt{d})^n, \quad n \in \mathbb{Z},$$

gdje je $u + v\sqrt{d}$ fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$.

Nadalje, iz ograničenosti fundamentalnih rješenja, jasno je da je broj klasa konačan, no ukoliko je N kvadratno slobodan možemo dobiti i bolju ocjenu za broj klasa u sljedećoj propoziciji.

Propozicija 1.8 *Neka je N kvadratno slobodan cijeli broj. Broj klasa rješenja jednadžbe $x^2 - dy^2 = N$ je najviše $2^{\omega(N)}$, gdje je $\omega(N)$ broj prostih faktora od N .*

Sljedeća propozicija nam govori kako možemo tražiti rješenja pellovske jednadžbe ako je $|N| < \sqrt{d}$.

Propozicija 1.9 *Pretpostavimo da je $|N| < \sqrt{d}$. Ako je $x + y\sqrt{d}$ rješenje jednadžbe $x^2 - dy^2 = N$ u prirodnim brojevima, onda je $\frac{x}{y}$ neka konvergenta u razvoju u verižni razlomak od \sqrt{d} .*

Dokaz. Ukoliko je $N > 0$, tada je $x > y\sqrt{d}$, pa vrijedi

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

Sada iz Legendreovog teorema slijedi da je $\frac{x}{y}$ neka konvergenta od \sqrt{d} .

Neka je sad $N < 0$. Tada vrijedi $x < y\sqrt{d}$ pa imamo

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

Odnosno možemo zaključiti da je $\frac{y}{x}$ neka, recimo i -ta konvergenta od $\frac{1}{\sqrt{d}}$. No tada je $\frac{x}{y}$ $(i - 1)$ -va konvergenta od \sqrt{d} . ■

Znači, rješivost jednadžbe $x^2 - dy^2 = N$ u relativno prostim brojevima x, y , ako je $|N| < \sqrt{d}$, možemo ustanoviti tako da \sqrt{d} razvijamo u verižni razlomak, te provjerimo zadovoljava li neka od prvih $2l$ konvergenti

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

Primjer 1.4 *Nađimo fundamentalna rješenja jednadžbe*

$$x^2 - 2y^2 = 119.$$

Fundamentalno rješenje jednadžbe $x^2 - 2y^2 = 1$ dano je sa $3 + 2\sqrt{2}$. Tada fundamentalna rješenja $x^ + y^*\sqrt{2}$ moraju zadovoljavati*

$$0 \leq y^* \leq \frac{2}{\sqrt{2} \cdot 4} \cdot \sqrt{119} < 8,$$

$$0 < |x^*| \leq \sqrt{\frac{1}{2} \cdot 4 \cdot 119} < 16.$$

Sada vidimo da jedino rješenja

$$11 + \sqrt{2}, -11 + \sqrt{2}, 13 + 5\sqrt{2}, -13 + 5\sqrt{2},$$

zadovoljavaju tražene nejednakosti i to su sva fundamentalna rješenja. Lako se vidi da ova rješenja nisu asocirana, znači u ovom slučaju imamo četiri klase rješenja.

Primjer 1.5 Riješimo jednadžbu

$$x^2 - 6y^2 = -29.$$

Fundamentalno rješenje jednadžbe $x^2 - 6y^2 = 1$ dano je sa $5 + 2\sqrt{6}$. Tada fundamentalna rješenja moraju zadovoljavati nejednakosti

$$0 \leq y^* \leq \frac{2}{\sqrt{2} \cdot 4} \cdot \sqrt{29} < 4,$$

$$0 < |x^*| \leq \sqrt{\frac{1}{2} \cdot 4 \cdot 29} < 8.$$

Pa dobivamo da su jedina fundamentalna rješenja $5 + 3\sqrt{6}$, $-5 + 3\sqrt{6}$ i ona nisu asocirana. Tada su sva rješenja dana sa

$$x + y\sqrt{6} = \pm(5 + 3\sqrt{6})(5 + 2\sqrt{6})^n$$

ili

$$x + y\sqrt{6} = \pm(-5 + 3\sqrt{6})(5 + 2\sqrt{6})^n,$$

gdje je $n \in \mathbb{Z}$.

Primjer 1.6 Pokažimo da jednadžba $x^2 - 82y^2 = 23$ nema rješenja. Naime, fundamentalno rješenje jednadžbe $x^2 - 82y^2 = 1$ dano je sa $163 + 18\sqrt{82}$. No tada za fundamentalno rješenje polazne jednadžbe $x^* + y^*\sqrt{82}$ vrijedi ocjena $y < 5$, a lako se provjeri da jednadžba $x^2 - 82y^2 = 23$ nema rješenja za $y = 1, 2, 3, 4$.

Poglavlje 2

Metode i algoritmi iz diofantskih aproksimacija

2.1 Liouvilleov i Rothov teorem

U ovom poglavlju ćemo obraditi neke metode koje dolaze iz diofantskih aproksimacija, a koje ćemo kasnije koristiti kod rješavanja nekih diofantskih problema i jednadžbi.

Definicija 2.1 *Neka je α kompleksan broj. Kažemo da je α algebarski broj, ako postoji polinom $f(x)$ s racionalnim koeficijentima, različit od nulpolinoma, takav da je $f(\alpha) = 0$. Ukoliko kompleksan broj nije algebarski, kažemo da je transcendentan.*

Teorem 2.1 *Neka je α algebarski broj. Tada postoji jedinstveni normirani polinom $P_\alpha(x)$ s racionalnim koeficijentima takav da je $P_\alpha(\alpha) = 0$. Nadalje, svaki polinom $Q(x) \in \mathbb{Q}[x]$ kojeg α poništava djeljiv je sa $P_\alpha(x)$.*

Dokaz. Kako je α algebarski broj, to postoji polinom $P(x) \in \mathbb{Q}[x]$ najmanjeg stupnja kojeg α poništava. Definirajmo $P_\alpha(x) = \frac{1}{c}P(x)$, gdje je c vodeći koeficijent od $P(x)$. Tada je očito $P_\alpha(x) = 0$ i P_α je normiran. Pokažimo sad da je P_α ireducibilan. U suprotnom bi bilo $P_\alpha(x) = p_1(x)p_2(x)$, pa bi imali $p_1(\alpha) = 0$ ili $p_2(\alpha) = 0$ što je u kontradikciji s minimalnošću stupnja od $P(x)$.

Neka je sad $Q(x) \in \mathbb{Q}[x]$ takav da vrijedi $Q(\alpha) = 0$. Ako podijelimo Q sa P_α , dobivamo $Q(x) = P_\alpha(x)q(x) + r(x)$, gdje je $\deg r < \deg P_\alpha$. No imamo

$r(\alpha) = 0$, pa iz minimalnosti stupnja od P_α zaključujemo da je $r(x)$ nulpolinom, odnosno da je Q djeljiv sa P_α .

Ostaje još pokazati jedinstvenost od P_α . No kad bi postojao neki ireducibilan normiran polinom $P_1(x) \in \mathbb{Q}[x]$ takav da je $P_1(\alpha) = 0$, prema upravo dokazanom imamo $P_1(x) = P_\alpha(x)q(x)$. No ireducibilnost od P_1 povlači da je $q(x)$ konstanta i to vrijedi $q(x) = 1$ jer su $P_1(x)$ i $P_\alpha(x)$ normirani. ■

Definicija 2.2 *Minimalni polinom algebarskog broja α je polinom $P_\alpha(x)$ opisan u prethodnom teoremu. Stupanj algebarskog broja je stupanj njegovog minimalnog polinoma.*

Definicija 2.3 *Za algebarski broj α kažemo da je algebarski cijeli broj, ako minimalni polinom od α ima cjelobrojne koeficijente.*

Teorem 2.2 (Liouville) *Neka je α algebarski broj stupnja d . Tada postoji konstanta $c(\alpha) > 0$ takva da za svaki racionalan broj $\frac{x}{y} \neq \alpha$, gdje je $y > 0$ vrijedi*

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

Dokaz. Dokaz ćemo podijeliti u tri dijela.

- (i) Neka je $P(x) \in \mathbb{Z}[x]$ polinom stupnja d za koji vrijedi $P(\alpha) = 0$ i čiji su koeficijenti relativno prosti.
- (ii) Tada za racionalan broj $\frac{x}{y} \neq \alpha$ trivijalno vrijedi

$$\left| P\left(\frac{x}{y}\right) \right| \geq \frac{1}{y^d}.$$

- (iii) Razvijmo P u Taylorov red oko α . Kako je $P(\alpha) = 0$, dobivamo

$$P\left(\frac{x}{y}\right) = \sum_{i=1}^d \left(\frac{x}{y} - \alpha\right)^i \frac{P^{(i)}(\alpha)}{i!}.$$

Nadalje možemo pretpostaviti da vrijedi

$$\left| \alpha - \frac{x}{y} \right| \leq 1,$$

jer smo inače gotovi s dokazom. Tada imamo

$$\frac{1}{y^d} \leq \left| P\left(\frac{x}{y}\right) \right| \leq \left| \alpha - \frac{x}{y} \right| \sum_{i=1}^d \frac{|P^{(i)}(\alpha)|}{i!}.$$

Sada tvrdnja teorema slijedi ako $c(\alpha)$ definiramo sa

$$\sum_{i=1}^d \frac{|P^{(i)}(\alpha)|}{i!} = \frac{1}{2c(\alpha)}.$$

■

Korolar 2.1 Broj $\alpha = \sum_{\nu=1}^{\infty} 10^{-\nu!}$ je transcendentan.

Dokaz. Definirajmo $y(k) = 10^{k!}$ i $x(k) = 10^{k!} \sum_{\nu=1}^k 10^{-\nu!}$. Tada su $y(k)$ i $x(k)$ cijeli brojevi i vrijedi

$$\begin{aligned} \alpha - \frac{x(k)}{y(k)} &= \sum_{\nu=k+1}^{\infty} 10^{-\nu!} < 10^{-(k+1)!} + 10^{-(k+1)!-1} + \dots = \\ &= \frac{10}{9} \cdot 10^{-(k+1)!} = \frac{10}{9y(k+1)} < \frac{c}{y(k)^d}, \end{aligned}$$

za bilo koje dane c i d , ukoliko je $k > k_0(c, d)$. Znači, možemo zaključiti da za bilo koji dani d , α nije algebarski broj stupnja d po Liouvilleovom teoremu, pa α mora biti transcendentan. ■

Liouville je bio prvi koji je pokazao postojanje transcendentnih brojeva, i to baš na ovaj način.

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

$$\left| \alpha - \frac{x}{y} \right| < \frac{1}{y^\mu} \quad (2.1)$$

ima samo konačno mnogo rješenja u racionalnim brojevima $\frac{x}{y}$.

Thue (1908) je poboljšao ovaj rezultat dokazavši da nejednakost (2.1) ima samo konačno mnogo rješenja ako je $\mu > \frac{1}{2}d + 1$. Siegel (1921) je dokazao kako

ista nejednadžba ima samo konačno mnogo rješenja ukoliko je $\mu > 2\sqrt{d}$. Dok su Dyson (1947) i Gelfond (1952) dokazali istu tvrdnju za $\mu > \sqrt{2d}$. 1955, Roth je dokazao isti rezultat za $\mu > 2$. Činjenica kako postoji beskonačno mnogo racionalnih brojeva $\frac{x}{y}$ tako da vrijedi

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

što slijedi iz Dirichletovog teorema (odnosno Korloara 1.1 ako \sqrt{d} zamijenimo bilo kojim iracionalnim brojem α), nam pokazuje kako je Rothov rezultat najbolji mogući.

Teorem 2.3 (Roth) *Ako je α algebarski broj i $\delta > 0$, onda postoji samo konačno mnogo racionalnih brojeva $\frac{x}{y}$ za koje vrijedi*

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

Napomena 2.1 • Rothov teorem je točan, ali trivijalan za $\alpha \in \mathbb{C} \setminus \mathbb{R}$.

- Znamo da postoji beskonačno mnogo racionalnih brojeva $\frac{x}{y}$ tako da vrijedi

$$\left| \alpha - \frac{x}{y} \right| < \frac{1}{y^2}$$

i samo konačno mnogo racionalnih brojeva $\frac{x}{y}$ tako da vrijedi

$$\left| \alpha - \frac{x}{y} \right| < \frac{1}{y^{2+\delta}},$$

za $\delta > 0$. Dok je za dani algebarski broj α stupnja ≥ 3 još uvijek nepoznato da li je α slabo aproksimabilan, odnosno da li postoji konstanta $c > 0$ takva da vrijedi

$$\left| \alpha - \frac{x}{y} \right| > \frac{c}{y^2}$$

za svaki racionalan broj $\frac{x}{y}$. Slutnja je da to ne vrijedi ni za jedan algebarski broj stupnja ≥ 3 .

- Slutnja je da vrijedi i jača tvrdnja od Rothovog teorema, odnosno da nejednadžba

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

ima samo konačno mnogo rješenja za $k > 1$.

Ideja dokaza Rothovog teorema. Ideja dokaza Rothovog teorema je da se modificiraju koraci u dokazu Liouvilleovog teorema.

(i) Izaberimo polinom $P(x) \in \mathbb{Z}[x]$, različit od nulpolinoma, koji je stupnja r i kojem je α korijen kratnosti q .

(ii) Sada se pokaže da je $P\left(\frac{x}{y}\right) \neq 0$, osim za konačno mnogo $\frac{x}{y}$. Tada je

$$\left|P\left(\frac{x}{y}\right)\right| \geq \frac{1}{y^r}.$$

(iii) Promotrimo Taylorov razvoj

$$P\left(\frac{x}{y}\right) = \sum_{i=q}^r \left(\frac{x}{y} - \alpha\right)^i \frac{P^{(i)}(\alpha)}{i!}.$$

Tada ako je $\left|\frac{x}{y} - \alpha\right| \leq 1$, imamo

$$\left|P\left(\frac{x}{y}\right)\right| \leq \left|\frac{x}{y} - \alpha\right|^q \cdot C(\alpha),$$

za neku konstantu $C(\alpha)$. Odnosno

$$\left|\frac{x}{y} - \alpha\right| \geq \frac{C'}{y^q},$$

za neku konstantu C' .

Ovakav pristup je dobar samo ako je $\frac{r}{q}$ malo. No ako je stupanj od α jednak d , onda je $r \geq qd$, odnosno $\frac{r}{q} \geq d$, pa ne dobivamo nikakvo poboljšanje Liouvilleovog teorema. U svom poboljšanju Liouvilleovog teorema Thue je koristio polinom u dvije varijable oblika $P(x_1, x_2) = x_2 Q(x_1) - P(x_1)$. Siegel je koristio nešto općenitiji polinom u dvije varijable, a isti pristup su imali Dyson i Gelfond. Dok je Roth prvi uspio riješiti sve poteškoće koje se javljaju kad se razmatra polinom u više od dvije varijable. Kod ovakvog pristupa najveća je poteškoća u koraku (ii). Naime, skup rješenja jednadžbe $P(x_1, \dots, x_m)$ je neka algebarska mnogostrukost u \mathbb{R}^m . U tom slučaju je teško pokazati da je $P\left(\frac{x}{y}, \dots, \frac{x}{y}\right) \neq 0$. Kako bi se to riješilo, promatraju se m -torke $\frac{x_1}{y_1}, \dots, \frac{x_m}{y_m}$ različitih racionalnih

aproksimacija i pokušava se dokazati da je $P\left(\frac{x_1}{y_1}, \dots, \frac{x_m}{y_m}\right) \neq 0$. Pokazuje se da $y_1 < y_2 < \dots < y_m$ moraju brzo rasti.

Kako bi ovaj pristup dao željeni rezultat, apsolutne vrijednosti $\left|\alpha - \frac{x_i}{y_i}\right|$ moraju biti male za svaki $i = 1, \dots, m$. Na primjer, u slučaju $m = 2$, trebamo dvije dobre aproksimacije $\frac{x_1}{y_1}$ i $\frac{x_2}{y_2}$ takve da je y_2 puno veće od y_1 . To je razlog zašto jedna dobra aproksimacija ne daje kontradikciju i zašto je ovaj rezultat (kao i sva ostala poboljšanja Liouvilleovog teorema dobivena ovom metodom) neefektivan, u smislu da ne daje nikakvu ogradu za veličinu nazivnika u dobrim aproksimacijama.

Efektivno poboljšanje Liouvilleovog teorema za određenu klasu iracionalnih algebarskih brojeva stupnja 3 je dao A. Baker (1964). Nakon toga je Feldman (1971) koristeći Bakerovu teoriju linearnih formi u logaritmima dao poboljšanje za općeniti algebarski broj α . Naime, dobio je rezultat tipa

$$\left|\alpha - \frac{x}{y}\right| > \frac{c(\alpha)}{y^{d-c_1(\alpha)}},$$

gdje su $c(\alpha)$ i $c_1(\alpha)$ eksplicitne konstante. Nažalost, $c_1(\alpha)$ dobivena na ovaj način je obično jako mala.

2.2 Hipergeometrijska metoda. Simultane diofantske aproksimacije

Kao što smo vidjeli u prošlom odjeljku, ukoliko je α algebarski broj stupnja $d \geq 2$ i $\kappa > 2$, onda Rothov teorem povlači da postoji konstanta $c = c(\alpha, \kappa) > 0$ takva da vrijedi

$$\left|\alpha - \frac{x}{y}\right| > \frac{c}{y^\kappa} \tag{2.2}$$

za sve racionalne brojeve $\frac{x}{y}$, $y > 0$. No, dokaz Rothovog teorema nije efektivan, odnosno ne daje nam metodu za eksplicitno određivanje konstante c . Mi ćemo sada dokazati nejednakost (2.2) s eksplicitnim vrijednostima od c i $\kappa < d$, za jednu specijalnu klasu algebarskih brojeva.

Neka je $n \in \mathbb{N}$. Definirajmo

$$\mu_n = \prod_{p|n} p^{\frac{1}{p-1}}.$$

Može se pokazati da vrijedi $1 \leq \mu_n \leq n$.

Teorem 2.4 (Baker) *Neka su $m, n \in \mathbb{N}$, takvi da vrijedi $n \geq 3$ i $1 \leq m \leq n$. Neka su nadalje a i b prirodni brojevi za koje vrijedi $\frac{7}{8}a \leq b < a$ i $a \equiv b \pmod{n}$. Pretpostavimo, nadalje da je*

$$\lambda = 4b(a-b)^{-2}\mu_n^{-1} > 1.$$

Tada $\alpha = \left(\frac{a}{b}\right)^{\frac{m}{n}}$ zadovoljava nejednakost (2.2) za sve racionalne brojeve $\frac{x}{y}$, $y > 0$, gdje su c i κ dani sa

$$\lambda^{\kappa-1} = 2\mu_n(a+b),$$

$$c^{-1} = 2^{\kappa+2}(a+b).$$

Napomena 2.2 *Primjetimo da se uvjet $a \equiv b \pmod{n}$ može uvijek zadovoljiti, i to tako da a i b pomnožimo s n ako je potrebno. No to nam povećava vrijednosti konstanti κ i c^{-1} . Također, primjetimo da je rezultat teorema interesantan (u svjetlu Liouvilleovog teorema) samo ako je $\kappa \leq n$.*

Korolar 2.2 *Za sve racionalne brojeve $\frac{x}{y}$, $y > 0$, vrijedi*

$$\left| \sqrt[3]{2} - \frac{x}{y} \right| > \frac{1.36 \cdot 10^{-6}}{y^{2.954}}.$$

Dokaz. Stavimo u prethodnom teoremu $n = 3, m = 1, a = 128$ i $b = 125$. Tada je $\left(\frac{a}{b}\right)^{\frac{m}{n}} = \frac{4}{5}\sqrt[3]{2}$. Nadalje dobivamo $\mu_3 = \sqrt{3}$ i $\lambda = \frac{500}{9\sqrt{3}} > 1$. Tada za konstante c i κ dobivamo

$$c \approx 0.0001275, \kappa \approx 2.95377$$

pa nam prethodni teorem povlači da za sve racionalne brojeve $\frac{x}{y}$, $y > 0$, vrijedi

$$\left| \frac{4}{5}\sqrt[3]{2} - \frac{4x}{5y} \right| > \frac{0.000127}{(5y)^{2.954}},$$

odnosno

$$\left| \sqrt[3]{2} - \frac{x}{y} \right| > \frac{1.36 \cdot 10^{-6}}{y^{2.954}}.$$

■

Ovaj rezultat je poboljšao Easton (1986) i dobio nejednakost

$$\left| \sqrt[3]{2} - \frac{x}{y} \right| > \frac{2.2 \cdot 10^{-8}}{y^{2.795}},$$

a najbolji rezultat ovakvog tipa dobio je Bennett (1997):

$$\left| \sqrt[3]{2} - \frac{x}{y} \right| > \frac{0.25}{y^{2.45}}.$$

Mi ćemo se vratiti na nejednakosti ovog tipa vrlo skoro. No ono što će nama trebati u primjenama za rješavanje nekih problema su simultane diofantske aproksimacije. Već smo vidjeli da se problemi vezani uz diofantske jednadžbe mogu preformulirati u odgovarajuće probleme iz diofantskih aproksimacija. No, u nekim problemima se osim običnih aproksimacija, mogu pojaviti i tzv. simultane diofantske aproksimacije, odnosno problemi istovremene aproksimacije više realnih brojeva. Jedan primjer toga je sustav simultanih Pellovih (ili pellovskih) jednadžbi koji ćemo mi detaljno rješavati kasnije. Primjer takvog sustava je

$$x^2 - 2y^2 = 1, \quad z^2 - 3y^2 = 1.$$

Ovo zovemo sustav simultanih jednadžbi, jer nam se u dvije jednadžbe pojavljuje ista nepoznanica y . U ovom konkretnom primjeru imamo

$$\left| \sqrt{2} - \frac{x}{y} \right| < \frac{1}{2y^2}, \quad \left| \sqrt{3} - \frac{z}{y} \right| < \frac{1}{2y^2},$$

odnosno vidimo da bi iracionalni brojevi $\sqrt{2}$ i $\sqrt{3}$ trebali imati jako dobre aproksimacije racionalnim brojevima s istim nazivnikom. Pitanje je mogu li takve aproksimacije uopće postojati, te posebno koji je "kritični" eksponent koji razdvaja aproksimacije kojih ima beskonačno mnogo, od onih kojih može biti samo konačno mnogo.

Navedimo sada analogne rezultate iz običnih aproksimacija, odnosno analogone Dirichletovog i Rothovog teorema.

Teorem 2.5 (Dirichlet) *Neka su α_{ij} , $i = 1, \dots, n; j = 1, \dots, m$ realni brojevi, te neka je $Q > 1$ prirodan broj. Tada postoje cijeli brojevi $q_1, \dots, q_m, p_1, \dots, p_n$ takvi da vrijedi*

$$1 \leq \max\{|q_1|, \dots, |q_m|\} < Q^{\frac{n}{m}},$$

$$|\alpha_{i1}q_1 + \dots + \alpha_{im}q_m - p_i| \leq \frac{1}{Q}, \quad i = 1, \dots, n. \quad (2.3)$$

Dokaz. Promotrimo točke

$$(\{\alpha_{11}y_1 + \dots + \alpha_{1m}y_m\}, \dots, \{\alpha_{n1}y_1 + \dots + \alpha_{nm}y_m\}),$$

gdje su y_j cijeli brojevi koji zadovoljavaju $0 \leq y_j < Q^{\frac{n}{m}}$, za $j = 1, \dots, m$. Tada postoji barem Q^n takvih točaka i to tako da svaka od njih leži u jediničnoj kocki $I^n = [0, 1]^n$, pa zajedno s točkom $(1, 1, \dots, 1) \in I^n$ imamo barem $Q^n + 1$ točaka iz I^n .

Podijelimo sada I^n na Q^n u parovima disjunktnih potkocaka čiji su bridovi duljine $\frac{1}{Q}$. Tada po Dirichletovom principu barem dvije od promatranih točaka pripadaju istoj potkocki, pa neka su to točke

$$(\alpha_{11}y_1 + \dots + \alpha_{1m}y_m - x_1, \dots, \alpha_{n1}y_1 + \dots + \alpha_{nm}y_m - x_n)$$

i

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

Naravno, možemo pretpostaviti da vrijedi $(y_1, \dots, y_m) \neq (y'_1, \dots, y'_m)$. Definirajmo sad $q_j = y_j - y'_j$ za $j = 1, \dots, m$ i $p_i = x_i - x'_i$ za $i = 1, \dots, n$. Sada se lako provjeri da ovako definirani p_i i q_j zadovoljavaju (2.3). ■

Korolar 2.3 *Neka je barem jedan od brojeva $\alpha_1, \alpha_2, \dots, \alpha_n$ iracionalan. Tada postoji beskonačno mnogo n -torki racionalnih brojeva $\frac{p_1}{q}, \dots, \frac{p_n}{q}$ takvih da vrijedi*

$$\left| \alpha_i - \frac{p_i}{q} \right| < \frac{1}{q^{1+\frac{1}{n}}}, \quad i = 1, \dots, n. \quad (2.4)$$

Dokaz. Primjenimo teorem 2.5 za $m = 1$. Tada za svaki prirodan broj $Q > 1$ postoje relativno prosti cijeli brojevi q, p_1, \dots, p_n takvi da vrijedi

$$1 \leq q < Q^n, \quad |\alpha_i q - p_i| \leq \frac{1}{Q}, \quad i = 1, \dots, n. \quad (2.5)$$

Jasno je da (2.5) povlači (2.4). Sada bez smanjenja općenitosti možemo pretpostaviti da je α_1 iracionalan. Tada je $|\alpha_1 q - p_1| \neq 0$, pa za fiksne q, p_1, \dots, p_n (2.5) može vrijediti samo ako je $Q \leq \frac{1}{|\alpha_1 q - p_1|}$. Pa ako sad pustimo $Q \rightarrow \infty$, dobivamo beskonačno mnogo različitih rješenja. ■

Korolar 2.4 Neka su $1, \alpha_1, \dots, \alpha_m$ realni brojevi, linearno nezavisni nad \mathbb{Q} . Tada postoji beskonačno mnogo $(m+1)$ -torki relativno prostih brojeva (q_1, \dots, q_m, p) sa svojstvom

$$q = \max\{|q_1|, \dots, |q_m|\} > 0, \quad |\alpha_1 q_1 + \dots + \alpha_m q_m - p| < \frac{1}{q^m}.$$

Sada ćemo dokazati analogon Rothovog teorema. Za to nam treba poznati Schmidov teorem o potprostorima.

Teorem 2.6 (Schmidt) Neka je dano n linearno nezavisnih linearnih formi L_1, \dots, L_n u n varijabli s algebarskim koeficijentima, te neka je $\delta > 0$. Tada sve cjelobrojne točke $x = (x_1, \dots, x_n)$ koje zadovoljavaju

$$|L_1(x) \cdot \dots \cdot L_n(x)| < \frac{1}{\|x\|^\delta}$$

leže u konačno mnogo pravih potprostora od \mathbb{Q}^n , gdje je $\|x\| = \max\{|x_i| : i = 1, \dots, n\}$.

Korolar 2.5 Neka su $\alpha_1, \dots, \alpha_n$ algebarski brojevi takvi da su $1, \alpha_1, \dots, \alpha_n$ linearno nezavisni nad \mathbb{Q} , te neka je $\delta > 0$. Tada postoji samo konačno mnogo n -torki racionalnih brojeva $\frac{p_1}{q}, \dots, \frac{p_n}{q}$ takvih da vrijedi

$$\left| \alpha_i - \frac{p_i}{q} \right| < \frac{1}{q^{1+\frac{1}{n}+\delta}}, \quad i = 1, \dots, n. \quad (2.6)$$

Dokaz. Ukoliko pomnožimo sve nejednakosti u (2.6) i onda još sve to pomnožimo s q^{n+1} , dobivamo

$$q|\alpha_1 q - p_1| \cdots |\alpha_n q - p_n| < \frac{1}{q^\delta}.$$

Sada ćemo pokazati da ovu nejednakost može zadovoljavati samo konačno mnogo n -torki. Definirajmo $x = (p_1, \dots, p_n, q) \in \mathbb{Z}^{n+1}$ i promotrimo linearne forme

$$L_i(x_1, x_2, \dots, x_{n+1}) = \alpha_i x_{n+1} - x_i, \quad i = 1, \dots, n$$

i

$$L_{n+1}(x_1, x_2, \dots, x_{n+1}) = x_{n+1}.$$

Tada za dovoljno veliki q dobivamo

$$|L_1(x) \cdot \dots \cdot L_{n+1}(x)| < \frac{1}{q^\delta} < \frac{1}{\|x\|^{\frac{\delta}{2}}}.$$

2.2. HIPERGEOMETRIJSKA METODA. SIMULTANE DIOFANTSKE APROKSIMACIJE37

Sada po teoremu 2.6 zaključujemo da rješenja ove nejednadžbe leže u konačno mnogo pravih potprostora od \mathbb{Q}^{n+1} . Takvi potprostori zadani su jednadžbom

$$c_1x_1 + \dots + c_{n+1}x_{n+1} = 0, \quad c_i \in \mathbb{Q}.$$

Pa rješenja nejednakosti (2.6) koja leže u takvom potprostoru zadovoljavaju

$$(c_1\alpha_1 + \dots + c_n\alpha_n + c_{n+1})q = c_1(\alpha_1q - p_1) + \dots + c_n(\alpha_nq - p_n).$$

Definirajmo sada $\gamma = |c_1\alpha_1 + \dots + c_n\alpha_n + c_{n+1}|$. Onda je $\gamma > 0$ zbog linearne nezavisnosti od $1, \alpha_1, \dots, \alpha_n$. Za dani potprostor γ je fiksna, a vrijedi

$$\gamma \cdot q \leq |c_1||\alpha_1q - p_1| + \dots + |c_n||\alpha_nq - p_n| \leq |c_1| + \dots + |c_n|.$$

Znači, za dani potprostor, q je omeđen, pa samo konačno mnogo q pa i n -torki $\frac{p_1}{q}, \dots, \frac{p_n}{q}$ zadovoljava (2.6), a kako potprostora ima samo konačno mnogo tvrdnja korolara je dokazana. ■

Kao i kod Rothovog teorema, i ovaj rezultat je neefektivan u smislu da ne daje eksplicitnu gornju ogradu za veličinu q -ova koji zadovoljavaju (2.6). Postoje neki efektivni rezultati ovog tipa za specijalne klase algebarskih brojeva, a mi ćemo spomenuti Bennettov teorem, koji ćemo kasnije i koristiti.

Teorem 2.7 (Bennett) *Neka su a_i, p_i, q i N cijeli brojevi za $0 \leq i \leq 2$, takvi da vrijedi $a_0 < a_1 < a_2$ i $a_j = 0$ za neki $0 \leq j \leq 2$. Neka je nadalje $q \neq 0$ i $N > M^9$, gdje je*

$$M = \max_{0 \leq i \leq 2} \{|a_i|\}.$$

Tada vrijedi

$$\max_{0 \leq i \leq 2} \left\{ \left| \sqrt{1 + \frac{a_i}{N}} - \frac{p_i}{q} \right| \right\} > (130N\gamma)^{-1}q^{-\mu},$$

gdje je

$$\mu = 1 + \frac{\log(33N\gamma)}{\log(1.7N^2 \prod_{0 \leq i < j \leq 2} (a_i - a_j)^{-2})}$$

i

$$\gamma = \begin{cases} \frac{(a_2 - a_0)^2 (a_2 - a_1)^2}{2a_2 - a_0 - a_1}; & a_2 - a_1 \geq a_1 - a_0, \\ \frac{(a_2 - a_0)^2 (a_2 - a_1)^2}{2a_2 - a_0 - a_1}; & a_2 - a_1 < a_1 - a_0. \end{cases}$$

2.3 LLL-algoritam

U ovom odjeljku ćemo opisati jednu metodu koja dolazi iz diofantskih aproksimacija, a kojom ćemo reducirati gornju ogradu za rješenja diofantskih jednadžbi kojima ćemo se kasnije baviti. Za to nam prvo treba definicija rešetke.

Definicija 2.4 *Neka je $n \in \mathbb{N}$. Rešetka je \mathbb{Z} -modul razapet s n linearno nezavisnih vektora iz \mathbb{R}^n . Skup tih vektora zovemo baza rešetke. Znači rešetka je skup*

$$\mathcal{L} = \left\{ \sum_{i=1}^n x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\},$$

gdje su vektori $\mathbf{b}_1, \dots, \mathbf{b}_n$ baza rešetke \mathcal{L} .

Očito vektori $\mathbf{b}_1, \dots, \mathbf{b}_n$ čine bazu i od \mathbb{R}^n . Sada sa B označimo matricu čiji su stupci vektori $\mathbf{b}_1, \dots, \mathbf{b}_n$. Može se pokazati da je baza rešetke jedinstvena do na množenje s desna s elementom iz $GL_n(\mathbb{Z})$. Znači dobro je definirana determinanta rešetke $\Delta(\mathcal{L}) = |\det(B)|$, jer ne ovisi o izboru baze. Prisjetimo se sada Gram-Schmidtoveg postupka ortogonalizacije. Unitarni prostor \mathbb{R}^n s bazom $\mathbf{b}_1, \dots, \mathbf{b}_n$ ima pripadnu ortogonalnu bazu $\mathbf{b}_1^*, \dots, \mathbf{b}_n^*$ gdje je

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^*, \quad i = 1, \dots, n,$$

$$\mu_{i,j} = \frac{(\mathbf{b}_i, \mathbf{b}_j^*)}{(\mathbf{b}_j^*, \mathbf{b}_j^*)}.$$

U našoj situaciji od toga nećemo imati previše koristi jer mi promatramo bazu rešetke \mathcal{L} , a ne cijelog prostora \mathbb{R}^n pa možemo napraviti takvu promjenu baze samo ako su $\mu_{i,j} \in \mathbb{Z}$, jer bi se inače moglo dogoditi da izađemo iz rešetke. Znači, Gram-Schmidtovim postupkom nećemo općenito moći dobiti ortogonalnu bazu rešetke, pa je ideja da nađemo neku drugu bazu koja će biti blizu te ortogonalne baze. To ćemo napraviti LLL-algoritmom, ali prije nego prijedemo na algoritam i kažemo nešto o njemu, definirajmo tu bazu, i spomenimo neka osnovna svojstva koja ta baza ima.

Definicija 2.5 *Bazu $\mathbf{b}_1, \dots, \mathbf{b}_n$ rešetke \mathcal{L} ćemo zvati LLL-reducirana, ako pripadna ortogonalna baza dobivena Gram-Schmidtovim postupkom $\mathbf{b}_1^*, \dots, \mathbf{b}_n^*$ i*

brojevi $\mu_{i,j}$ zadovoljavaju:

$$|\mu_{i,j}| \leq \frac{1}{2}, \quad 1 \leq j < i \leq n, \quad (2.7)$$

$$\|\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*\|^2 \geq \frac{3}{4}\|\mathbf{b}_{i-1}^*\|^2, \quad 1 < i \leq n. \quad (2.8)$$

Napomena 2.3 Koristeći ortogonalnost vektora \mathbf{b}_i^* relacija (2.8) se može ekvivalentno zapisati:

$$\|\mathbf{b}_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|\mathbf{b}_{i-1}^*\|^2. \quad (2.9)$$

Takvu reduciranu bazu je uvijek moguće naći, i to vrlo brzo, u polinomijalnom vremenu, LLL-algoritmom. Napomenimo još da reducirana baza nije jedinstvena.

Teorem 2.8 Neka je $\mathbf{b}_1, \dots, \mathbf{b}_n$ LLL-reducirana baza rešetke \mathcal{L} , te neka su $\mathbf{b}_1^*, \dots, \mathbf{b}_n^*$ vektori pripadne ortogonalne baze dobivene Gram-Schmidtovim postupkom ortogonalizacije. Tada vrijedi

- (i) $\|\mathbf{b}_j\|^2 \leq 2^{i-1}\|\mathbf{b}_i^*\|^2$ za $1 \leq j \leq i \leq n$.
- (ii) $\Delta(\mathcal{L}) \leq \prod_{i=1}^n \|\mathbf{b}_i\| \leq 2^{\frac{n(n-1)}{4}} \Delta(\mathcal{L})$,
- (iii) $\|\mathbf{b}_1\| \leq 2^{\frac{n-1}{4}} \Delta(\mathcal{L})^{\frac{1}{n}}$,
- (iv) Za svaki vektor $\mathbf{x} \in \mathcal{L}$, $\mathbf{x} \neq (0, \dots, 0)$ vrijedi $\|\mathbf{b}_1\|^2 \leq k_1 \|\mathbf{x}\|^2$, gdje je $k_1 = \max \left\{ \frac{\|\mathbf{b}_i\|^2}{\|\mathbf{b}_i^*\|^2} : 1 \leq i \leq n \right\}$.
- (v) Neka je \mathbf{y} vektor koji ne pripada rešetki \mathcal{L} . Definirajmo $\sigma = (\sigma_1, \dots, \sigma_n)^t \in \mathbb{R}^n$, $\sigma = B^{-1}\mathbf{y}$, gdje je $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ matrica čiji su stupci LLL-reducirana baza rešetke \mathcal{L} . Neka je nadalje i_0 najveći indeks tako da je $\{\sigma_{i_0}\} \neq 0$. Tada za sve vektore $\mathbf{x} \in \mathcal{L}$ vrijedi

$$\|\mathbf{x} - \mathbf{y}\|^2 \geq k_1^{-1} \{\sigma_{i_0}\} \|\mathbf{b}_1\|^2.$$

Dokaz. Dokazat ćemo tvrdnje (i) i (iv).

(i) Za $i = 2, \dots, n$ vrijedi

$$\|\mathbf{b}_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|\mathbf{b}_{i-1}^*\|^2 \geq \frac{1}{2} \|\mathbf{b}_{i-1}^*\|^2.$$

Sada se indukcijom može pokazati da za $1 \leq j \leq i \leq n$ vrijedi

$$\|\mathbf{b}_j^*\|^2 \leq 2^{i-j} \|\mathbf{b}_i^*\|^2.$$

Tada iz definicije Gram-Schmidtove baze, zbog ortogonalnosti imamo

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

A iz toga za $1 \leq j \leq i \leq n$ dobivamo

$$\|\mathbf{b}_j\|^2 \leq 2^{j-1} \|\mathbf{b}_j^*\|^2 \leq 2^{j-1+i-j} \|\mathbf{b}_i^*\|^2 = 2^{i-1} \|\mathbf{b}_i^*\|^2.$$

(iv) Iz definicije broja k_1 slijedi $\|\mathbf{b}_1\|^2 \leq k_1 \|\mathbf{b}_i^*\|^2$ za $1 \leq i \leq n$. Nadalje imamo

$$\mathbf{x} = \sum_{i=1}^n r_i \mathbf{b}_i = \sum_{i=1}^n r_i^* \mathbf{b}_i^*,$$

za neke $r_i \in \mathbb{Z}$ i $r_i^* \in \mathbb{R}$. Označimo sad s i_0 najveći indeks tako da je $r_{i_0} \neq 0$. Tada je jasno $r_{i_0} = r_{i_0}^*$, pa vrijedi

$$\|\mathbf{x}\|^2 = \sum_{i=1}^n r_i^{*2} \|\mathbf{b}_i^*\|^2 \geq r_{i_0}^{*2} \|\mathbf{b}_{i_0}^*\|^2 \geq \|\mathbf{b}_{i_0}^*\|^2 \geq k_1^{-1} \|\mathbf{b}_1\|^2.$$

■

Napomena 2.4 U primjenama se pokazuje da je konstanta k_1 iz prethodnog teorema u jako puno slučajeva jako blizu 1. Znači kad dobijemo reduciranu bazu, njen prvi vektor \mathbf{b}_1 će biti jako dobra aproksimacija najmanjeg vektora u rešetki.

Primijetimo da nam zadnji teorem daje donju ogradu za

$$l(\mathcal{L}, \mathbf{y}) = \begin{cases} \min\{\|\mathbf{x} - \mathbf{y}\| : \mathbf{x} \in \mathcal{L}\}, & \mathbf{y} \notin \mathcal{L} \\ \min\{\|\mathbf{x}\| : \mathbf{x} \in \mathcal{L}, \mathbf{x} \neq (0, \dots, 0)\}, & \mathbf{y} \in \mathcal{L} \end{cases}$$

jednom kada imamo reduciranu bazu.

Opišimo sad sami algoritam. Na ulazu ćemo imati vektore baze rešetke $\mathbf{b}_1, \dots, \mathbf{b}_n$, a na izlazu vektore reducirane baze $\mathbf{b}_1, \dots, \mathbf{b}_n$ te iste rešetke. LLL-algoritam prvi je puta objavljen 1982. kada su A.K.Lenstra, H.W.Lenstra Jr. i L.Lovasz taj algoritam koristili za faktorizaciju polinoma s racionalnim koeficijentima, a algoritam je izumio L.Lovasz 1981. Mi ćemo koristiti LLL-algoritam kod diofantskih aproksimacija (aproksimacija linearnih formi) i rješavanja nekih diofantskih jednadžbi i problema koji će voditi na te aproksimacije, a osim toga algoritam se još koristi u kriptografiji kod kriptanalize nekih kriptosustava s javnim ključem.

Iako to općenito nije slučaj s rešetkama, nama će za primjene biti zanimljive rešetke koje leže u \mathbb{Z}^n , pa bi željeli imati takvu verziju algoritma, gdje ćemo raditi samo s cjelobrojnom aritmetikom. Razlog tome je što ne znamo kolika nam preciznost treba ako radimo s realnim brojevima, a da rezultat bude točan. A ako pak radimo s aritmetikom racionalnih brojeva, možda ćemo dobivati prevelike brojnike i nazivnike. Zato ćemo koristiti de Wegerovu verziju LLL-algoritma, koja će koristiti samo cjelobrojnu aritmetiku. Tu verziju ćemo još zvati cjelobrojna verzija LLL-algoritma. Opišimo sada detaljnije tu verziju algoritma.

Prvo što trebamo napraviti je izračunati ortogonalne vektore (Gram-Schmidtovim postupkom) bez ikakvog dijeljenja koje bi moglo dovesti do necjelobrojnog rezultata. Ono što ovdje pretpostavljamo to je da su vektori $\mathbf{b}_1, \dots, \mathbf{b}_n$ cjelobrojni, odnosno da su iz \mathbb{Z}^n . Definirajmo

$$D_i = \det((\mathbf{b}_j, \mathbf{b}_l))_{1 \leq j \leq i, 1 \leq l \leq i} = \prod_{k=1}^i (\mathbf{b}_k^*, \mathbf{b}_k^*).$$

Brojeve D_i ćemo koristiti kod definiranja brojeva

$$\mathbf{c}_i = D_{i-1} \mathbf{b}_i^* \in \mathbb{Z}^n, \quad \lambda_{i,j} = D_j \mu_{i,j} \in \mathbb{Z},$$

gdje su brojevi $\mu_{i,j}$ i vektori \mathbf{b}_i^* definirani kao prije. Na samom početku nam treba procedura koja će inicijalizirati brojeve $\lambda_{i,j}$ i vektore \mathbf{c}_i , odnosno to je procedura koja će nam dati cjelobrojnu ortogonalnu bazu, bez korištenja aritmetike racionalnih brojeva. Na ulazu imamo vektore \mathbf{b}_i , a na izlazu brojeve $\lambda_{i,j}$ i D_i .

PROCEDURA INIT

```

 $D_0 = 1;$ 
for  $i = 1, \dots, n$  do begin
   $\mathbf{c}_i = \mathbf{b}_i;$ 
  for  $j = 1, \dots, i - 1$  do begin
     $\lambda_{i,j} = (\mathbf{b}_i, \mathbf{c}_j);$ 
     $\mathbf{c}_i = \frac{D_j \mathbf{c}_i - \lambda_{i,j} \mathbf{c}_j}{D_{j-1}};$ 
  endfor;
   $D_i = \frac{(\mathbf{c}_i, \mathbf{c}_i)}{D_{i-1}};$ 
endfor;
end.

```

Nakon što smo napravili inicijalizaciju, trebaju nam još dvije procedure.

U prvoj ćemo na ulazu imati dva cijela broja k i l , vektore \mathbf{b}_i , brojeve $\lambda_{i,j}$ te brojeve D_i . Na izlazu ćemo imati to isto, samo će sada vrijediti $2|\lambda_{k,l}| \leq D_l$, ukoliko to nije bilo zadovoljeno na početku. Uočimo da je zbog definicije brojeva $\lambda_{i,j}$ ta relacija ekvivalentna s $|\mu_{k,l}| \leq \frac{1}{2}$. Dok će druga procedura zamijeniti vektore \mathbf{b}_k i \mathbf{b}_{k-1} . Naravno, tada ćemo morati promijeniti i odgovarajuće brojeve $\lambda_{i,j}$ i D_i .

PROCEDURA LAMBDA ($k.l$)

```

if  $2|\lambda_{k,l}| > D_l$  then begin
   $r = \left[ \frac{\lambda_{k,l}}{D_l} \right];$ 
   $\mathbf{b}_k = \mathbf{b}_k - r\mathbf{b}_l;$ 
  for  $j = 1, \dots, l - 1$  do  $\lambda_{k,j} = \lambda_{k,j} - r\lambda_{l,j};$ 
   $\lambda_{k,l} = \lambda_{k,l} - rD_l;$ 
endif;
end.

```

PROCEDURA ZAMIJENI

```

swap  $\mathbf{b}_k$  and  $\mathbf{b}_{k-1}$ ;
for  $j = 1, \dots, k-2$  do swap  $\lambda_{k-1,j}$  and  $\lambda_{k,j}$ ;
for  $i = 1, \dots, n$  do begin
     $t = \lambda_{i,k-1}$ ;
     $\lambda_{i,k-1} = \frac{\lambda_{i,k-1}\lambda_{k,k-1} + \lambda_{i,k}D_{k-2}}{D_{k-1}}$ ;
     $\lambda_{i,k} = \frac{tD_k\lambda_{i,k}\lambda_{k,k-1}}{D_{k-1}}$ ;
endfor;
 $D_{k-1} = \frac{D_{k-2}D_k + \lambda_{k,k-1}^2}{D_{k-1}}$ ;
end.

```

I na kraju imamo glavni algoritam:

DE WEGEROV LLL-ALGORITAM

```

PROCEDURA INIT;
 $k = 2$ ;
repeat
    PROCEDURA LAMBDA ( $k, k-1$ );
    if  $4D_{k-2}D_k < (3D_{k-1}^2 - 4\lambda_{k,k-1}^2)$  then begin ;
        PROCEDURA ZAMIJENI;
        if  $k > 2$  then  $k = k-1$ ;
    else begin
        for  $l = k-2, \dots, 1$  do PROCEDURA LAMBDA ( $k, l$ );
         $k = k+1$ ;
    endif;
until  $k > n$ ;
end.

```

Očito je da će upravo opisani algoritam dati reduciranu bazu, ako algoritam staje. To nećemo ovdje dokazivati, ali spomenimo da se može pokazati ako znamo da je rešetka diskretna i iskoristimo ocjenu za prvi sukcesivni minimum rešetke.

Napomena 2.5 Kod definiranja LLL-reducirane baze mogli uzeti bilo koju drugu konstantu $\omega \in \langle \frac{1}{4}, 1 \rangle$, umjesto $\frac{3}{4}$. Ako uzmemo veću konstantu, dobit ćemo bolju reduciranu bazu, odnosno prvi vektor reducirane baze bit će bliži najmanjem vektoru rešetke. S druge strane, što veću konstantu uzmemo duže će nam trebati da algoritam stane, pa je $\frac{3}{4}$ standardna konstanta i čini se kao dobar kompromis.

Promotrimo sada detaljnije problem kod kojeg ćemo mi koristiti LLL-algoritam. Neka su dani brojevi $\alpha_0, \alpha_1, \dots, \alpha_n \in \mathbb{C}$ i dvije pozitivne realne konstante k_2 i k_3 . Mi ćemo pokušati smanjiti gornju ogradu za H u nejednakosti

$$\left| \alpha_0 + \sum_{i=1}^n x_i \alpha_i \right| \leq k_2 e^{-k_3 H}. \quad (2.10)$$

Neka su dane cjelobrojne varijable x_i ograničene tako da je $|x_i| \leq X_i$, gdje su X_i neke velike pozitivne konstante za $i = 1, \dots, n$. Pokazat ćemo da je moguće dobiti novu gornju ogradu za H oblika $O(\log X_0)$, gdje je $X_0 = \max\{X_i : i = 1, \dots, n\}$. Razmatrat ćemo tri slučaja i u svakom od njih opisati postupak redukcije ograde.

Slučaj 1:

$$\alpha_i \in \mathbb{R}, i = 0, 1, \dots, n.$$

Prvo izaberimo konstantu C veličine oko X_0^n . Nadalje, našoj linearnoj formi

$$\Lambda = \alpha_0 + \sum_{i=1}^n x_i \alpha_i$$

pridružimo rešetku \mathcal{L} generiranu stupcima matrice

$$A = \begin{pmatrix} 1 & & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & 1 & 0 \\ [C\alpha_1] & \cdot & [C\alpha_{n-1}] & [C\alpha_n] \end{pmatrix} \in M_n(\mathbb{Z}).$$

Konstantu C biramo veličine oko X_0^n jer tada možemo očekivati da je najmanji vektor reducirane baze veličine oko X_0 . Sada koristeći cjelobrojnu verziju LLL-algoritma možemo naći donju ogradu k_4 za

$$l(\mathcal{L}, \mathbf{y}) = \begin{cases} \min\{\|\mathbf{x} - \mathbf{y}\| : \mathbf{x} \in \mathcal{L}\}, & \mathbf{y} \notin \mathcal{L} \\ \min\{\|\mathbf{x}\| : \mathbf{x} \in \mathcal{L}, \mathbf{x} \neq (0, \dots, 0)\}, & \mathbf{y} \in \mathcal{L} \end{cases}$$

gdje je $\mathbf{y} = (0 \dots 0 - [C\alpha_0])^t \in \mathbb{Z}^n$. Ako smo imali sreće, možda smo našli konstantu k_4 tako da možemo primijeniti sljedeću lemu koja će nam dati novu gornju ogradu za naš H i to baš onakvog oblika kakav smo htjeli.

Lema 2.1 *Neka je*

$$S = \sum_{i=1}^{n-1} X_i^2, \quad T = 0.5 \cdot (1 + \sum_{i=1}^n X_i).$$

Ako je $k_4^2 \geq T^2 + S$, onda vrijedi

$$H \leq \frac{1}{k_3} (\log(Ck_2) - \log(\sqrt{k_4^2 - S - T}))$$

ili je $x_1 = \dots = x_{n-1} = 0$, $x_n = -\frac{[C\alpha_0]}{[C\alpha_n]}$.

Dokaz. Označimo

$$\Phi = [C\alpha_0] + \sum_{i=1}^n x_i [C\alpha_i].$$

Tada vrijedi

$$|\Phi - C(\alpha_0 + \sum_{i=1}^n x_i \alpha_i)| \leq \sum_{i=1}^n \frac{X_i}{2} + \frac{1}{2} = T.$$

Iz toga nadalje dobivamo

$$|\Phi| \leq T + Ck_2 e^{-k_3 H}.$$

Označimo sada sa $\mathbf{z} = A\mathbf{x}$, gdje je $\mathbf{x} = (x_1 \dots x_n)^t$. Tada je $\mathbf{z} - \mathbf{y} = (x_1 \dots x_{n-1} \Phi)^t$.

Odnosno jer je \mathbf{z} element rešetke \mathcal{L} dobivamo da je $\mathbf{z} = \mathbf{y}$ ako je \mathbf{y} element rešetke što nam odmah daje $x_1 = \dots = x_{n-1} = 0$, $x_n = -\frac{[C\alpha_0]}{[C\alpha_n]}$ ili vrijedi

$$k_4^2 \leq l(\mathcal{L}, \mathbf{y})^2 \leq \sum_{i=1}^{n-1} x_i^2 + \Phi^2 \leq S + (T + Ck_2 e^{-k_3 H})^2,$$

ako \mathbf{y} nije elemnt rešetke. Iz pretpostavke $k_4 \geq S$ dalje zaključujemo

$$e^{-k_3 H} \geq \frac{1}{Ck_2} (\sqrt{k_4^2 - S - T}),$$

odnosno logaritmirajući obje strane (ako je $k_4^2 \geq T^2 + S$)

$$H \leq \frac{1}{k_3} (\log(Ck_2) - \log(\sqrt{k_4^2 - S - T})).$$

■

Napomena 2.6 U slučaju da smo dobili konstantu k_4 tako da nisu zadovoljeni uvjeti leme 2.1 možemo pokušati uzeti veću konstantu C . No ako nam se neprestano događa da nije zadovoljena pretpostavka leme, obično se dogodila jedna od sljedećih situacija:

- gornja ograda za H je jako velika ili ne postoji,
- gornju ogradu za H smo već jako smanjili, tako da se ne može više smanjivati,
- vektor y je vektor rešetke \mathcal{L} različit od nulvektora,
- brojevi α_i su linearno zavisni nad \mathbb{Q} .

Slučaj 2:

$$\operatorname{Re}(\alpha_i) = 0, \quad i = 0, 1, \dots, n.$$

Ovaj slučaj se svodi na prethodni ako definiramo $\alpha'_i = \frac{\alpha_i}{\sqrt{-1}}$.

Slučaj 3: Općenit slučaj kad su

$$\alpha_i \in \mathbb{C}, \quad i = 0, 1, \dots, n.$$

U ovom slučaju našoj linearnoj formi

$$\Lambda = \alpha_0 + \sum_{i=1}^n x_i \alpha_i$$

pridružimo rešetku \mathcal{L} generiranu stupcima matrice

$$A = \begin{pmatrix} 1 & & & 0 & & 0 & & 0 \\ \cdot & \cdot & & \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & & \cdot & & \cdot \\ 0 & & \cdot & \cdot & 1 & & 0 & 0 \\ [C \cdot \operatorname{Re}(\alpha_1)] & \cdot & \cdot & [C \cdot \operatorname{Re}(\alpha_{n-2})] & [C \cdot \operatorname{Re}(\alpha_{n-1})] & [C \cdot \operatorname{Re}(\alpha_n)] & & \\ [C \cdot \operatorname{Im}(\alpha_1)] & \cdot & \cdot & [C \cdot \operatorname{Im}(\alpha_{n-2})] & [C \cdot \operatorname{Im}(\alpha_{n-1})] & [C \cdot \operatorname{Im}(\alpha_n)] & & \end{pmatrix} \in M_n(\mathbb{Z}).$$

Na ovom mjestu, ukoliko je to potrebno permutirajmo brojeve α_i tako da determinanta pridružene matrice bude različita od nule. Dok konstantu C , biramo

veliĉine oko $\sqrt{X_0^n}$. Sada koristeĉi cjelobrojnu verziju LLL-algoritma nađimo donju ogradu k_4 za

$$l(\mathcal{L}, \mathbf{y}) = \begin{cases} \min\{\|\mathbf{x} - \mathbf{y}\| : \mathbf{x} \in \mathcal{L}, \mathbf{y} \notin \mathcal{L}\} \\ \min\{\|\mathbf{x}\| : \mathbf{x} \in \mathcal{L}, \mathbf{x} \neq (0, \dots, 0)\}, \mathbf{y} \in \mathcal{L} \end{cases},$$

gdje je $\mathbf{y} = (0 \dots 0 \quad - [C \cdot \text{Re}(\alpha_0)] \quad - [C \cdot \text{Im}(\alpha_0)])^t \in \mathbb{Z}^n$. I sada imamo analogon lemi 2.1.

Lema 2.2 *Neka je*

$$S = \sum_{i=1}^{n-2} X_i^2, \quad T = \frac{1 + \sum_{i=1}^n X_i}{\sqrt{2}}.$$

Ako je $k_4^2 \geq T^2 + S$, onda vrijedi

$$H \leq \frac{1}{k_3} (\log(Ck_2) - \log(\sqrt{k_4^2 - S} - T))$$

ili je $x_1 = \dots = x_{n-2} = 0$, a x_{n-1} i x_n zadovoljavaju sustav

$$x_{n-1}[C \cdot \text{Re}(\alpha_{n-1})] + x_n[C \cdot \text{Re}(\alpha_n)] = [C \cdot \text{Re}(\alpha_0)],$$

$$x_{n-1}[C \cdot \text{Im}(\alpha_{n-1})] + x_n[C \cdot \text{Im}(\alpha_n)] = [C \cdot \text{Im}(\alpha_0)].$$

Pokađimo sada na jednom primjeru kako se koristi upravo opisana metoda.

Primjer 2.1 *Nađimo sva rješenja nejednađbe*

$$|x_1 \log 2 + x_2 \log 3 + x_3 \log 5 - \log 7| \leq e^{-X},$$

gdje su $x_1, x_2, x_3 \in \mathbb{Z}$, a $X = \max\{|x_i| : i = 1, 2, 3\} \leq X_0 = 10^{30}$.

Oznaĉimo linearnu formu

$$\Lambda = x_1 \log 2 + x_2 \log 3 + x_3 \log 5 - \log 7.$$

Tada je naša nejednakost oblika

$$|\Lambda| \leq k_2 e^{-k_3 X},$$

48POGLAVLJE 2. METODE I ALGORITMI IZ DIOFANTSKIH APROKSIMACIJA

gdje je $k_2 = 1$ i $k_3 = 1$. Sada našoj linearnoj formi pridružimo rešetku \mathcal{L} generiranu stupcima matrice

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ [C \log 2] & [C \log 3] & [C \log 5] \end{pmatrix}.$$

Sada izaberemo konstantu C veličine oko X_0^3 , ali kako je uvijek dobro uzeti malo veću konstantu, uzet ćemo $C = 10^{100}$. Tada za prvi vektor reducirane baze (dobivene LLL-algoritmom) dobivamo

$$b_1 = \begin{pmatrix} -1515246263903680163735468625616799 \\ -50289739459725489063203391695738 \\ 1155937255867757166304329056366403 \end{pmatrix},$$

a za konstantu k_4 nakon kraćeg računa dobivamo $k_4^2 = 1.446071 \cdot 10^{66}$. Nadalje, lako se provjeri da vrijedi $k_4^2 \geq T^2 + S$, jer je $S = 2 \cdot 10^{60}$, a $T = 0.5 \cdot (1 + 3 \cdot 10^{30})$ pa možemo primjeniti lemu 2.1 koja nam daje $X \leq 154$. Primjetimo koliko je ta ograda manja u odnosu na prvotnu.

Sada nastavljamo isti postupak za $X \leq X_0 = 154$. Nakon još dva koraka redukcije, moguće je dobiti $X \leq 10$. Tada nije teško provjeriti uvrštavanje koji x_i -ovi zadovoljavaju početnu nejednakost. Dobivamo da su to

$$(x_1, x_2, x_3) = (-5, 2, 2), (-2, 0, 2), (-2, 3, 0), (-1, -2, 3), (-1, 1, 1),$$

$$(0, 0, 1), (1, 0, 1), (1, 1, 0), (1, 7, -4), (2, -1, 1), (2, 2, -1).$$

Primjer 2.2 Opišimo sada još jednu primjenu LLL-algoritma. Pokušajmo naći polinom stupnja 3 s "malim" cjelobrojnim koeficijentima čiji će korijen biti jako blizu broja π . Recimo da želimo naći takav polinom s koeficijentima reda 10^2 . Jedan od načina kako riješiti taj problem je naći jako malu vrijednost linearne forme

$$\Lambda = x_1\pi^3 + x_2\pi^2 + x_3\pi + x_4,$$

gdje želimo da su x_i reda 10^2 . U tu svrhu definirajmo rešetku generiranu stupcima matrice

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 3101 & 987 & 314 & 100 \end{pmatrix},$$

gdje je zadnji redak dan sa $[100\pi^{4-i}]$. Jasno je da će mali vektor rešetke generiran stupcima od A odgovarati polinomu trećeg stupnja s "malim" koeficijentima i korijenom blizu broja π . Ako nađemo LLL-reduciranu bazu rešetke, njen prvi element će biti jako dobra aproksimacija najmanjeg elementa u rešetki, a iz toga je onda moguće naći traženi polinom.

Koristeći GP-Pari, nalazimo da je reducirana baza naše rešetke dana stupcima matrice AU , gdje je

$$U = \begin{pmatrix} -1 & -1 & -2 & -3 \\ 0 & 1 & 2 & -6 \\ 0 & 1 & -5 & 2 \\ 31 & 18 & 58 & 146 \end{pmatrix}.$$

Sada iz prvog stupca matrice U očitavamo polinom trećeg stupnja $x^3 - 31$ koji ima korijen α za koji vrijedi $|\alpha - \pi| \leq 0.00022$.

Pretpostavimo sada da želimo naći polinom trećeg stupnja s korijenom još bližim broju π . Sada zadnji redak matrice A zamijenimo s $[1000\pi^{4-i}]$. Dobivamo

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 31006 & 9870 & 3142 & 1000 \end{pmatrix}.$$

U ovom slučaju je reducirana baza dana sa AU , gdje je

$$U = \begin{pmatrix} 2 & -1 & 3 & 5 \\ -1 & 0 & -1 & 9 \\ -1 & 0 & 6 & 1 \\ -49 & 31 & -102 & -247 \end{pmatrix},$$

pa dobivamo polinom trećeg stupnja $2x^3 - x^2 - x - 49$ koji ponovo ima korijen β jako blizu broju π . Naime, vrijedi $|\beta - \pi| \leq 0.000027$.

Ako pak želimo naći polinom trećeg stupnja s jednim korijenom blizu broja e i jednim korijenom blizu π , onda definiramo matricu

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2009 & 739 & 272 & 100 \\ 3101 & 987 & 314 & 100 \end{pmatrix},$$

čija su zadnja dva retka dana sa $[100e^{4-i}]$ i $[100\pi^{4-i}]$. Tada je LLL-reducirana baza rešetke generirana stupcima matrice A dana sa AU , gdje je

$$U = \begin{pmatrix} -3 & 0 & -8 & 1 \\ 2 & 1 & -1 & -9 \\ 66 & -6 & 214 & 27 \\ -134 & 9 & -414 & -27 \end{pmatrix}.$$

Iz prvog stupca matrice U očitavamo polinom trećeg stupnja $3x^3 - 2x^2 - 66x + 134$ čija su dva korijena dana sa $x_1 \approx 2.72532$ i $x_2 \approx 3.14788$.

2.4 Baker-Davenportova redukcija

I prije nego prijedemo na glavni dio kolegija, primjenu linearnih formi u logaritima na diofantske jednadžbe i probleme, spomenimo još jednu redukciju koju ćemo isto koristiti kod smanjivanja gornje ograde za veličinu rješenja. Verzija Baker-Davenportove redukcije koju ćemo mi koristiti opisana je u sljedećoj lemi.

Lema 2.3 *Neka su κ, μ realni brojevi i N prirodan broj. Neka je nadalje $\frac{p}{q}$ 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 $\|\cdot\|$ označena udaljenost do najbližeg cijelog broja. Ako je $\varepsilon > 0$, onda nejednadžba*

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

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

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

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

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

odnosno

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

iz čega zaključujemo

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

■

Napomena 2.7 *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 $\|\mu q\|$ općenito ne znamo ništa. Zato je razumno uzeti barem $q > 2N$, a uvjet $q > 6N$ se pokazao eksperimentalno kao dobar izbor.*

Napomena 2.8 *Ako nam uvjet $\varepsilon > 0$ nije zadovoljen, onda možemo pokušati uzeti sljedeću konvergentu i vidjeti hoće li nam za nju uvjet biti zadovoljen.*

Poglavlje 3

Linearne forme u logaritmima

3.1 Uvod

Kažimo na početku nešto o povijesti razvoja teorije linearnih formi u logaritmima algebarskih brojeva. 1900. godine, David Hilbert je na međunarodnoj matematičkoj konferenciji u Parizu predstavio 23 problema za koje je vjerovao da će biti riješena u narednom stoljeću i da će za njihovo rješavanje biti potreban razvoj nekih novih metoda. Jedan od tih problema je sedmi Hilbertov problem gdje je trebalo dokazati transcendentnost broja α^β za $\alpha \neq 0, 1$ algebarski broj i β algebarski iracionalan broj.

Taj problem su 1934. neovisno riješili Gelfond i Scheider. Njihov teorem kaže da ako su α_1 i α_2 nenul 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 algebarske brojeve β_1, β_2 . No osim što su pokazali da je taj izraz različit od nule, Gelfond je 1935. dobio i donju ogradu za apsolutnu vrijednost linearne forme $\Lambda = \beta_1 \log \alpha_1 + \beta_2 \log \alpha_2$. Preciznije, dokazao je da vrijedi

$$\log |\Lambda| \gg -h(\Lambda)^\kappa,$$

gdje je $h(\Lambda)$ logaritamska visina linearne forme, a $\kappa > 5$. Sam Gelfond je četrdesetih godina prošlog stoljeća primjetio da bi poopćenje ovakvih rezultata na linearnu formu u više logaritama omogućilo rješavanje mnogih problema iz teorije brojeva.

To je 1966. napravio engleski matematičar Alan Baker. Dokazao je da ukoliko su $\alpha_1, \dots, \alpha_n$ nenul algebarski brojevi takvi da su $\log \alpha_1, \dots, \log \alpha_n$ linearno nezavisni nad \mathbb{Q} , onda su $1, \log \alpha_1, \dots, \log \alpha_n$ linearno nezavisni nad poljem algebarskih brojeva. Također, Baker je dokazao i kvantitativan rezultat. To je bilo dovoljno da se riješi Gaussov problem broja klasa, da se dobije eksplicitna konstanta u Liouvilleovom teoremu bolja od one koju je dobio sam Liouville, a dan je i algoritam za efektivno rješavanje Thueovih jednadžbi.

Prijedimo sada na definiranje osnovnih pojmov.

Definicija 3.1 *Linearna forma u logaritmima algebarskih brojeva je izraz oblika*

$$\beta_1 \log \alpha_1 + \dots + \beta_n \log \alpha_n,$$

gdje su α_i i β_i kompleksni algebarski brojevi.

Ovdje ćemo razmatrati samo slučaj kad su β_i cijeli brojevi, i označavat ćemo ih s b_1, \dots, b_n . To je jedini slučaj koji ima primjenu na diofantske jednadžbe. Također, u ovom poglavlju \log će uvijek označavati glavnu vrijednost kompleksnog logaritma.

Neka je K polje algebarskih brojeva stupnja D . Neka su nadalje $\alpha_1, \dots, \alpha_n$ elementi od K različiti od 0 i b_1, \dots, b_n cijeli brojevi. Definirajmo

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

i

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

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

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

gdje je $b_{n+1} = 0$, ako je K realno polje, a $|b_{n+1}| \leq nB$ inače. Iako su linearne forme Λ^* i Λ usko povezane (posebice jedna je jednaka nuli ako i samo ako je i druga), bit će korisno koristiti obje ove forme. Također, prisjetimo se definicije apsolutne logaritamske visine algebarskog broja.

Definicija 3.2 Neka je K polje algebarskih brojeva stupnja D i neka je $\alpha \in K^*$ algebarski broj stupnja $d|D$. Neka je nadalje $\sum_{0 \leq k \leq d} a_k X^k$ njegov minimalan primitivni (koeficijenti su mu relativno prosti) polinom u $\mathbb{Z}[X]$ tako da je $a_d \neq 0$. Definiramo apsolutnu logaritamsku visinu $h(\alpha)$ algebarskog broja α sa

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

gdje su α_i konjugati od α .

Neka su nadalje A_1, \dots, A_n realni brojevi tako da vrijedi

$$A_j \geq h'(\alpha_j) = \max\{Dh(\alpha_j), \log |\alpha_j|, 0.16\}$$

za $j = 1, \dots, n$. h' zovemo modificiranom visinom. Koristeći gornje oznake vrijede sljedeći teoremi Matveeva.

Teorem 3.1 (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

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

Teorem 3.2 (Matveev, 2001) Pretpostavimo da vrijedi $\Lambda = b_1 \log \alpha_1 + \dots + b_n \log \alpha_n \neq 0$, gdje su α_i algebarski brojevi, a b_i cjelobrojni koeficijenti. Tada vrijedi

$$\log |\Lambda| > -2 \cdot 30^{n+4} (n+1)^6 D^2 A_1 \cdots A_n (1 + \log D)(1 + \log B),$$

gdje je $B = \max\{|b_i| : 1 \leq i \leq n\}$.

Iako će za nas biti dovoljno dobiti donje ograde za linearnu formu u logaritima koje slijede iz ovih teorema, u nekim primjerima koristit ćemo i sljedeći Baker-Wüstholzov teorem.

Teorem 3.3 (Baker-Wüstholz) Pretpostavimo da vrijedi $\Lambda = b_1 \log \alpha_1 + \dots + b_n \log \alpha_n \neq 0$, gdje su α_i algebarski brojevi, a b_i cjelobrojni koeficijenti. Onda je

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

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

U nekim primjenama na diofantske jednadžbe potrebna je bolja ocjena u ovisnosti o B , poput sljedećeg rezultata. Koristeći gornje oznake, pretpostavljajući da su algebarski brojevi $\alpha_1, \dots, \alpha_n$ multiplikativno nezavisni nad \mathbb{Q} i da je $b_n \neq 0$, postoji pozitivna eksplicitna konstanta $C(n)$ tako da vrijedi

$$\log |\Lambda| > -C(n) \cdot D^2(\log D) A_1 \cdots A_n \log B',$$

gdje je

$$B' = \max_{1 \leq j < n} \left\{ \frac{|b_n|}{A_j} + \frac{|b_j|}{A_n} \right\}.$$

Uspoređujući to s teoremom 3.2, dobivamo poboljšanje posebno kad α_n ima veliku visinu i kad je $|b_n|$ malo.

Također je važno usporediti dobivenu ogradu za $|\Lambda|$ s elementarnom donjom ogralom koja daje

$$\log |\Lambda| > -D(1 + |b_1|h(\alpha_1) + \dots + |b_n|h(\alpha_n)).$$

U ovoj ocjeni ovisnost o D i svakom $h(\alpha_j)$ je bolje nego u spomenutim teoremima, ali je u teoremima ovisnost o B logaritamska, za razliku od linearne u elementarnoj ocjeni. To je najveća razlika, i zato ova elementarna ocjena nema primjenu u diofantskim jednadžbama. Ustvari, za primjenu ne trebamo donju ogradu koja je logaritamska u ovisnosti o B . Sljedeći rezultat bi bio dovoljan: za svaki $\varepsilon > 0$ postoji pozitivna konstanta C_ε takva da vrijedi

$$\log |\Lambda| > -\varepsilon B,$$

za $B > C_\varepsilon$, gdje C_ε ne ovisi o B , nego o $\alpha_1, \dots, \alpha_n$ i njihovim logaritmima. U praksi, najbolji rezultat za dva i tri logaritma ovisi o $\log^2 B$.

3.2 Primjena linearnih formi na diofantske jednadžbe i probleme

U primjeni na diofantske probleme strategija je sljedeća. U prvom koraku, različitim i često "ad hoc" algebarskim manipulacijama pridružimo "velika" rješenja jednadžbe "jako malim" vrijednostima određene linearne forme u logaritmima, što znači da imamo gornju ogradu za vrijednosti linearne forme koja odgovara

rješenju jednadžbe. Uspoređujući tu gornju ogradu s donjom ogradom dobivenom iz Bakerove teorije (odnosno teorema 3.1, 3.2 i 3.3), dobivamo gornju ogradu M za apsolutne vrijednosti nepoznanica u našoj jednadžbi.

Sada imamo dva slučaja u kojima ćemo riješiti jednadžbu. Prvo, ako M nije prevelik, tada jednostavnim uvrštavanjem nalazimo kompletanu listu rješenja koja su manja od M .

Drugi važan slučaj je kad pridružena linearna forma ima svojstvo da su samo koeficijenti b_i nepoznati. Tada iz ograde $|b_i| \leq M$ dobivene na opisani način možemo dobiti puno manju ogradu. Zaista, efektivne tehnike iz diofantskih aproksimacija, kao što su verižni razlomci (Baker-Davenportova redukcija) i LLL-algoritam, mogu se koristiti za dobiti dobru donju ogradu za $|\sum_{i=1}^n b_i x_i|$ koja se može koristiti umjesto ocjene Bakerovog tipa. Uspoređujući tu donju ogradu s gornjom ogradom, dobivamo vrijednost M' tako da je $|b_i| \leq M'$. Taj postupak možemo ponavljati dok više ne dobivamo novo poboljšanje.

3.2.1 Donja ograda za $|2^m - 3^n|$

Jedna od jednostavnih primjena linearnih formi u logaritmima je dokaz da $|2^m - 3^n|$ teži u beskonačnost kad $m + n$ teži u beskonačno, kao i za dobivanje eksplisitne donje ograde za ovaj izraz.

Neka je $n \geq 2$ cijeli broj i definirajmo m i m' tako da vrijedi

$$2^{m'} < 3^n < 2^{m'+1}$$

i

$$|3^n - 2^m| = \min\{3^n - 2^{m'}, 2^{m'+1} - 3^n\}.$$

Tada vrijedi

$$|2^m - 3^n| < 2^m, (m-1) \log 2 < n \log 3 < (m+1) \log 2$$

i problem nalaženja donje ograde za $|2^m - 3^n|$ se očito svodi na taj poseban slučaj.

Sada definirajmo linearnu formu

$$\Lambda^* = 3^n 2^{-m} - 1.$$

Koristeći teorem 3.1 dobivamo

$$\log |\Lambda^*| > -c_0(1 + \log m),$$

gdje se kratkim računom dobiva $c_0 = 5.862 \cdot 10^8$. To nam daje sljedeću ocjenu.

Teorem 3.4 *Neka su m i n prirodni brojevi. Tada vrijedi*

$$|2^m - 3^n| > 2^m(em)^{-5.862 \cdot 10^8}.$$

Općenitije, ako sa S označimo konačan skup prostih brojeva i ako je $(x_j)_{j \geq 1}$ rastući niz svih cijelih brojeva čiji prosti djelitelji pripadaju skupu S , tada vrijedi

$$|x_{j+1} - x_j| \geq x_j(\log x_j)^{-c},$$

gdje se konstanta c može eksplicitno izračunati u ovisnosti o prostim brojevima iz S .

Korolar 3.1 *Sva cjelobrojna rješenja diofantske jednadžbe*

$$2^m - 3^n = 5,$$

dana su sa $(m, n) = (3, 1), (5, 3)$.

Dokaz. Koristeći teorem 3.4 dobivamo

$$5 > 2^m(em)^{-5.862 \cdot 10^8},$$

što povlači

$$\log 5 > m \log 2 - 5.862 \cdot 10^8(1 + \log m),$$

odnosno $m < 2.1 \cdot 10^{10}$ i $n < \frac{m \log 2}{\log 3} < 1.4 \cdot 10^{10}$. Nadalje $|2^m - 3^n| = 5$ povlači

$$\left| m - n \frac{\log 3}{\log 2} \right| < \frac{5}{\log 2} 3^{-n}.$$

Iz toga zaključujemo, kako je $\frac{5}{\log 2} 3^{-n} < \frac{1}{2n}$, za $n \geq 4$, da ako je (m, n) rješenje naše jednadžbe tako da je $n \geq 4$, tada je $\frac{m}{n}$ konvergenta razvoja u verižni razlomak broja $\xi = \frac{\log 3}{\log 2}$.

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME 59

Ali primjetimo da za $n < N = 1.4 \cdot 10^{10}$, najmanja vrijednost od $|m - n\xi|$ se dobiva za najveću konvergentu verižnog razlomka od ξ tako da je nazivnik manji od N . Tada dobivamo

$$\frac{5}{\log 2} 3^{-n} > \left| m - n \frac{\log 3}{\log 2} \right| > 10^{-11},$$

za $0 < n < 1.4 \cdot 10^{10}$. Sada vidimo da ako je (m, n) rješenje našeg problema, tada je $n \leq 24$. I sada provjerom za $1 \leq n \leq 24$, dokazujemo našu tvrdnju. ■

Vrijedi i općenitiji rezultat, koji je dokazao Bennett 2001.

Teorem 3.5 (Bennett) *Za dane cijele brojeve a , b i c , različite od nule, jednadžba $a^m - b^n = c$ ima najviše dva cjelobrojna rješenja.*

Opišimo na kraju ovog odjeljka još jedan malo općenitiji problem, kako riješiti nejednadžbu

$$0 < u - v \leq X,$$

gdje su u i v cijeli brojevi s prostim faktorima iz danog skupa $\{p_1, \dots, p_r\}$, a X dani prirodan broj. Primjetimo da smo malo prije do zadnjeg koraka i provjere da li (m, n) zadovoljava jednadžbu, ustvari rješavali $0 \leq 2^m - 3^n \leq 5$.

Zapišimo prvo

$$u = \prod_{i=1}^r p_i^{u_i}, \quad v = \prod_{i=1}^r p_i^{v_i}.$$

Za početak ćemo se skoncentrirati na primitivna rješenja, odnosno ona za koja vrijedi $(u, v) = 1$. Neprimitivna rješenja se kasnije lako dobivaju iz primitivnih. Tada za svaki $i = 1, \dots, r$ vrijedi $u_i v_i = 0$. Definirajmo sada linearnu formu

$$0 < \Lambda^* = \prod_{i=1}^r p_i^{u_i - v_i} - 1 \leq X v^{-1},$$

što povlači

$$0 < \Lambda := \sum_{i=1}^r (u_i - v_i) \log p_i \leq X v^{-1}.$$

Definirajmo sada $m_i = u_i - v_i$ i $M = \max\{|m_i| : i = 1, \dots, r\}$. Također bez smanjenja općenitosti možemo pretpostaviti $p_1 < p_2 < \dots < p_r$. Sad je

ili $M = \max |v_i|$, što povlači $v \geq p_1^M$ ili je pak $M = \max |u_i|$ kada možemo zaključiti $v \geq u - X \geq \frac{u}{2} \geq \frac{p_1^M}{2}$, ako je $u \geq 2X$. Znači, ako je $u \geq 2X$, imamo

$$0 < \Lambda := \sum_{i=1}^r (u_i - v_i) \log p_i \leq Xv^{-1} \leq 2Xe^{-M \log p_1}. \quad (3.1)$$

Uspoređujući tu ogradu s donjom ogradom iz teorema 3.1 zaključujemo

$$M \log p_1 \leq \log(2X) + 1.4 \cdot 30^{r+3} r^{4.5} \left(\prod_{i=1}^r \log p_i \right) (1 + \log M).$$

Za dobiti gornju ogradu za M možemo koristiti sljedeću lemu.

Lema 3.1 (*Pethö, de Weger*) *Neka je B nenegativan cijeli broj takav da vrijedi*

$$\alpha \log B + \beta \geq \gamma B.$$

Ako je $\alpha \geq e\gamma$, onda vrijedi

$$B \leq \frac{2}{\gamma} \left(\alpha \log \frac{\alpha}{\gamma} + \beta \right).$$

I sada imamo sljedeći algoritam za naći sva rješenja nejednadžbe $0 < u - v \leq X$, gdje u i v imaju sve proste faktore u skupu $\{p_1, p_2, \dots, p_r\}$:

- Prvo nađimo gornju ogradu za M koristeći zadnju lemu. Ukoliko definiramo

$$\lambda_1 = \log p_1, \lambda_2 = 1.4 \cdot 30^{r+3} r^{4.5} \left(\prod_{i=1}^r \log p_i \right), \lambda_3 = \lambda_2 + \log(2X),$$

imamo

$$M \leq \frac{2}{\lambda_1} \left(\lambda_2 \log \frac{\lambda_2}{\lambda_1} + \lambda_3 \right).$$

- Sada primjetimo da nam nejednakost (3.1) ima isti oblik kao i (2.10) za $k_2 = 2X$ i $k_3 = \log p_1$. Pa možemo primjeniti LLL-algoritam i smanjiti gornju ogradu za M .
- Kada nam je gornja ograda za M dovoljno mala, provjerimo za sve

$$u = \prod_{i=1}^r p_i^{u_i}, v = \prod_{i=1}^r p_i^{v_i},$$

gdje su $|u_i|, |v_i| \leq M$ i $u_i v_i = 0$, da li je zadovoljena nejednadžba $0 < u - v \leq X$.

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME61

- Provjerimo ima li primitivnih rješenja takvih da vrijedi $u < 2X$.
- I na kraju dodamo neprimitivna rješenja ako ih ima. Njih dobivamo tako da primitivno rješenje množimo prostim brojevima p_1, \dots, p_r i provjeravamo je li zadovoljena početna nejednadžba $0 < u - v \leq X$.

Primjer 3.1 Pokažimo sad na jednom primjeru kako funkcionira opisani postupak. Riješimo nejednadžbu

$$0 < u - v \leq 5,$$

gdje su jedini prosti djelitelji od u i v dani sa $p_1 = 2$ i $p_2 = 3$.

Tada prema upravo opisanom, našem problemu pridružimo linearnu formu u logaritmima

$$\Lambda = m_1 \log 2 + m_2 \log 3,$$

gdje je $m_1 = u_1 - v_1$, $m_2 = u_2 - v_2$, a

$$u = 2^{u_1} 3^{u_2}, \quad v = 2^{v_1} 3^{v_2}.$$

Tada, ukoliko je $u \geq 10$ imamo nejednakost oblika (2.10) za $k_2 = 10$ i $k_3 = \log 2$. Nadalje prema prethodno opisanom, lako je dobiti gornju ogradu za $M = \max\{|m_1|, |m_2|\}$. Vrijedi

$$M < 3.65 \cdot 10^{10}.$$

Tada našoj linearnoj formi pridružimo rešetku generiranu stupcima matrice

$$A = \begin{pmatrix} 1 & 0 \\ [C \log 2] & [C \log 3] \end{pmatrix},$$

gdje ćemo uzeti $C = 10^{30}$. Tada nam cjelobrojna verzija LLL-algoritma daje da nam je reducirana baza dana stupcima matrice

$$B = \begin{pmatrix} 766512153894657 & -683381996816440 \\ -476302006617303 & -1008615542976179 \end{pmatrix}.$$

Tada nije teško izračunati konstante koje smo prije označili s k_1 i k_4 . Dobivamo $k_1 = 1$ i $k_4^2 = 8.15 \cdot 10^{29}$. Kako je nadalje $S = 1.34 \cdot 10^{21}$ i

$T = 3.66 \cdot 10^{10}$, primjenom leme 2.2, dobivamo novu gornju ogradu za M , $M \leq 53$. Sada primjenjujući isti postupak još dva puta možemo još smanjiti ogradu za M . Dobivamo $M \leq 9$.

Tada nije teško provjeriti koja su primitivna rješenja naše nejednakosti. Dobivamo da su to

$$(u, v) = (1, 0), (2, 0), (2, 1), (4, 0), (4, 1), (4, 3), (8, 3), (32, 27), (3, 0), (3, 1), (3, 2), \\ (9, 4), (9, 8), (0, -1), (0, -2), (-1, -2), (0, -4), (-3, -4), (-3, -8), \\ (-27, -32), (0, -3), (-1, -3), (-2, -3), (-4, -9), (-8, -9), (1, -1), (1, -2), \\ (1, -3), (1, -4), (2, -1), (2, -3), (3, -1), (3, -2), (4, -1).$$

I tu treba još dodati neprimitivna rješenja

$$(u, v) = (4, 2), (6, 3), (8, 4), (8, 6), (12, 9), (16, 12), (6, 2), (6, 4), \\ (9, 6), (12, 8), (18, 16), (27, 24), (36, 32), (-2, -4), (-3, -6), (-4, -8), \\ (-6, -8), (-9, -12), (-12, -16), (-2, -6), (-4, -6), (-6, -9), \\ (-8, -12), (-16, -18), (-24, -27), (-32, -36), (2, -2).$$

Opišimo sada još nekoliko problema kod kojih možemo koristiti linearne forme u logaritmima algebarskih brojeva.

3.2.2 Donje ograde za trag od α^n

U ovom odjeljku ćemo opisati kako teorem 3.2 možemo koristiti u dobivanju donje ograde za trag algebarskog broja.

Neka je α algebarski broj stupnja $d > 1$, koji nije korijen iz jedinice. Neka su $\alpha = \alpha_1, \alpha_2, \dots, \alpha_d$ njegovi konjugati takvi da zadovoljavaju

$$|\alpha_1| \geq |\alpha_2| > |\alpha_3| \geq \dots \geq |\alpha_d|.$$

Tada se trag od α^n može računati po formuli

$$\text{Tr}(\alpha^n) = \alpha_1^n + \alpha_2^n + \dots + \alpha_d^n.$$

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME 63

Promotrimo prvo trivijalan slučaj $|\alpha_1| > |\alpha_2|$. Tada vrijedi

$$|\alpha_1|^n - (d-1)|\alpha_2|^n \leq |\text{Tr}(\alpha^n)| \leq |\alpha_1|^n + (d-1)|\alpha_2|^n,$$

odnosno $|\text{Tr}(\alpha^n)| \approx |\alpha|^n$.

Pretpostavimo sada da vrijedi $|\alpha_1| = |\alpha_2|$ i $\alpha_1 \neq -\alpha_2$. Tada ako stavimo $\alpha = \varrho e^{i\varphi}$, $\varrho > 0$, imamo

$$\alpha_1^n + \alpha_2^n = \varrho^n (e^{in\varphi} + e^{-in\varphi}) = 2\varrho^n \cos(n\varphi).$$

Ova formula nam pokazuje da je traženje donje ograde za $|\alpha_1^n + \alpha_2^n|$, ekvivalentno traženju donje ograde za linearnu formu

$$\Lambda_1 = ni\varphi - ki\pi,$$

gdje je $i = \sqrt{-1}$, a k cijeli broj. Linearna forma Λ_1 je linearna forma u logaritmicima algebarskih brojeva s cjelobrojnim koeficijentima. Zaista, vrijedi

$$i\varphi = \log\left(\frac{\alpha}{|\alpha|}\right), \quad i\pi = \log(-1),$$

gdje su $\frac{\alpha}{|\alpha|}$ i -1 algebarski brojevi. Tada, koristeći teorem 3.2, znamo da postoji pozitivna konstanta $c_1(\alpha)$ koja ovisi samo o α , takva da vrijedi

$$\log |\Lambda_1| \geq -c_1(\alpha) \log n.$$

A iz toga odmah slijedi

$$|\text{Tr}(\alpha^n)| \geq 0.5|\alpha|^n n^{-c_1(\alpha)},$$

za $n > c_2(\alpha)$, gdje su $c_1(\alpha)$ i $c_2(\alpha)$ pozitivne konstante koje ovise samo o α . Može se dokazati i općenitiji rezultat.

Teorem 3.6 *Neka su a i α algebarski brojevi različiti od 0 i neka $\alpha \notin \mathbb{Q}$. Tada vrijedi*

$$|a\alpha^n + \bar{a}\bar{\alpha}^n| > |\alpha|^n n^{-c_3},$$

za $n > c_4$, gdje su c_3 i c_4 pozitivne konstante koje ovise samo o a i α .

3.2.3 Čiste potencije u binarno rekurzivnim nizovima

Prisjetimo se prvo definicije Fibonaccijevih i Lucasovih brojeva. Ta dva niza (F_n) i (L_n) su definirana sa

$$F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n,$$

$$L_0 = 2, L_1 = 1, L_{n+2} = L_{n+1} + L_n.$$

Tada vrijedi

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}, L_n = \alpha^n + \beta^n,$$

za $n \geq 0$, gdje je $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$.

Pretpostavimo sada da je $F_n = y^p$ čista potencija. Tada vrijedi

$$\alpha^n - \sqrt{5}y^p = O(\alpha^{-n}),$$

odnosno

$$\Lambda_2 = n \log \alpha - p \log y - \log \sqrt{5} = O(\alpha^{-2n}) = O(y^{-2p}). \quad (3.2)$$

Tada postoje cijeli brojevi k i r takvi da vrijedi $n = kp + r$ i $|r| \leq \frac{p}{2}$, pa dobivamo

$$\Lambda_2 = p \log \left(\frac{\alpha^k}{y} \right) + r \log \alpha - \log \sqrt{5},$$

što je linearna forma u tri logaritma. Ako na nju primjenimo teorem 3.1, dobivamo

$$\log |\Lambda_2| \geq -c_5 \log y \log p.$$

Ako to usporedimo s (3.2), vidimo da je eksponent p ograničen. Preciznije, Matveevi teoremi nam daju $p < 3 \cdot 10^{13}$. No u specijalnom slučaju linearne forme u tri logaritma imamo i poboljšanje teorema Matveeva koje su napravili Bugeaud, Mignotte i Siksek, pa dobivamo $p < 2 \cdot 10^8$, što onda više nije problem provjeriti kompjuterom, jer se pokazuje da gornja ograda za p povlači gornju ogradu za n . Slična razmatranja, ako pretpostavimo da je $L_n = y^p$, vode na linearnu formu u dva logaritma, te koristeći rezultat Laurenta, Mignottea i Nesterenka dobivamo još bolju ocjenu, $p < 300$. Tada možemo zaključiti da su jedine čiste potencije u danim nizovima dane sa

$$F_0 = 0, F_1 = F_2 = 1, F_6 = 8 = 2^3, F_{12} = 144 = 12^2, L_1 = 1, L_3 = 4 = 2^2.$$

Općenito vrijedi sljedeći teorem.

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME65

Teorem 3.7 *Neka je (u_n) niz cijelih brojeva oblika*

$$u_n = a\alpha^n + O(|\alpha|^{\theta n}), \quad 0 < \theta < 1,$$

gdje su a i α nenul algebarski brojevi, takvi da vrijedi $|\alpha| > 1$, neka je θ fiksiran i neka je $u_n - a\alpha^n \neq 0$ za sve n . Tada jednadžba

$$u_n = y^p, \quad u_n \notin \{0, \pm 1\},$$

povlači $p < c_6$, gdje c_6 ovisi samo o a , α i θ te o implicitnoj konstanti u O .

Promotrimo sada na jednom konkretnom primjeru kako koristiti linearne forme u logaritmima algebarskih brojeva kod Fibonaccijevog niza.

Primjer 3.2 *Pokažimo da je jedini Fibonaccijev broj koji u dekadskom zapisu ima sve znamenke jednake, $F_{10} = 55$.*

Rješenje. Nalaženje Fibonaccijevih brojeva koji u dekadskom zapisu imaju sve znamenke iste ekvivalentan je rješavanju diofantske jednadžbe

$$F_n = \overline{dd \dots d} = d \cdot 10^{m-1} + d \cdot 10^{m-2} + \dots + d = d \frac{10^m - 1}{10 - 1}, \quad (3.3)$$

pa riješimo tu jednadžbu.

Pretpostavimo da je $n > 1000$. Tada, ako označimo $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$, onda (3.3) možemo zapisati

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

što dalje možemo zapisati kao

$$\left| \alpha^n - \frac{d\sqrt{5}}{9} 10^m \right| = \left| \beta^n - \frac{d\sqrt{5}}{9} \right| \leq \alpha^{-1000} + \sqrt{5} < 2.5. \quad (3.4)$$

Nadalje se indukcijom po n lako može pokazati da vrijedi

$$\alpha^{n-2} < F_n < \alpha^{n-1}$$

za sve $n \geq 3$. 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 $c = \frac{\log 10}{\log \alpha} \approx 4.78497$. Kako je $c > 4$, vidimo da za sve $n > 1000$ vrijedi $n \geq m$. Definirajmo sad linearnu formu

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

za koju iz (3.4) zaključujemo da vrijedi

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

odnosno

$$\log |\Lambda^*| < -(n - 2) \log \alpha.$$

S druge strane donju ogradu za $|\Lambda^*|$ možemo dobiti iz teorema 3.1. Označimo

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

$$b_1 = 1, b_2 = -n, b = m.$$

Nadalje primjetimo da je $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\sqrt{5})$ pa je u notaciji teorema $D = 2$. I jasno je $B = n$. Nadalje, α_2 i α_3 su očito algebarski cijeli brojevi, dok je minimalni polinom od α_1 nad \mathbb{Z} djelitelj od

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

Tada vrijedi

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

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME67

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

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

Tada za A_i -ove možemo izabrati

$$A_1 = 6.02, A_2 = 1.5, A_3 = 4.62,$$

pa nam teorem 3.1 povlači

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

Ako to usporedimo s gornjom ogradom i malo sredimo, dobivamo

$$n - 2 < 1.2 \cdot 10^{14}(1 + \log n),$$

odnosno $n < 4.5 \cdot 10^{15}$.

Sada nam ostaje još reducirati ovu ogradu. To ćemo napraviti Baker-Davenportovom redukcijom, pa ćemo prije morati dobiti nejednakost kao u lemi 2.3. Primjetimo prvo da nam je u jednakosti

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

desna strana negativna, pa ako označimo

$$z = \log \alpha_1 - n \log \alpha_2 + m \log \alpha_3,$$

dobivamo

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

Nadalje, 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

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

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

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

što je baš nejednakost kakvu želimo. A iz $n < 4.5 \cdot 10^{15}$, možemo zaključiti $m < 4.5 \cdot 10^{14}$. Sada primjenjujući Baker-Davenportovu redukciju, nakon prvog koraka dobivamo novu ogradu m , $m \leq 21$, a iz toga odmah $n \leq 102$. Znači ostaje samo provjeriti što se događa za $n \leq 1000$. No onda se, recimo u Mathematici, vidi da je jedino rješenje stvarno dano sa $F_{10} = 55$.

3.2.4 Najveći prosti faktori članova rekurzivnih nizova

Kao i u prethodnom odjeljku promatrajmo niz nenul cijelih brojeva u_n takav da vrijedi

$$u_n = a\alpha^n + O(|\alpha|^{\theta n}), \quad 0 < \theta < 1, \quad u_n \neq a\alpha^n,$$

gdje su a i α nenul algebarski brojevi, $|\alpha| > 1$ i θ fiksiran. Neka je nadalje $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \dots$ rastući niz prostih brojeva. Pretpostavimo da je najveći prosti faktor od u jednak p_k , odnosno

$$u_n = p_1^{r_1} \cdots p_k^{r_k},$$

gdje je $r_k > 0$. Definirajmo linearnu formu u logaritmima algebarskih brojeva

$$\Lambda_3 = n \log \alpha + \log a - r_1 \log p_1 - \dots - r_k \log p_k.$$

Tada definicija broja u_n povlači

$$\log |\Lambda_3| \leq -c_7 n,$$

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME 69

gdje je c_7 pozitivna konstanta koja ovisi samo o a , α , θ i implicitnoj konstanti u O . S druge strane teorem 3.2 povlači

$$\log |\Lambda_3| \geq -c_8 (\log p_k)^k \log n,$$

gdje je c_8 pozitivna konstanta koja ovisi samo o a i α . Uspoređujući te dvije ocjene i koristeći $p_k \sim k \log k$ dobivamo sljedeći teorem.

Teorem 3.8 *Neka je (u_n) niz nenul cijelih brojeva oblika*

$$u_n = a\alpha^n + O(|\alpha|^{\theta n}), \quad 0 < \theta < 1,$$

gdje su a i α nenul algebarski brojevi, takvi da je $|\alpha| > 1$, θ fiksiran i neka je $u_n \neq a\alpha^n$ za sve n . Neka je nadalje (p_k) rastući niz svih prostih brojeva i pretpostavimo da je najveći prosti faktor od u_n jednak p_k . Tada vrijedi

$$k > \frac{c_9 \log n}{\log \log \log n},$$

gdje je c_9 pozitivna konstanta koja ovisi samo o a , α , θ i implicitnoj konstanti u O .

3.2.5 Najveći prosti faktori u vrijednostima cjelobrojnih polinoma

Neka je $f(X) \in \mathbb{Z}[X]$ ireducibilan polinom stupnja $n \geq 2$ i neka je x prirodan broj. Koristeći Bakerovu teoriju, moguće je naći donju ogradu za najveći prosti faktor od $f(x)$. Uzmimo, na primjer, $f(X) = X(X - 1)$. Tada u istoj notaciji kao u prethodnom odjeljku zapišimo

$$x(x - 1) = p_1^{r_1} \cdots p_k^{r_k},$$

gdje je $r_k > 0$. Tada za odgovarajuće $\varepsilon_i \in \{\pm 1\}$, dobivamo

$$|p_1^{\varepsilon_1 r_1} \cdots p_k^{\varepsilon_k r_k} - 1| \leq \frac{1}{x - 1}.$$

Kako je $p_j \sim j \log j$, teorem 3.1 nam povlači da postoji pozitivna konstanta c_{10} , takva da vrijedi

$$\log x \leq c_{10}^{k \log \log k} \log \log x.$$

A to nadalje povalči

$$p_k \sim k \log k \gg \log \log x \frac{\log \log \log x}{\log \log \log \log x}.$$

Sličan rezultat se može dobiti za proizvoljan ireducibilan polinom u $\mathbb{Z}[X]$ stupnja $n \geq 2$.

3.2.6 Diofantska jednadžba $ax^n - by^n = c$

Promotrimo sada eksponencijalnu diofantsku jednadžbu

$$ax^n - by^n = c,$$

gdje su a i b dani prirodni brojevi, a c nenul cijeli broj, dok su x , y i n nepoznanice. Ako je za neki eksponent n postoji rješenje ove jednadžbe za $|y| > 1$, tada vrijedi

$$\Lambda_4 = \log \left| \frac{a}{b} \right| - n \log \left| \frac{x}{y} \right| = O(|y|^{-n}).$$

S druge strane nam teorem 3.1 povlači

$$\log |\Lambda_4| \geq -c_{11} \log |y| \cdot \log n.$$

Uspoređujući te dvije ograde, dobivamo gornju ogradu za n , $n < c_{12}$, gdje je c_{12} pozitivna konstanta koja ovisi samo o a , b i c . U sljedeća dva teorema dani su i eksplicitni rezultati.

Teorem 3.9 *Pretpostavimo da eksponencijalna diofantska nejednadžba*

$$|ax^n - by^n| \leq c,$$

gdje su a, b i c prirodni brojevi i $a \neq b$, ima rješenje u prirodnim brojevima x i y takvim da je $\max\{x, y\} > 1$. Tada vrijedi

$$n \max \left\{ 3 \log \left(\frac{1.5c}{b} \right), 7400 \frac{\log A}{\log \left(1 + \frac{\log A}{\log a - \log b} \right)} \right\},$$

gdje je $A = \max\{a, b, 3\}$.

Teorem 3.10 (Bennett) *Ako je $n \geq 3$, onda jednadžba*

$$|ax^n - by^n| = 1, \quad a, b \in \mathbb{N},$$

ima najviše jedno rješenje u prirodnim brojevima x i y .

Napomena 3.1 *Iz posljednjeg teorema slijedi da odmah znamo sva rješenja parametarske familije jednadžbi*

$$(b+1)x^n - by^n = \pm 1.$$

Takve jednadžbe se inače zovu Thueove jednadžbe i jako brzo ćemo detaljno opisati postupak njihovog rješavanja.

3.2.7 Catalanova jednadžba

Catalan je 1844 postavio sljedeći problem. Da li postoje uzastopni prirodni brojevi, osim 8 i 9, takvi da su oba čiste potencije? To odgovara rješavanje eksponentijalne diofantske jednadžbe

$$x^m - y^n = 1.$$

Iako je taj problem u potpunosti negativno riješio Mihailescu 2002, ovdje ćemo vidjeti kako se na ovu jednadžbu može primjeniti Bakerova teorema linearnih formi u logaritima algebarskih brojeva. Naime, dat ćemo skicu dokaza Tijdemanovog teorema iz 1976.

Teorem 3.11 (Tijdeman) *Neka su $x, y, m, n \geq 2$ prirodni brojevi takvi da vrijedi*

$$x^m - y^n = 1.$$

Tada postoji efektinva apsolutna konstanta takva da vrijedi $\max\{x, y, m, n\} < C$.

Skica dokaza. Prvo se može pokazati da možemo pretpostaviti da su m i n neparni. Tada promatramo jednadžbu

$$x^m - y^n = \varepsilon,$$

gdje su x, y, m, n prirodni brojevi takvi da vrijedi $n > m > 2$, a $\varepsilon = \pm 1$. Kako je

$$\frac{c^n - 1}{c - 1} = n + (c - 1) \sum_{1 \leq k \leq n-1} \binom{n}{k+1} (c - 1)^{k-1},$$

možemo zaključiti

$$\left(\frac{c^n - 1}{c - 1}, c - 1 \right) n.$$

Tada imamo relacije

$$x - \varepsilon = \frac{u^n}{m^*} \quad y + \varepsilon = \frac{v^m}{n^*},$$

gdje su u i v cijeli brojevi takvi da vrijedi $|u|, |v| > 1$ i gdje su m^* i n^* djeljitelji od m i n . Iz pretpostavka $n > m$ slijedi $x > y$. Definirajmo sad dvije linearne forme u logaritmima

$$\begin{aligned} \Lambda_5 &= n \log(yu^{-m}) + m \log m^*, \\ \Lambda_6 &= mn \log\left(\frac{u}{v}\right) - m \log m^* + n \log n^*. \end{aligned}$$

Kako je

$$\left| \frac{y^n}{u^{mn}(m^*)^{-m}} - 1 \right| = \left| \frac{x^m - \varepsilon}{(x - \varepsilon)^m} - 1 \right| \ll \frac{m}{x},$$

možemo zaključiti $|\Lambda_5| \ll \frac{m}{x}$, i nadalje primjenjujući teorem 3.1 i gornju ogradu $y \leq 2u^m$,

$$\log x \ll m(\log m)(\log n)(\log u),$$

odnosno

$$n \ll m(\log m)(\log n). \quad (3.5)$$

Nadalje iz

$$\left| \frac{u^{mn}}{(m^*)^m} \cdot \frac{(n^*)^n}{v^{mn}} - 1 \right| = \left| \frac{(x - \varepsilon)^m}{(y + \varepsilon)^n} - 1 \right| \ll \frac{n}{y},$$

zaključujemo $|\Lambda_6| \ll \frac{n}{y}$. Tada iz $u \leq 3v$ i teorema 3.1 dobivamo

$$\log y \ll (\log mn)(\log m)(\log n)(\log v),$$

odnosno

$$m \ll (\log m)(\log n)^2. \quad (3.6)$$

Uspoređujući sad (3.5) i (3.6) vidimo da je n odozgo ograničen apsolutnom konstantom. Tada iz (3.6) slijedi da je i m ograničen. A činjenica da su x i y ograničeni slijedi iz nekih rezultata o supereliptičkim jednadžbama. ■

3.2.8 Sustavi simultanih pellovskih jednadžbi

U ovom odjeljku ćemo vidjeti kako Bakerove teoriju linearnih formi u logaritmima možemo koristiti u rješavanju sustava simultanih pellovskih jednadžbi. Jedan od problema koji vodi na rješavanje takvog sustava je problem proširenja Diofantovih m -torki. Diofantova m -torka je skup m različitih prirodnih brojeva, takvih da je umnožak bilo koja dva njegova člana uvećan za 1 kvadrat cijelog broja. Starogrčki matematičar Diofant od Aleksandrije je bio prvi koji se bavio problemom pronalazjenja takvih skupova. No prvu cjelobrojnu Diofantovu četvorku, skup $\{1, 3, 8, 120\}$, pronašao je Fermat. Slutnja je kako ne postoji Diofantova petorka i kako se svaka Diofantova trojka možem proširiti do četvorke (s najvećim elementom) na jedinstven način. To je pokazano za više primjera trojki, a mi ćemo ovdje pokazati da ako je $\{1, 3, 8, d\}$ Diofantova četvorka, onda je $d = 120$. To su inače dokazali Baker i Davenport 1969, kada je prvi puta uspješno primjenjena Bakerova teorija linearnih formi u logaritmima na traženje presjeka dva binarno rekurzivna niza. Spomenimo još da je Dujella dokazao kako ne postoji Diofantova šestorka i da ima samo konačno mnogo petorki.

Primjetimo da ukoliko želimo proširiti Diofantovu trojku $\{1, 3, 8\}$ do četvorke $\{1, 3, 8, d\}$, onda postoje prirodni brojevi x , y i z takvi da vrijedi

$$d + 1 = x^2, \quad 3d + 1 = y^2, \quad 8d + 1 = z^2.$$

Ako iz ovoga eliminiramo d , dobivamo sljedeći sustav simultanih pellovskih jednadžbi

$$y^2 - 3x^2 = -2, \quad (3.7)$$

$$z^2 - 8x^2 = -7. \quad (3.8)$$

Kako se rješavaju pellovske jednadžbe detaljno smo opisali u prvom poglavlju, pa ako tražimo da je x pozitivan, dobivamo da su rješenja jednadžbi (3.7) i (3.8) redom dana sa

$$y + x\sqrt{3} = (1 \pm \sqrt{3})(2 + \sqrt{3})^m, \quad (3.9)$$

$$z + x\sqrt{8} = (1 \pm \sqrt{8})(3 + \sqrt{8})^n, \quad (3.10)$$

gdje su m i n cijeli brojevi za koje vrijedi $m, n \geq 0$. Nadalje, kako vrijedi $(1 - \sqrt{3})(2 + \sqrt{3}) = 1 + \sqrt{3}$, u (3.9) možemo uzeti samo $+$ predznak. Tada

zaključujemo sljedeće. $x = v_m$, za neki $m \geq 0$, gdje je niz (v_m) dan sa

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

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

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

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

Sada smo problem proširenja Diofantove trojke sveli na rješavanje diofantske jednačbe $v_m = w_n^{+,-}$. Lako se vidi $m \geq n$. Dokažimo sada sljedeću lemu.

Lema 3.2 *Ako je $v_m = q_n^{+,-}$, $m, n > 2$, onda vrijedi*

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

gdje je

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

Dokaz. Primjetimo da nam $v_m = w_n^{+,-}$, povlači

$$\frac{(1 + \sqrt{3})(2 + \sqrt{3})^m - (1 - \sqrt{3})(2 - \sqrt{3})^m}{2\sqrt{3}} = \frac{(2\sqrt{2} \pm 1)(3 + 2\sqrt{2})^n + (2\sqrt{2} \mp 1)(3 - 2\sqrt{2})^n}{4\sqrt{2}}. \quad (3.11)$$

Nadalje je očito da vrijedi

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

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

što povlači

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

Pa ako (3.11) podijelimo s $\frac{2\sqrt{2} \pm 1}{2\sqrt{2}}(3 + 2\sqrt{2})^n$, dobivamo

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

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME 75

$$\begin{aligned} &\leq \frac{2\sqrt{2}+1}{2\sqrt{2}-1}(3-2\sqrt{2})^{2n} + \frac{2\sqrt{2}(\sqrt{3}-1)}{\sqrt{3}(2\sqrt{2}-1)}(2-\sqrt{3})^m(3-2\sqrt{2})^n < \\ &< 7.29(2-\sqrt{3})^{2n}. \end{aligned}$$

Sada tvrdnja slijedi iz sljedeće leme, i činjenice da je $\Lambda \neq 0$, što nije teško vidjeti. ■

Lema 3.3 *Neka je $a \in \mathbb{R}$, $a < 1$. Ako je $|x| < a$, onda vrijedi*

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

Dokaz. Primijetimo činjenicu da je funkcija $\frac{\log(1+x)}{x}$, pozitivna i strogo padajuća funkcija za $|x| < 1$. Tada je ista funkcija za $|x| < a$ po vrijednosti manja od vrijednosti u točki $x = -a$. ■

Sada imamo sve spremno za primjenu teorema 3.3. U notaciji teorema imamo

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

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

Nadalje, minimalni polinomi nad \mathbb{Z} su zadani sa

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

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

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

pa vrijedi

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

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

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

Pa imamo

$$\log |\Lambda| \geq -3.96 \cdot 10^{15} \log m,$$

što nam zajedno s lemom 3.2 daje

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

Sada nam je ostalo još reducirati ovako veliku gornju ogradu za m . To možemo napraviti Baker-Davenportovom redukcijom. U notaciji leme 2.3 imamo

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

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

Lema nam daje novu ogradu za m , $m \leq 16$. Sada ako još jednom ponovimo istu redukciju, dobivamo $m \leq 4$, što je dovoljno mala ograda da provjerimo što se događa u našim nizovima kad su indeksi mali. Dobivamo samo dva rješenja,

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

što daje trivijalno proširenje naše Diofantove trojke s $d = 0$ i

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

što daje proširenje s elementom $d = 120$, što smo i željeli pokazati.

3.2.9 Thueove jednadžbe

U ovom odjeljku ćemo detaljno opisati postupak rješavanja Thueovih jednadžbi.

Definicija 3.3 *Neka je $F(X, Y) \in \mathbb{Z}[X, Y]$ homogena binarna forma s cjelobrojnim koeficijentima, ireducibilna nad \mathbb{Q} stupnja $n \geq 3$ te neka je $m \in \mathbb{Z}$. Diofantsku jednadžbu*

$$F(X, Y) = m$$

zovemo Thueova jednadžba.

Thue je 1909. dokazao da takva jednadžba ima samo konačno mnogo rješenja, iako njegov dokaz nije efektivan jer nije dao eksplicitnu gornju ogradu za rješenja.

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME 77

Primjetimo da forma $F(X, Y)$ ne može biti ireducibilna nad \mathbb{C} . Naime,

$$F(X, 1) = f_0(X - \theta_1) \cdots (X - \theta_n),$$

gdje su $\theta_1, \dots, \theta_n$ algebarski brojevi stupnja n . Pa je

$$F(X, Y) = Y^n F\left(\frac{X}{Y}, 1\right) = f_0(X - \theta_1 Y) \cdots (X - \theta_n Y).$$

No ireducibilnost nad \mathbb{Q} povlači da $F(X, 1)$ nema višestrukih korijena, odnosno da su θ_i -ovi međusobno različiti. Dokažimo prvo da Thueova jednadžba ima samo konačno mnogo rješenja u jednom specijalnom slučaju.

Teorem 3.12 *Ako jednadžba $F(X, 1) = 0$ nema realnih rješenja, tada jednadžba $F(X, Y) = m$ ima samo konačno mnogo rješenja. Preciznije, sva rješenja zadovoljavaju nejednakost*

$$|Y| \leq \frac{|m|}{\min\{|Im(\theta_i)| : i = 1, \dots, n\}},$$

gdje su θ_i korijeni polinoma $F(X, 1)$.

Dokaz. Neka je (X, Y) rješenje Thueove jednadžbe $F(X, Y) = m$ i definirajmo θ_k tako da vrijedi $|X - \theta_k Y| = \min\{|X - \theta_i Y| : i = 1, \dots, n\}$. Tada vrijedi

$$|Y| \cdot |Im(\theta_k)| = |Im(\theta_k Y)| \leq |X - \theta_k Y| \leq |m|.$$

■

Teorem 3.13 (Thue) *Thueova jednadžba ima samo konačno mnogo rješenja.*

Dokaz. Neka je $F(X, Y) = m$. Tada uz prethodne oznake vrijedi

$$f_0(X - \theta_1 Y) \cdots (X - \theta_n Y) = m. \quad (3.12)$$

Pretpostavimo da je $Y \neq 0$, jer za $Y = 0$ imamo najviše dva rješenja. Tada dijeleći (3.12) sa Y^n dobivamo

$$|f_0| \cdot \left| \theta_1 - \frac{X}{Y} \right| \cdots \left| \theta_n - \frac{X}{Y} \right| = \left| \frac{m}{Y^n} \right|. \quad (3.13)$$

Nadalje definirajmo θ_k tako da vrijedi

$$|X - \theta_k Y| = \min\{|X - \theta_i Y| : i = 1, \dots, n\},$$

odnosno

$$\left| \theta_k - \frac{X}{Y} \right| = \min \left\{ \left| \theta_i - \frac{X}{Y} \right| : i = 1, \dots, n \right\}.$$

Neka je $\gamma = \frac{1}{2} \min\{|\theta_i - \theta_j| : i \neq j\} > 0$. Tada za dovoljno velik Y obje strane u (3.13) mogu biti po volji male. Posebno onda to vrijedi i za najmanji faktor na lijevoj strani, $|\theta_k - \frac{X}{Y}|$. Znači, postoji $Y_0 > 0$ takav da za $Y \geq Y_0$ vrijedi $|\theta_k - \frac{X}{Y}| < \gamma$. Za $i \neq k$ dobivamo

$$\left| \theta_i - \frac{X}{Y} \right| \geq |\theta_i - \theta_k| - \left| \theta_k - \frac{X}{Y} \right| \geq 2\gamma - \gamma = \gamma.$$

Pa iz (3.13) možemo zaključiti

$$\left| \theta_k - \frac{X}{Y} \right| \leq \left| \frac{m}{f_0 Y^n \gamma^{n-1}} \right| = \frac{c}{|Y|^n}. \quad (3.14)$$

Kako je $n \geq 3$, Rothov teorem povlači da nejednadžba (3.14) ima samo konačno mnogo rješenja, što je i trebalo dokazati. ■

Prvi efektivan dokaz konačnosti broja rješenja Thueove jednadžbe dao je Baker 1968. Na početku ćemo opisati kako Thueovoj jednadžbi možemo pridružiti linearnu formu u logaritmima algebarskih brojeva. Kada dobijemo pripadnu linearnu formu Λ , prijeći ćemo na dobivanje nejednakosti oblika (2.10), koju forma mora zadovoljavati. Pokazat ćemo da rješenja Thueove jednadžbe, koja nam daju tu formu, uz neke uvjete, zadovoljavaju danu nejednakost. Tada ćemo na tu nejednakost primjenjivati postupak opisan u odjeljku 2.3.

Neka je

$$F(X, Y) = \sum_{i=0}^n f_i X^{n-i} Y^i \in \mathbb{Z}[X, Y], \quad n \geq 3$$

binarna forma stupnja n , ireducibilna nad \mathbb{Q} i neka je $m \in \mathbb{Z}$, $m \neq 0$. Promotrimo sada Thueovu jednadžbu

$$F(X, Y) = m$$

u nepoznicama X i Y . Označimo sa g polinom $g(X) = F(X, 1)$. Pokazali smo da ako jednadžba $g(X) = 0$ nema realnih rješenja, trivijalno je naći gornju

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME79

ogradu za $|Y|$. Pa pretpostavljamo da jednađba $g(X) = 0$ ima barem jedno realno rješenje. Numerirajmo korijene polinoma $g(X)$ na sljedeći način. Realne korijene označimo $\xi^{(1)}, \dots, \xi^{(s)}$, a nerealne (kompleksne) $\xi^{(s+1)} = \overline{\xi^{(s+t+1)}}, \dots, \xi^{(s+t)} = \overline{\xi^{(s+2t)}}$. Znači imamo s realnih i $2t$ kompleksnih rješenja jednađbe $g(X) = 0$. Naša je pretpostavka $s \geq 1, t \geq 0$ i jasno vrijedi $s + 2t = n$.

Sada promotrimo polje algebarskih brojeva $K = \mathbb{Q}(\xi)$, gdje je $g(\xi) = 0$. Ovdje nam nije važno koji korijen polinoma uzimamo jer su sva polja algebarskih brojeva $K = \mathbb{Q}(\xi)$ \mathbb{Q} -izomorfna. To trivijalno slijedi iz toga što je F ireducibilna nad \mathbb{Q} .

Također, definirajmo tri pozitivna realna broja $Y_1 < Y_2 < Y_3$ koji će nam podijeliti skup mogućih rješenja (X, Y) jednađbe $F(X, Y) = m$ u četiri klase i to na sljedeći način:

- jako mala rješenja, za koja će vrijediti $|Y| \leq Y_1$, i njih ćemo naći provjeravanjem svih mogućnosti
- mala rješenja, za koja će vrijediti $Y_1 < |Y| \leq Y_2$, koja ćemo naći iz razvoja u verižni razlomak jednog korijena $\xi^{(i)}$
- velika rješenja, za koja će vrijediti $Y_2 < |Y| \leq Y_3$, i dokazat ćemo da ne postoje reduciranjem gornje ograde Y_3
- jako velika rješenja, za koja će vrijediti $|Y| > Y_3$, i za njih ćemo dokazati da ne postoje koristeći Bakerovu teoriju linearnih formi u logaritmima

Za definiciju tih konstanti koristimo sljedeće leme.

Lema 3.4 *Neka je (X, Y) rješenje jednađbe $F(X, Y) = m$. Definirajmo $\beta^{(i)} = X - \xi^{(i)}Y$, te $Y_0 = 1$, ako je $t = 0$. A ako je $t \geq 1$ definiramo*

$$Y_0 = \left[\left(\frac{2^{n-1}}{\min\{|g'(\xi^{(s+i)})| : i = 1, \dots, t\} \cdot \min\{|Im(\xi^{(s+i)})| : i = 1, \dots, t\}} \right)^{\frac{1}{n}} \right].$$

Neka je nadalje

$$c_1 = \frac{2^{n-1}|m|}{\min\{|g'(\xi^{(i)})| : i = 1, \dots, s\}}, \quad c_2 = \frac{1}{2} \cdot \min\{|\xi^{(i)} - \xi^{(j)}| : 1 \leq i < j \leq n\},$$

$$Y_1 = \max \left\{ Y_0, \left[(4c_1)^{\frac{1}{n-2}} \right] \right\}.$$

Tada vrijedi

(i) Ako je $|Y| > Y_0$, onda postoji $i_0 \in \{1, \dots, s\}$ takav da vrijedi

$$|\beta^{(i_0)}| \leq c_1 |Y|^{-(n-1)},$$

$$|\beta^{(i)}| \geq c_2 |Y|, \quad i \neq i_0.$$

(ii) Ako je $|Y| > Y_1$, onda je $\frac{X}{Y}$ konvergenta razvoja u verižni razlomak broja $\xi^{(i_0)}$.

Dokaz. Definirajmo broj $i_0 \in \{1, \dots, n\}$ tako da vrijedi

$$|\beta^{(i_0)}| = \min\{|\beta^{(i)}| : i = 1, \dots, n\}.$$

Iz jednadžbe $F(X, Y) = m$, gdje je

$$F(X, Y) = \sum_{i=0}^n f_i X^{n-i} Y^i \in \mathbb{Z}[X, Y], \quad n \geq 3,$$

imamo

$$|f_0| \prod_{i=1}^n |\beta^{(i)}| = |m|.$$

Iz minimalnosti $|\beta^{(i_0)}|$ za sve $i = 1, \dots, n$ vrijedi

$$|Y| \cdot |\xi^{(i)} - \xi^{(i_0)}| = |\beta^{(i)} - \beta^{(i_0)}| \leq |\beta^{(i)}| + |\beta^{(i_0)}| \leq 2|\beta^{(i)}|.$$

Iz ovoga odmah slijedi drugi dio tvrdnje (i), odnosno vrijedi $|\beta^{(i)}| \geq c_2 |Y|$ za $i \neq i_0$.

Nadalje imamo

$$\begin{aligned} |\beta^{(i_0)}| &= \frac{|m|}{|f_0|} \cdot \prod_{i \neq i_0} |\beta^{(i)}|^{-1} \leq \frac{|m|}{|f_0|} \cdot \prod_{i \neq i_0} \left(\frac{1}{2} |Y| \cdot |\xi^{(i)} - \xi^{(i_0)}| \right)^{-1} = \\ &= \frac{2^{n-1} |m|}{|f_0 \cdot \prod_{i \neq i_0} (\xi^{(i)} - \xi^{(i_0)})| \cdot |Y|^{n-1}} = \frac{2^{n-1} |m|}{|g'(\xi^{(i_0)})| \cdot |Y|^{n-1}}. \end{aligned}$$

Sada ako bi bilo $i_0 > s$, odnosno $t \geq 1$, iz definicije broja Y_0 imamo

$$\left| \frac{X}{Y} - \xi^{(i_0)} \right| = \frac{|\beta^{(i_0)}|}{|Y|} \leq \frac{2^{n-1} |m|}{|g'(\xi^{(i_0)})| \cdot |Y|^n} \leq \left(\frac{Y_0}{|Y|} \right)^n \cdot \min\{|Im(\xi^{(i)})| : s+1 \leq i \leq s+t\}.$$

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME81

No to je nemoguće ako je $|Y| > Y_0$. Znači mora biti $i_0 \in \{1, \dots, s\}$ pa smo dokazali tvrdnju (i).

Neka je sada $|Y| > Y_1$. Tada vrijedi

$$\left| \frac{X}{Y} - \xi^{(i_0)} \right| = |\beta^{(i_0)}| \cdot |Y|^{-1} \leq c_1 \cdot |Y|^{-n} \leq \frac{1}{4} Y_1^{n-2} \cdot |Y|^{-n} < \frac{1}{4} |Y|^{-2} < \frac{1}{2|Y|^2},$$

iz čega slijedi slijedi da je $\frac{X}{Y}$ konvergenta razvoja u verižni razlomak broja $\xi^{(i_0)}$ što je baš tvrdnja (ii) koju je ostalo dokazati. ■

Opišimo sada postupak kojim našoj Thueovoj jednadžbi pridružujemo linearnu formu u logaritmima.

Neka je od sada nadalje $|Y| > Y_1$, a (X, Y) nam je i dalje rješenje jednadžbe $F(X, Y) = m$. Definirajmo $i_0 \in \{1, \dots, s\}$ kao u lemi 3.4. Sada ćemo izabrati proizvoljne indekse $j, k \in \{1, \dots, n\}$ i to tako da su i_0, j, k međusobno različiti, ali da vrijedi ili da je $j, k \in \{1, \dots, s\}$ ili je $j + t = k$ odnosno $\xi^{(k)} = \overline{\xi^{(j)}}$. Promatrajmo sustav jednadžbi $\beta^{(i)} = X - \xi^{(i)}Y$, $i = i_0, j, k$. Eliminirajući X i Y iz sustava dobivamo

$$\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\beta^{(k)}}{\beta^{(j)}} - 1 = -\frac{\xi^{(k)} - \xi^{(j)}}{\xi^{(k)} - \xi^{(i_0)}} \cdot \frac{\beta^{(i_0)}}{\beta^{(j)}}. \quad (3.15)$$

Razmatrat ćemo dva slučaja. Ako je $j, k \in \{1, \dots, s\}$, to ćemo zvati realan slučaj i onda ćemo našoj Thueovoj jednadžbi pridružiti linearnu formu u logaritmima

$$\Lambda = \log \left| \frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\beta^{(k)}}{\beta^{(j)}} \right|.$$

Ako je pak $j + t = k$, odnosno $\xi^{(k)} = \overline{\xi^{(j)}}$, to ćemo zvati kompleksan slučaj i onda jednadžbi $F(X, Y) = m$ pridružujemo linearnu formu

$$\Lambda = \frac{1}{i} \text{Log} \left(\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\beta^{(k)}}{\beta^{(j)}} \right),$$

gdje za $z \in \mathbb{C}$, Log označava glavnu vrijednost logaritma, odnosno vrijedi $-\pi < \text{Im}(\text{Log}(z)) \leq \pi$. Iz $\xi^{(k)} = \overline{\xi^{(j)}}$, vidimo da vrijedi $\Lambda \in \mathbb{R}$ i $|\Lambda| \leq \pi$. Sada ćemo dobiti jednu gornju ogradu za $|\Lambda|$.

Lema 3.5 Neka je $0 < a \leq \pi$. Ako je $|x| < a$, onda vrijedi

$$|x| < \frac{a}{2 \sin \frac{a}{2}} \cdot |e^{ix} - 1|.$$

Dokaz. Primijetimo da je $|e^{ix} - 1| = 2 \left| \sin \frac{x}{2} \right|$, te da je funkcija $\frac{2}{x} \sin \frac{x}{2}$ pozitivna i parna i da je padajuća za $0 \leq x < a$. Tada je jasno da postiže svoj minimum u točki $x = a$, iz čega slijedi tvrdnja leme. ■

Lema 3.6 *Neka je*

$$c_3 = \max \left\{ \left| \frac{\xi^{(i_1)} - \xi^{(i_2)}}{\xi^{(i_1)} - \xi^{(i_3)}} \right| : i_1 \neq i_2 \neq i_3 \neq i_1 \right\},$$

$$Y_2^* = \max \left\{ Y_1, \left[\left(\frac{2c_1 c_3}{c_2} \right)^{\frac{1}{n}} \right] \right\}.$$

Ako je $|Y| > Y_2^$, onda vrijedi*

$$|\Lambda| < \frac{1.39c_1 c_3}{c_2} |Y|^{-n}.$$

Dokaz. Dokažimo prvo realan slučaj. Iz $|Y| > Y_2^*$ i leme 3.4 slijedi da je desna strana u (3.15) po apsolutnoj vrijednosti manja od $\frac{1}{2}$. Iz toga nadalje dobivamo

$$\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\beta^{(k)}}{\beta^{(j)}} > 0.$$

Lijeva strana u (3.15) je jednaka $e^\Lambda - 1$, pa iz definicije konstante c_3 i leme 3.4 zaključujemo

$$|e^\Lambda - 1| < c_3.$$

U kompleksnom slučaju trebamo primijetiti da je lijeva strana u (3.15) jednaka $e^{i\Lambda} - 1$. Tada trivijalno kao i u realnom slučaju dobivamo

$$|e^{i\Lambda} - 1| < \frac{c_1 c_3}{c_2} |Y|^{-n} < \frac{1}{2}.$$

Kako je $|e^{i\Lambda} - 1| = 2 \left| \sin \frac{\Lambda}{2} \right|$, vrijedi $\left| \sin \frac{\Lambda}{2} \right| < \frac{1}{4}$. Tada iz leme 3.5, za $x = \Lambda$ i $a = \frac{1}{2}$, slijedi

$$|\Lambda| \leq 2 \cdot \frac{\frac{1}{4}}{\sin \frac{1}{4}} \left| \sin \frac{\Lambda}{2} \right| = \frac{\frac{1}{4}}{\sin \frac{1}{4}} |e^{i\Lambda} - 1| \leq 1.02 |e^{i\Lambda} - 1|.$$

A iz ovoga slijedi tvrdnja leme i u kompleksnom slučaju. ■

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME83

Sada ćemo promatrati prsten cijelih brojeva \mathcal{O}_K našeg polja algebarskih brojeva $K = \mathbb{Q}(\xi)$. U njemu postoji sustav fundamentalnih jedinica $\varepsilon_1, \dots, \varepsilon_r$, gdje iz Dirichletovog teorema o jedinicama slijedi $r = s + t - 1$. Jer je F ireducibilna nad \mathbb{Q} i iz pretpostavke $s > 0$ može se pokazati da su jedini korijeni iz jedinice koji pripadaju polju K samo 1 i -1. To slijedi iz toga što K ima barem jedno realno ulaganje, a jedini korijeni iz jedinice u skupu \mathbb{R} su baš 1 i -1. Za sada ćemo pretpostaviti da nam je na neki način poznat sustav fundamentalnih jedinica.

Nadalje, može se pokazati da postoji samo konačno mnogo neasociranih elemenata $\mu_1, \dots, \mu_\nu \in \mathcal{O}_K$ takvih da je za $f_0 \cdot N_{K/\mathbb{Q}}(\mu_i) = m$ za $i = 1, \dots, \nu$. To slijedi iz toga što postoji samo konačno mnogo cijelih ideala u \mathcal{O}_K sa fiksnom normom, i jer vrijedi da je za $\gamma \in \mathcal{O}_K$, (γ) cijeli ideal u \mathcal{O}_K sa normom $|N_{K/\mathbb{Q}}(\gamma)|$. Ako vrijedi $(\gamma_1) = (\gamma_2)$, onda su γ_1 i γ_2 asocirani. Spomenimo da se uvijek može određenim transformacijama dobiti da f_0 dijeli m . Također pretpostavljamo da nam je i taj skup $\mu_1, \dots, \mu_\nu \in \mathcal{O}_K$ na neki način poznat.

Sa M označimo skup svih brojeva oblika $\zeta \cdot \mu_i$ gdje je ζ korijen iz jedinice koji leži u K . U posebnom slučaju kada je $|f_0| = |m| = 1$, jasno je $M = \{-1, 1\}$. Sada za svako cjelobrojno rješenje (X, Y) jednadžbe $F(X, Y) = m$ postoji $\mu \in M$ i brojevi $a_1, \dots, a_r \in \mathbb{Z}$, takvi da je $\beta = \mu \cdot \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$, gdje smo označili $\beta = X - \xi Y$, $g(\varepsilon) = 0$ i $r = s + t - 1$.

Sada smo naš originalni problem rješavanja Thueove jednadžbe sveli na traženje svih cjelobrojnih r -torki (a_1, \dots, a_r) tako da je $\mu \cdot \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$ za neko $\mu \in M$ oblika $X - \xi Y$. Relacija (3.15) naš problem svodi na rješavanje konačno mnogo sustava oblika

$$\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\mu^{(k)}}{\mu^{(j)}} \cdot \prod_{i=1}^r \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}} \right)^{a_i} - 1 = - \frac{\xi^{(k)} - \xi^{(j)}}{\xi^{(k)} - \xi^{(i_0)}} \cdot \frac{\mu^{(i_0)}}{\mu^{(j)}} \cdot \prod_{i=1}^r \left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}} \right)^{a_i}.$$

Tada u realnom slučaju naša linearna forma u logaritmima izgleda

$$\Lambda = \log \left| \frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\mu^{(k)}}{\mu^{(j)}} \right| + \sum_{i=1}^r a_i \log \left| \frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}} \right|.$$

Dok nam je kompleksnom slučaju linearna forma dana sa

$$\Lambda = \arg \left(\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \cdot \frac{\mu^{(k)}}{\mu^{(j)}} \right) + \sum_{i=1}^r a_i \arg \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}} \right) + a_0 \cdot 2\pi,$$

za neki $a_0 \in \mathbb{Z}$, a prisjetimo se i da je $-\pi \leq \arg(z) \leq \pi$ za $z \in \mathbb{C}$.

Sada ćemo opisati kako doći do nama poznate nejednakosti oblika (2.10)

$$|\Lambda| \leq k_2 e^{-k^3 A},$$

gdje je $A = \max\{|a_i| : i_1, \dots, r\}$ te kako naći gornju ogradu za A . Kada nađemo i reduciramo ogradu za A , jednostavno ćemo za sve mogućnosti provjeriti da li je $\mu \cdot \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$ za neko $\mu \in M$ oblika $X - \xi Y$. Tada za te X i Y provjerimo da li zadovoljavaju jednadžbu $F(X, Y) = m$.

Prvo ćemo pronaći gornju ogradu za A u ovisnosti o $|Y|$. O tome nam govori sljedeća lema.

Lema 3.7 *Neka je $I = \{h_1, \dots, h_r\}$. Definirajmo $U_I = (\log |\varepsilon_l^{(h_i)}|)_{1 \leq i, l \leq r}$, gdje je i indeks retka, a l indeks stupca matrice U_I . Nadalje definirajmo*

$$U_I^{-1} = (u_{il}), \quad N(U_I^{-1}) = \max \left\{ \sum_{l=1}^r |u_{il}| : 1 \leq i \leq r \right\},$$

$$\mu_- = \min\{|\mu^{(i)}| : \mu \in M, 1 \leq i \leq n\}, \quad \mu_+ = \max\{|\mu^{(i)}| : \mu \in M, 1 \leq i \leq n\},$$

$$c_4 = \frac{\frac{1}{2} + \max\{|\xi^{(i_1)} - \xi^{(i_2)}| : 1 \leq i_1 < i_2 \leq n\}}{\mu_-},$$

$$c_5 = \min\{(n-1) \cdot \min\{N(U_I^{-1})\}, \max\{N(U_I^{-1})\}\}.$$

Tada za $|Y| > \max\left\{Y_1, 2|m|^{1/n}, \frac{\mu_+}{c_2}\right\}$, vrijedi

$$A < c_5 \cdot \log(c_4 |Y|).$$

Dokaz. Iz $\beta = \mu \cdot \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$ imamo

$$\begin{pmatrix} \log \left| \frac{\beta^{(h_1)}}{\mu^{(h_1)}} \right| \\ \cdot \\ \cdot \\ \log \left| \frac{\beta^{(h_r)}}{\mu^{(h_r)}} \right| \end{pmatrix} = U_I \cdot \begin{pmatrix} a_1 \\ \cdot \\ \cdot \\ a_r \end{pmatrix}.$$

S druge strane za svaki $h \in \{1, \dots, n\}$ koristeći lemu 3.4 možemo zaključiti

$$|\beta^{(h)}| = |X - \xi^{(h)} Y| \leq |X - \xi^{(i_0)} Y| + |Y| \cdot |\xi^{(h)} - \xi^{(i_0)}| \leq \frac{1}{2|Y|} + |Y| \cdot |\xi^{(h)} - \xi^{(i_0)}|$$

$$< \left(\frac{1}{2} + \max\{|\xi^{(i_1)} - \xi^{(i_2)}| : 1 \leq i_2 < i_1 \leq n\} \right) \cdot |Y|,$$

odnosno

$$\left| \frac{\beta^{(h)}}{\mu^{(h)}} \right| < c_4 |Y|, \quad h \in \{1, \dots, n\}.$$

Primjetimo nadalje da je $c_4 |Y| > 1$. Zaista iz

$$\prod_{i=1}^n |\mu^{(i)}| = \frac{|m|}{|f_0|} \leq |m|$$

slijedi

$$\mu_- \leq |m|^{\frac{1}{n}}.$$

Znači

$$c_4 |Y| \geq \left(\frac{1}{2} + \max\{|\xi^{(i_1)} - \xi^{(i_2)}|\} \right) \cdot |Y| \cdot \frac{1}{\mu_-} > \frac{|Y|}{2|m|^{\frac{1}{n}}} > 1.$$

Iz toga zaključujemo

$$\log \left| \frac{\beta^{(h)}}{\mu^{(h)}} \right| < \log(c_4 |Y|)$$

za $h = 1, \dots, n$. Pokažimo sada da je

$$\left| \log \left| \frac{\beta^{(i)}}{\mu^{(i)}} \right| \right| < (n-1) \log(c_4 |Y|), \quad i = 1, \dots, n.$$

To očito vrijedi ako je $\left| \frac{\beta^{(i)}}{\mu^{(i)}} \right| \geq 1$, pa pogledajmo što se dešava u slučaju kad je $\left| \frac{\beta^{(i)}}{\mu^{(i)}} \right| < 1$. Iz

$$\prod_{h=1}^n \left| \frac{\beta^{(h)}}{\mu^{(h)}} \right| = 1$$

imamo

$$\left| \log \left| \frac{\beta^{(i)}}{\mu^{(i)}} \right| \right| = -\log \left| \frac{\beta^{(i)}}{\mu^{(i)}} \right| = \sum_{h \neq i} \log \left| \frac{\beta^{(h)}}{\mu^{(h)}} \right| < (n-1) \log(c_4 |Y|).$$

Sada odmah dobivamo nejednakost

$$A < (n-1) \cdot \min\{N(U_I^{-1})\} \cdot \log(c_4 |Y|).$$

Još nam ostaje pokazati da vrijedi i nejednakost

$$A < \max\{N(U_I^{-1})\} \cdot \log(c_4|Y|).$$

To ćemo dokazati tako da prvo izaberemo skup I tako da vrijedi $i_0 \notin I$. Tada iz leme 3.4 odmah slijedi za svako $h \in I$ vrijedi

$$\left| \frac{\beta^{(h)}}{\mu^{(h)}} \right| > \frac{c_2|Y|}{\mu_+} > 1.$$

Tada dobivamo

$$\left| \log \left| \frac{\beta^{(h)}}{\mu^{(h)}} \right| \right| < \log(c_4|Y|),$$

iz čega odmah slijedi tvrdnja leme. ■

Leme 3.6 i 3.7 nam odmah daju sljedeću lemu.

Lema 3.8 *Definirajmo*

$$c_6 = \frac{1.391 \cdot c_3 \cdot c_4^n}{c_2},$$

$$Y_2' = \max \left\{ Y_2^*, 2|m|^{1/n}, \frac{\mu_+}{c_2} \right\}.$$

Tada, ako je $|Y| > Y_2'$, onda vrijedi

$$|\Lambda| < c_6 \cdot \exp \left(-\frac{n}{c_5} A \right).$$

Sada vidimo da smo uspjeli dobiti nejednakost oblika (2.10) na koju možemo primjeniti LLL-algoritam, a u nekim slučajevima i Baker-Davenportovu redukciju, za smanjivanje gornje ograde za A jednom kad ju nađemo.

Koristeći teorem 3.3 (ili neki drugi teorem takvog tipa), sada možemo naći pozitivne konstante c_7 i c_8 , takve da za $|Y| > Y_2'$ vrijedi

$$\log |\Lambda| > -c_7 \cdot (\log A + c_8).$$

Napomena 3.2 *Ukoliko se radi o kompleksom slučaju, teorem 3.3 primjenjujemo na linearnu formu $i\Lambda$. Tada $2a_0\pi i$ možemo zapisati kao $2a_0 \log(-1)$. Nadalje, lako se pokaže da vrijedi $|a_0| \leq rA$, pa ovdje moramo napraviti malu modifikaciju i c_8 zamijeniti s $c_8 + \log 2r$.*

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME87

Sada nam treba još jedna pomoćna lema koju nećemo dokazivati.

Lema 3.9 Neka je $a \geq 0$, $b > 0$ i neka je $x \in \mathbb{R}$, $x > 1$ takav da vrijedi

$$x \leq a + b \log x.$$

Tada vrijedi

(i) Ako je $b > e^2$, onda je $x < 2(a + b \log b)$.

(ii) Ako je $b \leq e^2$, onda je $x \leq 2(a + 2e^2)$.

I na kraju imamo:

Lema 3.10 Neka je

$$c_9 = \frac{2c_5}{n} \left(\log c_6 + c_7 \cdot c_8 + c_7 \log \frac{c_5 c_7}{n} \right).$$

Tada ako je $|Y| > Y'_2$, onda vrijedi $A < c_9$.

Dokaz. Kao što smo prije vidjeli, vrijedi $|e^\Lambda| < \frac{1}{2}$. Nadalje, jer je $\beta^{(i_0)} \neq 0$, zaključujemo da je $i \neq 0$. Tada lema 3.8 povlači

$$A < \frac{c_5}{n} (\log c_6 + c_7 \cdot c_8 + c_7 \log A)$$

pa tvrdnja slijezi iz leme 3.9. ■

Ilustrirajmo sada kako riješiti Thueovu jednadžbu na jednom primjeru.

Primjer 3.3 Riješimo jednadžbu

$$X^4 - 2Y^4 = \pm 1,$$

gdje su $X, Y \in \mathbb{Z}$.

Rješenje. Pošto je ovo očito Thueova jednadžba, primjenit ćemo upravo opisani postupak, te ćemo koristiti iste oznake za konstante. U našem slučaju je $F(X, Y) = X^4 - 2Y^4$, a $m = \pm 1$. Prisjetimo se da je $g(X) = F(X, 1) = X^4 - 2$,

i nađimo rješenja jednadžbe $g(X) = 0$. Korijene polinoma g numerirajmo na sljedeći način:

$$\xi^{(1)} = \sqrt[4]{2}, \xi^{(2)} = -\sqrt[4]{2}, \xi^{(3)} = \sqrt[4]{2} \cdot i, \xi^{(4)} = -\sqrt[4]{2} \cdot i.$$

Nadalje definirajmo polje algebarskih brojeva $K = \mathbb{Q}(\xi)$, gdje je $g(\xi) = 0$. To ponovo možemo napraviti, ne gubeći ništa na općenitosti, jer su sva ta polja \mathbb{Q} -izomorfna. Sada pomoću programskog paketa GP-Pari dobivamo sustav fundamentalnih jedinica u \mathcal{O}_K . Dobivamo da nam je taj sustav jednak $\varepsilon_1 = \xi + 1$, $\varepsilon_2 = \xi - 1$. Tada dolazimo do problema, koji su od brojeva oblika $\pm \varepsilon_1^{a_1} \varepsilon_2^{a_2}$, za $a_1, a_2 \in \mathbb{Z}$, oblika $X - \xi Y$.

Prisjetimo se također da u ovom (kompleksnom) slučaju našoj Thueovoj jednadžbi pridružujemo linearnu formu

$$\Lambda = \arg \left(\frac{\xi^{(i_0)} - \xi^{(j)}}{\xi^{(i_0)} - \xi^{(k)}} \right) + a_1 \arg \left(\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}} \right) + a_2 \arg \left(\frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}} \right) + a_0 \cdot 2\pi.$$

Neka je $A = \max\{|a_1|, |a_2|\}$, te izračunajmo sada sve konstante potrebne da nađemo gornju ogradu za A . Kroz računanje konstanti imamo $s = 2$, $t = 1$, $n = 4$, $m = \pm 1$ i $g'(X) = 4X^3$. Redom dobivamo

$$\begin{aligned} Y_0 &= 1, c_1 = \sqrt[4]{2}, c_2 = \frac{\sqrt{2} \cdot \sqrt[4]{2}}{2}, \\ Y_1 &= 3, c_3 = \sqrt{2}, Y_2^* = 3, c_4 = \frac{1}{2} + 2 \cdot \sqrt[4]{2}, \\ c_5 &\approx 1.9514351, c_6 \approx 190.83, Y_2' = 3. \end{aligned}$$

Sada znamo da ako je $(X, Y) \in \mathbb{Z}^2$ rješenje jednadžbe $X^4 - 2Y^4 = \pm 1$ i $|Y| > 3$, onda postoje konstante c_7 i c_8 tako da vrijedi

$$\log |\Lambda| > -c_7(\log A'' + c_8),$$

gdje je $A'' = \max\{|2a_0|, |a_1|, |a_2|\}$. Te konstante nalazimo primjenom Baker-Wüstholzovog teorema (teorem 3.3), no prije toga promotrimo malo bolje našu linearnu formu .

Ono što znamo o formi je da je $i_0 \in \{1, 2\}$, $j = 3$ i $k = 4$. Tada je naša linearna forma oblika

$$\Lambda = \pm \frac{\pi}{2} + a_1 \cdot \alpha + a_2 \cdot (-\alpha) + a_0 \cdot 2\pi,$$

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME89

gdje je $\alpha = \arg\left(\frac{1-\sqrt[4]{2}\cdot i}{1+\sqrt[4]{2}\cdot i}\right)$. Također primjetimo da je naša linearna forma u logaritima algebarskih brojeva u ovom slučaju $i\Lambda$, no što se tiče primjene teorema 3.3 to nije nikakav problem jer vrijedi $|\Lambda| = |i\Lambda|$.

Označimo

$$\alpha_1 = \pm i, \alpha_2 = \frac{1 - \sqrt[4]{2} \cdot i}{1 + \sqrt[4]{2} \cdot i}, \alpha_3 = \frac{1 + \sqrt[4]{2} \cdot i}{1 - \sqrt[4]{2} \cdot i}, \alpha_4 = -1.$$

Tada su njihovi minimalni polinomi dani sa

$$P_{\alpha_1}(x) = x^2 + 1, P_{\alpha_4}(x) = x + 1,$$

$$P_{\alpha_2}(x) = P_{\alpha_3}(x) = x^4 + 12x^3 + 6x^2 + 12x + 1.$$

Pa za brojeve $h''(\alpha_i)$ dobivamo sljedeće

$$h''(\alpha_1) = \frac{\pi}{4}, h''(\alpha_4) = \pi,$$

$$h''(\alpha_2) \leq \log\left(\frac{\max\{|\varepsilon_1^{(j)}| : j = 1, 2, 3, 4\}}{\min\{|\varepsilon_1^{(j)}| : j = 1, 2, 3, 4\}}\right) < 2.44848,$$

$$h''(\alpha_3) \leq \log\left(\frac{\max\{|\varepsilon_2^{(j)}| : j = 1, 2, 3, 4\}}{\min\{|\varepsilon_2^{(j)}| : j = 1, 2, 3, 4\}}\right) < 2.44848.$$

Nadalje $D = [K : \mathbb{Q}] = 8$, pa imamo sve za primjeniti teorem 3.3. Dobivamo $c_7 = 3.83 \cdot 10^{22}$ i $c_8 = 0$. No prisjetimo se se da treba uzeti $c_8 = \log 4$ u primjeni leme 3.10. Tada dobivamo

$$A < 1.97 \cdot 10^{24}.$$

I sada dolazimo do nejednakosti oblika

$$|\lambda| < k_2 e^{-k_3 A},$$

gdje za konstante k_2 i k_3 možemo uzeti $k_2 = 190.83$, $k_3 = 2.05$. Također ako sad sa A označimo $A = \max\{|a_0|, |a_1|, |a_2|\}$ možemo uzeti $A < 3.94 \cdot 10^{24}$, jer vrijedi $|a_0| \leq rA$.

Sada možemo prijeći na smanjenje gornje ograde za A . No nailazimo na jedan, čini se, veliki problem. Pošto su koeficijenti u linearnoj formi Λ očito zavisni nad \mathbb{Q} , nećemo moći primijeniti LLL-algoritam. No to ipak nije tako veliki problem kako se u početku čini i sada ćemo opisati općeniti postupak,

kako postupiti u ovakvoj situaciji, kad su nam koeficijenti linearne forme linearno zavisni.

Neka je dana linearna forma

$$\Lambda = \delta + \sum_{i=1}^q \delta_i \mu_i,$$

koja zadovoljava nejednakost oblika

$$|\Lambda| < k_2 e^{-k_3 A},$$

gdje je $A = \max\{|\delta_i| : i = 1, \dots, q\}$, $A < c_9$ te neka su μ_1, \dots, μ_q linearno zavisni nad \mathbb{Q} .

Tada postupamo na sljedeći način. Uzmimo $M = \{\mu_1, \dots, \mu_p\}$ maksimalni linearno nezavisan podskup μ_i -ova. Tada znamo da postoje $d, d_{ij} \in \mathbb{Z}$ $d > 0$, $1 \leq i \leq p$, $p+1 \leq j \leq q$, takvi da je

$$d\mu_j = \sum_{i=1}^p d_{ij} \mu_i,$$

za $j = p+1, \dots, q$. Definirajmo sada novu linearnu formu $\Lambda' = d\Lambda$. Ako sada označimo $\delta' = d\delta$ i definiramo

$$a'_i = d\delta_i + \sum_{j=p+1}^q d_{ij} \delta_j,$$

za $i = 1, \dots, p$. Pa dobivamo

$$\Lambda' = \delta' + \sum_{i=1}^p a'_i \mu_i.$$

Koeficijenti ove norme su očito linearno nezavisni nad \mathbb{Q} . Definirajmo nadalje

$$\Delta = \max\{|d|, |d_{ij}| : 1 \leq i \leq p, p+1 \leq j \leq q\}.$$

Tada je jasno da vrijedi

$$|a'_i| \leq (q-p+1)\Delta \cdot A,$$

za $i = 1, \dots, p$. Ako sada stavimo $A' = \max\{|a'_i| : i = 1, \dots, p\}$. Tada vrijedi nejednakost

$$|\Lambda'| < k'_2 e^{-k'_3 A'},$$

3.2. PRIMJENA LINEARNIH FORMI NA DIOFANTSKE JEDNADŽBE I PROBLEME91

gdje je $k'_2 = dk_2$, $k'_3 = \frac{k_3}{(q-1+p)\Delta}$ i $A' < (q-p+1)c_9$.

Kao što vidimo sada smo našoj linearnoj formi s linearno zavisnim koeficijentima, pridružili drugu linearnu formu gdje su koeficijenti linearno nezavisni pa ćemo bez ikakvih problema moći primijeniti LLL-algoritam, te ćemo moći reducirati gornju ogradu za A' . Kada to napravimo, provjerit ćemo sva moguća rješenja, da li zadovoljavaju traženu nejednakost i za sva rješenja ćemo računati vrijednost forme Λ' . Tako ćemo naći L tako da vrijedi $|\Lambda'| \geq L$. I iz toga ćemo dobiti reduciranu gornju ogradu za A . Naime, lako se vidi da vrijedi

$$A < \frac{1}{k_3} \log \left(\frac{k_2}{L} \right)$$

i tako dobivena gornja ograda će biti zaista vrlo mala.

Primjenjujući sada detaljno opisan postupak, dobivamo $A \leq 3$, pa ostaje provjeriti koji su od brojeva $\pm \varepsilon_1^{a_1} \varepsilon_2^{a_2}$ oblika $X - \xi Y$, te tada za te X i Y provjerimo je li zadovoljena jednačba $X^4 - 2Y^4 = \pm 1$. Naravno, ne smijemo zaboraviti provjeriti što se događa za $|Y| \leq 3$. Na kraju dobivamo da su sva rješenja naše jednačbe dana sa

$$(X, Y) = (1, 0), (-1, 0), (1, 1), (-1, -1), (1, -1), (-1, 1).$$

Bibliografija

- [1] A. Baker, G. Wüstholz, *Logarithmic Forms and Diophantine Geometry*, Cambridge University Press, Cambridge, 2008.
- [2] H. Cohen, *Number Theory. Volume I: Tools and Diophantine Equations*, Springer Verlag, Berlin, 2007.
- [3] H. Cohen, *Number Theory. Volume II: Analytic And Modern Tools*, Springer Verlag, Berlin, 2007.
- [4] I. Gaal, *Diophantine Equations and Power Integral Bases*, Birkhauser, Boston, 2002.
- [5] M. J. Jacobson, Jr., H. C. Williams, *Solving the Pell Equation*, CMS Books in Mathematics, Springer, 2009.
- [6] F. Luca, *Diophantine Equations*, Winter School on Explicit Methods in Number Theory, Debrecen, Hungary, January 26-30, 2009.
- [7] T. Nagell, *Introduction to Number Theory*, Chelsea, New York, 1964.
- [8] W. M. Schmidt, *Diophantine Approximation and Diophantine Equations*, Springer Verlag, Berlin, 1996.
- [9] T. H. Shorey, R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Universitys Press, Cambridge, 1986.
- [10] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, Cambridge University Press, Cambridge, 1996.
- [11] V. G. Sprindžuk, *Classical Diophantine equations*, Springer Verlag, Berlin, 1993.

- [12] J. Steuding, *Diophantine Analysis*, Chapman Hall/CRC, Boca Raton, 2005.
- [13] B. M. M. de Weger, *Algorithms for Diophantine Equations*, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.
- [14] G. Wüstholz (Ed.), *A Panorama of Number Theory or The View from Baker's Garden*, Cambridge University Press, Cambridge, 2002.
- [15] U. Zannier, *Some applications of Diophantine Approximation to Diophantine Equations*, Forum Editrice, Udine, 2003.