MANUALIA UNIVERSITATIS STUDIORUM ZAGRABIENSIS
PRIRUČNICI SVEUČILIŠTA U ZAGREBU

DIOFANTOVI SKUPOVI

Alan Filipin, Zrinka Franušić

MANUALIA UNIVERSITATIS STUDIORUM ZAGRABIENSIS
PRIRUČNICI SVEUČILIŠTA U ZAGREBU

Autori
prof. dr. sc. Alan Filipin
izv. prof. dr. sc. Zrinka Franušić

Naslov
Diofantovi skupovi

Recenzenti
akad. Andrej Dujella
doc. dr. sc. Nikola Adžaga

Lektorica
dr. sc. Ana Ostroški Anić

Nakladnik
Prirodoslovno-matematički fakultet Sveučilišta u Zagrebu

Mjesto i godina izdavanja
Zagreb, 2022.

ISBN: 978-953-6076-92-5

Status **sveučilišnog priručnika** odobrio je Senat Sveučilišta u Zagrebu, Odlukom klasa: 032-01/21-02/10, ur. broj: 380-061/36-21-5, sa sjednice Senata 21. rujna 2021.

Sadržaj

Uvod

Neka je m prirodan broj. *Diofantova m-torka* je skup međusobno različitih prirodnih brojeva $\{a_1, a_2, \ldots, a_m\}$ za koji vrijedi da je umnožak bilo koja dva broja uvećan za 1 jednak punom kvadratu nekog prirodnog broja, odnosno

$$a_i a_j + 1 = n_{ij}^2,\ n_{ij} \in \mathbb{N},$$

za sve $1 \leq i < j \leq m$, ili kraće simbolički pisano

$$a_i a_j + 1 = \square, i \neq j.$$

Opisani skup nosi naziv prema starogrčkom matematičaru Diofantu iz Aleksandrije (3. st.) koji je uspio pronaći četiri pozitivna racionalna broja sa svojstvom da umnožak bilo koja dva među njima uvećan za 1 daje potpuni kvadrat u $\mathbb{Q}$:

$$\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}.$$

Zaista,

$$\frac{1}{16}\cdot\frac{33}{16}+1=\left(\frac{17}{16}\right)^2, \frac{1}{16}\cdot\frac{17}{4}+1=\left(\frac{9}{8}\right)^2, \frac{1}{16}\cdot\frac{105}{16}+1=\left(\frac{19}{16}\right)^2,$$
$$\frac{33}{16}\cdot\frac{17}{4}+1=\left(\frac{25}{8}\right)^2, \frac{33}{16}\cdot\frac{105}{16}+1=\left(\frac{61}{16}\right)^2, \frac{17}{4}\cdot\frac{105}{16}+1=\left(\frac{43}{8}\right)^2.$$

U 17. stoljeću francuski matematičar (i pravnik) Pierre de Fermat pronalazi prvu Diofantovu četvorku

$$\{1, 3, 8, 120\}.$$

Ponovo vrijedi:

$$1\cdot 3+1=2^2, 1\cdot 8+1=3^2, 1\cdot 120+1=11^2, 3\cdot 8+1=5^2, 3\cdot 120+1=19^2, 8\cdot 120+1=31^2.$$

Ova četvorka se ponekad naziva *Fermatova četvorka.*

Euler (18. st.) konstruira beskonačnu familiju Diofantovih četvorki:

$$\{a, b, a+b+2r, 4r(r+a)(r+b)\},$$

gdje je $ab+1=r^2$. Dakle, postoji beskonačno mnogo Diofantovih četvorki. Dugo godina se slutilo da ne postoji Diofantova petorka (u cijelim brojevima). Jedan od prvih koraka prema dokazu te slutnje bio je rezultat Bakera i Davenporta iz 1969., [4], koji kaže da se Diofantova trojka $\{1, 3, 8\}$ jedinstveno proširuje do Diofantove (Fermatove) četvorke $\{1, 3, 8, 120\}$. U dokazu se koristila Bakerova teorija o linearnim formama u logaritmima algebarskih brojeva i metoda redukcije koja se zasniva na verižnim razlomcima. Nakon toga slutnja o nepostojanju

Diofantove petorke provjerena je na mnogim familijama Diofantovih trojki i parova. Na primjer, Diofantova trojka $\{k-1, k+1, 4k\}$ do četvorke se jedinstveno nadopunjuje elementom $16k^3 - 4k$ ([15]]); Diofantov par $\{k-1, k+1\}$ ne može se nadopuniti do Diofantove petorke ([42]). Dujella godine 2004. u [25] dokazuje da postoji konačno mnogo Diofantovih petorki, pri čemu postavlja efektivnu gornju ogradu na veličinu elemenata ($< 10^{10^{26}}$). Nakon što se ograda u više navrata značajno smanjivala (Fujita, Filipin, Elsholtz, Cipu, Trudgian), no ipak ne dovoljno da bi se tvrdnja efektivno provjerila na računalu, 2019. godine objavljen je rad autora He, Togbé i Ziegler u kojem je dokazana slutnja o nepostojanju Diofantove petorke, odnosno vrijedi:

Teorem. ([47]) *Ne postoji Diofantova petorka.*

Ova tema još ipak nije potpuno zatvorena. Naime, postavljena je tzv. jača slutnja o nepostojanju Diofantove petorke koja kaže:

Slutnja. *Ako je $\{a, b, c, d\}$ Diofantova četvorka i $d > \max\{a, b, c\}$, tada je*

$$d = a + b + c + 2abc + 2rst,$$

pri čemu je $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$.

Obično se označava $d_+ = a + b + c + 2abc + 2rst$, a Diofantova četvorka $\{a, b, c, d\}$ za koju je $a < b < c$ i $d = d_+$ naziva se *regularnom.*

Problem nadopunjavanja Diofantove trojke $\{a, b, c\}$ do četvorke $\{a, b, c, d\}$ ekvivalentan je određivanju cjelobrojne trojke (x, y, z) za koju vrijedi

$$ad + 1 = x^2,\ bd + 1 = y^2,\ cd + 1 = z^2.$$

Eliminacijom broja d prethodne jednadžbe svode se na sustav diofantskih jednadžbi:

$$ay^2 - bx^2 = a - b, \tag{1}$$
$$az^2 - cx^2 = a - c. \tag{2}$$

Budući da svaku od prethodnih jednadžbi jednostavno možemo svesti na pelovsku jednadžbu (npr. $(ay)^2 - abx^2 = a(a-b)$), jedan od naših prvih zadataka bit će proučiti rješivost i opisati skup rješenja Pellove, odnosno pelovske jednadžbe (poglavlje 2).

Sustave jednadžbi pelovskog tipa (1), (2), koje ćemo još nazivati sustavima simultanih pelovskih jednadžbi, rješavamo pomoću „alata" koji predstavljamo u poglavljima 3 i 4. U poglavlju 3 navedeni su rezultati iz područja *diofanskih aproksimacija*, područja koje se bavi aproksimacijom iracionalnih brojeva racionalnim. Od posebne važnosti su nam rezultati koji govore o tome koliko se dobro više iracionalnih (preciznije algebarskih) brojeva može aproksimirati racionalnim brojevima s istim nazivnikom (npr. Bennettov teorem 3.2.10), tj. rezultati iz područja tzv. *simultanih aproksimacija.* Nadalje, sustavi tipa (1), (2) mogu se rješavati i primjenom rezultata iz *teorije linearnih formi u logaritmima algebarskih brojeva*, odnosno rezultatima vezanih uz izraze oblika

$$\Lambda = b_1 \log \alpha_1 + \cdots b_n \log \alpha_n,$$

gdje su $b_1, \ldots, b_n \in \mathbb{Q}$, a $\alpha_1, \ldots, \alpha_n$ algebarski brojevi. Konkretno, sustav (1), (2) može se rješavati primjenom Bakerovog teorema 5.2.2 koji linearnu formu $|\Lambda|$ ocjenjuje odozdo (u ovisnosti o koeficijentima b_i, te stupnjevima i visinama algebarskih brojeva α_i). U poglavlju 4 istaknuto je nekoliko teorema koji poboljšavaju originalni Bakerov rezultat (Baker-Wüstholzov teorem 4.1.5 te teoremi Matveeva 4.1.3 i 4.1.4). Na kraju, neizostavni dio postupka rješavanja simultanih pelovskih jednadžbi je smanjivanje ograde na rješenja koju dobivamo iz Bakerovih teorema. Opisali smo i primjenjivali tzv. Baker-Davenportovu redukciju (lema 3.3.1) koja koristi razvoj u verižni razlomak.

U poglavlju 5 konkretno se primjenjuju rezultati iz prethodnih poglavlja na problem proširenja Diofantove trojke do Diofantove četvorke. Najprije se bavimo proširenjem „najpoznatije" trojke $\{1, 3, 8\}$, zatim proširenjem familije $\{k-1, k+1, 4k\}$, $k \in \mathbb{N}$, $k > 2$, a na kraju i sasvim općenito proširenjem trojke $\{a, b, c\}$. Tek nakon svega toga možemo dobiti, barem djelomičan, uvid u to što „stoji" iza teorema „o nepostojanju Diofantove petorke".

U posljednja dva poglavlja 6 i 7 bavimo se nekim od brojnih poopćenja pojma Diofantove m-torke. Za početak možemo promatrati Diofantove m-torke u nekim drugim „ambijentalnim prostorima", npr. u polju racionalnih brojeva ili u prstenu Gaussovih cijelih brojeva. Zanimljivo je pitati se koliko veliki Diofantovi skupovi mogu biti u tim drugim „prostorima". Na primjer, za sada je pokazano da postoji beskonačno mnogo racionalnih Diofantovih šestorki, ali nije pronađena nijedna racionalna Diofantova sedmorka. Njihova konstrukcija koristi vezu Diofantovih m-torki s eliptičkim krivuljama. U prstenu Gaussovih cijelih brojeva nije pronađena nijedna petorka, no trenutna ograda na njihovu veličinu još uvijek je puno puno veća ($m \leq 42$).

Diofantove m-torke sa svojstvom $D(n)$ ili kraće $D(n)$-m-torke su m-člani skupovi $\{a_1, \ldots, a_m\}$, $a_i \neq 0$, za koje vrijedi

$$a_i a_j + n = \square, 1 \leq i < j \leq m,$$

a smisleno ih je proučavati u komutativnim prstenima s jedinicom. Uz te skupove veže se zanimljiva slutnja da postoji $D(n)$-četvorka ako i samo ako se n može prikazati kao razlika kvadrata, $u^2 - v^2$, do na konačan skup izuzetaka. Vrlo proučavan slučaj-izuzetak je $n = -1$ i sluti se da $D(-1)$-četvorka u $\mathbb{Z}$ ne postoji. U trenutku nastajanja ove skripte autori Bonciocat, Cipu i Mignotte najavili su da je slutnja o nepostojanju $D(-1)$-četvorke $\mathbb{Z}$ ipak pokazana. Njihov još nerecenzirani rad nalazi se na arXiv-u, [8].

Ovom skriptom obuhvatili smo samo jedan manji dio rezultata koji se vežu uz pojam Diofantovih skupova. Još puno toga zanimljivog i aktualnog može se naći na stranici *Diophantine m-tuples page* koju godinama brižljivo uređuje akademik Andrej Dujella, a koji je i sam dao veliki doprinos ovom dijelu teorije brojeva te je svoje znanje i znanstveni interes prenio na mnoge generacije studenata i mladih istraživača (a čini to neumorno i dalje), na čemu mu se iskreno zahvaljujemo.

Poglavlje 1

Jednostavni verižni razlomci

1.1 Definicija i osnovna svojstva

Neka je $x \in \mathbb{R}$. *Najveće cijelo* od x, u oznaci $\lfloor x \rfloor$, je najveći cijeli broj koji nije veći od x. Razlika broja x i njegova najvećeg cijela naziva se *razlomljeni dio* od x i zapisuje kao $\{x\}$. Očito je $\lfloor x \rfloor \in \mathbb{Z}$ i $\{x\} \in [0, 1\rangle$ za svaki $x \in \mathbb{R}$. Udaljenost broja x do najbližeg cijelog broja označava se s $\|x\|$. Lako se vidi da je $\|x\| = \min\{\{x\}, 1 - \{x\}\} \in [0, \frac{1}{2}]$.

Neka je $\alpha \in \mathbb{R}$ te

$$a_0 = \lfloor \alpha \rfloor.$$

Ako je $\alpha \neq a_0$, onda postoji α_1 takav da je

$$\alpha = a_0 + \frac{1}{\alpha_1}.$$

Zaista, $\alpha_1 = \dfrac{1}{\alpha - a_0} = \dfrac{1}{\{\alpha\}}$. Kako je $\alpha_1 > 1$, tada je

$$a_1 = \lfloor \alpha_1 \rfloor$$

prirodan broj. Ako je $\alpha_1 \neq a_1$, postoji α_2 takav da je

$$\alpha_1 = a_1 + \frac{1}{\alpha_2},$$

odnosno

$$\alpha = a_0 + \frac{1}{a_1 + \dfrac{1}{\alpha_2}}.$$

Opisani postupak moguće je ponavljati sve dok je $a_k \neq \alpha_k$. Pretpostavimo da je $a_n = \alpha_n$ za neki $n \in \mathbb{N}$. Tada se postupak prekida i vrijedi

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}. \tag{1.1}$$

Kažemo da (1.1) predstavlja prikaz broja α u *jednostavni konačni verižni razlomak.* Kraće ga zapisujemo kao

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

Brojevi $a_0 \in \mathbb{Z}$ i $a_1, a_2, \ldots, a_n \in \mathbb{N}$ nazivaju se *kvocijenti* verižnog razlomka.

Uočimo da je α racionalan broj ako je $a_n = \alpha_n$ za neki $n \in \mathbb{N}_0$, odnosno ako vrijedi (1.1). No, vrijedi i obrat. Ako je $\alpha \in \mathbb{Q}$, tada postoji $n \in \mathbb{N}_0$ takav da je $a_n = \alpha_n$. U tom slučaju, odnosno ako je $\alpha = \dfrac{b}{c} \in \mathbb{Q}$, kvocijente $a_0, a_1, \ldots, a_n$ verižnog razlomka određujemo pomoću *Euklidova algoritma* primijenjenog na brojeve b i c:

$$\begin{aligned}
b &= ca_0 + r_0,\ 0 < r_0 < c,\\
c &= r_0a_1 + r_1,\ 0 < r_1 < r_0,\\
r_0 &= r_1a_2 + r_2,\ 0 < r_2 < r_1,\\
&\vdots\\
r_{n-2} &= r_{n-1}a_n + r_n,\ 0 < r_n < r_{n-1},\\
r_{n-1} &= r_na_{n+1}.
\end{aligned}$$

Primjer 1. *Broj* $\dfrac{173}{119}$ *razvit ćemo u verižni razlomak koristeći Euklidov algoritam.*

$$\begin{aligned}
173 = 119 \cdot 1 + 54 \quad &\Rightarrow \quad \frac{173}{119} = 1 + \frac{54}{119},\\
119 = 54 \cdot 2 + 11 \quad &\Rightarrow \quad \frac{119}{54} = 2 + \frac{11}{54},\\
54 = 11 \cdot 4 + 10 \quad &\Rightarrow \quad \frac{54}{11} = 4 + \frac{10}{11},\\
11 = 10 \cdot 1 + 1 \quad &\Rightarrow \quad \frac{11}{10} = 1 + \frac{1}{10},\\
10 = 1 \cdot 10 + 0 \quad &\Rightarrow \quad \frac{10}{1} = 10.
\end{aligned}$$

Dakle, $\dfrac{173}{119} = [1; 2, 4, 1, 10]$.

Napomena 1.1.1. *Racionalan broj α koji nije cijeli ima točno dva razvoja u jednostavni verižni razlomak ako je $a_n \geq 2$: $[a_0, a_1, \ldots, a_n]$ i $[a_0, a_1, \ldots, a_{n-1}, a_n - 1, 1]$. Cijeli broj α isto ima točno dva razvoja u jednostavni verižni razlomak: $[\alpha]$ i $[\alpha - 1, 1]$.*

S druge strane, pokazuje se da se postupak razvoja u verižni razlomak može provoditi beskonačno ako i samo ako je broj α iracionalan. U tom slučaju njegov razvoj zapisujemo kao

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{\alpha_n}}}} = [a_0; a_1, a_2, \ldots, \alpha_n].$$

Neka su $a_0, a_1, \ldots, a_k$ kvocijenti razvoja u verižni razlomak broja α. Racionalni broj

$$\frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k],$$

naziva se k-ta *konvergenta* verižnog razlomka broja α. Prvih nekoliko konvergenti jednako je sljedećim izrazima:

$$\frac{p_0}{q_0} = a_0,\ \frac{p_1}{q_1} = \frac{a_0a_1+1}{a_1},\ \frac{p_2}{q_2} = \frac{a_0a_1a_2+a_0+a_2}{a_1a_2+1},\ \dots$$

Konvergente zadovoljavaju svojstva koja ćemo navesti u sljedećoj propoziciji.

Propozicija 1.1.2. *Neka su* $\frac{p_n}{q_n}$ *konvergente verižnog razlomka broja* α. *Vrijedi:*

(a)

$$p_n = a_np_{n-1} + p_{n-2},\ p_{-2} = 0,\ p_{-1} = 1, \tag{1.2}$$
$$q_n = a_nq_{n-1} + q_{n-2},\ q_{-2} = 1,\ q_{-1} = 0,\ n \geq 0; \tag{1.3}$$

(b)

$$q_np_{n-1} - p_nq_{n-1} = (-1)^n, n \geq -1;$$

(c) $\gcd(p_n, q_n) = 1$, $n \geq -2$;

(d) niz $\left(\frac{p_{2n}}{q_{2n}}\right)$ *je rastući, a niz* $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)$ *padajući;*

(e)

$$\frac{p_{2n}}{q_{2n}} < \frac{p_{2m+1}}{q_{2m+1}},\ m, n \in \mathbb{N}_0;$$

(f)

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha; \tag{1.4}$$

(g)

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2},\ n \in \mathbb{N}_0. \tag{1.5}$$

Dokazi gore navedenih svojstava konvergenti mogu se naći od 8.13 – 8.22 u [32].

Istaknimo da relacije (1.2) i (1.3) predstavljaju linearne rekurzije drugog reda za vrlo efikasno računanje brojnika i nazivnika konvergenti, odnosno nizova (p_n) i (q_n).

Već smo istaknuli da će realan broj imati beskonačan razvoj u verižni razlomak ako i samo ako je broj α iracionalan, no sada, s obzirom na konvergenciju niza $(\frac{p_n}{q_n})$, odnosno zbog (1.4) opravdano je pisati

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}} = [a_0; a_1, a_2, \dots]. \tag{1.6}$$

Kažemo da je (1.6) razvoj broja α u *jednostavni beskonačni verižni razlomak*.

1.2 Aproksimacije iracionalnih brojeva verižnim razlomcima

Konvergente su *jako dobre* (racionalne) aproksimacije iracionalnog broja α, što se već može zaključiti iz (1.5), no i iz teorema koji slijede.

Teorem 1.2.1. *Neka su* $\frac{p_{n-1}}{q_{n-1}}$ *i* $\frac{p_n}{q_n}$ *dvije uzastopne konvergente od* α*. Tada barem jedna od njih zadovoljava nejednakost*

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

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

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

Ako bi vrijedilo da je $\left|\alpha - \frac{p_n}{q_n}\right| \geq \frac{1}{2q_n^2}$ i $\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| \geq \frac{1}{2q_{n-1}^2}$, onda bismo dobili da je

$$\frac{1}{q_n q_{n-1}} \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n-1}^2}$$

što je ekvivalentno s nejednakošću $(q_n - q_{n-1})^2 \leq 0$, a to nije moguće. Dakle, $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2}$ ili $\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q_{n-1}^2}$. □

Neku vrstu obrata ovog teorema pokazao je Legendre i ona će se pokazati ključnom za određivanje fundamentalnog rješenja Pellove jednadžbe.

Teorem 1.2.2 (Legendre)**.** *Neka su* p *i* q *cijeli brojevi takvi da je*

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

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

Dokaz. Možemo pretpostaviti da je $\alpha \neq \frac{p}{q}$, inače je tvrdnja trivijalno zadovoljena. Tada možemo pisati $\alpha - \frac{p}{q} = \frac{\varepsilon\vartheta}{q^2}$, gdje je $0 < \vartheta < \frac{1}{2}$ i $\varepsilon = \pm 1$. Neka je $\frac{p}{q} = [b_0, b_1, \ldots, b_{n-1}]$ razvoj od $\frac{p}{q}$ u jednostavni verižni razlomak gdje je n izabran tako da vrijedi $(-1)^{n-1} = \varepsilon$. To uvijek možemo postići jer je $[a_0, a_1, \ldots, a_m] = [a_0, a_1, \ldots, a_m - 1, 1]$.

Sada se definira broj ω kao

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

Otuda je

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

pa je

$$\alpha = [b_0, b_1, \ldots, b_{n-1}, \omega].$$

Zbog svojstava konvergenti i povoljno odabranog n može se pokazati da je $\omega > 1$ što znači da $[b_0, b_1, \ldots, b_{n-1}]$ upravo predstavlja konvergentu $\frac{p}{q} = \frac{p_{n-1}}{q_{n-1}}$ broja α, što je i trebalo pokazati. □

Sljedeća tvrdnja poopćava teorem 1.2.2.

Teorem 1.2.3 (Dujella, [26]). *Neka je α realan broj, te c pozitivan realan broj. Ako racionalan broj $\frac{p}{q}$ zadovoljava nejednakost*

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

tada je

$$\frac{p}{q} = \frac{rp_n \pm sp_{n-1}}{rq_n \pm sq_{n-1}}$$

za neke nenegativne cijele brojeve n, r, s takve da je $rs < 2c$ i neki izbor predznaka.

1.3 Periodski verižni razlomci

Periodski verižni razlomak je beskonačni verižni razlomak $[a_0, a_1, a_2, \ldots]$ ako postoje cijeli brojevi $k \geq 0$, $m \geq 1$ za koje vrijedi

$$a_{m+n} = a_n$$

za sve $n \geq k$. Zapisujemo ga u obliku

$$[a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+m-1}}], \tag{1.7}$$

gdje $\overline{a_k, a_{k+1}, \ldots, a_{k+m-1}}$ označava blok kvocijenata koji se ponavljaju unedogled. Ako je (1.7) razvoj u verižni razlomak broja α, onda se $\beta = [\overline{a_k, a_{k+1}, \ldots, a_{k+m-1}}]$ naziva *čisto periodski dio* od α. *Duljina perioda* verižnog razlomka (1.7) jednaka je m.

Teorem 1.3.1 (Euler, Lagrange). *Razvoj u jednostavni verižni razlomak realnog broja α je periodski ako i samo ako je α kvadratna iracionalnost (tj. algebarski broj stupnja 2).*

Skica dokaza. Ako je verižni razlomak realnog broja α periodski, to jest

$$\alpha = [b_0, b_1, \ldots, b_{k-1}, \overline{a_0, a_1, \ldots, a_{m-1}}]$$

pri čemu njegov čisto periodski dio označimo s

$$\beta = [\overline{a_0, a_1, \ldots, a_{m-1}}] = [a_0, a_1, \ldots, a_{m-1}, \beta],$$

onda je

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

prema (1.2) i (1.3), a to znači da je β kvadratna iracionalnost pa je time i α kvadratna iracionalnost.

Obratno, neka je α kvadratna iracionalnost. Tada postoje $d, s_0, t_0 \in \mathbb{Z}$, $t_0 \neq 0$, $d \neq \square$ takvi da je

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

i $t_0 \mid (d - s_0^2)$. (Uočimo da je ovaj uvjet uvijek moguće postići; ako $t_0 \nmid (d - s_0^2)$, onda razlomak proširimo s t_0 pa $t_0^2 \mid (dt_0^2 - (s_0 t_0)^2)$). Neka je $a_0 = \lfloor \alpha \rfloor$. Za $i \geq 0$ računamo:

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

Pokazuje se da postoje $j, k \in \mathbb{N}$, $j < k$, t.d. je $(s_j, t_j) = (s_k, t_k)$ te da je

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

□

Razvoj specijalne kvadratne iracionalnosti $\sqrt{d}$ u verižni ralomak u vezi je s rješenjem Pellove jednadžbe te stoga u sljedećem teoremu navodimo njegova svojstva. Za dokaz vidjeti Teorem 8.41 u [32].

Teorem 1.3.2. *Verižni razlomak realnog broja $\sqrt{d}$ gdje d nije potpuni kvadrat oblika je*

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

gdje je $a_0 = \lfloor \sqrt{d} \rfloor$, a ostali kvocijenti se dobivaju pomoću rekurzije

$$s_{i+1} = a_i t_i - s_i,\ t_{i+1} = \frac{d - s_{i+1}^2}{t_i},\ a_{i+1} = \left\lfloor \frac{s_{i+1} + a_0}{t_{i+1}} \right\rfloor,\ i = 0, \ldots, r-1, \tag{1.8}$$

uz početne uvjete $s_0 = 0$, $t_0 = 1$.

Kvocijenti $a_1, a_2, \ldots, a_{r-1}$ su centralno simetrični, to jest $a_1 = a_{r-1}$, $a_2 = a_{r-2}$, ...

Napomena 1.3.3. *Budući da ne znamo unaprijed duljinu perioda u razvoju broja $\sqrt{d}$, algoritam (1.8) provodimo sve dok se vrijednosti s_1 i t_1 ne ponove. Ako je duljina perioda jednaka r, onda ćemo dobiti da je $(s_1, t_1) = (s_{r+1}, t_{r+1})$, što će nam biti znak da prestajemo s postupkom.*

Poglavlje 2

Pellova jednadžba. Pelovske jednadžbe

2.1 Egzistencija rješenja Pellove jednadžbe

Definicija 2.1.1. *Neka je d prirodni broj koji nije potpuni kvadrat. Diofantska jednadžba oblika*

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

zove se Pellova jednadžba.

Jednadžba oblika

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

gdje je N cijeli broj naziva se pelovska jednadžba.

Prirodno pitanje koje se nameće jest imaju li jednadžbe (2.1) i (2.2) rješenja. Odgovor je potvrdan za Pellovu jednadžbu. Štoviše, (2.1) ima beskonačno mnogo rješenja u skupu prirodnih brojeva za svaki prirodni broj d koji nije potpuni kvadrat. Za razliku od toga, pelovske jednadžbe ne moraju imati rješenja. Sljedeći problem koji se postavlja jest kojom metodom odrediti rješenja te kako opisati skup svih rješenja.

Zanimljivo da jednadžba (2.1) nosi ime engleskog matematičara 17. stoljeća Johna Pella, koji nije značajno doprinio njezinu rješavanju. Zaslugu mu je pogrešno pripisao Euler. No jednadžba je pobuđivala zanimanje matematičara i znatno ranije. Tako se jednadžba $x^2-2y^2 = 1$ pojavljuje kod starogrčkih matematičara (6. st. pr. Kr.) u vezi s istraživanjem prirode broja $\sqrt{2}$. Nadalje, njome su se bavili i indijski matematičari iz 7. stoljeća, Brahmagupta i Bhaskara, koji su našli rješenje za neke specijalne vrijednosti broja d, konkretno $d = 11, 31, 61, 67$. Ove vrijednosti nipošto nisu nasumično odabrane nego su takve da je najmanje rješenje u skupu prirodnih brojeva neočekivano veliko. Tako je najmanje rješenje jednadžbe $x^2 - 61y^2 = 1$ jednako $x = 1776319049$, $y = 22615390$. Pet stoljeća kasnije Bhaskara II usavršava metodu za rješavanje pelovskih jednadžbi svojih prethodnika te tu metodu naziva *caravala* (cikličkі postupak). Ono što nije uspio dokazati jest je li metoda učinkovita za svaki d. Prvi Europljani koji su značajnije sudjelovali u izučavanju bili su Fermat, Frenicle de Bessy, Brouncker i Wallis sredinom 17. stoljeća, no najveće zasluge pripadaju Lagrangeu (18. st.) koji će ponuditi sasvim novi pristup baziran na verižnim razlomcima.

Teorem 2.1.2. *Neka je d prirodan broj koji nije potpuni kvadrat. Postoji bar jedan par prirodnih brojeva (x, y) koji zadovoljava Pellovu jednadžbu (2.1).*

Teorem 2.1.2 je iskazao Fermat, ali bez dokaza. Dokaz se zasniva na sljedećoj posljedici Dirichletovog teorema (vidi na primjer Teorem 6.1. u [32]) koji navodimo bez dokaza, ali slijedi i direktno iz propozicije 1.1.2(g)).

Lema 2.1.3. *Ako je α iracionalan broj, onda postoji beskonačno mnogo relativno prostih cijelih brojeva p i q, takvih da je*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{2.3}$$

Korolar 2.1.4. *Neka je d prirodan broj koji nije potpuni kvadrat. Postoji beskonačno mnogo parova prirodnih brojeva (x, y) koji zadovoljavaju nejednakost*

$$|x^2 - dy^2| < 1 + 2\sqrt{d}. \tag{2.4}$$

Dokaz. Broj $\sqrt{d}$ je iracionalan, i prema lemi 2.1.3 postoji beskonačno mnogo parova pozitivnih cijelih brojeva (x, y), takvih da je

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

Nadalje, vrijedi

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

Stoga je

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

Dakle, nejednakost (2.4) ima beskonačno mnogo cjelobrojnih rješenja x i y. □

Dokaz teorema 2.1.2. Prema korolaru 2.1.4 postoji cijeli broj $k \neq 0$ takav da je $x^2 - dy^2 = k$ za beskonačno mnogo parova cijelih brojeva (x, y). Među ovim parovima moraju postojati najmanje dva para (x_1, y_1) i (x_2, y_2) za koja vrijedi

$$x_1 \equiv x_2 \pmod{|k|}, \quad y_1 \equiv y_2 \pmod{|k|}. \tag{2.5}$$

Sada imamo

$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_1x_2 - y_1y_2d + (x_1y_2 - x_2y_1)\sqrt{d}.$$

Iz (2.5) i $x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = k$ dobivamo sljedeće kongruencije

$$x_1x_2 - y_1y_2d \equiv x_1^2 - y_1^2d \equiv 0 \pmod{|k|},\ x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{|k|}.$$

Prema tome,

$$x_1x_2 - y_1y_2d = ku,\ x_1y_2 - x_2y_1 = kv,$$

za neke cijele brojeve u i v. Stoga vrijedi

$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = k(u + v\sqrt{d}),$$

$$(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = k(u - v\sqrt{d}).$$

Množenjem ovih dviju jednadžbi dobivamo

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = k^2 = k^2(u^2 - dv^2).$$

Dakle, imamo da je $u^2 - dv^2 = 1$.

Tvrdnja teorema bit će dokazana ako ustanovimo da je $v \neq 0$. Pretpostavimo da je $v = 0$. Tada je $x_1 y_2 = x_2 y_1$, $u = \pm 1$, pa je

$$(x_1 - y_1\sqrt{d})k = (x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d})(x_2 - y_2\sqrt{d}) = \pm k(x_2 - y_2\sqrt{d}).$$

Nakon dijeljenja s k dobivamo $x_1 - y_1\sqrt{d} = \pm(x_2 - y_2\sqrt{d})$, što implicira da je $x_1 = \pm x_2$ i $y_1 = \pm y_2$. Budući da možemo izabrati $|x_1| \neq |x_2|$, slijedi da je $v \neq 0$. □

Ustanovili smo da Pellova jednadžba uvijek ima rješenje (u, v) u skupu prirodnih brojeva. Uobičajeno je to rješenje formalno označiti kao

$$u + v\sqrt{d},$$

to jest kao element kvadratnog polja $\mathbb{Q}(\sqrt{d})$. Uskoro ćemo vidjeti da takav zapis ima i tehničkih prednosti. Na ovaj je način lako uvesti i uređaj u skupu rješenja. Rješenje $u + v\sqrt{d}$ veće je od rješenja $u' + v'\sqrt{d}$ ako vrijedi numerička nejednakost $u + v\sqrt{d} > u' + v'\sqrt{d}$. S obzirom na to, ima smisla izdvojiti i najmanje rješenje. Najmanje rješenje Pellove jednadžbe (2.1) u skupu prirodnih brojeva naziva se *fundamentalno rješenje* i označava s $x_1 + y_1\sqrt{d}$.

Primjer 2. *Ako su $u + v\sqrt{d}$ i $u' + v'\sqrt{d}$ rješenja od (2.1), onda je i $(u + v\sqrt{d})(u' + v'\sqrt{d})$ rješenje od (2.1). Ako je $a + b\sqrt{d}$ rješenje pelovske jednadžbe $x^2 - dy^2 = -1$, onda je $(a + b\sqrt{d})^2$ rješenje Pellove jednadžbe (2.1).*

Budući da smo uočili smislenost označavanja rješenja Pellove, odnosno pelovske jednadžbe kao elementa kvadratnog polja, istaknut ćemo neke osnovne pojmove i svojstva koja se vežu uz kvadratna polja. Neka je $d \in \mathbb{Z}$ i d nije potpuni kvadrat. Tada skup

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \,:\, a, b \in \mathbb{Q}\}$$

uz operacije standardnog zbrajanja i množenja ima algebarsku strukturu polja te ga nazivamo *kvadratno polje*. Uočimo: ako za neki $k \in \mathbb{Z}$, $k \neq 0$, $k^2 | d$, tj. $d = k^2 d'$, tada je $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$, što znači da možemo pretpostaviti da je d kvadratno slobodan. Svaki element kvadratnog polja $\mathbb{Q}(\sqrt{d})$ može se shvatiti kao nultočka jedinstvenoga normiranog kvadratnog polinoma $x^2 + Ax + B = 0$, gdje su $A, B \in \mathbb{Q}$. Ako je element $\alpha \in \mathbb{Q}(\sqrt{d})$ nultočka kvadratnog polinoma $x^2 + Ax + B = 0$, gdje su A, B cijeli brojevi, onda se α naziva *algebarski cijeli broj* ili kraće samo *cijeli broj*. Skup svih cijelih brojeva nekog kvadratnog polja čini prsten, tzv. *prsten cijelih brojeva* i označava se s $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. U ovisnosti o broju d znamo precizno opisati sve elemente prstena cijelih brojeva. Naime, vrijedi

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \,:\, a, b \in \mathbb{Z}\}, \ d \equiv 2 \text{ ili } 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{a + b\frac{1+\sqrt{d}}{2} \,:\, a, b \in \mathbb{Z}\}, \\ \qquad\qquad = \{\frac{u+v\sqrt{d}}{2} \,:\, u, v \in \mathbb{Z}, u \equiv v \pmod 2\}, \ d \equiv 1 \pmod 4. \end{cases}$$

Skup invertibilnih elemenata u $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ čini multiplikativnu grupu koju nazivamo *grupom jedinica*.

Norma elementa $\alpha = a + b\sqrt{d}$ definira se kao

$$N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

Istaknimo neka svojstva norme:

- $N(\alpha\beta) = N(\alpha)N(\beta)$, za sve $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$,
- $N(\alpha) = 0$ ako i samo ako je $\alpha = 0$,
- $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \Rightarrow N(\alpha) \in \mathbb{Z}$,
- $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ je jedinica ako i samo ako $N(\alpha) \in \{-1, 1\}$.

Zbog posljednjeg svojstva vidimo da su jedinice iz prstena $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ u vezi s Pellovom te s nekim pelovskim jednadžbama. Precizno, uz pretpostavku $d \equiv 2$ ili $3 \pmod 4$, $\alpha = a+b\sqrt{d}$ je jedinica ako i samo ako je $a + b\sqrt{d}$ rješenje jedne od jednadžbi $x^2 - dy^2 = \pm 1$. Uz $d \equiv 1 \pmod 4$, $\alpha = a + b\sqrt{d}$ je jedinica ako i samo ako je $a + b\sqrt{d}$ rješenje jedne od jednadžbi $x^2 - dy^2 = \pm 4$.

2.2 Struktura skupa rješenja Pellove jednadžbe

Teorem 2.2.1. *Neka je $x_1 + y_1\sqrt{d}$ fundamentalno rješenje Pellove jednadžbe (2.1). Tada su sva rješenja u skupu prirodnih brojeva dana formulom*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n. \tag{2.6}$$

Konkretno, vrijedi

$$\begin{aligned} x_n &= \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} x_1^{n-2k} y_1^{2k} d^k, \\ y_n &= \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k+1} x_1^{n-2k-1} y_1^{2k+1} d^k. \end{aligned}$$

Dokaz. Lako se provjeri da je $x_n + y_n\sqrt{d}$ rješenje. Zaista, množenjem izraza $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ i $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$ dobivamo

$$x_n^2 - dy_n^2 = (x_1 + y_1\sqrt{d})^n(x_1 - y_1\sqrt{d})^n = (x_1^2 - dy_1^2)^n = 1.$$

Sada je potrebno dokazati da nema drugih rješenja. Pretpostavimo da je $u + v\sqrt{d}$ rješenje, $u, v \in \mathbb{N}$ koje nije dobiveno formulom (2.6). Tada postoji $n \in \mathbb{N}$ za koji je

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

Otuda je

$$1 < (u + v\sqrt{d})(x_1 + y_1\sqrt{d})^{-n} < x_1 + y_1\sqrt{d},$$

odnosno jer je $(x_1 + y_1\sqrt{d})^{-1} = x_1 - y_1\sqrt{d}$

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

Lako se provjeri da je

$$a + b\sqrt{d} = (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^n$$

rješenje jednadžbe. Ako ustanovimo da su a i b prirodni brojevi, onda smo dobili kontradikciju s činjenicom da je $x_1 + y_1\sqrt{d}$ fundamentalno rješenje. Zaista, vrijedi

$$2a = a + b\sqrt{d} + (a - b\sqrt{d}) = a + b\sqrt{d} + (a + b\sqrt{d})^{-1} > 0,$$

te

$$2b\sqrt{d} = a + b\sqrt{d} - (a - b\sqrt{d}) = a + b\sqrt{d} - (a + b\sqrt{d})^{-1} > 0,$$

jer je $a + b\sqrt{d} > 1$ i $0 < (a - b\sqrt{d}) = (a + b\sqrt{d})^{-1} < 1$. □

Označimo sa S skup svih rješenja (x, y) Pellove jednadžbe takvih da je x prirodan, a y cjelobrojan, to jest

$$S = \{x + y\sqrt{d} : x^2 - dy^2 = 1, (x, y) \in \mathbb{N} \times \mathbb{Z}\}.$$

Uočimo da rješenja Pellove jednadžbe leže na hiperboli $x^2 - dy^2 = 1$, a točke skupa S leže na desnoj grani te hiperbole. Pokazat ćemo da skup S ima algebarsku strukturu grupe.

Teorem 2.2.2. *Skup S je multiplikativna ciklička grupa.*

Dokaz. Najprije provjerimo da je skup S zatvoren na množenje. Neka su $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ iz S. Tada je

$$(x + y\sqrt{d})(x' + y'\sqrt{d}) = xx' + yy'd + (xy' + x'y)\sqrt{d}.$$

Vrijedi da je

$$(xx' + yy'd)^2 - d(xy' + x'y)^2 = x^2(x'^2 - dy'^2) - dy^2(x'^2 - dy'^2) = x^2 - dy^2 = 1,$$

pa $(x + y\sqrt{d})(x' + y'\sqrt{d})$ zadovoljava Pellovu jednadžbu. S druge strane, $xx' + yy'd \in \mathbb{N}$ jer je $x^2 = 1 + dy^2 > dy^2$, odnosno $x > \sqrt{d}|y|$ pa je i $xx' > d|yy'|$. Stoga zaključujemo da je $(x + y\sqrt{d})(x' + y'\sqrt{d}) \in S$.

Multiplikativna jedinica 1 je element iz S jer je $(1, 0)$ trivijalno rješenje. Multiplikativni inverz od $x + y\sqrt{d}$ je $x - y\sqrt{d}$, a to je element skupa S. Prema teoremu 2.2.1 jasno je da je fundamentalno rješenje $x_1 + y_1\sqrt{d}$ generator grupe S. □

2.3 Rekurzivne formule za rješenja Pellove jednadžbe

Teorem 2.3.1. *Rješenja Pellove jednadžbe (2.1) u skupu prirodnih brojeva (x_n, y_n) zadovoljavaju rekurzivne relacije*

$$\begin{aligned} x_n &= x_1x_{n-1} + dy_1y_{n-1}, \\ y_n &= y_1x_{n-1} + x_1y_{n-1}, \ n \geq 1, \end{aligned} \tag{2.7}$$

pri čemu je (x_1, y_1) fundamentalno, a $(x_0, y_0) = (1, 0)$ trivijalno rješenje jednadžbe (2.1).

Nadalje, uz iste početne uvjete vrijede i relacije

$$\begin{aligned} x_n &= 2x_1x_{n-1} - x_{n-2}, \\ y_n &= 2x_1y_{n-1} - y_{n-2}, \ n \geq 2. \end{aligned} \tag{2.8}$$

Dokaz. Rekurzije u (2.7) direktno slijede prema (2.6), to jest iz

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

Nadalje, jer je $x_1 - y_1\sqrt{d} = (x_1 + y_1\sqrt{d})^{-1}$ imamo

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

Raspisivanjem gornjih jednakosti

$$\begin{aligned} x_1x_{n-1} + y_1x_{n-1}\sqrt{d} + x_1y_{n-1}\sqrt{d} + y_1y_{n-1}d &= x_n + y_n\sqrt{d}, \\ x_1x_{n-1} - y_1x_{n-1}\sqrt{d} + x_1y_{n-1}\sqrt{d} - y_1y_{n-1}d &= x_{n-2} + y_{n-2}\sqrt{d} \end{aligned}$$

i njihovim zbrajanjem slijedi (2.8). □

Rekurzije u (2.7) matrično se mogu prikazati na sljedeći način

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{2.9}$$

Slično, vrijedi i

$$\begin{pmatrix} x_n & dy_n \\ y_n & x_n \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_{n-1} & dy_{n-1} \\ y_{n-1} & x_{n-1} \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^n. \tag{2.10}$$

Ovaj matrični zapis rekurzija omogućava nam da izvedemo zgodne identitete koji zadovoljavaju rješenja Pellove jednadžbe.

Korolar 2.3.2. *Neka je (x_n, y_n) niz rješenja Pellove jednadžbe (2.1). Vrijede sljedeći identiteti* zbroja*, odnosno* razlike*:*

$$\begin{aligned} x_{m\pm n} &= x_m x_n \pm d y_m y_n, \\ y_{m\pm n} &= x_n y_m \pm x_m y_n,\ m \geq n. \end{aligned}$$

Dokaz. Iz (2.10) dobivamo

$$\begin{pmatrix} x_{m+n} & dy_{m+n} \\ y_{m+n} & x_{m+n} \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^{m+n} = \begin{pmatrix} x_m & dy_m \\ y_m & x_m \end{pmatrix} \begin{pmatrix} x_n & dy_n \\ y_n & x_n \end{pmatrix},$$

što nam daje identitete zbroja. Da bismo dobili identitete razlike, uočimo da je

$$\begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^{-1} = \frac{1}{x_1^2 - dy_1^2} \begin{pmatrix} x_1 & -dy_1 \\ -y_1 & x_1 \end{pmatrix} = \begin{pmatrix} x_1 & -dy_1 \\ -y_1 & x_1 \end{pmatrix},$$

i stoga je

$$\begin{pmatrix} x_{m-n} & dy_{m-n} \\ y_{m-n} & x_{m-n} \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^{m-n} = \begin{pmatrix} x_m & dy_m \\ y_m & x_m \end{pmatrix} \begin{pmatrix} x_n & -dy_n \\ -y_n & x_n \end{pmatrix}$$

□

Direktno iz korolara 2.3.2 za $m = n$ dobivamo još jedan zanimljiv identitet.

Korolar 2.3.3. *Neka je (x_n, y_n) niz rješenja Pellove jednadžbe (2.1). Vrijedi sljedeći identitet* dvostrukog kuta*:*

$$\begin{aligned} x_{2n} &= 2x_n^2 - 1, \\ y_{2n} &= 2x_n y_n,\ n \geq 0. \end{aligned}$$

2.4 Veza rješenja Pellove jednadžbe s verižnim razlomcima

Do sada smo ustanovili da je Pellova jednadžba uvijek rješiva, te opisali njezin skup rješenja. Iz svega do sada iznesenog vidi se da je najbitnije pronaći najmanje rješenje u skupu prirodnih brojeva – *fundamentalno* rješenje. Jedna od metoda pomoću koje ćemo se sigurno domoći fundamentalnog rješenja jest ta da ispitujemo redom je li broj $1 + dy^2$ potpuni kvadrat za $y = 1, 2, \ldots$. No primjer Pellove jednadžbe za $d = 61$ pokazuje da ta metoda nije učinkovita. Metoda koja se pokazuje djelotvornom leži u razvoju broja $\sqrt{d}$ u *jednostavni verižni razlomak* koji smo opisali u odjeljku 1.3.

Teorem 2.4.1. *Neka je $(u, v) \in \mathbb{N}^2$ rješenje Pellove jednadžbe $x^2 - dy^2 = 1$. Onda je $\frac{u}{v}$ neka konvergenta razvoja $\sqrt{d}$ u verižni razlomak.*

Dokaz. Faktorizacijom Pellove jednadžbe imamo

$$(u - v\sqrt{d})(u + v\sqrt{d}) = 1. \tag{2.11}$$

Iz toga možemo zaključiti da je $u - v\sqrt{d}$ pozitivan broj i da je $\frac{u}{v} > \sqrt{d}$. Jednakost (2.11) možemo zapisati kao $u - v\sqrt{d} = \frac{1}{u + v\sqrt{d}}$. Na taj način imamo

$$\frac{u}{v} - \sqrt{d} = \frac{1}{v(u + v\sqrt{d})} = \frac{1}{v^2\left(\frac{u}{v} + \sqrt{d}\right)} < \frac{1}{2\sqrt{d}v^2} < \frac{1}{2v^2}.$$

Kako je $\frac{u}{v} - \sqrt{d}$ pozitivan, vrijedi $\left|\frac{u}{v} - \sqrt{d}\right| < \frac{1}{2v^2}$. Sada po Teoremu 1.2.2 slijedi da je $\frac{u}{v}$ konvergenta razvoja $\sqrt{d}$ u verižni razlomak. □

Napomena 2.4.2. *Uz male modifikacije može se pokazati da tvrdnja teorema 2.4.1 vrijedi i za sve jednadžbe oblika $x^2 - dy^2 = N$ gdje je $|N| < \sqrt{d}$.*

Sva rješenja Pellove jednadžbe u prirodnim brojevima nalaze se među konvergentama u razvoju od $\sqrt{d}$. Štoviše, ta se veza može i sasvim precizno opisati.

Teorem 2.4.3. *Neka je r duljina perioda u razvoju od $\sqrt{d}$ te neka su (p_n/q_n) konvergente od $\sqrt{d}$.*

Ako je r paran, onda jednadžba $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja od $x^2 - dy^2 = 1$ su dana s (p_{nr-1}, q_{nr-1}) za $n \in \mathbb{N}$.

Ako je r neparan, onda su sva rješenja jednadžbe $x^2 - dy^2 = -1$ dana s (p_{nr-1}, q_{nr-1}) za $n \in \mathbb{N}$ neparan, dok su sva rješenja jednadžbe $x^2 - dy^2 = 1$ dana s (p_{nr-1}, q_{nr-1}) za $n \in \mathbb{N}$ paran.

Napomena 2.4.4. *Ako je r paran, onda je fundamentalno rješenje od $x^2 - dy^2 = 1$ dano s (p_{r-1}, q_{r-1}). Ako je r neparan, onda je fundamentalno rješenje od $x^2 - dy^2 = -1$ dano s (p_{r-1}, q_{r-1}), a fundamentalno rješenje od $x^2 - dy^2 = 1$ s (p_{2r-1}, q_{2r-1}), odnosno s $(p_{r-1} + q_{r-1}\sqrt{d})^2$.*

Iz prethodne napomene sada nam je jasno kako se dogodilo da je fundamentalno rješenje nekih Pellovih jednadžbi za relativno mali d jako veliko. Sjetimo se jednadžbe koju smo spominjali na samom početku $x^2 - 61y^2 = 1$. Razlog tomu leži u velikom periodu:

$$\sqrt{61} = [7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$$

pa je

$$(x_0, y_0) = (p_{21}, q_{21}) = (1\,766\,319\,049, 226\,153\,980).$$

2.5 Pelovske jednadžbe

U prethodnim odjeljcima pokazali smo da je Pellova jednadžba (2.1) uvijek rješiva te detaljno opisali skup svih njenih rješenja u skupu prirodnih brojeva. Za razliku od toga, pelovska jednadžba $x^2 - dy^2 = N$ ne mora biti rješiva za svaki d i N. Međutim, ako je $a + b\sqrt{d}$ rješenje pelovske jednadžbe (2.2), a $u + v\sqrt{d}$ rješenje Pellove jednadžbe (2.1), onda je

$$(a + b\sqrt{d})(u + v\sqrt{d}) = (ua + vb) + (av + ub)\sqrt{d}$$

rješenje jednadžbe (2.2). To znači da će svaka pelovska jednadžba, ako je rješiva, imati beskonačno mnogo rješenja.

Za dva rješenja $a + b\sqrt{d}$, $a' + b'\sqrt{d}$ pelovske jednadžbe (2.2) kažemo da su *asocirana* ako vrijedi

$$(a + b\sqrt{d})(u + v\sqrt{d}) = a' + b'\sqrt{d},$$

za neko rješenje $u+v\sqrt{d}$ Pellove jednadžbe (2.1). Lako se može uočiti da je *biti asociran* relacija ekvivalencije na skupu svih rješenja jednadžbe (2.2). Zbog toga se skup svih rješenja pelovske jednadžbe raspada na klase. Za klasu kažemo da je *dvoznačna* ako je klasa

$$K = \{x_i + y_i\sqrt{d} \,:\, i \in \mathbb{N}\}$$

jednaka tzv. *konjugiranoj klasi*

$$\overline{K} = \{x_i - y_i\sqrt{d} \,:\, i \in \mathbb{N}\}.$$

Pripadnost rješenja istoj klasi može se karakterizirati sljedećim jednostavnim uvjetima:

Propozicija 2.5.1. *Rješenja $a + b\sqrt{d}$ i $a' + b'\sqrt{d}$ pelovske jednadžbe $x^2 - dy^2 = N$ asocirana su ako i samo ako*

$$aa' \equiv bb'd \pmod{N},\ ab' \equiv a'b \pmod{N}.$$

U klasi rješenja K posebno ćemo istaknuti rješenje $x^*+y^*\sqrt{d}$, takvo da y^* poprima najmanju nenegativnu vrijednost među elementima u K. Ako je klasa dvoznačna ($K = \overline{K}$), onda pripadni x^* nije jednoznačno određen, pa tada uzimamo onaj za koji je $x^* \geq 0$. To istaknuto rješenje $x^* + y^*\sqrt{d}$ naziva se *fundamentalno rješenje*.

Iz sljedećeg teorema zaključit ćemo da postoji konačno mnogo klasa, odnosno konačno mnogo fundamentalnih rješenja pelovske jednadžbe $x^2 - dy^2 = N$.

Teorem 2.5.2. *Neka je $u+v\sqrt{d}$ fundamentalno rješenje Pellove jednadžbe $x^2-dy^2 = 1$. Tada svako fundamentalno rješenje $x^* + y^*\sqrt{d}$ pelovske jednadžbe $x^2 - dy^2 = N$ zadovoljava sljedeće nejednakosti:*

$$0 \leq y^* \leq \frac{v}{\sqrt{2(u+\varepsilon)}}\sqrt{|N|},\ |x^*| \leq \sqrt{\frac{1}{2}(u+\varepsilon)|N|}, \tag{2.12}$$

pri čemu je $\varepsilon = 1$ za $N > 0$, odnosno $\varepsilon = -1$ za $N < 0$.

Dokaz. Pretpostavimo da je $N < 0$. Neka je

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

gdje je

$$\delta = \begin{cases} 1, & x^* \geq 0, \\ -1, & x^* < 0. \end{cases}$$

Očito je $x' + y'\sqrt{d}$ rješenje od $x^2 - dy^2 = N$ koje pripada klasi reprezentiranoj fundamentalnim rješenjem, $[x^* + y^*\sqrt{d}]$. Stoga je

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

odnosno

$$\underbrace{x^*\delta}_{|x^*|} v = y^*u - y' \leq y^*(u-1).$$

Budući da su obje strane prethodne nejednakosti veće ili jednake 0, možemo ju kvadrirati pa dobivamo

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

tj.

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

Otuda je

$$y^{*2}(\underbrace{dv^2 - u^2}_{-1} + 2u - 1) \leq \underbrace{-N}_{|N|} v^2$$

što povlači prvu nejednakost u (2.12). Drugu nejednakost dobivamo iz

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

□

Primjer 3. *Riješimo jednadžbu*

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

Fundamentalno rješenje pripadne Pellove jednadžbe $x^2 - 6y^2 = 1$ *je* $5 + 2\sqrt{6}$. *Sva fundamentalna rješenja jednadžbe* $x^2 - 6y^2 = -29$ *moraju zadovoljavati nejednakosti*

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

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

Dobivamo da su jedina fundamentalna rješenja $5 + 3\sqrt{6}$ *i* $-5 + 3\sqrt{6}$ *i ona ne pripadaju istoj klasi. Stoga su sva cjelobrojna rješenja od* $x^2 - 6y^2 = -29$:

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

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

Primjer 4. *Pokažimo da jednadžba*

$$x^2 - 82y^2 = 23$$

nema cjelobrojnih rješenja. Fundamentalno rješenje pripadne Pellove jednadžbe $x^2 - 82y^2 = 1$ *je* $162 + 18\sqrt{82}$. *Za fundamentalno rješenje* $x^* + y^*\sqrt{82}$ *polazne jednadžbe vrijedi ocjena* $y^* < 5$. *Lako se provjeri da jednadžba* $x^2 - 82y^2 = 23$ *nema cjelobrojnih rješenja za* $y = 1, 2, 3, 4$.

Poglavlje 3

Metode i algoritmi iz diofantskih aproksimacija

3.1 Liouvilleov i Rothov teorem

U ovom ćemo poglavlju obraditi neke metode koje dolaze iz diofantskih aproksimacija, a koje ćemo kasnije koristiti kod problema vezanih za Diofantove m-torke, kao i kod rješavanja nekih srodnih diofantskih problema i jednadžbi.

Definicija 3.1.1. *Neka je $\alpha \in \mathbb{C}$. Kažemo da je α* algebarski broj *ako postoji polinom $f(x) \in \mathbb{Q}[X]$ različit od nulpolinoma, takav da vrijedi $f(\alpha) = 0$. Ako $\alpha \in \mathbb{C}$ nije algebarski, kažemo da je* transcendentan.

Teorem 3.1.2. *Neka je α algebarski broj. Tada postoji jedinstveni normirani ireducibilan polinom $P_\alpha(x) \in \mathbb{Q}[X]$ takav da vrijedi $P_\alpha(\alpha) = 0$. Nadalje, svaki polinom $Q(x) \in \mathbb{Q}[X]$ koji α poništava djeljiv je s $P_\alpha(x)$.*

Dokaz. Kako je α algebarski broj, postoji polinom $P(x) \in \mathbb{Q}[X]$, najmanjeg stupnja, koji α poništava. Definirajmo polinom $P_\alpha(x) = \frac{1}{c}P(x)$, gdje je c vodeći koeficijent od $P(x)$. Tada je očito $P_\alpha(x) = 0$ i $P_\alpha(x)$ je normiran. Nadalje, $P_\alpha(x)$ je ireducibilan. Naime, u suprotnom bismo imali $P_\alpha(x) = p_1(x)p_2(x)$ gdje je $p_1(\alpha) = 0$ ili $p_2(\alpha) = 0$ što je u kontradikciji s minimalnošću stupnja od $P(x)$.

Neka je sada $Q(x) \in \mathbb{Q}[X]$ takav da vrijedi $Q(\alpha) = 0$. Ako podijelimo $Q(x)$ s $P_\alpha(x)$, dobivamo $Q(x) = P_\alpha(x)q(x) + r(x)$, gdje je $\deg r < \deg P_\alpha$. No, kako je $r(\alpha) = 0$, zbog minimalnosti stupnja od $P_\alpha(x)$, zaključujemo kako je $r(x)$ nulpolinom, odnosno da je $Q(x)$ djeljiv s $P_\alpha(x)$.

Ostaje još pokazati jedinstvenost polinoma $P_\alpha(x)$. Kad bi postojao još neki ireducibilan normiran polinom $P_1(x) \in \mathbb{Q}[X]$ takav da vrijedi $P_1(\alpha) = 0$, prema upravo dokazanom imamo $P_1(x) = P_\alpha(x)q(x)$. Nadalje, ireducibilnost od $P_1(x)$ povlači da je q polinom stupnja nula, odnosno konstantan polinom i to $q(x) = 1$ jer su $P_1(x)$ i $P_\alpha(x)$ normirani polinomi.

□

Definicija 3.1.3. *Polinom $P_\alpha(x)$ opisan u teoremu 3.1.2 naziva se* minimalni polinom algebarskog broja α. Stupanj algebarskog broja α *je stupanj njegova minimalnog polinoma $P_\alpha(x)$.*

Definicija 3.1.4. *Za algebarski broj α kažemo da je* algebarski cijeli broj *ako njegov minimalni polinom ima cjelobrojne koeficijente, tj. $P_\alpha(x) \in \mathbb{Z}[X]$.*

Teorem 3.1.5 (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*

$$\left|\alpha - \frac{x}{y}\right| > \frac{c(\alpha)}{y^d}. \tag{3.1}$$

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

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

Razvojem polinoma $P(x)$ u Taylorov red oko α dobivamo

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

pri čemu smo koristili da je $P(\alpha) = 0$. Nadalje, možemo pretpostaviti da vrijedi $\left|\alpha - \frac{x}{y}\right| \leq 1$ jer je u suprotnom nejednakost (3.1) zadovoljena. Tada vrijedi

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

Nejednakost (3.1) je ispunjena za konstantu $c(\alpha)$ definiranu relacijom

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

□

Korolar 3.1.6. *Broj $\alpha = \sum_{\nu=1}^{\infty} 5^{-\nu!}$ je transcendentan.*

Dokaz. Za $k \in \mathbb{N}$ definiramo prirodne brojeve

$$y(k) = 5^{k!},\ x(k) = 5^{k!} \sum_{\nu=1}^{k} 5^{-\nu!}.$$

Tada vrijedi

$$\alpha - \frac{x(k)}{y(k)} = \sum_{\nu=k+1}^{\infty} 5^{-\nu!} < 5^{-(k+1)!} + 5^{-(k+1)!-1} + 5^{-(k+1)!-2} + \dots$$

$$= \frac{5}{4} \cdot 5^{-(k+1)!} = \frac{5}{4y(k+1)}.$$

Kako za bilo koje prirodne brojeve c i $d \geq 2$ postoji dovoljno velik k za koji vrijedi

$$\frac{5}{4y(k+1)} < \frac{c}{y(k)^d},$$

odnosno

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

imamo kontradikciju s Liouvilleovim teoremom, što znači da α mora biti transcendentan broj. □

Liouville je bio prvi koji je pokazao postojanje transcendentnih brojeva i to baš na način opisan u korolaru 3.1.6. Nadalje, trivijalna posljedica Liouvilleova teorema je sljedeća tvrdnja.

Korolar 3.1.7. *Neka je α algebarski broj stupnja $d \geq 2$ i $\mu > d$. Tada nejednakost*

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^\mu} \tag{3.2}$$

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

Thue (1908.) je poboljšao ovaj rezultat, dokazavši da nejednakost (3.2) ima samo konačno mnogo rješenja ako je $\mu > d/2 + 1$. Siegel (1921.) je dokazao isti rezultat za $\mu > 2\sqrt{d}$, dok su Dyson (1947.) i Gelfond (1952.) dokazali istu tvrdnju za $\mu > \sqrt{2d}$. Godine 1955. Roth je dokazao isti rezultat za $\mu > 2$. Činjenica (lema 2.1.3) kako postoji beskonačno mnogo racionalnih brojeva $\frac{x}{y}$ takvih da vrijedi

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

pokazuje nam kako je Rothov rezultat najbolji mogući.

Teorem 3.1.8 (Roth)**.** *Ako je α algebarski broj i $\delta > 0$, onda postoji samo konačno mnogo racionalnih brojeva $\frac{x}{y}$ za koje vrijedi*

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

3.2 Simultane diofantske aproksimacije. Hipergeometrijska metoda

Kako smo vidjeli u prošlom odjeljku, ako 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

$$\left|\alpha - \frac{x}{y}\right| > \frac{c}{y^\kappa} \tag{3.3}$$

za sve racionalne brojeve $\frac{x}{y}$, $y > 0$. No dokaz Rothova teorema nije efektivan, odnosno ne daje metodu za eksplicitno određivanje konstante c. Ipak, za specijalne klase algebarskih brojeva postoje rezultati koji daju eksplicitne vrijednosti konstanti c i $\kappa < d$. Ovdje ćemo prikazati

jedan od takvih rezultata.

Za $n \in \mathbb{N}$ definiramo

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

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

Teorem 3.2.1 (Baker)**.** *Neka su $m, n \in \mathbb{N}$ takvi da vrijedi $n \geq 3$, $1 \leq m \leq n$. Nadalje, neka su $a, b \in \mathbb{N}$ takvi da vrijedi $7a/8 \leq b < a$ i $a \equiv b \pmod{n}$. Ako je*

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

onda $\alpha = \left(\frac{a}{b}\right)^{m/n}$ zadovoljava nejednakost (3.3) za sve racionalne brojeve $\frac{x}{y}$, $y > 0$, gdje su c i κ dani relacijama

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

Napomena 3.2.2. *Primijetimo da se uvjet $a \equiv b \pmod{n}$ može uvijek zadovoljiti tako da a i b pomnožimo s n, no to povećava vrijednosti konstanti κ i c^{-1}.*

Napomena 3.2.3. *S obzirom na Liouvilleov teorem, rezultat prethodnog teorema zanimljiv je samo ako je $\kappa \leq n$.*

Korolar 3.2.4. *Za sve racionalne brojeve $\frac{x}{y}$, $y > 0$, vrijedi*

$$\left|\sqrt[3]{2} - \frac{x}{y}\right| > \frac{4.06 \cdot 10^{-6}}{y^{2.48}}.$$

Dokaz. U oznakama teorema 3.2.1 za $n = 3$, $m = 1$, $a = 128$ i $b = 125$ imamo

$$\left(\frac{a}{b}\right)^{m/n} = \frac{4}{5}\sqrt[3]{2},\ \mu_3 = \sqrt{3},\ \lambda = \frac{500}{9\sqrt{3}} > 1.$$

Za konstante c i κ dobivamo vrijednosti

$$c \approx 0.000176659,\ \kappa \approx 2.48375,$$

pa prema teoremu 3.2.1 za sve racionalne brojeve $\frac{x}{y}$, $y > 0$, vrijedi nejednakost (3.3), odnosno

$$\left|\frac{4}{5}\sqrt[3]{2} - \frac{4x}{5y}\right| > \frac{0.000177}{(5y)^{2.484}},$$

što množenjem s $5/4$ upravo daje traženu nejednakost. □

Ocjena iz prethodnog korolara može se i poboljšati. Najbolji rezultat ovakvog tipa dobio je Bennett (1997.), koji je dokazao da za sve racionalne brojeve $\frac{x}{y}$, $y > 0$, vrijedi

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

Vezano uz probleme kojima ćemo se baviti pojavit će se potreba za „istovremenom" aproksimacijom algebarskih brojeva, odnosno potreba za tzv. *simultanim diofantskim aproksimacijama*. Jedan takav primjer jest rješavanje sustava Pellovih (odnosno općenito i pelovskih) jednadžbi kao što je

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

Ponekad ćemo sustave slične prethodnom nazivati sustavima *simultanih* pelovskih jednadžbi jer se u svakoj od jednadžbi pojavljuje točno jedna zajednička nepoznanica, y. U ovom konkretnom primjeru za rješenje sustava (x, y, z) trebalo bi vrijediti

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

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

Navedimo sada neke analogne rezultate iz običnih diofantskih aproksimacija, konkretno analogone Dirichletova i Rothova teorema.

Teorem 3.2.5 (Dirichlet)**.** *Neka su α_{ij}, $i = 1, \ldots, n$, $j = 1, \ldots, m$ realni brojevi, te neka je $Q > 1$ prirodan broj. Tada postoje cijeli brojevi $q_1, \ldots, q_m, p_1, \ldots, p_n$ takvi da vrijedi*

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

$$|\alpha_{i1}q_1 + \ldots + \alpha_{im}q_m - p_i| \leq \frac{1}{Q},\ i = 1, \ldots, n. \tag{3.4}$$

Dokaz. Neka je $y = (y_1, \ldots, y_m)$ uređena m-torka cijelih brojeva za koje vrijedi $0 \leq y_j < Q^{n/m}$ za $j = 1, \ldots, m$. Definiramo pripadnu točku

$$T(y) = (\{\alpha_{11}y_1 + \ldots + \alpha_{1m}y_m\}, \ldots, \{\alpha_{n1}y_1 + \ldots + \alpha_{nm}y_m\}),$$

pri čemu $\{\ \}$ označava razlomljeni dio broja. Kako je $\{a\} = a - \lfloor a \rfloor$ za svaki realan broj a, točku $T(y)$ možemo zapisati i kao

$$T(y) = (\alpha_{11}y_1 + \ldots + \alpha_{1m}y_m - x_1, \ldots, \alpha_{n1}y_1 + \ldots + \alpha_{nm}y_m - x_n),$$

za pripadni $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$. Odnosno, $T(y) = T(y, x)$ pri čemu je $x \in \mathbb{Z}_n$ određen s $y \in \mathbb{Z}^m$.

Očito je da točka $T(y, x)$ leži u jediničnoj kocki $I^n = [0, 1]^n$. Nadalje, jasno je da postoji barem barem Q^n takvih točaka (jer je $Q^{n/m} > 1$), pa zajedno s točkom $(1, \ldots, 1) \in I^n$ imamo barem $Q^n + 1$ točaka iz I^n. Podijelimo sada I^n na Q^n u parovima disjunktnih potkocaka čiji su bridovi duljine $1/Q$. Tada po Dirichletovu principu barem dvije od promatranih točaka pripadaju istoj potkocki. Neka su to točke $T(y, x)$ i $T(y', x')$, pri čemu $y \neq y'$. Lako se vidi da cijeli brojevi $q_1, \ldots, q_m, p_1, \ldots, p_n$ definirani s

$$(q_1, \ldots, q_m) = y - y' \neq 0,\ (p_1, \ldots, p_n) = x - x'$$

zadovoljavaju nejednakosti u (3.4). □

Korolar 3.2.6. *Neka je barem jedan od brojeva $\alpha_1, \alpha_2, \ldots, \alpha_n$ iracionalan. Tada postoji beskonačno mnogo n-torki racionalnih brojeva $\frac{p_1}{q}, \ldots, \frac{p_n}{q}$, $q > 0$, takvih da vrijedi*

$$\left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+\frac{1}{n}}}, \; i = 1, \ldots, n. \tag{3.5}$$

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

$$1 \leq q < Q^n, \; |\alpha_i q - p_i| \leq \frac{1}{Q}, \; i = 1, \ldots, n. \tag{3.6}$$

Napomenimo da uvjet $\gcd(p_1, \ldots, p_n, q) = 1$ uvijek možemo ispuniti. Jasno je da (3.6) povlači (3.5). Sada pretpostavimo da je npr. α_1 iracionalan. Tada je $|\alpha_1 q - p_1| \neq 0$, pa za fiksne $p_1, \ldots, p_n, q$, (3.6) može vrijediti samo ako je $Q \leq \frac{1}{|\alpha_1 q - p_1|}$. Ako sad pustimo $Q \to \infty$, dobivamo beskonačno mnogo različitih rješenja. □

Korolar 3.2.7. *Neka su realni brojevi $1, \alpha_1, \ldots, \alpha_m$ linearno nezavisni nad $\mathbb{Q}$. Tada postoji beskonačno mnogo $(m+1)$-torki cijelih relativno prostih brojeva $(q_1, \ldots, q_m, p)$ sa svojstvom*

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

Dokaz. Analogno kao dokaz korolara 3.2.6 jer $|\alpha_1 q_1 + \cdots + \alpha_n q_n - p| \neq 0$ za $q_1, \ldots, q_m, p \in \mathbb{Z}$. □

Sljedeća tvrdnja je analogon Rothova teorema 3.1.8.

Teorem 3.2.8. *Neka su $\alpha_1, \ldots, \alpha_n$ algebarski brojevi takvi da su $1, \alpha_1, \ldots, \alpha_n$ linearno nezavisni nad $\mathbb{Q}$, te $\delta > 0$. Tada postoji* konačno *mnogo n-torki racionalnih brojeva $(\frac{p_1}{q}, \ldots, \frac{p_n}{q})$, $q > 0$, takvih da vrijedi*

$$\left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+\frac{1}{n}+\delta}}, \; i = 1, \ldots, n. \tag{3.7}$$

Za dokaz teorema 3.2.8 ćemo koristiti poznati *Schmidtov teorem o potprostorima* iz 1972. ([54]). Funkcija oblika

$$L(x) = L(x_1, \ldots, x_n) = \alpha_1 x_1 + \cdots + \alpha_n x_n$$

naziva se *linearna forma* s koeficijentima α_i, $i = 1, \ldots, n$. Skup linearnih formi $\{L_1, \ldots, L_n\}$ je linearno nezavisan skup ako je linearno nezavisan nad algebarskim poljem koeficijenta linearnih formi.

Teorem 3.2.9 (Schmidt)**.** *Neka je dano n linearno nezavisnih linearnih formi $L_1, \ldots, L_n$ u n varijabli s algebarskim koeficijentima, te neka je $\delta > 0$. Tada sve cjelobrojne točke $x = (x_1, \ldots, x_n)$ koje zadovoljavaju*

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

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

Dokaz teorema 3.2.8. Množenjem nejednakosti iz (3.7) te množenjem s q^{n+1} dobivamo

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

za neki $\delta' > 0$. Želimo pokazati da prethodnu nejednakost može zadovoljavati samo konačno mnogo n-torki $(\frac{p_1}{q}, \ldots, \frac{p_n}{q})$.

Za $x = (p_1, \ldots, p_n, q)$ definiramo linearne forme

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

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

Tada za dovoljno veliki q vrijedi

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

Prema Schmidtovu teoremu 3.2.9 vrijedi da cjelobrojna rješenja prethodne nejednadžbe leže u konačno mnogo pravih potprostora od $\mathbb{Q}^{n+1}$. Takvi potprostori presjeci su konačno hiperravnina oblika

$$c_1 x_1 + \ldots + c_{n+1} x_{n+1} = 0,\ c_1, \ldots, c_n \in \mathbb{Q},\ \sum_{i=1}^{n} |c_i| > 0.$$

Dakle, svako rješenje $(p_1, \ldots, p_n, q)$ nejednakosti (3.7) leži u nekom od potprostora od $\mathbb{Q}^{n+1}$, odnosno u nekoj hiperravnini. Pretpostavimo da je

$$c_1 p_1 + \ldots + c_n p_n + c_{n+1} q = 0,$$

odnosno ekvivalentno

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

Definirajmo sada $\gamma = |c_1\alpha_1 + \ldots + c_n\alpha_n + c_{n+1}|$. Tada je $\gamma > 0$ zbog linearne nezavisnosti od $1, \alpha_1, \ldots, \alpha_n$. Za dani potprostor γ je fiksan i vrijedi

$$\gamma \cdot q \leq |c_1||\alpha_1 q - p_1| + \ldots + |c_1||\alpha_1 q - p_1| \leq |c_1| + \ldots + |c_n|.$$

Znači, za dani potprostor q je omeđen, pa samo konačno mnogo q-ova, a onda i n-torki $\frac{p_1}{q}, \ldots, \frac{p_n}{q}$ zadovoljava (3.7), a kako potprostora ima samo konačno mnogo, tvrdnja korolara je dokazana. □

Kao i kod Rothova teorema, taj rezultat je neefektivan, u smislu da ne daje eksplicitnu gornju ogradu za veličinu q-ova koji zadovoljavaju (3.7). Ipak, postoje i neki efektivni rezultati tog tipa za specijalne klase algebarskih brojeva. Mi ćemo spomenuti Bennettov teorem iz [7] koji se može koristiti kod rješavanja simultanih pelovskih jednadžbi.

Teorem 3.2.10 (Bennett, 1998.)**.** *Neka su a_i, p_i, q i N cijeli brojevi za $i = 0, 1, 2$, 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*

$$M = \max\{|a_0|, |a_1|, |a_2|\}.$$

Tada vrijedi

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

gdje je

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

i

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

3.3 Baker-Davenportova redukcija

U ovom odjeljku ćemo iskazati tvrdnju, poznatu pod nazivom Baker-Davenportova redukcija, koju ćemo često koristiti kod smanjivanja gornje ograde za veličinu rješenja diofantskih jednadžbi. Praktičnu verzija redukcije iz [22] koju ćemo primjenjivati dajemo je u sljedećoj lemi:

Lema 3.3.1. *Neka su κ, μ realni brojevi i $N \in \mathbb{N}$. 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 $s\ ||.||$ označena udaljenost do najbližeg cijelog broja. Ako je $\varepsilon > 0$, onda za $A > 0$, $B > 1$ nejednadžba*

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

nema rješenja u prirodnim brojevima m i n takvima da vrijedi

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

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

$$0 < n(\kappa q - p) + np - mq + \mu q < qAB^{-n},$$

odnosno

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

što dalje povlači

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

□

Napomena 3.3.2. *Uvjet $q > 6N$ u lemi 3.3.1 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 i nova ograda bila manja. Iz svojstva konvergenti znamo da vrijedi $||\kappa q|| < 1/q$, dok o $||\mu q||$ općenito ne znamo ništa. Zato je razumno uzeti $q > 2N$, a uvjet $q > 6N$ pokazao se kao eksperimentalno dobar izbor.*

Napomena 3.3.3. *Ako uvjet $\varepsilon > 0$ nije zadovoljen, onda možemo pokušati uzeti sljedeću konvergentu i provjeriti hoće li taj uvjet biti zadovoljen.*

Poglavlje 4

Linearne forme u logaritmima

U ovom poglavlju opisat ćemo glavne rezultate iz Bakerove teorije linearnih formi u logaritmima algebarskih brojeva, što ćemo koristiti u rješavanju simultanih Pellovih, odnosno pelovskih jednadžbi, ali i nekih drugih diofantskih problema.

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

Taj problem su 1934. godine neovisno riješili Gelfond i Scheider. Njihov teorem kaže da ako su $\alpha_1, \alpha_2 \neq 0$ algebarski brojevi takvi da su $\log \alpha_1$ i $\log \alpha_2$ linearno nezavisni nad $\mathbb{Q}$, onda je

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

za sve algebarske brojeve β_1 i β_2. Osim što su pokazali da je taj izraz različit od nule, Gelfond je 1935. dobio i donju ogradu za 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 $\kappa > 5$. (Oznaka $\gg$ znači da postoji dovoljno velika konstanta $C > 0$ takva da je $\log |\Lambda| > -Ch(\Lambda)\kappa$). Sam Gelfond je četrdesetih godina prošlog stoljeća primijetio da bi poopćenje ovakvih rezultata na linearne forme u više logaritama omogućilo rješavanje mnogih problema iz teorije brojeva.

To poopćenje je 1966. napravio engleski matematičar Alan Baker. On je dokazao da ako su $\alpha_1, \ldots, \alpha_n$ nenul algebarski brojevi takvi da su $\log \alpha_1, \ldots, \log \alpha_n$ linearno nezavisni nad $\mathbb{Q}$, onda su $1, \log \alpha_1, \ldots, \log \alpha_n$ linearno nezavisni nad poljem algebarskih brojeva. Također, Baker je dobio i efektivan rezultat u obliku donje ograde za apsolutnu vrijednost linearne forme u logaritmima algebarskih brojeva, poznat kao *Bakerov teorem*. Taj se teorem pokazao moćnim alatom u rješavanju različitih problema kao što je Gaussov problem klasa (za broj klasa jednak 1), dobivanje eksplicitne konstante u Liouvilleovu teoremu bolje od one koju je dobio sam Liouville, dobivanje efektivnih ograda za rješenja nekih diofantovih jednadžbi te algoritma za efektivno rješavanje Thueovih jednadžbi. Za svoj važan doprinos teoriji brojeva Baker je 1970. godine nagrađen Fieldsovom medaljom.

4.1 Pregled važnijih teorema

U ovom odjeljku navest ćemo nekoliko teorema koji su varijante Bakerova teorema i primjenjuju se za rješavanje simultanih pelovskih jednadžbi. Najprije ćemo definirati neke standardne pojmove i oznake.

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

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

gdje su α_i, β_i, $i = 1, \ldots, n$ *kompleksni algebarski brojevi, a* log *označava glavnu vrijednost (granu) kompleksnog logaritma.*

Budući da nas zanima isključivo primjena za rješavanje diofantskih jednadžbi, bit će dovoljno pretpostaviti da su β_i cijeli brojevi, a označavat ćemo ih s $b_1, \ldots, b_n$.

Neka je K polje algebarskih brojeva stupnja D. Neka su nadalje $\alpha_1, \ldots, \alpha_n \neq 0$ elementi od K, a $b_1, \ldots, b_n \in \mathbb{Z}$. Definirajmo

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

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 kad $|x|$ teži u 0, naš problem svodi se na nalaženje donje ograde linearne forme u logaritmima

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

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 0 ako i samo ako je i druga), bit će korisno koristiti obje forme.

Definicija 4.1.2. *Neka je K polje algebarskih brojeva stupnja D i neka je $\alpha \in K^*$ algebarski broj stupnja d pri čemu $d|D$. Neka je nadalje $\sum_{k=0}^{d} a_k X^k$ njegov minimalan primitivni*[1] *polinom iz $\mathbb{Z}[X]$.* Apsolutnu logaritamsku visinu, $h(\alpha)$, *algebarskog broja α definiramo kao*

$$h(\alpha) = \frac{1}{d}\left(\log|a_d| + \sum_{i=1}^{d} \max\{\log|\alpha_i'|, 0\}\right), \tag{4.1}$$

gdje su α_i', $i = 1, \ldots, d$, konjugati od α. Ponekad se za $h(\alpha)$ još koristi naziv standardna logaritamska (Weilova) visina.

Ponekad koristimo i sljedeće *modificirane* visine:

$$h'(\alpha) = \max\{Dh(\alpha), \log|\alpha|, 0.16\},$$

odnosno

$$h''(\alpha) = \max\{h(\alpha), \frac{1}{D}|\log\alpha|, \frac{1}{D}\}.$$

Koristimo li gore navedene oznake i pretpostavke, vrijede sljedeći teoremi Matveeva:

[1] polinom s relativno prostim koeficijentima

Teorem 4.1.3 (Matveev, 2001.). *Pretpostavimo da vrijedi $\Lambda \neq 0$ te da su $A_1, \ldots, A_n$ realni brojevi za koje vrijedi $A_j \geq h'(\alpha_j)$, $j = 1, \ldots, n$. Tada je*

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

Nadalje, ako je K realno polje, vrijedi

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

Teorem 4.1.4 (Matveev, 2001.). *Pretpostavimo da vrijedi*

$$\Lambda = b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n \neq 0,$$

gdje su α_i algebarski brojevi, a b_i cjelobrojni koeficijenti, e $A_i \geq h'(\alpha_i)$ realni brojevi za $i = 1, \ldots, n$. Tada vrijedi

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

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

U nekim primjerima koristit ćemo i sljedeći teorem koji je slabija varijanta prethodnog teorema.

Teorem 4.1.5 (Baker-Wüstholz, 1993). *Pretpostavimo da vrijedi*

$$\Lambda = b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n \neq 0,$$

gdje su α_i algebarski brojevi, a b_i cjelobrojni koeficijenti za $i = 1, \ldots, n$. Tada vrijedi

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

gdje je D stupanj proširenja polja $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, $B = \max\{|b_1|, \ldots, |b_n|\}$.

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

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

gdje je

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

Uspoređujući ovo s teoremom 4.1.4, 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 ogradom

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

U toj ocjeni ovisnost o D i svakom $h(\alpha_j)$ bolja je nego u spomenutim teoremima, ali je u njima ovisnost o B logaritamska. To je najveća razlika i zato ta elementarna ocjena nema primjenu na diofantske jednadžbe.

4.2 Primjer

U ovom odjeljku pokazat ćemo kako se pomoću rezultata iz Bakerove teorije linearnih formi u logaritmima algebarskih brojeva, konkretno pomoću teorema 4.1.3, mogu riješiti neki zanimljivi problemi iz teorije brojeva. Konkretno, primjenit ćemo spomenutu teoriju da bismo pokazali sljedeću tvrdnju.

Tvdnja. *Jedini Fibonaccijev broj s više od jedne znamenke koji u dekadskom zapisu ima sve znamenke jednake jest* $F_{10} = 55$.

Niz Fibonaccijevih brojeva ili *Fibonaccijev niz* zasigurno je najpoznatiji niz u teoriji brojeva i matematici općenito. Obično ga se definira rekurzivno kao

$$F_1 = 1,\ F_2 = 1,\ F_n = F_{n-1} + F_{n-2},\ n > 2.$$

Pretpostavimo da Fibonaccijev broj F_n ima u dekadskom zapisu sve znamenke jednake. Stoga postoji $m \in \mathbb{N}$ za koji vrijedi

$$F_n = \overline{dd\cdots d} = d \cdot 10^{m-1} + d \cdot 10^{m-2} + \ldots + d = d\frac{10^m - 1}{10 - 1}.$$

To znači da se naš problem svodi na rješavanje diofantske jednadžbe

$$F_n = d\frac{10^m - 1}{10 - 1} \tag{4.2}$$

u nepoznanicama n i m.

Lako se provjeri da je za $1 \leq n \leq 1000$ jedini Fibonaccijev broj koji u dekadskom zapisu ima sve znamenke jednake samo F_{10}. Zato pretpostavimo da je $n > 1000$.

Rješavanjem rekurzije za Fibbonaccijev niz dobili bismo da je

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}},\ n \geq 1,$$

pri čemu je

$$\alpha = \frac{1 + \sqrt{5}}{2},\ \beta = \frac{1 - \sqrt{5}}{2}.$$

Broj $\alpha \approx 1.618$ poznat je pod nazivom *zlatni rez*. Vrijedi $\beta = -\alpha^{-1}$. Uz ove oznake jednadžbu (4.2) možemo zapisati

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

Zbog $n > 1000$ vrijedi ocjena

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

Nadalje, indukcijom po n se pokaže da za sve $n \geq 3$ vrijedi

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

Tada imamo

$$\alpha^{n-2} < F_n < 10^m$$

što povlači

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

i

$$10^{m-1} < F_n < \alpha^{n-1}. \tag{4.4}$$

Otuda je

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

pa zaključujemo

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

gdje je $c = (\log 10)/(\log \alpha) \approx 4.78497$. 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 (4.3) zaključujemo da vrijedi

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

odnosno

$$\log |\Lambda^*| < -(n-2) \log \alpha. \tag{4.5}$$

S druge strane, donju ogradu za $\log |\Lambda^*|$ možemo dobiti iz teorema 4.1.3. Označimo

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

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

Nadalje, primijetimo da je $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\sqrt{5})$ pa u notaciji teorema imamo $D = 2$ i $B = n$. Također, minimalni polinom od α_1 nad $\mathbb{Z}$ je djelitelj od

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

Tada vrijedi

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

Imamo i

$$h(\alpha_2) = \frac{1}{2}(\log \alpha + 0) < 0.25,$$

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

Tada za A_i-ove možemo uzeti

$$A_1 = 6.02,\ A_2 = 0.5,\ a_3 = 4.62.$$

Teorem 4.1.3 nam tada povlači

$$\log |\Lambda^*| > -1.4 \cdot 30^6 \cdot 4^{4.5} \cdot 4 \cdot 6.02 \cdot 0.5 \cdot 4.62(1 + \log 2)(1 + \log n).$$

Ako to usporedimo s gornjom ogradom (4.5) i malo sredimo, dobivamo

$$n - 2 < 1.023 \cdot 10^{14}(1 + \log n),$$

što povlači $n < 4 \cdot 10^{15}$.

Sada nam ostaje još reducirati ovu ogradu. To ćemo napraviti Baker-Davenportovom redukcijom, lema 3.3.1. Ona govori o rješivosti nejednadžbe oblika $0 < n\kappa - m + \mu < A \cdot B^{-n}$, u prirodnim brojevima m i n, pa stoga naš problem najprije treba svesti na nejednadžbu tog oblika. Primijetimo 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 da vrijedi

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

što možemo zapisati kao

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

Kako je

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

imamo

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

odnosno

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

To nam daje

$$0 < m\left(\frac{\log\alpha_3}{\log\alpha_2}\right) - n + \frac{\log\alpha_1}{\log\alpha_2} < \frac{9}{10^m}, \tag{4.6}$$

što je upravo nejednakost kakvu želimo. Sada možemo primijeniti Baker-Davenportovu redukciju 3.3.1uz zamijenjene parametre m i n, $\kappa = \log\alpha_3/\log\alpha_2$, $\mu = \log\alpha_1/\log\alpha_2$, $A = 9$, $B = 10$ te $N = 4 \cdot 10^{15}$, za svaki $d = 1, 2, \ldots, 9$. Već nakon jedne primjene leme 3.3.1 dobivamo da (4.6) nema rješenja za $20 \leq m \leq 4 \cdot 10^{15}$, za svaki $d \in \{1, 2, \ldots, 9\}$. To nam daje novu gornju ogradu $m \leq 20$ pa iz (4.2) slijedi $n \leq 97$, a to je u kontradikciji s pretpostavkom $n > 1000$.

Poglavlje 5

O proširenju Diofantove trojke

5.1 Diofantove m-torke

Definicija 5.1.1. Diofantova m-torka *je skup međusobno različitih prirodnih brojeva* $\{a_1, a_2, \ldots, a_m\}$ *za koji vrijedi da je umnožak bilo koja dva broja uvećan za 1 jednak punom kvadratu nekog prirodnog broja, odnosno*

$$a_i a_j + 1 = n_{ij}^2, \ n_{ij} \in \mathbb{N},$$

za sve $1 \leq i < j \leq m$

Prvi i najistaknutiji primjer Diofantove m-torke, odnosno specijalno Diofantove četvorke je skup $\{1, 3, 8, 120\}$ koji je pronašao Fermat. Često je nazivamo *Fermatovom četvorkom.* Euler je ustanovio da postoji beskonačno mnogo Diofantovih četvorki. Naime, ako su $a, b \in \mathbb{N}$ takvi da je $ab + 1 = r^2$ za neki $r \in \mathbb{N}$, onda je skup

$$\{a, b, a + b + 2r, 4r(r + a)(r + b)\}$$

Diofantova četvorka. Na primjer, za $a = k - 1$, $b = k + 1$, $k > 1$, dobivamo jednoparametarsku familiju Diofantovih četvorki

$$\{k - 1, k + 1, 4k, 16k^3 - 4k\}$$

koja poopćava Fermatovu četvorku $\{1, 3, 8, 120\}$. Još jedno zanimljivo poopćenje Fermatove četvorke jest familija

$$\{F_{2k}, F_{2k+2}, F_{2k+4}, 4F_{2k+1}F_{2k+2}F_{2k+3}\}, \ k \geq 1,$$

gdje je F_n n-ti Fibonaccijev broj. Iz ovoga je jasno da postoji beskonačno mnogo cjelobrojnih Diofantovih četvorki. Pitanje postojanja (cjelobrojne) Diofantove petorke bilo je dugi niz godina otvoreno, no slutilo se da takav skup ne postoji. Prije konačnog dokaza koji su nedavno dali He, Togbé i Ziegler u [47], mnogi autori su pokazali rezultate koji su išli u prilog slutnji o nepostojanju Diofantove petorke. Jedan od prvih radova vezanih uz tu tematiku bio je članak [4] Bakera i Davenporta iz 1969. koji su dokazali sljedeću tvrdnju:

Teorem 5.1.2. *Neka je* $d \in \mathbb{N}$ *takav da je* $\{1, 3, 8, d\}$ *Diofantova četvorka. Tada je* $d = 120$.

Prethodni teorem možemo „pročitati" i kao tvrdnju da se Fermatova četvorka $\{1, 3, 8, 120\}$ ne može proširiti do petorke. Stoga je prirodno proučiti problem *jedinstvenog proširenja* Diofantove trojke do Diofantove četvorke. Naime, svaka Diofantove trojka $\{a, b, c\}$ proširuje se elementom

$$d = a + b + c + 2abc + 2rst,$$

gdje je $ab+1=r^2$, $ac+1=s^2$, $bc+1=t^2$. Zaista, $ad+1=(at+rs)^2$, $bd+1=(bs+rt)^2$, $cd=(cr+st)^2$.

5.2 Proširenje Diofantove trojke $\{1,3,8\}$

U ovom odjeljku pokazat ćemo kako primjenom Bakerove teorije linearnih formi u logaritmima algebarskih brojeva, odnosno konkretno primjenom Baker-Wüstholzovog teorema 4.1.5 ili njemu sličnog, možemo dokazati teorem 5.1.2. Kao što smo već spomenuli, to su prvi učinili Baker i Davenport u [4]. S problemom ih je upoznao J.H. van Lint (u ožujku 1968.) koji je teorem 5.1.2 uspio dokazati za $d < 10^{1\,700\,000}$.

Pretpostavimo da je d prirodan broj takav da je $\{1,3,8,d\}$ Diofantova četvorka. Tada postoje $x,y,z \in \mathbb{N}$ takvi da je

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

Eliminacijom d iz prethodnih jednadžbi dobivamo sustav pelovskih jednadžbi

$$y^2-3x^2 = -2, \tag{5.1}$$
$$z^2-8x^2 = -7. \tag{5.2}$$

Problem nadopunjavanja Diofantove trojke $\{1,3,8\}$ stoga je ekvivalentan rješavanju sustava (5.1), (5.2). Uočimo da je jedno rješenje sustava očito $(1,1,1)$, no ono odgovara *nepravom* nadopunjenju $d=0$. Nadalje, rješenje $(11,19,31)$ odgovara nadopunjenju $d=120$. Želimo istražiti ima li sustav (5.1), (5.2) još rješenja. Za početak znamo da ima konačno mnogo rješenja, što slijedi prema sljedećem teoremu iz [55].

Teorem 5.2.1 (Siegel, 1926.)**.** *Neka je $f(x)$ polinom s cjelobrojnim koeficijentima koji ima barem tri različite nultočke u $\mathbb{C}$. Tada jednadžba*

$$y^2=f(x)$$

ima konačno mnogo rješenja u $\mathbb{Z}$.

Uz $t=yz$, množenjem (5.1) i (5.2) slijedi jednadžba

$$t^2=(3x^2-2)(8x^2-7)$$

koja prema teoremu 5.2.1 ima konačno mnogo cjelobrojnih rješenja i stoga je broj mogućih nadopunjenja skupa $\{1,3,8\}$ konačan.

Strategija rješavanja koju su Baker i Davenport dali u svom radu sastojala se od sljedećih koraka:

(i) Opisati skup svih rješenja jednadžbi (5.1), (5.2) pomoću nizova potencija kvadratnih iracionalnosti.

(ii) Dobiti nejednakost u kojoj se pojavljuje cjelobrojna linearna kombinacija logaritma tri algebarska broja, odnosno tzv. linearna forma u logaritmima algebarskih brojeva.

(iii) Pomoću Bakerovog rezultata koji daje donju ogradu za vrijednost linearne forme odrediti $X>0$ tako da sustav (5.1), (5.2) nema rješenja za $x>X$.

(iv) Reducirati gornju ogradu X pomoću metode opisane u odjeljku 3.3, a koja je izvorno upravo opisana u [4].

5.2.1 Rješenja jednadžbi

Prvo opišimo skup rješenja jednadžbe (5.1). Fundamentalno rješenje pripadne Pellove jednadžbe $y^2 - 3x^2 = 1$ je $(u, v) = (2, 1)$. Prema teoremu 2.5.2 vrijede sljedeće ocjene za fundamentalno rješenje (y^*, x^*) jednadžbe (5.1):

$$0 \leq x^* \leq \frac{v}{\sqrt{2(u+\varepsilon)}}\sqrt{|N|} = 1,$$

$$|y^*| \leq \sqrt{\frac{1}{2}(u+\varepsilon)|N|} = 1.$$

Stoga je $(y^*, x^*) \in \{(1,1), (-1,1)\}$. No, koristeći propoziciju 2.5.1 lako možemo ustanoviti da su ova dva fundamentalna rješenja asocirana, odosno pripadaju istoj klasi. Stoga je $(y^*, x^*) = (1,1)$ jedino fundamentalno rješenje jednadžbe (5.1), a sva rješenja (y, x) u skupu prirodnih brojeva dana su s

$$y + x\sqrt{3} = (1+\sqrt{3})(2+\sqrt{3})^m,\ m \geq 0. \tag{5.3}$$

Otuda je i

$$y - x\sqrt{3} = (1-\sqrt{3})(2-\sqrt{3})^m,\ m \geq 0. \tag{5.4}$$

Oduzimanjem relacija (5.3) i (5.4) dobivamo

$$2x\sqrt{3} = (1+\sqrt{3})(2+\sqrt{3})^m - (1-\sqrt{3})(2-\sqrt{3})^m,\ m \geq 0. \tag{5.5}$$

Uobičajeno je sva rješenja od (5.1) u x definirati pomoću niza $(v_m)_{m\geq 0}$:

$$v_m = \frac{1+\sqrt{3}}{2\sqrt{3}}(2+\sqrt{3})^m - \frac{1-\sqrt{3}}{2\sqrt{3}}(2+\sqrt{3})^{-m},\ m \geq 0,$$

pri čemu smo iskoristili da je $2 - \sqrt{3} = (2+\sqrt{3})^{-1}$.

Sada rješavamo jednadžbu (5.2). Fundamentalno rješenje pripadne Pellove jednadžbe $z^2 - 8x^2 = 1$ je $(u, v) = (3, 1)$. Za fundamentalno rješenje (z^*, x^*) jednadžbe (5.2) pomoću teorema 2.5.2 dobivamo ocjene

$$0 \leq x^* \leq \frac{\sqrt{7}}{2},\ |z^*| \leq \sqrt{7}.$$

Dakle, $(z^*, x^*) \in \{(1,1), (-1,1)\}$. Kako prema propoziciji 2.5.1 rješenja $(1,1)$ i $(-1,1)$ nisu asocirana, slijedi da su sva rješenja (z, x) od (5.2) u skupu prirodnih brojeva dana s

$$z + x\sqrt{8} = (\pm 1 + \sqrt{8})(3+\sqrt{8})^n,\ n \geq 0,$$

odnosno

$$2x\sqrt{8} = (\pm 1 + \sqrt{8})(3+\sqrt{8})^n - (\pm 1 - \sqrt{8})(3-\sqrt{8})^n,\ n \geq 0. \tag{5.6}$$

Kao i u prethodnom slučaju, sva rješenja od (5.2) u x zapisujemo pomoću nizova $(w_n)_{m\geq 0}$ i $(w'_n)_{m\geq 0}$:

$$w_n = \frac{1+\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^n - \frac{1-\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^{-n},\ n \geq 0,$$

$$w'_n = \frac{-1+\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^n - \frac{-1-\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^{-n},\ n \geq 0.$$

Odrediti x koji zadovoljava sustav jednadžbi (5.1) i (5.2) ekvivalentno je određivanju nenegativnih cijelih brojeva m i n za koje je $v_m = w_n$ ili $v_m = w'_n$, odnosno drugim riječima traženju presjeka nizova (v_m) i (w_n), odnosno (v_m) i (w'_n). Ti nizovi se sijeku za $m = n = 0$, $v_0 = w_0 = w'_0 = 1$, te za $m = n = 2$, $v_2 = w'_2 = 11$. Ti presjeci odgovaraju već spomenutim proširenjima Diofantove trojke $d = 0$ (nepravo) i $d = 120$. U onom što slijedi pokazat ćemo da su to jedini presjeci.

5.2.2 Primjena Bakerove teorije o linearnim formama u logaritmima

U [4] autori su koristili sljedeći rezultat iz [3] o ocjeni linearne forme u logaritmima algebarskih brojeva:

Teorem 5.2.2 (Baker, 1968.)**.** *Neka su $\alpha_1, \ldots, \alpha_k$ algebarski brojevi različiti od 0 stupnja manjeg ili jednakog d, visina manjih ili jednakih A, pri čemu je $d, A \geq 4$. Ako za neke $b_1, \ldots, b_k \in \mathbb{Q}$ vrijedi*

$$0 < |b_1 \log \alpha_+ \cdots + |b_k \log \alpha_k| < e^{-\delta H},$$

gdje su $0 < \delta \leq 1$ i $H = \max\{|b_1|, \ldots, |b_k|\}$, tada je

$$H < \left(4^{k^2} \delta^{-1} d^{2k} \log A\right)^{(2k+1)^2}.$$

Napominjemo da se u prethodnom teoremu pod pojmom *visine* algebarskog broja misli na tzv. *naivnu visinu* koja se računa kao maksimum apsolutnih vrijednosti koeficijenata minimalnog polinoma.

Pretpostavimo da je $v_m = w_n$ za neke $m, n \geq 2$, tj.

$$\frac{1+\sqrt{3}}{\sqrt{3}}(2+\sqrt{3})^m - \frac{1-\sqrt{3}}{\sqrt{3}}(2+\sqrt{3})^{-m} = \frac{1+\sqrt{8}}{\sqrt{8}}(3+\sqrt{8})^n - \frac{1-\sqrt{8}}{\sqrt{8}}(3+\sqrt{8})^{-n} = 2x. \quad (5.7)$$

Uz supstitucije

$$P = \frac{1+\sqrt{3}}{\sqrt{3}}(2+\sqrt{3})^m, \; Q = \frac{1+\sqrt{8}}{\sqrt{8}}(3+\sqrt{8})^n,$$

relacija (5.7) glasi

$$P + \frac{2}{3}P^{-1} = Q + \frac{7}{8}Q^{-1}.$$

Iz nejednakosti

$$P - Q = \frac{7}{8}Q^{-1} - \frac{2}{3}P^{-1} > \frac{2}{3}(Q^{-1} - P^{-1}) = \frac{2}{3}(P-Q)Q^{-1}P^{-1}$$

slijedi da je $P > Q$, što povlači i $m \geq n$. Definiramo

$$\Lambda = \log \frac{P}{Q} = m \log(2+\sqrt{3}) - n \log(3+\sqrt{8}) + \log \frac{(1+\sqrt{3})\sqrt{8}}{(1+\sqrt{8})\sqrt{3}}.$$

Λ je linearna forma u logaritmima algebarskih brojeva

$$\alpha_1 = 2+\sqrt{3}, \; \alpha_2 = 3+\sqrt{8}, \; \alpha_3 = \frac{(1+\sqrt{3})\sqrt{8}}{(1+\sqrt{8})\sqrt{3}},$$

te očito vrijedi $\Lambda > 0$ jer $P/Q > 1$. Ako pokažemo da je $\Lambda < e^{-m}$, Bakerov teorem 5.2.2 implicira postojanje $M > 0$ takvog da je $m < M$.

Vrijedi

$$P - Q = \frac{7}{8}Q^{-1} - \frac{2}{3}P^{-1} = \frac{7}{8}(P - \frac{7}{8})^{-1} - \frac{2}{3}P^{-1} < \frac{1}{4}P^{-1},$$

jer $Q > P - \frac{7}{8}Q^{-1} > P - \frac{7}{8}$ i $P > 80$ za $m \geq 3$. Otuda je

$$0 < \Lambda = \log\frac{P}{Q} = -\log\left(1 - \frac{P-Q}{P}\right) < \frac{1}{4}P^{-2} + \left(\frac{1}{4}P^{-2}\right)^2 < 0.26P^{-2},$$

pri čemu je u prethodnoj nejednakosti korišteno da je

$$-\log(1-x) < x + x^2,$$

za $|x| < 0.5$. Nadalje je

$$\Lambda < 0.26\left(\frac{1+\sqrt{3}}{\sqrt{3}}\right)^{-2}(7+4\sqrt{3})^{-m} < 13^{-m} < e^{-m}. \tag{5.8}$$

Budući da želimo izračunati gornju ogradu za m pomoću teorema 5.2.2, trebamo odrediti minimalne polinome algebarskih brojeva α_i, $i = 1, 2, 3$. Oni su redom

$$\begin{aligned} p_1(t) &= t^2 - 4t + 1, \\ p_2(t) &= t^2 - 6t + 1, \\ p_3(t) &= 441t^4 - 2016t^3 + 2880t^2 - 1536t + 256. \end{aligned}$$

Algebarski brojevi α_1 i α_2 su stupnja 2, a α_3 je stupnja 4, pa uzimamo $d = 4$. Nadalje, gornja ograda za visine je $A = 2880$. Stoga zaključujemo da, ako je $v_m = w_n$, onda

$$n \leq m < 10^{487},$$

prema ocjeni iz teorema 5.2.2, pri čemu je $H = \max\{b_1 = m, |b_2| = n, b_3 = 1\} = m$.

Za usporedbu primijenit ćemo i *jaču* varijantu teorema 5.2.2, Baker-Wüstholzov teorem 4.1.5. U oznakama tog teorema b_i, α_i, $i = 1, 2, 3$, su kao i do sada. Kako je $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha_3)$, slijedi $D = 4$. Izračunajmo standardne logaritamske (Weilove) visine algebarskih brojeva prema formuli

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

pri čemu je a_d vodeći koeficijent minimalnog polinoma od α, d stupanj od α, a $\alpha^{(i)}$ nultočke minimalnog polinoma od α (odnosno konjugati od α). Dobivamo redom

$$\begin{aligned} h(\alpha_1) &= \frac{1}{2}\log\alpha_1 < 0.66, \\ h(\alpha_2) &= \frac{1}{2}\log\alpha_2 < 0.89, \\ h(\alpha_3) &= \frac{1}{4}\log(441\alpha_3\alpha_3') < 1.88, \end{aligned}$$

gdje je $\alpha_3' = \frac{4}{21}(\sqrt{3(2+\sqrt{3})} - 2(3+\sqrt{3})) > 1$ (a ostale dvije nultočke od p_3 su manje od 1 po apsolutnoj vrijednosti). Modificirane visine računaju se kao

$$h''(\alpha) = \max\{h(\alpha), \frac{1}{D}|\log\alpha|, \frac{1}{D}\},$$

pa vidimo da je $h''(\alpha_i) = h(\alpha_i)$, $i = 1, 2, 3$. Sada ocjena iz teorema 4.1.5 glasi

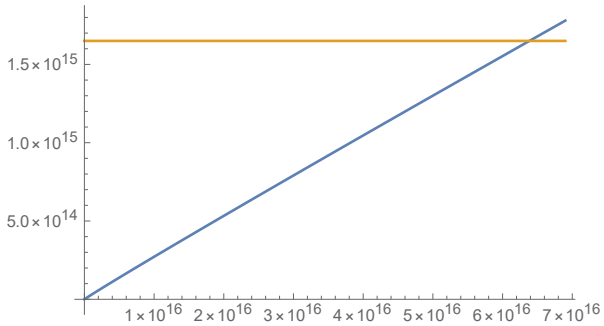
$$\log\Lambda > -18(3+1)!3^{3+1}(32\cdot 4)^{3+2}\log(2\cdot 3\cdot 4)0.66\cdot 0.89\cdot 1.88\log m > -4.22\cdot 10^{15}\log m,$$

pa uspoređujući s (5.8) imamo

$$-m\log 13 > -4.22\cdot 10^{15}\log m,$$

odnosno

$$\frac{m}{\log m} < 1.65\cdot 10^{15}.$$



Slika 5.1: $x \mapsto \frac{x}{\log x}$, $x \mapsto 1.65\cdot 10^{15}$

Budući da je $m \mapsto \frac{m}{\log m}$ rastuća funkcija, prethodna nejednakost ne vrijedi za dovoljno velike m. Konkretno za

$$m > 6.4\cdot 10^{16}, \tag{5.9}$$

dobit ćemo kontradikciju s (5.9). Dakle, ako je $v_m = w_n$, onda

$$n \le m < 6.4\cdot 10^{16},$$

što je značajno bolja ocjena za indekse m i n od ocjene koju daje teorem 5.2.2.

5.2.3 Primjena Baker-Davenportove metode redukcije

U prethodnom dijelu pokazali smo da je $\Lambda < 13^{-m}$ i $m < M$ gdje je $M = 6.4\cdot 10^{16}$. Dijeljenjem nejednakosti

$$0 < m\log\alpha_1 - n\log\alpha_2 + \log\alpha_3 < 13^{-m}.$$

s $\log\alpha_2$ dobivamo

$$0 < m\frac{\log\alpha_1}{\log\alpha_2} - n + \frac{\log\alpha_3}{\log\alpha_2} < \frac{1}{\log\alpha_2}13^{-m}, \tag{5.10}$$

što upravo odgovara nejednakosti koja se pojavljuje u lemi 3.3.1. Uz

$$\kappa = \frac{\log\alpha_1}{\log\alpha_2},\ \mu = \frac{\log\alpha_3}{\log\alpha_2},\ A = \frac{1}{\log\alpha_2},\ B = 13,$$

lema 3.3.1 povlači da nejednakost 5.10 nema rješenja u prirodnim brojevima m i n takvima da vrijedi

$$\frac{\log\left(\frac{Aq}{\varepsilon}\right)}{\log B} \leq m \leq M, \tag{5.11}$$

gdje je $\frac{p}{q}$ konvergenta razvoja u verižni razlomak broja κ takva da vrijedi $q > 6M$, te $\varepsilon = ||\mu q|| - M \cdot ||\kappa q|| > 0$.

Prva konvergenta koja zadovoljava uvjet $q > 6M$ je 36. konvergenta, no $\varepsilon < 0$ pa nisu ispunjeni svi uvjeti leme. Sljedeća, 37. konvergenta ispunjava oba uvjeta,

$$q = 3\,075\,296\,607\,888\,933\,649 > 6M,\ \varepsilon \approx 0.295,$$

pa je prema (5.11) *novi* $M = 16$. Sedma konvergenta, $q = 518$, ispunjava uvjete leme za $M = 16$ ($\varepsilon \approx 0.0262$) pa je nova granica spuštena na samo $M = 4$.

Analogan postupak opisan u odjeljcima 5.2.2 i 5.2.3 provodi se i za jednadžbu $v_m = w'_n$, $m, n \geq 2$, nakon čega je dokaz teorema 5.1.2 konačno priveden kraju.

5.3 Proširenje familije Diofantovih trojki $\{k-1, k+1, 4k\}$

Možemo pretpostaviti da je $k > 2$ jer je slučaj $k = 2$ riješen u prethodnom odjeljku. Nadalje, pretpostavimo da je $\{k-1, k+1, 4k, d\}$ Diofantova četvorka, odnosno da postoje $x, y, z \in \mathbb{N}$ takvi da je

$$(k-1)d + 1 = x^2,\ (k+1)d + 1 = y^2,\ 4kd + 1 = z^2,$$

što je ekvivalentno sustavu

$$(k-1)y^2 - (k+1)x^2 = -2, \tag{5.12}$$
$$(k-1)z^2 - 4kx^2 = -3k - 1. \tag{5.13}$$

Problem proširenja ove parametarske familije riješio je A. Dujella u [15], odnosno pokazao da vrijedi sljedeći teorem.

Teorem 5.3.1. *Neka je $k > 2$, te $d \in \mathbb{N}$ takav da je $\{k-1, k+1, 4k, d\}$ Diofantova četvorka. Tada je $d = 16k^3 - 4k$.*

Mi ćemo najprije pokušati riješiti problem analogno kao za slučaj $k = 2$, tj. pomoću Bakerove teorije o formama u logaritmima algebarskih brojeva, no tim pristupom nećemo moći u potpunosti dokazati 5.3.1. U [15] je Dujella koristio Rickertov rezultat o simultanim racionalnim aproksimacijama brojeva $\sqrt{(k-1)/k}$ i $\sqrt{(k+1)/k}$ te ćemo opisati i tu metodu.

5.3.1 Rješenja jednadžbi

Jednadžbu (5.12) napišimo u obliku pelovske jednadžbe

$$y'^2 - (k^2-1)x^2 = -2(k-1), \tag{5.14}$$

gdje je $y' = (k-1)y$. Fundamentalno rješenje pripadne Pellove jednadžbe $y'^2 - (k^2-1)x^2 = 1$ je $(u, v) = (k, 1)$. Za fundamentalno rješenje $((k-1)y^*, x^*)$ jednadžbe (5.14) prema teoremu 2.5.2 vrijede sljedeće ocjene:

$$0 \leq x^* \leq 1,\ |(k-1)y^*| \leq k-1,$$

pa je $(y^*, x^*) \in \{(1,1),(-1,1)\}$. Kako su $(1,1)$ i $(-1,1)$ asocirana rješenja, slijedi da je $(y^*, x^*) = (1,1)$ jedino fundamentalno rješenje jednadžbe (5.12) pa su sva rješenja u x dana s

$$2x\sqrt{k^2-1} = (k-1+\sqrt{k^2-1})(k+\sqrt{k^2-1})^m - (k-1-\sqrt{k^2-1})(k+\sqrt{k^2-1})^{-m},\ m \geq 0.$$

Dijeljenjem prethodne relacije s $\sqrt{k-1}$ imamo

$$2x\sqrt{k+1} = (\sqrt{k-1}+\sqrt{k+1})(k+\sqrt{k^2-1})^m - (\sqrt{k-1}-\sqrt{k+1})(k+\sqrt{k^2-1})^{-m}, \quad (5.15)$$

za $m \geq 0$. Skup rješenja jednadžbe (5.12) u nepoznanici x obično označavamo, kao i u prethodnom slučaju, kao niz (v_m):

$$v_m = \frac{\sqrt{k-1}+\sqrt{k+1}}{2\sqrt{k+1}}(k+\sqrt{k^2-1})^m + \frac{\sqrt{k+1}-\sqrt{k-1}}{2\sqrt{k+1}}(k+\sqrt{k^2-1})^{-m}, m \geq 0. \quad (5.16)$$

Odredimo sada rješenja pelovske jednadžbe

$$z'^2 - 4k(k-1)x^2 = -(3k+1)(k-1), \quad (5.17)$$

gdje je $z' = (k-1)z$. Fundamentalno rješenje pripadne Pellove jednadžbe $z'^2 - 4k(k-1)x^2 = 1$ je $(u,v) = (2k-1,1)$. Fundamentalno rješenje $((k-1)z^*, x^*)$ jednadžbe (5.17) zadovoljava nejednakosti:

$$0 \leq x^* \leq \frac{1}{2}\sqrt{3k+1} < \sqrt{k},\ |(k-1)z^*| \leq (k-1)\sqrt{3k+1},$$

odnosno $|z^*| \leq \sqrt{3k+1}$. Kako je

$$-4k(x^*)^2 \equiv -3k-1 \pmod{(k-1)},$$

odnosno $(x^*)^2 \equiv 1 \pmod{(k-1)}$, slijedi da je

$$(x^*)^2 = (k-1)t + 1 < k,$$

pa je $t = 0$ i $x^* = 1$. Stoga imamo dva fundamentalna rješenja od (5.13), $(z^*, x^*) = (1,1)$ i $(-1,1)$, a skup svih rješenja u nepoznanici x dan je nizovima (w_n) i (w'_n):

$$w_n = \frac{\sqrt{k-1}+2\sqrt{k}}{4\sqrt{k}}(2k-1+2\sqrt{k^2-k})^n + \frac{2\sqrt{k}-\sqrt{k-1}}{4\sqrt{k}}(2k-1+2\sqrt{k^2-k})^{-n}, n \geq 0, \quad (5.18)$$

$$w'_n = \frac{-\sqrt{k-1}+2\sqrt{k}}{4\sqrt{k}}(2k-1+2\sqrt{k^2-k})^n + \frac{2\sqrt{k}+\sqrt{k-1}}{4\sqrt{k}}(2k-1+2\sqrt{k^2-k})^{-n}, n \geq 0. \quad (5.19)$$

Očito se oba niza mogu objediniti pomoću $(w_n)_{n\in\mathbb{Z}}$.

Nizovi (v_m), (w_n) i (w'_n) zadovoljavaju sljedeće rekurzije:

$$v_0 = 1,\ v_1 = 2k-1,\ v_{m+2} = 2kv_{m+1} - v_m,\ m \geq 0, \quad (5.20)$$

$$w_0 = 1,\ w_1 = 3k-2,\ w_{n+2} = (4k-2)w_{n+1} - w_n,\ n \geq 0, \quad (5.21)$$

$$w'_0 = 1,\ w'_1 = k,\ w'_{n+2} = (4k-2)w_{n+1} - w_n,\ n \geq 0. \quad (5.22)$$

Nizovi (v_m) i (w_n), odnosno (v_m) i (w'_n), sijeku se za $n = m = 0$ i $n = m = 2$, tj. $v_0 = w_0 = w'_0 = 1$, $v_2 = w'_2 = 4k^2 - 2k - 1$ (ili $v_2 = w_{-2}$), što rezultira nepravim proširenjem Diofantove trojke, $d = 0$, te proširenjem $d = 16k^3 - 4k$, respektivno.

5.3.2 Metoda kongruencije

Ova jednostavna metoda omogućit će nam da iz pretpostavke $v_m = w_n$ zaključimo nešto o barem jednom od indeksa m ili n.

Promatramo nizove (v_m), (w_n) i (w'_n) modulo $2k-1$:

$$(v_m \mod (2k-1)) = (1, 0, -1, -1, 0, 1, 1, 0, -1, -1, \ldots);$$

$$(w_n \mod (2k-1)) = (1, -k, -1, k, 1, -k, -1, k, 1, -k, \ldots);$$

$$(w'_n \mod (2k-1)) = (1, k, -1, -k, 1, k, -1, -k, 1, k, \ldots).$$

Principom matematičke indukcije pokazuje se da je

$$v_m \mod (2k-1) \in \{-1, 0, 1\},\ |w_{2l} \mod (2k-1)| = 1,\ |w_{2l+1} \mod (2k-1)| > 1,$$

za sve $m \geq 0$, $l \in \mathbb{Z}$. Otuda slijedi: ako $v_m = w_n$ za neke $m \geq 0$ i $n \in \mathbb{Z}$, onda je indeks n paran, tj. $n = 2l$.

Sada pogledajmo (v_m), (w_n) i (w'_n) modulo $4k(k-1)$:

$$(v_m \mod 4k(k-1)) = (1, -1+2k, -1+2k, 1, 1, -1+2k, -1+2k, 1, 1, -1+2k, \ldots);$$

$$(w_{2l} \mod 4k(k-1)) = (1, 3-2k, 5-4k, 7-6k, 9-8k, 11-10k, 13-12k, 15-14k);$$

$$(w'_{2l} \mod 4k(k-1)) = (1, -1+2k, -3+4k, -5+6k, -7+8k, -9+10k, -11+12k, -13+14k, \ldots).$$

Indukcijom bi se dokazalo da je

$$v_m \mod 4k(k-1) \in \{1, 2k-1\},\ w_{2l} \mod (2k-1) = (2l+1) - 2lk,$$

za sve $m \geq 0$, $l \in \mathbb{Z}$. Zato iz $v_m = w_{2l}$ proizlaze dvije mogućnosti:

(i) $2l + 1 - 2lk \equiv 1 \pmod{4k(k-1)}$,
$2l(k-1) \equiv 0 \pmod{4k(k-1)}$,
$2l \equiv 0 \pmod{4k}$;

(ii) $2l + 1 - 2lk \equiv 2k - 1 \pmod{4k(k-1)}$,
$(2l+2)(k-1) \equiv 0 \pmod{4k(k-1)}$,
$2l \equiv -2 \pmod{4k}$.

Na temelju prethodnog zaključujemo sljedeću tvrdnju.

Lema 5.3.2. *Ako je $v_m = w_n$ za neke $m \geq 0$ i $n \in \mathbb{Z}$, onda je $n \equiv 0$ ili $-2 \pmod{4k}$.*

Za posljedicu prethodne leme imat ćemo: ako je $(m, n) \in \mathbb{N}_0 \times \mathbb{Z}$ rješenje jednadžbe $v_m = w_n$ i $(m, n) \notin \{(0, 0), (2, -2)\}$, onda je $|n| > 4k - 2$.

5.3.3 Primjena Bakerove teorije o linearnim formama u logaritmima

Izjednačavanjem $2v_m = 2w_n$ iz (5.16) i (5.18) za neke $m, n \geq 3$ dobivamo

$$\frac{\sqrt{k-1}+\sqrt{k+1}}{\sqrt{k+1}}(k+\sqrt{k^2-1})^m + \frac{\sqrt{k+1}-\sqrt{k-1}}{\sqrt{k+1}}(k+\sqrt{k^2-1})^{-m} =$$

$$\frac{\sqrt{k-1}+2\sqrt{k}}{2\sqrt{k}}(2k-1+2\sqrt{k^2-k})^n + \frac{2\sqrt{k}-\sqrt{k-1}}{2\sqrt{k}}(2k-1+2\sqrt{k^2-k})^{-n},$$

što uz supstituciju

$$P = \frac{\sqrt{k-1}+\sqrt{k+1}}{\sqrt{k+1}}(k+\sqrt{k^2-1})^m,\ Q = \frac{\sqrt{k-1}+2\sqrt{k}}{2\sqrt{k}}(2k-1+2\sqrt{k^2-k})^n,$$

prelazi u

$$P + \frac{2}{k+1}P^{-1} = Q + \frac{3k+1}{4k}Q^{-1}.$$

Iz nejednakosti

$$P - Q = \frac{3k+1}{4k}Q^{-1} - \frac{2}{k+1}P^{-1} > \frac{2}{k+1}(Q^{-1}-P^{-1}) = \frac{2}{k+1}(P-Q)P^{-1}Q^{-1}$$

zaključujemo da je $P > Q$, te uz manju manipulaciju i da je $m > n$. S druge strane,

$$P - Q = \frac{3k+1}{4k}Q^{-1} - \frac{2}{k+1}P^{-1} < \frac{3k+1}{4k}(P-\frac{3k+1}{4k})^{-1} - \frac{2}{k+1}P^{-1},$$

jer je $Q > P - \frac{3k+1}{4k}Q^{-1} > P - \frac{3k+1}{4k}$. Otuda je

$$P - Q < \frac{3}{4}P^{-1}.$$

Definiramo linearnu formu

$$\Lambda = \log\frac{P}{Q} = m\log\alpha_1 - n\log\alpha_2 + \log\alpha_3,$$

gdje je

$$\alpha_1 = k+\sqrt{k^2-1},\ \alpha_2 = 2k-1+2\sqrt{k^2-k},\ \alpha_3 = \frac{2(\sqrt{k-1}+\sqrt{k+1})\sqrt{k}}{(\sqrt{k-1}+2\sqrt{k})\sqrt{k+1}}.$$

Zbog $0 < P - Q < \frac{3}{4}P^{-1}$ vrijedi

$$0 < \Lambda < -\log(1-\frac{P-Q}{P}) < \frac{3}{4}P^{-2} + (\frac{3}{4}P^{-2})^2 < \frac{4}{5}P^{-2},$$

odnosno

$$0 < \Lambda < \frac{4}{5}\frac{k+1}{2k+\sqrt{k^2-1}}(k+\sqrt{k^2-1})^{-2m} < e^{-2m\log(2k-1)}. \tag{5.23}$$

Sada ćemo primijeniti Baker-Wüstholzov teorem 4.1.5:

$$\log\Lambda > -18(3+1)!3^{3+1}(32D)^{3+2}\log(2\cdot 3\cdot D)h''(\alpha_1)h''(\alpha_2)h''(\alpha_3)\log B, \tag{5.24}$$

gdje je D stupanj algebarskog proširenja polja $\mathbb{Q}(\alpha_1\alpha_2, \alpha_3)$, $B = \max\{m, n, 1\} = m$, a $h''(\alpha) = \max\{h(\alpha), \frac{1}{D}|\log\alpha|, \frac{1}{D}\}$, te $h(\alpha)$ standardna visina dana u (4.1). Kako je

$$\alpha_3 = \frac{2}{3k^2+4k+1}\left(2k^2+2k+2k\sqrt{k^2-1}-(1+k)\sqrt{k^2-k}-(k-1)\sqrt{k^2+k}\right),$$

može se pokazati da je $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha_3)$.

Za određivanje navedenih veličina (D i $h''(\alpha_i)$) trebamo naći minimalne polinome algebarskih brojeva α_i. (Napomenimo da postoje slučajevi gdje možemo odrediti polinom sa cjelobrojnim koeficijentima p za koji je $p(\alpha) = 0$, ali ne možemo sa sigurnošću reći da je to baš minimalni polinom za sve vrijednosti parametra, tj. algebarski broj α poprima stupanj u ovisnosti o parametru k). Minimalni polinomi algebarskih brojeva α_1, α_2, α_3 su redom

$$\begin{aligned}
p_1(t) &= t^2 - 2kt + 1,\\
p_2(t) &= t^2 - 2(2k-1)t + 1,\\
p_3(t) &= (1+k)^2(1+3k)^2t^4 - 16k(1+k)^2(1+3k)t^3 + 48k^2(1+k)(3+k)t^2\\
&\quad -128k^2(1+k)t + 64k^2.
\end{aligned}$$

Najprije možemo zaključiti da je $D = 4$ jer je to stupanj od α_3 i $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha_3)$. Nadalje, nultočke od p_1 su α_1 i $\alpha_1' = k - \sqrt{k^2-1} \in \langle 0, 1\rangle$ pa je

$$h(\alpha_1) = \frac{1}{2}\log\alpha_1 \leq \frac{1}{2}\log(2k).$$

Analogno, nultočke od p_2 su α_2 i $\alpha_2' = 2k - 1 - 2\sqrt{k^2-k} \in \langle 0, 1\rangle$ pa je

$$h(\alpha_2) = \frac{1}{2}\log\alpha_2 \leq \frac{1}{2}\log(4k-2).$$

Uz nešto truda možemo odrediti i sve nultočke od p_3. To su α_3,

$$\alpha_3' = \frac{2(\sqrt{k-1}+\sqrt{k+1})\sqrt{k}}{(-\sqrt{k-1}+2\sqrt{k})\sqrt{k+1}},$$

$$\alpha_3'', \alpha_3''' = \frac{4k^2+4k(1-\sqrt{k^2-1}) \pm 2\sqrt{2k(k^2-1)(k-\sqrt{k^2-1})}}{1+4k+3k^2}.$$

Kako su $\alpha_3'', \alpha_3''' \in \langle 0, 1\rangle$, te $\alpha_3, \alpha_3' > 1$ slijedi

$$h(\alpha_3) = \frac{1}{4}\log\left((1+k)^2(1+3k)^2\alpha_3\alpha_3'\right) = \frac{1}{4}\log\left((1+k)^2(1+3k)^2\frac{8k(k+\sqrt{k^2-1})}{(k+1)(3k+1)}\right),$$

tj.

$$h(\alpha_3) \leq \frac{1}{4}\log\left(16k^2(k+1)(3k+1)\right).$$

Očito je $h''(\alpha_i) = h(\alpha_i)$ za sve $i = 1, 2, 3$. Kombinirajući (5.29) i (5.24) dobivamo

$$-2m\log(2k-1) > -2.4\cdot 10^{14}\log(2k)\log(4k-2)\log\left(16k^2(k+1)(3k+1)\right)\log m,$$

tj.

$$\frac{m}{\log m} < 1.2 \cdot 10^{14} \underbrace{\frac{\log(2k)\log(4k-2)\log\left(16k^2(k+1)(3k+1)\right)}{\log(2k-1)}}_{<20\log^2 k,\ \text{ za } k>3} < 2.4 \cdot 10^{15}\log^2 k. \tag{5.25}$$

Kako je $m \mapsto \frac{m}{\log m}$ rastuća funkcija, za dovoljno velik m dobit ćemo kontradikciju u prethodnoj nejednakosti, npr. sigurno za $m \geq 5.76 \cdot 10^{30}\log^4 k$. Stoga zaključujemo:

Propozicija 5.3.3. *Ako je $v_m = w_n$ za neke $n, m \geq 0$, onda je $m < 5.76 \cdot 10^{30}\log^4 k$.*

Još nam preostaje iskoristiti lemu 5.3.2. Pretpostavimo da je $v_m = w_n$ te $m \geq n > 2$. Tada je prema lemi 5.3.2 i propoziciji 5.3.3

$$\frac{4k-2}{\log^4 k} < 5.76 \cdot 10^{30}.$$

Ponovo koristimo argument da je $k \mapsto \frac{4k+2}{\log^4 k}$ rastuća funkcija, pa ćemo za dovoljno velik k, konkretno za $k \geq 8.4 \cdot 10^{37}$, dobiti kontradikciju s prethodnom nejednakosti.

Sada bismo trebali provesti račun za $2v_m = 2w'_n$ iz (5.16) i (5.19). Međutim, ovaj slučaj vodi na formu u logaritmima algebarskih brojeva α_1, α_2, α'_3 pa vrijede sve ocjene. Konačno možemo izreći sljedeću tvrdnju:

Teorem 5.3.4. *Neka je $k \geq 8.4 \cdot 10^{37}$. Ako je $d \in \mathbb{N}$ takav da je $\{k-1, k+1, 4k, d\}$ Diofantova četvorka, onda je $d = 16k^3 - 4k$.*

5.3.4 Primjena simultanih diofantskih aproksimacija

Bakerova teorija omogućila nam je da pokažemo da se Diofantova trojka $\{k-1, k+1, 4k\}$ jedinstveno nadopunjuje do Diofantove četvorke, osim za konačno mnogo k, $k < 8.4 \cdot 10^{37}$. No gornja ograda za k je prevelika da bismo tvrdnju efektivno mogli provjeriti. U ovom dijelu opisat ćemo primjenu simultanih racionalnih aproksimacija kvadratnih iracionalnosti o kojima je bilo riječ u 3.2, uz koje se može dobiti puno bolja gornja ograda parametra k. U tu svrhu koristit ćemo teorem Rickerta iz [53] pomoću kojeg je pokazano da sustav Pellovih jednadžbi

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

ima samo trivijalno rješenje.

Teorem 5.3.5 (Rickert, 1993.)**.** *Neka je $k \geq 2$, te*

$$\theta_1 = \sqrt{1 - \frac{1}{k}},\ \theta_2 = \sqrt{1 + \frac{1}{k}}. \tag{5.26}$$

Tada za sve $p_1, p_2, q \in \mathbb{Z}$, $q > 0$, vrijedi

$$\max\{\left|\theta_1 - \frac{p_1}{q}\right|, \left|\theta_2 - \frac{p_2}{q}\right|\} > (271k)^{-1}q^{-1-\lambda},$$

gdje je

$$\lambda = \lambda(k) = \frac{\log(12k\sqrt{3} + 24)}{\log(27(k^2-1)/32)}.$$

Umjesto sustava (5.12), (5.13), krećemo od njemu ekvivalentnog sustava

$$(k-1)z^2 - 4kx^2 = -3k-1, \tag{5.27}$$
$$(k+1)z^2 - 4ky^2 = -3k+1. \tag{5.28}$$

Uočimo da je

$$\left|\frac{k-1}{k} - \left(\frac{2x}{z}\right)^2\right| = \left|\sqrt{\frac{k-1}{k}} - \frac{2x}{z}\right| \cdot \left|\sqrt{\frac{k-1}{k}} + \frac{2x}{z}\right| = \frac{3k+1}{kz^2}, \tag{5.29}$$

te analogno

$$\left|\sqrt{\frac{k+1}{k}} - \frac{2y}{z}\right| \cdot \left|\sqrt{\frac{k+1}{k}} + \frac{2y}{z}\right| = \frac{3k-1}{kz^2},$$

pa očekujemo da su racionalni brojevi $2x/z$ i $2y/z$, pri čemu je (x,y,z) rješenje sustava (5.27), (5.28), dobre aproksimacije kvadratnih iracionalnosti $\sqrt{(k-1)/k}$ i $\sqrt{(k+1)/k}$. To ćemo i pokazati u sljedećoj lemi.

Lema 5.3.6. *Neka je $k \geq 2$, θ_1 i θ_2 dani s* (5.26)*, te $(x,y,z) \in \mathbb{N}^3$ rješenje sustava jednadžbi* (5.27) *i* (5.28)*. Tada je*

$$\max\{|\theta_1 - \frac{2x}{z}|, |\theta_2 - \frac{2y}{z}|\} < 2.5z^{-2}.$$

Dokaz. Iz (5.29) je

$$\left|\sqrt{\frac{k-1}{k}} - \frac{2x}{z}\right| = \frac{3k+1}{kz^2}\left|\sqrt{\frac{k-1}{k}} + \frac{2x}{z}\right|^{-1},$$

a kako je $4kx^2 = (k-1)z^2 + 3k + 1 > (k-1)z^2$, odnosno $\frac{2x}{z} > \sqrt{\frac{k-1}{k}}$ te $\sqrt{\frac{k-1}{k}} + \frac{2x}{z} > 2\sqrt{\frac{k-1}{k}} > \sqrt{2}$, dobivamo

$$\left|\sqrt{\frac{k-1}{k}} - \frac{2x}{z}\right| < \frac{3k+1}{k\sqrt{2}}z^{-2} < \frac{7}{2\sqrt{2}}z^{-2} < 2.475z^{-2}.$$

Slično,

$$\left|\sqrt{\frac{k+1}{k}} - \frac{2y}{z}\right| = \frac{3k-1}{kz^2}\left|\sqrt{\frac{k+1}{k}} + \frac{2y}{z}\right|^{-1} < \frac{3k-1}{kz^2}\left(2\sqrt{\frac{k+1}{k}}\right)^{-1} < \frac{3k-1}{2k}z^{-2} < 1.5z^{-2}.$$

□

Prema ocjeni iz Rickertova teorema 5.3.5 za $(p_1, p_2, q) = (2x, 2y, z)$ dobivamo

$$2.475z^{-2} > \max\{|\theta_1 - \frac{2x}{z}|, |\theta_2 - \frac{2y}{z}|\} > (271k)^{-1}z^{-1-\lambda},$$

tj.

$$\log(670.5k) > (1-\lambda)\log z,$$

gdje je

$$1 - \lambda = 1 - \lambda(k) = 1 - \frac{\log(12k\sqrt{3}+24)}{\log(27(k^2-1)/32)}.$$

Funkcija $k \mapsto 1 - \lambda(k)$ je rastuća i za $k \geq 29$ je $1 - \lambda(k) > 0.01873$. Stoga je

$$\log z < 53.4\log(670.5k).$$

Lema 5.3.7. *Neka je* $(x, y, z) \in \mathbb{N}^3$ *rješenje sustava jednadžbi* (5.27), (5.28) *i* $z \notin \{1, 8k^2 - 1\}$. *Tada je*

$$\log z \geq (4k-2)\log(4k-3).$$

Dokaz. U odjeljku 5.3.1 pokazali smo da je $x = w_n$ ili $x = w'_n$ za neki $n \geq 3$, gdje su nizovi (w_n) i (w'_n) dani rekurzijama (5.21) i (5.22). Otuda slijedi da je pripadni $z = s_n$ ili $z = s'_n$ gdje su nizovi (s_n) i (s'_n) dani rekurzijama

$$s_0 = 1,\ s_1 = 2k+1,\ s_{n+2} = (4k-2)s_{n+1} - s_n,\ n \geq 0,$$

$$s'_0 = 1,\ s'_1 = 6k-1,\ s'_{n+2} = (4k-2)s'_{n+1} - s'_n,\ n \geq 0.$$

Lako možemo ustanoviti da su nizovi (s_n) i (s'_n) rastući, pa je stoga

$$s_n = (4k-2)s_{n-1} - s_{n-2} > (4k-2)s_{n-1} - s_{n-1} > (4k-3)s_{n-1} > (4k-3)^n,$$

te analogno $s'_n > (4k-3)^n$. Dakle,

$$\log z > n\log(4k-3).$$

No prema lemi 5.3.2 je $n > 4k-2$ (jer je $n \neq 0$) pa slijedi tražena nejednakost. □

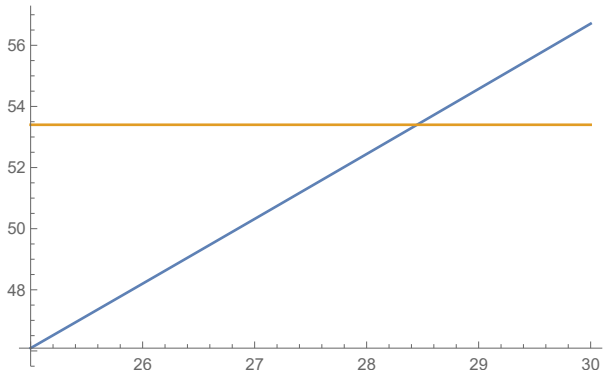
Dakle, za $k \geq 29$ treba vrijediti

$$(4k-2)\frac{\log(4k-3)}{\log(670.5k)} < 53.4,$$

no s druge strane

$$f(k) = (4k-2)\frac{\log(4k-3)}{\log(670.5k)}$$

je rastuća funkcija (za $k \geq 2$) i $f(29) > 54.5$, što je u kontradikciji s prethodnom nejednakosti.



Slika 5.2: $x \mapsto (4x-2)\frac{log(4x-3)}{\log 670.5x}$, $x \mapsto 53.4 \cdot 10^{15}$

Uočimo da smo primjenom Rickertova teorema dobili znatno bolji rezultat nego primjenom Bakerove teorije.

Teorem 5.3.8. *Neka je* $k \geq 29$. *Ako je* $d \in \mathbb{N}$ *takav da je* $\{k-1, k+1, 4k, d\}$ *Diofantova četvorka, onda je* $d = 16k^3 - 4k$.

5.3.5 Slučajevi $3 \leq k \leq 28$

Još nam preostaje riješiti konačno mnogo slučajeva za $3 \leq k \leq 28$. Pokazat ćemo da se oni mogu učinkovito riješiti pomoću Bakerove teorije te ćemo iskoristiti račun iz odjeljka 5.3.3. Budući da je $k \leq 28$, iz nejednakosti (5.25) dobivamo

$$\frac{m}{\log m} < 2.7 \cdot 10^{16}.$$

Kontradikciju u prethodnoj nejednakosti dobivamo za $m \geq 1.2 \cdot 10^{18}$. Sada nam predstoji provesti Baker-Davenportovu metodu redukcije za svaki $k = 3, 4, \ldots, 28$, redom. Prema (5.23) vrijedi

$$0 < \Lambda = m \log \alpha_1 - n \log \alpha_2 + \log \alpha_3 < (2k-1)^{-2m},$$
$$0 < m\frac{\log \alpha_1}{\log \alpha_2} - n + \frac{\log \alpha_3}{\log \alpha_2} < \frac{1}{\log \alpha_2}(4k^2 - 4k + 1)^{-m}. \tag{5.30}$$

Uz

$$\kappa = \frac{\log \alpha_1}{\log \alpha_2},\ \mu = \frac{\log \alpha_3}{\log \alpha_2},\ A = \frac{1}{\log \alpha_2},\ B = 4k^2 - 4k + 1,$$

lema 3.3.1 povlači da nejednakost (5.30) nema rješenja u prirodnim brojevima m i n takvima da vrijedi

$$M_1 \leq m \leq M, \tag{5.31}$$

gdje su $M_1 = \log\left(\frac{Aq}{\varepsilon}\right) / \log B$, $\frac{p}{q}$ konvergenta razvoja u verižni razlomak broja κ takva da vrijedi $q > 6M$, te $\varepsilon = ||\mu q|| - M \cdot ||\kappa q|| > 0$. U prvom koraku redukcije pokazuje se da 41. konvergenta od κ zadovoljava uvjete leme 3.3.1 za sve $3 \leq k \leq 28$, te dobivamo sljedeće vrijednosti za M_1:

k	3	4	5	6	7	...	15	16	17	...	25	26	27	28
M_1	14	12	11	10	9	...	7	7	7	...	6	6	6	6

U sljedećem koraku redukcije koji primijenimo za $M = 14$ dovoljna je 4. konvergenta od κ, za sve $3 \leq k \leq 28$ i imamo:

k	3	4	5	6	7	...	15	16	17	...	25	26	27	28
M_1	3	2	2	2	2	...	2	2	2	...	1	1	1	1

U slučaju jednadžbe $2v_m = 2w'_n$ dobivamo u prvom koraku redukcije iste vrijednosti kao u prethodnom slučaju, dok je u drugom koraku redukcije za $M = 14$ u više slučajeva bilo potrebno uzeti 9. konvergentu zbog $\varepsilon < 0$, te dobivamo sljedeće vrijednosti:

k	3	4	5	6	7	...	15	16	17	...	25	26	27	28
M_1	7	6	5	5	4	...	3	3	3	...	3	3	3	3

5.4 Proširenje Diofantove trojke $\{a, b, c\}$ i dokaz nepostojanja Diofantove petorke

U prethodnim odjeljcima pokazali smo kako se riješio problem proširenja Fermatove trojke $\{1, 3, 8\}$, te problem proširenja familije Diofantovih trojki $\{k-1, k+1, 4k\}$, $k \geq 3$. Ovdje ćemo

taj problem istražiti općenito za neku Diofantovu trojku $\{a, b, c\}$, pri čemu su a, b, c prirodni brojevi i $a < b < c$. Nadalje, u ovom odsječku prezentirat ćemo rezultate Dujelle [23, 25] gdje je dokazano nepostojanje Diofantove šestorke te da je broj petorki konačan. Na kraju odsječka dat ćemo pregled metoda i ideja koje su dovele do dokaza slutnje o nepostojanju Diofantove petorke.

Označimo s $r, s, t \in \mathbb{N}$ takve da je

$$ab + 1 = r^2,\ ac + 1 = s^2,\ bc + 1 = t^2. \tag{5.32}$$

Već smo na početku poglavlja spomenuli da se svaka Diofantova trojka $\{a, b, c\}$ može nadopuniti elementom

$$d = d_+ = a + b + c + 2abc + 2rst,$$

gdje su r, s, t dani u (5.32). Diofantovu četvorku $\{a, b, c, d_+\}$ nazivamo *regularnom* ili *Eulerovom četvorkom*. Lako možemo vidjeti da se trojka može nadopuniti i elementom

$$d = d_- = a + b + c + 2abc - 2rst.$$

No za ovo nadopunjenje vrijedi $0 \leq d_- < c$ i $c = d_+(a, b, d_-)$. Nadalje, $d_- = 0$ ako i samo ako vrijedi $c = a + b + 2r$.

U vezi nadopunjenja elementom d, odnosno nadopunjenja Diofantove trojke do četvorke, postavljene su sljedeće slutnje.

Slutnja 5.4.1. *Ako je $\{a, b, c, d\}$ Diofantova četvorka, onda je $d \in \{d_-, d_+\}$.*

Slutnja 5.4.2. *Ako je $\{a, b, c, d\}$ Diofantova četvorka takva da je $a < b < c < d$, onda je $d = d_+$.*

Ako bi se slutnja 5.4.2 pokazala točnom, tada bismo za posljedicu imali da ne postoji Diofantova petorka. Kao što smo već napomenuli, tvrdnja o nepostojanju Diofantove petorke i sama je niz godina bila poznata kao *slutnja o Diofantovoj petorci*, no nedavno je dokazana ([47]).

Teorem 5.4.3 (He, Togbé, Ziegler, 2019.)**.** *Ne postoji Diofantova petorka.*

U onom što slijedi istaknut ćemo neke bitne činjenice koje su omogućile dokaz ove važne tvrdnje (teorem 5.4.3), a koje su usko vezane uz problem proširenja općenite Diofantove trojke.

Propozicija 5.4.4. *Neka je $\{a, b, c\}$ Diofantova trojka takva da je $a < b < c$. Tada je*

$$c = a + b + 2r \quad \textit{ili} \quad c \geq 4ab + a + b > 4b,$$

pri čemu je r dan u (5.32)*. U svakom slučaju vrijedi $c > 4r > 4a$.*

Dokaz. Dokaz se može naći u [49], iako treba napomenuti da autor nije koristio notaciju i terminologiju vezanu uz Diofantove m-torke kojom se koristimo ovdje, a koja je standardna već dugi niz godina. □

Diofantovu trojku $\{a, b, a + b + 2r\}$ nazivamo *regularnom* ili *Eulerovom trojkom*.

Problem proširenja Diofantove trojke $\{a, b, c\}$ do Diofantove četvorke $\{a, b, c, d\}$ vodi na rješavanje sustava

$$ad + 1 = x^2,\ bd + 1 = y^2,\ cd + 1 = z^2, \tag{5.33}$$

u nepoznanicama $d, x, y, z \in \mathbb{N}$. Eliminacijom nepoznanice d može se pokazati da je sustav (5.33) ekvivalentan sustavu jednadžbi pelovskog tipa

$$az^2 - cx^2 = a - c, \tag{5.34}$$
$$bz^2 - cy^2 = b - c. \tag{5.35}$$

Rješenje jednadžbe (5.34) zapisivat ćemo često kao $z\sqrt{a} + x\sqrt{c}$, odnosno kao element polja $\mathbb{Q}(\sqrt{a}, \sqrt{c})$, a rješenje jednadžbe (5.35) kao $z\sqrt{b}+y\sqrt{c}$, što je element polja $\mathbb{Q}(\sqrt{b}, \sqrt{c})$. Pokazuje se da je takav zapis od praktične koristi, što smo imali prilike vidjeti u prethodnim odsječcima 5.2, 5.3.

5.4.1 Rekurzivni nizovi

Lema 5.4.5. *Postoje $i_0, j_0 \in \mathbb{N}$ i $z_0^{(i)}, x_0^{(i)}, z_1^{(j)}, y_1^{(j)} \in \mathbb{Z}$ za $i = 1, \ldots, i_0$, $j = 1, \ldots, j_0$ sa svojstvima:*

(i) $(z_0^{(i)}, x_0^{(i)})$ $(z_1^{(j)}, y_1^{(j)})$ su rješenja od (5.34), (5.35), respektivno;

(ii)

$$\begin{aligned}
1 \leq \quad & x_0^{(i)} \quad \leq \sqrt{\frac{a(c-a)}{2(s-1)}} < \sqrt{\frac{s+1}{2}}, \\
1 \leq \quad & |z_0^{(i)}| \quad \leq \sqrt{\frac{(s-1)(c-a)}{2a}} < \sqrt{\frac{c\sqrt{c}}{2\sqrt{a}}}, \\
1 \leq \quad & y_1^{(j)} \quad \leq \sqrt{\frac{b(c-b)}{2(t-1)}} < \sqrt{\frac{t+1}{2}}, \\
1 \leq \quad & |z_1^{(j)}| \quad \leq \sqrt{\frac{(t-1)(c-b)}{2b}} < \sqrt{\frac{c\sqrt{c}}{2\sqrt{b}}},
\end{aligned}$$

za $s, t \in \mathbb{N}$ dane u (5.32);

(ii) ako su (z, x) (z, y) rješenja u prirodnim brojevima od (5.34), (5.35), tada postoje $i \in \{1, \ldots, i_0\}$, $j \in \{1, \ldots, j_0\}$, $m, n \in \mathbb{Z}$, $m, n \geq 0$ takvi da vrijedi

$$\begin{aligned}
z\sqrt{a} + x\sqrt{c} &= (z_0^{(i)}\sqrt{a} + x_0^{(i)}\sqrt{c})(s + \sqrt{ac})^m, \\
z\sqrt{b} + y\sqrt{c} &= (z_1^{(j)}\sqrt{b} + y_1^{(j)}\sqrt{c})(t + \sqrt{bc})^n.
\end{aligned}$$

Dokaz. Jasno je da je dovoljno dokazati tvrdnje samo za prvu jednadžbu (5.34). Neka je (z, x) rješenje od (5.34) u prirodnim brojevima. Promotrimo sve parove (z^*, x^*) cijelih brojeva danih s

$$z^*\sqrt{a} + x^*\sqrt{c} = (z\sqrt{a} + x\sqrt{c})(s + \sqrt{ac})^m,\ m \in \mathbb{Z}.$$

Lako se vidi da (z^*, x^*) zadovoljava (5.34) te da je x^* prirodan broj. Sada iz svih takvih parova (z^*, x^*) izaberimo onaj gdje je x^* minimalan i označimo taj par s (z_0, x_0). Definirajmo cijele brojeve z' i x' sa

$$z'\sqrt{a} + x'\sqrt{c} = (z_0\sqrt{a} + x_0\sqrt{c})(s - \varepsilon\sqrt{ac}),$$

gdje je $\varepsilon = 1$, ako je $z_0 > 0$, a $\varepsilon = -1$ ako je $z_0 < 0$. Iz minimalnosti od x_0 zaključujemo

$$x' = sx_0 - \varepsilon a z_0 \geq x_0,$$

što povlači

$$a|z_0| \leq (s-1)x_0,$$

odnosno

$$acx_0^2 + a(a-c) \leq (ac + 2 - 2s)x_0^2.$$

Na kraju zaključujemo

$$x_0^2 \leq \frac{a(c-a)}{2(s-1)}.$$

Sada iz toga dobivamo i

$$z_0^2 = \frac{1}{a}(cx_0^2 + a - c) \leq \frac{1}{a}\left(\frac{ac(c-a)}{2(s-1)} + a - c\right) = \frac{(s-1)(c-a)}{2a}.$$

Upravo smo dokazali da postoji rješenje (z_0, x_0) jednadžbe (5.34) koje zadovoljava tražene ocjene i $m \in \mathbb{Z}$ tako da vrijedi

$$z\sqrt{a} + x\sqrt{c} = (z_0\sqrt{a} + x_0\sqrt{c})(s + \sqrt{ac})^m.$$

Ostaje pokazati da je $m \geq 0$. Pretpostavimo suprotno, odnosno da je $m < 0$. Tada vrijedi

$$(s + \sqrt{ac})^m = \alpha - \beta\sqrt{ac},$$

gdje su α i β prirodni brojevi koji zadovoljavaju $\alpha^2 - ac\beta^2 = 1$. Sada imamo $z = \alpha z_0 - \beta c x_0$ i iz uvjeta $z > 0$ dobivamo

$$z_0^2 > \beta^2 c(c-a) \geq c(c-a),$$

što je očito u kontradikciji s ocjenom za $|z_0|$. □

Rješenja $(z_0^{(i)}, x_0^{(i)})$, $(z_1^{(j)}, y_1^{(j)})$ za $i = 1, \ldots, i_0$, $j = 1, \ldots, j_0$ nazivamo *fundamentalnim rješenjima* jednadžbi (5.34) i (5.35). Iz prethodne Leme odmah slijedi:

Propozicija 5.4.6. *Neka je $(x, y, z) \in \mathbb{Z}^3$ rješenje sustava (5.34), (5.35). Tada postoje $i \in \{1, \ldots, i_0\}$, $j \in \{1, \ldots, j_0\}$, $m, n \in \mathbb{Z}$, $m, n \geq 0$ takvi da je*

$$z = v_m^{(i)} = w_n^{(j)},$$

gdje su $(v_m^{(i)})$ i $(w_n^{(j)})$ nizovi zadani rekurzijama

$$v_0^{(i)} = z_0^{(i)}, \quad v_1^{(i)} = sz_0^{(i)} + cx_0^{(i)}, \quad v_{m+2}^{(i)} = 2sv_{m+1}^{(i)} - v_m^{(i)}, \ m \geq 0; \tag{5.36}$$

$$w_0^{(j)} = z_1^{(j)}, \quad w_1^{(j)} = tz_1^{(j)} + cy_1^{(j)}, \quad w_{n+2}^{(j)} = 2tw_{n+1}^{(j)} - w_n^{(j)}, \ n \geq 0. \tag{5.37}$$

Zbog jednostavnosti odsad nadalje ćemo izostavljati indekse (i) i (j). Spomenimo da uvijek postoje fundamentalna rješenja jednadžbi (5.34) i (5.35) koja će nam dati proširenje naše Diofantove trojke do četvorke s elementom d.

Očito je da su

$$(z_0, x_0) = (\pm 1, 1), \ (z_1, y_1) = (\pm 1, 1)$$

fundamentalna rješenja jednadžbi (5.34) i (5.35) koja daju

$$z = v_0 = w_0 = \pm 1,$$

odnosno trivijalna rješenja sustava (5.34), (5.35). Ovo rješenje sustava odgovara *nepravom* proširenju Diofantove trojke $d = 0$.

Nadalje, fundamentalna rješenja

$$(z_0, x_0) = (\pm t, r),\ (z_1, y_1) = (\pm s, r)$$

impliciraju

$$z = v_1 = w_1 = cr \pm st,$$

rješenja sustava (5.34), (5.35) koja odgovaraju proširenjima Diofantove trojke s elementom

$$d = \frac{z^2 - 1}{c} = d_{\pm}.$$

Mi želimo pokazati da su to jedina rješenja sustava jednadžbi (5.34) i (5.35) koja će voditi na proširenje trojke do četvorke s prirodnim brojem.

Lema 5.4.7. *Za $m, n \geq 0$ vrijedi*

$$v_{2m} \equiv z_0 \pmod{2c},\ v_{2m+1} \equiv sz_0 + cx_0 \pmod{2c},$$

$$w_{2n} \equiv z_1 \pmod{2c},\ w_{2n+1} \equiv tz_1 + cy_1 \pmod{2c},$$

gdje su (v_m) i (w_n) dani rekurzijama (5.36) i (5.37).

Dokaz. Primjenom principa matematičke indukcije. □

Nadalje, zanimaju nas samo ona rješenja sustava jednadžbi (5.34) i (5.35) koja će nam dati proširenje trojke takvo da je $d = (z^2 - 1)/c \in \mathbb{Z}$. Kako indukcijom možemo dokazati

$$v_m^2 \equiv z_0^2 \pmod{c},\ w_n^2 \equiv z_1^2 \pmod{c},$$

iz $z = v_m = w_n$ vidimo da nas zanimaju samo ona fundamentalna rješenja za koja vrijedi

$$z_0^2 \equiv z_1^2 \equiv 1 \pmod{c}.$$

Spomenimo ovdje da iz rezultata u [49] slijedi da u slučaju $c = a + b + 2r$ imamo $z_0 = z_1 = \pm 1$.

Sljedeća lema daje nam neke informacije o fundamentalnim rješenjima u ovisnosti o parnosti indeksa u $v_m = w_n$.

Lema 5.4.8. *(i) Ako je $v_{2m} = w_{2n}$, onda je $z_0 = z_1$.*

(ii) Ako je $v_{2m+1} = w_{2n}$, onda je $z_0 z_1 < 0$ i $cx_0 - s|z_0| = |z_1|$.

(iii) Ako je $v_{2m} = w_{2n+1}$, onda je $z_0 z_1 < 0$ i $cy_1 - t|z_1| = |z_0|$.

(iv) Ako je $v_{2m+1} = w_{2n+1}$, onda je $z_0 z_1 > 0$ i $cx_0 - s|z_0| = cy_1 - t|z_1|$.

Dokaz. Dokazat ćemo prve dvije tvrdnje.

(i) Neka je $v_{2m} = w_{2n}$. Tada iz leme 5.4.7 imamo

$$z_0 \equiv z_1 \pmod{2c}$$

pa iz ocjena $|z_0|, |z_1| < c$ zaključujemo $z_0 = z_1$.

(ii) U slučaju da je $v_{2m+1} = w_{2n}$ iz leme 5.4.7 imamo

$$sz_0 + cx_0 \equiv z_1 \pmod{2c}.$$

Primijetimo da vrijedi

$$cx_0 - s|z_0| = \frac{c^2 - ac - z_0^2}{cx_0 + s|z_0|} < \frac{c^2 - s^2}{c + s} < c.$$

Nadalje iz $c > 4a$ i ocjene za $|z_0|$ dobivamo

$$0 < cx_0 - s|z_0| < c.$$

Sada možemo zaključiti, koristeći $|z_1| < c$, da ako je $z_0 > 0$, onda je $z_1 = sz_0 - cx_0$, a ako je $z_0 < 0$, onda je $z_1 = sz_0 + cx_0$.

□

5.4.2 Veza između indeksa m i n

U sljedećoj lemi iskazat ćemo vezu između indeksa m i n iz jednadžbe $v_m = w_n$. Za dokaz ćemo koristiti sljedeće ocjene za fundamentalna rješenja

$$1 \leq x_0 < 0.841\sqrt[4]{ac},\ 1 \leq |z_0| < 0.421c,$$

$$1 \leq y_1 < 0.783\sqrt[4]{bc},\ 1 \leq |z_1| < 0.32c,$$

koja se lako dobiju iz leme 5.4.5, kao i $a \geq 1$, $b \geq 3$, $c \geq 8$.

Lema 5.4.9. *Ako vrijedi $v_m = w_n$, onda je $n - 1 \leq m \leq 2n + 1$.*

Dokaz. Principom matematičke indukcije pokazuje se da za $m \geq 1$ vrijedi

$$v_1(2s - 1)^{m-1} \leq v_m \leq v_1(2s)^{2m-1}.$$

Ocijenimo sad v_1. Imamo

$$v_1 = sz_0 + cx_0 \geq cx_0 - s|z_0| = \frac{c^2 - ca - z_0^2}{cx_0 + s|z_0|} > \frac{c^2 - \frac{c^2}{4} - \frac{c\sqrt{c}}{2\sqrt{a}}}{2cx_0} > \frac{c}{4x_0} > \frac{c}{3.364\sqrt[4]{ac}}$$

i

$$v_1 < 2cx_0 < 1.682c\sqrt[4]{ac}.$$

Znači, za $m \geq 1$ vrijedi

$$\frac{c}{3.364\sqrt[4]{ac}}(2s - 1)^{m-1} < v_m < 1.682c\sqrt[4]{ac}(2s)^{m-1}.$$

Potpuno analogno za $n \geq 1$ dobivamo

$$\frac{c}{3.132\sqrt[4]{bc}}(2t-1)^{n-1} < w_n < 1.566c\sqrt[4]{bc}(2t)^{n-1}.$$

Sada $v_m = w_n$, za $m, n \geq 1$ povlači

$$(2s-1)^{m-1} < 5.269\sqrt[4]{abc^2}(2t)^{n-1}.$$

Kako je

$$2s - 1 = 2\sqrt{ac+1} - 1 > 1.767\sqrt{ac}$$

i

$$2t = 2\sqrt{bc+1} < 2.042\sqrt{bc},$$

zaključujemo

$$(2s-1)^2 > 3.12ac > 2t.$$

To nam daje

$$(2s-1)^{m-1} < 2.635 \cdot (2t)^n < (2t)^{n+0.43} < (2s-1)^{2n+0.86},$$

odnosno $m \leq 2n+1$. Slično iz

$$(2t-1)^{n-1} < 5.269\sqrt[4]{abc^2}(2s)^{m-1},$$

te iz $v_m = w_n$, za $m, n \geq 1$, dobivamo $n \leq m+1$.

Ostaje dokazati $v_0 < w_2$ i $w_0 < v_2$. Dokažimo prvu nejednakost. Vrijedi

$$w_2 = 2tw_1 - w_0 > \frac{2ct}{3.132\sqrt[4]{bc}} - \sqrt{\frac{c\sqrt{c}}{2\sqrt{b}}} > c\left(\frac{\sqrt[4]{bc}}{1.566} - \frac{1}{\sqrt{2\sqrt{bc}}}\right) > 1.093c > v_0.$$

□

Na isti način, ako je c dovoljno „velik" i ako imamo neku „rupu" između elemenata b i c, možemo dokazati sljedeći rezultat.

Lema 5.4.10. *Neka je $c > 10^{10}$ i neka vrijedi $v_m = w_n$ za $m, n \geq 2$.*

(i) Ako je $c > b^{4.5}$, onda vrijedi $m \leq \frac{11}{9}n + \frac{7}{9}$.

(ii) Ako je $c > b^{2.5}$, onda vrijedi $m \leq \frac{7}{5}n + \frac{3}{5}$.

(iii) Ako je $c > b^2$, onda vrijedi $m \leq \frac{3}{2}n + \frac{1}{2}$.

(iv) Ako je $c > b^{5/3}$, onda vrijedi $m \leq \frac{8}{5}n + \frac{3}{5}$.

5.4.3 Principi rupa

Sada ćemo prvo pokazati da jedina rješenja jednadžbi $z = v_m = w_n$ s malim indeksima vode na trivijalno (nepravo) proširenje trojke s elementom $d = 0$ ili na poširenje do regularne četvorke. To slijedi iz dokaza sljedeće leme.

Lema 5.4.11. *Neka je $v_m = w_n$ i $d = (v_m^2 - 1)/c$. Ako je $\{0, 1, 2\} \bigcap \{m, n\} \neq \emptyset$, onda je $d < c$ ili je $d = d_+$.*

Dokaz. Iz leme 5.4.9 slijedi da moramo provjeriti što se događa za

$$(m,n) \in \{(0,0),(0,1),(1,0),(1,1),(1,2),(2,1),(2,2),(3,1),(2,3),(3,2),(4,2),(5,2)\}.$$

Za ilustraciju ćemo dati dokaz za $(m,n) = (0,0)$ i $(m,n) = (1,2)$. Ideja dokaza za preostale slučajeve je slična, iako su neki od njih tehnički zahtjevniji.

Neka je $(m,n) = (0,0)$. Tada iz ocjena $|z_0|, |z_1| < c$ odmah dobivamo $d < c$.

Neka je sad $(m,n) = (1,2)$. Tada je $v_1 = sz_0 + cx_0$ i $w_2 = z_1 + 2c(bz_1 + ty_1)$. Koristeći lemu 5.4.8, ako je $z_1 > 0$, onda je $z_0 < 0$ i $cx_0 + sz_0 = z_1$. Tada je $w_2 > w_0 = v_1$, pa u ovom slučaju ne možemo imati jednakost $v_1 = w_2$.

Ako je pak $z_1 < 0$, $z_0 > 0$ i

$$cx_0 - sz_0 = -z_1.$$

Ako to uvrstimo u relaciju $v_1 = w_2$, dobivamo

$$bz_1 + ty_1 = x_0.$$

Iz toga, i koristeći da su (z_0, x_0) i (z_1, y_1) rješenja jednadžbi (5.34) i (5.35), dobivamo

$$(b-a)t^2 = z_0^2(b-a).$$

Iz toga nadalje zaključujemo $z_0 = t$, $x_0 = r$, $z_1 = st - cr$ i $y_1 = rt - bs$. To povlači $v_1 = st + cr$ i na kraju

$$d = \frac{(cr+st)^2 - 1}{c} = d_+.$$

□

Sada lako možemo dokazati sljedeće:

Lema 5.4.12. *Neka je $\{a,b,c,d\}$ Diofantova četvorka za koju vrijedi $a < b < c < d$. Tada je $d = d_+$ ili vrijedi $d > 1.16c^{2.5}b^{1.5}$.*

Dokaz. Iz posljednje leme, ako je $d \neq d_+$, imamo $m, n \geq 3$. Tada iz

$$w_3 > (2t-1)^2 \cdot \frac{c}{3.132\sqrt[4]{bc}} > \frac{81}{24 \cdot 3.132}\sqrt[4]{b^3c^3} \cdot c,$$

gdje smo koristili $b \geq 3$, $c \geq 8$, $t \geq 5$, dobivamo

$$d \geq \frac{1.161b^{1.5}c^{3.5} - 1}{c} > 1.16c^{2.5}b^{1.5}.$$

□

Koristeći posljednju Lemu, može se dokazati:

Lema 5.4.13. *Koristeći prethodnu notaciju, vrijedi $v_3 \neq w_3$.*

Sada, potpuno analogno kao lemu 5.4.12 možemo dokazati sljedeće:

Propozicija 5.4.14. *Neka je $\{a,b,c,d\}$ Diofantova četvorka za koju vrijedi $a < b < c < d$. Tada je $d = d_+$ ili vrijedi $d > 2.695c^{3.5}a^{2.5}$.*

Također primijetimo da nam za regularnu Diofantovu četvorku $\{a, b, c, d_+\}$ vrijedi

$$c(4ab + 1) < d_+ < 4c(ab + 1).$$

Korolar 5.4.15. *Neka je $\{a, b, c, d, e\}$ Diofantova petorka za koju vrijedi $a < b < c < d < e$. Tada vrijedi $e > 2.695d^{3.5}b^{2.5}$.*

Dokaz. Pretpostavimo da je $\{b, c, d, e\}$ regularna Diofantova četvorka. Tada vrijedi

$$e < 4d(bc + 1) < d^3.$$

No tada četvorka $\{a, c, d, e\}$ nije regularna, pa prema propoziciji 5.4.14 imamo

$$e > 2.695d^{3.5}a^{2.5} > d^3,$$

što je kontradikcija. Znači, četvorka $\{b, c, d, e\}$ nije regularna, pa iz propozicije 5.4.14 dobivamo tvrdnju korolara. □

5.4.4 Fundamentalna rješenja

Nakon svega što smo pokazali skoro ćemo u potpunosti moći odrediti moguća fundamentalna rješenja jednadžbi (5.34) i (5.35) u ovisnosti o parnostima indeksa m i n.

Lema 5.4.16. *(i) Ako je $v_{2m} = w_{2n}$, onda je $z_0 = z_1$. Nadalje, $|z_0| = 1$, $|z_0| = cr - st$ ili vrijedi $|z_0| < \min\{0.869a^{-5/14}c^{9/14}, 0.972b^{-0.3}c^{0.7}\}$.*

(ii) Ako je $v_{2m+1} = w_{2n}$, onda je $z_0z_1 < 0$, $|z_0| = t$ i $|z_1| = cr - st$.

(iii) Ako je $v_{2m} = w_{2n+1}$, onda je $z_0z_1 < 0$, $|z_0| = cr - st$ i $|z_1| = s$.

(iv) Ako je $v_{2m+1} = w_{2n+1}$, onda je $z_0z_1 > 0$, $|z_0| = t$ i $|z_1| = s$.

Dokaz. Za ilustraciju, dokazat ćemo tvrdnju (i). Otprije znamo da je u ovom slučaju $z_0 = z_1$. Definirajmo

$$d_0 = \frac{z_0^2 - 1}{c} \in \mathbb{N}.$$

Iz (5.34) i (5.35) slijedi

$$ad_0 + 1 = x_0^2,\ bd_0 + 1 = y_1^2,\ cd_0 + 1 = z_0^2,$$

odnosno skup $\{a, b, c, d_0\}$ je Diofantova četvorka. Imamo tri mogućnosti. Ili je $d_0 = 0$, što povlači $|z_0| = 1$, ili je ta četvorka regularna, ili je neregularna. Ako je $\{a, b, c, d_0\}$ regularna četvorka, iz $d_0 < c$ (što slijedi iz ocjene za $|z_0|$), imamo $d_0 = d_-$, odnosno $|z_0| = cr - st$. Ako je pak $\{a, b, c, d_0\}$ neregularna četvorka (pri čemu se računalom može provjeriti da su sve Diofantove četvorke $\{a, b, c, d\}$ za koje vrijedi $a < b < c < d \leq 10^6$ regularne) i $|z_0| \neq 1$, onda možemo zaključiti $z_0^2 \geq c + 1$ i $c > 10^6$. Tada imamo

$$d_0 = \frac{z_0^2 - 1}{c} \geq \frac{z_0^2}{c}\left(1 - \frac{1}{c+1}\right) > 0.999\frac{z_0^2}{c}.$$

Iz toga, zajedno s propozicijom 5.4.14 koja povlači $c \geq 2.695d_0^{3.5}a^{2.5}$, dobivamo

$$c^{4.5} > 2.685|z_0|^7a^{2.5},$$

odnosno

$$|z_0| < 0.869a^{-5/14}c^{9/14}.$$

Analogno, iz leme 5.4.12 dobivamo $|z_0| < 0.972b^{-0.3}c^{0.7}$. □

5.4.5 Metoda kongruencija

U ovom dijelu idemo prema tome da dobijemo donju ogradu za indekse m i n u ovisnosti o c. Za to nam prvo treba definicija standardnih Diofantovih trojki.

Definicija 5.4.17. *Neka je $\{a,b,c\}$ Diofantova trojka za koju vrijedi $a<b<c$. Trojku $\{a,b,c\}$ zovemo Diofantova trojka*

- prve vrste*, ako vrijedi $c>b^{4.5}$,*
- druge vrste*, ako vrijedi $b>4a$ i $c>b^{2.5}$,*
- treće vrste*, ako vrijedi $b>12a$ i $b^{5/3}<c<b^2$,*
- četvrte vrste*, ako vrijedi $b>4a$ i $b^2\leq c<6ab^2$.*

Trojku $\{a,b,c\}$ zovemo standardnom Diofantovom trojkom *ako je ona Diofantova trojka prve, druge, treće ili četvrte vrste.*

Propozicija 5.4.18. *Svaka Diofantova četvorka sadrži standardnu trojku.*

Dokaz. Neka je $\{a,b,c,d\}$ Diofantova četvorka za koju vrijedi $a<b<c<d$. Ako ta četvorka nije regularna, iz propozicije 5.4.14 imamo $d>c^{3.5}$, a otprije i $c>4a$ pa je trojka $\{a,c,d\}$ druge vrste.

Neka je sad $\{a,b,c,d\}$ regularna četvorka. Tada vrijedi

$$c(4ab+1)<d<4c(ab+1).$$

Ako je $b>4a$ i $c\geq b^{1.5}$, onda vrijedi $d>b^{2.5}$, odnosno trojka $\{a,b,d\}$ je druge vrste.

Ako je $b>4a$ i $c<b^{1.5}$, imamo dvije mogućnosti. Prvo, $c=a+b+2r<4b$ i tada je $c^2<d<4ac^2<6ac^2$, pa je trojka $\{a,c,d\}$ četvrte vrste. Druga je mogućnost da je $c\geq 4ab+a+b$ i tada je $d<c^2$ i $d>bc>c^{5/3}$, odnosno trojka $\{a,c,d\}$ je treće vrste.

Ostaje nam još slučaj kad je $b<4a$. Tada iz [49] imamo da je $c=c_k$ za $k\geq 1$ ili $c=c'_k$ za $k\geq 2$, gdje su nizovi (c_k) i (c'_k) definirani s

$$c_0=0,\ c_1=a+b+2r,\ c_k=(4ab+2)c_{k-1}-c_{k-2}+2(a+b),$$
$$c'_0=0,\ c'_1=a+b-2r,\ c'_k=(4ab+2)c'_{k-1}-c'_{k-2}+2(a+b).$$

Ako je sad $c>b^{2.5}$, onda vrijedi $d>4abc>b^{4.5}$, odnosno trojka $\{a,b,d\}$ je prve vrste. Kako je

$$c_2=4r(a+r)(b+r)>4ab^2>b^3,$$

uvjet $c\leq b^{2.5}$ povlači $c=c_1$ ili $c=c'_2$. Ako je $c=c_1$, imamo

$$c\leq a+b+\frac{4}{\sqrt{3}}\sqrt{ab}=\sqrt{ab}\left(\sqrt{\frac{a}{b}}+\sqrt{\frac{b}{a}}+\frac{4}{\sqrt{3}}\right)\leq\sqrt{ab}\left(0.5+2+\frac{4}{\sqrt{3}}\right)<4.81\sqrt{ab}.$$

Također, $c\geq 4r$. Sada imamo $d>4abc>0.172c^3>c^2$ i $d<4cr^2\leq c^2r<2ac^2$ pa je trojka $\{a,c,d\}$ četvrte vrste. Ako je $c\leq b^{2.5}$ i

$$c=c'_2\geq 4ab+2a+2b,$$

imamo $d<c^2$ i $d>4abc>b^2c>c^{1.8}>c^{5/3}$. Znači, trojka $\{a,c,d\}$ je treće vrste. □

Indukcijom lako možemo dokazati sljedeću lemu.

Lema 5.4.19. *Vrijedi:*

(i) $v_{2m} \equiv z_0 + 2c(az_0m^2 + sx_0m) \pmod{8c^2}$,

(ii) $v_{2m+1} \equiv sz_0 + c[2asz_0m(m+1) + x_0(2m+1)] \pmod{4c^2}$,

(iii) $w_{2n} \equiv z_1 + 2c(bz_1n^2 + ty_1n) \pmod{8c^2}$,

(iv) $w_{2n+1} \equiv tz_1 + c[2btz_1n(n+1) + y_1(2n+1)] \pmod{4c^2}$.

Sada ćemo dobiti donju ogradu za n u ovisnosti o c. To ćemo napraviti metodom kongruencija koju su uveli Dujella i Pethő u [22]. Ideja je da promatrajući neke kongruencije, uz neke uvjete, te kongruencije postaju jednakosti za koje se onda obično pokaže da vode na kontradikciju. U našem slučaju, kako bismo primijenili tu metodu trebat će nam neka „rupa" između elemenata u trojci. Dokazat ćemo samo jedan slučaj kao ilustraciju. Također, u dokazima sljedećih lema koristi se i lema 5.4.10.

Lema 5.4.20. *Neka je $\{a, b, c\}$, gdje je $a < b < c$, Diofantova trojka prve vrste i neka je $c > 10^{100}$. Ako je $v_m = w_n$ i $n > 2$, onda vrijedi $n > c^{0.01}$.*

Dokaz. Pretpostavimo suprotno, odnosno $n \leq c^{0.01}$. Ilustrirat ćemo tehniku dokaza u slučaju $v_{2m} = w_{2n}$ i $|z_0| = 1$. Tada leme 5.4.7 i 5.4.19 povlače

$$\pm am^2 + sm \equiv \pm bn^2 + tn \pmod{4c}.$$

Kako je $c > b^{4.5}$, imamo $am^2 < c^{0.243} < c$, $sm < c^{0.623} < c$, $bn^2 < c^{0.243} < c$ i $tn < c^{0.623} < c$. Odnosno, naša kongruencija ustvari je jednakost

$$\pm am^2 + sm = \pm bn^2 + tn.$$

Ako to dvaput kvadriramo, dobivamo

$$[(am^2 - bn^2)^2 - m^2 - n^2]^2 \equiv 4m^2n^2 \pmod{c}.$$

Sada imamo $4m^2n^2 < c^{0.047} < c$ i $[(am^2 - bn^2)^2 - m^2 - n^2]^2 < c^{0.969} < c$, odnosno ponovno imamo jednakost

$$[(am^2 - bn^2)^2 - m^2 - n^2]^2 = 4m^2n^2,$$

što povlači

$$am^2 - bn^2 = \pm m \pm n.$$

Ako to kombiniramo s $\pm am^2 + sm = \pm bn^2 + tn$, zaključujemo

$$m(s \pm 1) = n(t \pm 1).$$

Nadalje imamo

$$n = \frac{(s \pm 1)[t(s \pm 1) - (t \pm 1)s]}{\pm[a(t \pm 1)^2 - b(s \pm 1)^2]} = \frac{(s \pm 1)(\pm t \mp s)}{\pm(\pm 2at + 2s \pm 2bs - 2b)}.$$

Kako vrijedi

$$|(s \pm 1)(\pm t \mp s)| \geq (s-1)(t-s) = \frac{(s-1)c(b-a)}{t+s} > \frac{2c(s-1)}{2\sqrt{bc}} > c \cdot \frac{\sqrt{a}}{2\sqrt{b}}$$

i

$$|\pm 2at + 2a \mp 2bs - 2b| \leq 4bs + 4b < 6b\sqrt{ac},$$

imamo

$$n > \frac{\sqrt{c}}{12\sqrt{b}} > c^{0.377},$$

odnosno dobili smo kontradikciju s $n \leq c^{0.01}$. □

Lema 5.4.21. *Neka je $\{a, b, c\}$, gdje je $a < b < c$, Diofantova trojka druge vrste i neka je $c > 10^{100}$. Ako je $v_m = w_n$ i $n > 2$, onda vrijedi $n > c^{0.04}$.*

Lema 5.4.22. *Neka je $\{a, b, c\}$, gdje je $a < b < c$, Diofantova trojka treće vrste i neka je $c > 10^{100}$. Ako je $v_m = w_n$ i $n > 2$, onda vrijedi $n > c^{0.15}$.*

Lema 5.4.23. *Neka je $\{a, b, c\}$, gdje je $a < b < c$, Diofantova trojka četvrte vrste i neka je $c > 10^{100}$. Ako je $v_m = w_n$ i $n > 2$, onda vrijedi $n > c^{0.2}$.*

5.4.6 Linearne forme u logaritmima

Slično kako je to napravljeno u prethodnim odsječcima, u slučajevima proširenja trojke $\{1, 3, 8\}$ i parametarske familije trojki $\{k-1, k+1, 4k\}$ možemo dokazati sljedeći rezultat.

Lema 5.4.24. *Ako je $v_m = w_n$ za $m, n \neq 0$, onda vrijedi*

$$0 < m\log(s + \sqrt{ac}) - n\log(t + \sqrt{bc}) + \log\frac{\sqrt{b}(x_0\sqrt{c} + z_0\sqrt{a})}{\sqrt{a}(y_1\sqrt{c} + z_1\sqrt{b})} < \frac{8}{3}ac(s + \sqrt{ac})^{-2m}.$$

Dokaz. Primijetimo prvo da za svaku Diofantovu trojku $\{a, b, c\}$ vrijedi $c > b + \sqrt{c}$. Nadalje,

$$v_m = \frac{1}{2\sqrt{a}}[(z_0\sqrt{a} + x_0\sqrt{c})(s + \sqrt{ac})^m + (z_0\sqrt{a} - x_0\sqrt{c})(s - \sqrt{ac})^m],$$

$$w_n = \frac{1}{2\sqrt{b}}[(z_1\sqrt{b} + y_1\sqrt{c})(t + \sqrt{bc})^n + (z_1\sqrt{b} - y_1\sqrt{c})(t - \sqrt{bc})^n].$$

Ako definiramo

$$P = \frac{1}{\sqrt{a}}(z_0\sqrt{a} + x_0\sqrt{c})(s + \sqrt{ac})^m,$$

$$Q = \frac{1}{\sqrt{b}}(z_1\sqrt{b} + y_1\sqrt{c})(t + \sqrt{bc})^n,$$

relacija $v_m = w_n$ povlači

$$P - \frac{c-a}{a}P^{-1} = Q - \frac{c-b}{b}Q^{-1}.$$

Kako je $m, n \geq 1$, lako se pokaže da vrijedi $P, Q > 1$. Sada imamo

$$P - Q = \left(\frac{c}{a} - 1\right)P^{-1} - \left(\frac{c}{b} - 1\right)Q^{-1} > \left(\frac{c}{a} - 1\right)(P^{-1} - Q^{-1}) = \left(\frac{c}{a} - 1\right)(Q - P)P^{-1}Q^{-1},$$

iz čega zaključujemo $P > Q$. Nadalje,

$$\frac{P - Q}{P} < \left(\frac{c-a}{a}\right)P^{-2} < \frac{1}{2},$$

pa imamo

$$0 < \log\frac{P}{Q} = -\log\left(1 - \frac{P-Q}{P}\right) < \frac{2(c-a)}{a}P^{-2} =$$
$$= \frac{2(c-a)}{a} \cdot \frac{a}{(z_0\sqrt{a} + x_0\sqrt{c})^2}(s + \sqrt{ac})^{-2m}.$$

Sada tvrdnja leme slijedi iz

$$\frac{2(c-a)}{a} \cdot \frac{a}{(z_0\sqrt{a} + x_0\sqrt{c})^2} = \frac{2(z_0\sqrt{a} - x_0\sqrt{c})^2}{c-a} \leq \frac{2(|z_0|\sqrt{a} + x_0\sqrt{c})^2}{c-a} \leq \frac{2ac^2}{\frac{3}{4}c} = \frac{8}{3}ac.$$

□

Ako ovo kombiniramo s donjom ogradom za linearne forme koju možemo dobiti iz jednog od Matveevih teorema, uz uvjet $c > \max\{b^{5/3}, 10^{100}\}$, dobivamo da $v_m = w_n$, $m, n \neq 0$ povlači

$$\frac{m}{\log(31.3(m+1))} < 3.826 \cdot 10^{12} \log^2 c.$$

5.4.7 Postoji samo konačno mnogo Diofantovih petorki

Propozicija 5.4.25. *Neka je $\{a, b, c\}$ standardna Diofantova trojka za koju vrijedi $c \geq 10^{2171}$. Ako je $\{a, b, c, d\}$ Diofantova četvorka za koju vrijedi $d > c$, onda je $d = d_+$.*

Dokaz. Pretpostavimo $d \neq d_+$. Tada imamo $m \geq 3$ i $n \geq 3$ pa imamo donju ogradu $n > c^{0.01}$, odnosno

$$m + 1 \geq n > c^{0.01}.$$

To nadalje povlači

$$\frac{m}{\log(31.3(m+1))\log^2(m+1)} < 3.826 \cdot 10^{16},$$

odnosno $m < 5.108 \cdot 10^{21}$ i konačno $c < (m+1)^{100} < 10^{2171}$. □

Korolar 5.4.26. *Neka je $\{a, b, c\}$ standardna Diofantova trojka za koju vrijedi $c < 2.695b^{3.5}$ i $c \geq 10^{2171}$. Ako je $\{a, b, c, d\}$ Diofantova četvorka, onda je $d = d_+$ ili $d = d_-$.*

Korolar 5.4.27. *Neka je $\{a, b, c\}$ standardna Diofantova trojka treće ili četvrte vrste i $c \geq 10^{2171}$. Ako je $\{a, b, c, d\}$ Diofantova četvorka, onda je $d = d_+$ ili $d = d_-$.*

Dokažimo sada da postoji samo konačno mnogo Diofantovih petorki.

Teorem 5.4.28. *Neka je $\{a, b, c, d, e\}$ Diofantova petorka za koju vrijedi $a < b < c < d < e$. Tada je $e < 10^{10^{26}}$.*

Dokaz. Promotrimo Diofantovu četvorku $\{a, b, c, d\}$. Tada znamo da ona sadrži standardnu trojku $\{A, B, C\}$, gdje je $A < B < C = d$. Ako pretpostavimo da je $d \geq 10^{2171}$, $\{A, B, C, e\}$ je regularna četvorka i vrijedi

$$e < 4d(bc + 1) < d^3.$$

S druge strane iz korolara 5.4.15 imamo

$$e > 2.695d^{3.5}b^{2.5} > d^3,$$

odnosno dobivamo kotradikciju. Znači $d < 10^{2171}$.

Promotrimo sada četvorku $\{A, B, C = d, e\}$. Element e dobivamo proširenjem trojke $\{A, B, C = d\}$ pa možemo koristiti rezultate koje smo dobili za proširenje općenite trojke $\{a, b, c\}$ u ovom odsječku. Tada je $ed + 1 = V_m^2$. Iz gornje ograde za d dobivamo

$$\frac{m}{\log(31.3(m+1))} < 9.561 \cdot 10^{19},$$

odnosno $m < 5.109 \cdot 10^{21}$. Nadalje,

$$V_m < 1.7C\sqrt[4]{AC}(2\sqrt{AC+1})^{m-1} < 2^m \cdot d^{m+0.5}.$$

Sada imamo

$$e = \frac{V_m^2 - 1}{C} < \frac{V_m^2}{d} < 4^m \cdot d^{2m}$$

pa tvrdnja teorema slijedi iz gornjih ograda za m i d koje imamo. □

Korolar 5.4.29. *Neka je $\{a, b, c, d, e\}$ Diofantova petorka za koju vrijedi $a < b < c < d < e$. Tada je $d < 10^{2171}$ i $e < 10^{10^{26}}$.*

Spomenimo kao napomenu, da bismo korištenjem teorema Bakera i Wüstholza umjesto teorema Matveeva dobili malo lošiji rezultat: $d < 10^{2411}$ i $e < 10^{10^{28}}$.

5.4.8 Ne postoji Diofantova šestorka

U ovom odsječku ćemo dokazati nepostojanje Diofantove šestorke. Tu ćemo umjesto linearnih formi u logaritmima koristiti hipergeometrijsku metodu, odnosno Bennettov teorem koji smo ranije naveli.

Prvo definirajmo brojeve

$$\theta_1 = \sqrt{1 + \frac{1}{ac}} = \sqrt{1 + \frac{b}{abc}},$$
$$\theta_2 = \sqrt{1 + \frac{1}{bc}} = \sqrt{1 + \frac{a}{abc}}.$$

Propozicija 5.4.30. *Neka su $x, y, z \in \mathbb{N}$ rješenja sustava jednadžbi* (5.34) *i* (5.35)*. Tada vrijedi*

$$\max\left\{\left|\theta_1 - \frac{sbx}{abz}\right|, \left|\theta_2 - \frac{tay}{abz}\right|\right\} < \frac{c}{2a} \cdot z^{-2}.$$

Dokaz. Imamo

$$\left|\theta_1 - \frac{sbx}{abz}\right| = \left|\frac{s}{a}\sqrt{\frac{a}{c}} - \frac{sbx}{abz}\right| = \frac{s}{az\sqrt{c}}|z\sqrt{a} - x\sqrt{c}| =$$
$$\frac{s}{az\sqrt{c}} \cdot \frac{c-a}{z\sqrt{a} + x\sqrt{c}} < \frac{s(c-a)}{2a\sqrt{ac}z^2} < \frac{c}{2a} \cdot z^{-2}.$$

Analogno dobivamo

$$\left|\theta_2 - \frac{tay}{abz}\right| < \frac{c}{2b} \cdot z^{-2} < \frac{c}{2a} \cdot z^{-2}.$$

□

Kombinirajući ovu prethodnu propoziciju s Bennettovim teoremom 3.2.10 možemo dokazati:

Lema 5.4.31. *Neka je $\{a, b, c, d\}$ Diofantova četvorka za koju vrijedi $a < b < c < d$.*

(i) Ako je $c > 344.9b^{9.5}a^{3.5}$, onda vrijedi $d < c^{27.62}$.

(ii) Ako je $c > 296.4b^{11.6}a^{1.4}$, onda vrijedi $d < c^{21.47}$.

Dokaz. Dokažimo tvrdnju (i). U notaciji Bennettova teorema 3.2.10 imamo $a_0 = 0$, $a_1 = a$, $a_2 = b$, $N = abc$, $M = b$, $q = abz$, $p_1 = sbx$ i $p_2 = tay$. Kombinirajući donju ogradu iz tog teorema za

$$\max\left\{\left|\theta_1 - \frac{sbx}{abz}\right|, \left|\theta_2 - \frac{tay}{abz}\right|\right\}$$

zajedno s gornjom ogradom iz propozicije 5.4.30 dobivamo

$$\log z < \frac{\log(32.5a^2b^6c^2)\log(1.7c^2(b-a)^{-2})}{\log\left(\frac{1.7c}{16.5ab^4(b-a)^2}\right)}.$$

Iz uvjeta $c > 344.9b^{9.5}a^{3.5}$ zaključujemo

$$\log z < 14.31 \log c,$$

odnosno

$$z < c^{14.31}$$

i

$$d = \frac{z^2 - 1}{c} < c^{27.62}.$$

□

Metodom kongruencija možemo kao i prije dobiti donju ogradu za n u ovisnosti o c.

Lema 5.4.32. *Neka je $\{a, b, c\}$ Diofantova trojka za koju vrijedi $a < b < c$. Pretpostavimo da je $z = v_m = w_n$ za $n > 2$.*

(i) Ako je $c > \max\{b^{11.6}, 2.97 \cdot 10^{16}\}$, onda vrijedi $n > c^{0.0815}$.

(ii) Ako je $b > 4a$ i $c > \max\{b^{9.5}, 1.5 \cdot 10^{13}\}$, onda vrijedi $n > c^{0.11}$.

Propozicija 5.4.33. *Ako je $\{a, b, c, d\}$ Diofantova četvorka za koju vrijedi $c > \max\{296.4b^{11.6}a^{1.4}, 2.97 \cdot 10^{16}\}$ ili $b > 4a$ i $c > \max\{344.9b^{9.5}a^{3.5}, 1.5 \cdot 10^{13}\}$ te $d > c$, onda vrijedi $d = d_+$.*

Dokaz. Dokažimo tvrdnju za $c > \max\{296.4b^{11.6}a^{1.4}, 2.97 \cdot 10^{16}\}$. Pretpostavimo da je $d \neq d_+$. Tada je $n \geq 3$ i

$$z = w_n > \frac{c}{3.132\sqrt[4]{bc}}(1.999\sqrt{bc})^{n-1} > c^{\frac{n}{2}+\frac{1}{4}}.$$

S druge strane, iz leme 5.4.31 imamo $z < c^{11.24}$, što povlači $n \leq 22$. To nam daje $c < 12.97 \cdot 10^{16}$, kontradikciju. □

Dokažimo da ne postoji Diofantova šestorka. Pretpostavimo suprotno, neka je $\{a, b, c, d, e, f\}$ Diofantova šestorka za koju vrijedi $a < b < c < d < e < f$. Iz korolara 3.5 imamo

$$e > 2.695d^{3.5}b^{2.5} > 2.695(4abc)^{3.5}b^{2.5} > 344.9b^{9.5}a^{3.5}.$$

Ako je $b < 4a$, onda je $c \geq a + b + 2r > \frac{9}{4}b$ pa imamo

$$e > 2.695 \cdot 2.25^{3.5}b^{9.5}(4a)^{1.4}b^{2.1} > 296.4b^{11.6}a^{1.4}.$$

Pretpostavimo sad da je

$$e > 2.97 \cdot 10^{16}$$

ili

$$b < 4a,\ e > 1.5 \cdot 10^{13}.$$

Iz propozicije 5.4.33 zaključujemo da je $\{a, b, e, f\}$ regularna četvorka, što povlači

$$f < 4e(ab + 1) < e^3,$$

no s druge strane iz korolara 5.4.15 imamo $f > e^{3.5}$, što je kontradikcija.

Ostaje vidjeti što se događa ako je

$$e \leq 2.97 \cdot 10^{16}$$

ili

$$b < 4a,\ c \leq 1.5 \cdot 10^{13},$$

no ti preostali slučajevi su dovoljno „mali" da se računalnim programom može provjeriti da takva šestorka ne postoji. Primijetimo da nam gornja ograda za e daje i gornju ogradu za elemente a, b, c i d.

5.4.9 Ideje dokaza o nepostojanju Diofantove petorke

Prvi veliki korak u dokazivanju nepostojanja Diofantove petorke napravio je Dujella koji je dokazao da postoji konačno petorki i da ne postoji Diofantova šetorka. Te rezultate smo prezentirali u prethodnim odsječcima. Dujella je u [27] dao i prvu ogradu za broj Diofantovih petorki; dokazao je da ih ima najviše 10^{1930}.

Sljedeći važan korak napravio je Fujita [41] koji je dokazao da ako je $\{a, b, c, d, e\}$ Diofantova petorka takva da vrijedi $a < b < c < d < e$, onda je $\{a, b, c, d\}$ regularna četvorka. U svom dokazu Fujita je provjerio da za još više malih indeksa ne možemo imati rješenje jednadžbe $z = v_m = w_n$, osim ako je $c < d = (z^2 - 1)/c = d_+$. To je omogućilo dobivanje bolje rupe između elemenata u četvorki. Nadalje, uveo je precizniju definiciju standardnih Diofantovih trojki te je poboljšao teoreme Rickerta i Bennetta u posebnom slučaju. Također, njegovi rezultati u kojima je dobio i bolju ogradu za elemente u petorci omogućili su znatno poboljšanje gornje ograde za broj petorki. Naime, u [43] je dokazano da petorki ima najviše 10^{276}.

Nakon toga uslijedila je serija rezultata gdje je znatno poboljšana ograda za broj petorki. Prvo su Filipin i Fujita [35] dalje poboljšavajući hipergeometrijsku metodu dokazali da je petorki najviše 10^{96}. Zatim su isti autori zajedno s Elsholtzom [34] dokazali da je petorki najviše

$6.8 \cdot 10^{32}$, gdje je uveden potpuno novi način prebrojavanja petorki kada znamo gornju ogradu za njihove elemente. Koristeći slične metode, najbolji rezultat prije dokaza o nepostojanju petorke dali su Cipu i Trudgian [12], gdje su dokazali da petorki može biti najviše $1.18 \cdot 10^{27}$.

Konačno, za dokaz nepostojanja Diofantove petorke [47] korištene su sljedeće inovativne ideje i metode:

- Autori su uveli definiciju operatora na Diofantovim trojkama koji je dao udaljenost određene trojke do Eulerove trojke $\{a, b, a + b + 2r\}$; tako su klasificirali sve trojke.
- Nadalje, autori su koristili najbolje poznate rezultate iz Bakerove teorije linearnih formi u logaritmima, što im je omogućilo dobivanje dovoljno „male“ gornje ograde za elemente kako bi se preostali slučajevi mogli provjeriti računalom.
- Konačno, autori su koristili potpuno nove kongruencije u slučaju Eulerovih četvorki $\{a, b, a+b+2r, 4r(r+a)(r+b)\}$ kada se promatralo proširenje takve četvorke do petorke. Ako se prisjetimo, kada su Dujella i Pethő uveli metodu kongruencija, morali smo imati neku dovoljno veliku rupu između elemenata da bi metoda bila učikovita.

Poglavlje 6

Diofantove m-torke u različitim prstenima

Diofantovu m-torku definirali smo kao skup međusobno različitih prirodnih brojeva za koji vrijedi da je umnožak bilo koja dva broja uvećan za 1 jednak punom kvadratu nekog prirodnog broja. Cijelo prethodno poglavlje posvećeno je tome da se obrazloži činjenica da je najveći mogući takav skup Diofantova četvorka, odnosno da ne postoji Diofantova petorka u $\mathbb{Z}$. Dakle, naš problem određivanja najveće moguće veličine Diofantovog skupa do sada je bio smješten u prstenu cijelih brojeva $\mathbb{Z}$. Prirodni slijed razmatranja bio bi proučiti moguće veličine takvih skupova u nekom drugom prstenu ili polju. Naime, u komutativnom prstenu s jedinicom 1, $\mathcal{R}$, smisleno je definirati Diofantovu m-torku u $\mathcal{R}$ kao skup $\{a_1, \ldots, a_m\} \subset \mathcal{R}$ za koji vrijedi

- $a_i \neq a_j$, $1 \leq i < j \leq m$,
- $a_i \neq 0$, $i = 1, \ldots, m$,
- $a_i a_j + 1 = \xi_{ij}^2$, $\xi_{ij} \in \mathcal{R}$, $1 \leq i < j \leq m$.

U ovom poglavlju reći ćemo nešto o Diofantovim m-torkama u polju racionalnih brojeva i prstenu Gaussovih cijelih brojeva.

6.1 Racionalne Diofantove m-torke

Diofantovu m-torku u polju $\mathbb{Q}$ nazivamo *racionalna Diofantova m-torka*. Diofant je našao prvu takvu četvorku

$$\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}.$$

Euler je Fermatovu cjelobrojnu četvorku $\{1, 3, 8, 120\}$ uspio nadopuniti do racionalne Diofantove petorke elementom

$$e = \frac{777480}{8288641}.$$

Općenito, Dujella ([16]) je racionalnu Diofantovu četvorku $\{a_1, a_2, a_3, a_4\}$ nadopunio do petorke elementima $a_5^{\pm}$:

$$\frac{((a_1+a_2+a_3+a_4)(a_1a_2a_3a_4+1)+2(a_1a_2a_3+a_1a_2a_4+a_1a_3a_4+a_2a_3a_4 \pm \xi_{12}\xi_{13}\xi_{14}\xi_{23}\xi_{24}\xi_{34}))}{(a_1a_2a_3a_4-1)^2}, \tag{6.1}$$

gdje je $a_ia_j+1=\xi_{ij}^2$ za $1\leq i<j\leq 4$. Zaista,

$$a_1a_5^{\pm}+1=\frac{(a_1\xi_{23}\xi_{24}\xi_{34}\pm\xi_{12}\xi_{13}\xi_{14})^2}{(a_1a_2a_3a_4-1)^2},$$

to analogno vrijedi i za ostale $a_ia_5^{\pm}+1=\square$, $i=2,3,4$.

Prvi primjer racionalne Diofantove šestorke našao je Gibbs 1999. godine ([44]):

$$\{\frac{11}{192},\frac{35}{192},\frac{155}{27},\frac{512}{27},\frac{1235}{48},\frac{180873}{16}\}.$$

Zanimljivi su i primjeri racionalnih Diofantovi šestorki s različitim (mješovitim) predznacima koje je pronašao Dujella ([29]). Na tisuće pronađenih primjera racionalnih šestorki dalo je naslutiti da bi ih moglo biti beskonačno mnogo, što je 2017. godine i dokazano u [30].

Teorem 6.1.1 (Dujella, Kazalicki, Mikić, Szikszai, 2017.)**.** *Postoji beskonačno mnogo racionalnih Diofantovih šestorki, kako onih s pozitivnim elementima, tako i onih s različitim predznacima.*

Za prethodni rezultat primijenila se veza Diofantovih m-torki s eliptičkim krivuljama. Svaka racionalna Diofantova trojka $\{a,b,c\}$ inducira jednu eliptičku krivulju. Naime, problem proširenja skupa $\{a,b,c\}$ do četvorke ekvivalentan je sustavu

$$ax+1=\xi^2,\ bx+1=\eta^2,\ cx+1=\nu^2 \tag{6.2}$$

koji rješavamo u polju $\mathbb{Q}$. Prethodnom sustavu možemo pridružiti eliptičku krivulju

$$E\ :\quad y^2=(ax+1)(bx+1)(cx+1) \tag{6.3}$$

za koju još kažemo da je *inducirana Diofantovom trojkom* $\{a,b,c\}$. Općenito, skup racionalnih točaka eliptičke krivulje E u oznaci $E(\mathbb{Q})$ čini Abelovu grupu s obzirom na prirodno definirano zbrajanje točaka s krivulje uz pridruženu točku u beskonačnosti $\mathcal{O}$ koja je neutralni element zbrajanja (za detalje vidjeti u npr. [32], poglavlje 15). Konkretno, za eliptičku krivulju (6.3) vrijedi da su

$$A=\left[-\frac{1}{a},0\right],\quad B=\left[-\frac{1}{b},0\right],\quad C=\left[-\frac{1}{c},0\right]$$

racionalne točke reda 2 te

$$P=[0,1],\quad S=\left[\frac{1}{abc},\frac{\sqrt{(ab+1)(ac+1)(bc+1)}}{abc}\right] \tag{6.4}$$

još dvije racionalne točke. Lako se može pokazati da svako rješenje $x\in\mathbb{Q}$ sustava (6.2) inducira racionalnu točku eliptičke krivulje E. Sljedeći teorem daje odgovor na pitanje kada racionalna točka s E inducira rješenje sustava (6.2).

Teorem 6.1.2 (Dujella, [24])**.** *x-koordinata točke $T\in E(\mathbb{Q})$ zadovoljava sustav (6.2) ako i samo ako je $T-P\in 2E(\mathbb{Q})$ (gdje je $2E(\mathbb{Q})=\{T+T\ :\ T\in E(\mathbb{Q})\}$).*

U nastavku x-koordinatu točke $T\in E(\mathbb{Q})$ označavat ćemo s $x(T)$. Nadalje, može se pokazati da je $S\in 2E(\mathbb{Q})$, odnosno da je $S=[2]R$ gdje je

$$R=\left[\frac{rs+rt+st+1}{abc},\frac{(r+s)(r+t)(s+t)}{abc}\right]$$

te $ab+1=r^2$, $ac+1=s^2$, $bc+1=t^2$. Stoga, ako $x(T)$ zadovoljava sustav (6.2), onda i $x(T\pm S)$ također zadovoljavaju taj sustav. Prethodna tvrdnja može se provjeriti direktnim računom. Naime, $x(T\pm S)$ su upravo navedeni elementi $a_5^{\pm}$, u (6.1), za $(a_1,a_2,a_3,a_4)=(a,b,c,x(T))$ te vrijedi da su $a_4a_5^+ +1$ i $a_4a_5^- +1$ potpuni kvadrati. Dakle, $x(T)x(T\pm S)+1$ su potpuni kvadrati. Stoga se četvorka $\{a,b,c,x(T)\}$ može nadopuniti do petorke na dva načina: $\{a,b,c,x(T),x(T-S)\}$ i $\{a,b,c,x(T),x(T+S)\}$, a uz samo jedan dodatni uvjet skup $\{a,b,c,x(T-S),x(T),x(T+S)\}$ čini racionalnu Diofantovu šestorku. Taj uvjet glasi:

$$x(T-S)x(T+S)+1=q^2$$

za neki $q\in\mathbb{Q}$. Pokazuje se da je taj uvjet zadovoljen ako je S reda 3 (tj. $[3]S=\mathcal{O}$) jer je tada $x(T-S)=x(T+2S)$.

Uz supstituciju $x\mapsto\frac{x}{abc}$, $y\mapsto\frac{y}{abc}$ eliptička krivulja E transformira se u

$$E':\qquad y^2=(x+ab)(x+ac)(x+bc).$$

Točka S prelazi u $S'=[1,rst]$ i reda je 3 ako i samo ako vrijedi

$$-a^4b^2c^2+2a^3b^3c^2+2a^3b^2c^3-a^2b^4c^2+2a^2b^3c^3-a^2b^2c^4+12a^2b^2c^2+6a^2bc+$$

$$6ab^2c+6abc^2+4ab+4ac+4bc+3=0.$$

Prethodni izraz može se shvatiti kao simetrična jednadžba u a,b,c pa je se može svesti na jednostavniju pomoću elementarnih simetričnih polinoma

$$\sigma_1=a+b+c,\ \sigma_2=ab+ac+bc,\ \sigma_3=abc.$$

Tako dobivamo

$$4\sigma_2(1+\sigma_3^2)=\sigma_1^2\sigma_3^2-12\sigma_3^2-6\sigma_1\sigma_3-3. \tag{6.5}$$

Kombinirajući prethodnu jednadžbu s uvjetom $(ab+1)(ac+1)(bc+1)=(rst)^2$ koji je ekvivalentan

$$\sigma_3^2+\sigma_1\sigma_3+\sigma_2+1=\square,$$

dobivamo

$$\frac{(2\sigma_3^2+\sigma_1\sigma_3-1)^2}{4(1+\sigma_3^2)}=\square\ \Rightarrow\ 1+\sigma_3^2=\square.$$

Zadnji uvjet može biti ispunjen za $\sigma_3=\frac{t^2-1}{2t}$.

Iz uvjeta da polinom

$$p(X)=X^3-\sigma_1X^2+\sigma_2X-\sigma_3=(X-a)(X-b)(X-c)$$

ima tri racionalna korijena slijedi da je diskriminanta polinoma p kvadrat:

$$\sigma_1^2\sigma_2^2-4\sigma_2^3-4\sigma_1^3\sigma_3+18\sigma_1\sigma_2\sigma_3-27\sigma_3^2=\square.$$

Kako se prema (6.5) varijabla σ_2 može prikazati preko σ_1 i σ_3, slijedi da je prethodni izraz jednak

$$\frac{(-27-9\sigma_1^2-27\sigma_1\sigma_3+\sigma_1^3\sigma_3-54\sigma_3^2)(-1+\sigma_1\sigma_3+2\sigma_3^2)^3}{16(1+\sigma_3^2)^3}=\square,$$

odnosno

$$(-27-9\sigma_1^2-27\sigma_1\sigma_3+\sigma_1^3\sigma_3-54\sigma_3^2)(-1+\sigma_1\sigma_3+2\sigma_3^2)\underbrace{(1+\sigma_3^2)}_{=\square}=\square.$$

Prethodna relacija može se shvatiti kao kvartika u varijabli σ_1, pri čemu uzimamo da je σ_3 fiksan. Kvartika se može transformirati u eliptičku krivulju na $\mathbb{Q}(t)$ (npr. vidjeti Propoziciju 15.1 na str. 461 iz [32]) pa se uz $\sigma_3=\frac{t^2-1}{2t}$ dobiva:

$$y^2=x^3+(3t^4-21t^2+3)x^2+(3t^8+12t^6+18t^4+12t^2+3)x+(t^2+1)^6. \tag{6.6}$$

Detaljan izvod ove konstrukcije prikazan je u [30]. Točka $R=[0,(t^2+1)^3]$ s krivulje (6.6) je točka beskonačnog reda. Svakom višekratniku točke R, odnosno točki $[m]R$, odgovarat će jedna racionalna Diofantova trojka $\{a,b,c\}$ (pri čemu ih se može dobiti tako što se točka $[m]R$ transformira na kvartiku). Za točku $[2]R$ dobiva se familija racionalnih Diofantovih trojki:

$$(a,b,c)=\left(\frac{18t(t-1)(t+1)}{(t^2-6t+1)(t^2+6t+1)},\frac{(t-1)(t^2+6t+1)^2}{6t(t+1)(t^2-6t+1)},\frac{(t+1)(t^2-6t+1)^2}{6t(t-1)(t^2+6t+1)}\right)$$

koja se do šestorke nadopunjuje elementima $d=x([3]P)$, $e=x([3]P+S)$, $f=x([3]P-S)$ (a točke P,S su kao u (6.4)). Elementi d,e,f dani su sljedećim (nimalo jednostavnim) izrazima:

$$\begin{aligned}
d &= \big(6(t+1)(t-1)(t^2+6t+1)(t^2-6t+1)(8t^6+27t^5+24t^4-54t^3+24t^2+27t+8)(8t^6-27t^5+24t^4+54t^3+24t^2-27t+8)\\
&\quad (t^8+22t^6-174t^4+22t^2+1)\big)/\big(t(37t^{12}-885t^{10}+9735t^8-13678t^6+9735t^4-885t^2+37)^2\big),\\
e &= \big(-2t(4t^6-111t^4+18t^2+25)(3t^7+14t^6-42t^5+30t^4+51t^3+18t^2-12t+2)(3t^7-14t^6-42t^5-30t^4+51t^3-18t^2-12t-2)\\
&\quad (t^2+3t-2)(t^2-3t-2)(2t^2+3t-1)(2t^2-3t-1)(t^2+7)(7t^2+1)\big)/\\
&\quad \big(3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1)(16t^{14}+141t^{12}-1500t^{10}+7586t^8-2724t^6+165t^4+424t^2-12)^2\big),\\
f &= \big(2t(25t^6+18t^4-111t^2+4)(2t^7-12t^6+18t^5+51t^4+30t^3-42t^2+14t+3)(2t^7+12t^6+18t^5-51t^4+30t^3+42t^2+14t-3)\\
&\quad (2t^2+3t-1)(2t^2-3t-1)(t^2-3t-2)(t^2+3t-2)(t^2+7)(7t^2+1)\big)/\\
&\quad \big(3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1)(12t^{14}-424t^{12}-165t^{10}+2724t^8-7586t^6+1500t^4-141t^2-16)^2\big).
\end{aligned}$$

Iz opisane konstrukcije zaključujemo da postoji beskonačno mnogo racionalnih Diofantovih trojki koje se na beskonačno načina mogu proširiti do racionalne Diofantove šestorke. No postoji konstrukcija koja nadopunjuje racionalnu Diofantovu četvorku do šestorke i pomoću koje se dobiju parametarske formule za elemente šestorke koje su nešto jednostavnije ([31]).

Na kraju navedimo da nije poznato postoji li racionalna Diofantova sedmorka. Poznati su primjeri „skoro sedmorki" u kojima nedostaje samo jedan uvjet za „pravu sedmorku". Tako je Gibbs pronašao nekoliko primjera racionalnih Diofantovih petorki koje se na dva načina mogu proširiti do šestorke, npr.

$$\{\frac{243}{560},\frac{1147}{5040},\frac{1100}{63},\frac{7820}{567},\frac{95}{112}\}$$

može se nadopuniti elementom $\frac{38269}{6480}$ ili elementom $\frac{196}{45}$. Ostali zanimljivi primjeri racionalnih Diofantovih šestorki mogu se naći na `https://web.math.pmf.unizg.hr/~duje/ratio.html`.

6.2 Diofantove m-torke u prstenu Gaussovih cijelih brojeva

U proučavanju Diofantovih m-torki u prstenu Gaussovih cijelih brojeva, $\mathbb{Z}[i]=\{a+bi:a,b\in\mathbb{Z}\}$, može se, za početak, slijediti strategija koja se primijenila u skupu cijelih brojeva (zapravo u $\mathbb{N}$). Stoga ćemo ukratko reći nešto o proširenju Diofantove trojke

$$\{k-1,k+1,4k\},\ k\in\mathbb{Z}[i]\backslash\{0,\pm1\},$$

u prstenu $\mathbb{Z}[i]$ ([36]). Podsjetimo se, u odjeljku 5.3 pokazano je da je proširenje navedene Diofantove trojke u $\mathbb{N}$ jedinstveno i to elementom $d = 16k^3 - 4k$ (teorem 5.3.1). Štoviše, tamo smo efektivno pokazali da je primjena teorema za simultanu aproksimaciju kvadratnih korijena racionalnih brojeva blizu 1 vrlo učinkovita. Konkretno smo primijenili Rickertov teorem 5.3.5, no mogao se koristiti i općenitiji Bennettov teorem 3.2.10. Navedeni teoremi vrijede u prstenu cijelih brojeva pa ih se u ovom slučaju ne može primijeniti. No 2006. godine Jadrijević i Ziegler ([48]) uspjeli su poopćiti Bennettov teorem za prsten cijelih brojeva imaginarnih kvadratnih polja. Za neki kvadratno slobodan $D \in \mathbb{N}$ označimo kvadratno prošrenje od $\mathbb{Q}$ s $K = \mathbb{Q}(\sqrt{-D})$ (imaginarno kvadratno polje) te skup svih algebarskih cijelih brojeva u K s $\mathcal{O}_K$. Uz dogovorene oznake vrijedi sljedeći teorem:

Teorem 6.2.1 (Jadrijević, Ziegler, 2006.)**.** *Neka su $a_1, \ldots, a_m$ međusobno različiti algebarski cijeli brojevi iz $\mathcal{O}_K$, $A = \max|a_i|$, $T \in \mathcal{O}_K$, $|T| > A$ te*

$$\theta_i = \sqrt{1 + \frac{a_i}{T}},\ 1 \leq i \leq m.$$

Nadalje, neka je $a_0 = 0$ i

$$\begin{aligned}
l &= c_m \frac{(m+1)^{m+1}}{m^m} \cdot \frac{|T|}{|T| - A}, \\
L &= |T|^m \frac{(m+1)^{m+1}}{4m^m \prod_{0 \leq i < j \leq m} |a_j - a_i|^2} \cdot \left(\frac{|T| - A}{|T|} \right)^m, \\
p &= \sqrt{\frac{2|T| + 3A}{2|T| - 2A}}, \\
P &= |T| \cdot 2^{m+3} \frac{\prod_{0 \leq i < j \leq m} |a_i - a_j|^2}{\min_{i \neq j} |a_i - a_j|^{m+1}} \cdot \frac{2|T| + 3A}{2|T|},
\end{aligned}$$

gdje je $c_m = \frac{3\Gamma\left(m - \frac{1}{2}\right)}{4\sqrt{\pi}\Gamma(m+1)}$. Ako je $L > 1$, onda

$$\max\left\{ \left| \theta_1 - \frac{p_1}{q} \right|, \ldots, \left| \theta_m - \frac{p_m}{q} \right| \right\} > cq^{-\lambda}$$

za sve algebarske cijele brojeve $p_1, \ldots, p_m, q \in \mathcal{O}_K$, pri čemu je

$$\begin{aligned}
\lambda &= 1 + \frac{\log P}{\log L}, \\
c^{-1} &= 2mpP \left(\max\{1, 2l\} \right)^{\lambda - 1}.
\end{aligned}$$

U slučaju $m = 2$, koji je i potreban za primjenu proširenja familije Diofantove trojke $\{k-1, k+1, 4k\}$ do četvorke, iskaz prethodnog teorema je jednostavniji:

Korolar 6.2.2. *Neka su $a_1 \neq a_2 \in \mathcal{O}_K$, $A = \max\{|a_1|, |a_2|\}$, $T \in \mathcal{O}_K$, $|T| > A$ te*

$$\theta_1 = \sqrt{1 + \frac{a_1}{T}},\ \theta_2 = \sqrt{1 + \frac{a_2}{T}}.$$

Ako je

$$l = \frac{27|T|}{64(|T|-A)}, \quad L = \frac{27(|T|-A)^2}{16|a_1|^2|a_2|^2|a_1-a_2|^2} > 1,$$
$$p = \sqrt{\frac{2|T|+3A}{2|T|-2A}}, \quad P = \frac{16|a_1|^2|a_2|^2|a_1-a_2|^2}{(\min\{|a_1|,|a_2|,|a_1-a_2|\})^3}(2|T|+3A),$$
$$\lambda = 1 + \frac{\log P}{\log L}, \qquad c^{-1} = 4pP\left(\max\{1,2l\}\right)^{\lambda-1},$$

onda nejednakost

$$\max\left\{\left|\theta_1 - \frac{p_1}{q}\right|, \left|\theta_2 - \frac{p_2}{q}\right|\right\} > cq^{-\lambda}$$

vrijedi za sve algebarske cijele brojeve $p_1, p_2, q \in \mathcal{O}_K$.

Prethodni rezultat se, slično kao što je pokazano u odjeljku 5.3.4, koristi da bi se pokazalo da su jedina rješenja u $x \in \mathbb{Z}[i]$ sustava pelovskih jednadžbi:

$$(k+1)x^2 - (k-1)y^2 = 2, \ 4kx^2 - (k-1)z^2 = 3k+1 \tag{6.7}$$

za dovoljno veliku vrijednost parametra k, $k \in \mathbb{Z}[i]\backslash\{0,\pm 1\}$, jednaka $x = \pm 1$ i $x = \pm(4k^2 - 2k - 1)$. Konkretno, primjenjuje se na brojeve $\theta_1^{(1)}$ i $\theta_2^{(1)}$ koji su definirani na sljedeći način:

$$\theta_1^{(1)} = \pm\sqrt{\frac{k+1}{k-1}}, \ \theta_1^{(2)} = -\theta_1^{(1)},$$

$$\theta_2^{(1)} = \pm\sqrt{\frac{k}{k-1}}, \ \theta_2^{(2)} = -\theta_2^{(1)},$$

a predznaci su odabrani tako da vrijedi

$$\left|\theta_1^{(1)} - \frac{y}{x}\right| \leq \left|\theta_1^{(2)} - \frac{y}{x}\right|, \ \left|\theta_2^{(1)} - \frac{z}{2x}\right| \leq \left|\theta_2^{(2)} - \frac{z}{2x}\right|,$$

pri čemu je $(x,y,z) \in \mathbb{Z}[i]^3$ rješenje sustava (6.7). Napomenimo da za $\sqrt{\alpha}$, $\alpha \in \mathbb{C}$, uzimamo onaj korijen za koji je $\mathrm{Re}(\sqrt{\alpha}) > 0$, a u slučaju $\mathrm{Re}(\sqrt{\alpha}) = 0$ onaj za koji je $\mathrm{Im}(\sqrt{\alpha}) > 0$. Konačno, dobiva se tražena tvrdnja (o rješenjima sustava (6.7)) uz pretpostavku $|k| \geq 350$. Prehodni slučajevi, $|k| < 350$, mogu se riješiti pomoću Bakerove teorije o linearnim formama u logaritmima algebarskih brojeva i metode redukcije. Zanimljivo je da se ovdje provjera uvjeta Bakerova teorema (tj. nekog od teorema tog „tipa", npr. 4.1.5): $\Lambda = \log\frac{|P|}{|Q|} \neq 0$ pretvara u izazovan problem. Nadalje, zanimljivo je da se za neke k, $1 \leq |k| \leq 5$, dobivaju još neka fundamentalna rješenja jednadžbi (6.7) osim $x = \pm 1$, što rezultira da su rješenja pojedinih jednadžbi opisana s još nekim rekurzivnim nizovima. Konačno, pokazuje se da vrijedi tvrdnja analogna onoj u realnom slučaju:

Teorem 6.2.3. *Neka je* $k \in \mathbb{Z}[i]\backslash\{0,\pm 1\}$ *i* $\{k-1, k+1, 4k, d\}$ *Diofantova četvorka u* $\mathbb{Z}[i]$. *Tada je* $d = 16k^3 - 4k$.

U [5] je potpuno analogno pokazano da se Diofantova trojka $\{k, 4k+4, 9k+6\}$, $k \in \mathbb{Z}[i]\backslash\{0,-1\}$ jedinstveno proširuje u $\mathbb{Z}[i]$ elementom $d = 144k^3 + 240k^2 + 124k + 20$. Zanimljivo je da se ista procedura, konkretno primjena teorema 6.2.1, nije mogla provesti u slučaju

Diofantove trojke $\{k-1, k+1, 16k^3-4k\}$ ([1]). U slučaju primjene teorema 6.2.1 na sustav jednadžbi

$$(k+1)x^2-(k-1)y^2=2,\ (16k^3-4k)x^2-(k-1)z^2=16k^3-5k+1,$$

uvjet $L>1$ nije zadovoljen za dovoljno velike k. S druge strane, ako se isti teorem pokuša primijeniti na sustav

$$(16k^3-4k)y^2-(k+1)z^2=16k^3-5k-1,\ (16k^3-4k)x^2-(k-1)z^2=16k^3-5k+1,$$

ograda za $|z|$ koju bismo dobili ne bi bila polinomijalna (jer je $\lambda>2$ za $|k|>1.9$). Ipak, primjenom Baker-Wüstholzovog teorema 4.1.5 problem nadopunjenja trojke $\{k-1, k+1, 16k^3-4k\}$ do četvorke može se riješiti djelomično, za $|k|>5\cdot 10^{37}$. Navedena trojka može se nadopuniti elementima $d\in\{4k, 64k^5-48k^3+8k\}$.

Vratimo se na problem veličine Diofantovih m-torki u prstenu $\mathbb{Z}[i]$. Koristeći Teorem Jadrijević-Ziegler 6.2.1 i princip rupa, Adzaga je u [2] pokazao da ne postoji Diofantova m-torka za $m\geq 43$ u prstenu cijelih brojeva imaginarnog kvadratnog polja.

Poglavlje 7

Diofantove m-torke sa svojstvom $D(n)$

7.1 Definicija. Pregled rezultata

U prethodnim poglavljima bavili smo se Diofantovim m-torkama, tj. skupovima sa svojstvom da umnožak svaka dva elementa uvećan za 1 (jedinicu iz prstena) daje puni kvadrat. Jedno od mogućih poopćenja ovog pojma jest zamijeniti *jedinicu* s nekim drugim elementom prstena. O takvim skupovima reći ćemo nešto u ovom dijelu.

Definicija 7.1.1. *Neka je $\mathcal{R}$ komutativni prsten s jedinicom, $m \in \mathbb{N}$ te $n \in \mathcal{R}$. Skup $\{a_1, \ldots, a_m\} \in \mathcal{R}$ sa svojstvom da je umnožak bilo koja dva elementa uvećan za n jednak potpunom kvadratu nekog elementa iz $\mathcal{R}$ naziva se* skup sa svojstvom $D(n)$.

Skup sa svojstvom $D(n)$ iz $\mathcal{R}\backslash\{0\}$ naziva se Diofantova m-torka sa svojstvom $D(n)$ *u prstenu $\mathcal{R}$ ili kraće $D(n)$-m-torka.*

Kao i do sada, i ovdje se postavlja pitanje koliko veliki ti skupovi mogu biti. Uočimo najprije da je $D(n)$-par u nekom prstenu $\mathcal{R}$ uvijek moguće nadopuniti do $D(n)$-trojke. Zaista, ako je $\{a, b\} \subset \mathcal{R}$ takav da je $ab + n = r^2$, onda je $\{a, b, a + b + 2r\}$ $D(n)$-trojka (uz uvjet da $a + b + 2r \notin \{0, a, b\}$). Što se tiče postojanja $D(n)$-četvorke, ona ne mora postojati za svaki n. No, krenimo redom i za početak pretpostavimo da je $\mathcal{R} = \mathbb{Z}$. Sljedeću tvrdnju pokazali su 1985. neovisno jedni o drugima Brown, Gupta i Singh, te Mohanty i Ramasamy (vidi [9, 45, 51]):

Teorem 7.1.2. *Neka je $n = 4k + 2$ za cijeli broj k. Tada ne postoji $D(n)$-četvorka u $\mathbb{Z}$.*

Nešto kasnije u [13] Dujella pokazuje da je u $\mathbb{Z}$ moguće konstruirati $D(n)$-četvorku ako $n \neq 4k + 2$, osim u konačno mnogo slučajeva.

Teorem 7.1.3 (Dujella, 1993.)**.** *Ako cijeli broj n nije oblika $4k+2$ i $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$, onda postoji $D(n)$-četvorka u $\mathbb{Z}$.*

Dujella je dokaz prethodnog teorema bazirao na konstrukciji tzv. *polinomijalnih formula* za $D(n)$-četvorke. Vrlo korisnom i praktičnom pokazala se formula, odnosno polinomijalni skup sa svojstvom $D(2m(2k + 1) + 1)$:

$$\{m, m(3k + 1)^2 + 2k, m(3k + 2)^2 + 2k + 2, 9m(2k + 1)^2 + 8k + 4\}. \tag{7.1}$$

Uz uvjet da je svaki od elemenata skupa (7.1) različit od 0, dobit ćemo $D(2m(2k+1)+1)$-četvorku. Nultočke nekog od polinoma (elementa) skupa (7.1) upravo su izuzetci pobrojani u teoremu 7.1.3 (skup S).

Teoremi 7.1.2 i 7.1.3 daju sljedeću karakterizaciju cjelobrojnih $D(n)$-četvorki:

Teorem 7.1.4. *Neka je n cijeli broj i $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$. Tada postoji $D(n)$-četvorka u $\mathbb{Z}$ ako i samo ako $n \not\equiv 2 \pmod 4$.*

Zanimljivo je uočiti da se svaki cijeli broj n može zapisati kao razlika kvadrata dva cijela broja ako i samo ako je $n \not\equiv 2 \pmod 4$, pa se stoga karakterizacija iz teorema 7.1.4 može izreći kao:

Teorem 7.1.5. *Postoji $D(n)$-četvorka u $\mathbb{Z}$ ako i samo ako je n razlika kvadrata dva cijela broja, do na elemente skupa S.*

Elemente skupa S nazivamo *izuzetcima* i nije poznato postoji li $D(n)$-četvorka u $\mathbb{Z}$ za $n \in S$. Sluti se da ne postoji, a tome u prilog idu mnogi radovi koji se bave prominentnim slučajem za $n = -1$, odnosno tzv. $D(-1)$-slučajem. O njemu će biti riječi u odjeljku 7.2.

Slutnja 7.1.6. *Ako je $n \in S$, onda ne postoji $D(n)$-četvorka u $\mathbb{Z}$*

Što se tiče gornje granice za veličinu skupova sa svojstvom $D(n)$, za sada nije poznata apsolutna gornja granica. Ipak, poznato je da su takvi skupovi konačni. Uz oznaku

$$M_n = \sup\{|D| \,:\, D \subset \mathbb{Z},\ D \text{ ima svojstvo } D(n)\}$$

Dujella je u [17, 25] pokazao da vrijedi

$$M_n \leq 31,\ |n| \leq 400,$$

$$M_n < 15.476 \log |n|,\ |n| > 400.$$

U [6] je taj rezultat poboljšan. Preciznije, dokazano je kako je $M_n < 2.6071 \log |n|$ za dovoljno velike $|n|$. Nadalje, Dujella i Luca [21] dokazali su kako vrijedi $M_p < 3 \cdot 2^{168}$ za sve proste brojeve p, te da za skoro sve n vrijedi $M_n < \log\log |n|$.

Na kraju recimo još ponešto o $D(n)$-četvorkama u nekim drugim prstenima. Uočimo da formula (7.1) implicira postojanje četveročlanog skupa sa svojstvom $D(n)$ u svakom prstenu. Pokazano je da se u prstenima cijelih brojeva nekih kvadratnih polja te određenog kubičnog ($\mathbb{Q}(\sqrt[3]{2})$) i kvartičnog polja ($\mathbb{Q}(\sqrt{2}, \sqrt{3})$) može pokazati analogna tvrdnja iz teorema 7.1.5 ([37, 38, 39, 40]). To bi upućivalo na slutnju:

Slutnja 7.1.7. *Neka je $\mathcal{R}$ komutativan prsten s jedinicom i $n \in \mathcal{R}$. $D(n)$-četvorka postoji ako i samo ako je $n = u^2 - v^2$ za neke $u, v \in \mathcal{R}$, do na konačno mnogo mogućih izuzetaka.*

Za sada nije poznato kako prethodnu slutnju „napasti" općenito jer su se dokazi u specifičnim prstenima bazirali na karakterizaciji elemenata prstena koji se mogu reprezentirati kao razlika kvadrata te polinomijalnim formulama (uglavnom (7.1)). U odjeljku 7.3 opisat ćemo strategiju dokaza slutnje u specifičnom prstenu $\mathbb{Z}[\sqrt{d}]$, za neke d.

7.2 $D(-1)$-m-torke

Kao što smo naveli u prethodnom odjeljku, sluti se kako ne postoji $D(-1)$-četvorka[1]. Ovdje ćemo dati kratki prikaz rezultata koji podupiru tu slutnju.

Prvi važan korak u tom smjeru napravili su Dujella i Fuchs [20], koji su dokazali da ako je $\{a, b, c, d\}$ $D(-1)$-četvorka za koju vrijedi $a < b < c < d$, onda je $a = 1$. Ideja proširenja trojke do četvorke slična je kao i u slučaju $D(1)$. Naime, neka je $\{a, b, c\}$ $D(-1)$-trojka za koju vrijedi $a < b < c$ i neka su r, s i t prirodni brojevi tako da je

$$ab - 1 = r^2,\ ac - 1 = s^2,\ bc - 1 = t^2.$$

Ako želimo tu trojku proširiti s elementom d, postoje cijeli brojevi x, y i z za koje vrijedi

$$ad - 1 = x^2,\ bd - 1 = y^2,\ cd - 1 = z^2.$$

Eliminirajući d dobivamo sustav simultanih Diofantskih jednadžbi

$$az^2 - cx^2 = c - a,$$

$$bz^2 - cy^2 = c - b.$$

Analogno kao u slučaju $D(1)$ može se dokazati da ako su (z, x) i (z, y) nenegativna rješenja danog sustava, onda vrijedi

$$z\sqrt{a} + x\sqrt{c} = (z_0\sqrt{a} + x_0\sqrt{c})(s + \sqrt{ac})^{2m},$$

$$z\sqrt{b} + y\sqrt{c} = (z_1\sqrt{a} + y_1\sqrt{c})(t + \sqrt{bc})^{2n},$$

za cijele brojeve $m, n \geq 0$. Ovdje su (z_0, x_0) i (z_1, y_1) fundamentalna rješenja danih jednadžbi i za njih vrijedi

$$0 \leq |x_0| < s,$$

$$0 < z_0 < c,$$

$$0 \leq |y_1| < t,$$

$$0 < z_1 < c.$$

Znači, ovdje rješavamo konačan broj Diofantskih jednadžbi $z = v_m = w_n$, gdje su binarno rekurzivni nizovi (v_m) i (w_n) dani s

$$v_0 = z_0,\ v_1 = (2ac - 1)z_0 + 2scx_0,\ v_{m+2} = (4ac - 2)v_{m+1} - v_m,$$

$$w_0 = z_1,\ w_1 = (2bc - 1)z_1 + 2tcy_1,\ w_{n+2} = (4bc - 2)w_{n+1} - w_n.$$

Iz kongruencija

$$v_m \equiv (-1)^m z_0 \pmod{2c},$$

$$w_n \equiv (-1)^n z_1 \pmod{2c},$$

koje se lako dokažu indukcijom, slijedi $z_0 = z_1$ i $m \equiv n \pmod 2$. Sada smo spremni dokazati kako u $D(-1)$-četvorki najmanji element mora biti 1.

[1] dokaz je nedavno najavljen u [8]

Teorem 7.2.1. *Neka je $\{a, b, c, d\}$ $D(-1)$-četvorka za koju vrijedi $a < b < c < d$. Tada je $a = 1$.*

Dokaz. Pretpostavimo da postoji takva četvorka gdje je $a \neq 1$. Tada postoji takva četvorka gdje d ima najmanju moguću vrijednost. Promotrimo takvu četvorku. Iz maloprije napisanih kongruencija, te zato što nas zanimaju samo rješenja x, y i z koja će dati proširenje do četvorke s $d \in \mathbb{N}$, imamo

$$cd - 1 = z^2 \equiv z_0^2 \equiv z_1^2 \equiv -1 \pmod{c}.$$

Znači, $z_0 = z_1$ i

$$z_0^2 \equiv -1 \pmod{c}.$$

Tada postoji cijeli broj

$$d_0 = \frac{z_0^2 + 1}{c} = \frac{z_0^2 + 1}{c}$$

i vrijedi

$$ad_0 - 1 = x_0^2,\ bd_0 - 1 = y_1^2,\ cd_0 - 1 = z_0^2,$$

odnosno skup $\{a, b, c, d_0\}$ ima svojstvo $D(-1)$. No iz ocjena za z_0 i z_1 imamo $d_0 < c$ pa iz pretpostavke minimalnosti od d zaključujemo da $\{a, b, c, d_0\}$ nije „prava" $D(-1)$-četvorka, što je moguće samo ako imamo dva jednaka elementa, a to je u slučaju kad njihov umnožak umanjen za 1 mora biti kvadrat moguće samo kad je $a = d_0 = 1$. □

Sada nam ostaje da promotrimo proširenje $D(-1)$-trojke $\{1, b, c\}$, gdje je $b < c$ do četvorke. Ako bi postojala takva četvorka $\{1, b, c, d\}$ za koju vrijedi $b < c < d$, ponovo možemo pretpostaviti da promatramo takvu četvorku za koju je vrijednost od d minimalna. Iz dokaza prošlog teorema, gdje smo pokazali da je u tom slučaju $d_0 = 1$, ako promatramo proširenje naše trojke do četvorke s većim elementom, imamo sljedeću lemu koja nam daje vrijednosti za fundamentalna rješenja:

Lema 7.2.2. *Neka su cijeli brojevi z_0, x_0, z_1 i y_1 definirani kao prije. Tada vrijedi*

$$z_0 = z_1 = \sqrt{c-1} = s,\ x_0 = 0,\ y_1 = \pm\sqrt{b-1} = \pm r.$$

Sada ćemo krenuti prema skici dokaza da postoji samo konačno mnogo $D(-1)$-četvorki, što je napravljeno u [19]. Dokaz je sličan kao u $D(1)$ slučaju, pa nećemo sve raspisivati, ali napomenut ćemo metode koje se koriste. Naime, i ovdje želimo pokazati da $z = v_m = w_n$ može imati rješenje samo za male indekse i to u ovom slučaju $z = v_0 = w_0 = s$, što daje $d = 1$. Kako u četvorki ne dozvoljavamo iste elemente, a ni ne vrijedi $c < d$, to nije rješenje koje nas zanima. Ali kada bismo dokazali da je to jedino rješenje, slijedilo bi da ne postoji $D(-1)$-četvorka.

Indukcijom se može dokazati

$$v_m \equiv (-1)^m(z_0 - 2cm^2 z_0 - 2csmx_0) \pmod{8c^2},$$
$$w_n \equiv (-1)^n(z_1 - 2bcn^2 z_1 - 2ctny_1) \pmod{8c^2},$$

što povlači da ako je $v_m = w_n$, onda vrijedi

$$m^2 z_0 + smx_0 \equiv bn^2 z_1 + tny_1 \pmod{4c},$$

odnosno

$$m^2 s \equiv bsn^2 + rtn \pmod{4c}.$$

To nam, zajedno s $n \leq m \leq 2n$, uz pretpostavku da postoji neka rupa između b i c, daje donju ogradu za n u ovisnosti o c. Tu se koriste metode kongruencija.

Lema 7.2.3. *Ako je $v_m = w_n$, $n \neq 0, 1$ i $c \geq 11b^6$, onda vrijedi $n > c^{\frac{1}{6}}$.*

Lema 7.2.4. *Ako je $v_m = w_n$, $n \neq 0, 1$ i $b^3 \leq c < 11b^6$, onda vrijedi $n > c^{\frac{1}{12}}$.*

Lema 7.2.5. *Ako je $v_m = w_n$, $n \neq 0, 1$, $b^{1.1} \leq c < b^3$ i $c > 10^{100}$, onda vrijedi $n \geq c^{0.04}$.*

Lema 7.2.6. *Ako je $v_m = w_n$, $n \neq 0, 1, 2$, $3b < c < b^{1.1}$, onda vrijedi $n \geq 0.25 \cdot c^{0.2}$.*

S ovim su lemama pokriveni svi slučajevi osim $c = a + b + 2r$, jer kao i u slučaju $n = 1$, ovdje vrijedi sličan rezultat: ili je $c = a + b + 2r$, ili je $c > 3b$. Kako je ovdje $a = 1$ i $b - 1 = r^2$, vidimo da je b oblika $b = r^2 + 1$ za neki prirodan broj r. U tom ćemo slučaju $c = 1 + b + 2r$, našu trojku $\{1, b, c\}$ zapisati parametarski

$$\{1, k^2 + 1, (k + 1)^2 + 1\}$$

i za nju vrijedi sljedeća lema:

Lema 7.2.7. *Ako je $v_m = w_n$, $n \neq 0, 1$, onda vrijedi $4n^2 > k$.*

Također spomenimo da se $n \leq m \leq 2n$ dobije iz

$$(c - 1)(4c - 3)^{m-1} < v_m < 4c^2(4c - 2)^{m-1},$$
$$(c - b)(4bc - 3)^{n-1} < w_n < 4bc^2(4bc - 2)^{n-1},$$

što se dokaže indukcijom za $m, n \geq 1$. Nadalje, lako se pokaže da vrijedi

$$v_1 \neq w_1,\ v_2 \neq w_2,\ v_4 \neq w_2.$$

Sada po slučajevima, u ovisnosti kolika je rupa između elemenata b i c, možemo dobiti gornju ogradu za elemente u eventualnoj četvorki.

Ako je $c \geq 11b^6$, koristimo hipergeometrijsku metodu. Naime, ako definiramo brojeve

$$\theta_1 = \frac{s\sqrt{b}}{t} = \sqrt{1 + \frac{1 - b}{t^2}},$$
$$\theta_2 = \frac{\sqrt{bc}}{t} = \sqrt{1 + \frac{1}{N}},$$

može se dokazati sljedeća lema:

Lema 7.2.8.

$$\max\left\{\left|\theta_1 - \frac{bsx}{ty}\right|, \left|\theta_2 - \frac{bz}{ty}\right|\right\} < \frac{b - 1}{y^2}.$$

Dokaz. Imamo

$$\left|\theta_1 - \frac{bsx}{ty}\right| = \frac{s\sqrt{b}}{t}\left|1 - \frac{x\sqrt{b}}{y}\right| = \frac{s\sqrt{b}}{t}\left|1 - \frac{bx^2}{y^2}\right| \cdot \left|1 + \frac{x\sqrt{b}}{y}\right|^{-1} < \frac{b - 1}{y^2},$$

$$\left|\theta_2 - \frac{bz}{ty}\right| = \frac{1}{t}\left|\sqrt{bc} - \frac{bz}{y}\right| = \frac{b}{t}\left|c - \frac{bz^2}{y^2}\right| \cdot \left|\sqrt{bc} + \frac{bz}{y}\right|^{-1} <$$
$$< \frac{b}{t} \cdot \frac{c - b}{y^2} \cdot \frac{1}{2\sqrt{bc}} < \frac{1}{2y^2} \cdot \frac{bc - 1}{\sqrt{bc(bc - 1)}} < \frac{b - 1}{y^2}.$$

□

Navedenu gornju ogradu možemo kombinirati s donjom ogradom dobivenom hipergeometrijskom metodom (teoremi Rickerta i Benneta), ali za to nam treba uvjet $c \geq 11b^6$, te dobivamo sljedeću propoziciju:

Propozicija 7.2.9. *Neka je $\{1, b, c\}$ $D(-1)$-trojka za koju vrijedi $1 < b < c$. Ako je $c \geq 11b^6$, onda ne postoji $D(-1)$-četvorka $\{1, b, c, d\}$ za koju vrijedi $d > c$.*

U preostalim slučajevima koristimo linearne forme u logaritmima (teoremi Matveeva). Naime, standardnim metodama možemo dokazati:

Lema 7.2.10. *Ako vrijedi $v_m = w_n$, $n \neq 0$, onda je*

$$0 < 2n \log(t + \sqrt{bc}) - 2m \log(s + \sqrt{c}) + \log \frac{s\sqrt{b} \pm r\sqrt{c}}{2\sqrt{b}} < (3.96bc)^{-n+1}.$$

Kombinirajući to s donjom ogradom za linearnu formu u logaritmima te donjom ogradom za n u ovisnosti o c, dobit ćemo gornju ogradu za n i c. Tada imamo gornju ogradu i za element

$$d = \frac{w_n^2 - 1}{c}.$$

Teorem 7.2.11. *Neka je $\{1, b, c, d\}$ $D(-1)$-četvorka za koju vrijedi $1 < b < c < d$. Tada vrijedi*

$$d < 10^{10^{23}}.$$

Spomenimo na kraju ovog odjeljka da i tu postoji gornja ograda za broj $D(-1)$-četvorki. Trenutno najbolja poznata [50] je da postoji najviše $3.713 \cdot 10^{58}$ $D(-1)$-četvorki. Ta ograda je naravno prevelika da bi se preostali slučajevi (u toj ogradi su sadržane i ograde za veličinu elemenata) provjerili računalnim programom. No u $D(-1)$ slučaju ipak je dokazano kako ne postoji $D(-1)$-četvorka oblika $\{1, b, c, d\}$ gdje je $c = 1 + b + 2r$ ([8]).

7.3 $D(n)$-četvorke u prstenima cijelih brojeva kvadratnog polja

Neka je d kvadratno slobodan prirodan broj, takav da je $d \equiv 3 \pmod 4$. U tom je slučaju prsten cijelih brojeva kvadratnog polja $\mathbb{Q}(\sqrt{d})$ jednak

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \,:\, a, b \in \mathbb{Z}\}.$$

Označimo s $\mathcal{R}_\square$ skup svih elemenata iz $\mathbb{Z}[\sqrt{d}]$ koji se mogu prikazati kao razlika kvadrata dva elementa iz $\mathbb{Z}[\sqrt{d}]$, tj.

$$\mathcal{R}_\square = \{n \in \mathbb{Z}[\sqrt{d}] \,:\, n = a^2 - b^2, a, b \in \mathbb{Z}[\sqrt{d}]\}.$$

Dokaz slutnje 7.1.7 u prstenu $\mathbb{Z}[\sqrt{d}]$ provest ćemo u tri koraka:

(i) Karakterizacija svih elemenata iz $\mathcal{R}_\square$.

(ii) Nepostojanje $D(n)$-četvorke za sve $n \in \mathbb{Z}[\sqrt{d}] \backslash \mathcal{R}_\square$.

(iii) Efektivna konstrukcija $D(n)$-četvorke pomoću polinomijalnih formula za sve $n \in \mathcal{R}_\square$.

Korak (i): Pokazuje se da reprezentabilnost nekih cijelih brojeva kao razlike kvadrata ne ovisi o d, no potpunu karakterizaciju skupa $\mathcal{R}_\square$ možemo dati samo za d koji zadovoljavaju neke dodatne uvjete. Ti dodatni uvjeti vezuju se uz rješivost nekih pelovskih jednadžbi. Sljedeći teorem u potpunosti opisuje skup $\mathcal{R}_\square$ u $\mathbb{Z}[\sqrt{d}]$ za neke $d \equiv 3 \pmod 4$.

Teorem 7.3.1. *Neka je $d \equiv 3 \pmod 4$ te neka je jedna od jednadžbi $x^2 - dy^2 = \pm 2$ rješiva. Tada se $n \in \mathbb{Z}[\sqrt{d}]$ može prikazati kao razlika kvadrata dvaju elementa iz $\mathbb{Z}[\sqrt{d}]$ ako i samo ako je n jednog od sljedećih oblika*

$$2u + 1 + 2v\sqrt{d},\ 4u + 4v\sqrt{d},\ 4u + (4v+2)\sqrt{d},\ 4u + 2 + 4v\sqrt{d},\ u, v \in \mathbb{Z}.$$

Skica dokaza. Lako se pokaže da $n = u + (2v+1)\sqrt{d} \notin \mathcal{R}_\square$. Nadalje, vrijede relacije

$$2u + 1 + 2v\sqrt{d} = (u + 1 + v\sqrt{d})^2 - (u + v\sqrt{d})^2,$$
$$4u + 4v\sqrt{d} = (u + 1 + v\sqrt{d})^2 - (u - 1 + v\sqrt{d})^2.$$

Još nam preostaje ispitati jesu li brojevi oblika

$$4u + (4v+2)\sqrt{d}, \quad (4u+2) + 4v\sqrt{d}, \quad (4u+2) + (4v+2)\sqrt{d}$$

elementi skupa $\mathcal{R}_\square$ ili nisu. Pokazuje se da pretpostavka $(4u+2) + (4v+2)\sqrt{d} \in \mathcal{R}_\square$ povlači $d \equiv 1$ ili $2 \pmod 4$. Stoga, $(4u+2) + (4v+2)\sqrt{d} \notin \mathcal{R}_\square$.

Pretpostavimo da je $4u + (4v+2)\sqrt{d} \in \mathcal{R}_\square$ za sve $u, v \in \mathbb{Z}$. Stoga iz

$$4u + (4v+2)\sqrt{d} = (x_1 + y_1\sqrt{d})^2 - (x_2 + y_2\sqrt{d})^2, \tag{7.2}$$

gdje su $x_1, x_2, y_1, y_2 \in \mathbb{Z}$, zbog $d \equiv 3 \pmod 4$ slijedi

$$x_1 \equiv y_1 \pmod 2,\ x_2 \equiv y_2 \pmod 2,\ x_1 \not\equiv x_2 \pmod 2.$$

Neka su $\alpha, \beta \in \mathbb{Z}$ takvi da je $x_1 = x_2 + \alpha$ i $y_1 = y_2 + \beta$. Očito su α, β neparni. Uvrštavanjem u (7.2) dobivamo

$$\begin{aligned} \alpha x_2 + d\beta y_2 &= 2u - \tfrac{\alpha^2 + d\beta^2}{2}, \\ \beta x_2 + \alpha y_2 &= 2v + 1 - \alpha\beta. \end{aligned} \tag{7.3}$$

Jednakosti u (7.3) možemo shvatiti kao sustav linearnih jednadžbi u nepoznanicama x_2 i y_2. Taj sustav mora imati cjelobrojno rješenje za sve $u, v \in \mathbb{Z}$. Za $u = v = 0$ i pripadne α_0, β_0 rješenje sustava (7.3) glasi:

$$x_2 = -\left(\frac{\alpha_0^2 - d\beta_0^2}{2}\alpha_0 + d\beta_0\right)/(\alpha_0^2 - d\beta_0^2),\ y_2 = \left(\frac{\alpha_0^2 - d\beta_0^2}{2}\beta_0 + \alpha_0\right)/(\alpha_0^2 - d\beta_0^2).$$

Otuda vidimo da $\alpha_0^2 - d\beta_0^2 \mid 2d\beta_0$ i $\alpha_0^2 - d\beta_0^2 \mid 2\alpha_0$. Zbog neparnosti brojeva α_0 i β_0 može se pokazati da Pellova jednadžbe $x^2 - dy^2 = 1$ ima rješenja u parnom x i neparnom y. Neka su sada $u, v \in \mathbb{Z}$ takvi da je $(2u)^2 - d(2v+1)^2 = 1$. Za pripadne $\alpha, \beta \in \mathbb{Z}$ pokazuje se da vrijedi $\alpha^2 - d\beta^2 = \pm 2$.

Obratno, ako su $\alpha, \beta \in \mathbb{Z}$ takvi da vrijedi $\alpha^2 - d\beta^2 = \pm 2$, onda sustav (7.3) ima rješenje $(x_2, y_2) \in \mathbb{Z}^2$. Sada se lako provjeri da vrijedi (7.2) za $x_1 + y_1\sqrt{d} = x_2 + \alpha + (y_2 + \beta)\sqrt{d}$. Ovime smo dokazali tvrdnju da se *cijeli brojevi oblika $4u + (4v+2)\sqrt{d}$ mogu prikazati kao razlika kvadrata dva broja iz $\mathbb{Z}[\sqrt{d}]$ ako i samo ako jedna od jednadžbi $x^2 - dy^2 = \pm 2$ ima rješenja.*

Pokazuje se da potpuno analogna tvrdnja vrijedi i za cijele brojeve oblika $4u + 2 + 4v\sqrt{d}$. $\square$

Detalji prethodnog dokaza kao i karakterizacije razlika kvadrata za neke druge oblike broja d mogu se naći u [28]. Napomenimo još da je za $d \neq 2$ rješiva najviše jedna od jednadžbi $x^2 - dy^2 = 2$, $x^2 - dy^2 = -2$.

Korak (ii): Prema teoremu 7.3.1 je

$$\mathbb{Z}[\sqrt{d}]\backslash\mathcal{R}_{\square} = \{u + (2v+1)\sqrt{d}, 4u + 2 + (4v+2)\sqrt{d} \,:\, u, v \in \mathbb{Z}\}.$$

Mogu se pokazati i nešto općenitije tvrdnje:

Teorem 7.3.2. *Neka su $d, u, v \in \mathbb{Z}$, $|d|$ nije potpuni kvadrat. Tada ne postoji $D(u+(2v+1)\sqrt{d})$-četvorka u $\mathbb{Z}[\sqrt{d}]$. Ako je $d \equiv 3 \pmod 4$, onda ne postoji $D(4u+2+(4v+2)\sqrt{d})$-četvorka u $\mathbb{Z}[\sqrt{d}]$.*

Iskazani teorem dokazuje se metodom kontradikcije. Pretpostavka o postojanju $D(n)$-četvorke za $n \notin \mathcal{R}_{\square}$ implicira nekonzistentne sustave kongruencija modulo 4.

Korak (iii): Za efektivnu konstrukciju $D(n)$-četvorki koriste se sljedeće leme koje vrijede u proizvoljnom komutativnom prstenu s jedinicom $\mathcal{R}$:

Lema 7.3.3 (Dujella, 1996.)**.** *Neka su $\mu, \kappa \in \mathcal{R}$. Skup*

$$\{\mu, (3\kappa+1)^2\mu + 2\kappa, (3\kappa+2)^2\mu + 2\kappa + 2, 9(2\kappa+1)^2\mu + 8\kappa + 4\} \tag{7.4}$$

ima svojstvo $D(2\mu(2\kappa+1)+1)$.

Podsjećamo da pojam *skup ima svojstvo $D(n)$* znači da su svi umnošci elemenata tog skupa uvećani za n jednaki potpunom kvadratu u prstenu, ali nije isključeno da su neka dva elementa jednaka ili da je neki od elemenata jednak nuli. Stoga su skupovi sa svojstvom $D(n)$ *dobri kandidati* za $D(n)$-četvorke. U [14] može se pronaći još primjera takvih skupova, a opisana je i tehnika pomoću kojih su oni izvedeni.

Lema 7.3.4. *Ako je $\{n_1, n_2, n_3, n_4\} \subset \mathcal{R}$ skup sa svojstvom $D(n)$, onda je $\{n_1 w, n_2 w, n_3 w, n_4 w\}$ skup sa svojstvom $D(nw^2)$ za svaki $w \in \mathcal{R}$.*

Tvrdnja prethodne leme slijedi direktno iz definicije skupa sa svojstvom $D(n)$.

Sada pokušavamo pronaći efektivne vrijednosti za $\mu, \kappa, w \in \mathbb{Z}[\sqrt{d}]$ iz gornjih lema takve da se određena klasa brojeva iz $\mathcal{R}_{\square}$ može prikazati u obliku oblika $(2\mu(2\kappa+1)+1)w^2$. Često se μ fiksira i vrlo je poželjno da je male norme (npr. 1 ili 2). Pokazat ćemo najjednostavniji slučaj:

Propozicija 7.3.5. *Neka je $d \in \mathbb{N}$ kvadratno slobodan, $d \equiv 3 \pmod 4$ te neka je jedna od jednadžbi $x^2 - dy^2 = \pm 2$ rješiva. Postoji beskonačno mnogo $D(4u+3+4v\sqrt{d})$-četvorki u $\mathbb{Z}[\sqrt{d}]$*

Skica dokaza. Za $\mu = 1$ i $\kappa = u + v\sqrt{d}$ formula (7.4) predstavlja skup sa svojstvom $D(4u+3+4v\sqrt{d})$, odnosno

$$\{1, 9\kappa^2 + 8\kappa + 1, 9\kappa^2 + 14\kappa + 6, 36\kappa^2 + 44\kappa + 13\} \tag{7.5}$$

je $D(4u+3+4v\sqrt{d})$-četvorka za sve $u, v \in \mathbb{Z}$ i $4u + 3 + 4v\sqrt{d} \notin \{3, 7, -1, 11, 15\}$.

Štoviše, možemo pokazati da postoji beskonačno $D(4u+3+4v\sqrt{d})$-četvorki u $\mathbb{Z}[\sqrt{d}]$ te da izuzetaka nema. Uočimo da iz pretpostavke da jedna od jednadžbi $x^2 - dy^2 = \pm 2$ rješiva slijedi da Pellova jednadžba $x^2 - dy^2 = 1$ rješiva u parnom x i neparnom y. Zaista, ako za neke

$x_1, y_1 \in \mathbb{Z}$ vrijedi $x_1^2 - dy_1^2 = 2$ (ili $x_1^2 - dy_1^2 = -2$), onda je $(x_1^2 - 1, x_1y_1)$ (ili $(x_1^2 + 1, x_1y_1)$) rješenje pripadne Pellove jednadžbe s odgovarajućim parnostima jer su x_1, y_1 neparni. Neka je $w = s + t\sqrt{d}$ rješenje jednadžbe $x^2 - dy^2 = 1$ u parnom s i neparnom t. Uočimo da broj $4u + 3 + 4v\sqrt{d}$ ne mijenja svoj oblik ako ga se pomnoži sa $(s + t\sqrt{d})^4$. Sada pretpostavimo da skupovi $\{c_1, c_2, c_3, c_4\}$ i $\{d_1, d_2, d_3, d_4\}$ predstavljaju $D(4u + 3 + 4v\sqrt{d})$-četvorku i $D((4u + 3 + 4v\sqrt{d})w)$-četvorku, redom, te da su oba skupa dobivena formulom (7.5). Prema lemi 7.3.4, skup $\{d_1(s-t\sqrt{d})^2, d_2(s-t\sqrt{d})^2, d_3(s-t\sqrt{d})^2, d_4(s-t\sqrt{d})^2\}$ je *nova* $D(4m+3+4n\sqrt{d})$-četvorka (različita od $\{c_1, c_2, c_3, c_4\}$). Budući da smo w izabrali kao rješenje Pellove jednadžbe, takvih četvorki je beskonačno mnogo. Koristeći analognu argumentaciju možemo dokazati postojanje $D(n)$-četvorke za $n \in \{3, 7, -1, 11, 15\}$. □

Kako se postupalo u ostalim slučajevima koraka (iii) može se pronaći u [37]. Stoga je za ovaj prsten provjerena slutnja 7.1.7.

Teorem 7.3.6. *Neka je $d \in \mathbb{N}$ kvadratno slobodan, $d \equiv 3 \pmod 4$ te neka je jedna od jednadžbi $x^2 - dy^2 = \pm 2$ rješiva. Za svaki $n \in \mathbb{Z}[\sqrt{d}]$ koji se može prikazati kao razlika kvadrata elemenata iz $\mathbb{Z}[\sqrt{d}]$ postoji beskonačno mnogo $D(n)$-četvorki u $\mathbb{Z}[\sqrt{d}]$. I obratno, ako postoji $D(n)$-četvorka u $\mathbb{Z}[\sqrt{d}]$, onda je n prikaziv kao razlika kvadrata elemenata iz $\mathbb{Z}[\sqrt{d}]$.*

Uvjete prethodnog teorema zadovoljava beskonačno mnogo $d \in \mathbb{N}$. Primjerice jednadžbe $x^2 - (4t^2 + 4t - 1)y^2 = 2$ i $x^2 - (4t^2 + 4t + 3)y^2 = -2$ imaju rješenja za svaki $t \in \mathbb{N}$.

Na kraju, opažamo da u prstenu $\mathbb{Z}[\sqrt{d}]$, uz uvjete teorema 7.3.6, ne postoji tzv. skup izuzetaka koji na primjer postoji u prstenima $\mathbb{Z}$ i $\mathbb{Z}[i]$. Kao što smo mogli mogli vidjeti iz skice dokaza propozicije 7.3.5, razlog *nepostojanju izuzetaka* jest u direktnoj vezi s brojem jedinica u konkretnom prstenu. Ako je grupa jedinica u prstenu beskonačnog reda, onda očekujemo da izuzetaka neće biti. S druge strane, ako je taj red konačan (kao npr. u prstenima imaginarnih kvadratnih polja), onda se pojavljuju izuzetci koje teško možemo riješiti standarnim metodama. Najpoznatiji primjer toga jest slutnja o nepostojanju $D(-1)$-četvorke u $\mathbb{Z}$ o kojem je bilo riječi u prethodnom odjeljku.

Bibliografija

[1] N. Adžaga, A. Filipin, Z. Franušić, *On the extensions of the Diophantine triples in Gaussian integers*, `https://arxiv.org/abs/1905.09332`

[2] N. Adžaga, *On the size of Diophantine m-tuples in imaginary quadratic number rings*, Bull. Math. Sci. 9(3) (2019) 1950020 (10 pages).

[3] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika 15 (1968), 204–216.

[4] A. Baker and H. Davenport, *The equations* $3x^2-2=y^2$ *and* $8x^2-7=z^2$, Quart. J. Math. Oxford Ser. (2) 20 (1969), 129–137.

[5] A. Bayad, A. Filipin, A. Togbé, *Extension of a parametric family of Diophantine triples in Gaussian integers*, Acta Math. Hungar. 148 (2016), 312-327.

[6] R. Becker and M. Ram Murty, *Diophantine m-tuples with the property* $D(n)$, Glas. Mat. Ser. III 54 (2019), 65–75.

[7] M.A. Bennett, *On the number of solutions of simultaneous Pell equations*, J. Reine Angew. Math. 498 (1998) 173–199.

[8] N. C. Bonciocat, M. Cipu, M. Mignotte, *There is no Diophantine* $D(-1)$*-quadruple*, `https://arxiv.org/abs/2010.09200`

[9] E. Brown, *Sets in which* $xy+k$ *is always a square*, Math. Comp. 45 (1985), 613–620.

[10] S. Bujačić, A. Filipin, *Linear forms in logarithms, in Diophantine Analysis: Course Notes from a Summer School* (J. Steuding, Ed.), Birkhäuser, Basel, 2016, pp. 1-59.

[11] Y. Bugeaud, *Linear Forms in Logarithms and Applications*, IRMA Lectures in Mathematics and Theoretical Physics Vol. 28, European Mathematical Society, Zürich, 2018.

[12] M. Cipu, T. Trudgian, *Searching for Diophantine quintuples*, Acta Arith. 173 (2016), 365–382.

[13] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arith. 65 (1993), 15–27.

[14] A. Dujella, *Some polynomial formulas for Diophantine quadruples*, Grazer Math. Ber. 328(1996), 25–30.

[15] A. Dujella, *The problem of the extension of a parametric family of Diophantine triples*, Publ. Math. Debrecen 51 (1997), 311–322.

[16] A. Dujella, *On Diophantine quintuples*, Acta Arith. 81 (1997), 69–79.

[17] A. Dujella, *On the size of Diophantine m-tuples*, Math. Proc. Cambridge Philos. Soc. 132 (2002), 23–33.

[18] A. Dujella, *Bounds for the size of sets with the property $D(n)$*, Glas. Mat. Ser. III 39 (2004), 199–205.

[19] A. Dujella, A. Filipin and C. Fuchs, *Effective solution of the $D(-1)$-quadruple conjecture*, Acta Arith. 128 (2007), 319–338.

[20] A. Dujella and C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. 71(2005), 33–52. ,

[21] A. Dujella and F. Luca, *Diophantine m-tuples for primes*, Int. Math. Res. Not. 47 (2005), 2913–2940.

[22] A. Dujella and A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2), 49 (1998), 291–306.

[23] A. Dujella, *An absolute bound for the size of Diophantine m-tuples*, J. Number Theory 89 (2001), 126–150.

[24] A. Dujella, *Diophantine m-tuples and elliptic curves*, J. Theor. Nombres Bordeaux 13 (2001), 111–124.

[25] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. 566 (2004), 183-214.

[26] A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. 29 (2004), 101–112.

[27] A. Dujella, *On the number of Diophantine m-tuples*, Ramanujan J. 15 (2008), 37–46.

[28] A. Dujella and Z. Franušić, *On differences of two squares in some quadratic fields*, Rocky Mountain J. Math. 37 (2007), 429–453.

[29] A. Dujella, *Rational Diophantine sextuples with mixed signs*, Proc. Japan Acad. Ser. A Math. Sci. 85 (2009), 27–30.

[30] A. Dujella, M. Kazalicki, M. Mikić and M. Szikszai, *There are infinitely many rational Diophantine sextuples*, Int. Math. Res. Not. IMRN 2017 (2) (2017), 490–508.

[31] A. Dujella and M. Kazalicki, *More on Diophantine sextuples*, in Number Theory - Diophantine problems, uniform distribution and applications, Festschrift in honour of Robert F. Tichy's 60th birthday (C. Elsholtz, P. Grabner, Eds.), Springer-Verlag, Berlin, 2017, pp. 227-235.

[32] A. Dujella, *Teorija brojeva*, Školska knjiga, 2019.

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

[34] C. Elsholtz, A. Filipin, Y. Fujita, *On Diophantine quintuples and $D(-1)$-quadruples*, Monatsh. Math., 175 (2) (2014), 227–239.

[35] A. Filipin, Y. Fujita, *The number of Diophantine quintuples II*, Publ. Math. Debrecen 82 (2013), 293–308.

[36] Z. Franušić, *On the extensibility of Diophantine triples $\{k-1, k+1, 4k\}$ for Gaussian integers*, Glasnik matematički 43 (2008) , 2, 265–291.

[37] Z. Franušić, *Diophantine quadruples in $\mathbb{Z}[\sqrt{4k+3}]$*, Ramanujan J. 17 (2008), 77–88.

[38] Z. Franušić, *A Diophantine problem in $Z[(1+\sqrt{d})/2]$*, Studia Sci. Math. Hungar. 46 (2009), 103–112.

[39] Z. Franušić, *Diophantine quadruples in the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$*, Miskolc Math. Notes 14 (2013), 893–903.

[40] Z. Franušić, B. Jadrijević, *$D(n)$-quadruples in the ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$*, Math. Slovaca 69 (2019), 1263–1278.

[41] Y. Fujita, *Any Diophantine quintuple contains a regular Diophantine quadruple*, J. Number Theory 129 (2009), 1678–1697.

[42] Y. Fujita, *The extensibility of Diophantine pairs $\{k-1, k+1\}$*, J. Number Theory 128 (2008), 322-353.

[43] Y. Fujita, *The number of Diophantine quintuples*, Glas. Mat. Ser. III 45 (2010), 15–29.

[44] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III 41 (2006), 195–203.

[45] H. Gupta and K. Singh, *On k-triad sequences*, Internat. J. Math. Math. Sci. 5 (1985), 799–804.

[46] B. He, A. Togbé, *On the $D(-1)$-triple $\{1, k^2+1, k^2+2k+2\}$ and its unique $D(1)$-extension*, J. Number Theory 131 (2011), 120–137.

[47] B. He, A. Togbé, V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. 371 (2019), 6665–6709.

[48] B. Jadrijević, V. Ziegler, *A system of relative Pellian equations and a related family of relative Thue equations*, Int. J. Number Theory, Vol. 2, No. 4 (2006), 569–590.

[49] B. W. Jones, *A second variation on a problem of Diophantus and Davenport*, Fibonacci Quart. 16 (1978), 155–165.

[50] K. Lapkova, *Explicit upper bound for the average number of divisors of irreducible quadratic polynomials*, Monatsh. Math. 186 (2018), 663–673.

[51] S. P. Mohanty and A. M. S. Ramasamy, *On $P_{r,k}$ sequences*, Fibonacci Quart. 23 (1985), 36–44.

[52] F. Najman, *Eliptičke krivulje nad poljima algebarskih brojeva*, `https://web.math.pmf.unizg.hr/~fnajman/elipticke.pdf`, Bilješke s predavanja (2013).

[53] J. H. Rickert, *Simultaneous rational approximations and related diophantine equations*, Math. Proc. of the Cambridge Philos. Soc. 113(1993), 461–472.

[54] W. M. Schmidt, Wolfgang M, *Norm form equations*, Annals of Mathematics, Second Series. 96 (3) (1972), 526–551.

[55] C.L. Siegel (pod pseudonimom X): *The integer solutions of the equation* $y^2 = ax_n + bx_{n-1} + \cdots + k$, J. London Math. Soc. 1 (1926), 66–68.

Kazalo