Diofantove m-torke u prstenima cijelih brojeva

Adžaga, Nikola

Sveučilište u Zagrebu

PRIRODOSLOVNO - MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Nikola Adžaga

Diofantove m-torke u prstenima cijelih brojeva

DOKTORSKI RAD

Zagreb, 2018.

University of Zagreb

FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS

Nikola Adžaga

Diophantine m-tuples in the rings of integers

DOCTORAL THESIS

Zagreb, 2018

Sveučilište u Zagrebu

PRIRODOSLOVNO - MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Nikola Adžaga

Diofantove m-torke u prstenima cijelih brojeva

DOKTORSKI RAD

Mentor:
prof. dr. sc. Alan Filipin

Zagreb, 2018.

University of Zagreb

FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS

Nikola Adžaga

Diophantine m-tuples in the rings of integers

DOCTORAL THESIS

Supervisor:
prof. dr. sc. Alan Filipin

Zagreb, 2018

Mentor:

prof. dr. sc. Alan Filipin
Sveučilište u Zagrebu,
Građevinski fakultet,
Zavod za matematiku,
Fra Andrije Kačića-Miošića 26, 10000 Zagreb
e-mail: filipin@grad.hr

Supervisor:

prof. dr. sc. Alan Filipin
University of Zagreb,
Faculty of Civil Engineering,
Department of Mathematics,
Fra Andrije Kačića-Miošića 26, 10000 Zagreb
e-mail: filipin@grad.hr

Sažetak

U radu se proučavaju Diofantove m-torke i $D(n)$-skupovi u prstenu cijelih brojeva $\mathbb{Z}$ i prstenu Gaussovih cijelih brojeva $\mathbb{Z}[i]$. Prvo, koristeći elementarne metode, promatramo proširivost parametarske familije $D(-2k^2)$-parova $\{2k^2, 2k^2+1\}$ u prstenu $\mathbb{Z}$. Pokazujemo da se svaki takav par može proširiti najviše do $D(-2k^2)$-četvorke.

Proučava se i naizgled sličan problem proširenja Diofantovih trojki iz jednoparametarske familije u Gaussovim cijelim brojevima. Zatim se bavimo općenitijim problemom pronalaženja gornje granice na veličinu Diofantove m-torke u Gaussovim cijelim brojevima. Dokazuje se prva uniformna gornja granica na veličinu Diofantove m-torke u Gaussovim cijelim brojevima; pritom se koriste rezultati iz diofantskih aproksimacija.

Konačno, koristeći eliptičke krivulje, ispitujemo postoji li beskonačno mnogo Diofantovih trojki koje su ujedno i $D(n)$-skup za više dodatnih prirodnih brojeva n različitih od 1.

Ključne riječi: Diofantove m-torke, $D(n)$-skupovi, Gaussovi cijeli brojevi, Pellove jednadžbe, diofantske aproksimacije, eliptičke krivulje

Zahvala

Autor je, tokom cijelog trajanja izrade ove disertacije, suradnik na projektu Hrvatske zaklade za znanost "Diofantove m-torke, eliptičke krivulje, Thueove i indeksne jednadžbe" (HRZZ-6422) voditelja akademika Andreja Dujelle.

Summary

This work studies Diophantine m-tuples and $D(n)$-sets in the ring of integers $\mathbb{Z}$ and in the ring of Gaussian integers $\mathbb{Z}[i]$. First, using elementary methods, we consider the extendibility of a parametric family of $D(-2k^2)$-pairs $\{2k^2, 2k^2+1\}$. We show that none such pair can be extended to a $D(-2k^2)$-quintuple.

We study the seemingly similar problem of extending Diophantine triples from another one-parametric family in Gaussian integers. Afterwards we deal with a more general problem of finding an upper bound on the size of Diophantine m-tuple in Gaussian integers. We prove the first upper bound on the size of Diophantine m-tuple in Gaussian integers; thereat, we use the results from Diophantine approximations.

Finally, by using elliptic curves, we consider if Diophantine triples can also be a $D(n)$-set for more additional positive integers n different from 1.

The outline of the thesis is as follows. In Chapter 1 ("Introduction") we introduce the Diophantine m-tuples and explain the objectives of this research.

Chapter 2 ("Preliminary results") gives the definitions and preliminary results regarding continued fractions, Pellian equations, Diophantine m-tuples, and elliptic curves. These results are used throughout the whole work.

In Chapter 3 ("The Extendibility of $D(-2k^2)$-pairs $\{2k^2, 2k^2+1\}$") we deal with the extendibility of $D(-2k^2)$-pairs $\{2k^2, 2k^2+1\}$. We show that each such pair can be extended at most up to a $D(-2k^2)$-quadruple and explicitly describe such extensions.

In Chapter 4 ("Family of Diophantine triples $\{k-1, k+1, 16k^3-4k\}$ in Gaussian integers") we study the problem of extending the triples from the chapter title. We have not been able to resolve this problem completely, but studying it helped us in the next chapter.

Chapter 5 ("Diophantine m-tuples in Gaussian integers") is in some way central to the whole thesis. We try to find a uniform upper bound on the size of Diophantine m-tuple in Gaussian integers. By using Diophantine approximations, we show that $m \leqslant 42$. We prove some results which might be used in lowering this bound, as well as in further research of parametric families of Diophantine triples in Gaussian integers. We also describe how our result could be generalized for obtaining an upper bound on the size of Diophantine m-tuples in the rings of integers of imaginary quadratic fields.

In Chapter 6 ("Diophantine triples with additional $D(n)$-properties") we deal with the question of how many $D(n)$-properties can one Diophantine triple have. Using elliptic curves, we construct an infinitely many Diophantine triples which are $D(n)$-sets for two additional positive integers n different from 1.

It is hard to overestimate the importance of computers in doing this research. Almost all results in Chapter 3 were proven using identities which were conjectured using Mathematica [46]. In Chapter 6, one of the constructions of infinitely many Diophantine triples which have two additional $D(n)$-properties was conjectured using a computer and The On-Line Encyclopedia of Integer Sequences [43]. In the same chapter, a significant amount of computing on elliptic curves was done with Sage [45].

Keywords: Diophantine m-tuples, $D(n)$-sets, Gaussian integers, Pell equations, Diophantine approximations, elliptic curves

Acknowledgement

The author was supported by the Croatian Science Foundation under the project no. 6422 (HRZZ-6422) "Diophantine m-tuples, elliptic curves, Thue and index form equations", led by Academician Andrej Dujella.

Sadržaj

Poglavlje 1

Uvod

Istraživanje Diofantovih m-torki traje barem od trećeg stoljeća i antičkog grčkog matematičara Diofanta iz Aleksandrije, u čijoj Aritmetici nalazimo prvi primjer racionalne četvorke brojeva takve da je produkt svaka dva različita elementa uvećan za 1 potpun kvadrat (kvadrat racionalnog broja). Njemu u čast takvi skupovi brojeva nazivaju se Diofantovim m-torkama.

Fermat je pronašao prvu cjelobrojnu Diofantovu četvorku $\{1, 3, 8, 120\}$, a Euler beskonačnu familiju takvih četvorki. U 20. stoljeću Baker i Davenport, koristeći Bakerovu teoriju linearnih formi u logaritmima, dokazuju da, ako je d prirodan broj takav da je $\{1, 3, 8, d\}$ Diofantova četvorka, onda d mora biti 120 [3]. Drugim riječima, skup $\{1, 3, 8\}$ se do Diofantove četvorke može proširiti na jedinstven način i tada dobivamo Fermatov primjer. Iz toga također slijedi i da se Fermatova četvorka ne može proširiti do Diofantove petorke. Prirodno pitanje je može li se neka druga četvorka proširiti do petorke, odnosno, koliko velika Diofantova m-torka može biti? Pojavila se slutnja da ne postoji Diofantova petorka, koja je motivirala brojna istraživanja. Vrlo nedavno prihvaćen je dokaz ove slutnje, za koji su zaslužni He, Togbé i Ziegler ([28]), pa je danas možemo smatrati teoremom.

Izuzimajući Bakerov rezultat, glavni doprinosi prema dokazivanju ovog teorema pojavljuju se tek u 21. stoljeću. Dujella je u [13] dokazao da Diofantova m-torka u prirodnim brojevima može imati najviše osam članova, a 2004. poboljšao je ovu granicu dokazavši da ne postoji Diofantova šestorka ([15]). Također je u istom radu pokazano da, ako Diofantove petorke postoje, ima ih konačno mnogo.

U međuvremenu, pojavio se niz modifikacija i poopćenja ovog problema. Prirodno poopćenje pojma Diofantove m-torke je u promjeni broja koji se dodaje: umjesto 1, može se dodavati i neki drugi broj. Tako ćemo za skup od m prirodnih brojeva $\{a_1, a_2, \ldots, a_{m-1}, a_m\}$ reći da ima $D(n)$-svojstvo ako je $a_i a_j + n$ potpun kvadrat za sve različite i i j iz skupa $\{1, \ldots, m\}$. Još jednostavnije, takav skup nazivamo $D(n)$-skupom. Npr. Fujita i Togbé u [23] promatrali su parametarsku familiju $D(-k^2)$-parova $\{k^2, k^2+1\}$. Elementarnim metodama pokazali su da se svaki par tog oblika može proširiti do $D(-k^2)$-četvorke na najviše jedan način. Direktno slijedi da se nikoji takav par ne može proširiti do $D(-k^2)$-petorke.

Problemi s $D(n)$-skupovima u cijelim brojevima često se mogu rješavati slično kao i analogni problemi s Diofantovim m-torkama. Tako je npr. Filipin u [17] pokazao da $D(4)$-skup ne može imati šest elemenata, i to na sličan način kako je pokazano da ne postoji Diofantova šestorka [15].

Diofant je promatrao ovaj problem u racionalnim brojevima i tu su pitanja još uvijek širom otvorena. Tek nedavno pronađena je beskonačna familija Diofantovih šestorki ([16]) i ne zna se postoji li uniformna gornja granica na veličinu takvog skupa u racionalnim brojevima. S druge strane, razumno je pretpostaviti da će prijelaz na analogne probleme u drugim prstenima cijelih brojeva biti lakši. Ipak, ni u takvom okruženju nema mnogo rezultata. Npr. u području analognih problema u prstenu Gaussovih cijelih brojeva pronalazimo manje od deset radova, od kojih možemo istaknuti [21] i [5], koji se bave problemom proširenja Diofantovih trojki iz jednoparametarskih familija, te [6] u kojem se proučava sličan tip problema s $D(4)$-trojkama. Zbog sličnosti ovog prstena s uobičajenim prstenom cijelih brojeva $\mathbb{Z}$, možemo očekivati da će vrijediti slični rezultati i da će se moći dokazati sličnim tehnikama kao u racionalnim cijelim brojevima.

U svim dosad spomenutim istraživanjima ispituje se moguća veličina Diofantove m-torke ili nekog $D(n)$-skupa. Međutim, logično pitanje je i postoji li Diofantova m-torka koja je također $D(n)$-skup za neki prirodan broj n različit od 1. Ovo pitanje 2001. godine postavili su Kihel i Kihel [33]. Oni su izrazili i slutnju da ne postoje Diofantove trojke koje su ujedno i $D(n)$-skup za neki n različit od 1. Ta slutnja ne vrijedi jer je, npr. $\{8, 21, 55\}$ i Diofantova trojka i $D(4321)$-trojka (primijećeno u MathSciNet recenziji njihovog članka, Dujella). Ovime se otvara pitanje postoji li takvih Diofantovih trojki beskonačno, te koliko različitih $D(n)$-svojstava može imati jedna Diofantova trojka.

Ova disertacija organizirana je na sljedeći način.

U Poglavlju 2 izlažemo osnovne pojmove i rezultate potrebne u ostatku rada. Napomenimo da ćemo iskaze značajnih teorema koje koristimo najčešće i ponoviti prije primjene u kasnijim poglavljima, kako bi ih se lakše pratilo.

U Poglavlju 3 bavimo se proširenjem $D(-2k^2)$-parova $\{2k^2, 2k^2+1\}$ i na elementaran način pokazujemo da se svaki takav par može proširiti na najviše jedan način do $D(-2k^2)$-četvorke. Većina rezultata ovog poglavlja objavljena je u koautorstvu s Filipinom u članku "On the extension of $D(-8k^2)$-pair $\{8k^2, 8k^2+1\}$" u Moscow Mathematical Journal [1].

U Poglavlju 4 proučavamo proširivost Diofantove trojke $\{k-1, k+1, 16k^3-4k\}$ u Gaussovim cijelim brojevima $\mathbb{Z}[i]$. Na tim rezultatima surađivala je Franušić. Taj problem nismo uspjeli u potpunosti razriješiti, ali proučavanje njega pomoglo nam je u daljnjem istraživanju.

Poglavlje 5 na neki način je središnje u disertaciji. U njemu se bavimo pitanjem koliko najviše elemenata može imati Diofantova m-torka Gaussovih cijelih brojeva, odnosno pronalaženjem gornje granice na veličinu m. Oslanjajući se na rezultate iz diofantskih aproksimacija, uspjeli smo dokazati da je $m \leqslant 42$. Dokazujemo i neke rezultate koji bi

se mogli iskoristiti u poboljšanju te granice, kao i u daljnjem istraživanju parametarskih familija Diofantovih trojki u Gaussovim cijelim brojevima. Također, opisujemo kako bi se taj rezultat mogao poopćiti za dobivanje gornje granice na veličinu Diofantove m-torke u prstenu cijelih brojeva imaginarnog kvadratnog polja. Napomenimo da je savjet za dokaz donje granice na veličinu elementa koji proširuje Diofantovu trojku dao Dujella.

U Poglavlju 6 bavimo se pitanjem koliko različitih $D(n)$-svojstava može imati jedna Diofantova trojka. Koristeći eliptičke krivulje, pokazujemo da postoji beskonačno mnogo Diofantovih trojki $\{a, b, c\}$ koje su ujedno i $D(n)$-skupovi za dva različita prirodna broja n koja nisu 1. Također, prikazat ćemo neke primjere Diofantovih trojki $\{a, b, c\}$ koje su i $D(n)$-skupovi za tri različita prirodna broja $n \neq 1$. Rezultati ovog poglavlja objavljeni su u koautorstvu s Dujellom, Kreso i Tadić u članku "Triples which are $D(n)$-sets for several n's" u Journal of Number Theory [2].

Želimo naglasiti važnost korištenja računala u ovom istraživanju i nastanku ove disertacije. Većina rezultata u Poglavlju 3 dokazana je koristeći identitete koji su prethodno naslućeni u Mathematici [46], a čak i neki dokazi dobiveni su u istom programu. U Poglavlju 6, jedna od konstrukcija familije beskonačno Diofantovih trojki koje imaju dva dodatna $D(n)$-svojstva naslućena je računalom i uz pomoć online enciklopedije nizova cijelih brojeva [43]. U istom poglavlju je i značajan dio računanja (faktorizacija, množenja i pojednostavljivanja) napravljen u Mathematici [46], dok je za eliptičke krivulje korišten Sage [45].

Poglavlje 2

Osnovni pojmovi i rezultati

U ovom poglavlju, preglednog karaktera, definiramo pojmove i iskazujemo tvrdnje koje ćemo primjenjivati u sljedećim poglavljima. Iako izostavljamo dokaze, napomenimo da je i pokoji dokaz u disertaciji nastao modifikacijom dokaza ovih klasičnih rezultata.

Potpoglavlje o verižnim razlomcima nastalo je prema [11], a rezultati o Pellovim i sličnim jednadžbama preuzeti su iz [30], [18] i [11]. O Diofantovim m-torkama više se može pročitati na web stranici Diophantine m-tuples A. Dujelle [10]. Za osnovne činjenice o eliptičkim krivuljama korišten je [41].

2.1 Verižni razlomci

Neka je α realan broj. Označimo s $a_0 = \lfloor \alpha \rfloor$, najveći cijeli broj koji nije veći od α. Ako $a_0 \neq \alpha$, onda možemo zapisati α kao $\alpha = a_0 + \frac{1}{\alpha_1}$, gdje je $\alpha_1 > 1$ (jer je $\alpha - a_0 < 1$), i označimo s $a_1 = \lfloor \alpha_1 \rfloor$. Ako $a_1 \neq \alpha_1$, onda α_1 možemo zapisati kao $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, gdje je $\alpha_2 > 1$. Označimo s $a_2 = \lfloor \alpha_2 \rfloor$. Ovaj postupak možemo nastaviti. Ako je $a_n = \alpha_n$ za neki prirodan n, onda je α racionalan, jer je

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{}{a_{n-1} + \cfrac{1}{a_n}}}}}.$$

Ovakav razlomak nazivamo *verižnim* i kraće zapisujemo kao $[a_0, a_1, \ldots, a_n]$. Ako je pak $a_n \neq \alpha_n$ za svaki n, onda definiramo racionalne brojeve

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

koje nazivamo (n-tim) *konvergentama* od α.

Ako je α iracionalan, onda niz konvergenti teži u α, tj. $\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$. Ovdje govorimo o *beskonačnom verižnom razlomku* koji zapisujemo kao $[a_0, a_1, a_2, \dots]$ i nazivamo ga *razvojem* broja α.

Definicija 2.1.1. Za beskonačni verižni razlomak $[a_0, a_1, a_2, \dots]$ kažemo da je *periodičan* ako postoje cijeli brojevi $n_0 \geqslant 0$ i $m \geqslant 1$ takvi da je $a_{m+n} = a_n$ za sve $n \geqslant n_0$. Tada verižni razlomak pišemo u obliku

$$[a_0, a_1, \dots, a_{n_0-1}, \overline{a_{n_0}, a_{n_0+1}, \dots, a_{n_0+m-1}}].$$

Definicija 2.1.2. Iracionalan broj α je *kvadratna iracionalnost* ako je rješenje kvadratne jednadžbe s racionalnim koeficijentima.

Teorem 2.1.3. [Euler, Lagrange] *Razvoj u verižni razlomak realnog broja α je periodičan ako i samo ako je α kvadratna iracionalnost.*

2.2 Pellove i pellovske jednadžbe

Definicija 2.2.1. Neka je d prirodan broj koji nije potpun kvadrat. Jednadžbu oblika

$$x^2 - dy^2 = 1, \tag{2.2.1}$$

nazivamo Pellovom jednadžbom. Rješenja tražimo u skupu prirodnih brojeva.

Ova jednadžba uvijek ima rješenje i uobičajeno je rješenje (x, y) zapisivati i kao $x+y\sqrt{d}$.

Definicija 2.2.2. Rješenje $x_0 + y_0\sqrt{d}$ jednadžbe (2.2.1) zovemo *fundamentalnim* ako je $x_0 + y_0\sqrt{d}$ najmanje među svim rješenjima jednadžbe (2.2.1).

Teorem 2.2.3. *Neka je (x_0, y_0) fundamentalno rješenje jednadžbe (2.2.1). Tada je za svaki cijeli broj n i $(x_0 + y_0\sqrt{d})^n$ rješenje iste jednadžbe.*

Obratno, ako je (x, y) rješenje jednadžbe (2.2.1) u prirodnim brojevima, onda postoji prirodan broj n takav da je $x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^n$.

Dokaz Teorema 2.2.3 može se naći u [30] ili na hrvatskom u [18].

S Pellovom jednadžbom usko je povezana i jednadžba $x^2 - dy^2 = -1$. Rješenja obje te jednadžbe skupa su opisana u sljedećem teoremu.

Teorem 2.2.4 ([11, Teorem 7.10])**.** *Sva rješenja u prirodnim brojevima jednadžbe $x^2 - dy^2 = \pm 1$ nalaze se među $x = p_n$, $y = q_n$, gdje su $\frac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$. Prema Teoremu 2.1.3, $\sqrt{d}$ ima periodičan razvoj u verižni razlomak. Neka je r duljina perioda u tom razvoju. Ako je r paran, onda jednadžba $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja od $x^2 - dy^2 = 1$ dana su sa $x = p_{nr-1}, y = q_{nr-1}$, za $n \in \mathbb{N}$. Ako je r neparan, onda su sva rješenja jednadžbe $x^2 - dy^2 = -1$ dana sa $x = p_{nr-1}, y = q_{nr-1}$ za neparne n, dok su sva rješenja jednadžbe $x^2 - dy^2 = 1$ dana sa $x = p_{nr-1}, y = q_{nr-1}$ za parne n.*

Budući da je (q_n) rastući niz (vidjeti npr. Teorem 6.3 u [11]), a fundamentalno rješenje je najmanje, ovaj teorem omogućava nam da pronađemo to rješenje.

Primjer 2.2.1. *Pogledajmo Pellovu jednadžbu* $x^2 - 5y^2 = 1$. *Broj* $\sqrt{5}$ *razvijmo u verižni razlomak:* $a_0 = \left\lfloor \sqrt{5} \right\rfloor = 2$, *pa je* $\sqrt{5} = 2 + \frac{1}{\alpha_1}$. *Tada je* $\alpha_1 = \frac{1}{\sqrt{5}-2} = 2+\sqrt{5}$ *i* $a_1 = \lfloor \alpha_1 \rfloor = 4$, *pa je* $\sqrt{5} = 2 + \cfrac{1}{4 + \cfrac{1}{\alpha_2}}$. *Odavdje je* α_2 *ponovo* $\alpha_2 = 2 + \sqrt{5}$, *pa je* $a_2 = 4$, *kao i* $a_3, a_4, \ldots$.

Dakle $\sqrt{5} = [2, \overline{4}]$. *Duljina perioda je* $r = 1$, *pa po prethodnom teoremu, rješenja jednadžbe* $x^2 - 5y^2 = 1$ *dana su s* $x = p_{2k-1}, y = q_{2k-1}$. *Kako je* $\frac{p_1}{q_1} = [2, 4] = 2 + \frac{1}{4} = \frac{9}{4}$, *dobivamo fundamentalno rješenje* $9+4\sqrt{5}$ *naše jednadžbe* $(9^2 - 5 \cdot 4^2 = 1)$, *a potenciranjem njega možemo odrediti sva rješenja. Npr. iduće rješenje dano je s* $(9+4\sqrt{5})^2 = 161+72\sqrt{5}$, *dakle* $x_1 = 161, y_1 = 72$.

Teorem 2.2.5 (Teorem 7.12 u [11])**.** *Neka je* (x_n, y_n), $n \in \mathbb{N}_0$ *niz svih rješenja Pellove jednadžbe* $x^2 - dy^2 = 1$ *u prirodnim brojevima, zapisan u rastućem redoslijedu. Tada je* (x_0, y_0) *fundamentalno rješenje. Dodatno, uzmimo da je* $(x_{-1}, y_{-1}) = (1, 0)$. *Tada vrijedi:*

$$x_{n+2} = 2x_0x_{n+1} - x_n, \quad y_{n+2} = 2x_0y_{n+1} - y_n, \quad n \geqslant -1.$$

Definicija 2.2.6. Neka je $N \neq 0$ cijeli broj, a d prirodan broj koji nije kvadrat. Jednadžbu

$$x^2 - dy^2 = N \tag{2.2.2}$$

nazivamo *pellovskom jednadžbom.* Zanimaju nas njena rješenja u cijelim brojevima.

Pellovska jednadžba ne mora imati rješenje. Ali ako je $x + y\sqrt{d}$ jedno njeno rješenje, a $t + u\sqrt{d}$ bilo koje cjelobrojno rješenje pripadne Pellove jednadžbe $x^2 - dy^2 = 1$, onda je i $(x + y\sqrt{d})(t + u\sqrt{d})$ također rješenje pellovske jednadžbe (2.2.2). Za to rješenje kažemo da je *asocirano* s rješenjem $x + y\sqrt{d}$. Skup svih međusobno asociranih rješenja čini jednu klasu rješenja. Ako se klasa rješenja sastoji od $x_i + y_i\sqrt{d}, i = 0, 1, 2, \ldots$, onda rješenja $x_i - y_i\sqrt{d}$ također tvore jednu klasu rješenja, koju nazivamo *konjugiranom* klasom. Ako se klasa podudara sa sebi konjugiranom klasom, onda je zovemo *dvoznačnom.*

Definicija 2.2.7. Među svim rješenjima $x + y\sqrt{d}$ jednadžbe (2.2.2) u istoj klasi izabrat ćemo jedno rješenje $x_0+y_0\sqrt{d}$ na sljedeći način. Neka je y_0 najmanja nenegativna vrijednost od y koja se pojavljuje u toj klasi. Ako klasa nije dvoznačna, time je jedinstveno određen x_0. Ako je klasa dvoznačna, onda uzimamo $x_0 \geqslant 0$. Ovako izabrano rješenje $x_0 + y_0\sqrt{d}$ nazivamo *fundamentalnim* rješenjem pellovske jednadžbe (2.2.2).

Za razliku od Pellove jednadžbe koja ima jednu klasu rješenja, pellovska jednadžba ih može imati više i ne postoji uniformna konstantna granica na broj klasa. Međutim, znamo

gornje granice na fundamentalna rješenja, pomoću kojih možemo odrediti fundamentalna, a onda i sva rješenja pellovske jednadžbe. Te gornje granice, koje ovise o fundamentalnom rješenju pripadne Pellove jednadžbe, iskazane su u sljedećem teoremu.

Teorem 2.2.8 ([37, Theorem 108 i 108a]). *Ako je $u + v\sqrt{D}$ fundamentalno rješenje jednadžbe*

$$u^2 - Dv^2 = N$$

za cijeli broj N i ako je $x_0 + y_0\sqrt{D}$ fundamentalno rješenje pripadne Pellove jednadžbe $x^2 - Dy^2 = 1$, onda je

$$0 \leqslant v \leqslant \frac{y_0}{\sqrt{2(x_0-1)}} \cdot \sqrt{|N|},$$
$$0 \leqslant |u| \leqslant \sqrt{\frac{1}{2}(x_0+1)|N|}.$$

Napomenimo da je ovaj teorem nastao spajanjem dva teorema iz [37], koja govore o ogradi ovisno o predznaku broja N. Ovdje je za svaku varijablu iskazana slabija od dvije gornje granice.

Primjer 2.2.2. *Pogledajmo pellovsku jednadžbu $u^2-5v^2 = 20$. Budući da smo u Primjeru 2.2.1 našli fundamentalno rješenje $9+4\sqrt{5}$ pripadne Pellove jednadžbe, Teorem 2.2.8 daje nam granicu za fundamentalno rješenje $v \leqslant \sqrt{20}$. Sad lako nalazimo fundamentalna rješenja ove pellovske jednadžbe $5+\sqrt{5}$, $-5+\sqrt{5}$, $10+4\sqrt{5}$ i $-10+4\sqrt{5}$. Svako od tih rješenja generira beskonačnu klasu rješenja, npr. $u_n + v_n\sqrt{5} = \pm(-5+\sqrt{5})(9 \pm 4\sqrt{5})^n$.*

2.3 Diofantove m-torke

Definicija 2.3.1. *Diofantova m-torka* je skup prirodnih brojeva $\{a_1, a_2, \ldots, a_m\}$ takav da je $a_i a_j + 1$ potpun kvadrat za $1 \leqslant i < j \leqslant m$.

Diofantov par uvijek se može proširiti do Diofantove trojke. Kod ovakvih pitanja, najčešće govorimo naprosto o proširenju skupa, pritom podrazumijevajući da će i proširenje biti Diofantova m-torka.

Ako je $ab + 1 = r^2$, onda za $c = a + b + 2r$ vrijedi da je

$$ac + 1 = a(a + b + 2r) + 1 = a^2 + ab + 2ar + 1 = a^2 + r^2 - 1 + 2ar + 1 = (a + r)^2.$$

Analogno se pokazuje da je $bc + 1 = (b + r)^2$, pa je $\{a, b, c\}$ Diofantova trojka.

Definicija 2.3.2. Za Diofantovu trojku $\{a, b, c\}$ kažemo da je *regularna* ako je $a < b$ i $c = a + b + 2r$, gdje je $r^2 = ab + 1$.

Diofantova trojka $\{a, b, c\}$ uvijek se može proširiti do Diofantove četvorke.

Definicija 2.3.3. Za Diofantovu četvorku $\{a, b, c, d\}$ kažemo da je *regularna* ako je $a < b < c$ i $d = d_+ = a + b + c + 2abc + 2rst$, gdje su r, s i t prirodni brojevi takvi da je $r^2 = ab + 1, s^2 = ac + 1$ i $t^2 = bc + 1$.

Naime, slično kao gore, račun potvrđuje da je

$$ad_+ + 1 = (at + rs)^2, \quad bd_+ + 1 = (bs + rt)^2, \quad cd_+ + 1 = (cr + st)^2.$$

Osim već spomenutog teorema o nepostojanju Diofantove petorke u prirodnim brojevima ([28]), postoji i jača slutnja da je svaka Diofantova četvorka regularna. Primijetimo da to znači da se svaka trojka može proširiti do četvorke s većim elementom na jedinstven način (iz toga jasno slijedi da ne postoji Diofantova petorka).

Umjesto 1, možemo dodavati i druge cijele brojeve. Preciznije, dolazimo do sljedećeg poopćenja pojma Diofantove m-torke.

Definicija 2.3.4. Za skup prirodnih brojeva $\{a_1, a_2, \ldots, a_m\}$ kažemo da ima $D(n)$-*svojstvo* ako je $a_i a_j + n$ potpun kvadrat za $1 \leqslant i < j \leqslant m$. Kraće, $\{a_1, a_2, \ldots, a_m\}$ je $D(n)$-*skup* ili $D(n)$-*m-torka*.

Diofantove m-torke su $D(1)$-skupovi. Prirodno pitanje je ponovo slično, koliko veliki $D(n)$-skupovi mogu biti.

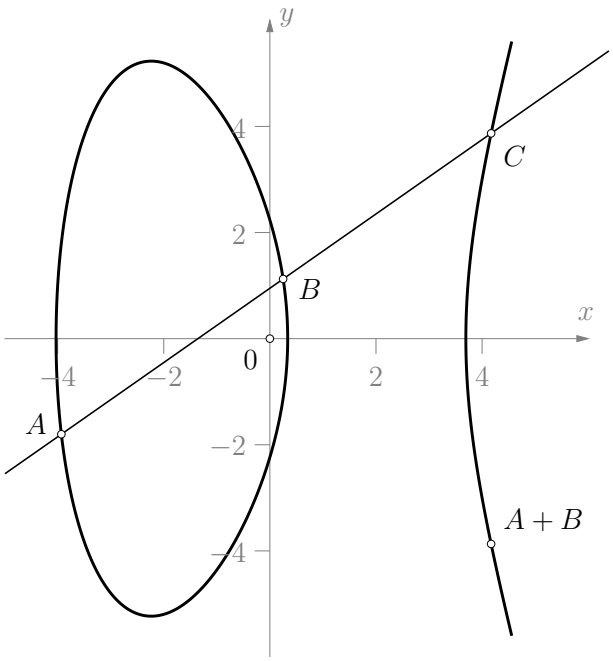
2.4 Eliptičke krivulje

Pod eliptičkom krivuljom podrazumijevat ćemo skup točaka (x, y) dan sljedećom jednadžbom:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Ova jednadžba naziva se Weierstrassovom jednadžbom. Pretpostavljat ćemo da je eliptička krivulja *glatka*, što znači da u svakoj točki možemo povući jedinstvenu tangentu (analitički, parcijalne derivacije postoje i nisu obje jednake nuli). Iako o krivuljama razmišljamo u ravnini (i tako ih skiciramo), za nas su od posebnog značaja točke krivulje s cjelobrojnim koordinatama i racionalne točke krivulje, tj. točke s racionalnim koordinatama. Opisat ćemo način na koji se mogu zbrajati racionalne točke.

Prvo ćemo opisati ovaj postupak geometrijski i pritom pretpostavljamo da je $a_1 = a_3 = 0$. Vidjeti Sliku 2.1. Kroz dvije točke A i B na eliptičkoj krivulji možemo provući sekantu (ili tangentu kad je $A = B$). Ona će u pravilu sijeći eliptičku krivulju u ukupno tri točke (jer je jednadžba kojom se zadaje eliptička krivulja trećeg stupnja), pa ćemo osim početne dvije imati još jedno sjecište, točku C. Budući da jednadžba sad ima oblik $y^2 = f(x)$, slijedi da na krivulji imamo i točku simetričnu točki C s obzirom na x-os. Upravo ta točka bit će zbroj početnih točaka A i B.



Slika 2.1: Geometrijski opis zbrajanja točaka na eliptičkoj krivulji $y^2 = x^3 - 15x + 5$

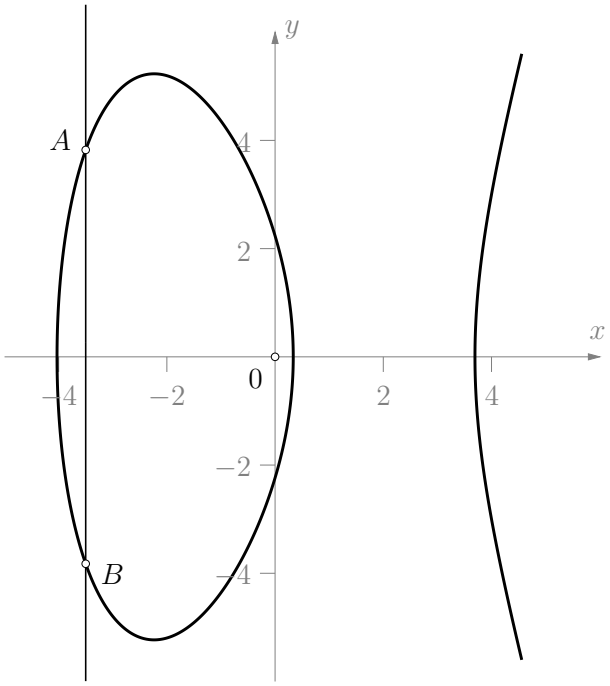
Međutim, ako su točke A i B međusobno simetrične s obzirom na x-os, onda ovaj postupak ne možemo provesti. Vidjeti Sliku 2.2. Čini se da nam nedostaje neka točka na ovoj krivulji. Zamišljajući točku u beskonačnosti $\mathcal{O}$, možemo za zbroj $A + B$ uzeti upravo tu točku $\mathcal{O}$.

Algoritam (za zbrajanje točaka na eliptičkoj krivulji, prema Silvermanu [41])**.** *Neka su $P_1(x_1, y_1)$ i $P_2(x_2, y_2)$ točke na E. Pretpostavimo da je $x_1 \neq x_2$. Definirajmo λ i ν u Tablici 2.1.*

Tablica 2.1
Definicija λ i ν potrebnih za zbrajanje točaka na eliptičkoj krivulji

	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}$	$\dfrac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}$

Tada je $y = \lambda x + \nu$ pravac kroz P_1 i P_2, odnosno tangenta na E ako je $P_1 = P_2$.



Slika 2.2: Par točaka koji ne možemo zbrojiti po prethodno opisanom postupku (slučaj $x_1 = x_2$)

Točka $P_3 = P_1 + P_2$ ima sljedeće koordinate

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3. \end{aligned} \tag{2.4.1}$$

Ako je $x_1 = x_2$ i $y_1 + y_2 + a_1x_2 + a_3 = 0$, onda je $P_1 + P_2 = \mathcal{O}$.

Spomenimo ovdje i da, iako ćemo uvijek raditi s eliptičkim krivuljama na ovdje opisan način, pravilnije je gledati na njih kao na projektivne krivulje. Naime, na skupu uređenih trojki $\mathbb{Q}^3 \setminus \{(0,0,0)\}$ možemo definirati relaciju ekvivalencije $T_1(x_1, y_1, z_1) \sim T_2(x_2, y_2, z_2)$ ako i samo ako postoji $\lambda \neq 0$ takav da je $x_1 = \lambda x_2, y_1 = \lambda y_2, z_1 = \lambda z_2$. Skup klasa ekvivalencije u $\mathbb{Q}^3 \setminus \{(0,0,0)\}$ zovemo *projektivnim prostorom*. Tada točke (x, y) možemo identificirati s točkama $(x, y, 1)$ na krivulji u projektivnom prostoru zadanoj jednadžbom

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

a točku u beskonačnosti $\mathcal{O}$ ovdje možemo eksplicitno zapisati kao $\mathcal{O} = (0, 1, 0)$.

Uz ovako definirano zbrajanje, skup racionalnih točaka na eliptičkoj krivulji $E(\mathbb{Q})$ dobiva strukturu Abelove grupe. Prema Mordellovom teoremu, ta grupa je konačno generirana [36]. Prema strukturnom teoremu za konačno generirane Abelove grupe [39] slijedi da je $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \mathbb{Z}_{\text{tor}}$, gdje je $r \in \mathbb{N}_0$, a $\mathbb{Z}_{\text{tor}}$ grupa elemenata konačnog reda. Broj r nazivamo *rangom eliptičke krivulje*, a $\mathbb{Z}_{\text{tor}}$ *torzijskom grupom*.

*

* *

Detaljniji uvod u eliptičke krivulje zainteresirani čitatelj može naći u knjizi "Rational Points on Elliptic Curves" [42], koja ima elementarni pristup, dok napredniji pristup imaju [41], [34] i [29], kao i [38] (na hrvatskom).

Spomenimo i da su ovdje prikazane slike nastale u Asymptoteu [27].

Poglavlje 3

Proširenje $D(-2k^2)$-para $\{2k^2, 2k^2+1\}$

Dokazujemo da se $D(-2k^2)$-par $\{2k^2, 2k^2+1\}$ može proširiti na najviše jedan način do $D(-2k^2)$-četvorke. Konkretno opisujemo to proširenje i uvjete uz koje postoji. Za neparan k opisujemo sva proširenja do $D(-2k^2)$-trojke. Svi rezultati ovdje predstavljeni, osim potpoglavlja 3.5 (u kojem rješavamo problem proširenja kad je k neparan), objavljeni su u članku "On the extension of $D(-8k^2)$-pair $\{8k^2, 8k^2+1\}$" u Moscow Mathematical Journal ([1]).

3.1 Problem

Kad govorimo o m-torkama, govorimo o skupovima. Tako ćemo, u skladu s Definicijom 2.3.4, koristiti izraze $D(n)$-par, $D(n)$-trojka, $D(n)$-m-torka, itd.

Prirodno pitanje vezano za $D(n)$-skupove je njihova veličina. Počevši od $D(n)$-trojke $\{a, b, c\}$, možemo konstruirati eliptičku krivulju $E : y^2 = (ax+n)(bx+n)(cx+n)$. Naime, za svaki x takav da $\{a, b, c, x\}$ ima $D(n)$-svojstvo, postoje $r, s, t \in \mathbb{Z}$ takvi da je $ax+n = r^2, bx+n = s^2, cx+n = t^2$, pa dobivamo cjelobrojnu točku (x, rst) na E. Kako eliptička krivulja ima konačno mnogo cjelobrojnih točaka [40], svaka $D(n)$-trojka može se proširiti samo s konačnim brojem elemenata ako želimo da zadrži $D(n)$-svojstvo. Zaključujemo da je svaki $D(n)$-skup konačan.

Međutim, ovime ne dobivamo uniformnu granicu na veličinu takvih skupova. Većina rezultata u ovom području, posebno novijih rezultata, oslanja se na linearne forme u logaritmima, teoreme o diofantskim aproksimacijama i eliptičke krivulje.

S druge strane, Fujita i Togbé u [23] dokazali su, na elementaran i relativno jednostavan način, sljedeći rezultat. Ako je $\{k^2, k^2+1, c, d\}$ četvorka s $D(-k^2)$-svojstvom i $c < d$, onda je $c = 1$ i $d = 4k^2+1$ (u tom slučaju, $3k^2+1$ mora biti kvadrat). Ovdje proučavamo sličan, ali složeniji problem.

Neka je k prirodan broj. Skup $\{2k^2, 2k^2+1\}$ ima $D(-2k^2)$-svojstvo, jer je $2k^2(2k^2+1)-2k^2 = 4k^4 = (2k^2)^2$. Trojka $\{1, 2k^2, 2k^2+1\}$ također ima $D(-2k^2)$-svojstvo. Koliko prirodnih brojeva možemo dodati u ove skupove, a da zadrže $D(-2k^2)$-svojstvo? Kod ovakvih pitanja, najčešće govorimo naprosto o proširenju skupa, pritom podrazumijevajući da će i proširenje imati isto svojstvo, u ovom slučaju $D(-2k^2)$-svojstvo.

Za neparan k je $-2k^2 \equiv 2 \pmod 4$, pa ne postoji proširenje do četvorke. Naime, poznat je teorem da za $n \equiv 2 \pmod 4$ ne postoji $D(n)$-četvorka, koji su 1985. nezavisno dokazali Brown [8], Gupta i Singh [25], te Mohanty i Ramasamy [35].

S druge strane, očito postoji proširenje do trojke $\{1, 2k^2, 2k^2+1\}$. Rekurzivno ćemo opisati sve prirodne c takve da skup $\{2k^2, 2k^2+1, c\}$ ima $D(-2k^2)$-svojstvo.

Odsada radimo za parne k-ove, sve do potpoglavlja 3.5, gdje radimo s neparnim k.

Pokazat ćemo da, ako $\{1, 8k^2, 8k^2+1, d\}$ ima $D(-8k^2)$-svojstvo, onda je d jedinstveno određen ($d = 32k^2+1$). Nadalje, pokazat ćemo da se čak i par $\{8k^2, 8k^2+1\}$ može proširiti do četvorke na najviše jedan način (treći i četvrti element mogu biti samo 1 i $32k^2+1$). Jasno, iz toga slijedi da se par $D(-8k^2)$-par $\{8k^2, 8k^2+1\}$ ne može proširiti do petorke. Prvo promatramo proširivost trojke $\{1, 8k^2, 8k^2+1\}$.

3.2 Proširivost $D(-8k^2)$-trojke $\{1, 8k^2, 8k^2+1\}$

U ovom dijelu dokazujemo sljedeći teorem.

Teorem 3.2.1. *Ako skup $\{1, 8k^2, 8k^2+1, d\}$ ima $D(-8k^2)$-svojstvo, onda je $d = 32k^2+1$. U tom slučaju, $24k^2+1$ mora biti kvadrat.*

3.2.1 Sustav simultanih pellovskih jednadžbi

Zbog $D(-8k^2)$-svojstva skupa $\{1, 8k^2, 8k^2+1, d\}$ postoje cijeli brojevi x, y' i z takvi da je

$$\begin{aligned} d - 8k^2 &= x^2, \\ 8k^2 d - 8k^2 &= (y')^2, \\ (8k^2+1)d - 8k^2 &= z^2. \end{aligned}$$

Iz druge jednadžbe možemo zaključiti da $8k^2$ dijeli $(y')^2$. Slijedi da $4k$ dijeli y', odnosno da postoji cijeli broj y takav da je $y' = 4ky$. Time se druga jednadžba pojednostavljuje u $d - 1 = 2y^2$. Iz te i zadnje jednadžbe slijedi $z^2 - (8k^2+1)\cdot 2y^2 = (8k^2+1)d - 8k^2 - (8k^2+1)(d-1)$, tj. dobivamo Pellovu jednadžbu $z^2 - 2(8k^2+1)y^2 = 1$.

Slično, eliminacijom d iz prve jednadžbe i pojednostavljene druge slijedi pellovska jednadžba $x^2 - 2y^2 = -8k^2 + 1$.

Rezimirajmo, ako se $D(-8k^2)$ trojka s kojom radimo može proširiti, onda postoje cijeli brojevi x, y i z koji zadovoljavaju sljedeći sustav:

$$x^2 - 2y^2 = -8k^2 + 1, \tag{3.2.1}$$
$$z^2 - (16k^2+2)y^2 = 1. \tag{3.2.2}$$

Problem proširenja $D(-k^2)$-para $\{k^2, k^2+1\}$ u [23] sveden je na sličan sustav na isti način kao ovdje. Međutim, tamo je jedna od jednadžbi bila jako jednostavna ($y^2 - x^2 = k^2 - 1$), što je olakšalo rješavanje problema. Primijetimo da $16k^2+2$ nije potpun kvadrat jer je između dva uzastopna kvadrata, preciznije, $(4k)^2 < 16k^2+2 < (4k+1)^2$.

Jednadžba (3.2.1) je pellovska jednadžba i može imati velik broj beskonačnih klasa rješenja. S druge strane, Pellova jednadžba (3.2.2) ima jednu beskonačnu klasu rješenja, koju generira fundamentalno rješenje. Kao što je uobičajeno, rješenje (z, y) te Pellove jednadžbe, zapisivat ćemo i kao $z + y\sqrt{16k^2+2}$.

Lema 3.2.2. *Sva rješenja jednadžbe* (3.2.2), $z^2 - (16k^2+2)y^2 = 1$, *u prirodnim brojevima dana su sa* $(16k^2+1+4k\sqrt{16k^2+2})^n$ *za prirodne* n. *Ako je* (z, y) *rješenje ove jednadžbe u nenegativnim cijelim brojevima, onda je* y *element niza*

$$y_{-1} = 0, y_0 = 4k, y_{m+2} = 2(16k^2+1)y_{m+1} - y_m. \tag{3.2.3}$$

Dokaz. Korištenjem verižnih razlomaka ($\sqrt{16k^2+2} = [4k; \overline{4k, 8k}]$) dobivamo fundamentalno rješenje $16k^2+1+4k\sqrt{16k^2+2}$. Detaljnije, algoritmom za zapis broja u verižni razlomak (v. [11, Dokaz Teorema 6.15]), računamo:

$$\alpha_0 = \sqrt{16k^2+2}, a_0 = \lfloor\sqrt{16k^2+2}\rfloor \Rightarrow a_0 = 4k,$$
$$S_1 = 4k, t_1 = 2, \alpha_1 = 2k + \frac{\sqrt{16k^2+2}}{2} \Rightarrow a_1 = 4k,$$
$$S_2 = 8k - 4k = 4k, t_2 = \frac{16k^2+2-16k^2}{2} = 1, \alpha_2 = 4k + \sqrt{16k^2+2} \Rightarrow a_2 = 8k,$$
$$S_3 = 8k - 4k = 4k, t_3 = \frac{16k^2+2-16k^2}{1} = 2, \alpha_3 = \frac{4k+\sqrt{16k^2+2}}{2} \Rightarrow a_3 = 4k.$$

Kako je $(S_1, t_1, a_1) = (S_3, t_3, a_3)$, dobivamo periodički verižni razlomak $[4k; \overline{4k, 8k}]$.

Iz verižnih razlomaka može se naći fundamentalno, a onda i sva rješenja Pellove jednadžbe. Za naše potrebe dovoljan je Teorem 2.2.4 iz preglednog dijela disertacije.

Kako je $\sqrt{16k^2+2} = [4k; \overline{4k, 8k}]$, period je duljine 2, pa je najmanje rješenje $z = p_1, y = q_1$, gdje je

$$\frac{p_1}{q_1} = [4k, 4k] = 4k + \frac{1}{4k} = \frac{16k^2+1}{4k}.$$

Dakle, fundamentalno rješenje zaista je $16k^2+1+4k\sqrt{16k^2+2}$ (tj. $z_0 = 16k^2+1$, $y_0 = 4k$).

Rješenja $z_n + y_n\sqrt{16k^2+2}$ dana su sa $z_n + y_n\sqrt{16k^2+2} = (16k^2+1+4k\sqrt{16k^2+2})^n$,

pa je $z_{n+1} + y_{n+1}\sqrt{16k^2+2} = (z_n + y_n\sqrt{16k^2+2})(16k^2+1+4k\sqrt{16k^2+2})$. Iz toga je

$$z_{n+1} = (16k^2+1)z_n + 4k(16k^2+2)y_n, \quad z_0 = 16k^2+1,\ z_{-1} = 1 \tag{3.2.4}$$

$$y_{n+1} = (16k^2+1)y_n + 4kz_n, \qquad y_0 = 4k,\ y_{-1} = 0. \tag{3.2.5}$$

Ovaj rekurzivan sustav nizova $(z_n)_{n\geqslant -1}$ i $(y_n)_{n\geqslant -1}$ sadrži sva nenegativna cjelobrojna rješenja (z, y) jednadžbe (3.2.2).

Prema Teoremu 2.2.5, moguće je dobiti zasebne rekurzivne definicije za svaki od nizova y_n i z_n. Slijedi da je $y_{n+2} = 2(16k^2+1)y_{n+1} - y_n$.

□

S druge strane, y treba biti i rješenje od (3.2.1), tj. x^2 treba biti $2y_n^2 - 8k^2 + 1$ za neki $n \in \mathbb{N}_0$. Zato uvodimo novi niz $X_n = 2y_n^2 - 8k^2 + 1$.

3.2.2 Kvadrati u nizu (X_n)

U ovom dijelu ispitujemo može li X_n biti potpun kvadrat za neki indeks n. Koristeći veze između y_n i z_n, npr. $y_{2n+1} = 2y_nz_n$, rastavit ćemo X_n na produkt dva faktora, od kojih jedan očito neće biti kvadrat. Pokazat ćemo da su ti faktori relativno prosti (npr. principom spusta za neparne indekse). Faktorizacija i cijeli dokaz ovise o parnosti indeksa elementa niza (X_n). Jednom kad se identiteti koji povezuju nizove (y_n) i (z_n) naslute, dokaz je potpuno računski i stoga je odgođen za kasnije.

Neparni indeksi

Za neparne indekse koristimo identitet koji ćemo dokazati u Lemi 3.4.1,

$$y_{2n+1} = 2y_nz_n, \tag{3.2.6}$$

kako bismo pokazali da X_{2n+1} nikad nije kvadrat. Koristeći (3.2.6) i (3.2.2) dobivamo

$$\begin{aligned} X_{2n+1} &= 2y_{2n+1}^2 - 8k^2 + 1 = 8y_n^2z_n^2 - 8k^2 + 1 = 8y_n^2(1 + (16k^2+2)y_n^2) - 8k^2 + 1 \\ &= (4y_n^2+1)(32y_n^2k^2 + 4y_n^2 - 8k^2 + 1). \end{aligned}$$

Prvi faktor ne može biti kvadrat, jer je $(2y_n)^2 < 4y_n^2 + 1 < (2y_n+1)^2$ (za $y_n \in \mathbb{N}$). Dakle, da bismo zaključili da X_{2n+1} nije kvadrat ni za koji n, dovoljno je dokazati da su dobiveni faktori relativno prosti. To ćemo dokazati principom spusta. Preciznije, dokazat ćemo da pretpostavka

$$p \mid 4y_n^2 + 1 \text{ i } p \mid 32y_n^2k^2 + 4y_n^2 - 8k^2 + 1$$

povlači

$$p \mid 4y_{n-1}^2 + 1 \text{ i } p \mid 32y_{n-1}^2k^2 + 4y_{n-1}^2 - 8k^2 + 1,$$

što će nas dovesti do kontradikcije.

Pretpostavimo da p dijeli $4y_n^2+1$ i $32y_n^2k^2+4y_n^2-8k^2+1$. Tada p također dijeli $32y_n^2k^2+4y_n^2-8k^2+1-(4y_n^2+1)=32k^2y_n^2-8k^2=8k^2(4y_n^2-1)$. Budući da je p neparan (jer dijeli neparan broj $4y_n^2+1$), slijedi da $p \mid k^2(4y_n^2-1)$. Ne može dijeliti drugi faktor, jer bi tada dijelio i $4y_n^2+1-(4y_n^2-1)=2$. Zaključujemo da p dijeli k^2, a kako je prost, onda dijeli i k.

Dokažimo sada da p dijeli i $4y_{n-1}^2+1$ i $32y_{n-1}^2k^2+4y_{n-1}^2-8k^2+1$. Iz (3.2.5), rekurzivne relacije za (y_n), dobivamo $y_n-y_{n-1}=16k^2y_{n-1}+4kz_{n-1}$, a kako p dijeli k, slijedi da dijeli y_n-y_{n-1}. Dakle, $y_n \equiv y_{n-1} \pmod{p}$, pa slijedi da p dijeli $4y_{n-1}^2+1$. S druge strane, kako je $32y_{n-1}^2k^2+4y_{n-1}^2-8k^2+1=8k^2(4y_{n-1}^2-1)+4y_{n-1}^2+1$, vrijedi i da p dijeli $32y_{n-1}^2k^2+4y_{n-1}^2-8k^2+1$.

Daljnji spust implicirao bi da p dijeli $4y_0^2+1=64k^2+1$ (i $32y_0^2k^2+4y_0^2-8k^2+1$). Ali, kako p dijeli k, dijelio bi i 1, što je kontradikcija. Dakle, $4y_n^2+1$ i $32y_n^2k^2+4y_n^2-8k^2+1$ nemaju zajedničkih prostih faktora, odnosno relativno su prosti.

Parni pozitivni indeksi

Za parne indekse, koristimo sljedeći identitet iz Leme 3.4.1,

$$z_{2n}-1=(y_n+y_{n-1})^2, \tag{3.2.7}$$

kako bismo pokazali da X_{2n} nije kvadrat za prirodne brojeve n. Računamo

$$\begin{aligned} X_{2n} &= 2y_{2n}^2-8k^2+1 \overset{(3.2.2)}{=} 2\cdot\frac{z_{2n}^2-1}{16k^2+2}-8k^2+1= \\ &= \frac{z_{2n}^2-64k^2}{8k^2+1}=\frac{z_{2n}-8k^2}{8k^2+1}\cdot(z_{2n}+8k^2). \end{aligned}$$

Uočimo da zadnji faktor, $z_{2n}+8k^2$, ne može biti kvadrat za $n \geqslant 1$, jer se nalazi između kvadrata dva uzastopna prirodna broja:

$$(y_n+y_{n-1})^2 < z_{2n}+8k^2 = (y_n+y_{n-1})^2+1+8k^2 < (y_n+y_{n-1}+1)^2.$$

Zaista, nejednakost s lijeve strane je očita zbog (3.2.7). Nejednakost s desne strane vrijedi ako i samo ako je $1+8k^2 < 2(y_n+y_{n-1})+1$, tj. $4k^2 < y_n+y_{n-1}$. Kako je već $y_1=2(16k^2+1)\cdot 4k$ i y_n je rastući niz prema (3.2.5), potrebna nejednakost zaista vrijedi za $n \geqslant 1$.

Sada pokazujemo da su faktori $\dfrac{z_{2n}-8k^2}{8k^2+1}$ i $z_{2n}+8k^2$ relativno prosti. Prije toga uočimo da je $\dfrac{z_{2n}-8k^2}{8k^2+1}$ cijeli broj. Induktivno se pokazuje da elementi niza (z_n) rekurzivno zadanog s (3.2.4) daju pri dijeljenju s $8k^2+1$ ostatke 1 i $8k^2$. Preciznije, $z_{2n-1} \equiv 1 \pmod{8k^2+1}$ za $n \in \mathbb{N}_0$ i $z_{2n} \equiv 8k^2 \pmod{8k^2+1}$, pa je stoga $z_{2n}-8k^2$ djeljivo s $8k^2+1$.

Sada pretpostavimo da prost p dijeli $\dfrac{z_{2n}-8k^2}{8k^2+1}$ i $z_{2n}+8k^2$. Tada dijeli i $z_{2n}-8k^2$, kao i razliku $z_{2n}+8k^2-(z_{2n}-8k^2)=16k^2$. Primijetimo da je z_n neparan za svaki indeks n, prema principu matematičke indukcije iz rekurzivne definicije (3.2.4). Budući da p dijeli neparan broj $z_{2n}+8k^2$, slijedi da je p neparan. Stoga iz $p \mid 16k^2$ slijedi $p|k^2$. Iz toga i iz $p \mid z_{2n}+8k^2$ zaključujemo da $p \mid z_{2n}$. Ali elementi niza (z_n) relativno su prosti s k jer svi daju ostatak 1 pri dijeljenju s k (ovo opet slijedi induktivno). Dakle, nemoguće je da z_{2n} i k imaju zajednički prosti faktor p, pa dobivamo kontradikciju.

Ostaje nam slučaj $n=0$, tj. kad je $X_0 = \dfrac{z_0-8k^2}{8k^2+1}\cdot(z_0+8k^2) = 24k^2+1$ potpun kvadrat. Na temelju toga, vrijedi sljedeća tvrdnja.

Propozicija 3.2.3. *Jedini element niza $(X_n)_{n\geqslant 0}$ koji može biti potpun kvadrat je $X_0 = 24k^2+1$.*

U tom slučaju, kako je $x^2 = 24k^2+1$ i $d-8k^2=x^2$, slijedi da četvrti element, koji proširuje $D(-8k^2)$-trojku $\{1, 8k^2, 8k^2+1\}$, može biti samo $d=32k^2+1$. Međutim, $24k^2+1$ je kvadrat samo za neke k i to upravo one koji su rješenja Pellove jednadžbe $m^2-24k^2=1$. Time je dokazan Teorem 3.2.1.

3.3 Proširivost $D(-8k^2)$-para $\{8k^2, 8k^2+1\}$

U ovom dijelu dokazujemo glavni rezultat poglavlja, sljedeći teorem.

Teorem 3.3.1. *Neka je k prirodan broj. Ako skup $\{8k^2, 8k^2+1, c, d\}$ ima $D(-8k^2)$-svojstvo i $d>c$, onda je $c=1$, a $d=32k^2+1$. U tom slučaju, k je element niza (k_n), definiranog rekurzivno s $k_1=1, k_2=10, k_{n+2}=10k_{n+1}-k_n$ za $n\in\mathbb{N}$.*

Dokaz. Pretpostavimo da skup $\{8k^2, 8k^2+1, c\}$ ima $D(-8k^2)$-svojstvo, gdje je $c>1$. Tada postoje prirodni brojevi s' i t za koje vrijedi

$$8k^2c-8k^2=(s')^2,\ (8k^2+1)c-8k^2=t^2.$$

Očito $8k^2$ dijeli $(s')^2$, pa slijedi da $4k$ dijeli s'. Dakle, postoji prirodan broj s takav da je $s'=4ks$, što nam pojednostavljuje jednadžbu u $c-1=2s^2$. Eliminirajući c, dobivamo jednadžbu

$$t^2-(16k^2+2)s^2=1. \tag{3.3.1}$$

Iz Leme 3.2.2 već znamo da je $t+s\sqrt{16k^2+2} = (16k^2+1+4k\sqrt{16k^2+2})^\nu$ za $\nu\in\mathbb{N}_0$. Stoga je $s=s_\nu$ za neki ν, gdje je $s_0=0, s_1=4k, s_{\nu+2}=2(16k^2+1)s_{\nu+1}-s_\nu$. Jednadžba (3.3.1) tada ima rješenja (s_i, t_i) za $i\in\mathbb{N}_0$.

Pretpostavimo sad da postoje $D(-8k^2)$-četvorke $\{8k^2, 8k^2+1, c, d\}$ takve da su c i d veći od 1. Tada postoji $\nu \in \mathbb{N}$ takav da je $c = 2s_\nu^2 + 1$. Preciznije, neka su cijeli brojevi $d > c > 1$ takvi da skup $\{8k^2, 8k^2+1, c, d\}$ ima $D(-8k^2)$-svojstvo, pri čemu je c najmanji mogući $c > 1$ za koji postoji četvrti element d koji proširuje $\{8k^2, 8k^2+1, c\}$. Stoga je

$$8k^2d - 8k^2 = (x')^2, \quad (8k^2+1)d - 8k^2 = y^2, \quad cd - 8k^2 = z^2.$$

Prva jednadžba pojednostavljuje se u $d - 1 = 2x^2$ na isti način kao prije. Eliminacijom d dobivamo sustav

$$y^2 - (16k^2+2)x^2 = 1 \tag{3.3.2}$$

$$z^2 - 2cx^2 = c - 8k^2 \tag{3.3.3}$$

pa ponovo po Lemi 3.2.2 znamo da je $y + x\sqrt{16k^2+2} = (16k^2+1+4k\sqrt{16k^2+2})^m$, za $m \in \mathbb{N}_0$, tj. x je element niza

$$v_0 = 0, v_1 = 4k, v_{m+2} = 2(16k^2+1)v_{m+1} - v_m. \tag{3.3.4}$$

S druge strane, fundamentalno rješenje Pellove jednadžbe $z^2 - 2cx^2 = 1$, koja odgovara pellovskoj jednadžbi (3.3.3), jest $(2c-1, 2s)$. To slijedi, kao ranije, iz Teorema 2.2.4 i razvoja $\sqrt{2c} = \sqrt{4s^2+2}$ u verižni razlomak, odnosno iz prve konvergente $(p_1, q_1) = (2c-1, 2s)$.

Sada ćemo iskoristiti Teorem 2.2.8, koji nam daje ogradu na fundamentalno rješenje pellovske jednadžbe ako znamo fundamentalno rješenje pripadne Pellove jednadžbe. Naime, ako je (z, x) rješenje jednadžbe (3.3.3), $z^2 - 2cx^2 = c - 8k^2$, onda postoji fundamentalno rješenje (z_0, x_0) takvo da je $z + x\sqrt{2c} = (z_0 + x_0\sqrt{2c})(2c - 1 + 2s\sqrt{2c})^n$ za nenegativan cijeli broj n i

$$0 < x_0 \leqslant \frac{2s}{\sqrt{2(2c-2)}}\sqrt{c-8k^2} = \frac{s}{\sqrt{2s^2}}\sqrt{c-8k^2} = \sqrt{\frac{c}{2} - 4k^2} = \sqrt{s^2 + \frac{1}{2} - 4k^2} < s.$$

Druga nejednakost ovdje upravo je ograda na fundamentalna rješenja dana u Teoremu 2.2.8. A $x_0 \neq 0$ jer bi u suprotnom iz $z^2 = c - 8k^2$ slijedilo da $\{1, 8k^2, 8k^2+1, c\}$ ima $D(-8k^2)$-svojstvo, pa po Teoremu 3.2.1 ne može postojati d.

Iz $z + x\sqrt{2c} = (z_0 + x_0\sqrt{2c})(2c - 1 + 2s\sqrt{2c})^n$, kao prije, dobivamo rekurzivno definirane nizove koji sadrže rješenja x. Zaključujemo da je x također i element niza

$$w_0 = x_0, w_1 = (2c-1)x_0 + 2sz_0, w_{n+2} = 2(2c-1)w_{n+1} - w_n.$$

Primijetimo da je $w_n \equiv x_0 \pmod{s}$ za sve n, jer je $c = 2s^2 + 1 \equiv 1 \pmod{s}$, pa induktivno iz $w_1 \equiv w_2 \equiv x_0 \pmod{s}$ i pretpostavke da je $w_n \equiv w_{n+1} \equiv x_0 \pmod{s}$ slijedi da je

$w_{n+2} \equiv 2x_0 - x_0 \equiv x_0 \pmod{s}$. Također je

$$(v_m)_{m\geqslant 0} \equiv (0, s_1, s_2, \ldots, s_{\nu-1}, 0, -s_{\nu-1}, -s_{\nu-2}, \ldots, -s_1, 0, s_1, s_2, \ldots) \pmod{s},$$

jer je niz (3.3.4) isti kao i niz s_ν. Iz ovih kongruencija, rasta niza v_m i $x_0 < s$, slijedi da je $x_0^2 = s_i^2$ za neki $i < \nu$.

Neka je sada $d_0 = 2x_0^2+1$. Tada je $(8k^2+1)d_0-8k^2 = (16k^2+2)x_0^2+1 = (16k^2+2)s_i^2+1$, pa je

$$(8k^2+1)d_0 - 8k^2 = t_i^2.$$

Također je

$$8k^2d_0 - 8k^2 = 16k^2x_0^2 = (4kx_0)^2$$

i

$$cd_0 - 8k^2 = c(2x_0^2+1) - 8k^2 = 2cx_0^2 + c - 8k^2 = z_0^2 - c + 8k^2 + c - 8k^2 = z_0^2.$$

Zaključujemo da je skup $\{8k^2, 8k^2+1, d_0, c\}$ također $D(-8k^2)$-četvorka. Primijetimo da je $d_0 = 2x_0^2 + 1 < 2s^2 + 1 = c$ te, kako je c najmanja moguća vrijednost veća od 1, d_0 mora biti $d_0 = 1$, tj. $x_0 = 0 > 0$, što je kontradikcija.

Ne postoji $D(-8k^2)$-četvorka $\{8k^2, 8k^2+1, c, d\}$ takva da je $1 < c < d$.

Za zadnju tvrdnju ovog teorema koristimo Teorem 3.2.1 kako bismo zaključili da $24k^2+1$ mora biti kvadrat. Ali to je ponovo Pellova jednadžba: $m^2 - 24k^2 = 1$. Fundamentalno rješenje $5 + \sqrt{24}$ daje nam rekurzivan niz za moguće vrijednosti k,

$$k_1 = 1, k_2 = 10, k_{n+2} = 10k_{n+1} - k_n, \text{ za sve } n \in \mathbb{N}.$$

□

3.4 Dokaz korištenih identiteta

U dokazu Teorema 3.2.1 koristili smo identitete (3.2.6) i (3.2.7), koje ovdje dokazujemo. Budući da je riječ o identitetima između rekurzivno definiranih nizova, riješit ćemo rekurzije, odnosno dobiti eksplicitne izraze za elemente tih nizova.

Lema 3.4.1. *Ako sa $(z_n, y_n)_{n\geqslant -1}$ označimo sva nenegativna cjelobrojna rješenja jednadžbe $z^2-(16k^2+2)y^2 = 1$, tako da su nizovi (y_n) i (z_n) u rastućem poretku, onda je $y_{2n+1} = 2y_nz_n$ i $z_{2n} - 1 = (y_n + y_{n-1})^2$.*

Dokaz. Fundamentalno rješenje ove Pellove jednadžbe je $16k^2 + 1 + 4k\sqrt{16k^2+2}$, što znači da se svako rješenje (z_{n+1}, y_{n+1}) može dobiti iz prethodnog (z_n, y_n) iz $z_{n+1} + y_{n+1}\sqrt{16k^2+2} = (z_n + y_n\sqrt{16k^2+2})(16k^2 + 1 + 4k\sqrt{16k^2+2})$. To nam daje povezani sustav rekurzija (3.2.4) i (3.2.5). Iz toga, odnosno iz Teorema 2.2.5, slijedi da

je $z_{n+2} = 2(16k^2+1)z_{n+1} - z_n$, s početnim uvjetima $z_{-1} = 1, z_0 = 16k^2+1$. Također je $y_{n+2} = 2(16k^2+1)y_{n+1} - y_n$, s početnim uvjetima $y_{-1} = 0, y_0 = 4k$.

Rješavanjem ovih rekurzija, dobivamo eksplicitne izraze:

$$y_n = c_1(16k^2+1+4k\sqrt{16k^2+2})^n + c_2(16k^2+1-4k\sqrt{16k^2+2})^n$$
$$z_n = c_3(16k^2+1+4k\sqrt{16k^2+2})^n + c_4(16k^2+1-4k\sqrt{16k^2+2})^n,$$

gdje je

$$c_1 = \frac{64k^3+8k+(16k^2+1)\sqrt{16k^2+2}}{2(16k^2+2)}, \quad c_2 = \frac{64k^3+8k-(16k^2+1)\sqrt{16k^2+2}}{2(16k^2+2)},$$

$$c_3 = \frac{128k^4+24k^2+1+(32k^3+4k)\sqrt{16k^2+2}}{16k^2+2},$$
$$c_4 = \frac{128k^4+24k^2+1-(32k^3+4k)\sqrt{16k^2+2}}{16k^2+2}.$$

Računamo

$$\begin{aligned}2y_nz_n &= 2(c_1(16k^2+1+4k\sqrt{16k^2+2})^n + c_2(16k^2+1-4k\sqrt{16k^2+2})^n)\cdot\\ &\quad\cdot(c_3(16k^2+1+4k\sqrt{16k^2+2})^n + c_4(16k^2+1-4k\sqrt{16k^2+2})^n) =\\ &= 2\Big(c_1c_3(16k^2+1+4k\sqrt{16k^2+2})^{2n}+\\ &\quad c_2c_4(16k^2+1-4k\sqrt{16k^2+2})^{2n} + c_1c_4 + c_2c_3\Big)\end{aligned}$$

Sad sve što trebamo učiniti da bismo dokazali da je $y_{2n+1} = 2y_nz_n$ jest izračunati, tj. usporediti ove koeficijente (najbolje računalom):

$$\begin{aligned}2c_1c_3 &= 2\frac{64k^3+8k+(16k^2+1)\sqrt{16k^2+2}}{2(16k^2+2)}\cdot\frac{128k^4+24k^2+1+(32k^3+4k)\sqrt{16k^2+2}}{16k^2+2}\\ &= \frac{(64k^3+8k)(128k^4+24k^2+1)+(16k^2+1)(32k^3+4k)(16k^2+2)}{(16k^2+2)^2}+\\ &\quad+\frac{((64k^3+8k)(32k^3+4k)+(16k^2+1)(128k^4+24k^2+1))\sqrt{16k^2+2}}{(16k^2+2)^2} =\\ &= \frac{16k+512k^3+5120k^5+16384k^7+(1+72k^2+1024k^4+4096k^6)\sqrt{16k^2+2}}{(16k^2+2)^2} =\\ &= \frac{16k(8k^2+1)^2(16k^2+1)+(8k^2+1)(512k^4+64k^2+1)\sqrt{16k^2+2}}{(16k^2+2)^2} =\\ &= \frac{8k(8k^2+1)(16k^2+1)+\frac{1}{2}(512k^4+64k^2+1)\sqrt{16k^2+2}}{16k^2+2} =\\ &= \frac{16k(8k^2+1)(16k^2+1)+(512k^4+64k^2+1)\sqrt{16k^2+2}}{2(16k^2+2)}.\end{aligned}$$

S druge strane, u y_{2n+1}, koeficijent od $(16k^2+1+4k\sqrt{16k^2+2})^{2n}$ je

$$\begin{aligned}
&c_1(16k^2+1+4k\sqrt{16k^2+2}) \\
&\quad = \frac{64k^3+8k+(16k^2+1)\sqrt{16k^2+2}}{2(16k^2+2)}(16k^2+1+4k\sqrt{16k^2+2}) \\
&\quad = \frac{(64k^3+8k)(16k^2+1)+4k(16k^2+1)(16k^2+2)}{2(16k^2+2)} \\
&\qquad + \frac{((64k^3+8k)\cdot 4k+(16k^2+1)^2)\sqrt{16k^2+2}}{2(16k^2+2)} \\
&\quad = \frac{16k(128k^4+24k^2+1)+(512k^4+64k^2+1)\sqrt{16k^2+2}}{2(16k^2+2)},
\end{aligned}$$

pa je zaista koeficijent od $(16k^2+1+4k\sqrt{16k^2+2})^{2n}$ jednak u y_{2n+1} i u $y_n z_n$.

Analogno za konjugat $(16k^2+1-4k\sqrt{16k^2+2})^{2n}$, pri čemu je $c_1c_4+c_2c_3=0$.

Drugi identitet, $z_{2n}-1=(y_n+y_{n-1})^2$, može se dokazati na sličan način. Ali radije opišimo ovdje kako to u praksi radimo računalom. Sljedeći dio koda u Wolfram Mathematici [46] definira nizove y_n i z_n.

```
c1 = (64k^3+8k+(16k^2+1)Sqrt[16k^2+2])/(2(16k^2+2))
c2 = (64k^3+8k-(16k^2+1)Sqrt[16k^2+2])/(2(16k^2+2))
c3 = (128k^4+24k^2+1+(32k^3+4k)Sqrt[16k^2+2])/(16k^2+2)
c4 = (128k^4+24k^2+1-(32k^3+4k)Sqrt[16k^2+2])/(16k^2+2)
y[n_] = c1*(16k^2+1+4k*Sqrt[16k^2+2])^n
                +c2*(16k^2+1-4k*Sqrt[16k^2+2])^n
z[n_]= c3*(16k^2+1+4k*Sqrt[16k^2+2])^n
                +c4*(16k^2+1-4k*Sqrt[16k^2+2])^n
```

Provjerimo zadovoljavaju li jednadžbu:

```
Simplify[z[n]^2-(16k^2+2)y[n]^2].
```

Ispis je

```
(1+16k^2- 4kSqrt[2+16 k^2])^n (1+16k^2 +4kSqrt[2+16 k^2])^n.
```

Dobiveni izraz je

$$\begin{aligned}
(1+16k^2-4k\sqrt{2+16k^2})^n(1+16k^2+4k\sqrt{2+16k^2})^n &= ((1+16k^2)^2-(4k\sqrt{2+16k^2})^2 \\
&= 1+32k^2 56k^4-16k^2(2+16k^2) \\
&= 1.
\end{aligned}$$

Provjerimo sad korištene identitete.

```
Simplify[y[2n+1]-2y[n]z[n]]
Out = 0
```

Ovime je dokazan identitet koji smo već dokazali raspisivanjem. Za naredbu

```
Simplify[((y[n]+y[n-1]))^2+1-z[2n]],
```

rezultat je

```
1-(1+16k^2-4kSqrt[2+16 k^2])^n(1+16k^2+4kSqrt[2+16 k^2])^n.
```

Dobiveni izraz je

$$\begin{aligned}
&= 1-(1+16k^2-4k\sqrt{2+16k^2})^n(1+16k^2+4k\sqrt{2+16k^2})^n \\
&= 1-(1+16k^2)^2+(4k\sqrt{2+16k^2})^2 \\
&= 1-1-32k^2-256k^4+16k^2(2+16k^2) \\
&= 0.
\end{aligned}$$

Ovime je dokazan drugi korišteni identitet, $z_{2n}-1=(y_n+y_{n-1})^2$. □

Napomena. Identitet $y_{2n+1}=2y_nz_n$ slijedi i iz Korolara 7 u [20], tzv. identiteta zbroja i razlike koji vrijede za Pellovu jednadžbu. Prema njima je

$$y_{m\pm(n+1)}=z_ny_m\pm z_my_n,\ m\geqslant n.$$

Za $m=n$, iz zadnje jednakosti slijedi upravo $y_{2n+1}=2y_nz_n$.

3.5 Proširenje $D(-2k^2)$-para $\{2k^2, 2k^2+1\}$ za neparan k

Zasad smo potpuno riješili problem proširenja $D(-2k^2)$-para $\{2k^2, 2k^2+1\}$ za paran k. Već smo komentirali da ne postoji $D(-2k^2)$-četvorka za neparan k, pa u tom slučaju preostaje pitanje za koje c je $\{2k^2, 2k^2+1, c\}$ skup s $D(-2k^2)$-svojstvom. Na ovo pitanje lako je odgovoriti koristeći prethodne tehnike.

Naime, ako je $\{2k^2, 2k^2+1, c\}$ skup s $D(-2k^2)$-svojstvom, onda je $2k^2c - 2k^2 = (s')^2$. Tada $2k$ dijeli s', odnosno, postoji nenegativan cijeli broj s takav da je $s' = 2ks$, pa je $c - 1 = 2s^2$. Također je $(2k^2+1)c - 2k^2 = t^2$, za neki nenegativan cijeli broj t. Eliminacijom c dobivamo Pellovu jednadžbu $t^2 - (4k^2+2)s^2 = 1$. Fundamentalno rješenje je $(t, s) = (4k^2+1, 2k)$, pa možemo dobiti rekurzivnu relaciju za moguća rješenja s:

$$s_0 = 0, s_1 = 2k, s_{\nu+2} = 2(4k^2+1)s_{\nu+1} - s_\nu. \tag{3.5.1}$$

Dakle, svi mogući c određeni su kao $c = 2s_\nu^2 + 1$ za neki $\nu \in \mathbb{N}_0$.

Iz ovog možemo dobiti i rekurzivnu relaciju za moguće vrijednosti c. Rješavanjem rekurzije (3.5.1) dobivamo

$$s_\nu = \frac{1}{2\sqrt{4k^2+2}} \left((4k^2+1+2k\sqrt{4k^2+2})^n + (4k^2+1-2k\sqrt{4k^2+2})^n \right).$$

Iz toga vidimo da se u izrazu za $c_\nu = 2s_\nu^2 + 1$ pojavljuju $(4k^2+1+2k\sqrt{4k^2+2})^2$ s eksponentom n, $(4k^2+1-2k\sqrt{4k^2+2})^2$ s eksponentom n, te neke konstante. Budući da je $(4k^2+1\pm 2k\sqrt{4k^2+2})^2 = 32k^4+16k^2+1 \pm 4k(4k^2+1)\sqrt{4k^2+2}$, te je zbroj ova dva konjugata $64k^4+32k^2+2$, a produkt 1, znači da c_ν zadovoljaju rekurziju s karakterističnom jednadžbom $(x^2-(64k^4+32k^2+2)x+1)(x-1) = 0$, tj. $x^3-(64k^4+32k^2+3)x^2+(64k^4+32k^2+3)x-1 = 0$.

Dakle, rekurzivna relacija za brojeve c_ν je

$$c_{\nu+3} = (64k^4+32k^2+3)(c_{\nu+2} - c_{\nu+1}) + c_\nu,$$

s početnim uvjetima $c_0 = 1, c_1 = 8k^2+1, c_2 = 2s_2^2+1 = 512k^6+256k^4+32k^2+1$.

Time smo dokazali sljedeći teorem.

Teorem 3.5.1. *Neka je k neparan prirodan broj. Za svaki c takav da je $\{2k^2, 2k^2+1, c\}$ skup s $D(-2k^2)$-svojstvom postoji $\nu \in \mathbb{N}_0$ takav da je $c = c_\nu$, gdje je*

$$c_{\nu+3} = (64k^4+32k^2+3)(c_{\nu+2} - c_{\nu+1}) + c_\nu,$$

uz početne uvjete $c_0 = 1, c_1 = 8k^2+1, c_2 = 512k^6+256k^4+32k^2+1$.

3.6 Sličan problem – proširenje $D(-k^2)$-trojke $\{1, 2k^2, 2k^2+2k+1\}$

Možemo promatrati proširenje $D(-k^2)$-trojke $\{1, 2k^2, 2k^2+2k+1\}$ na sličan način. Dujella je pokazao (Remark 3 u [12]) da, ako $\{a_1, a_2, a_3, a_4\}$ ima $D(16n+12)$-svojstvo, onda su svi a_i parni. Kako je $2k^2+2k+1$ neparan, zaključujemo da $-k^2$ ne može biti kongruentno 12 modulo 16, odnosno da k ne može biti kongruentan 2 mod 4.

Proširujući $\{1, 2k^2, 2k^2+2k+1\}$ s d, dobivamo $d-k^2 = x^2, 2k^2d-k^2 = (y')^2$, $(2k^2+2k+1)d-k^2 = z^2$. Iz druge jednadžbe zaključujemo da $k|y'$, odnosno da postoji prirodan broj y takav da je $y' = ky$, pa druga jednadžba postaje $2d-1 = y^2$. Eliminirajući d iz ove i prve jednadžbe je $y^2 - 2x^2 = 2k^2 - 1$. Analogno, eliminirajući d iz $2d-1 = y^2$ i $(2k^2+2k+1)d - k^2 = z^2$ slijedi $z^2 - (4k^2+4k+2)y^2 = 4k+2$. Dobili smo sustav simultanih pellovskih jednadžbi

$$\begin{aligned} y^2 - 2x^2 &= 2k^2 - 1 \\ z^2 - (4k^2+4k+2)y^2 &= 4k+2. \end{aligned}$$

Iako nijedna od ovih jednadžbi nije Pellova, druga jednadžba ima samo dva fundamentalna rješenja, $(z^*, y^*) \in \{(2k+2, 1), (-2k-2, 1)\}$. Ovo možemo pokazati smještanjem $(z^*)^2$ između kvadrata od $(2k+1)y^*$ i $(2k+1)y^*+1$, koristeći poznatu gornju granicu za fundamentalno rješenje y^*. Konkretnije, $z^2 = (4k^2+4k+2)y^2+4k+2 > (4k^2+4k+1)y^2 = ((2k+1)y)^2$ očito vrijedi. S druge strane, kako bismo dokazali $(z^*)^2 \leqslant ((2k+1)y^*+1)^2$, promotrimo Pellovu jednadžbu $z^2-(4k^2+4k+2)y^2 = 1$, koja pripada drugoj dobivenoj jednadžbi iz sustava. Ona ima fundamentalno rješenje $8k^2+8k+3+(4k+2)\sqrt{4k^2+4k+2}$. Naime, za $(z, y) = (2k+1, 1)$ dobivamo $z^2-(4k^2+4k+2)y^2 = -1$, pa kvadriranjem $2k+1+\sqrt{4k^2+4k+2}$ dobivamo fundamentalno rješenje Pellove jednadžbe. Iz toga je, prema Teoremu 2.2.8,

$$0 \leqslant y^* \leqslant \frac{4k+2}{\sqrt{2(8k^2+8k+2)}} \cdot \sqrt{4k^2+4k+2}. \tag{3.6.1}$$

Tvrdnja $(z^*)^2 < ((2k+1)y^*+1)^2$ ekvivalentna je tvrdnji $(4k^2+4k+2)(y^*)^2+4k+2 < ((2k+1)y^*+1)^2$, odnosno $(y^*)^2-(4k+2)y^*+4k+1 < 0$. Kvadratni polinom $y^2-(4k+2)y+4k+1$ ima nultočke 1 i $4k+1$, pa će željena nejednakost vrijediti ako je $y^* \in \langle 1, 4k+1\rangle$. Iz (3.6.1) vidimo da je za $y^* < 4k+1$ dovoljno dokazati da je

$$\frac{\sqrt{4k^2+4k+2}}{\sqrt{2(8k^2+8k+2)}} < \frac{4k+1}{4k+2},$$

što je, sređivanjem, ekvivalentno sa $192k^4+256k^3+96k^2-4 > 0$. Ova tvrdnja vrijedi jer

je k prirodan broj.

Rješenje $y^* = 0$ nije moguće jer 2 nije kvadratni ostatak modulo 4 ($z^2 \neq 4k+2$). Stoga je $(2k+1)y^* < z^* < (2k+1)y^* + 1$ (što nije moguće za prirodan z^*) , osim ako je $y^* = 1$. Time dobivamo jedina fundamentalna rješenja $(2k+2, 1)$ i $(-2k-2, 1)$ jednadžbe $z^2 - (4k^2+4k+2)y^2 = 4k+2$.

Fundamentalno rješenje $(2k+2, 1)$ daje nam rekurzije za rješenja druge jednadžbe, $y_{n+1} = (8k^2+8k+3)y_n + (4k+2)z_n$ iz čega zaključujemo da je $y_{n+1} \equiv y_n \pmod{4k+2}$, tj. $y_n \equiv y_0 = 1 \pmod{4k+2}$. Isto vrijedi za niz koji generira drugo fundamentalno rješenje, a za rješenja koja se dobivaju množenjem s rješenjem -1 pripadne Pellove jednadžbe vrijedi $y \equiv -1 \pmod{4k+2}$. U svakom slučaju, iz prve jednadžbe je $2x^2 = y^2 - 2k^2 + 1 \equiv 1 - 2k^2 + 1 = 2(1-k^2) \pmod{4k+2}$, pa je $x^2 \equiv 1 - k^2 \pmod{2k+1}$ i

$$x^2 \equiv 1 - k^2 = (1-k)(1+k) \equiv (k+2)(k+1) = k^2 + 3k + 2 \equiv k^2 + k + 1 \pmod{2k+1}$$

Množenjem s 4 slijedi da je $4x^2 \equiv 4k^2 + 4k + 4 - (2k+1)^2 = 3 \pmod{2k+1}$.

Dakle, 3 je kvadratni ostatak modulo $2k+1$. Također je i kvadratni ostatak modulo svaki prost faktor od $2k+1$. Sad ćemo pokazati da je 3 kvadratni ostatak modulo prost broj p ako i samo ako je $p \equiv \pm 1 \pmod{12}$. Iz Gaussovog kvadratnog reciprociteta je

$$\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$$

pa imamo dva slučaja.

- $p \equiv 1 \pmod 4$ Tada je $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$. Budući da je 1 jedini kvadratni ostatak modulo 3 , da bi 3 bio kvadrat modulo p, mora biti $p \equiv 1 \pmod 3$.
  Iz toga i iz $p \equiv 1 \pmod 4$ slijedi da je $p \equiv 1 \pmod{12}$.
- $p \equiv 3 \pmod 4$ Tada je $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$, pa da bi 3 bio kvadratni ostatak modulo p, mora p biti kvadratni neostatak modulo 3 tj. $p \equiv 2 \pmod 3$.
  Sada je $p \equiv 11 = -1 \pmod{12}$.

Kako je 3 kvadratni ostatak modulo prost p ako i samo ako je $p \equiv \pm 1 \pmod{12}$, slijedi da su svi prosti faktori od $2k+1$ tog oblika ili jednaki 3. Samo jedna trojka može dijeliti $2k+1$, jer $3 \mid 4x^2 - 3$ implicira $9 \nmid 4x^2 - 3$. Stoga $2k+1 \not\equiv 0 \pmod 9$, odnosno $k \not\equiv 4 \pmod 9$. Da $2k+1 \not\equiv 1, 3, 9, 11 \pmod{12}$, odnosno, da je $2k+1 \equiv 5, 7 \pmod{12}$, onda bi $2k+1$ imao proste faktore koji nisu ni 3 niti daju ostatke ± 1 pri dijeljenju s 12.

Stoga možemo zaključiti da za $k \equiv 2, 3 \pmod 6$ i $k \equiv 4 \pmod 9$ ne postoji proširenje do četvorke.

Poglavlje 4

Familija Diofantovih trojki $\{k-1, k+1, 16k^3-4k\}$ u Gaussovim cijelim brojevima

U ovom poglavlju proučavamo proširivost trojke $\{k-1, k+1, 16k^3-4k\}$ u Gaussovim cijelim brojevima $\mathbb{Z}[i]$. Slična parametarska familija, $\{k-1, k+1, 4k\}$, proučavana je u [21], gdje je pokazano da je proširenje do Diofantove četvorke jedinstveno, i to s elementom $16k^3-4k$. Napomenimo da je familija trojki istog oblika kao ovdje proučavana u skupu racionalnih cijelih brojeva u [9], gdje je dokazana sljedeća tvrdnja. Ako je $\{k-1, k+1, 16k^3-4k, d\}$ Diofantova četvorka cijelih brojeva, onda je $d = 4k$ ili $d = 64k^5-48k^3+8k$. Ova familija trojki pojavila se kao zaseban slučaj u proučavanju proširenja Diofantovog para $\{k-1, k+1\}$, kod kojeg nije bilo moguće primijeniti istu metodu kao kod ostalih slučajeva. Kao što autori (Bugeaud, Dujella i Mignotte) ističu, poteškoće dolaze zbog toga što rupa (udaljenost) između $k+1$ i $16k^3-4k$ nije dovoljno velika. Isti problem susrest ćemo i ovdje. Iako ćemo dobiti neke potencijalno korisne rezultate, ovaj problem nećemo moći razriješiti kao problem u prošlom poglavlju.

4.1 Uvod – sustav pellovskih jednadžbi

Skup $\{k-1, k+1, 16k^3-4k\}$ je Diofantova trojka za svaki Gaussov cijeli broj k. Naime, vrijedi da je $(k-1)(k+1)+1 = k^2$, $(k-1)(16k^3-4k)+1 = (4k^2-2k-1)^2$ i $(k+1)(16k^3-4k)+1 = (4k^2+2k-1)^2$. Označimo sa $s = 4k^2-2k-1, t = 4k^2+2k-1$. Pretpostavimo sad da d proširuje ovu Diofantovu trojku, odnosno, neka je

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

Diofantova četvorka u $\mathbb{Z}[i]$. Tada postoje $x, y, z \in \mathbb{Z}[i]$ takvi da je

$$(k-1)d+1 = x^2,\ (k+1)d+1 = y^2,\ (16k^3-4k)d+1 = z^2.$$

Eliminacijom parametra d dobivamo sustav

$$(k+1)x^2 - (k-1)y^2 = 2, \tag{4.1.1}$$
$$(16k^3-4k)x^2 - (k-1)z^2 = 16k^3 - 5k + 1 \tag{4.1.2}$$

Neka je $|k| > 3$. Prema Lemmi 2.4 u članku [21], sva rješenja jednadžbe (4.1.1) dana su sa $x = \pm v_n$, gdje je (v_n) niz rekurzivno zadan kao

$$v_0 = 1,\ v_1 = 2k-1,\ v_{n+2} = 2kv_{n+1} - v_n,\ \text{za sve } n \geqslant 0. \tag{4.1.3}$$

Sva rješenja jednadžbe (4.1.2) opisuju se u sljedećoj lemi, koja se dokazuje potpuno analogno kao Lemma 2.2 u [21]. Također, kasnije u disertaciji dokazana je općenitija tvrdnja (Lema 5.1.2).

Lema 4.1.1. *Neka je $k \in \mathbb{Z}[i]\backslash\{0,1\}$. Tada postoje $j_0 \in \mathbb{N}$, $x_1^{(j)}, z_1^{(j)} \in \mathbb{Z}[i]$, $j = 1, \ldots, j_0$ takvi da je*

a) $(x_1^{(j)}, z_1^{(j)})$ rješenje od (4.1.2) za sve $j = 1, \ldots, j_0$,

b) vrijedi

$$\begin{aligned} |x_1^{(j)}|^2 &\leqslant \frac{|16k^3-5k+1||k-1|}{|4k^2-2k-1|-1} \\ |z_1^{(j)}|^2 &\leqslant \frac{|16k^3-4k||16k^3-5k+1|}{|4k^2-2k-1|-1} + \frac{|16k^3-5k+1|}{|k-1|} \end{aligned}$$

za sve $j = 1, \ldots, j_0$,

c) za svako rješenje (x, z) od (4.1.2) postoje $j \in \{1, \ldots, j_0\}$ i $m \in \mathbb{Z}$ takvi da je

$$\begin{aligned} x\sqrt{16k^3-4k} + z\sqrt{k-1} =& (x_1^{(j)}\sqrt{16k^3-4k} + z_1^{(j)}\sqrt{k-1})\cdot \\ &\cdot \left(4k^2-2k-1+\sqrt{(k-1)(16k^3-4k)}\right)^m. \end{aligned}$$

Dakle, za rješenje x jednadžbe (4.1.2) vrijedi $x = w_m^{(j)}$ za neki $j \in \{1, \ldots, j_0\}$ i $m \in \mathbb{N}_0$, pri čemu je niz $(w_m^{(j)})$ rekurzivno zadan s

$$w_0^{(j)} = x_1^{(j)},\ w_1^{(j)} = x_1^{(j)}(4k^2-2k-1) + z_1^{(j)}(k-1),\ w_{m+2}^{(j)} = 2(4k^2-2k-1)w_{m+1}^{(j)} - w_m^{(j)},\ m \geqslant 0.$$

U nastavku teksta privremeno ispuštamo gornji indeks (j).

Ako x zadovoljava obje jednadžbe (4.1.1) i (4.1.2), onda je $x = v_n = w_m$. Dakle, zapravo tražimo zajedničke članove nizova (v_n) i (w_m).

Sada primjenjujemo metodu kongruencija. Promotrimo ostatke koje elementi nizova (v_n) i (w_m) daju pri dijeljenju sa $s = 4k^2 - 2k - 1$. Induktivno se pokazuje sljedeća lema.

Lema 4.1.2. *Za nizove (v_n) i (w_m) vrijedi da je*

$$v_n \equiv 0, \pm 1, \pm(2k-1) \pmod{4k^2-2k-1} \text{ i}$$
$$w_m \equiv \pm x_1, \pm z_1(k-1) \pmod{4k^2-2k-1}$$

za sve indekse n i m.

Analizom ovih kombinacija, dolazimo do toga su, kad je $|k| > 17$, sva fundamentalna rješenja koja generiraju nizove (w_m) koji mogu imati presjek s nizom (v_n),

$$(x_1, z_1) \in \{(\pm 1, \pm 1), (\pm k, \pm(4k^2+2k-1)), (\pm(2k-1), \pm(8k^2-1))\}.$$

Npr. ako je $x_1 \equiv 0 \pmod{4k^2-2k-1}$, onda je $x_1 = 0$ ili $|x_1| \geqslant 4|k|^2 - 2|k| - 1$. Međutim, iz ograde u Lemi 4.1.1 je onda

$$(4|k|^2 - 2|k| - 1)^2 \leqslant \frac{|16k^3 - 5k + 1||k-1|}{|4k^2-2k-1| - 1},$$

odnosno $(4|k|^2-2|k|-1)^2(|4k^2-2k-1|-1) \leqslant |16k^3-5k+1||k-1|$, iz čega slijedi $16|k|^4+16|k|^3+5|k|^2+4|k|+1 \geqslant 64|k|^6-96|k|^5-16|k|^4-56|k|^3-4|k|^2-10|k|-2$, što je ekvivalentno s $-64|k|^6+96|k|^5+32|k|^4+72|k|^3+9|k|^2+14|k|+3 \geqslant 0$, što ne vrijedi za dovoljno velik $|k|$, a numerički je određena najveća nultočka polinoma s lijeve strane u $|k|$ kao 2.04414. Za $x_1 \equiv \pm 1, \pm(2k-1)$ slično isključimo sve mogućnosti osim $x_1 = \pm 1$ i $x_1 = \pm(2k-1)$, što daje rješenja $(\pm 1, \pm 1), (\pm(2k-1), \pm(8k^2-1))$.

Ako je $z_1(k-1) \equiv 0, \pm 1, \pm(2k-1) \pmod{4k^2-2k-1}$, onda je $z_1 = u(4k^2-2k-1)+r$ gdje je u Gaussov cijeli broj, a $r \in \{0, \pm 4k, \pm(4k+2)\}$, jer je $-4k-2$ inverz od $k-1$ modulo $4k^2-2k-1$. Iz jednadžbe (4.1.2) slijedi da $k|1-z_1^2$. S druge strane je $z_1 \equiv -u+r \equiv -u, -u \pm 2 \pmod{k}$, pa $k|1-u^2$ ili $k|1-(u\pm 2)^2$. Ako je $|u| \leqslant 2$, slijedi da je $|1-u^2| \leqslant 1+|u|^2 \leqslant 5$ i $|1-(u\pm 2)^2| \leqslant |u|^2+4|u|+5 \leqslant 17$, pa dobivena djeljivost ne može vrijediti za $|k| > 17$, osim ako je višekratnik 0, tj. $u = \pm 1$. Ovdje dobivamo rješenja $(\pm k, \pm(4k^2+2k-1))$ za $u = \pm 1$ i $z_1 = u(4k^2-2k-1)$. Nije moguće da je $u = \pm 1$ i $r = \mp(4k+2)$ jer iz jednadžbe (4.1.2) slijedi da je $x_1^2 = \frac{(k-1)(4k^2-6k-3)^2+(16k^3-5k+1)}{16k^3-4k} \in \mathbb{Z}[i]$. Iz toga dobivamo da $2k^2-k|8k+8$, što nije moguće za $|k| > 17$ (jer je $8k+8 = 0$ ili $8|k|+8 \geqslant 2|k|^2-|k|$). Ako je $|u| \geqslant \sqrt{5}$, ponovo suprotstavljanjem s gornjom ogradom iz Leme 4.1.1 vidimo da ne može vrijediti za $|k| > 17$: $|z_1| \geqslant \sqrt{5}(4|k|^2-2|k|-1)-4|k|-2 = 4\sqrt{5}|k|^2-(4+2\sqrt{5})|k|-(2+\sqrt{5})$, pa prema Lemi 4.1.1 slijedi

$$80|k|^4 - 32\sqrt{5}|k|^3 - 80|k|^3 - 4|k|^2 + 16\sqrt{5}|k| + 36|k| + 4\sqrt{5} + 9 \leqslant$$
$$\leqslant \frac{(16|k|^3+4|k|)(16|k|^3+5|k|+1|}{4|k|^2-2|k|-2} + \frac{16|k|^3+5|k|+1|}{|k|-1},$$

pa množenjem i sređivanjem slijedi $-64|k|^7 + (544+128\sqrt{5})|k|^6 + (-256-192\sqrt{5})|k|^5 +$

$(-488-64\sqrt{5})|k|^4+(332+144\sqrt{5})|k|^3+(40+24\sqrt{5})|k|^2+(-88-32\sqrt{5})|k|-8\sqrt{5}-20 \leqslant 0$, što ne vrijedi za $|k| > 12.019$.

Lema 4.1.3. *Ako je $|k| > 17$ i sustav jednadžbi (4.1.1) i (4.1.2) ima rješenje $x \neq \pm 1$, onda postoje prirodni m i n te $1 \leqslant j \leqslant 6$ takvi da je*

$$v_n = \pm w_m^{(j)},$$

gdje su nizovi $(w_m^{(j)})$ dani sljedećim početnim uvjetima

$$\begin{aligned} w_0^{(1)} = 1, &\quad w_1^{(1)} = 4k^2-k-2, \\ w_0^{(2)} = 1, &\quad w_1^{(2)} = 4k^2-3k, \\ w_0^{(3)} = k, &\quad w_1^{(3)} = 8k^3-4k^2-4k+1, \\ w_0^{(4)} = k, &\quad w_1^{(4)} = 2k-1, \\ w_0^{(5)} = 2k-1, &\quad w_1^{(5)} = 16k^3-16k^2-k+2, \\ w_0^{(6)} = 2k-1, &\quad w_1^{(6)} = k, \end{aligned}$$

a svi ostali članovi s

$$w_{m+2}^{(j)} = 2(4k^2-2k-1)w_{m+1}^{(j)} - w_m^{(j)}, \ m \geqslant 0.$$

Primijetimo da se nizovi $(w_m^{(j)})_{j=1,\ldots,6}$ sijeku s (v_n) redom u $\{1\}$, $\{1\}$, $\{8k^3-4k^2-4k+1\}$, $\{2k-1\}$, $\{2k-1\}$, $\{2k-1, 8k^3-4k^2-4k+1\}$ što je očekivano jer odgovara proširenjima $d \in \{0, 4k, 64k^5-48k^3+8k\}$.

4.2 Donja granica za rješenja

S ciljem dobivanja donje ograde za rješenje $|x|$ gledamo dobivene nizove modulo $4k(k-1)$. Tamo gdje nije dana ograda na $|k|$, pretpostavljamo da je $|k| > 17$. Izračunom prvih nekoliko vrijednosti ovih nizova, dobivamo da vrijedi

$$\begin{aligned} (v_n)_{n\geqslant 0} &\equiv (1, 2k-1, 2k-1, 1, 1, 2k-1, \ldots) && \pmod{4k(k-1)}, \\ (w_m^{(1)})_{m\geqslant 0} &\equiv (1, 3k-2, -2k+3, 5k-4, -4k+5, 7k-6, \ldots) && \pmod{4k(k-1)}, \\ (w_m^{(2)})_{m\geqslant 0} &\equiv (1, k, 2k-1, -k+2, 4k-3, -3k+4, \ldots) && \pmod{4k(k-1)}, \\ (w_m^{(3)})_{m\geqslant 0} &\equiv (k, 1, 3k-2, -2k+3, 5k-4, -4k+5, \ldots) && \pmod{4k(k-1)}, \\ (w_m^{(4)})_{m\geqslant 0} &\equiv (k, 2k-1, -k+2, 4k-3, -3k+4, 6k-5, \ldots) && \pmod{4k(k-1)}, \\ (w_m^{(5)})_{m\geqslant 0} &\equiv (2k-1, -k+2, 4k-3, -3k+4, 6k-5, \ldots) && \pmod{4k(k-1)}, \\ (w_m^{(6)})_{m\geqslant 0} &\equiv (2k-1, k, 1, 3k-2, -2k+3, 5k-4, \ldots) && \pmod{4k(k-1)}. \end{aligned}$$

Lema 4.2.1. *Neka je k Gaussov cijeli broj modula većeg od 1. Za niz $(v_n)_n$ definiran u (4.1.3) vrijedi da je $v_n \equiv 1 \pmod{4k(k-1)}$ ako je $n \equiv 0, 3 \pmod 4$, dok je $v_n \equiv 2k-1 \pmod{4k(k-1)}$ za $n \equiv 1, 2 \pmod 4$.*

Za niz $w_m^{(1)}$ definiran u Lemi 4.1.3 vrijedi da je $w_{2m}^{(1)} \equiv -2mk+2m+1 \pmod{4k(k-1)}$ i $w_{2m+1}^{(1)} \equiv (2m+3)k-2m-2 \pmod{4k(k-1)}$ za sve $m \in \mathbb{N}_0$. Također, niz $w_m^{(1)}$ je rastući po apsolutnoj vrijednosti, te je $|w_m^{(1)}| \geqslant (8|k|^2-4|k|-3)^{m-1}$ za svaki indeks $m \geqslant 0$. Slično, za ostale nizove $w_m^{(j)}$ za $j = 2, \ldots, 6$ vrijedi da su rastući nakon indeksa $m = 1$ te $|w_m^{(j)}| \geqslant (8|k|^2-4|k|-3)^{m-1}$. Vrijede i sljedeće kongruencije:

$$\begin{aligned}
&w_{2m}^{(2)} \equiv 2mk-(2m-1), && w_{2m+1}^{(2)} \equiv -(2m-1)k+2m && \pmod{(4k(k-1))}\\
&w_{2m}^{(3)} \equiv (2m+1)k-2m, && w_{2m+1}^{(3)} \equiv -2mk+2m+1 && \pmod{(4k(k-1))}\\
&w_{2m}^{(4)} \equiv (1-2m)k+2m, && w_{2m+1}^{(4)} \equiv 2mk-(2m+1) && \pmod{(4k(k-1))}\\
&w_{2m}^{(5)} \equiv (2m+2)k-(2m+1), && w_{2m+1}^{(5)} \equiv (-2m-1)k+2m && \pmod{(4k(k-1))}\\
&w_{2m}^{(6)} \equiv (2-2m)k+(2m-1), && w_{2m+1}^{(6)} \equiv (2m+1)k-2m && \pmod{(4k(k-1))}
\end{aligned}$$

Dokaz. Sve tvrdnje dokazuju se indukcijom. Dokažimo prvo da je niz $|w_m^{(1)}|$ rastući.

Baza, $|w_1| \geqslant |w_0|$, vrijedi jer je $|4k^2-k-2| \geqslant 4|k|^2-|k|-2 \geqslant 1 = |w_0|$ za $|k| \geqslant 1$.

Iz $w_{m+1} = 2(4k^2-2k-1)w_m - w_{m-1}$ slijedi

$$\begin{aligned}
|w_{m+1}| &\geqslant (8|k|^2-4|k|-2)|w_m| - |w_{m-1}|\\
&\geqslant (8|k|^2-4|k|-3)|w_m| + |w_m| - |w_{m-1}|\\
&\geqslant (8|k|^2-4|k|-3)|w_m|
\end{aligned}$$

Iz ovoga direktno slijedi ne samo da je niz rastući, nego i $|w_m| \geqslant (8|k|^2-4|k|-3)^{m-1}$ za sve $m \geqslant 0$. Također, ovo vrijedi za $w_m^{(i)}$ za sve $i = 1, \ldots, 6$.

Induktivno se pokaže i da je $w_{2m}^{(1)} \equiv -2mk+2m+1 \pmod{4k(k-1)}$ te $w_{2m+1}^{(1)} \equiv (2m+3)k-2m-2 \pmod{4k(k-1)}$. Baza, za $m = 0$, izračunata je prije iskaza leme. Ako induktivno pretpostavimo da je $w_{2m}^{(1)} \equiv -2mk+2m+1 \pmod{4k(k-1)}$ te $w_{2m+1}^{(1)} \equiv (2m+3)k-2m-2 \pmod{4k(k-1)}$, onda je

$$\begin{aligned}
w_{2m+2}^{(1)} &= 2(4k^2-2k-1)w_{2m+1} - w_{2m}\\
&\equiv 2(2k-1)\cdot((2m+3)k-2m-2) - (-2mk+2m+1)\\
&= (2m+3)(4k^2-2k) - (2m+2)(4k-2) + 2mk - 2m - 1\\
&\equiv (2m+3)\cdot 2k - 8mk + 4m - 8k + 4 + 2mk - 2m - 1\\
&= -2mk - 2k + 2m + 3\\
&= -2(m+1)k + 2m + 3 \pmod{4k(k-1)},
\end{aligned}$$

što je i trebalo dokazati. Slično dobivamo, koristeći ovu dokazanu tvrdnju, da je

$$\begin{aligned} w^{(1)}_{2m+3} &= 2(4k^2-2k-1)w_{2m+2} - w_{2m+1} \\ &\equiv 2(2k-1)(-2(m+1)k+2m+3) - ((2m+3)k-2m-2) \\ &= -2(m+1)(4k^2-2k) + 2(2k-1)(2m+3) - (2m+3)k + 2m + 2 \\ &\equiv -2(m+1)\cdot 2k + 8mk + 12k - 4m - 6 - 2mk - 3k + 2m + 2 \\ &= (2m+5)k - 2m - 4 \pmod{4k(k-1)}. \end{aligned}$$

Ovime smo induktivno dokazali kongruencijske tvrdnje za $(w^{(1)}_m)$, a potpuno analogno dokazuju se tvrdnje za preostale nizove. □

Promotrimo parni slučaj: $w^{(1)}_{2m} = v_{2n} \Rightarrow -2mk + 2m + 1 \equiv 1 \pmod{4k(k-1)}$ pa $4k^2 - 4k$ dijeli $2mk - 2m$, tj. $2k(k-1)|m(k-1)$ i, najbitnije $2k|m$. Analogno se iz $w_{2m} = v_{2n+1} \equiv 2k-1 \pmod{4k(k-1)}$ dobiva da $2k|m+1$. Iz oba ta zaključka, $2k|m$ i $2k|m+1$ slijedi da je $m \geqslant 2|k| - 1$, osim ako je m takav da je višekratnik od $2k$ zapravo jednak 0. Dakle, ako $m \neq 0, -1$, slijedi da je

$$|x| \geqslant (8|k|^2 - 4|k| - 3)^{4|k|-3}.$$

Za neparne indekse u nizu $(w^{(1)}_m)$, iz $(2m+3)k - 2m - 2 \equiv 1 \pmod{4k(k-1)}$ slijedi da $4k(k-1)|(2m+3)(k-1)$, odnosno da $4k|2m+3$, što je očito nemoguće (parni broj bi dijelio neparni). Analogno iz $(2m+3)k-2m-2 \equiv 1 \pmod{4k(k-1)}$ slijedi da $4k|2m+1$, također nemoguće.

Slični zaključci dobivaju se na isti način i za ostale nizove $(w^{(i)}_m)_m$ $(i = 2, \ldots, 6)$: za jednu parnost indeksa dobiva se kontradikcija, a za drugu $2k|m$ ili $2k|m \pm 1$. U svakom slučaju je $m \geqslant 2|k| - 1$ ako $m \notin \{-1, 0, 1\}$ i vrijedi ista donja granica, ili eventualno još veća (kad je m u neparnom indeksu $2m+1$). Dakle. dokazali smo sljedeći rezultat.

Propozicija 4.2.2. *Ako je (x, y, z) rješenje sustava*

$$(k+1)x^2 - (k-1)y^2 = 2, \tag{4.1.1}$$
$$(16k^3 - 4k)x^2 - (k-1)z^2 = 16k^3 - 5k + 1, \tag{4.1.2}$$

za $|k| > 17$ i $x \notin \{1, k, 2k-1, 8k^3 - 4k^2 - 4k + 1\}$, onda je $|x| \geqslant (8|k|^2 - 4|k| - 3)^{4|k|-3}$.

Napomenimo da iznimke $x = 1$, $x = k$, $x = 2k-1$ i $x = 8k^3 - 4k^2 - 4k + 1$ dolaze od indeksa $m = 0$ (ili $m = 1$), odnosno od situacija kad iz $2k|m$ ne možemo zaključiti da je $m \geqslant 2|k|$.

4.3 Problem primjene teorema Jadrijević–Ziegler

Postoje dva bitno različita sustava koja se ovdje mogu rješavati. Jedan je iskazan u Propoziciji 4.2.2 i sad ćemo pokazati da se teorem Jadrijević–Ziegler [31] ne može primijeniti jer uvjeti nisu zadovoljeni. Drugi sustav je kad se u obje jednadžbe s lijeve strane pojavljuje koeficijent $16k^3-4k$, a za njega ćemo kasnije pokazati da, iako su uvjeti teorema zadovoljeni, on ne može dati koristan rezultat.

Lema 4.3.1. *Ako su x, y, z rješenja sustava (4.1.1) i (4.1.2), a $\theta_1^{(1)} = \pm\sqrt{\dfrac{k+1}{k-1}}$, $\theta_1^{(2)} = -\theta_1^{(1)}$, $\theta_2^{(1)} = \pm\sqrt{\dfrac{4k^2-1}{4k(k-1)}}$, $\theta_2^{(2)} = -\theta_2^{(1)}$, pri čemu su predznaci odabrani tako da je*

$$\left|\theta_1^{(1)} - \frac{y}{x}\right| \leqslant \left|\theta_1^{(2)} - \frac{y}{x}\right| \quad i \quad \left|\theta_2^{(1)} - \frac{z}{4kx}\right| \leqslant \left|\theta_2^{(2)} - \frac{z}{4kx}\right|,$$

onda je

$$\begin{aligned}\left|\theta_1^{(1)} - \frac{4ky}{4kx}\right| &\leqslant \frac{2}{\sqrt{|k^2-1|}} \cdot \frac{1}{|x|^2}\\ \left|\theta_2^{(1)} - \frac{z}{4kx}\right| &\leqslant \frac{|16k^3-5k+1|}{8\sqrt{|4k^6-4k^5-k^4+k^3|}} \cdot \frac{1}{|x|^2}.\end{aligned}$$

Dokaz. Prva nejednakost, $\left|\theta_1^{(1)} - \dfrac{4ky}{4kx}\right| \leqslant \dfrac{2}{\sqrt{|k^2-1|}} \cdot \dfrac{1}{|x|^2}$, dobivena je već u članku [21]. Isto tako, vrijedi

$$\begin{aligned}\left|\theta_2^{(1)} - \frac{z}{4kx}\right| &= \left|(\theta_2^{(1)})^2 - \frac{z^2}{16k^2x^2}\right| \cdot \left|\theta_2^{(1)} + \frac{z}{4kx}\right|^{-1}\\ &= \left|\frac{1}{16k^2}\left(\frac{16k^3-4k}{k-1} - \frac{z^2}{x^2}\right)\right| \cdot \left|\theta_2^{(2)} - \frac{z}{4kx}\right|^{-1}\\ &\overset{(4.1.2)}{=} \frac{|16k^3-5k+1|}{|16k^3-16k^2|} \cdot \frac{1}{|x|^2} \cdot \left|\theta_2^{(2)} - \frac{z}{4kx}\right|^{-1} \qquad (4.3.1)\end{aligned}$$

Nadalje, zbog odabira predznaka je

$$\left|\theta_2^{(2)} - \frac{z}{4kx}\right| \geqslant \frac{1}{2}\left(\left|\theta_2^{(1)} - \frac{z}{4kx}\right| + \left|\theta_2^{(2)} - \frac{z}{4kx}\right|\right) \geqslant \frac{1}{2}|\theta_2^{(1)} - \theta_2^{(2)}| = \left|\sqrt{\frac{4k^2-1}{4k^2-4k}}\right|$$

Uvrštavanjem u (4.3.1) dobivamo

$$\left|\theta_2^{(1)} - \frac{z}{4kx}\right| \leqslant \frac{|16k^3-5k+1|}{|16k^3-16k^2|} \cdot \left|\sqrt{\frac{4k(k-1)}{4k^2-1}}\right| \cdot \frac{1}{|x|^2} = \frac{|16k^3-5k+1|}{8\sqrt{|4k^6-4k^5-k^4+k^3|}} \cdot \frac{1}{|x|^2}$$

□

Sad želimo primijeniti sljedeći teorem iz [31].

Teorem 4.3.2 ([31, Theorem 7.1]). *Neka je $\theta_i = \sqrt{1+\frac{a_i}{T}}, i = 1, 2$ s $a_1 \neq a_2$ i T u prstenu cijelih brojeva imaginarnog kvadratnog polja K. Neka je $|T| > M = \max\{|a_1|, |a_2|\}$,*

$$L = \frac{27}{16|a_1|^2|a_2|^2|a_1-a_2|^2}(|T|-M)^2 > 1.$$

Tada je

$$\max\left\{\left|\theta_1 - \frac{p_1}{q}\right|, \left|\theta_2 - \frac{p_2}{q}\right|\right\} > c|q|^{-\lambda},$$

za sve algebarske cijele $p_1, p_2, q \in K$, gdje je $\lambda = 1 + \dfrac{\log P}{\log L}$, $c^{-1} = 4pP(\max\{1, 2l\})^{\lambda-1}$,

$$l = \frac{27}{64}\frac{|T|}{|T|-M}, p = \sqrt{\frac{2|T|+3M}{2|T|-2M}}, P = 16\frac{|a_1|^2|a_2|^2|a_1-a_2|^2}{\min\{|a_1|,|a_2|,|a_1-a_2|\}^3}(2|T|+3M).$$

Kad se napiše $\theta_1 = \sqrt{\dfrac{k+1}{k-1}} = \sqrt{1+\dfrac{2}{k-1}}$, $\theta_2 = \sqrt{\dfrac{4k^2-1}{4k(k-1)}} = \sqrt{1+\dfrac{4k-1}{4k^2-4k}}$, vidimo da treba, da bi nazivnici bili isti, a brojnici algebarski cijeli, zapisati θ_1 kao $\theta_1 = \sqrt{1+\dfrac{8k}{4k^2-4k}}$, pa je $a_1 = 8k, a_2 = 4k-1, T = 4k^2-4k$. Tada je $M = \max\{|a_1|, |a_2|\} = 8|k|$, a za $|k| > 3$ je $|k-1| \geqslant |k|-1 > 2$, pa je $|T| = 4|k||k-1| > 8|k| = M$.

Međutim, $L = \dfrac{27}{16\cdot(8|k|)^2\cdot|4k-1|^2\cdot|4k+1|^2}(4|k^2-k|-8|k|)^2$ je, za dovoljno velik k, manji od 1 (jer stupanj od $|k|$ u nazivniku je 6, a u brojniku 4), a ne veći što se traži u uvjetu ovog teorema. Dakle, ne možemo direktno primijeniti ovaj teorem.

S druge strane, umjesto sustava (4.1.1) i (4.1.2), možemo rješavati sustav

$$(16k^3-4k)y^2 - (k+1)z^2 = 16k^3-5k-1, \tag{4.3.2}$$
$$(16k^3-4k)x^2 - (k-1)z^2 = 16k^3-5k+1 \tag{4.1.2}$$

i ϑ_1, ϑ_2 definirati preko

$$\vartheta_1^2 = 1 + \frac{1}{(k-1)(16k^3-4k)}, \ \theta_2^2 = 1 + \frac{1}{(k+1)(16k^3-4k)},$$

pri čemu izaberemo predznake ϑ_1 i ϑ_2 na isti način kao u Lemi 4.3.1. U tom slučaju je, uz oznake kao u Jadrijević-Ziegler teoremu,

$$a_1 = k+1, \ a_2 = k-1, \ T = (k^2-1)(16k^3-4k).$$

Napomena 7.2 iz [31] kaže da je uvjet $L > 1$ ispunjen uvijek kad je $|T| > (4M)^3$. Ovdje je

$$|(k^2-1)(16k^3-4k)| > |4(k+1)|^3,$$

što vrijedi za $k \geqslant 3.21$.

Naime, lijeva strana je $|16k^5 - 20k^3 + 4k| \geqslant 16|k|^5 - 20|k|^3 - 4|k|$, a desna je $64|k^3 + 3k^2 + 3k + 1| \leqslant 4(16|k|^3 + 48|k|^2 + 48|k| + 16)$, pa je dovoljno dokazati $4|k|^5 - 5|k|^3 - |k| > 16|k|^3 + 48|k|^2 + 48|k| + 16$ tj. $4|k|^5 - 21|k|^3 - 48|k|^2 - 49|k| - 16 > 0$, što očito vrijedi za dovoljno velik $|k|$, a najveća realna nultočka ovog polinoma $(4x^5 - 21x^3 - 48x^2 - 49x - 16)$ približno iznosi 3.20929. Sada treba pokazati da ovako izabrani ϑ_1, ϑ_2 dobro aproksimiraju kvocijent rješenja do na umnožak s nekim brojem iz $\mathbb{Q}[i]$. Konkretno, ocjenjujemo

$$\left|\vartheta_1 - \frac{sx}{(k-1)z}\right|,$$

gdje je $s^2 = (4k^2 - 2k - 1)^2$ i sličan izraz za ϑ_2, u sljedećoj lemi.

Lema 4.3.3. *Za $|k| \geqslant 5$ je*

$$\max\left\{\left|\vartheta_1^{(1)} - \frac{s(k+1)x}{(k-1)(k+1)z}\right|, \left|\vartheta_2^{(1)} - \frac{t(k-1)y}{(k-1)(k+1)z}\right|\right\} < 40|k|^2|z|^{-2},$$

gdje je $t = 4k^2 + 2k - 1$.

Dokaz.

$$\begin{aligned}
&\left|\vartheta_1^{(1)} - \frac{sx}{(k-1)z}\right| = \\
&= \left|(\vartheta_1^{(1)})^2 - \frac{s^2x^2}{(k-1)^2z^2}\right| \cdot \left|\vartheta_1^{(1)} + \frac{sx}{(k-1)z}\right|^{-1} \\
&= \left|1 + \frac{1}{(k-1)(16k^3-4k)} - \frac{s^2x^2}{(k-1)^2z^2}\right| \cdot \left|\vartheta_1^{(2)} - \frac{sx}{(k-1)z}\right|^{-1} \\
&= \left|\frac{(k-1)^2(16k^3-4k)z^2 + (k-1)z^2 - ((k-1)(16k^3-4k)+1)(16k^3-4k)x^2}{(k-1)^2(16k^3-4k)z^2}\right| \cdot \\
&\quad \cdot \left|\vartheta_1^{(2)} - \frac{sx}{(k-1)z}\right|^{-1} \\
&= \left|\frac{(k-1)(16k^3-4k)((k-1)z^2 - (16k^3-4k)x^2) + (k-1)z^2 - (16k^3-4k)x^2}{(k-1)^2(16k^3-4k)z^2}\right| \cdot \\
&\quad \cdot \left|\vartheta_1^{(2)} - \frac{sx}{(k-1)z}\right|^{-1} \\
&= \left|\frac{((k-1)(16k^3-4k)+1)((k-1)z^2 - (16k^3-4k)x^2)}{(k-1)^2 - (16k^3-4k)z^2}\right| \cdot \left|\vartheta_1^{(2)} - \frac{sx}{(k-1)z}\right|^{-1} \\
&\overset{(4.1.2)}{=} \left|\frac{s^2((k-1) - (16k^3-4k))}{(k-1)^2(16k^3-4k)}\right| \cdot \left|\vartheta_1^{(2)} - \frac{sx}{(k-1)z}\right|^{-1} \cdot |z|^{-2}.
\end{aligned}$$

Budući da je $t^2 = (k+1)(16k^3-4k)+1 = (4k^2+2k-1)^2$, na isti način dobivamo

$$\left|\vartheta_2^{(1)} - \frac{ty}{(k+1)z}\right| = \left|\frac{t^2((k+1)-(16k^3-4k))}{(k+1)^2(16k^3-4k)}\right| \cdot \left|\vartheta_2^{(2)} - \frac{ty}{(k+1)z}\right|^{-1} \cdot |z|^{-2}.$$

Analogno kao prije je

$$\left|\vartheta_1^{(2)} - \frac{sx}{(k-1)z}\right| \geqslant \frac{1}{2}|\vartheta_1^{(1)} - \vartheta_1^{(2)}| = \left|\sqrt{1+\frac{1}{(k-1)(16k^3-4k)}}\right| = \left|\frac{4k^2-2k-1}{\sqrt{(k-1)(16k^3-4k)}}\right|,$$

$$\left|\vartheta_2^{(2)} - \frac{ty}{(k+1)z}\right| \geqslant \frac{1}{2}|\vartheta_2^{(1)} - \vartheta_2^{(2)}| = \left|\sqrt{1+\frac{1}{(k+1)(16k^3-4k)}}\right| = \left|\frac{4k^2+2k-1}{\sqrt{(k+1)(16k^3-4k)}}\right|.$$

Sada je

$$\begin{aligned}
&\left|\frac{s^2((k-1)-(16k^3-4k))}{(k-1)^2(16k^3-4k)}\right| \cdot \left|\vartheta_1^{(2)} - \frac{sx}{(k-1)z}\right|^{-1} \leqslant \\
&\quad \left|\frac{s^2((k-1)-(16k^3-4k))}{(k-1)^2(16k^3-4k)}\right| \cdot \left|\frac{4k^2-2k-1}{\sqrt{(k-1)(16k^3-4k)}}\right|^{-1} \\
&= \left|\frac{(4k^2-2k-1)^2(16k^3-5k+1)}{(k-1)^2(16k^3-4k)}\right| \cdot \left|\frac{\sqrt{(k-1)(16k^3-4k)}}{4k^2-2k-1}\right| \\
&= \left|\frac{(4k^2-2k-1)(16k^3-5k+1)}{(k-1)^2(16k^3-4k)}\right| \cdot |\sqrt{(k-1)(16k^3-4k)}| \\
&= \left|\frac{64k^5-32k^4-36k^3+14k^2+3k-1}{16k^5-32k^4+12k^3+8k^2-4k}\right| \cdot \sqrt{|k-1|\cdot|16k^3-4k|} \\
&\leqslant \frac{64|k|^5+32|k|^4+36|k|^3+14|k|^2+3|k|+1}{16|k|^5-32|k|^4-12|k|^3-8|k|^2-4|k|}\sqrt{16|k|^4+16|k|^3+4|k|^2+|k|} \\
&\leqslant \frac{64|k|^5+32|k|^4+36|k|^3+14|k|^2+3|k|+1}{16|k|^5-32|k|^4-12|k|^3-8|k|^2-4|k|} \cdot (4|k|^2+2|k|+1)
\end{aligned}$$

Zadnja upotrebljena nejednakost lako se dokaže kvadriranjem. Sad je dovoljno dokazati da je $(64|k|^5+32|k|^4+36|k|^3+14|k|^2+3|k|+1)(4|k|^2+2|k|+1) \leqslant 40|k|^2(16|k|^5-32|k|^4-12|k|^3-8|k|^2-4|k|)$, što je množenjem ekvivalentno s $384|k|^7-1536|k|^6-752|k|^5-480|k|^4-236|k|^3-24|k|^2-5|k|-1 \geqslant 0$. Za $|k| \geqslant 5$ je $384|k|^7 \geqslant 1920|k|^6$, pa je dovoljno dokazati da je $384|k|^6-752|k|^5-480|k|^4-236|k|^3-24|k|^2-5|k|-1 \geqslant 0$. Ponavljajući ovaj argument dobivamo dokaz željene nejednakosti. □

Pokažimo da je

$$2l = 2 \cdot \frac{27}{64}\frac{|T|}{|T|-M} < 1.$$

Ta nejednakost je ekvivalentna tvrdnji da je $27|T| < 32|T| - 32M$, tj.

$$32M < 5|T|. \tag{4.3.3}$$

Kako je M veći od brojeva $|k-1|$ i $|k+1|$, a oba ta broja su, prema nejednakosti trokuta, manja ili jednaka $|k|+1$, slijedi da je $M \leqslant |k|+1$. Stoga je dovoljno dokazati $32(|k|+1) < 5|16k^5 - 20k^3 + 4|$, što vrijedi za $|k| \geqslant 1.33$. Naime, desna strana je $5|16k^5-20k^3+4| \geqslant 80|k|^5-100|k|^3-20$, pa je dovoljno dokazati da je $80|k|^5-100|k|^3-20 > 32|k|+32$, odnosno $80|k|^5-100|k|^3-32|k|-52 > 0$. Ova tvrdnja očito vrijedi za dovoljno veliku apsolutnu vrijednost od k, a numerički je utvrđena najveća realna nultočka polinoma $80x^5 - 100x^3 - 32x - 52$.

Sada je $c = \dfrac{1}{4pP}, L = \dfrac{27(|T|-M)^2}{64|k^2-1|^2}, p = \sqrt{1 + \dfrac{5M}{2|T|-2M}}, P = 8(2|T|+3M)|k^2-1|^2$, $q = (k-1)(k+1)z$.

Ako krenemo primijeniti Jadrijević-Ziegler teorem, onda je

$$\lambda = 1 + \frac{\log 8 + \log(2|T|+3M) + 2\log|k^2-1|}{\log 27 + 2\log(|T|-M) - \log 64|k^2-1|^2},$$

i označimo

$$\mathrm{Max} = \max\left\{\left|\vartheta_1^{(1)} - \frac{s(k+1)x}{(k-1)(k+1)z}\right|, \left|\vartheta_2^{(1)} - \frac{t(k-1)y}{(k-1)(k+1)z}\right|\right\}.$$

Tada je

$$\mathrm{Max} > \frac{1}{4pP}|q|^{-\lambda} = \frac{\sqrt{2|T|-2M}}{32\sqrt{2|T|+3M}(2|T|+3M)|k^2-1|^2}|q|^{-\lambda}.$$

Budući da je $M < \frac{5}{32}|T|$, slijedi da je $2|T| - 2M > \frac{27}{16}|T|$, i analogno $2|T| + 3M < \frac{79}{32}|T| < \frac{5}{2}|T|$. Stoga je

$$\mathrm{Max} > \frac{\sqrt{\frac{27}{16}|T|}}{32\cdot\frac{5}{2}\sqrt{\frac{5}{2}}|T|^{\frac{3}{2}}|k^2-1|^2}|q|^{-\lambda} = \frac{3\sqrt{3}}{160\sqrt{10}}\frac{|T|^{-1}|q|^{-\lambda}}{|k^2-1|^2} = C|k^2-1|^{-\lambda-3}|16k^3-4k|^{-1}|z|^{-\lambda},$$

gdje je $C = \dfrac{3\sqrt{3}}{160\sqrt{10}}$. Sad slijedi da je $C|k^2-1|^{-\lambda-3}|16k^3-4k|^{-1}|z|^{-\lambda} < 40|k|^2|z|^{-2}$, tj.

$$|z|^{2-\lambda} < \frac{40}{C}|k|^2|k^2-1|^{\lambda+3}|16k^3-4k| = \frac{6400\sqrt{10}}{3\sqrt{3}}|k|^2|k^2-1|^{\lambda+3}|16k^3-4k|.$$

Iz ovakve nejednakosti može se dobiti ograda na veličinu rješenja $|z|$ kad je $\lambda < 2$, jer je tad lijeva strana pozitivna potencija od $|z|$. Postupak dobivanja donje ograde za $|x|$ lako se modificira da bi se dobila donja ograda za $|z|$. Štoviše, nije teško vidjeti da je $|z| \geqslant |x|$, tako da bi se zapravo mogla upotrijebiti ista donja granica. Kako je ta donja

ograda eksponencijalna u $|k|$, da je $\lambda < 2$, dobili bismo polinomijalnu gornju ogradu za $|z|$ i suprotstavljanjem ove dvije ograde, dobili bismo gornju granicu na $|k|$. Međutim, ovdje je u pravilu $\lambda > 2$. Naime, ta tvrdnja je ekvivalentna s $P > L$, odnosno

$$\begin{aligned} 8(2|T| + 3M)|k^2-1|^2 &> \frac{27(|T|-M)^2}{64|k^2-1|^2} \\ \Longleftrightarrow 512(2|(k^2-1)(16k^3-4k)| + 3M)|k^2-1|^4 &> 27(|(k^2-1)(16k^3-4k)| - M)^2, \end{aligned}$$

a kako je $M = \max\{|k-1|, |k+1|\}$, tj. linearno u k, sad već vidimo da je stupanj lijeve strane u k veći nego u desnoj ($13 > 10$). Preciznije, prema nejednakosti trokuta je lijeva strana $512(2|(k^2-1)(16k^3-4k)|+3M)|k^2-1|^4 \geqslant 512(32|k|^5-40|k|^3-11|k|-3)(|k|^2-1)^4$, a desna $27(|(k^2-1)(16k^3-4k)|-M)^2 < 27(16|k|^5+20|k|^3+4|k|)^2$, pa je dovoljno dokazati da je

$$\begin{aligned} 16384|k|^{13} - 86016|k|^{11} - 6912|k|^{10} + 174592|k|^9 - 18816|k|^8 - 165888|k|^7 - 8112|k|^6 + \\ + 64512|k|^5 - 13536|k|^4 + 2048|k|^3 + 5712|k|^2 - 5632|k| - 1536 > 0, \end{aligned}$$

što vrijedi za $|k| \geqslant 1.82$ (očito vrijedi za dovoljno velike $|k|$, a numerički je utvrđena najveća nultočka polinoma s lijeve strane u k i iznosi približno 1.81696).

4.4 Zaključak

Kako god pokušali primijeniti Jadrijević-Ziegler teorem, ne uspijevamo dobiti koristan rezultat. Razlog tome treba tražiti u konkretnom obliku početne Diofantove trojke. Iako je $c = 16k^3 - 4k$ po apsolutnoj vrijednosti veće od a i b, pokazuje se da udaljenost između njih nije dovoljno velika. U idućem poglavlju pokazat ćemo kako iskoristiti ovaj teorem za dobivanje uniformne granice na veličinu Diofantove m-torke u Gaussovim cijelim brojevima. Uz pretpostavku da je $|c| > |b|^{15}$, ovaj teorem pokazat će se izrazito korisnim. U ovom konkretnom slučaju nije bio dovoljan, upravo zato što ne vrijedi takva nejednakost između članova početne trojke.

Vratit ćemo se ovoj familiji na kraju idućeg poglavlja, gdje ćemo primijeniti drukčiju metodu i dobiti parcijalno rješenje problema proširenja.

Napomenimo još da je ovaj problem u cijelim brojevima u [9] riješen koristeći linearne forme u logaritmima, kojima ćemo se baviti na kraju idućeg poglavlja. Sličan problem u cijelim brojevima, proširenje $D(4)$-trojke $\{k'-2, k'+2, 4(k')^3-4k'\}$, proučavan je u [7]. Primijetimo da se za paran $k' = 2k$, dijeljenjem s 2, iz te familije dobiva upravo familija $D(1)$-trojki koju smo ovdje proučavali. U [7], problem je riješen sličnom metodom koju smo pokušali primijeniti ovdje. Tamo je dokazano poboljšanje analognog teorema u cijelim brojevima, ali za specifičnu situaciju (gdje su brojnici pod korijenom u θ_i jednaki točno $k-2$ i $k+2$, a nazivnik je djeljiv s k^2-4).

Poglavlje 5

Diofantove m-torke u Gaussovim cijelim brojevima

Diofant je promatrao ove skupove u racionalnim brojevima i tu su pitanja još uvijek širom otvorena. Tek nedavno u [16] pronađena je beskonačna familija Diofantovih šestorki racionalnih brojeva. Jasno je da prijelaz s problema u cijelim brojevima na analogne probleme u racionalnim brojevima može biti vrlo težak. S druge strane, razumno je pretpostaviti da će prijelaz na analogne probleme u drugim prstenovima cijelih brojeva biti lakši. Ipak, ni u takvom okruženju nema mnogo rezultata. Npr. u području analognih problema u prstenu Gaussovih cijelih brojeva pronalazimo manje od 10 radova, od kojih možemo istaknuti već spomenute radove [5] i [21], koji se bave proširenjem jednoparametarskih familija Diofantovih trojki. No, zbog sličnosti ovog prstena s uobičajenim prstenom cijelih brojeva, možemo očekivati da će vrijediti slični rezultati i da će se moći dokazati sličnim tehnikama kao u racionalnim cijelim brojevima.

Cilj ovog poglavlja jest odgovoriti na pitanje koliko najviše elemenata ima Diofantova m-torka Gaussovih cijelih brojeva, odnosno dati gornju granicu na m. U ovom općenitijem problemu, glavni rezultat na koji ćemo se osloniti ponovo je Jadrijević–Ziegler teorem (varijanta Bennettovog teorema). Kako nam ovdje nije cilj opisati kako izgledaju moguća proširenja, nego samo dati gornju granicu na broj mogućih proširenja, ne treba čuditi što će ta metoda biti djelotvorna u ovoj općenitijoj situaciji, iako nije pomogla u konkretnoj situaciji u prošlom poglavlju.

Rezultati prikazani ovdje nastali su prateći dokaz prve gornje granice na veličinu Diofantove m-torke u cijelim brojevima (Dujella, [13]), gdje je dobiveno da je $m \leqslant 8$. Tako smo dobili i neke rezultate koje (zasad) nismo iskoristili. Ovdje dobivena granica je slabija ($m \leqslant 42$), a dokaz je jednostavniji. Nakon toga ćemo dokazati i neke rezultate koji bi se mogli iskoristiti za poboljšanje ove granice.

5.1 Pellovski sustav

Neka su a, b i c Gaussovi cijeli brojevi koji čine Diofantovu trojku. Bez smanjenja općenitosti, pretpostavimo da je $0 < |a| \leqslant |b| \leqslant |c|$. Tada postoje Gaussovi cijeli brojevi r, s i t takvi da je

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

Budući da jednadžba $X^2 - Y^2 = 1$ u Gaussovim cijelim brojevima ima samo trivijalna rješenja ($XY = 0$), brojevi ac i bc nisu kvadrati. Vrijedi $ac \neq i^2 = -1$ jer ne postoje tri broja $\{a, b, c\}$ modula 1 koji čine Diofantovu trojku. Slično, vrijedi i $|s| \neq 1$ jer ne postoje tri broja $\{a, b, c\}$ modula 2 ili manjeg koji čine Diofantovu trojku. Broj ab također nije kvadrat: ako pretpostavimo suprotno, onda je $r = 0$ te je $a = -1, b = 1$ (ili obratno), pa ne postoji $c \neq 0$ koji bi s njima činio Diofantovu trojku. Naime, iz $-c+1 = s^2$ i $c+1 = t^2$ množenjem slijedi $1 - c^2 = s^2t^2$. Iz toga je $c = 0$ ili $st = 0$, iz čega slijedi $c = \pm 1 \in \{a, b\}$.

Napomenimo da su rješenja ove jednadžbe u prstenu cijelih brojeva imaginarnog kvadratnog polja opisana u [19]. Brojevi ac i bc nisu kvadrati ni u $\mathbb{Q}[i]$, jer je $\mathbb{Z}[i]$ integralno zatvoren u $\mathbb{Q}[i]$. Dokazali smo sljedeću lemu.

Lema 5.1.1. *Ako je $\{a, b, c\}$ Diofantova trojka u Gaussovim cijelim brojevima i $0 < |a| \leqslant |b| \leqslant |c|$, onda brojevi ab, ac i bc nisu kvadrati u $\mathbb{Q}[i]$.*

Ako postoji $d \in \mathbb{Z}[i]$ takav da je $\{a, b, c, d\}$ Diofantova četvorka, onda postoje $x, y, z \in \mathbb{Z}[i]$ takvi da je $ad + 1 = x^2, bd + 1 = y^2, cd + 1 = z^2$. Eliminirajmo d iz prve i treće dobivene jednadžbe, $a(cd + 1) - c(ad + 1) = az^2 - cx^2$. Slijedi da je $az^2 - cx^2 = a - c$. Analogno, eliminacijom d iz druge i treće jednadžbe je $bz^2 - cy^2 = b - c$. Dobivamo sustav jednadžbi

$$az^2 - cx^2 = a - c \tag{5.1.1}$$

$$bz^2 - cy^2 = b - c. \tag{5.1.2}$$

Dobivene jednadžbe sliče pellovskim jednadžbama i njihova rješenja imaju vrlo sličnu strukturu, koju opisujemo u sljedećoj lemi.

Lema 5.1.2. *Postoje prirodni brojevi i_0, j_0, Gaussovi cijeli brojevi $z_0^{(i)}, x_0^{(i)}, z_1^{(j)}, x_1^{(j)}$ za $i = 1, \ldots, i_0$ i $j = 1, \ldots, j_0$, takvi da vrijedi:*

a) $(z_0^{(i)}, x_0^{(i)})$ su rješenja (5.1.1), a $(z_1^{(j)}, y_1^{(j)})$ su rješenja (5.1.2). Ovdje označena rješenja nazivat ćemo fundamentalnima.

b) Za fundamentalna rješenja vrijede nejednakosti

$$1 \leqslant |x_0^{(i)}| \leqslant \sqrt{\frac{|a||c-a|}{|s|-1}},$$
$$1 \leqslant |z_0^{(i)}| \leqslant \sqrt{\frac{|c-a|}{|a|} + \frac{|c||c-a|}{|s|-1}},$$
$$1 \leqslant |y_1^{(j)}| \leqslant \sqrt{\frac{|b||c-b|}{|t|-1}},$$
$$1 \leqslant |z_1^{(j)}| \leqslant \sqrt{\frac{|c-b|}{|b|} + \frac{|c||c-b|}{|t|-1}}.$$

c) Ako je (z, x) rješenje jednadžbe (5.1.1), onda postoje $i \in \{1, \ldots, i_0\}$ i cijeli broj m takvi da je

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

Ako je (z, y) rješenje jednadžbe (5.1.2), onda postoje $j \in \{1, \ldots, j_0\}$ i cijeli broj n takvi da je

$$z\sqrt{b} + y\sqrt{c} = (z_1^{(j)}\sqrt{a} + y_1^{(j)}\sqrt{c})(t + \sqrt{bc})^n.$$

Dokaz. Ako je (x, z) rješenje (5.1.1), tada je par $(x_m, y_m) \in \mathbb{Z}[i]^2$, definiran preko

$$x_m\sqrt{c} + z_m\sqrt{a} = (x\sqrt{c} + z\sqrt{a})(s + \sqrt{ac})^m \tag{5.1.3}$$

također rješenje jednadžbe (5.1.1) za svaki $m \in \mathbb{Z}$. Ova tvrdnja dokazuje se indukcijom: za $m = 1$ je $x_1\sqrt{c} + z_1\sqrt{a} = (x\sqrt{c} + z\sqrt{a})(s + \sqrt{ac}) = (sx + az)\sqrt{c} + (sz + cx)\sqrt{a}$, odnosno $x_1 = sx + az, z_1 = sz + cx$. Tada je

$$\begin{aligned} az_1^2 - cx_1^2 &= a(sz + cx)^2 - c(sx + az)^2 \\ &= as^2z^2 + ac^2x^2 - cs^2x^2 - ca^2z^2 \\ &= s^2(az^2 - cx^2) + ac(cx^2 - az^2) \\ &= s^2(a - c) + ac(c - a) \\ &= (s^2 - ac)(a - c) = a - c \end{aligned}$$

Induktivno slijedi da je (x_m, z_m) rješenje (5.1.1) za svaki $m \in \mathbb{N}_0$. Analogno se pokazuje za $m = -1$ i slijedi da je (x_m, z_m) rješenje (5.1.1) za svaki $m \in \mathbb{Z}$.

Neka je (x^*, z^*) rješenje iz niza $(x_m, z_m)_{m\in\mathbb{Z}}$, definiranog u (5.1.3), takvo da je apsolutna vrijednost $|x^*|$ minimalna. Označimo s (x', z') i (x'', z'') iduće i prethodno rješenje u nizu. Preciznije, neka je $x' = sx^* + az^*, z' = sz^* + cx^*$, a $x'' = sx^* - az^*, z'' = sz^* - cx^*$. Tada je $|x'| \geqslant |x^*|$ i $|x''| \geqslant |x^*|$. S druge strane, kako je $|x'| + |x''| \geqslant |x' + x''| = 2|s||x^*|$, slijedi da

je $|x'| \geqslant |sx^*|$ ili $|x''| \geqslant |sx^*|$. U svakom slučaju, vrijedi da je produkt $|x'x''| \geqslant |sx^*| \cdot |x^*|$. Dobivamo niz ekvivalentnih nejednakosti

$$\begin{aligned}
&|x'x''| \geqslant |s| \cdot |x^*|^2 \\
\iff &|(sx^* + az^*)(sx^* - az^*)| \geqslant |s| \cdot |x^*|^2 \\
\iff &|s^2(x^*)^2 - a^2(z^*)^2| \geqslant |s| \cdot |x^*|^2 \\
\iff &|(ac+1)(x^*)^2 - a^2(z^*)^2| \geqslant |s| \cdot |x^*|^2 \\
\iff &|a(c(x^*)^2 - a(z^*)^2) + (x^*)^2| \geqslant |s| \cdot |x^*|^2, \\
\iff &|a(c-a) + (x^*)^2| \geqslant |s| \cdot |x^*|^2,
\end{aligned}$$

jer je (z^*, x^*) rješenje (5.1.1).

Iz posljednje dobivene nejednakosti izvodimo gornju granicu za $|x^*|$, $|a| \cdot |c-a| + |x^*|^2 \geqslant |a(c-a) + (x^*)^2| \geqslant |s| \cdot |x^*|^2$, pa je $|a| \cdot |c-a| \geqslant (|s|-1)|x^*|^2$ i konačno $|x^*|^2 \leqslant \dfrac{|a| \cdot |c-a|}{|s|-1}$.

Iz gornje granice na $|x^*|$ slijedi i gornja granica za $|z^*|$ preko sljedeće nejednakosti trokuta:

$$|z^*| = \frac{|c(x^*)^2 - c + a|}{|a|} \leqslant \frac{|c||x^*|^2}{|a|} + \frac{|c-a|}{|a|}.$$

Bez smanjenja općenitosti možemo pretpostaviti da je $x_0 = x^*, z_0 = z^*$.

Analogno se dobivaju gornje granice za fundamentalna rješenja jednadžbe (5.1.2). □

Napomena. Pod korijenom se ovdje uvijek misli na glavnu granu funkcije (dakle, vrijednost realnog dijela korijena je veća ili jednaka 0). Ali isto, do na predznake, dobiva se i za drugu vrijednost – npr. dobivaju se rješenja $(-z, x)$ jednadžbe (5.1.1) i druge kombinacije predznaka.

Rješenja pellovskih jednadžbi u Gaussovim cijelim brojevima opisana su u [19], gdje su za fundamentalna rješenja uzimane dodatne pretpostavke da su argumenti takvog rješenja u intervalu $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right\rangle$. Uz ovakve pretpostavke, tvrdnja Leme 5.1.2 c) može se pojačati jer tada postoje jedinstveni indeksi $i \in \{1, \ldots, i_0\}$ te $j \in \{1, \ldots, j_0\}$.

Korolar 5.1.3. *Za ova fundamentalna rješenja vrijedi* i $|z_0| < |c|$ *te* $|x_0| \leqslant \frac{3}{2}\sqrt{|c|}$, *pod uvjetom da je* $|a| \geqslant 4$ i $|c| \geqslant 5$. *Također je* $|x_0| < \sqrt{55/32}\sqrt[4]{|ac|}$ i $|z_0| < \sqrt{61/32}|c|^{3/4}|a|^{-1/4}$, *ako je* $|c| \geqslant 4|a|$.

Dokaz. Iz $|s|^2 = |ac+1| \geqslant |a|^2 - 1$ je $2|s| \geqslant 2\sqrt{|a|^2-1} \geqslant |a| + 2$, jer je to ekvivalentno s $3|a|^2 - 4|a| - 8 \geqslant 0$, što vrijedi za $|a| \geqslant 4$. Stoga je $\dfrac{|c-a|}{|s|-1} \leqslant \dfrac{2|c-a|}{|a|}$ i slijedi da je

$$\begin{aligned}|z_0|^2 &\leqslant \frac{|c-a|}{|a|} + \frac{|c||c-a|}{|s|-1} \leqslant \frac{|c-a|}{|a|} + \frac{2|c|\cdot|c-a|}{|a|} \\ &= \frac{|c-a|}{|a|}(2|c|+1) \leqslant \left(\left|\frac{c}{a}\right|+1\right)(2|c|+1) \\ &\leqslant \left(\frac{|c|}{4}+1\right)(2|c|+1) = \frac{|c|^2}{2} + \frac{9}{4}|c| + 1 < |c|^2\end{aligned}$$

ako je $|c| \geqslant 5$. Dakle, $|z_0| < |c|$.

Kako je $s^2 = ac+1$, slijedi da je $|s| \geqslant \sqrt{|ac|} - 1$, jer je ekvivalentno tvrdnji $|s^2| \geqslant |ac| - 2\sqrt{|ac|} + 1$, što vrijedi jer je $|s^2| = |ac+1| \geqslant |ac| - 1$, prema nejednakosti trokuta, a $|ac| \geqslant 1$. Slijedi da je $|s| - 1 \geqslant \sqrt{|ac|} - 2$.

Za $|x_0| \leqslant \frac{3}{2}\sqrt{|c|}$ dovoljno je dokazati $\dfrac{|a||c-a|}{|s|-1} \leqslant \dfrac{9}{4}|c|$, odnosno $|a||c-a| \leqslant \frac{9}{4}|c|(|s|-1)$. Budući da je $|s|-1 \geqslant \sqrt{|ac|}-2$ i $|c-a| \leqslant |c|+|a| \leqslant \dfrac{5}{4}|c|$, slijedi da je

$$\begin{aligned}\frac{9}{4}|c|(|s|-1) &\geqslant \frac{9}{4}|c|(\sqrt{|ac|}-2) \\ &\geqslant \frac{9}{5}|c-a|(\sqrt{|ac|}-2) \\ &\geqslant |a||c-a|,\end{aligned}$$

što je i trebalo dokazati.

Dokažimo i jaču tvrdnju. Kako je $|x_0|^2 \leqslant \dfrac{|a||c-a|}{|s|-1}$, dovoljno je dokazati da je

$$\frac{|a||c-a|}{|s|-1} < \frac{55}{32}\sqrt{|ac|}.$$

Ova tvrdnja ekvivalentna je s

$$32|ac-a^2| < 55(|s|-1)\sqrt{|ac|}. \tag{5.1.4}$$

Za desnu stranu (5.1.4) vrijedi sljedeće:

$$\begin{aligned}55(|s|-1)\sqrt{|ac|} &\geqslant 55(\sqrt{|ac|}-2)\sqrt{|ac|} \\ &= 55|ac| - 110\sqrt{|ac|} \\ &= 40|ac| + 15|ac| - 110\sqrt{|ac|},\end{aligned}$$

a kako je, s druge strane,

$$32|ac-a^2| \leqslant 32|ac| + 32|a|^2$$

$$\begin{aligned}&\leqslant 32|ac| + 32|a| \cdot \frac{|c|}{4}\\ &= 40|ac|,\end{aligned}$$

dovoljno je dokazati da je $15|ac| - 110\sqrt{|ac|} \geqslant 0$, odnosno $\sqrt{|ac|} \geqslant 7\frac{1}{3}$. Kako je $|c| \geqslant 4|a|$, slijedi da je $|ac| \geqslant 4|a|^2 \geqslant 64$, jer smo pretpostavili $|a| \geqslant 4$. Dakle, $\sqrt{|ac|} \geqslant 8 > 7\frac{1}{3}$, što je i trebalo dokazati. □

5.2 Primjena diofantskih aproksimacija

Lema 5.2.1. *Neka su x, y, z rješenja sustava jednadžbi (5.1.1) i (5.1.2), pri čemu je $|c| > 4|b|$ i $|a| \geqslant 2$. Ako je $\theta_1^{(1)} = \pm\frac{s}{a}\sqrt{\frac{a}{c}}, \theta_1^{(2)} = -\theta_1^{(1)}$ i $\theta_2^{(1)} = \pm\frac{t}{b}\sqrt{\frac{b}{c}}, \theta_2^{(2)} = -\theta_2^{(1)}$, te su predznaci odabrani tako da je*

$$\left|\theta_1^{(1)} - \frac{sx}{az}\right| \leqslant \left|\theta_1^{(2)} - \frac{sx}{az}\right| \quad i \quad \left|\theta_2^{(1)} - \frac{ty}{bz}\right| \leqslant \left|\theta_1^{(2)} - \frac{ty}{bz}\right|,$$

onda je

$$\begin{aligned}\left|\theta_1^{(1)} - \frac{sbx}{abz}\right| &\leqslant \frac{|s| \cdot |c-a|}{|a|\sqrt{|ac|}} \cdot \frac{1}{|z|^2} < \frac{21}{16}\frac{|c|}{|a|} \cdot \frac{1}{|z|^2} \quad i\\ \left|\theta_2^{(1)} - \frac{tay}{abz}\right| &\leqslant \frac{|s| \cdot |c-b|}{|b|\sqrt{|bc|}} \cdot \frac{1}{|z|^2} < \frac{21}{16}\frac{|c|}{|a|} \cdot \frac{1}{|z|^2}.\end{aligned}$$

Dokaz. Vrijedi

$$\begin{aligned}\left|\theta_1^{(1)} - \frac{sx}{az}\right| &= \left|(\theta_1^{(1)})^2 - \frac{s^2x^2}{a^2z^2}\right| \cdot \left|\theta_1^{(1)} + \frac{sx}{az}\right|^{-1}\\ &= \left|\frac{s^2}{a^2}\right| \cdot \frac{|az^2 - cx^2|}{|c||z|^2} \cdot \left|\theta_1^{(2)} - \frac{sx}{az}\right|^{-1}\\ &= \frac{|s|^2|c-a|}{|a|^2|c|}\left|\theta_1^{(2)} - \frac{sx}{az}\right|^{-1} \cdot \frac{1}{|z|^2}\end{aligned}$$

Također je $\left|\theta_1^{(2)} - \frac{sx}{az}\right| \geqslant \left|\frac{s}{a}\sqrt{\frac{a}{c}}\right|$, jer je

$$\begin{aligned}2\left|\theta_1^{(2)} - \frac{sx}{az}\right| &\geqslant \left|\theta_1^{(2)} - \frac{sx}{az}\right| + \left|\theta_1^{(1)} - \frac{sx}{az}\right| \geqslant \left|\theta_1^{(2)} - \frac{sx}{az} - \left(\theta_1^{(1)} - \frac{sx}{az}\right)\right|\\ &= |\theta_1^{(2)} - \theta_1^{(1)}| = 2\left|\frac{s}{a}\sqrt{\frac{a}{c}}\right|.\end{aligned}$$

Stoga je $\left|\theta_1^{(1)} - \frac{sbx}{abz}\right| \leqslant \frac{|s|^2|c-a|}{|a|^2|c|}\left|\frac{a}{s}\sqrt{\frac{c}{a}}\right| \cdot \frac{1}{|z|^2}$, tj. $\left|\theta_1^{(1)} - \frac{sbx}{abz}\right| \leqslant \frac{|s| \cdot |c-a|}{|a|\sqrt{|ac|}} \cdot \frac{1}{|z|^2}$, što je prva nejednakost u iskazu ove leme.

Još treba dokazati $\frac{|s|\cdot|c-a|}{|a|\sqrt{|ac|}}\cdot\frac{1}{|z|^2} < \frac{21}{16}\frac{|c|}{|a|}\cdot\frac{1}{|z|^2}$, tj. $|\sqrt{ac+1}|\cdot|c-a| < \frac{21}{16}|c|\sqrt{|ac|}$, što je ekvivalentno s $\left|\sqrt{1+\frac{1}{ac}}\right| < \frac{21}{16}\frac{|c|}{|c-a|}$. Iz $|c|>4|a|$ slijedi da je $\frac{21}{16}\frac{|c|}{|c-a|} \geqslant \frac{21}{16}\cdot\frac{4}{5} = \frac{21}{20}$. Lijeva strana je $\left|\sqrt{1+\frac{1}{ac}}\right| \leqslant \sqrt{\left|1+\frac{1}{|ac|}\right|} \leqslant \sqrt{1+\frac{1}{16}} = \frac{\sqrt{17}}{4}$, pa slijedi drugi dio željene nejednakosti.

Analogno se dokazuje drugi par nejednakosti (koristili smo samo $|c|>4|a|$ i $a \geqslant 2$). □

Sad ćemo primijeniti Jadrijević–Ziegler teorem iz [31]. Ponovimo iskaz radi lakšeg praćenja sljedećeg dokaza.

Teorem 5.2.2 ([31, Theorem 7.1])**.** *Neka je $\theta_i = \sqrt{1+\frac{a_i}{T}}, i=1,2$ s $a_1 \neq a_2$ i T u prstenu cijelih brojeva imaginarnog kvadratnog polja K. Neka je $|T| > M = \max\{|a_1|,|a_2|\}$,*

$$L = \frac{27}{16|a_1|^2|a_2|^2|a_1-a_2|^2}(|T|-M)^2 > 1.$$

Tada je

$$\max\left\{\left|\theta_1-\frac{p_1}{q}\right|,\left|\theta_2-\frac{p_2}{q}\right|\right\} > c|q|^{-\lambda},$$

za sve algebarske cijele $p_1,p_2,q\in K$, gdje je $\lambda = 1+\frac{\log P}{\log L}$, $c^{-1} = 4pP(\max\{1,2l\})^{\lambda-1}$,

$$l = \frac{27}{64}\frac{|T|}{|T|-M}, p = \sqrt{\frac{2|T|+3M}{2|T|-2M}}, P = 16\frac{|a_1|^2|a_2|^2|a_1-a_2|^2}{\min\{|a_1|,|a_2|,|a_1-a_2|\}^3}(2|T|+3M).$$

Pomoću tog teorema dokazat ćemo da, ako su drugi i treći element Diofantove m-torke dovoljno udaljeni, onda je udaljenost između trećeg i četvrtog elementa ograničena. Preciznije, dokazujemo sljedeću propoziciju.

Propozicija 5.2.3. *Ako je $\{a,b,c,d\}\subseteq\mathbb{Z}[i]$ Diofantova četvorka takva da je $|ac| \geqslant 9$, $|b| \geqslant \frac{3}{2}|a|$, $|b|>5$ i $|c|>|b|^{15}$, onda je $|d| < 4278^{20}|c|^{50}$.*

Dokaz. Ovdje se simultano aproksimiraju

$$\theta_1 = \pm\frac{s}{a}\sqrt{\frac{a}{c}} = \pm\sqrt{\frac{s^2a}{a^2c}} = \pm\sqrt{\frac{ac+1}{ac}} = \pm\sqrt{1+\frac{b}{abc}} \quad \text{i} \quad \theta_2 = \pm\sqrt{1+\frac{a}{abc}}.$$

Sad je $a_0=0, a_1=b, a_2=a, T=abc, M=|b|$, te je

$$l = \frac{27|abc|}{64(|abc|-|b|)} = \frac{27|ac|}{64(|ac|-1)} < \frac{1}{2},$$

jer je to ekvivalentno tvrdnji $27|ac| < 32(|ac|-1)$, što vrijedi za $|ac| \geqslant 9 > \frac{32}{5}$. Slično, vrijedi da je

$$p = \sqrt{\frac{2|abc|+3|b|}{2|abc|-2|b|}} = \sqrt{1+\frac{5}{2(|ac|-1)}} \leqslant \sqrt{1+\frac{5}{2(9-1)}} = \sqrt{\frac{21}{16}}. \tag{5.2.1}$$

Također je $\min\{|a|,|b|,|b-a|\} \geqslant \frac{|a|}{2}$ jer je $|b-a| \geqslant |b|-|a| \geqslant \frac{3}{2}|a|-|a| = \frac{|a|}{2}$ zbog pretpostavke $|b| \geqslant \frac{3}{2}|a|$. Stoga je

$$P = 16\frac{|a|^2|b|^2|b-a|^2}{\min\{|a|,|b|,|b-a|\}^3}(2|abc|+3|b|) \leqslant 128\frac{|b|^3|b-a|^2}{|a|}(2|ac|+3) \text{ i}$$
$$L = \frac{27}{16|a|^2|b|^2|b-a|^2}(|abc|-|b|)^2 = \frac{27(|ac|-1)^2}{16|a|^2|b-a|^2}.$$

Dakle, uvjet teorema $L > 1$ ovdje je ekvivalentan tvrdnji $27(|ac|-1)^2 > 16|a|^2|b-a|^2$. Korjenovanjem dobivamo jednostavniju tvrdnju $3\sqrt{3}(|ac|-1) > 4|a||b-a|$. Budući da je $|c| > |b|^3$ (i $|b| \geqslant \frac{3}{2}|a|$), vrijedi i jača tvrdnja $|ac|-1 > |a||b-a|$. Naime, vrijedi da je

$$\begin{aligned}
|ac|-1 &> |a|\cdot|b|^3 - 1 \\
&> 2|a|^2|b|-1 \quad (\text{jer je } |b| \geqslant \frac{3}{2}|a|) \\
&> |a|\cdot|b| + |a^2| \quad (\text{zbog } |b| \geqslant 2 \text{ i } |a| \geqslant 1) \\
&\geqslant |ab-a^2| = |a||b-a| \quad (\text{po nejednakosti trokuta}).
\end{aligned}$$

Time su uvjeti teorema zadovoljeni.

Budući da je $l < \frac{1}{2}$, slijedi da je $c = \frac{1}{4pP}$. Stoga je, prema (5.2.1), $c \geqslant \frac{1}{\sqrt{21}P}$.

Također, $\lambda > 1$ jer su i P i L veći od 1. Za L smo to već dokazali, a za $P > 1$ dovoljno je $|b| > |a|$.

Budući da je $|c| > |b|^{15}$, slijedi da je $\lambda < 1.9$. Kako je $\lambda = 1 + \frac{\log P}{\log L}$, vrijede sljedeće ekvivalencije $\lambda < 1.9 \iff \frac{\log P}{\log L} < 0.9 \iff P < L^{0.9}$. Stoga je dovoljno dokazati

$$\begin{aligned}
&128\frac{|b|^3|b-a|^2}{|a|}(2|ac|+3) < \left(\frac{27}{16}\right)^{0.9}\frac{(|ac|-1)^{1.8}}{|a|^{1.8}|b-a|^{1.8}} \\
\iff &128|b|^3|b-a|^{3.8}|a|^{0.8}(2|ac|+3) < \left(\frac{27}{16}\right)^{0.9}(|ac|-1)^{1.8}.
\end{aligned}$$

Budući da je $|ac|-1 > \frac{2|ac|+3}{3}$ (ekvivalentno je s $|ac| > 6$, što vrijedi jer smo pretpostavili

da je $|ac|$ barem 9), dovoljno je dokazati

$$384|b|^3|b-a|^{3.8}|a|^{0.8} < \left(\frac{27}{16}\right)^{0.9}(|ac|-1)^{0.8},$$

za što je dovoljno

$$240|b|^3|b-a|^{3.8}|a|^{0.8} < (|ac|-1)^{0.8}. \tag{5.2.2}$$

Za desnu stranu od (5.2.2) vrijedi $(|ac|-1)^{0.8} > (|ac|)^{0.8} - 1$, jer je funkcija $f(t) = (t-1)^{0.8} - t^{0.8} + 1$ u $t = 1$ jednaka 0 i raste. Stoga, ako je $|c| > |b|^{15}$, onda je $(|ac|-1)^{0.8} > |a|^{0.8}|b|^{12} - 1$, što je veće od lijeve strane od (5.2.2), $240|b|^3|b-a|^{3.8}|a|^{0.8}$, jer je veći stupanj od $|b|$. Konkretnije, jer je $|b| \geqslant \frac{3}{2}|a|$, odnosno $|a| \leqslant \frac{2}{3}|b|$, slijedi da je

$$\begin{aligned} 240|b|^3|b-a|^{3.8}|a|^{0.8} &\leqslant 240|b|^3\left(\frac{5}{3}|b|\right)^{3.8}\left|\frac{2b}{3}\right|^{0.8} \\ &< 1209|b|^{7.6} \\ &< |b|^{12} - 1. \end{aligned}$$

Zadnja nejednakost dobiva se ponovo jednostavnom analizom pomoćne funkcije $f(t) = t^{12} - 1209t^{7.6} - 1$, koja je očito veća od 0 za dovoljno velik t, a numerički je utvrđena najveća nultočka 5.01824. Ako je $|b| > 5$ kao što smo pretpostavili, onda je $|b| \geqslant \sqrt{26} > 5.02$, što znači da gornja nejednakost zbilja vrijedi. Time smo dokazali da je $\lambda < 1.9$.

Teorem Jadrijević-Ziegler nam onda, skupa s Lemom 5.2.1, daje

$$\begin{aligned} \frac{21}{16}\frac{|c|}{|a|}\cdot\frac{1}{|z|^2} &> \frac{1}{\sqrt{21}P}|abz|^{-\lambda} \\ &\geqslant \frac{|a|}{\sqrt{21}\cdot 128|b|^3|b-a|^2(2|ac|+3)}|abz|^{-\lambda}, \end{aligned}$$

odnosno

$$168\sqrt{21}\frac{|c|}{|a|^2}|b|^3|b-a|^2(2|ac|+3)\cdot|ab|^{\lambda} > |z|^{2-\lambda} > |z|^{0.1},$$

pa je

$$\begin{aligned} |z|^{0.1} &< 168\sqrt{21}|c|\cdot 3|ac|\cdot|b-a|^2|b|^{3+\lambda}|a|^{\lambda-2} \\ &< 504\sqrt{21}|c|^2\cdot\frac{2}{3}|b|\cdot\left(\frac{5}{3}|b|\right)^2|b|^{4.9} \quad \text{(jer je } |b| \geqslant 2|a| \text{ i } \lambda < 1.9) \\ &< 4728|c|^2|b|^{7.9} \\ &< 4728|c|^{\frac{30+7.9}{15}} \quad \text{(jer je } |c| > |b|^{15}) \\ &< 4728|c|^{2.53} \end{aligned}$$

te je, konačno, $|z| < 4728^{10}|c|^{2.53\cdot 10} = 4728^{10}|c|^{25.3}$.

Budući da je $d = \dfrac{z^2-1}{c}$, slijedi da je

$$\begin{aligned} |d| &\leqslant \frac{|z^2-1|}{|c|} \leqslant \frac{|z|^2+1}{|c|} \\ &\leqslant \frac{4728^{20}|c|^{50.6}+1}{|c|} < 4728^{20}|c|^{50} \end{aligned}$$

i time smo dokazali propoziciju. □

5.3 Donja granica na veličinu elementa koji proširuje Diofantovu trojku

U prethodnom potpoglavlju dokazali smo gornju ogradu na četvrti element Diofantove m-torke (uz neke uvjete). Sada ćemo naći donju ogradu kako bismo ih mogli suprotstaviti.

Definicija 5.3.1. Za Diofantovu trojku $\{a, b, c\}$ kažemo da je *regularna* ako je $c = a + b \pm 2r$, gdje je $r^2 = ab + 1$.

Lema 5.3.2. *Ako je $\{a, b, c, d\}$ Diofantova četvorka takva da je $2 \leqslant |a| \leqslant |b| \leqslant |c| \leqslant |d|$, onda nije moguće da su obje trojke $\{a, b, c\}$ i $\{a, b, d\}$ regularne, tj. nije moguće da je $c = a + b - 2r$ i $d = a + b + 2r$ (ni obratno), gdje je $ab + 1 = r^2$.*

Dokaz. Pretpostavimo suprotno. Kada bi to vrijedilo, onda bi bilo $cd = (a+b)^2 - 4r^2 = a^2 + 2ab + b^2 - 4(ab+1) = a^2 - 2ab + b^2 - 4$, pa je $cd + 1 = (a-b)^2 - 3$. Budući da je $\{c, d\}$ Diofantov par, postoji Gaussov cijeli z takav da je $cd + 1 = z^2$. Dakle, $(a-b)^2 - 3 = z^2$, odnosno $(a - b - z)(a - b + z) = 3$. Kako je 3 prost u $\mathbb{Z}[i]$, na produkt dva faktora u $\mathbb{Z}[i]$ može se rastaviti samo na sljedeće načine: $3 = 1 \cdot 3, 3 = -1 \cdot (-3), 3 = i \cdot (-3i), 3 = -i \cdot 3i$, do na poredak faktora. U prva dva slučaja, oduzimanjem faktora $a - b + z$ i $a - b - z$ je $2z = \pm 2$, odnosno $z = \pm 1$, što nije moguće jer bi tada bilo $cd = 0$. U druga dva slučaja, na isti način zaključujemo da je $z = \pm 2i$, pa je $cd + 1 = -4$, odnosno $cd = -5$, što nije moguće za $|c| > \sqrt{5}$. Sada smo samo provjerili da $|b| \geqslant |a| \geqslant 2$ povlači tu nejednakost za $|c|$, odnosno da ne postoji Diofantova trojka $\{a, b, c\}$ takva da je $2 \leqslant |a|, |b|, |c| \leqslant \sqrt{5}$. □

Lema 5.3.3. *Ako je $\{a, b, c, d\}$ Diofantova četvorka takva da je $2 \leqslant |a| \leqslant |b| \leqslant |c| \leqslant |d|$, onda je $|d| \geqslant \dfrac{|ab|}{8}$.*

Napomena. Slutimo da vrijedi i jača tvrdnja, ako $d \neq a + b + c + 2abc \pm 2rst$ (gdje su $s^2 = ac + 1$ i $t^2 = bc + 1$), onda je $|d| \geqslant 4|ab|$. Ta tvrdnja vrijedi u cijelim brojevima (vidi npr. [32]).

Dokaz. Prema prethodnoj lemi, možemo, bez smanjenja općenitosti, pretpostaviti da $\{a, b, d\}$ nije regularna trojka. Označimo $ab + 1 = r^2, ad + 1 = x^2, bd + 1 = y^2$.

Tada $c_\pm = a+b+d+2abd \pm 2rxy$ nije 0. Zaista, tvrdnja $c_\pm = 0$ ekvivalentna je sljedećim tvrdnjama

$$\begin{aligned}
& c_\pm = 0 \\
\iff & a+b+d+2abd = \mp 2rxy \\
\iff & (2ab+1)d + a + b = \mp 2rxy \\
\iff & (2ab+1)^2 d^2 + 2(a+b)(2ab+1)d + (a+b)^2 = 4(ab+1)(ad+1)(bd+1) \\
\iff & 4a^2b^2d^2 + 4abd^2 + d^2 + 4a^2bd + 4ab^2d + 2ad + 2bd + a^2 + 2ab + b^2 = \\
& \quad = 4a^2b^2d^2 + 4a^2bd + 4ab^2d + 4abd^2 + 4ab + 4ad + 4bd + 4 \\
\iff & d^2 - 2(a+b)d + (a-b)^2 - 4 = 0.
\end{aligned}$$

Rješenja ove kvadratne jednadžbe po d upravo su $a+b\pm 2r$. Dakle, kako $\{a,b,d\}$ nije regularna trojka, slijedi da $d \neq a+b\pm 2r$, pa je $c_\pm \neq 0$.

Promotrimo sad produkt

$$\begin{aligned}
c_+c_- &= (a+b+d+2abd)^2 - 4r^2x^2y^2 \\
&= (a+b+d+2abd)^2 - 4(ab+1)(ad+1)(bd+1) \\
&= a^2+b^2+d^2-2ab-2ad-2bd-4.
\end{aligned}$$

Stoga je $|c_+c_-| \leqslant |a|^2+|b|^2+|d|^2+2|ab|+2|ad|+2|bd|+4$. Kako je $|d| \geqslant |a|, |b|$ i $|d|^2 \geqslant 4$ (ne postoji Diofantova četvorka u kojoj bi najveći element po apsolutnoj vrijednosti bio manji od 2), slijedi da je $|c_+c_-| \leqslant 10|d|^2$.

S druge strane, $|c_+ + c_-| = 2|a+b+d+2abd|$. Pretpostavimo da je $|c_+| \geqslant |c_-|$. Tada je $2|c_+| \geqslant |c_+| + |c_-| \geqslant |c_+ + c_-|$ (prema nejednakosti trokuta). Slijedi da je $|c_+| \geqslant |a+b+d+2abd|$.

Budući da je $|b| \geqslant |a| \geqslant 2$, slijedi da je $|ab| \geqslant 4$, pa je $|a+b+d| \leqslant 3|d| \leqslant \frac{3}{4}|abd|$. Možemo zaključiti da je

$$|c_+| \geqslant |a+b+d+2abd| \geqslant 2|abd| - |a+b+d| \geqslant 2|abd| - \frac{3}{4}|abd| = \frac{5}{4}|abd|.$$

Usporedbom ove donje granice za $|c_+|$ s gornjom granicom za $|c_+c_-|$, slijedi da je

$$|c_-| \leqslant \frac{10|d|^2}{|c_+|} \leqslant \frac{10|d|^2}{\frac{5}{4}|abd|} = \frac{8|d|}{|ab|}.$$

Budući da $c_- \neq 0$, slijedi da je $\frac{8|d|}{|ab|} \geqslant |c_-| \geqslant 1$, pa je $|d| \geqslant \frac{|ab|}{8}$. □

5.4 Gornja granica na veličinu Diofantove m-torke

Teorem 5.4.1. *Ne postoji Diofantova m-torka u Gaussovim cijelim brojevima za $m \geqslant 42$.*

Dokaz. Pretpostavimo suprotno, da postoji m-torka $\{a_1, a_2, \ldots, a_m\}$ poredana po veličini $(0 < |a_1| \leqslant \cdots \leqslant |a_m|)$ i $m \geqslant 42$. Računalom je provjereno da do apsolutne vrijednosti 12 imamo najviše Diofantovu trojku, te da nema petorke do apsolutne vrijednosti 16. Dakle, $|a_3| \geqslant 2$, $|a_4| \geqslant 12, |a_5| \geqslant 16$. Sad ćemo više puta primijeniti Lemu 5.3.3 na različite podskupove od $\{a_1, a_2, \ldots, a_m\}$, te svaku dobivenu nejednakost iskoristiti u sljedećoj primjeni:

$$\begin{aligned}
\{a_6, a_7, a_8, a_9\} &\overset{5.3.3}{\Longrightarrow} |a_9| \geqslant \frac{|a_6 a_7|}{8} \geqslant \frac{|a_6|^2}{8} \\
\{a_9, a_{10}, a_{11}, a_{12}\} &\overset{5.3.3}{\Longrightarrow} |a_{12}| \geqslant \frac{|a_9|^2}{8} \geqslant \frac{|a_6|^4}{8^3} \\
\{a_{12}, a_{13}, a_{14}, a_{15}\} &\overset{5.3.3}{\Longrightarrow} |a_{15}| \geqslant \frac{|a_{12}|^2}{8} \geqslant \frac{|a_6|^8}{8^7} \\
\{a_{15}, a_{16}, a_{17}, a_{18}\} &\overset{5.3.3}{\Longrightarrow} |a_{18}| \geqslant \frac{|a_6|^{16}}{8^{15}} \\
\{a_{18}, a_{19}, a_{20}, a_{21}\} &\overset{5.3.3}{\Longrightarrow} |a_{21}| \geqslant \frac{|a_6|^{32}}{8^{31}} \\
\{a_{21}, a_{22}, a_{23}, a_{24}\} &\overset{5.3.3}{\Longrightarrow} |a_{24}| \geqslant \frac{|a_6|^{64}}{8^{63}}
\end{aligned}$$

Pokažimo sada da Propoziciju 5.2.3 možemo primijeniti na $\{a_3, a_6, a_{24}, a_{24+k}\}$, za $k > 0$ zbog toga što je $|a_3| \geqslant 2$ i $|a_4| \geqslant 12$. Naime, primjenom Leme 5.3.3 na $\{a_3, a_4, a_5, a_6\}$ slijedi da je $|a_6| \geqslant \frac{|a_3 a_4|}{8} \geqslant \frac{3}{2}|a_3|$. Prethodno dokazana nejednakost pak garantira da je $|a_{24}| > |a_6|^{15}$, jer je za to dovoljno da je $\frac{|a_6|^{64}}{8^{63}} > |a_6|^{15}$, odnosno $|a_6| > 14.49158$, što vrijedi zbog $|a_6| \geqslant |a_5| \geqslant 16$. Ispunjeni su uvjeti Propozicije 5.2.3.

Stoga je, prema Propoziciji 5.2.3,

$$|a_{24+k}| < 4278^{20}|a_{24}|^{50}. \tag{5.4.1}$$

Međutim, možemo nastaviti primijenjivati Lemu 5.3.3:

$$\begin{aligned}
\{a_{24}, a_{25}, a_{26}, a_{27}\} &\overset{5.3.3}{\Longrightarrow} |a_{27}| \geqslant \frac{|a_{24}|^2}{8} \\
\{a_{27}, a_{28}, a_{29}, a_{30}\} &\overset{5.3.3}{\Longrightarrow} |a_{30}| \geqslant \frac{|a_{27}|^2}{8} \geqslant \frac{|a_{24}|^4}{8^3} \\
\ldots &\overset{5.3.3}{\Longrightarrow} |a_{42}| \geqslant \frac{|a_{24}|^{64}}{8^{63}} > 4278^{20}|a_{24}|^{50},
\end{aligned}$$

što je u kontradikciji s nejednakošću (5.4.1).

Naime, zadnja nejednakost ekvivalentna je s $|a_{24}|^{14} \geqslant 8^{63} \cdot 4278^{20}$, tj. vrijedi za

$|a_{24}| > 1.784 \cdot 10^9$ što stoji jer znamo da je $|a_{24}| \geqslant \frac{|a_6|^{64}}{8^{63}} \geqslant \frac{16^{64}}{8^{63}}$. □

Istaknimo ovdje da se dokazani rezultati izvjesno mogu poopćiti za dobivanje gornje granice na veličinu Diofantove m-torke u prstenima cijelih brojeva imaginarnog kvadratnog polja. Ključan rezultat koji koristimo je Jadrijević-Ziegler teorem koji vrijedi u toj općenitijoj situaciji. Računalnim pretragama nismo uspjeli naći Diofantovu petorku u takvim prstenima, a ni sistematičnija potraga u [24] nije pronašla Diofantove petorke u $\mathbb{Z}[\sqrt{-d}]$ za $d < 50$. Ipak, ne vidimo neki a priori razlog zašto bi u svim prstenima cijelih brojeva imaginarnog kvadratnog polja najveća m-torka imala isti broj elemenata. Dosadašnjom metodom dokaza, koja funkcionira za općenita imaginarna kvadratna polja, vjerojatno nećemo moći dokazati najjaču gornju ogradu u konkretnoj situaciji Gaussovih cijelih brojeva.

Najdulji korak u poopćenju zapravo će biti računalna provjera da do apsolutne vrijednosti 12 imamo najviše Diofantovu trojku, odnosno, da do 16 nema petorke. U ovom slučaju provjera je napravljena u Mathematici, gdje je lako raditi s Gaussovim cijelim brojevim. Radi potpunosti i obnovljivosti, navodimo kod kojim je provjereno da ne postoji Diofantova četvorka u kojoj su svi elementi po apsolutnoj vrijednosti manji ili jednaki 12. Treba imati na umu da je tih brojeva skoro 450, pa je vrlo velik broj četvorki koje treba provjeriti.

Jednostavna funkcija provjerava je li kompleksan broj kvadrat u Gaussovim cijelim brojevima:

```
IsSquare[broj_] :=
 Return[Element[Re[Sqrt[broj]], Integers] &&
   Element[Im[Sqrt[broj]], Integers]]          .
```

Sljedeća funkcija vraća popis svih nenul Gaussovih cijelih brojeva apsolutne vrijednosti do određenog broja (radijusa).

```
GaussCircle[radijus_] := (
   lista = List[];
   For[re = Floor[-radijus], re <= radijus, re = re + 1,
    For[im = Floor[-radijus], im <= radijus, im = im + 1,
     If[re^2 + im^2 <= radijus^2 && re^2 + im^2 > 0,
       AppendTo[lista, re + im*I]]]];
   lista);
```

Sad generiramo popis Gaussovih cijelih brojeva apsolutne vrijednosti do 12 pomoću te funkcije.

```
popis = GaussCircle[12];
```

Nakon toga prolazimo po popisu i za svaki Diofantov par provjeravamo čini li Diofantovu četvorku s preostalim parovima.

```
maks = Length[popis];

For[j = 1, j <= maks - 3, j = j + 1,
 For[k = j + 1, k <= maks - 2, k = k + 1,
  a = popis[[j]]; b = popis[[k]];

  If[IsSquare[a*b + 1],
   For[l = k + 1, l <= maks - 1, l = l + 1,
    For[m = l + 1, m <= maks, m = m + 1,
     c = popis[[l]]; d = popis[[m]];
     If[IsSquare[a*c + 1] &&
        IsSquare[a*d + 1] &&
        IsSquare[b*c + 1] &&
        IsSquare[b*d + 1] &&
        IsSquare[c*d + 1],
      Print[a, " ", b, " ", c, " ", d]]]]]]]
```

5.5 Rekurzivna svojstva rješenja pellovskog sustava

Kao što smo već istaknuli, metoda kojom smo dokazali da Diofantova m-torka u Gaussovim cijelim brojevima ima najviše 42 elementa, vjerojatno se ne može iskoristiti da se dokaže bitno bolja granica. Iako tu granicu nismo uspjeli poboljšati, u ovom i sljedećem potpoglavlju navodimo neke rezultate koji bi mogli biti korisni za takvo poboljšanje.

Iz (c) dijela Leme 5.1.2 mogu se dobiti i riješiti rekurzije iste kao u [13]. Preciznije, vrijedi sljedeća lema.

Lema 5.5.1. *Svako rješenje z jednadžbe (5.1.1) nalazi se u jednom od sljedećih nizova*

$$v_0^{(i)} = z_0^{(i)}, \quad v_1^{(i)} = sz_0^{(i)} + cx_0^{(i)}, \quad v_{m+2}^{(i,)} = 2sv_{m+1}^{(i)} - v_m^{(i)} \quad za\ i = 1, \ldots, i_0. \tag{5.5.1}$$

Slično, svako rješenje z jednadžbe (5.1.2) nalazi se u jednom od nizova

$$w_0^{(j)} = z_1^{(j)}, \quad w_1^{(j)} = tz_1^{(j)} + cy_1^{(j)}, \quad w_{n+2}^{(i)} = 2tw_{n+1}^{(j)} - w_n^{(j)}, \quad za\ j = 1, \ldots, j_0. \tag{5.5.2}$$

Dokaz. Rekurzivna relacija (5.5.1) slijedi iz (5.1.3). Prema njoj je

$$\begin{aligned} x_{m+1}\sqrt{c} + z_{m+1}\sqrt{a} &= (x\sqrt{c} + z\sqrt{a})(s + \sqrt{ac})^{m+1} \\ &= (x\sqrt{c} + z\sqrt{a})(s + \sqrt{ac})^{m}(s + \sqrt{ac}) \end{aligned}$$

$$\begin{aligned} &= (x_m\sqrt{c} + z_m\sqrt{a})(s + \sqrt{ac}) \\ &= (sx_m + az_m)\sqrt{c} + (sz_m + cx_m)\sqrt{a}, \end{aligned}$$

pa je $x_{m+1} = sx_m + az_m$ i $z_{m+1} = sz_m + cx_m$. Iz toga je

$$\begin{aligned} z_{m+2} &= sz_{m+1} + cx_{m+1} \\ &= sz_{m+1} + c(sx_m + az_m) \\ &= sz_{m+1} + acz_m + scx_m \\ &= sz_{m+1} + acz_m + s(z_{m+1} - sz_m) \\ &= 2sz_{m+1} + (ac - s^2)z_m \\ &= 2sz_{m+1} - z_m. \end{aligned}$$

Dakle, za sve nizove rješenja $z_m^{(i)}$ vrijedi rekurzivna relacija istog oblika (5.5.1). Kako ne bismo označavali rješenja dviju različitih jednadžbi istim oznakama, označili smo sa $v_m^{(i)}$ nizove rješenja z jednadžbe (5.1.1). Nizove rješenja z jednadžbe (5.1.2) označili smo s $w_n^{(j)}$ i analogno se dokazuje njihova rekurzivna relacija (5.5.2). □

Ako je d proširenje početne trojke, onda je z rješenje u obje jednadžbe (5.1.1) i (5.1.2), pa se takav z nalazi i u jednom od nizova $v_m^{(i)}$ i u jednom od nizova $w_n^{(j)}$, tj. $z = v_m^{(i)} = w_n^{(j)}$.

Lema 5.5.2. *Vrijede i sljedeće kongruencije:*

$$\begin{aligned} v_{2m}^{(i)} &\equiv z_0^{(i)} \pmod{2c} \quad te \quad v_{2m+1}^{(i)} \equiv sz_0^{(i)} + cx_0^{(i)} \pmod{2c} \\ w_{2n}^{(j)} &\equiv z_1^{(j)} \pmod{2c} \quad te \quad w_{2n+1}^{(j)} \equiv tz_1^{(j)} + cy_1^{(j)} \pmod{2c} \end{aligned}$$

za sve cijele brojeve m i n.

Dokaz. U dokazu ispuštamo gornje indekse (i) i (j). Tvrdnje dokazujemo matematičkom indukcijom. Za $m = 0$ je $v_0 = z_0$ i $v_1 = sz_0 + cx_0$, pa očito vrijede i kongruencije modulo $2c$. Pretpostavimo da je $v_{2m} \equiv z_0 \pmod{2c}$ i $v_{2m+1} \equiv sz_0 + cx_0 \pmod{2c}$. Koristeći rekurzivnu relaciju za niz v_m, vrijedi da je

$$\begin{aligned} v_{2m+2} &= 2sv_{2m+1} - v_{2m} \\ &\equiv 2s(sz_0 + cx_0) - z_0 \\ &\equiv 2s^2z_0 + 2cx_0 - z_0 \\ &\equiv 2(ac+1)z_0 - z_0 \\ &\equiv z_0 \pmod{2c}. \end{aligned}$$

Koristeći ovu kongruenciju, induktivnu pretpostavku i rekurzivnu relaciju za v_m, slijedi i

da je

$$\begin{aligned} v_{2m+3} &= 2sv_{2m+2} - v_{2m+1} \\ &\equiv 2sz_0 - (sz_0 + cx_0) \\ &\equiv sz_0 - cx_0 \\ &\equiv sz_0 + cx_0 \pmod{2c}, \end{aligned}$$

što je i trebalo dokazati. Potpuno analogno dokazuje se tvrdnja za niz w_n. □

Korolar 5.5.3. *Pretpostavimo da je* $|a| \geqslant \sqrt{8}$ *i* $|c| > 2|b|$. *Ako je* $v_{2m}^{(i)} = w_{2n}^{(j)}$ *za cijele* m *i* n, *onda je* $z_0^{(i)} = z_1^{(j)}$.

Dokaz. Primijetimo da iz $v_{2m} = w_{2n}$, prema Lemi 5.5.2, slijedi da $2c$ dijeli $z_0^{(i)} - z_1^{(j)}$. Naime, iz Korolara 5.1.3 je $|z_1^{(j)}| < |c|$. Analogno je $|z_0^{(i)}| < |c|$. Stoga je, po nejednakosti trokuta, $|z_0^{(i)} - z_1^{(j)}| \leqslant |z_0^{(i)}| + |z_1^{(j)}| < 2|c|$. Budući da $2c \mid z_0^{(i)} - z_1^{(j)}$, slijedi da je $z_0^{(i)} - z_1^{(j)} = 0$, pa je $z_0^{(i)} = z_1^{(j)}$.

□

Lema 5.5.4. *Ako je* $v_m = w_n$, *onda vrijedi*

a) $|z_0| = 1$ *ili* $|z_0|^2 \geqslant |c| - 1$

b) $|c| \geqslant 4|a|$ *i* $|a| \geqslant 3 \Rightarrow |sz_0| < \sqrt{2}|cx_0|$

c) $3.1651|c|\sqrt[4]{|ac|} \geqslant |v_1| \geqslant \dfrac{|c|^{3/4}}{8|a|^{1/4}}$

d) Ako je $|c| \geqslant 4|b|$ *i* $|b| \geqslant |a| \geqslant 3$, *onda je* $m \leqslant 2n + 2$.

Dokaz. a) Budući da je $v_m^2 \equiv z_0^2 \equiv 1 \pmod{c}$, slijedi da je $z_0^2 = ck + 1$, pa ako k nije 0, slijedi da je $|z_0|^2 \geqslant |c| - 1$, prema nejednakosti trokuta.

b) Tvrdnja je ekvivalentna sljedećima

$$\begin{aligned} & |sz_0| < \sqrt{2}|cx_0| \\ \iff & \left|\frac{s^2}{c^2}\right| < 2\left|\frac{x_0^2}{z_0^2}\right| \\ \iff & \left|\frac{ac+1}{c^2}\right| \leqslant 2\left|\frac{az_0^2 + c - a}{cz_0^2}\right| \\ \iff & |ac+1| \cdot |z_0|^2 \leqslant 2|acz_0^2 + c(c-a)|. \end{aligned}$$

Desna strana je $\geqslant 2|ac||z_0|^2 - 2|c||c-a|$ pa je dovoljno $2|ac||z_0|^2 - 2|c||c-a| > |ac| \cdot |z_0|^2 + |z_0|^2$, što je ekvivalentno s $(|ac| - 1)|z_0|^2 > 2|c| \cdot |c-a|$.

Iz $|c| \geqslant 4|a|$ slijedi da je $|c-a| \leqslant |c|+|a| \leqslant \frac{5}{4}|c|$ pa je $2|c| \cdot |c-a| < \frac{5}{2}|c|^2$. S druge strane, po a) dijelu imamo dva slučaja.

Ako je $|z_0|^2 \geqslant |c|-1$, onda je $(|ac|-1)|z_0|^2 \geqslant (|ac|-1)(|c|-1) = |a||c|^2-(|a|+1)|c|+1$, pa je dovoljno dokazati $|a||c|^2-(|a|+1)|c|+1 > \frac{5}{2}|c|^2$. Ovo je kvadratno u $|c|$ pa se lako provjeri da vrijedi za $|c| \geqslant 8$. Ako je pak $z_0 = 1$, tada je i $x_0 = 1$, pa vrijedi i jača nejednakost $|s| \leqslant |c|$. U svakom slučaju je $|sz_0| < \sqrt{2}|cx_0|$.

c) Iz b) dijela te ograda za fundamentalna rješenja (tj. Korolara 5.1.3) je

$$|v_1| = |cx_0+sz_0| = \left|\frac{c^2x_0^2-(ac+1)z_0^2}{cx_0-sz_0}\right| = \left|\frac{c(c-a)-z_0^2}{cx_0-sz_0}\right| \geqslant \frac{|c|^2-|a|\cdot|c|-|z_0|^2}{|cx_0|+|sz_0|}$$
$$\geqslant \frac{|c|^2-\frac{|c|^2}{4}-\frac{61}{32}\frac{|c|^{3/2}}{|a|^{1/2}}}{(1+\sqrt{2})|cx_0|} \geqslant \frac{24|c|-61\frac{|c|^{1/2}}{|a|^{1/2}}}{32(1+\sqrt{2})|x_0|} \geqslant \frac{24|c|-61\frac{|c|^{1/2}}{|a|^{1/2}}}{32(1+\sqrt{2})\sqrt{\frac{55}{32}}|ac|^{1/4}} > \frac{24|a|^{1/2}|c|-61|c|^{1/2}}{102|a|^{3/4}|c|^{1/4}}$$
$$> \frac{13.83|a|^{1/2}|c|}{102|a|^{3/4}|c|^{1/4}} > \frac{|c|^{3/4}}{8|a|^{1/4}}$$

S druge strane je $|v_1| = |cx_0+sz_0| \leqslant (1+\sqrt{2})|cx_0| \leqslant (1+\sqrt{2})\sqrt{\frac{55}{32}}|c|\sqrt[4]{|ac|} < 3.1651|c|\sqrt[4]{|ac|}$.

d) Iz c) dijela i rekurzija ($|v_{m+1}| \geqslant |v_m|$) sad slijedi

$$\frac{|c|^{3/4}}{8|a|^{1/4}}(2|s|-1)^{m-1} < |v_m| < 3.1651|c|\sqrt[4]{|ac|}(2|s|+1)^{m-1}.$$

Slično, iz $|c| \geqslant 4|b|$, slijedi

$$|w_n| < (2|t|+1)^{n-1} \cdot 3.0606|c|\sqrt[4]{|bc|}.$$

Naime, vrijedi slična ograda za fundamentalno rješenje $|y_1| \leqslant \sqrt{\frac{45}{28}}\sqrt[4]{|bc|}$ i na isti način kao u b) i c) se dokazuje $|tz_1| < \sqrt{2}|cy_1|$ i $|w_1| < (1+\sqrt{2})|cy_1|$. Iz toga i rasta $|w_n|$ slijedi ova gornja ograda.

Nije teško (iz $|c| \geqslant 4|b|$) ograditi $2|t|+1 \leqslant \frac{19}{8}\sqrt{|bc|}$ i $2|s|-1 \geqslant \frac{13}{8}\sqrt{|ac|}$, pa je $(2|s|-1)^2 > 2|t|+1$ i sad se usporedbom donje granice za $|v_m|$ i gornje za $|w_n|$ dobiva $m \leqslant 2n+2$:

$$(2|s|-1)^{m-1} < 24.4848\sqrt[4]{|abc^2|}(2|t|+1)^{n-1} < 12.2424(2|t|+1)^n < (2|t|+1)^{n+0.9816}$$
$$< (2|s|-1)^{2n+1.97} \Longrightarrow m < 2n+2.97 \Longrightarrow m \leqslant 2n+2$$

□

5.6 Linearne forme u logaritmima

Rješavanjem rekurzija (5.5.1) i (5.5.2) dobivamo

$$v_m = \frac{1}{2\sqrt{a}}\left((z_0\sqrt{a}+x_0\sqrt{c})(s+\sqrt{ac})^m + (z_0\sqrt{a}-x_0\sqrt{c})(s-\sqrt{ac})^m\right) \tag{5.6.1}$$

$$w_n = \frac{1}{2\sqrt{b}}\left((z_1\sqrt{b}+y_1\sqrt{c})(t+\sqrt{bc})^n + (z_1\sqrt{b}-y_1\sqrt{c})(t-\sqrt{bc})^n\right). \tag{5.6.2}$$

Označimo s

$$P = \frac{1}{\sqrt{a}}(z_0\sqrt{a}+x_0\sqrt{c})(s+\sqrt{ac})^m, \text{ i s } Q = \frac{1}{\sqrt{b}}(z_1\sqrt{b}+y_1\sqrt{c})(t+\sqrt{bc})^n. \tag{5.6.3}$$

Iz $z = v_m = w_n$ slijedi da je $P - \frac{c-a}{a}P^{-1} = Q - \frac{c-b}{b}Q^{-1}$.

Lema 5.6.1. *Ako je* $|c| \geqslant 4|b|$ *i* $m, n \geqslant 3$, *onda je* $|P| > 12\left|\frac{c}{a}\right|$ *i* $|Q| > 12\left|\frac{c}{b}\right|$.

Dokaz. Primijetimo da je $|s+\sqrt{ac}| \geqslant \sqrt{|ac|}$. To slijedi iz: $\mathrm{Re}\sqrt{1+\frac{1}{ac}} > 0 \Rightarrow \left|\sqrt{1+\frac{1}{ac}}+1\right| > 1 \Rightarrow |\sqrt{ac+1}+\sqrt{ac}| > \sqrt{|ac|}$. Stoga je

$$\begin{aligned}
|P| =& \frac{1}{\sqrt{|a|}}|z_0\sqrt{a}+x_0\sqrt{c}|\cdot|s+\sqrt{ac}|^m \\
\geqslant& \frac{|c-a|}{\sqrt{|a|}}\frac{1}{|z_0\sqrt{a}-x_0\sqrt{c}|}\sqrt{|ac|}^m \\
\geqslant& \frac{|c|-|a|}{\sqrt{|a|}}\frac{1}{|x_0\sqrt{c}|+|z_0|\sqrt{|a|}}|ac|^{3/2} \\
\geqslant& \frac{|c|-|c|/4}{\sqrt{|a|}}\frac{1}{3|c|/2+|c|\sqrt{|a|}}|ac|^{3/2} \\
\geqslant& \frac{3|a||c|^{3/2}}{6+4\sqrt{|a|}} \\
>& 12\left|\frac{c}{a}\right|
\end{aligned}$$

Posljednja nejednakost ekvivalentna je s $|a|^2|c|^{1/2} > 2(12+8\sqrt{|a|})$. Budući da je $|c| > 4|a|$, dovoljno je pokazati da je $2|a|^{5/2} > 2(12+8|a|^{1/2})$, što zaista vrijedi za $|a|^{1/2} \geqslant 2$.

Analogno iz $|c| \geqslant 4|b|$ i $n \geqslant 3$ slijedi $|Q| > 12\left|\frac{c}{b}\right|$. □

Stoga je

$$||P| - |Q|| \leqslant |P-Q| = \left|\frac{c-a}{a}P^{-1} - \frac{c-b}{b}Q^{-1}\right|$$

$$\begin{aligned}
&\leqslant \left|\frac{c}{a}-1\right|\frac{1}{|P|}+\left|\frac{c}{b}-1\right|\frac{1}{|Q|}\\
&\leqslant \left|\frac{c}{a}-1\right|\cdot\frac{1}{12}\left|\frac{a}{c}\right|+\left|\frac{c}{b}-1\right|\cdot\frac{1}{12}\left|\frac{b}{c}\right|\\
&\leqslant \frac{1}{12}\left(\left|1-\frac{a}{c}\right|+\left|1-\frac{b}{c}\right|\right)\\
&\leqslant \frac{1}{12}\left(2+\frac{1}{4}+\frac{1}{4}\right)\\
&= \frac{5}{24}.
\end{aligned}$$

Slijedi da je $\left|\frac{|P|-|Q|}{|P|}\right| \leqslant \frac{5}{24}|P|^{-1} \leqslant \frac{5}{24} < 1$. Sada ćemo primijeniti jednostavnu Lemu B.2 iz [44].

Lema 5.6.2. *Neka je $\Delta > 0$ takav da je $|\Delta - 1| \leqslant a$. Tada je*

$$|\log \Delta| \leqslant \frac{-\log(1-a)}{a}|\Delta - 1|.$$

Pomoću nje dobivamo sljedeći niz nejednakosti za $\Lambda = \frac{|Q|}{|P|}$.

$$\begin{aligned}
|\log\Lambda| = \left|\log\frac{|Q|}{|P|}\right| &\leqslant \frac{24}{5}\log\frac{24}{19}\cdot\frac{5}{24}|P|^{-1}\\
&\leqslant \log\frac{24}{19}|P|^{-1}\\
&\leqslant \log\frac{24}{19}\sqrt{|a|}\frac{|x_0|\sqrt{|c|}+|z_0|\sqrt{|a|}}{|c-a|}|s+\sqrt{ac}|^{-m}\\
&\leqslant \log\frac{24}{19}\sqrt{|a|}\frac{3|c|^{3/2}/2+|c|^{3/2}/2}{3|c|/4}|s+\sqrt{ac}|^{-m}\\
&= \frac{8}{3}\log\frac{24}{19}\sqrt{|ac|}|s+\sqrt{ac}|^{-m}
\end{aligned}$$

Lema 5.6.3. *Ako s K označimo $K = \frac{8}{3}\log\frac{24}{19}$, onda je*

$$|\log\Lambda| = \left|m\log|s+\sqrt{ac}| - n\log|t+\sqrt{bc}| + \log\frac{|\sqrt{b}(z_0\sqrt{a}+x_0\sqrt{c})|}{|\sqrt{a}(z_1\sqrt{b}+y_1\sqrt{c})|}\right| < K\sqrt{|ac|}|s+\sqrt{ac}|^{-m}.$$

Lema 5.6.4. *Ako je $|b| > 14.232|a|, |c| > 100|b|$, $n \geqslant 3$ i ako za gornju linearnu formu vrijedi još i $0 < \log\Lambda$, onda je $m \geqslant n$.*

Dokaz. Lema 5.6.3 nam daje

$$\frac{m}{n} > \frac{\log|t+\sqrt{bc}|}{\log|s+\sqrt{ac}|} - \frac{\log|\gamma|}{n\log|s+\sqrt{ac}|},$$

gdje je $\gamma = \dfrac{\sqrt{b}(z_0\sqrt{a}+x_0\sqrt{c})}{\sqrt{a}(z_1\sqrt{b}+y_1\sqrt{c})}$. Dovoljno je dokazati

$$\begin{aligned}
&\frac{\log|t+\sqrt{bc}|}{\log|s+\sqrt{ac}|} - \frac{\log|\gamma|}{n\log|s+\sqrt{ac}|} > \frac{n-1}{n}\\
\iff &\frac{\log|t+\sqrt{bc}|/|s+\sqrt{ac}|}{\log|s+\sqrt{ac}|} - \frac{\log|\gamma|}{n\log|s+\sqrt{ac}|} > -\frac{1}{n}\\
\iff &\log\frac{|t+\sqrt{bc}|}{|s+\sqrt{ac}|} > \frac{\log|\gamma| - \log|s+\sqrt{ac}|}{n}\\
\iff &\left(\frac{|t+\sqrt{bc}|}{|s+\sqrt{ac}|}\right)^n > \frac{|\gamma|}{|s+\sqrt{ac}|}.
\end{aligned}$$

Ali, $\left(\dfrac{|t+\sqrt{bc}|}{|s+\sqrt{ac}|}\right)^3 > \left(\dfrac{1.99998\sqrt{|bc|}}{2.00012\sqrt{|ac|}}\right)^3 > 0.999\left(\dfrac{|b|}{|a|}\right)^{3/2}$, jer je $|t+\sqrt{bc}|+|t-\sqrt{bc}| = |t+\sqrt{bc}|+|\sqrt{bc}-t| \geqslant 2|\sqrt{bc}|$, pa je $\dfrac{|t+\sqrt{bc}|}{|\sqrt{bc}|} \geqslant 2 - \dfrac{1}{|t+\sqrt{bc}|\sqrt{|bc|}} > 2 - \dfrac{1}{200\cdot 200} = 1.99998$. S druge strane je, prema Korolaru 5.1.3,

$$\begin{aligned}
\frac{|\gamma|}{|s+\sqrt{ac}|} &\leqslant \frac{\sqrt{|b|}}{\sqrt{|a|}}\frac{2.692^2|a|^{1/4}|c|^{3/4}|b|^{1/4}|c|^{3/4}}{0.99|c|^{3/2}|a|^{1/2}}\\
&\leqslant 7.3201\left(\frac{|b|}{|a|}\right)^{3/4}
\end{aligned}$$

Stoga, za $n \geqslant 3$, dovoljno je da je $0.999\left(\frac{|b|}{|a|}\right)^{3/2} > 7.3201\left(\frac{|b|}{|a|}\right)^{3/4}$, odnosno $\frac{|b|}{|a|} > 14.232$, što smo i pretpostavili. □

Lema 5.6.5. *Ako je $\{a,b,c\}$ Diofantova trojka, $\dfrac{|c|}{|a|} \notin \mathbb{Q}$ i $\dfrac{|c|}{|b|} \notin \mathbb{Q}$, onda* $\log\Lambda \neq 0$.

Dokaz. Dokažimo da, ako je $v_m = w_n$, onda $|P| \neq |Q|$.

Da $P \neq Q$ nije teško pokazati, jer onda bi bilo i $P^{-1} = Q^{-1}$, pa ako je $v_m = w_n$, onda je i $\frac{c-a}{a} = \frac{c-b}{b}$, pa bi bilo $b = a$ (ako c nije 0).

Daljnji dokaz nastao je prateći dokaz Lemme 5.2. iz [21].

Po definiciji je $P = A + B\alpha, Q = C + D\beta$, gdje su $\alpha = \sqrt{\frac{c}{a}}$ i $\beta = \sqrt{\frac{c}{b}}$, $A, B, C, D \in \mathbb{Q}[i]$.

Iz $v_m = w_n$ je $\frac{A+B\alpha+A-B\alpha}{2} = \frac{C+D\beta+C-D\beta}{2}$, $(v_m = A, w_n = C)$ pa je $A = C$. Nadalje, $|P|^2 = (A+B\alpha)(\bar{A}+\bar{B}\bar{\alpha}) = A\bar{A} + \bar{A}B\alpha + A\bar{B}\bar{\alpha} + |B|^2|\alpha|^2$ tj.

$$\begin{aligned}
|P|^2 &= p + u\alpha + \bar{u}\bar{\alpha} + q|\alpha|^2\\
|Q|^2 &= r + v\beta + \bar{v}\bar{\beta} + s|\beta|^2,
\end{aligned}$$

gdje su $p, q, r, s \in \mathbb{Q}$, a $u, v \in \mathbb{Q}[i]$.

Tvrdnja A: Brojevi $\alpha = \sqrt{\frac{c}{a}}$, $\beta = \sqrt{\frac{c}{b}}$ i $\sqrt{\frac{a}{b}}$ su algebarski stupnja 2.

Iz Leme 5.1.1 slijedi da $\frac{c}{a}$, $\frac{c}{b}$ i $\frac{a}{b}$ nisu kvadrati u $\mathbb{Q}[i]$. □

Tvrdnja B: Baza za $\mathbb{Q}[i](\alpha, \bar{\alpha})$ nad $\mathbb{Q}[i]$ je $B_\alpha = \{1, \alpha, \bar{\alpha}, |\alpha|^2\}$. Analogno je za $\mathbb{Q}[i](\beta, \bar{\beta})$ baza $B_\beta = \{1, \beta, \bar{\beta}, |\beta|^2\}$.

Ako je $\gamma \in \mathbb{Q}[i](\alpha, \bar{\alpha})$, onda je $\gamma = \sum q_{ij}\alpha^i\bar{\alpha}^j$, gdje su $q_{ij} \in \mathbb{Q}[i]$. Međutim, kako su $\alpha^2 = \frac{c}{a}$ i $\bar{\alpha}^2$ u $\mathbb{Q}[i]$, te $\alpha\bar{\alpha} = |\alpha|^2$, slijedi da se γ može zapisati kao $\gamma = q_0 + q_1\alpha + q_2\bar{\alpha} + q_3|\alpha|^2$.

Preostaje pokazati da je B_α linearno nezavisan skup nad $\mathbb{Q}[i]$. Pokažimo prvo da je $\{1, \alpha, \bar{\alpha}\}$ linearno nezavisan. Pretpostavimo suprotno. Tada je $\bar{\alpha} = A + B\alpha$ za neke $A, B \in \mathbb{Q}[i]$. Kvadriranjem slijedi $\bar{\alpha}^2 - A^2 - B^2\alpha^2 = 2AB\alpha$, pa ako $AB \neq 0$, onda je

$$\alpha = \frac{\bar{\alpha}^2 - A^2 - B^2\alpha^2}{2AB} \in \mathbb{Q}[i], \text{ što je u kontradikciji s tvrdnjom } \mathbf{A}.$$

Ako je $B = 0$, onda je $\bar{\alpha} = A \in \mathbb{Q}[i]$. Tada bi i $\alpha = \sqrt{\frac{c}{a}}$ bilo u $Q[i]$, odnosno $\frac{c}{a} = \frac{x^2}{y^2}$ za neke $x, y \in \mathbb{Z}[i]$, pa je $\frac{|c|}{|a|} = \frac{|x|^2}{|y|^2} \in \mathbb{Q}$, što je u suprotnosti s pretpostavkom leme.

Ako je $A = 0$, onda je $\bar{\alpha} = B\alpha$, pa bi ponovo bilo

$$\frac{|c|}{|a|} = |\alpha|^2 = \alpha\bar{\alpha} = B\alpha^2 \in \mathbb{Q}[i] \cap \mathbb{R}, \text{ odnosno, ponovo bi bilo } \frac{|c|}{|a|} \in \mathbb{Q}.$$

Dakle, $\{1, \alpha, \bar{\alpha}\}$ je linearno nezavisan skup nad $\mathbb{Q}[i]$.

Sad je za linearnu nezavisnost B_α dovoljno dokazati da ne postoje $A, B, C \in \mathbb{Q}[i]$ takvi da je

$$|\alpha|^2 = A + B\alpha + C\bar{\alpha}. \tag{5.6.4}$$

Dokažimo prvo da $C \neq 0$. U suprotnom bi bilo $|\alpha|^2 = A + B\alpha$, pa je kvadriranjem $|\alpha|^4 = A^2 + B^2\alpha^2 + 2AB\alpha$. Slijedi da je $2AB\alpha \in \mathbb{Q}[i]$. Budući da $\alpha \notin \mathbb{Q}[i]$, slijedi da je $AB = 0$. Ako je $B = 0$, onda je $|\alpha^2| = A \in \mathbb{Q}$, što je u suprotnosti s pretpostavkom leme. Ako je pak $A = 0$, onda je $|\alpha|^2 = B\alpha$, pa je $\bar{\alpha} = B \in \mathbb{Q}[i]$, što je ponovo u kontradikciji s pretpostavkom leme.

Dakle, $C \neq 0$.

Iz (5.6.4) množenjem s α slijedi da je $\alpha^2\bar{\alpha} = A\alpha + B\alpha^2 + C|\alpha|^2$, iz čega slijedi $C|\alpha|^2 = -A\alpha - B\alpha^2 + \alpha^2\bar{\alpha}$, odnosno

$$|\alpha|^2 = -\frac{B}{C}\alpha^2 - \frac{A}{C}\alpha + \frac{1}{C}\alpha^2\bar{\alpha}. \tag{5.6.5}$$

Kako je $\{1, \alpha, \bar{\alpha}\}$ linearno nezavisan skup, iz jednakosti (5.6.4) i (5.6.5) slijedi da je $A = -\frac{B}{C}\alpha^2, B = -\frac{A}{C}, C = \frac{1}{C}\alpha^2$. Iz posljednje dobivene jednakosti je $C^2 = \alpha^2$, ali po tvrdnji $\mathbf{A}$, α^2 nije kvadrat u $\mathbb{Q}[i]$, čime dobivamo kontradikciju. □

Tvrdnja C: Skup $B = \{1, \alpha, \bar{\alpha}, |\alpha|^2, \beta, \bar{\beta}, |\beta|^2\}$ je linearno nezavisan nad $\mathbb{Q}[i]$.

Napomenimo da je dokaz ove tvrdnje sličan kao u [21], jer ni tamo ništa ne ovisi o konkretnom obliku trojke s kojom se radi. Ipak, navodimo ga radi potpunosti.

Prvo ćemo dokazati da $\beta, \bar{\beta}$ i $|\beta|^2$ nisu elementi od $\mathbb{Q}[i](\alpha, \bar{\alpha})$. Pretpostavimo da se β može prikazati kao

$$\beta = A + B\alpha + C\bar{\alpha} + D|\alpha|^2, \tag{5.6.6}$$

za neke $A, B, C, D \in \mathbb{Q}[i]$. Tada je

$$\begin{aligned}\beta^2 =& A^2 + B^2\alpha^2 + C^2\bar{\alpha}^2 + D^2|\alpha|^4 + \\ &+ 2AB\alpha + 2AC\bar{\alpha} + 2AD|\alpha|^2 + 2BC|\alpha|^2 + 2BD\alpha^2\bar{\alpha} + 2CD\bar{\alpha}^2\alpha.\end{aligned}$$

Iz $\beta^2 \in \mathbb{Q}[i]$ slijedi da su koeficijenti od algebarskih brojeva $\alpha, \bar{\alpha}$ i $|\alpha|^2$ jednaki nula, tj.

$$AB + CD\bar{\alpha}^2 = 0, \tag{5.6.7}$$

$$AC + BD\alpha^2 = 0, \tag{5.6.8}$$

$$AD + BC = 0. \tag{5.6.9}$$

Iz (5.6.7) i (5.6.9), množenjem (5.6.7) s A ili C, slijedi da je $A^2 = C^2\bar{\alpha}^2$ ili $B = D = 0$. Slično, iz (5.6.8) i (5.6.9) slijedi da je $A^2 = B^2\alpha^2$ ili $C = D = 0$, a iz (5.6.7) i (5.6.8) da je $A^2 = D^2|\alpha|^4$ ili $B = C = 0$. Sad imamo tri slučaja.

- $B = C = D = 0$. Iz (5.6.6) slijedi da je $\beta \in \mathbb{Q}[i]$ što je u kontradikciji s tvrdnjom **A**.
- $B \neq 0$, $C = D = 0$. Slijedi da je $\beta = B\alpha$, tj. $\sqrt{\frac{a}{b}} = B \in \mathbb{Q}[i]$, kontradikcija s tvrdnjom **A**.
- $B \neq 0$ i bar jedan od C ili D nije nula. Tada je $A^2 = C^2\bar{\alpha}^2 = B^2\alpha^2 = D^2|\alpha|^4$, pa je $\beta^2 = 4A^2$, što je ponovo u kontradikciji s tvrdnjom **A**.

Dakle, β se ne može prikazati preko B_α. Isto vrijedi za $\bar{\beta}$ i $|\beta|^2$ i dokazuje se na identičan način.

Koristit ćemo zatvorenost $L[\{1, \alpha, \bar{\alpha}, |\alpha|^2\}]$ na invertiranje, koja vrijedi jer je

$$\begin{aligned}\frac{1}{A + B\alpha + C\bar{\alpha} + D|\alpha|^2} &= \frac{(A + B\alpha) - (C\bar{\alpha} + D|\alpha|^2)}{K + L\alpha} \\ &= \frac{((A + B\alpha) - (C\bar{\alpha} + D|\alpha|^2))(K - L\alpha)}{K^2 - L^2\alpha^2},\end{aligned}$$

gdje je $K = A^2 + B^2\alpha^2 - C^2\bar{\alpha}^2 - D^2|\alpha|^4$, $L = 2(AB - CD\bar{\alpha}^2)$.

Pokažimo sada da se ni $\bar{\beta}$ ne može prikazati kao linearna kombinacija elemenata iz $B_\alpha \cup \{\beta\}$. Analogno se pokazuje linearna nezavisnost skupova $B_\alpha \cup \{\bar{\beta}, |\beta|^2\}$ i $B_\alpha \cup \{\beta, |\beta|^2\}$.

Naime, tada bi bilo $\bar{\beta} = q_1 + q_2\alpha + q_3\bar{\alpha} + q_4|\alpha|^2 + q_5\beta$ i $q_5 \neq 0$. Kvadriranjem slijedi

$$\begin{aligned}\bar{\beta}^2 =& q_1^2 + q_2^2\alpha^2 + q_3^2\bar{\alpha}^2 + q_4|\alpha|^4 + q_5^2 + \\ &+ 2(q_1q_2 + q_3q_4\bar{\alpha}^2)\alpha + 2(q_1q_3 + q_2q_4\alpha^2)\bar{\alpha} + 2(q_1q_4 + q_2q_3)|\alpha|^2 + \\ &+ 2q_1q_5\beta + 2(q_2q_5\alpha + q_3q_5\bar{\alpha})\beta + 2q_4q_5|x\alpha|^2\beta,\end{aligned}$$

iz čega vidimo da je $2q_5\beta(q_1 + q_2\alpha + q_3\bar{\alpha} + q_4|\alpha|^2) \in L[\{1, \alpha, \bar{\alpha}, |\alpha|^2\}]$. Budući da $q_5 \neq 0$, slijedi da je $q_1 + q_2\alpha + q_3\bar{\alpha} + q_4|\alpha|^2 = 0$, odnosno $q_1 = q_2 = q_3 = q_4 = 0$. Međutim, onda bi bilo $\bar{\beta} = q_5\beta$ za neki $q_5 \in \mathbb{Q}[i]$, pa bi slijedilo $|\beta|^2 = q_5\beta^2 \in \mathbb{Q}[i] \cap \mathbb{R}$, odnosno $|\beta|^2 \in \mathbb{Q}$, što je u suprotnosti s pretpostavkom leme.

Slično dobivamo ako pretpostavimo da se $|\beta|^2$ može prikazati kao linearna kombinacija elemenata iz $\{1, \alpha, \bar{\alpha}, |\alpha|^2, \beta, \bar{\beta}\}$. Iz $|\beta|^2 = q_1 + q_2\alpha + q_3\bar{\alpha} + q_4|\alpha|^2 + q_5\beta + q_6\bar{\beta}$ kvadriranjem i zamjenom $|\beta|^2$ slijedi da je $2(q_1 + q_2\alpha + q_3\bar{\alpha} + q_4|\alpha|^2 + q_5q_6)(q_5\beta + q_6\bar{\beta}) \in L[\{1, \alpha, \bar{\alpha}, |\alpha|^2\}]$, pa je $q_5\beta + q_6\bar{\beta} = 0$, iz čega bi opet slijedilo $|\beta|^2 \in \mathbb{Q}$, ili je $q_1 + q_2\alpha + q_3\bar{\alpha} + q_4|\alpha|^2 + q_5q_6 = 0$, iz čega, opet zbog linearne nezavisnosti B_α, slijedi $q_2 = q_3 = q_4 = 0$ i $q_1 + q_5q_6 = 0$. Stoga je $|\beta|^2 = q_1 + q_5\beta + q_6\bar{\beta}$, ali to je u kontradikciji s linearnom nezavisnošću B_β. □

Prisjetimo se da smo iz $P = A + B\alpha$ i $Q = C + D\beta$, preko $|P|^2 = (A + B\alpha)(\bar{A} + \bar{B}\bar{\alpha})$ i analogne tvrdnje za $|Q|^2$, dobili da je

$$\begin{aligned}|P|^2 &= p + u\alpha + \bar{u}\bar{\alpha} + q|\alpha|^2 \\ |Q|^2 &= r + v\beta + \bar{v}\bar{\beta} + s|\beta|^2,\end{aligned}$$

gdje su $p, q, r, s \in \mathbb{Q}$, a $u, v \in \mathbb{Q}[i]$. Kako želimo dokazati da $|P| \neq |Q|$, dovoljno je dokazati da $|P|^2 \neq |Q|^2$. Da je $|P|^2 = |Q|^2$, slijedilo bi

$$(p - r) + u\alpha + \bar{u\alpha} + q|\alpha|^2 - v\beta - \bar{v\beta} - s|\beta|^2 = 0,$$

pa po tvrdnji **C** slijedi da je $p - r = u = q = v = s = 0$, odnosno $P = A = C = Q$, što smo već dokazali da nije moguće.

Dakle $|P| \neq |Q|$, iz čega slijedi da $\log\Lambda = \log\dfrac{|P|}{|Q|} \neq 0$. □

Ova lema može biti korisna i kod proučavanja proširenja jednoparametarskih familija Diofantovih trojki u Gaussovim cijelim brojevima. Npr. specijalna verzija te leme dokazana je i korištena u [21], a korištena je i u [5]. Uz to, u oba ta članka korištena je tvrdnja slična Lemi 5.6.3. I u nekim drugačijim istraživanjima dokazivan je analogni rezultat, npr. u [22].

5.7 Primjena linearnih formi na familiju $\{k-1, k+1, 16k^3-4k\}$

Vraćamo se na problem proširenja Diofantovih trojki oblika $\{k-1, k+1, 16k^3-4k\}$. U ovom dijelu je niz (v_n) definiran kao u (4.1.3), a $(w_m^{(i)})$ kao u Lemi 4.1.3.

Lema 5.7.1. *Ako je $v_n = w_m^{(j)}$ za neke j, m, n te je $|k| > 2.5$, onda je $m \leqslant n \leqslant 3m+2$.*

Dokaz. Iz Leme 4.2.1, odnosno, iz rekurzivnih relacija induktivno slijede sljedeće nejednakosti,

$$(2|k|-1)^n \leqslant |v_n| \leqslant (2|k|+1)^n$$
$$(8|k|^2-4|k|-3)^{m-1} \leqslant |w_m^{(j)}| \leqslant (8|k|^2+4|k|+3)^{m+1}.$$

Ako je $v_n = w_m$, slijedi da je $(2|k|+1)^n > (8|k|^2-4|k|-3)^{m-1}$, pa je $n \geqslant m$. Pretpostavimo suprotno, da je $n \leqslant m-1$. Tada slijedi da je $8|k|^2-4|k|-3 < 2|k|+1$, što daje kontradikciju za $|k| > 2.5$.

Pretpostavimo $n \geqslant 3m+3$. Iz $v_n = w_m$ slijedi da je $(8|k|^2+4|k|+3)^{m+1} \geqslant (2|k|-1)^n \geqslant (2|k|-1)^{3m+3}$, pa je $8|k|^2+4|k|+3 > (2|k|-1)^3 = 8|k|^3-12|k|^2+6|k|-1$. Iz toga je $-2(4|k|^3-10|k|^2+|k|-2) > 0$, što nije moguće za $|k| > 2.5$. □

Rješenja rekurzija kojima su zadani nizovi (v_n) i (w_m) su

$$v_n = \frac{\sqrt{k+1}+\sqrt{k-1}}{2\sqrt{k+1}}(k+\sqrt{k^2-1})^n + \frac{\sqrt{k+1}-\sqrt{k-1}}{2\sqrt{k+1}}(k-\sqrt{k^2-1})^n,$$
$$w_m = \frac{1}{2\sqrt{16k^3-4k}}\Big((x_1\sqrt{16k^3-4k}+z_1\sqrt{k-1})(4k^2-2k-1+\sqrt{(16k^3-4k)(k-1)})^m +$$
$$+ (x_1\sqrt{16k^3-4k}-z_1\sqrt{k-1})(4k^2-2k-1-\sqrt{(16k^3-4k)(k-1)})^m\Big).$$

Uzmimo $P' = \frac{1}{\sqrt{c}}(x_1\sqrt{c}+z_1\sqrt{a})(s+\sqrt{ac})^m$ i $Q' = \frac{1}{\sqrt{b}}(\sqrt{a}+\sqrt{b})(r+\sqrt{ab})^n$. Napomenimo da je $Q' \neq Q$ i $P' = \sqrt{\frac{a}{c}}P$, međutim, uz $m \geqslant 3$, vrijede iste ograde na Q' i $|P'|-|Q'|$ te se dobivaju na sličan način:

$$|Q'| = \frac{1}{\sqrt{|b|}}|\sqrt{a}+\sqrt{b}|\cdot|r+\sqrt{ab}|^n \geqslant \frac{|b-a|}{\sqrt{|b|}}\cdot\frac{1}{|\sqrt{b}-\sqrt{a}|}|\sqrt{ab}|^3$$
$$\geqslant \frac{2}{\sqrt{|b|}}\cdot\frac{1}{|\sqrt{b}|+|\sqrt{a}|}|ab|^{3/2} \geqslant 12\frac{|b|}{|a|},$$

jer je $|a|^{5/2} \geqslant 6(\sqrt{|b|}+\sqrt{|a|})$, odnosno $|k+1|^{5/2} \geqslant 6(\sqrt{|k+1|}+\sqrt{|k-1|})$, što vrijedi za $|k| \geqslant 4.846$. Iz ovoga, ako je $|k| \geqslant 23$, slijedi da je $|Q'| \geqslant 11$ jer je $12\frac{|k+1|}{|k-1|} \geqslant 12\frac{|k|-1}{|k|+1} \geqslant 11$,

što je ekvivalentno s $|k| \geqslant 23$. Slično vrijedi da je $|P'| \geqslant 12$ pa je

$$\begin{aligned} ||P'| - |Q'|| &\leqslant \left|\frac{c-a}{c}(P')^{-1} - \frac{b-a}{b}(Q')^{-1}\right| \leqslant \left|1-\frac{a}{c}\right|\frac{1}{|P'|} + \left|1-\frac{a}{b}\right|\frac{1}{|Q'|} \\ &\leqslant \frac{1}{12}\left|1-\frac{a}{c}\right| + \frac{1}{11}\frac{2}{|b|} < \frac{5}{48} + \frac{5}{48} = \frac{5}{24}, \end{aligned}$$

za $|b| \geqslant |k| - 1 > \frac{96}{55}$. Stoga će i za linearnu formu $\Gamma = \log \Lambda' = \log \frac{|P'|}{|Q'|}$ vrijediti zaključak Leme 5.6.3.

Neka je $k = \mu + i\nu$ i

$$\begin{aligned} \alpha_1 &= |k + \sqrt{k^2-1}|, \\ \alpha_2 &= |4k^2 - 2k - 1 + \sqrt{(16k^3-4k)(k-1)}| \text{ i} \\ \alpha_3 &= \left|\frac{\sqrt{16k^3-4k}(\sqrt{k-1}+\sqrt{k+1})}{\sqrt{k+1}(x_1\sqrt{16k^3-4k}+z_1\sqrt{k+1})}\right|. \end{aligned}$$

Minimalni polinom za α_1 je $p_1(x) = x^8 - 4(\mu^2+\nu^2)x^6 + (8\mu^2 - 8\nu^2 - 2)x^4 - 4(\mu^2+\nu^2)x^2 + 1$ prema [21]. U tom radu pokazano je i $h(\alpha_1) \leqslant \frac{1}{4}\log(2|k|+1)$.

Minimalni polinom za α_2 je, uz pomoć Mathematice,

$$\begin{aligned} p_2(x) = x^8 &- 4\left((16(\mu^2+\nu^2) - 16\mu - 4)(\mu^2+\nu^2) + 16\nu^2 + 4\mu + 1\right)x^6 + \\ &+ \left((128\mu^4 - 128\mu^3 - 32\mu^2 + 32\mu + 6) + (-768\mu^2 + 384\mu + 32)\nu^2 + 128\nu^4\right)x^4 \\ &- 4\left((16(\mu^2+\nu^2) - 16\mu - 4)(\mu^2+\nu^2) + 16\nu^2 + 4\nu + 1)\right)x^2 + 1. \end{aligned}$$

Polinom $p_2(x)$ ima sljedeće nultočke:

$$\begin{aligned} x_{1,2} &= \pm\alpha_2, & x_{5,6} &= \pm\sqrt{|s|^2 - |ac| + \sqrt{(|s|^2-|ac|)^2 - 1}}, \\ x_{3,4} &= \pm|s - \sqrt{ac}|, & x_{7,8} &= \pm\sqrt{|s|^2 - |ac| - \sqrt{(|s|^2-|ac|)^2 - 1}}, \end{aligned}$$

te je $|x_i| = 1$ za $i = 5, 6, 7, 8$. Iz toga je

$$h(\alpha_2) \leqslant \frac{1}{8}\log|x_1||x_2| = \frac{1}{4}\log|4k^2 - 2k - 1 + \sqrt{(16k^3-4k)(k-1)}|,$$

pa slijedi $h(\alpha_2) \leqslant \frac{1}{4}\log|9k^2| = \frac{1}{2}\log 3|k|$.

Lema 5.7.2. *Ako je $|k| \geqslant 10^7$, onda za sve konjugate α_3' od α_3 vrijedi da je $|\alpha_3'| \leqslant |k|^4$.*

Dokaz. Može se pogoditi minimalni polinom za α_3, odnosno svi konjugati. Prvih osam su $x_{1,2}' = \pm\alpha_3$, $x_{3,4} = \pm\left|\frac{\sqrt{c}(\sqrt{b}+\sqrt{a})}{\sqrt{b}(x_1\sqrt{c}-z_1\sqrt{a})}\right|$, $x_{5,6} = \pm\left|\frac{\sqrt{c}(\sqrt{b}-\sqrt{a})}{\sqrt{b}(x_1\sqrt{c}-z_1\sqrt{a})}\right|$, $x_{7,8} = \pm\left|\frac{\sqrt{c}(\sqrt{b}-\sqrt{a})}{\sqrt{b}(x_1\sqrt{c}-z_1\sqrt{a})}\right|$.

Nadalje, $x_9, \ldots, x_{12}$ nultočke su od

$$q_1(x) = x^4 - 2\left|\frac{c}{b(x_1\sqrt{c}+z_1\sqrt{a})^2}\right|(|b|-|a|)x^2 + \left|\frac{c(b-a)}{b(x_1\sqrt{c}+z_1\sqrt{a})^2}\right|^2,$$

$x_{13}, \ldots, x_{16}$ od

$$q_2(x) = x^4 - 2\left|\frac{c}{b(x_1\sqrt{c}-z_1\sqrt{a})^2}\right|(|b|-|a|)x^2 + \left|\frac{c(b-a)}{b(x_1\sqrt{c}-z_1\sqrt{a})^2}\right|^2,$$

idućih osam od

$$q_3(x) = x^4 - 2\left|\frac{c(\sqrt{b}+\sqrt{a})^2}{b(c-a)^2}\right|(|cx_1^2|-|az_1^2|)x^2 + \left|\frac{c(\sqrt{b}-\sqrt{a})^2}{b(c-a)}\right|^2 \quad \text{i}$$

$$q_4(x) = x^4 - 2\left|\frac{c(\sqrt{b}-\sqrt{a})^2}{b(c-a)^2}\right|(|cx_1^2|-|az_1^2|)x^2 + \left|\frac{c(\sqrt{b}-\sqrt{a})^2}{b(c-a)}\right|^2,$$

zatim

$$q_5(x) = x^4 - 2\left|\frac{c}{b(c-a)^2}\right|(|x_1\sqrt{bc}+z_1a|^2-|x_1\sqrt{ac}+z_1\sqrt{ab}|^2)x^2 + \left|\frac{c(b-a)}{b(c-a)}\right|^2$$

i na kraju

$$q_6(x) = x^4 - 2\left|\frac{c}{b(c-a)^2}\right|(|x_1\sqrt{bc}-z_1a|^2-|x_1\sqrt{ac}-z_1\sqrt{ab}|^2)x^2 + \left|\frac{c(b-a)}{b(c-a)}\right|^2.$$

Iz tog se može dobiti željena ocjena. Naime, nultočka normiranog polinoma ograničena je odozgo sa zbrojem apsolutnih vrijednosti koeficijenata. Vidimo da su u ovim polinomima koeficijenti najviše reda $|c|^2\cdot|a|$ (ili $\cdot|b|$). Preciznije, pokazat ćemo da su svi koeficijenti uz x^2 manji od $3|k|^7$, a svi slobodni koeficijenti manji od $1025|k|^7$ za dovoljno velik k.

Koeficijent uz x^2 u q_1 i q_2 je manji ili jednak od $2|c|(|b|+|a|) \leqslant 2|16k^3-4k|(2|k|+2) \leqslant |k|^5$ za $|k| \geqslant 65$. Ovakve tvrdnje dokazuju se računski kao i dosad, nejednakošću trokuta i analizom dobivenih funkcija u $|k|$. Koeficijent uz x^2 u q_3 i q_4 je manji ili jednak od

$$\begin{aligned}
&\frac{2|c|(\sqrt{|a|}+\sqrt{|b|})(|cx_1^2|+|az_1^2|)}{|b|^2|c-a|}\\
\leqslant&\frac{2|16k^3-4k|\cdot 2\sqrt{|k|+1}(150|k|^5+65)}{(|k|-1)^2(16|k|^3-5|k|-1)}\\
<&|k|^4 \quad \text{za } |k| \geqslant 1.45\cdot 10^6.
\end{aligned}$$

Slično je koeficijent uz x^2 u q_5 i q_6 manji od $3|k|^7$ već za $|k| \geqslant 2$.

Slobodni koeficijenti manji su od $|16k^3-4k|^2(2\sqrt{|k|+1})^2 \leqslant 1025|k|^7$ za $|k| \geqslant 1025$.

Stoga za svaki konjugat α_3' vrijedi da je $|\alpha_3'|^2 \leqslant 1028|k|^7$, odnosno $|\alpha_3'| \leqslant |k|^4$ za

$|k| \geqslant 10^7$.

□

Lema 5.7.3. *Ako je* $|k| \geqslant 5 \cdot 10^{37}$, $\Gamma \neq 0$ *i* $v_n = w_m$, *onda je* $m \leqslant 2$ *ili* $n \leqslant 2$.

Dokaz. Pretpostavimo suprotno, da je $v_n = w_m$ i $n \geqslant m \geqslant 3$. Vrijedi $M(\alpha_3) \leqslant |a_d| \prod_{i=1}^{d} \max\{|\alpha^{'}|, 1\}$ i $|a_d| \leqslant \left(\sqrt{|k|+1}(|x_1|\sqrt{16|k|^3+4|k|}+|z_1|\sqrt{|k|+1})\right)^{32} < 257^{16}|k|^{65}$. Budući da je u Lemi 5.7.2 za konjugate $\alpha_3^{'}$ dobivena ograda $|\alpha_3'| \leqslant |k|^4$, slijedi da je

$$h(\alpha_3) \leqslant \frac{1}{32}\log\left(257^{16}|k|^{65} \cdot |k|^{4\cdot 32}\right) = 2.774538 + \frac{193}{32}\log|k|.$$

Za sve tri ograde vrijedi $h'(\alpha_i) \leqslant 7\log|k|$.

Iz Leme 5.6.3 je $|\Gamma| = |\log\Lambda'| < K\sqrt{|ac|}|s+\sqrt{ac}|^{-m}$ (ako je $m, n \geqslant 3$), gdje je $K = \frac{8}{3}\log\frac{24}{19} = 0.622973$. Budući da je $|s+\sqrt{ac}| \geqslant \sqrt{|ac|} = \sqrt{|(16k^3-4k)(k-1)|}$, slijedi $|s+\sqrt{ac}| > 3|k|^2$ (za $|k| > 3$). Stoga je

$$|\Gamma| < K\sqrt{|ac|}(3|k|^2)^{-m} < K(1.5|k|)^{1-m}.$$

Sada ćemo primijeniti sljedeći teorem iz [4].

Teorem 5.7.4 (Baker, Wüstholz)**.** *Neka je* $\Gamma = b_1\log\alpha_1 + b_2\alpha_2 + \cdots + b_n\log\alpha_n$ *linearna forma u logaritmima algebarskih brojeva* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *s cjelobrojnim koeficijentima* $b_1, b_2, \ldots, b_n$. *Ako* $\Gamma \neq 0$, *onda je*

$$\log|\Gamma| \geqslant -18(n+1)!n^{n+1}(32d)^{n+2}\log(2nd)h'(\alpha_1)h'(\alpha_2)\ldots h'(\alpha_n)\log B,$$

gdje je $d = [\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) : \mathbb{Q}]$, $B = \max\{|b_1|, |b_2|, \ldots, |b_n|\}$, *a* $h'(\alpha) = \max\{h(\alpha), \frac{1}{d}|\log\alpha|, \frac{1}{d}\}$, *pri čemu je* $h(\alpha)$ *logaritamska Weilova visina.*

Iz Baker–Wüstholz teorema je, ako $\Gamma \neq 0$,

$$\log K(1.5|k|)^{1-m} > \log|\Gamma| > -18\cdot 4!\cdot 3^4(32\cdot 2048)^5\cdot 343\log^3|k|\log(6\cdot 2048)\log n,$$

odnosno $(1-m)\log\frac{3}{2}|k| > \log K + (1-m)\log\frac{3}{2}|k| > -K'\log^3|k|\log n$, pri čemu je $\log K \approx -0.47325$. Iz toga i Leme 5.7.1 slijedi

$$\frac{m-1}{\log(3m+2)} \leqslant \frac{m-1}{\log n} < K'\frac{\log^3|k|}{\log\frac{3}{2}|k|} < K'\log^2|k|,$$

gdje je $K' = 18\cdot 4!\cdot 3^4(32\cdot 2048)^5\cdot 343\log(6\cdot 2048) \approx 1.3663\cdot 10^{32}$.

Budući da je $m \geqslant 2|k|-1$ (potpoglavlje 4.2), a funkcija $f(x) = \frac{x-1}{\log(3x+2)}$ rastuća, slijedi $\frac{2|k|-2}{\log(6|k|-1)} < K'\log^2|k|$ i $|k|-1 < 6.831506\cdot 10^{31}\log^2|k|\log(6|k|-1)$, što je nemoguće za $|k| \geqslant 5\cdot 10^{37}$. □

Lema 5.7.5. *Ako je k Gaussov cijeli broj takav da je* $\operatorname{Im} k \operatorname{Re} k \neq 0$*, onda* $\dfrac{|k+1|}{|k-1|} \notin \mathbb{Q}$.

Dokaz. Dovoljno je dokazati da $|k+1| \cdot |k-1|$ nije u $\mathbb{Q}$, pa je onda dovoljno i da nije cijeli broj. Ako je $k = x + yi$, onda je $|k+1|^2 \cdot |k-1|^2 = x^4 + y^4 + 1 + 2x^2y^2 - 2x^2 + 2y^2$, pa je dovoljno dokazati da taj izraz nije potpun kvadrat.

Vrijedi $x^4+y^4+1+2x^2y^2-2x^2+2y^2 > (x^2+y^2-2)^2$, jer je to ekvivalentno s $2x^2+6y^2 > 3$, što vrijedi. Slično, zbog $x \neq 0$, vrijedi $x^4 + y^4 + 1 + 2x^2y^2 - 2x^2 + 2y^2 < (x^2 + y^2 + 1)^2$.

Iz $x^4 + y^4 + 1 + 2x^2y^2 - 2x^2 + 2y^2 = (x^2 + y^2)^2$ bi slijedilo $1 - 2x^2 + 2y^2 = 0$, što zbog parnosti nije moguće, a iz $x^4 + y^4 + 1 + 2x^2y^2 - 2x^2 + 2y^2 = (x^2 + y^2 - 1)^2$ je $4y^2 = 0$, ponovo nemoguće zbog $y \neq 0$. □

Lema 5.7.6. *Ako je k Gaussov cijeli broj takav da je* $\operatorname{Im} k \neq 0$*, onda* $\dfrac{|16k^3 - 4k|}{|k-1|} \notin \mathbb{Q}$

Dokaz. Ponovo je dovoljno dokazati da $|16k^3 - 4k| \cdot |k - 1|$ nije cijeli broj, odnosno da $|4k^3 - k|^2 \cdot |k - 1|^2$ nije potpun kvadrat.

Ako je $k = x + yi$, onda je $|4k^3 - k|^2 \cdot |k - 1|^2 = |4x^4 - 4x^3 - 24x^2y^2 - x^2 + 12xy^2 + x + 4y^4 + y^2 + i(16x^3y - 12x^2y - 16xy^3 - 2xy + 4y^3 + y)|^2 = (x^2 - 2x + 1 + y^2)(4x^2 - 4x + 1 + 4y^2)(4x^2 + 4x + 1 + 4y^2)(x^2 + y^2)$. Zamjenom $z = -4x + 1$ dobiva se $(z^4 + (32y^2 - 10)z^2 + 160y^2 + 256y^4 + 9)^2 + 4096y^2z^2$. Supstitucijama $u = z^2, v = y^2$ slijedi da je $(u^2 + (32v - 10)u + 160v + 256v^2 + 9)^2 + 4096uv$ kvadrat, pri čemu u i v također trebaju biti potpuni kvadrati. Budući da $y = \operatorname{Im} k \neq 0$, ni v nije 0, a slično ni $u = (-4x + 1)^2 \neq 0$. Stoga je $(u^2+(32v-10)u+160v+256v^2+9)^2+4096uv > (u^2+(32v-10)u+160v+256v^2+9)^2$, pa ako je lijevi izraz kvadrat, postoji prirodan w takav da je $(u^2 + (32v - 10)u + 160v + 256v^2 + 9)^2 + 4096uv = (u^2 + (32v - 10)u + 160v + 256v^2 + 9 + w)^2$.

Slijedi da je $2w(u^2+(32v-10)u+160v+256v^2+9)+w^2-4096uv = 0$, što je kvadratna jednadžba po nepoznanici u. Diskriminanta je

$$\begin{aligned} 4D(v,w) &= -8(w^3 - 32w^2 + 65536v^2w - 2097152v^2 + 640vw^2 - 20480vw) \\ &= -4 \cdot 2((w^2(w-32) + 65536v^2(w-32) + 640wv(w-32)), \end{aligned}$$

što je negativno za $w > 32$. Da bi rješenje bilo cjelobrojno, diskriminanta mora biti potpun kvadrat. Budući da je w prirodan, slijedi da je $w \in \{1, 2, \ldots, 32\}$.

Kako je $D(v, 32) = 0$, rješavanjem kvadratne jednadžbe slijedi da je $u = 16v+5$, što nije kvadrat jer 5 nije kvadratni ostatak modulo 16. Za većinu preostalih vrijednosti w ćemo na sličan način pokazati da $D(v, w)$ nije kvadrat. Primijetimo da je $D(v, w) \equiv -2w^2(w - 32) \pmod{128}$.

Za neparan w je $D(v, w) \equiv 2 \pmod 4$, što ne može biti kvadrat. Za $w \equiv 2 \pmod 8$ je $D(v, w) \equiv -16 \pmod{64}$, a za $w \equiv 4 \pmod 8$ je $D(v, w) \equiv 128 \pmod{256}$, pa ponovo diskriminanta ne može biti kvadrat.

Za $w = 6$ je $\frac{D(v,6)}{16} = 212992v^2 + 12480v + 117 \equiv 5 \pmod{16}$, pa $D(v,6)$ ne može biti kvadrat. Slično, iz $\frac{D(v,8)}{256} \equiv 12 \pmod{16}$, $\frac{D(v,16)}{4096} \equiv 2 \pmod 4$ i $\frac{D(v,22)}{16} \equiv 13 \pmod{16}$ slijedi da $D(v,8)$, $D(v,16)$ i $D(v,22)$ ne mogu biti potpuni kvadrati.

Za $w = 14$ je $(128v+9)^2 > \frac{D(v,14)}{144} = (128v+7)^2+448v$, pa provjerom slijedi da $D(v,14)$ nije kvadrat jer je $v > 0$. Slično, iz $(32v+4)^2 > \frac{D(v,24)}{1024} = 1024v^2+240v+9 = (32v+3)^2+48$ i $(128v+19)^2 > \frac{D(v,30)}{16} = (128v+15)^2+960v$ slijedi da ni $D(v,24)$ ni $D(v,30)$ nije kvadrat jer je $v > 0$.

Budući da smo ispitali sve $w \in \{1, 2, \ldots, 31, 32\}$, lema je dokazana. □

Teorem 5.7.7. *Neka je k Gaussov cijeli broj takav da je $\operatorname{Re} k \neq 0$ i $|k| \geqslant 5 \cdot 10^{37}$. Tada se Diofantova trojka $\{k-1, k+1, 16k^3-4k\}$ do Diofantove četvorke može proširiti samo s $d = 4k$ ili $d = 64k^5 - 48k^3 + 8k$.*

Dokaz. Ako je $\operatorname{Im} k = 0$, onda su elementi niza (v_n) cijeli brojevi, te je stoga x cijeli broj. Budući da je $(k-1)d + 1 = x^2$, slijedi $d \in \mathbb{Q} \cap \mathbb{Z}[i]$, odnosno, d je cijeli broj. Također je d nužno istog predznaka kao i $k-1, k+1$ i $16k^3 - 4k$ (jer je $d = \frac{x^2-1}{k-1} \neq 0$), pa prema Theorem 1 iz [9], budući da je $|k| \geqslant 2$, slijedi da je $d = 4k$ ili $d = 64k^5 - 48k^3 + 8k$.

Pretpostavimo nadalje da je $\{a, b, c, d\}$ Diofantova četvorka za $a = k-1, b = k+1, c = 16k^3 - 4k$ te da $\operatorname{Im} k$ nije 0.

Provjerom v_n i w_m za male indekse dobivamo predviđena proširenja $4k$, $64k^5-48k^3+8k$ i kandidate poput $w_1^{(1)} = 4k^2 - k - 2$. Izračunom prvih nekoliko vrijednosti niza (v_n), $v_1 = 2k - 1$ i $v_2 = 4k^2 - 2k - 1$, vidimo da se $w_1^{(2)}$ za velike $|k|$ ne može poklopiti s tim vrijednostima, a ni s većim elementima v_n za $n \geqslant 3$, jer su veći od $w_1^{(1)}$ po apsolutnoj vrijednosti: $|v_n| - |w_1^{(2)}| \geqslant |v_3 - w_1^{(2)}| = |8k^3 - 4k^2 - 4k + 1 - (4k^2 - 2k - 1)| > 0$ za $|k| > 10^{37}$. Slično za $v_1 = 2k - 1$ i $v_2 = 4k^2 - 2k - 1$ vidimo da ne mogu ujedno biti element niza $w_m^{(1)}$. Analogno za nizove $w_m^{(j)}$ za preostale $j = 2, 3, 4, 5, 6$.

Dakle, indeksi n i m su veći od 2 ako $d \notin \{4k, 64k^5 - 48k^3 + 8k\}$.

Prema Lemi 5.7.5 i Lemi 5.7.6, $\frac{|c|}{|a|}$ i $\frac{|b|}{|a|}$ nisu racionalni. Iz toga slijedi, kao u Lemi 5.6.5, da linearna forma $\Gamma = \log \Lambda'$ nije 0. Da je $v_n = w_m$ za $m \geqslant 2$ i $n \geqslant 2$, onda bi po Lemi 5.7.3 slijedilo $|k| < 5 \cdot 10^{37}$, što je kontradikcija. Stoga je pogrešna pretpostavka $v_n = w_m$ za $m \geqslant 3$ i $n \geqslant 3$, a time i $d \notin \{4k, 64k^5 - 48k^3 + 8k\}$ za $|k| \geqslant 5 \cdot 10^{37}$. □

Poglavlje 6

Diofantove trojke s dodatnim $D(n)$-svojstvima

U ovom poglavlju bavimo se sljedećim pitanjem. Koliko različitih $D(n)$-svojstava može imati jedna Diofantova trojka $\{a, b, c\}$? Ovo pitanje 2001. godine postavili su A. Kihel i O. Kihel [33]. Oni su izrazili i slutnju da ne postoje Diofantove trojke koje su ujedno i $D(n)$-skup za neki n različit od 1. Ta slutnja ne vrijedi jer je, npr. $\{8, 21, 55\}$ i Diofantova trojka i $D(4321)$-trojka (primijećeno u MathSciNet recenziji njihovog članka, Dujella), a $\{1, 8, 120\}$ ima $D(1)$ i $D(721)$-svojstvo (ovaj primjer pronađen je u [47]).

Svaka trojka $\{a, b, c\}$ inducira eliptičku krivulju $E : y^2 = (x + ab)(x + bc)(x + ca)$. Ako uz to skup $\{a, b, c\}$ ima i $D(n)$-svojstvo, onda postoje cijeli brojevi r, s i t takvi da je $ab + n = r^2, ac + n = s^2, bc + n = t^2$. Stoga na E imamo cjelobrojnu točku (n, rst). Dakle, za svaki n za koji skup $\{a, b, c\}$ ima $D(n)$-svojstvo, postoji cjelobrojna točka na E. Ova implikacija ne može se direktno obrnuti, odnosno, cjelobrojna točka na E ne daje nužno n za koji trojka $\{a, b, c\}$ ima $D(n)$-svojstvo. Pokazuje se da dvostruke cjelobrojne točke (i samo one) imaju x-koordinatu n takvu da je skup $\{a, b, c\}$ ujedno i $D(n)$-trojka.

Ovu vezu s eliptičkim krivuljama iskoristit ćemo za konstrukciju nekoliko beskonačnih familija Diofantovih trojki $\{a, b, c\}$ koje su ujedno i $D(n)$-skupovi za dva različita prirodna n koja nisu 1. Također, prikazat ćemo neke primjere Diofantovih trojki $\{a, b, c\}$ koje su također i $D(n)$-skupovi za tri različita prirodna $n \neq 1$. Rezultati dobiveni ovdje objavljeni su u [2].

6.1 Eliptičke krivulje i Diofantove m-torke

Neka je $\{a, b, c\}$ Diofantova trojka. Tada postoje cijeli brojevi r, s i t takvi da je $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$. Ova trojka inducira eliptičku krivulju

$$E : y^2 = (x + ab)(x + ac)(x + bc). \tag{6.1.1}$$

Zanimaju nas cjelobrojna rješenja x sljedećeg sustava jednadžbi:

$$x + ab = \square, \quad x + ac = \square, \quad x + bc = \square, \tag{6.1.2}$$

gdje simbolom $\square$ označavamo potpune kvadrate (ali nas manje zanimaju konkretne vrijednosti). Jedno rješenje je $x = 1$ te imamo cjelobrojnu točku $S = (1, rst)$ na krivulji E. Theorem 4.2. iz [34] svodi problem traženja rješenja sustava (6.1.2) na traženje dvostrukih točaka na krivulji E.

Teorem 6.1.1. *Za $T = (x_T, y_T) \in E(\mathbb{Q})$ vrijedi da je x_T rješenje sustava (6.1.2) ako i samo ako je $T \in 2E(\mathbb{Q})$.*

Elementarni dokaz može se naći u [34, Theorem 4.2], a algebarski u [14, Proposition 1].

Primijetimo da E ima nekoliko očitih cjelobrojnih točaka:

$$A = (-bc, 0), \quad B = (-ac, 0), \quad C = (-ab, 0), \quad P = (0, abc), \quad S = (1, rst). \tag{6.1.3}$$

Prema Teoremu 6.1.1, za svaku točku $T \in 2E(\mathbb{Q}) \cap \mathbb{Z}^2$ vrijedi da skup $\{a, b, c\}$ ima $D(x_T)$-svojstvo. Budući da smo pretpostavili da je $\{a, b, c\}$ Diofantova trojka (ima $D(1)$-svojstvo), slijedi da je $S \in 2E(\mathbb{Q}) \cap \mathbb{Z}^2$. Zaista, vrijedi da je $S = 2R$, gdje je

$$R = (x_R, y_R) = (rs + rt + st + 1, (r + s)(r + t)(s + t)) \in E(\mathbb{Q}) \cap \mathbb{Z}^2.$$

Točka R je očito cjelobrojna, a leži na krivulji jer je

$$\begin{aligned} y_R^2 &= ((r + s)(r + t)(s + t))^2 \\ &= (r + s)(r + t) \cdot (r + s)(s + t) \cdot (r + t)(s + t) \\ &= (r^2 + rt + rs + st) \cdot (rs + rt + s^2 + st) \cdot (rs + rt + st + t^2) \\ &= (rs + rt + st + ab + 1)(rs + rt + st + ac + 1)(rs + rt + st + bc + 1) \\ &= (x_R + ab)(x_R + bc)(x_R + ca). \end{aligned}$$

Koristeći (2.4.1), računski se provjerava da je $S = 2R$.

6.2 Diofantove trojke s jednim dodatnim $D(n)$-svojstvom

Nove dvostruke cjelobrojne točke možemo pokušati naći kombinirajući poznate cjelobrojne točke (6.1.3). Međutim, vrijedi da je $2A = 2B = 2C = \mathcal{O}$. Stoga nastavljamo raditi samo s P i S. Npr. točka $2P$ ima x-koordinatu $x_{2P} = \lambda^2 - (ab + bc + ca)$, gdje je $\lambda = \dfrac{a + b + c}{2}$, prema (2.4.1). Kako je $2P \in E(\mathbb{Q})$, da bismo provjerili da je $2P \in E(\mathbb{Z})$,

dovoljno je pokazati da je x-koordinata cjelobrojna. Naime, u tom slučaju je y^2 cijeli broj jer je $y^2 = (x+ab)(x+bc)(x+ca)$, a kako je y racionalan, slijedi da je i cijeli. Dakle, točka $2P$ imat će cjelobrojne koordinate ako i samo ako 2 dijeli $a+b+c$. Dokazali smo sljedeću lemu.

Lema 6.2.1. *Neka su a, b i c cijeli brojevi takvi da je $a+b+c$ paran broj. Tada $\{a,b,c\}$ ima $D(n)$-svojstvo za*

$$n = \left(\frac{a+b+c}{2}\right)^2 - (ab+bc+ca).$$

Budući da želimo dodatno $D(n)$-svojstvo za Diofantovu trojku $\{a,b,c\}$, odnosno da n nije 1, provjerimo kad je $n=1$. Jednadžba

$$\left(\frac{a+b+c}{2}\right)^2 - (ab+bc+ca) = 1$$

je kvadratna u c i njeno rješenje je $c = a+b\pm 2\sqrt{ab+1}$. Dobivamo sljedeći korolar.

Korolar 6.2.2. *Neka je $\{a,b,c\}$ Diofantova trojka koja nije regularna (tj. $c \neq a+b\pm 2\sqrt{ab+1}$). Ako je $a+b+c$ paran broj, onda $\{a,b,c\}$ također ima i $D(n)$-svojstvo za neki $n \neq 1$.*

Ovim Korolarom dobivamo beskonačno mnogo Diofantovih trojki koje su i $D(n)$-trojke za $n \neq 1$. To su sve Diofantove trojke koje nisu regularne. Na primjer, Diofantova trojka $\{k-1, k+1, 16k^3-4k\}$ nije regularna ni za koji prirodan k (jer $16k^3-4k \neq 4k$).

6.3 Diofantove trojke s dva dodatna $D(n)$-svojstva

Računalna pretraga za Diofantove trojke $\{a,b,c\}$, odnosno za a, b i c u rasponu od 1 do 10000, pokazuje da odgovarajuće točke $S-2P$ i $4P$ nikad nemaju cjelobrojne koordinate. S druge strane, točka $S+2P$ ima cjelobrojne koordinate za trojke $(4,12,420)$, $(12,24,2380)$, $(24,40,7812)$.

Općenito, točka $S+2P$ na E, prema (2.4.1), ima sljedeću x-koordinatu:

$$-\frac{1}{4}(a+b+c)^2 - 1 + \\ +\frac{1}{4}\left(\frac{8abc + ((a+b+c)^2 - 4ab - 4ac - 4bc)(a+b+c) + 8\sqrt{ab+1}\sqrt{ac+1}\sqrt{bc+1}}{(a+b+c)^2 - 4ab - 4ac - 4bc - 4}\right)^2.$$

Međutim, već iz tri dobivena primjera može se naslutiti kako konstruirati jednu familiju Diofantovih trojki s dva dodatna $D(n)$-svojstva.

Propozicija 6.3.1. *Neka je i prirodan broj te*

$$a = 2(i+1)i, \quad b = 2(i+2)(i+1), \quad c = 4(2i^2+4i+1)(2i+3)(2i+1).$$

Tada $\{a, b, c\}$ *ima* $D(n)$*-svojstvo za* $n = n_1, n_2, n_3$*, gdje su*

$$\begin{aligned}
n_1 &= 1,\\
n_2 &= 32i^4 + 128i^3 + 172i^2 + 88i + 16,\\
n_3 &= 256i^8 + 2048i^7 + 6720i^6 + 11648i^5 + 11456i^4 + 6400i^3 + 1932i^2 + 280i + 16.
\end{aligned}$$

Dokaz. Jednom kad smo naslutili ovakvu konstrukciju, dokazati je možemo potpuno računski. Npr.

$$\begin{aligned}
ab + n_1 &= 4(i+2)(i+1)^2 i + 1 = 4i^4 + 16i^3 + 20i^2 + 8i + 1 = (2i^2 + 4i + 1)^2,\\
ac + n_1 &= 8(i+2)(i+1)(2i^2 + 4i + 1)(2i+3)(2i+1) + 1 = (8i^3 + 28i^2 + 28i + 7)^2,\\
&\vdots\\
ac + n_3 &= 8(i+2)(i+1)(2i^2 + 4i + 1)(2i+3)(2i+1) +\\
&\quad + 256i^8 + 2048i^7 + 6720i^6 + 11648i^5 + 11456i^4 + 6400i^3 + 1932i^2 + 280i + 16\\
&= 4(8i^4 + 32i^3 + 42i^2 + 21i + 4)^2,\\
bc + n_3 &= 8(i+2)(i+1)(2i^2 + 4i + 1)(2i+3)(2i+1) +\\
&\quad + 256i^8 + 2048i^7 + 6720i^6 + 11648i^5 + 11456i^4 + 6400i^3 + 1932i^2 + 280i + 16\\
&= 4(8i^4 + 32i^3 + 42i^2 + 21i + 4)^2.
\end{aligned}$$

Analogno za ostale parove i n-ove. □

Sličnom računalnom potragom nalazimo sljedeće primjere Diofantovih trojki koje imaju tri dodatna $D(n)$-svojstva (uz $D(1)$-svojstvo).

Tablica 6.1
Primjeri $D(n)$-trojki za $n = 1, n_2, n_3, n_4$

$\{a, b, c\}$	n_2, n_3, n_4
$\{4, 12, 420\}$	$436, 3796, 40756$
$\{4, 420, 14280\}$	$14704, 950896, 47995504$
$\{10, 44, 21252\}$	$825841, 6921721, 112338361$
$\{15, 528, 32760\}$	$66609, 5369841, 15984081$
$\{40, 60, 19404\}$	$19504, 3680161, 93158704$

Primijetimo da $\{4, 12, 420\}$ i $\{4, 420, 14280\}$ dijele dva od tri elementa. Unošenje $12, 420, 14280$ u online enciklopediju nizova cijelih brojeva (OEIS, [43]) pronalazi niz koji se može definirati rekurzivno:

$$a_0 = 0, a_1 = 12, a_2 = 420,\ a_{m+3} = 35a_{m+2} - 35a_{m+1} + a_m. \tag{6.3.1}$$

To su zapravo po redu brojevi koji se mogu napisati u dva oblika, $2p(p+1)$ i $q(q+1)$, za prirodne p i q. Iz toga vidimo da je $4a_m+1 = 4q(q+1)+1 = (2q+1)^2$ uvijek kvadrat, a $a_m a_{m+1}+1$ je kvadrat jer je $a_m a_{m+1} = 4t_m(t_m-1)$, gdje su t_m brojevi koji su kvadrati i trokutasti [43]. Dobivamo sljedeću konstrukciju.

Propozicija 6.3.2. *Neka je $a = 4$ i neka su b i c uzastopni članovi niza (6.3.1). Tada je $\{a, b, c\}$ Diofantova trojka s $D(n_i)$-svojstvom za $i = 2, 3$, pri čemu je $1 < n_2 \neq n_3$.*

Dokaz. Prije iskaza ove Propozicije pokazali smo da je $\{a, b, c\}$ Diofantova trojka. Neka je $ab+1 = r^2, ac+1 = s^2, bc+1 = t^2$, te neka je $E : y^2 = (x+ab)(x+bc)(x+ca)$ eliptička krivulja koju proučavamo.

Prema Korolaru 6.2.2, dovoljno je da $2|a+b+c$ kako bi $2P$ bila cjelobrojna i kod nas to vrijedi jer su a, b i c parni. Naime, $a = 4$, a parnost b i c vidi se iz rekurzivne definicije niza (6.3.1). Time smo dobili jedan $n_2 = x_{2P}$ za koji naša Diofantova trojka ima $D(n_2)$-svojstvo.

Preostaje dokazati da postoji n_3 takav da $\{a, b, c\}$ ima $D(n_3)$-svojstvo. Kako je $S = (1, rst)$, izračunajmo $S + 2P$. Tada je

$$\lambda = \frac{rst + (\sum a^3 - \sum a^2 b + 2abc)/8}{1 - (\sum a^2 - 2\sum ab)/4},$$

gdje je $\sum a^3 = a^3+b^3+c^3, \sum a^2 b = a^2b+a^2c+b^2a+b^2c+c^2a+c^2b, \sum a^2 = a^2+b^2+c^2, \sum ab = ab+bc+ca$. Tvrdimo da je x-koordinata točke $S+2P = 2(R+P)$ cjelobrojna, štoviše, jednaka $x_{S+2P} = a+b+c$.

Znamo da je $x = \lambda^2 - \sum ab - (\sum a^2 - 2\sum ab)/4 - 1$, pa je naša tvrdnja ekvivalentna tvrdnji da je

$$\begin{aligned}
&4\lambda^2 = 4\sum ab + \sum a^2 - 2\sum ab + 4 + 4(a+b+c)\\
\iff &4\lambda^2 - 4 = \sum a^2 + 2\sum ab + 4(a+b+c)\\
\iff &4\lambda^2 - 4 = (a+b+c)^2 + 4(a+b+c)\\
\iff &4\lambda^2 - 4 = (a+b+c)(a+b+c+4)\\
\iff &4\lambda^2 - 4 = (a+b+c+2)^2 - 4\\
\iff &\lambda = \pm\frac{a+b+c+2}{2}.
\end{aligned}$$

Dokazat ćemo da je $\lambda = -\frac{a+b+c+2}{2}$. Sad uvrštavamo $a = 4$ u

$$\frac{rst + (\sum a^3 - \sum a^2 b + 2abc)/8}{1 - (\sum a^2 - 2\sum ab)/4} = -\frac{a+b+c+2}{2},$$

izmnožimo to u Mathematici [46] i dobivamo da je gornja jednakost ekvivalentna s

$-2(4+b^2+c^2-10b-10c-18bc-4rst)=0$, tj.

$$4+b^2+c^2-10b-10c-18bc=4\sqrt{(4b+1)(4c+1)(bc+1)}.$$

Lijeva strana veća je od nule jer je $a_{m+1}>32a_m$, tj. $c>32b$, pa kvadriranjem i faktorizacijom dobivamo ekvivalentnu jednakost $(b^2+c^2-12b-12c-34bc)(b^2+c^2-8b-8c-2bc+12)=0$. Sad je dovoljno dokazati

$$b^2+c^2-12b-12c-34bc=0. \tag{6.3.2}$$

Dakle, treba dokazati $a_m^2+a_{m+1}^2-12a_m-12a_{m+1}-34a_ma_{m+1}=0$ za svaki $m\in\mathbb{N}_0$, što ćemo napraviti indukcijom. Ako tvrdnja vrijedi do $m-1$, onda je a_{m-1} jedno rješenje jednadžbe $x^2+a_m^2-12x-12a_m-34a_mx=0$, tj. $x^2-(34a_m+12)x+a_m^2-12a_m=0$, pa je drugo rješenje po Vièteovim formulama $x_2=34a_m+12-a_{m-1}$.

Stoga je dovoljna tvrdnja $a_{m+1}=34a_m-a_{m-1}+12$, koju opet dokazujemo indukcijom (ekvivalentna je s $35a_m-35a_{m-1}+a_{m-2}=34a_m-a_{m-1}+12$, tj. $a_m-34a_{m-1}+a_{m-2}=12$, što je početna tvrdnja za manji indeks, $a_m=34a_{m-1}-a_{m-2}+12$).

Dodajmo još da $n_2\neq n_3$, jer su to x-koordinate točaka $2P$ i $S+2P$, koje nisu jednake, jer bi to povlačilo $S=\mathcal{O}$ ili $S=-4P$, a nijedno od toga ovdje ne vrijedi. □

Napomena. Ovime smo dobili još jednu konstrukciju beskonačne familije Diofantovih trojki s dva dodatna $D(n)$-svojstva. Nismo uspjeli naći beskonačnu familiju Diofantovih trojki s tri dodatna $D(n)$-svojstva. Međutim, ovo nas usmjerava prema općenitijem rezultatu. Da nismo uvrstili $a=4$, jednakost (6.3.2), $b^2+c^2-12b-12c-34bc=0$, izgledala bi kao $b^2+c^2-4b-2ab-4c-2ac-2bc-8abc+a^2-4a=0$. Rješavanjem po c dobivamo $c=2+a+b+4ab\pm2\sqrt{(2a+1)(2b+1)(ab+1)}$. Ako uzmemo predznak $+$, dobivamo uvjet da je $\{2,a,b,c\}$ regularna Diofantova četvorka.

Teorem 6.3.3. *Neka je $\{2,a,b,c\}$ regularna Diofantova četvorka. Tada Diofantova trojka $\{a,b,c\}$ ima i $D(n)$-svojstva za dva različita n koja nisu 1.*

Dokaz. Tvrdimo da $n_2=x_{S+2P}$ i $n_3=x_{2P}$ (na eliptičkoj krivulji induciranoj s $\{a,b,c\}$) imaju željena svojstva. Primijetimo da su a, b i c veći od 2. Bez smanjenja općenitosti, možemo pretpostaviti da je $a<b<c$. Prvo ćemo pokazati da $\{a,b,c\}$ ima $D(n_3)$-svojstvo. Prisjetimo se da je

$$n_3=x_{2P}=\frac{1}{4}(a+b+c)^2-ab-ac-bc. \tag{6.3.3}$$

Budući da je $2a+1$ potpun kvadrat, slijedi da je a paran (inače bi $2a+1$ davalo ostatak 3 pri dijeljenju s 4, što kvadrati ne mogu). Analogno pokazujemo da su b i c parni. Prema [13, Lemma 14] znamo da je $c>4ab$ i stoga $c\neq a+b\pm2\sqrt{ab+1}$ (vidjeti opet [13] ili [32]). Po Korolaru 6.2.2 slijedi da $\{a,b,c\}$ ima $D(n_3)$-svojstvo za $n_3\neq1$.

Sad pokazujemo da $\{a,b,c\}$ također ima i $D(n_2)$-svojstvo. Budući da je $\{2,a,b,c\}$ regularna Diofantova četvorka, slijedi da je $n_2 = a+b+c$.

Naime, direktan račun pokazuje da je uvjet $x_{S+2P} = a+b+c$ ekvivalentan s $q_1q_2q_3 = 0$, gdje su

$$\begin{aligned}
q_1 &= a^2+b^2+c^2-2ab-2ac-2bc-4,\\
q_2 &= a^2+b^2+c^2-2ab-2ac-2bc-4a-4b-4c-8abc,\\
q_3 &= a^4+b^4+c^4-2a^2b^2-2a^2c^2-2b^2c^2+2a^3+2b^3+2c^3-2a^2b-2a^2c-2ab^2-2ac^2\\
&\quad -2bc^2-2b^2c+a^2+b^2+c^2-2ab-2ac-2bc-4abc-4a-4b-4c.
\end{aligned}$$

Uvjet $q_2 = 0$ je kvadratna jednadžba po c. Rješavanjem te jednadžbe, vidimo da je $q_2 = 0$ ekvivalentno s

$$c = 2+a+b+4ab \pm 2\sqrt{(2a+1)(2b+1)(ab+1)}, \tag{6.3.4}$$

a to je upravo pretpostavljeni uvjet da je $\{2,a,b,c\}$ regularna Diofantova četvorka.

Preostaje pokazati da je $n_2 \neq n_3$. Primijetimo da je $n_2 = n_3$ ekvivalentno s $2P = \pm(S+2P)$, tj. $2(R+2P) = \mathcal{O}$. Ovaj uvjet vodi do

$$(r \pm s)(r \pm t) = \frac{1}{4}(c-a-b)^2. \tag{6.3.5}$$

Lijeva strana je manja od $4c\sqrt{ab} < 2c\sqrt{c}$, dok je desna strana veća od $\dfrac{c^2}{16}$, pa za $c \geqslant 1024$ dobivamo kontradikciju. Jedina Diofantova trojka s $c < 1024$ takva da je $\{2,a,b,c\}$ regularna četvorka je $\{4,12,420\}$, za koju smo direktno provjerili da (6.3.5) ne vrijedi. □

Napomena. Druga dva faktora, q_1 i q_2, koja se pojavljuju u dokazu, ne mogu se iskoristiti za dobivanje Diofantovih trojki koje imaju dva dodatna $D(n)$-svojstva. Naime, uvjet $q_1 = 0$ ekvivalentan je s $c = a+b \pm 2\sqrt{ab+1}$. Stoga, ako je $c = a+b \pm 2\sqrt{ab+1}$, onda $\{a,b,c\}$ ima $D(n)$-svojstvo za $n = a+b+c = x_{S+2P}$. Ali, prema Korolaru 6.2.2, takva trojka $\{a,b,c\}$ ima $D(n)$-svojstvo za $n = x_{2P} = 1$, pa time ne dobivamo dodatni $n \neq 1$. Rješenja (a,b,c) od $q_3 = 0$ pak nisu Diofantove trojke. Da bismo to vidjeli, primijetimo da je q_3 simetričan polinom u a,b i c. Označimo elementarne simetrične polinome sa $\sigma_1 = a+b+c, \sigma_2 = ab+bc+ca, \sigma_3 = abc$. Tada je $q_3 = 0$ ekvivalentno sa $\sigma_1^4 + 2\sigma_1^3 + (1-4\sigma_2)\sigma_1^2 + (8\sigma_3 - 8\sigma_2 - 4)\sigma_1 + 8\sigma_3 - 4\sigma_2 = 0$, što se može zapisati kao $(\sigma_1^2 - 4\sigma_2)(\sigma_1+1)^2 + (8\sigma_3 - 4)(\sigma_1+1) + 4 = 0$. Iz toga slijedi da $(\sigma_1+1)|4$, tj. $\sigma_1 + 1 \in \{-4,-2,-1,1,2,4\}$, pa je $\sigma_1 = a+b+c \in \{-5,-3,-2,0,1,3\}$. Ako pretpostavimo da je (a,b,c) Diofantova trojka, onda a,b i c moraju imati isti predznak. Sad lako provjeravamo da $a+b+c \in \{-5,-3,-2,0,1,3\}$ ne daje Diofantove trojke.

6.4 Diofantove trojke s tri dodatna $D(n)$-svojstva

Budući da je prirodnih brojeva beskonačno, za fiksnu trojku $\{a, b, c\}$ nije očito kako provjeriti koliko točno $D(n)$-svojstava ima, stoga ćemo opisati kako to napraviti. Napomenimo da je ovo zapravo već otkriveno u [47], ali nije iskazano ovako općenito (vidjeti Theorem 2.7 i Remark 2.8 u [47]).

Lema 6.4.1. *Za svaku trojku $\{a, b, c\}$ postoji samo konačan broj kandidata za koje ona može imati $D(n)$-svojstvo. Kandidati se mogu odrediti preko djelitelja broja $P = b(c-a)$. Preciznije, za svaki n za koji $\{a, b, c\}$ ima $D(n)$-svojstvo postoji djelitelj d od $P = b(c-a)$ takav da je*

$$n = \frac{1}{4}\left(d + \frac{P}{d}\right)^2 - bc.$$

Dokaz. Pretpostavimo da $\{a, b, c\}$ ima $D(n)$-svojstvo. Neka su r, s i t cijeli brojevi takvi da je

$$ab + n = r^2, \quad ac + n = s^2, \quad bc + n = t^2.$$

Tada je $t^2 - r^2 = bc - ab = b(c-a)$, pa $t - r$ dijeli $b(c-a)$. Iz $d = t - r$ možemo odrediti n. Naime,

$$2t = (t-r) + (t+r) = t - r + \frac{t^2 - r^2}{t-r} = d + \frac{b(c-a)}{d},$$

pa iz $n = t^2 - bc$ vidimo da je n određen s t, pa onda i s d. Stoga, da bismo provjerili koja $D(n)$-svojstva može imati trojka $\{a, b, c\}$, možemo provjeriti sve djelitelje d od $P = b(c-a)$, koji određuju mogući

$$n = t^2 - bc = \frac{1}{4}\left(d + \frac{P}{d}\right)^2 - bc$$

i onda provjeriti je li $ac + n$ potpun kvadrat. Budući da tražimo prirodne n, primijetimo da je izraz u zagradi paran, pa je $bc + n = \frac{1}{4}\left(d + \frac{P}{d}\right)^2$ potpun kvadrat, kao i

$$\begin{aligned} ab + n &= ab + \frac{1}{4}\left(d + \frac{P}{d}\right)^2 - bc \\ &= b(a-c) + \frac{1}{4}\left(d^2 + 2P + \frac{P^2}{d^2}\right) \\ &= -P + \frac{1}{4}\left(d^2 + 2P + \frac{P^2}{d^2}\right) \\ &= \frac{1}{4}\left(d^2 - 2P + \frac{P^2}{d^2}\right) \\ &= \frac{1}{4}\left(d - \frac{P}{d}\right)^2. \end{aligned}$$

Dakle, za svaku trojku $\{a, b, c\}$ postoji samo konačan broj prirodnih n za koje ona može imati $D(n)$-svojstvo i mogući n-ovi određeni su s $n = \frac{1}{4}\left(d + \frac{P}{d}\right)^2 - bc$. □

Računalna pretraga na trojkama iz Propozicije 6.3.1, za $i < 100000$, pokazuje da ne postoji $n \notin \{n_1, n_2, n_3\}$ takav da

$$\{a, b, c\} = \{2(i+1)i, 2(i+2)(i+1), 4(2i^2+4i+1)(2i+3)(2i+1)\}$$

ima $D(n)$-svojstvo, osim za $i = 1$ te $i = 4$. To sugerira da ne postoji beskonačna potfamilija trojki koja ima $D(n)$-svojstvo za ukupno četiri različita prirodna n.

U konstrukciji iz Propozicije 6.3.2 pronašli smo još samo jedan primjer takve Diofantove trojke $\{4, a_m, a_{m+1}\}$ gdje su a_m kao u (6.3.1), za $m = 4$. Još neki primjeri pronađeni su računalnom pretragom. Ne znamo postoji li beskonačno mnogo Diofantovih trojki s tri dodatna $D(n)$-svojstva. Svi zasad pronađeni primjeri prikazani su u Tablici 6.2.

Tablica 6.2
Prošireni primjeri $D(n)$-trojki za $n = 1, n_2, n_3, n_4$

$\{a, b, c\}$	n_2, n_3, n_4
$\{4, 12, 420\}$	$436, 3796, 40756$
$\{4, 420, 14280\}$	$14704, 950896, 47995504$
$\{4, 485112, 16479540\}$	$16964656, 2007609136, 63955397832496$
$\{10, 44, 21252\}$	$825841, 6921721, 112338361$
$\{15, 528, 32760\}$	$66609, 5369841, 15984081$
$\{40, 60, 19404\}$	$19504, 3680161, 93158704$
$\{78, 308, 7304220\}$	$242805865, 4770226465, 13336497750865$

Napomena. Moguće je dati i formalnije argumente u smjeru tvrdnje da familija trojki iz Propozicije 6.3.1 nema beskonačnu potfamiliju trojki koje imaju $D(n)$-svojstvo za četiri različita prirodna n. U svim primjerima koje smo pronašli, pokazuje se da četvrti n dolazi od x-koordinate točke koja nije linearna kombinacija P i S, nego je riječ o točki nezavisnoj od P i S. Međutim, može se pokazati da krivulja:

$$E(\mathbb{Q}(t)): \quad y^2 = (x+ab)(x+ac)(x+bc),$$

gdje je

$$a = 2(t+1)t, \quad b = 2(t+2)(t+1), \quad c = (2t^2+4t+1)(2t+3)(2t+1),$$

ima rang 2 nad $\mathbb{Q}(t)$. Pritom se koristi Gusić–Tadić teorem (Theorem 1.1 iz [26]).

Zaključak

Dosad nije bila poznata uniformna gornja granica na veličinu Diofantove m-torke u Gaussovim cijelim brojevima. U ovoj disertaciji pokazali smo da je $m \leqslant 42$, oslanjajući se na rezultate iz diofantskih aproksimacija. Budući da korišteni rezultati vrijede u općenitijem okruženju, ukazujemo na mogućnost dobivanja gornje granice na veličinu Diofantove m-torke u prstenu cijelih brojeva imaginarnog kvadratnog polja. Također smo dokazali neke tvrdnje koje bi se u Gaussovim cijelim brojevima mogle iskoristiti za poboljšanje dobivene granice, kao i u proučavanju proširenja jednoparametarskih trojki u Gaussovim cijelim brojevima, što smo onda i pokazali na primjeru jedne takve familije.

Uz to, proučavali smo proširenja jedne parametarske familije $D(n)$-parova u racionalnim cijelim brojevima. Elementarno smo pokazali da se svaki takav par može proširiti do $D(n)$-četvorke na najviše jedan način i eksplicitno smo opisali taj jedan način, kao i situaciju u kojoj je moguć.

Na kraju smo se bavili pitanjem koliko različitih $D(n)$-svojstava može imati jedna Diofantova trojka. Koristeći eliptičke krivulje, pokazali smo da postoji beskonačno mnogo Diofantovih trojki $\{a, b, c\}$ koje su ujedno i $D(n)$-skupovi za dva različita prirodna n koja nisu 1.

Bibliografija

[1] N. Adžaga i A. Filipin. "On the extension of $D(-8k^2)$-pair $\{8k^2, 8k^2+1\}$". *Moscow Mathematical Journal* 17.2 (2017), str. 165–174.

[2] N. Adžaga, A. Dujella, D. Kreso i P. Tadić. "Triples which are $D(n)$-sets for several n's". *Journal of Number Theory* 184 (2018), str. 330–341.

[3] A. Baker i H. Davenport. "The equations $3x^2-2=y^2$ and $8x^2-7=z^2$". *Quarterly Journal of Mathematics. Oxford Series* 20.2 (1969), str. 129–137.

[4] A. Baker i G. Wüstholz. "Logarithmic Forms and Group Varieties". *Journal für die reine und angewandte Mathematik* 442 (1993), str. 19–62.

[5] A. Bayad, A. Filipin i A. Togbé. "Extension of a parametric family of Diophantine triples in Gaussian integers". *Acta Mathematica Hungarica* 148.2 (2016), str. 312–327.

[6] A. Bayad, A. Dossavi-Yovo, A. Filipin i A. Togbé. "On the extensibility of $D(4)$-triple $\{k-2, k+2, 4k\}$ over Gaussian integers". *Notes on Number Theory and Discrete Mathematics* 23 (2017), str. 1–26.

[7] Lj. Baćić. "Skupovi u kojima je $xy+4$ potpuni kvadrat i problem proširenja nekih parametarskih Diofantovih trojki". Prirodoslovno–matematički fakultet. 2014.

[8] E. Brown. "Sets in which $xy+k$ is always a square". *Mathematics of Computation* 45 (1985), str. 613–620.

[9] Y. Bugeaud, A. Dujella i M. Mignotte. "On the family of Diophantine triples $\{k-1, k+1, 16k^3-4k\}$". *Glasgow Mathematical Journal* 49 (2007), str. 333–344.

[10] A. Dujella. *Diophantine m-tuples.* URL: https://web.math.pmf.unizg.hr/~duje/dtuples.html.

[11] A. Dujella. *Uvod u teoriju brojeva.* skripta Prirodoslovno-matematičkog fakulteta. URL: https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf.

[12] A. Dujella. "Generalization of a problem of Diophantus". *Acta Arithmetica* 65.1 (1993), str. 15–27.

[13] A. Dujella. "An absolute bound for the size of Diophantine m-tuples". *Journal of Number Theory* 89 (2001), str. 126–150.

[14] A. Dujella. "Diophantine m-tuples and elliptic curves". *Journal de Théorie des Nombres de Bordeaux* 13 (2001), str. 111–124.

[15] A. Dujella. "There are only finitely many Diophantine quintuples". *Journal für die reine und angewandte Mathematik* 566 (2004), str. 183–214.

[16] A. Dujella, M. Kazalicki, M. Mikić i M. Szikszai. "There are Infinitely Many Rational Diophantine Sextuples". *International Mathematics Research Notices* 2017 (2) (2017), str. 490–508.

[17] A. Filipin. "There does not exist a $D(4)$-sextuple". *Journal of Number Theory* 128 (2008), str. 1555–1565.

[18] A. Filipin. *Pellove jednadžbe*. skripta Prirodoslovno-matematičkog fakulteta, 2015.

[19] L. Fjellstedt. "On a class of Diophantine equations of second degree in imaginary quadratic fields". *Arkiv för Matematik* 2.24 (1953), str. 435–461.

[20] Z. Franušić. *Pellova jednadžba*. skripta Prirodoslovno-matematičkog fakulteta. URL: https://web.math.pmf.unizg.hr/nastava/etb/materijali/pellova-web.pdf.

[21] Z. Franušić. "On the extensibility of Diophantine triples $\{k-1, k+1, 4k\}$ for Gaussian integers". *Glasnik matematički* 43.2 (2008), str. 265–291.

[22] Z. Franušić i B. Jadrijević. "Computing relative power integral bases in a family of quartic extensions of imaginary quadratic fields". *Publicationes Mathematicae Debrecen* 92 (2018), str. 293–315.

[23] Y. Fujita i A. Togbé. "The extension of the $D(-k^2)$-pair $\{k^2, k^2+1\}$". *Periodica Mathematica Hungarica* 65.1 (2012), str. 75–81.

[24] P. E. Gibbs. *Diophantine Quintuples over Quadratic Rings*. 2018. URL: https://www.researchgate.net/publication/323176085_Diophantine_Quintuples_over_Quadratic_Rings.

[25] H. Gupta i K. Singh. "On k-triad sequences". *International Journal of Mathematics and Mathematical Sciences* 5 (1985), str. 799–804.

[26] I. Gusić i P. Tadić. "Injectivity of the specialization homomorphism of elliptic curves". *Journal of Number Theory* 148 (2015), str. 137–152.

[27] A. Hammerlindl, J. C. Bowman i T. Prince. *Asymptote: The Vector Graphics Language*. Version 2.41. URL: http://asymptote.sourceforge.net.

[28] B. He, A. Togbé i V. Ziegler. "There is no Diophantine quintuple". *Transactions of the American Mathematical Society* (u objavi).

[29] D. Husemöller. *Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2004. URL: https://books.google.hr/books?id=ncK0XS2ruLcC.

[30] M. J. Jacobson Jr. i H. C. Williams. *Solving the Pell Equation*. Springer–Verlag, New York, 2009.

[31] B. Jadrijević i V. Ziegler. "A system of relative Pellian equations and a related family of relative Thue equations". *International Journal of Number Theory* 2.4 (2006), str. 569–590.

[32] B. W. Jones. "A second variation on a problem of Diophantus and Davenport". *Fibonacci Quarterly* 16 (1978), str. 155–165.

[33] A. Kihel i O. Kihel. "On the intersection and the extendibility of P_t sets". *Far East Journal of Mathematical Sciences* 3 (2001), str. 637–643.

[34] A. Knapp. *Elliptic Curves*. Princeton University Press, 1992.

[35] S. P. Mohanty i A. M. S. Ramasamy. "On $P_{r,k}$ sequences". *The Fibonacci Quarterly* 23.1 (1985), str. 36–44.

[36] L. J. Mordell. "On the rational solutions of the indeterminate equations of the third and fourth degrees". *Proceedings of the Cambridge Philosophical Society* 21 (1922), str. 179–192.

[37] T. Nagell. *Introduction to number theory*. John Wiley & Sons, 1951.

[38] F. Najman. *Eliptičke krivulje nad poljima algebarskih brojeva*. skripta Prirodoslovno-matematičkog fakulteta, 2013.

[39] H. Poincaré. "Second complément à l'Analysis Situs". *Proceedings of the London Mathematical Society* 32 (1900), 277–308.

[40] C. L. Siegel. "Uber einige Anwendungen diophantischer Approximationen". *On some applications of Diophantine approximations: a translation of Carl Ludwig Siegel's Über einige Anwendungen diophantischer Approximationen by Clemens Fuchs, with a commentary and the article Integral points on curves: Siegel's theorem after Siegel's proof by Clemens Fuchs and Umberto Zannie*. Ur. U. Zannier. Pisa: Edizioni della Normale, 2014, str. 81–138.

[41] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer–Verlag, New York, 2009.

[42] J. H. Silverman i J. T. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer New York, 1994. URL: https://books.google.hr/books?id=mAJei2-JcE4C.

[43] N. J. A. Sloane. *The On-Line Encyclopedia of Integer Sequences*. URL: http://oeis.org.

[44] N. P. Smart. *The algorithmic resolution of Diophantine equations*. London Mathematical Society, Cambridge University Press, 1998.

[45] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 6.0)*. `http://www.sagemath.org`. 2013.

[46] Research Inc. Wolfram. *Mathematica*. Version 9.0, Champaign, Illinois, SAD. 2012.

[47] Y. Zhang i G. Grossman. "On Diophantine triples and quadruples". *Notes on Number Theory and Discrete Mathematics* 21 (2015), str. 6–16.

Životopis

Nikola Adžaga rođen je 4. svibnja 1988. u Zagrebu. Godine 2007. upisao se na studij matematike Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu (gdje je završio preddiplomski studij 2010.), te 2008. na studij psihologije na Filozofskom fakultetu istog sveučilišta (završio preddiplomski 2011.). Diplomirao je summa cum laude 2012. s temom "Paralelizacija gramatičke evolucije".

Tokom studija, vodio je udrugu Mladi nadareni matematičari "Marin Getaldić", u sklopu koje je i organizirao Ljetni kamp mladih matematičara za učenike srednjih škola i završnih razreda osnovne škole 2011. i 2012. godine.

Nakon diplome, radio je kao programer mobilnih aplikacija u Nanobitu d.o.o., do svibnja 2013., kad je počeo raditi kao asistent na Građevinskom fakultetu Sveučilišta u Zagrebu. Doktorski studij matematike na Prirodoslovno-matematičkom fakultetu Sveučilišta u Zagrebu upisuje u studenom 2013. godine. Sudjeluje u radu *Seminara za teoriju brojeva i algebru*. Od 2013. sudjeluje i u radu Državnog povjerenstva za provedbu natjecanja iz matematike i pripremanju učenika za međunarodna natjecanja.

Objavio je tri znanstvena rada, od kojih možemo istaknuti "On the extension of $D(-8k^2)$-pair $\{8k^2, 8k^2+1\}$" u Moscow Mathematical Journal 17 (2017), br. 2; 165-174 (skupa s profesorom A. Filipinom). Dva puta je izlagao na međunarodnim konferencijama, te je sudjelovao u nekoliko domaćih i međunarodnih konferencija, te jednoj istraživačkoj školi. Sudjelovao je na tri radionice za doktorande Sveučilišta u Zagrebu, koje je vodio Armando Rodriguez Chapin.

Suradnik je na projektu Hrvatske zaklade za znanost (koji vodi akademik A. Dujella) gdje se bavi Diofantovim m-torkama. Također, surađivao je na bilateralnom hrvatsko-austrijskom projektu (koji je vodio profesor A. Filipin).

Popis objavljenih radova

1. Adžaga, Nikola. *Automated conjecturing of Frobenius numbers via grammatical evolution*, Experimental Mathematics 26 (2017), no. 2; str. 247–252.

2. Adžaga, Nikola; Filipin, Alan. *On the extension of $D(-8k^2)$-pair $\{8k^2, 8k^2+1\}$* Moscow Mathematical Journal 17 (2017), no. 2; str. 165–174.

3. Adžaga, Nikola; Dujella, Andrej; Kreso, Dijana; Tadić, Petra. *Triples which are $D(n)$-sets for several n's*, Journal of Number Theory 184 (2018), str. 330–341.

Izjava o izvornosti rada

Ja, Nikola Adžaga (JMBAG 1191212585), student Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu, s prebivalištem na adresi Ivana Pergošića 6, Zagreb, ovim putem izjavljujem pod materijalnom i kaznenom odgovornošću da je moj doktorski rad pod naslovom

Diofantove m-torke u prstenima cijelih brojeva
(Diophantine m-tuples in the rings of integers)

isključivo moje autorsko djelo, koje je u potpunosti samostalno napisano, uz naznaku izvora drugih autora i dokumenata korištenih u radu.

U Zagrebu, 8. svibnja 2018.

potpis