Diofantove četvorke sa svojstvom D(n)

Barović, Stela

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Stela Barović

DIOFANTOVE ČETVORKE SA SVOJSTVOM $D(N)$

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Zrinka Franušić

Zagreb, 2020.

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

1. ____________________________, predsjednik
2. ____________________________, član
3. ____________________________, član

Povjerenstvo je rad ocijenilo ocjenom ________________.

Potpisi članova povjerenstva:

1. ____________________________
2. ____________________________
3. ____________________________

Hvala dragom Bogu na talentima koje mi je darovao, nadi koju mi ulijeva i radosti koja je uvijek prisutna. Hvala i svetom Ivanu Boscu za otkrivanje profesorskog poziva te svetom Josipu Kupertinskom koji je pomogao kad ja više nisam mogla.
Hvala mojim roditeljima na svakoj žrtvi koju su učinili da bi mi ovo omogućili i cijeloj mojoj obitelji na ljubavi, podršci i iskazanom povjerenju.
Hvala svim mojim prijateljima koji su uvijek bili tu za mene i činili ljepšim svaki trenutak mojih studentskih dana.
Veliko hvala i mojoj mentorici, izv. prof. dr. sc. Zrinki Franušić na uloženom trudu i vremenu te na svim savjetima i ohrabrenjima tijekom pisanja ovog diplomskog rada kao i svim ostalim profesorima koji su mi prenijeli potrebno znanje.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

Neka je $n \in \mathbb{Z}$. Za skup cijelih brojeva $\{a_1, a_2, a_3, a_4\}$ kažemo da ima *Diofantovo svojstvo* $D(n)$ ako je umnožak bilo koja dva elementa tog skupa, uvećan za n, jednak potpunom kvadratu nekog cijelog broja. Ako su svi elementi navedenog skupa različiti od nule (i međusobno različiti) onda ga nazivamo *Diofantovom četvorkom sa svojstvom* $D(n)$ ili kraće $D(n)$*-četvorkom*. Diofantova četvorka sa svojstvom $D(1)$ naziva se *Diofantova četvorka*.

Skupovi s navedenim svojstvom dobili su ime u čast grčkog matematičara Diofanta Aleksandrijskog iz 3. stoljeća koji ih je prvi proučavao. O Diofantovom životu ne zna se mnogo, ali ga se smatra najznačajnijim matematičarom postklasičnog razdoblja grčke matematike i posljednjim velikim europskim matematičarom prije Fibonaccija. Iz originalnog Diofantovog rješenja koje je bilo racionalno, možemo dobiti cjelobrojnu Diofantovu četvorku $\{1, 33, 68, 105\}$ koja ima svojstvo $D(256)$.

U prstenu cijelih brojeva postoji beskonačno mnogo Diofantovih četvorki. Naime, ako je $\{a, b\} \subset \mathbb{N}$ Diofantov par, tj. skup za kojeg vrijedi $ab + 1 = r^2$ za neki $r \in \mathbb{N}$, onda je

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

Diofantova četvorka. Kažemo da smo Diofantov par $\{a, b\}$ *proširili* do Diofantove četvorke. Zbog toga je odmah jasno da postoji beskonačno mnogo Diofantovih četvorki. No, zanimljivo je da ne postoji Diofantova petorka. Ta je tvrdnja pokazana tek nedavno u [7] premda se dugi niz godina slutilo da vrijedi.

U ovom radu bavimo se problemom karakterizacije cijelog broja n za kojeg postoji Diofantova četvorka sa svojstvom $D(n)$. Pokazujemo da ako n pri dijeljenju s 4 daje ostatak 2, tj. $n \equiv 2 \pmod 4$, onda $D(n)$-četvorka ne postoji. U suprotnom, ako $n \not\equiv 2 \pmod 4$, onda $D(n)$-četvorka postoji, osim za konačno mnogo vrijednosti broja n. Ta se tvrdnja dokazuje korištenjem tzv. polinomijalnih formula koje služe za konstrukciju Diofantovih četvorki. Uočimo da se cijeli broj n može prikazati kao razlika kvadrata ako i samo ako n pri dijeljenju s 4 ne daje ostatak 2. Stoga možemo zaključiti da $D(n)$ - četvorka postoji ako i samo ako se n može prikazati kao razlika kvadrata dva cijela broja, do na konačno mnogo izuzetaka $S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$. Zanimljivo je da još nije poznato postoji li $D(n)$-četvorka za $n \in S$, no sluti se da ne postoji.

Na kraju se bavimo $D(n)$-četvorkama pri čemu je n jednak potpunom kvadratu, tj. $n = l^2$ za neki $l \in \mathbb{Z}$. Jednostavno se može pokazati da postoji beskonačno mnogo Diofantovih četvorki sa svojstvom $D(l^2)$ no ovdje se bavimo proširenjem $D(l^2)$-para do $D(l^2)$-četvorke. Ta konstrukcija uključuje rješavanje odgovarajuće jednadžbe pellovskog tipa a pomoću moguće je doći do zanimljivih formula koje uključuju Fibonaccijeve i Lucasove brojeve.

Poglavlje 1

Polinomijalne formule

1.1 Diofantovi skupovi

Grčki matematičar Diofant Aleksandrijski iz 3. stoljeća bavio se sljedećim problemom: *Postoje li četiri broja takva da je umnožak bilo koja dva od njih, uvećan za jedan, jednak potpunom kvadratu nekog broja.* Sam je pronašao je jedno rješenje u polju racionalnih brojeva. Skup

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\} \tag{1.1}$$

ima traženo svojstvo. Zaista, vrijedi

$$\begin{aligned} &\frac{1}{16}\cdot\frac{33}{16}+1=\left(\frac{17}{16}\right)^2,\ \frac{1}{16}\cdot\frac{17}{4}+1=\left(\frac{9}{8}\right)^2,\ \frac{1}{16}\cdot\frac{105}{16}+1=\left(\frac{19}{16}\right)^2,\\ &\frac{33}{16}\cdot\frac{17}{4}+1=\left(\frac{25}{8}\right)^2,\ \frac{33}{16}\cdot\frac{105}{16}+1=\left(\frac{61}{16}\right)^2,\ \frac{17}{4}\cdot\frac{105}{16}+1=\left(\frac{43}{8}\right)^2. \end{aligned} \tag{1.2}$$

Puno godina kasnije, krajem 17. stoljeća, francuski matematičar Pierre de Fermat pronašao je rješenje u skupu prirodnih brojeva:

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

Lako možemo provjeriti da je zadovoljeno svih šest uvjeta:

$$1\cdot3+1=2^2, 1\cdot8+1=3^2, 1\cdot120+1=11^2, 3\cdot8+1=5^2, 3\cdot120+1=19^2, 8\cdot120+1=31^2.$$

Skup $\{1, 3, 8, 120\}$ se često naziva *Fermatova četvorka*.

Na temelju ovih primjera smisleno je definirati takve skupove. Nazvani su u čast Diofanta za kojeg se smatra da ih je prvi proučavao.

Definicija 1.1.1. *Neka je $m \in \mathbb{N}$, $m > 1$. Skup prirodnih brojeva $\{a_1, a_2, \ldots, a_m\}$ sa svojstvom da je umnožak bilo koja dva od njih, uvećan za jedan, jednak potpunom kvadratu nekog prirodnog broja, odnosno*

$$a_i a_j + 1 = n_{ij}^2, \ 1 \leq i < j \leq m, \tag{1.3}$$

*za $n_{ij} \in \mathbb{N}$, naziva se **Diofantova m-torka**.*

Vrlo često relacije kao u (1.3) ćemo kraće zapisivati kao

$$a_i a_j + 1 = \square.$$

Napomenimo da često govorimo o Diofantovim m-torkama u prstenu cijelih brojeva pri čemu ne dozvoljavamo da element tih skupova bude 0. Nadalje, jasno je da ne postoji Diofantova m-torka za $m > 2$ koja se sastoji od elemenata mješovitih predznaka jer je $a_i a_j + 1 < 0$ osim u slučaju $\{a_i, a_j\} = \{-1, 1\}$. Zbog svega navedenog Diofantove m-torke izučavamo samo u skupu prirodnih brojeva.

Jedno od glavnih pitanja koje se prirodno nameće jest koliko veliki takvi skupovi mogu biti, tj. koji je najveći m za kojeg postoji Diofantova m-torka. Iz primjera Fermatove četvorke, možemo zaključiti da je $m \geq 4$. Dugi niz godina slutilo se da ne postoji Diofantova petorka. Tek nedavno grupa autora (He, Togbé, Ziegler) uspjela je pokazati da je slutnja istinita ([7]).

Problem koji je usko povezan s problemom veličine Diofantovih skupova jest problem nadopunjavanja neke dane Diofantove m-torke s bar još jednim elementom. Švicarski matematičar Leonhard Euler zaključio je da se svaki Diofantov par $\{a, b\}$, znači skup za kojeg je

$$ab + 1 = r^2 \tag{1.4}$$

za neki $r \in \mathbb{N}$, može nadopuniti do trojke pomoću elemenata $c_+ = a+b+2r$ ili $c_- = a+b-2r$ uz uvjet $c_- \neq 0$. Naime, vrijedi

$$ac_\pm + 1 = a^2 + ab \pm 2ar + 1 = a^2 + r^2 - 1 \pm 2ar + 1 = (a \pm r)^2,$$

te analogno $bc_\pm + 1 = (b \pm r)^2$. Nadalje, svaka Diofantova trojka $\{a, b, c\}$ se može nadopuniti elementima

$$d_\pm = a + b + c + 2abc \pm 2rst,$$

pri čemu je

$$ab + 1 = r^2, \ ac + 1 = s^2, \ bc + 1 = t^2, \tag{1.5}$$

za $r, s, t \in \mathbb{N}$. Pokažimo da je $ad_{\pm} + 1 = \square$. Vrijedi

$$\begin{aligned} ad_{\pm} + 1 &= a^2 + ab + ac + 2a^2bc \pm 2arst + 1 \\ &= a^2 + ab + ac + a^2bc + a^2bc \pm 2arst + 1 \\ &= a^2bc + ab + ac + 1 + a^2bc + a^2 \pm 2arst \\ &= (ab + 1)(ac + 1) + a^2(bc + 1) \pm 2arst \\ &= r^2s^2 + a^2t^2 \pm 2arst \\ &= (rs \pm at)^2, \end{aligned}$$

pri čemu smo koristili (1.5). Analogno se pokazuje da vrijedi

$$bd_{\pm} + 1 = (rt \pm bs)^2, \ cd_{\pm} + 1 = (st \pm cr)^2.$$

Stoga, ako trojku $\{a, b, a + b + 2r\}$ proširimo do četvorke pomoću d_+, dobit ćemo parametarsku Diofantovu četvorku

$$\{a, b, a + b + 2r, 4r(a + r)(b + r)\}. \tag{1.6}$$

Zaista,

$$\begin{aligned} d_+ &= 2(a + b + r) + 2ab(a + b + 2r) + 2r(a + r)(b + r) \\ &= 2(a + b + r) + 2(r^2 - 1)(a + b + 2r) + 2r(a + r)(b + r) \\ &= 2r(-1 + ar + br + 2r^2) + 2r(a + r)(b + r) \\ &= 2r(ab + ar + br + r^2) + 2r(a + r)(b + r) = 4r(a + r)(b + r). \end{aligned}$$

Budući da postoji beskonačno mnogo parova međusobno različitih prirodnih brojeva za koje vrijedi (1.4), iz Korolara 1.1.7 možemo zaključiti da postoji beskonačno mnogo Diofantovih četvorki. U ovom radu bavit ćemo se poopćenjem Diofantovih m-torki, odnosno Diofantovih četvorki, tako što u relacijama (1.3) zamijenimo broj 1 s nekim cijelim brojem n.

Definicija 1.1.2. *Neka je n cijeli broj. Kažemo da skup cijelih brojeva $\{a_1, a_2, \dots, a_m\}$ ima **Diofantovo svojstvo** $D(n)$, ako je umnožak bilo koja dva elementa tog skupa, uvećan za n, potpun kvadrat nekog broja, tj. ako vrijedi*

$$a_ia_j + n = n_{ij}^2, \ 1 \le i < j \le m \tag{1.7}$$

*za $n_{ij} \in \mathbb{Z}$. Ako su svi elementi tog skupa različiti od nule, $a_i \neq 0$, $i = 1, \dots, m$, onda se taj skup naziva **Diofantova m-torka sa svojstvom** $D(n)$ ili kraće $D(n)$-**m-torka**.*

Napomena 1.1.3. *Diofantove m-torke iz definicija 1.1.1 i 1.1.2 tradicionalno označavamo kao skupove* $\{a_1, a_2, \ldots, a_m\}$*, a ne kao uređene m-torke* $(a_1, a_2, \ldots, a_m)$ *te nam stoga ne treba pretpostavka da su svi elementi međusobno različiti iako je to često bitno za istaknuti posebno u kontekstu različitih parametarski familija koje opisuju te skupove.*

Napomena 1.1.4. *Definicija 1.1.2 je poopćenje Definicije 1.1.1. Naime,* Diofantova m-torka sa svojstvom $D(1)$ *je upravo "samo"* Diofantova m-torka.

Uočimo da je $\{1, 33, 68, 105\}$ Diofantova četvorka sa svojstvom $D(256)$ koju smo dobili iz racionalne Diofantove četvorke (1.1). Lako se može uočiti da ćemo množenjem svih jednakosti u (1.2) s 256 upravo zadovoljiti sve uvjete u (1.7) (za $n = 256$). Ovo se svojstvo lako može poopćiti što ćemo iskazati sljedećom jednostavnom ali vrlo korisnim propozicijom.

Propozicija 1.1.5. *Neka je* $\{a_1, a_2, \ldots, a_m\}$ *Diofantova m-torka sa svojstvom* $D(n)$*. Tada je za svaki* $w \in \mathbb{Z}$*,* $w \neq 0$*,*

$$\{a_1 w, a_2 w, \ldots, a_m w\}$$

Diofantova m-torka sa svojstvom $D(nw^2)$*.*

Dokaz. Množenjem relacija u (1.7) s w^2 dobivamo

$$(a_i w)(a_j w) + nw^2 = (n_{ij} w)^2, \ 1 \leq i < j \leq m,$$

iz čega direktno slijedi tvrdnja propozicije. □

Napomena 1.1.6. *Propozicija 1.1.5 se može primijeniti i na racionalnim Diofantovim m-torkama sa svojstvom* $D(n)$ *kao što smo vidjeli na primjeru racionalne Diofantove četvorke* (1.1)*. U tom slučaju, jer nas zanimaju samo cjelobrojni skupovi, samo trebamo provjeriti je li skup* $\{a_1 w, a_2 w, \ldots, a_m w\} \subset \mathbb{Z}$*, a ako* $n \notin \mathbb{Z}$*, onda treba provjeriti i je li* $nw^2 \in \mathbb{Z}$*.*

Želimo opisati skup svih cijelih brojeva n za koje postoji Diofantova četvorka sa svojstvom $D(n)$. Važnu ulogu u rješavanju tog problema igraju parametarske, odnosno polinomijalne formule za $D(n)$-četvorke. Opisat ćemo njihovu konstrukciju u sljedećem odjeljku. No, najprije istaknimo jednu očitu posljedicu Propozicije 1.1.5 koju primjenjujemo na činjenicu da postoji beskonačno mnogo Diofantovih četvorki, tj. $D(1)$-četvorki.

Korolar 1.1.7. *Za svaki* $l \in \mathbb{Z}$*,* $l \neq 0$*, postoji beskonačno mnogo Diofantovih četvorki sa svojstvom* $D(l^2)$*.*

1.2 Izvodi nekih polinomijalnih formula za $D(n)$-četvorke

Budući da će elementi naših Diofantovih skupova, tj. $D(n)$-m-torki biti polinomi u jednoj ili više varijabli s cjelobrojnim (a ponekad i s racionalnim) koeficijentima nadopunit ćemo Definiciju 1.1.2 sljedećim dogovorom. reći ćemo da skup polinoma ima svojstvo $D(P)$ ako je umnožak bilo koja dva njegova elementa uvećan za P jednak kvadratu nekog polinoma s cjelobrojnim (ili racionalnim) koeficijentima.

Ideju za konstrukciju polinomijalnih Diofantovih skupova možemo potražiti u sljedećem skupu polinoma:

$$\{x, x+2, 4x+4, 9x+6\}.$$

Provjerom uvjeta (1.7) za $n = 1$ dobivamo

$$x(x+2)+1 = (x+1)^2, x(4x+4)+1 = (2x+1)^2, x(9x+6)+1 = (3x+1)^2,$$

$$(x+2)(4x+4)+1 = (2x+3)^2, \underline{(x+2)(9x+6)+1 = 13+24x+9x^2}, (4x+4)(9x+6)+1 = (6x+5)^2,$$

iz čega možemo zaključiti da je navedeni skup polinoma *skoro* Diofantova četvorka. Za to nedostaje "podcrtani uvjet", tj. uvjet da je umnožak drugog i četvrtog elementa uvećan za jedan daje kvadrat nekog linearnog polinoma. Dakle, ako postoji racionalni broj x koji zadovoljava jednadžbu

$$(x+2)(9x+6)+1 = y^2,$$

onda je dani skup (racionalna) Diofantova četvorka. Pokazuje se da je jedno rješenje $x = \frac{1}{16}$ i ono upravo odgovara skupu (1.1) kojeg je pronašao sam Diofant.

Neka je $\{a, b\}$ proizvoljan skup sa svojstvom $D(n)$ za neki cijeli broj n. Tada po definiciji postoji $x \in \mathbb{Z}$ takav da vrijedi

$$ab + n = x^2. \tag{1.8}$$

Skup $\{a, b\}$ možemo proširiti do skupa $\{a, b, a+b+2x\}$. Uvjerimo se da novonastali skup također ima svojstvo $D(n)$:

$$a(a+b+2x)+n = a^2+ab+2ax+n = a^2+2ax+x^2 = (a+x)^2, \tag{1.9}$$

te analogno

$$b(a+b+2x)+n = (b+x)^2. \tag{1.10}$$

Kako bismo došli do četveročlanog skupa, primijenit ćemo istu konstrukciju na skup $\{b, a+b+2x\}$, tj. dodat ćemo mu element $b+(a+b+2x)+2(b+x) = a+4b+4x$. Stoga trojka $\{b, a+b+2x, a+4b+4x\}$ ima svojstvo $D(n)$. Analogno kao u (1.9) i (1.10) vrijedi

$$b(a+4b+4x)+n = (b+(b+x))^2 = (2b+x)^2, \tag{1.11}$$

$$(a+b+2x)(a+4b+4x)+n=(a+b+2x+(b+x))^2=(a+2b+3x)^2, \tag{1.12}$$

pri čemu pretpostavljamo da vrijedi (1.8).

Promotrimo sada skup

$$\{a,b,a+b+2x,a+4b+4x\}. \tag{1.13}$$

Lako možemo uočiti je (1.13) skoro skup sa svojstvom $D(n)$. Od 6 uvjeta koje bi trebao zadovoljiti, on zadovoljava njih 5, (1.8)-(1.12). Stoga zaključujemo da je (1.13) skup sa svojstvom $D(n)$ ako i samo ako je je umnožak prvog i četvrtog član uvećan za n potpun kvadrat, tj. ako i samo ako vrijedi sljedeće:

$$a(a+4b+4x)+n=y^2, \tag{1.14}$$

za neke $x,y\in\mathbb{Z}$. Raspišimo prethodnu jednadžbu i primijenimo (1.8):

$$\begin{aligned} a^2+4ab+4ax+n&=y^2,\\ a^2+4(x^2-n)+4ax+n&=y^2,\\ a^2+4ax+4x^2-3n&=y^2. \end{aligned}$$

Iz čega dobivamo:

$$\begin{aligned} 3n&=a^2+4x^2+4ax-y^2\\ &=(a+2x)^2-y^2\\ &=(a+2x-y)(a+2x+y). \end{aligned}$$

Riješit ćemo jednadžbu (1.14) tako da ćemo pretpostaviti neke od mogućih faktorizacija broja $3n$ te tako dobiti linearne sustave u x i y. Problem dalje rješavamo uz pretpostavku da vrijedi jedan od sljedeća dva slučaja:

1.
$$\begin{aligned} a+2x-y&=3,\\ a+2x+y&=n. \end{aligned} \tag{1.15}$$

2.
$$\begin{aligned} a+2x-y&=1,\\ a+2x+y&=3n. \end{aligned} \tag{1.16}$$

SLUČAJ 1. Rješavanjem sustava (1.15) dobivamo rješenje

$$(x,y)=\left(\frac{1}{4}(n-2a+3),\frac{1}{2}(n-3)\right). \tag{1.17}$$

Komponente rješenja (1.17) moraju biti cjelobrojne pa stoga dobivamo uvjete

$$n - 2a + 3 \equiv 0 \pmod 4, \; n - 3 \equiv 0 \pmod 2.$$

Drugi uvjet nam daje da n mora biti neparan, tj. $n = 2l + 1$ za neki $l \in \mathbb{Z}$. Uvrštavanjem u prvi uvjet dobivamo

$$\begin{aligned} 2l - 2a + 4 &\equiv 0 \pmod 4, \\ 2l &\equiv 2a \pmod 4, \\ l &\equiv a \pmod 2. \end{aligned}$$

Stoga je $l = a + 2k$, za neki $k \in \mathbb{Z}$, te

$$n = 2(a + 2k) + 1. \tag{1.18}$$

Prema (1.17) dobivamo da je

$$x = \frac{1}{4}(n - 2a + 3) = \frac{1}{4}(2(a + 2k) + 1 - 2a + 3) = k + 1,$$

pa skup (1.13) postaje

$$\{a, b, a + b + 2(k + 1), a + 4b + 4(k + 1)\} \tag{1.19}$$

te ima svojstvo $D(2(a+2k)+1)$ uz uvjet (1.8). Taj uvjet koristimo da bi eliminirali parametar b, odnosno

$$\begin{aligned} b = \frac{x^2 - n}{a} &= \frac{(k + 1)^2 - (2(a + 2k) + 1)}{a}, \\ &= \frac{k^2 - 2k - 2a}{a} = \frac{k^2 - 2k}{a} - 2. \end{aligned}$$

Posljednje što moramo ispuniti jest da je parametar b cjelobrojan, tj.

$$k^2 - 2k = k(k - 2) \equiv 0 \pmod a.$$

Vidimo da će b biti cijeli broj ako je k jednog od oblika

$$k = ak', \tag{1.20}$$

$$k = ak' + 2, \tag{1.21}$$

za $k' \in \mathbb{Z}$. S obzirom na to da k može poprimiti jedan od dva prethodna oblika razmatramo zasebno dva podslučaja.

1.A) Uz pretpostavku (1.20) dobivamo da je

$$b = \frac{ak'(ak'-2)}{a} - 2 = k'(ak'-2) - 2,$$

$$n = 2(a + 2ak') + 1 = 2a(2k'+1) + 1,$$

te uvrštavanjem u (1.19) dobivamo skup

$$\{a, k'(ak'-2) - 2, a + k'(ak'-2) - 2 + 2(ak'+1), a + 4(k'(ak'-2) - 2) + 4(ak'+1)\},$$

odnosno

$$\{a, ak'^2 - 2k' - 2, a(k'+1)^2 - 2k', a(2k'+1)^2 - 4(2k'+1)\}$$

sa svojstvom $D(2a(2k'+1)+1)$, za svaki $a, k' \in \mathbb{Z}$.

1.B) Uz pretpostavku (1.21) dobivamo da je

$$b = \frac{(ak'+2)(ak')}{a} - 2 = k'(ak'+2) - 2,$$

$$n = 2(a + 2(ak'+2)) + 1 = 2a(2k'+1) + 9,$$

te prema (1.19) dobivamo da skup

$$\{a, ak'^2 + 2k' - 2+, a(k'+1)^2 + 2(k'+2), a(2k'+1)^2 + 4(2k'+1)\}$$

ima svojstvo $D(2a(2k'+1)+9)$ za $a, k' \in \mathbb{Z}$.

<u>**SLUČAJ 2.**</u> Rješavanjem sustava (1.16) dobivamo rješenje

$$(x, y) = \left(\frac{1}{4}(3n - 2a + 1), \frac{1}{2}(3n - 1)\right). \tag{1.22}$$

Uvjet da je y cjelobrojan ekvivalentan je $3n - 1 \equiv 0 \pmod 2$, tj. $n = 2l + 1$, $l \in \mathbb{Z}$. Uvjet da je x cjelobrojan dobit ćemo za one $l \in \mathbb{Z}$ za koje je

$$\begin{aligned} 3(2l+1) &\equiv 2a - 1 \pmod 4 \\ 6l &\equiv 2a \pmod 4 \\ l &\equiv a \pmod 2 \end{aligned}$$

pa je stoga n istog oblika kao u (1.18), odnosno $n = 2(a + 2k) + 1$ za neki $k \in \mathbb{Z}$.

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

pa prema (1.13) dobivamo skup

$$\{a, b, 2 + 3a + b + 6k, 4 + 5a + 4b + 12k\} \tag{1.23}$$

sa svojstvom $D(2(a + 2k) + 1)$ uz pretpostavku (1.8). Analogno kao i u prvom slučaju, iz (1.8) eliminiramo parametar b:

$$\begin{aligned} b &= \frac{x^2 - n}{a} \\ &= \frac{a^2 + 2k + 6ak + 9k^2}{a}. \end{aligned}$$

Da bi parametar b bio cjelobrojan, mora vrijediti

$$9k^2 + 2k = k(9k + 2) \equiv 0 \pmod a$$

Dakle, k mora biti oblika

$$k = ak' \tag{1.24}$$

ili

$$k = \frac{1}{9}ak' - \frac{2}{9}, \tag{1.25}$$

za neki $k \in \mathbb{Z}$.

2.A) Ako pretpostavimo da vrijedi (1.24) imamo

$$\begin{aligned} b &= 9ak'^2 + 6ak' + 2k' + a, \\ n &= 2a(2k' + 1) + 1, \end{aligned}$$

pa je skup (1.23) oblika

$$\{a, a(1 + 3k')^2 + 2k', a(2 + 3k')^2 + 2(1 + k'), 9a(1 + 2k')^2 + 4(1 + 2k')\}$$

skup sa svojstvom $D(2a(2k' + 1) + 1)$.

2.B) Pretpostavimo li (1.25), dobivamo

$$b = \frac{1}{9}(a(3 + k')^2 - 2(6 + k')), \tag{1.26}$$

$$n = \frac{1}{9}(2a(2k' + 9) + 1), \tag{1.27}$$

pa dobivamo da je skup (1.19) oblika

$$\left\{a, \frac{1}{9}(a(3 + k')^2 - 2(6 + k')), \frac{1}{9}(a(6 + k')^2 - 2(3 + k')), \frac{1}{9}(a(9 + 2k')^2 - 4(9 + 2k'))\right\} \tag{1.28}$$

sa svojstvom $D\left(\frac{1}{9}(2a(2k'+9)+1)\right)$, za neke $a,k' \in \mathbb{Z}$. Problem koji sada imamo jest da za proizvoljne $a,k' \in \mathbb{Z}$, broj $n = \frac{1}{9}(2a(2k'+9)+1)$ te elementi skupa (1.28) ne moraju biti cjelobrojni. Na primjer, za $a = 1$ i $k' = 1$ pomoću formule (1.28) dobivamo skup $\left\{1, \frac{2}{9}, \frac{41}{9}, \frac{77}{9}\right\}$ koji predstavlja racionalnu $D\left(\frac{23}{9}\right)$-četvorku. Za $a = 1$ i $k' = 11$ dobivamo cjelobrojnu $D(7)$-četvorku $\{1, 18, 29, 93\}$. Stoga ćemo pokušati odrediti neke klase brojeva a i k' za koje su n i b cijeli brojevi (a tada će i elementi skupa (1.28) biti cjelobrojni). Lako se vidi da je n dan formulom (1.27) cjelobrojan ako i samo ako je

$$4ak' + 1 \equiv 0 \pmod 9,$$

odnosno

$$ak' \equiv 2 \pmod 9. \tag{1.29}$$

Uvjerimo se da je tada i $b \in \mathbb{Z}$. Zaista,

$$a(k'+3)^2-2(k'+6) = ak'^2+6ak'+9a-2k'-12 \equiv 2k'+12+9a-2k'-12 \equiv 0 \pmod 9.$$

Još nam preostaje odrediti cijele brojeve a i k' takve da vrijedi (1.29). Razlikujemo sljedeće slučajeve.

- Ako je a višekratnik od 3, odnosno $a \equiv 0, 3, 6 \pmod 9$, onda kongruencija (1.29) (u nepoznanici k') nema rješenja. Zaista, u tom slučaju $3 \mid \gcd(a, 9)$ i $3 \nmid 2$.
- Ako je $a \equiv 1 \pmod 9$, onda je $k' \equiv 2 \pmod 9$.
- Ako je $a \equiv 2 \pmod 9$, onda je $k' \equiv 1 \pmod 9$.
- Ako je $a \equiv 4 \pmod 9$, onda je $k' \equiv 5 \pmod 9$.
- Ako je $a \equiv 5 \pmod 9$, onda je $k' \equiv 4 \pmod 9$.
- Ako je $a \equiv 7 \pmod 9$, onda je $k' \equiv 8 \pmod 9$.
- Ako je $a \equiv 8 \pmod 9$, onda je $k' \equiv 7 \pmod 9$.

Možemo zaključiti sljedeće: ako je

$$(a, k') \mod 9 \in \{(1,2),(2,1),(4,5),(5,4),(7,8),(8,7)\},$$

onda su n i b dani s (1.26), (1.27) cjelobrojni, te isto vrijedi za elemente skupa (1.28). Konkretno dobivamo sljedeće polinomijalne formule:

- $a = 1 + 9a'$, $k' = 2 + 9k''$, $a', k'' \in \mathbb{Z}$ i skup sa svojstvom $D(a'(26 + 36k'') + 4k'' + 3)$:

$$\{9a' + 1, a'(9k'' + 5)^2 + 9k''^2 + 8k'' + 1, a'(9k'' + 8)^2 + 9k''^2 + 14k'' + 6,$$

$$a'(18k'' + 13)^2 + 36k''^2 + 44k'' + 13\}.$$

- $a = 2+9a', k' = 1+9k'', a', k'' \in \mathbb{Z}$, skup sa svojstvom $D(a'(22+36k''+22)+8k''+5)$:

$$\{9a' + 2, a'(9k'' + 4)^2 + 2(9k''^2 + 7k'' + 1), a'(9k'' + 7)^2 + 2(9k''^2 + 13k'' + 5),$$
$$(a'(18k'' + 11)^2 + (18k'' + 11)(4k'' + 2)\},$$

- $a = 4+9a', k' = 5+9k'', a', k'' \in \mathbb{Z}$, skup sa svojstvom $D(a'(36k''+38)+16k''+17)$:

$$\{9a' + 4, a'(9k'' + 8)^2 + 36k''^2 + 62k'' + 26, a'(9k'' + 11)^2 + 36k''^2 + 86k'' + 52,$$
$$(18k'' + 19)^2 + 8(k'' + 1)(18k'' + 19)\},$$

- $a = 5+9a', k' = 4+9k'', a', k'' \in \mathbb{Z}$, skup sa svojstvom $D(a'(36k''+34)+20k''+19)$:

$$\{9a' + 5, a'(9k'' + 7)^2 + 45k''^2 + 68k'' + 25, a'(9k'' + 10)^2 + 45k''^2 + 98k'' + 54,$$
$$(a'(18k'' + 17)^2 + (10k'' + 9)(18k'' + 17)\},$$

- $a = 7+9a', k' = 8+9k'', a', k'' \in \mathbb{Z}$, skup sa svojstvom $D(a'(36k''+50)+28k''+39)$:

$$\{9a' + 7, a'(9k'' + 11)^2 + 63k''^2 + 152k'' + 91, a'(9k'' + 14)^2 + 63k''^2 + 194k'' + 150,$$
$$a'(18k'' + 25)^2 + (14k'' + 19)(18k'' + 25)\},$$

- $a = 8+9a', k' = 7+9k'', a', k'' \in \mathbb{Z}$, skup sa svojstvom $D(a'(36k''+46)+32k''+41)$:

$$\{9a' + 8, a'(9k'' + 10)^2 + 72k''^2 + 158k'' + 86, a'(9k'' + 13)^2 + 72k''^2 + 206k'' + 148,$$
$$a'(18k'' + 23)^2 + (16k'' + 20)(18k'' + 23)\}.$$

Formule za skupove sa svojstvom $D(n)$ koje smo dobili u slučajevima 1.A, 1.B i 2.A istaknut ćemo u sljedećem teoremu.

Teorem 1.2.1. *Neka su $m, k \in \mathbb{Z}$. Skupovi*

$$\{m, mk^2 - 2k - 2, m(k + 1)^2 - 2k, m(2k + 1)^2 - 4(2k + 1)\}, \tag{1.30}$$

$$\{m, m(1 + 3k)^2 + 2k, m(2 + 3k)^2 + 2(1 + k), 9m(1 + 2k)^2 + 4(1 + 2k)\} \tag{1.31}$$

imaju svojstvo svojstvom $D(2m(2k + 1) + 1)$. Skup

$$\{m, mk^2 + 2k - 2+, m(k + 1)^2 + 2(k + 2), m(2k + 1)^2 + 4(2k + 1)\} \tag{1.32}$$

ima svojstvo $D(2m(2k + 1) + 9)$.

Napomena 1.2.2. *Teorem 1.2.1 vrijedi i u bilo kojem komutativnom prstenu s jedinicom.*

Primjer 1.2.3. *Za* $m, k \in \mathbb{Z}[\sqrt{2}]$, $m = 1 - \sqrt{2}$, $k = 2\sqrt{2}$, *skup* (1.30) *je oblika*

$$\{1 - \sqrt{2}, 6 - 12\sqrt{2}, 1 - 9\sqrt{2}, 13 - 41\sqrt{2}\} \tag{1.33}$$

sa svojstvom $D(6\sqrt{2} - 13)$. *Uvjerimo se da je to zaista* $D(n)$ *četvorka u prstenu* $\mathbb{Z}[\sqrt{2}]$ *za* $n = 6\sqrt{2} - 13$.

- $$(1 - \sqrt{2})(6 - 12\sqrt{2}) + 6\sqrt{2} - 13 = 17 - 12\sqrt{2} = (3 - 2\sqrt{2})^2$$
- $$(1 - \sqrt{2})(1 - 9\sqrt{2}) + 6\sqrt{2} - 13 = 6 - 4\sqrt{2} = (2 - \sqrt{2})^2$$
- $$(1 - \sqrt{2})(13 - 41\sqrt{2}) + 6\sqrt{2} - 13 = 82 - 48\sqrt{2} = (8 - 3\sqrt{2})^2$$
- $$(6 - 12\sqrt{2})(1 - 9\sqrt{2}) + 6\sqrt{2} - 13 = 209 - 60\sqrt{2} = (3 - 10\sqrt{2})^2$$
- $$(6 - 12\sqrt{2})(13 - 41\sqrt{2}) + 6\sqrt{2} - 13 = 738 - 152\sqrt{2} = (9 - 22\sqrt{2})^2$$
- $$(1 - 9\sqrt{2})(13 - 41\sqrt{2}) + 6\sqrt{2} - 13 = 738 - 152\sqrt{2} = (4 - 19\sqrt{2})^2$$

Vidimo da je umnožak svaka dva različita elementa iz skupa (1.33) *uvećan za* $n = 6\sqrt{2} - 13$ *jednak potpunom kvadratu nekog elementa iz prstena* $\mathbb{Z}[\sqrt{2}]$, *iz čega slijedi da je skup* (1.33) *Diofantova četvorka u prstenu* $\mathbb{Z}[\sqrt{2}]$ *sa svojstvom* $D(6\sqrt{2} - 13)$.

Napomena 1.2.4. *Skupovi iz Teorema 1.2.1 bit će Diofantove četvorke sa svojstvom* $D(n)$ *ako niti jedan od elemenata nije jednak nuli i svi elementi su međusobno različiti.*

Primjer 1.2.5. *Za* $m = 2$ *i* $k = 3$, *skup* (1.32) *će biti oblika*

$$\{-2, -14, -22, -70\},$$

dok će za $m = 1, k = -3$ *biti oblika*

$$\{1, 1, 2, 5\}.$$

Uočimo da za $m = 2$ *i* $k = 3$ *dobivamo Diofantovu četvorku sa svojstvom* $D(-19)$, *a za* $m = 1, k = -3$ *skup* (1.32) *ima svojstvo* $D(-1)$ *ali ne predstavlja* $D(-1)$*-četvorku jer nije dozvoljeno ponavljanje elemenata.*

Poglavlje 2

$D(n)$-četvorke u prstenu cijelih brojeva

U ovom poglavlju pokazat ćemo da u prstenu cijelih brojeva postoji Diofantova četvorka sa svojstvom $D(n)$ ako i samo ako se n može prikazati kao razlika kvadrata dva cijela broja, do na konačno mnogo izuzetaka.

2.1 Nepostojanje $D(n)$-četvorke u $\mathbb{Z}$

Teorem 2.1.1. *Neka je n cijeli broj takav da je $n \equiv 2 \pmod 4$. Tada ne postoji Diofantova četvorka sa svojstvom $D(n)$.*

Dokaz. Neka je $n = 4k+2$ za neki $k \in \mathbb{Z}$. Pretpostavimo suprotno, tj. neka je $\{a_1, a_2, a_3, a_4\} \subset \mathbb{N}$ skup sa svojstvom $D(4k+2)$. Tada vrijedi:

$$a_i a_j + (4k+2) = b_{ij}^2, \ 1 \le i < j \le 4,$$

gdje su $b_{ij} \in \mathbb{Z}$. Znamo da kvadrat cijelog broja daje ostatak 0 ili 1 pri dijeljenju sa 4 što povlači da je

$$a_i a_j \equiv 2 \text{ ili } 3 \pmod 4.$$

Zaključujemo da niti jedan a_i nije djeljiv s 4, tj. brojevi a_1, a_2, a_3, a_4 daju ostatak $1, 2$ ili 3 pri dijeljenju s četiri. To znači da, prema Dirichelotov principu, barem dva broja među njima daju isti ostatak pri dijeljenju s 4. Neka su to brojevi a_s i a_t. Dakle,

$$a_s \equiv a_t \equiv m \pmod 4,$$

i $m \in \{1, 2, 3\}$, iz čega slijedi

$$a_s a_t \equiv m^2 \pmod 4.$$

Dobili smo kontradikciju jer lijeva strana kongruencije pri dijeljenju sa 4 daje ostatak 2 ili 3, a desna 0 ili 1. $\square$

2.2 Postojanje $D(n)$-četvorke u $\mathbb{Z}$

U prethodnom odsječku smo pokazali da ako je n oblika $4k+2$, $k \in \mathbb{Z}$, onda $D(n)$-četvorka ne postoji. Ovdje pokazujemo obrat. Koristeći formule za Diofantove skupove sa svojstvom $D(n)$ dane u Teoremu 1.2.1 efektivno ćemo konstruirati $D(n)$-četvorke za $n \not\equiv 2 \pmod 2$, do na konačno mnogo izuzetaka, tako da biramo pogodne vrijednosti parametara m i k.

Teorem 2.2.1. *Ako cijeli broj n nije oblika $4k+2$ i n nije element skupa*

$$S = \{-4, -3, -1, 3, 5, 8, 12, 20\},$$

onda postoji barem jedna Diofantova četvorka sa svojstvom $D(n)$.

Dokaz. Skup (1.31) ima svojstvo $D(2m(2k+1)+1)$. Želimo pronaći vrijednosti parametara m i k za koje je $2m(2k+1)+1 = 2N+1$, te za koje je $2m(2k+1)+1 = 4N$, $N \in \mathbb{Z}$. Pretpostavit ćemo da m poprima neku fiksnu cjelobrojnu vrijednost.

I) Neka je $n = 2N+1$, za neki $N \in \mathbb{Z}$. Trebamo odrediti neka, po mogućnosti cjelobrojna, rješenja jednadžbe (u nepoznanicama m i k):

$$2m(2k+1)+1 = 2N+1. \tag{2.1}$$

Očito je prethodna jednadžba ekvivalenta s

$$m(2k+1) = N.$$

Ako pretpostavimo da je $m = 1$, onda će (2.1) imati cjelobrojno rješenje u k ako i samo ako je N neparan, tj. $N = 2l+1$. U tom slučaju je $k = l$. Uvrštavanjem $m = 1$ i $k = l$ u (1.31) slijedi da skup

$$\{1, 9l^2+8l+1, 9l^2+14l+6, 36l^2+44l+13\} \tag{2.2}$$

ima svojstvo $D(4l+3)$.

Još moramo pronaći neko rješenje jednadžbe (2.1) ako je N paran, tj. $N = 2l$. Tada je jednadžba (2.1) ekvivalentna s

$$m(2k+1) = 2l.$$

Za fiksan $m = 2$, rješenje prethodne jednadžbe je cjelobrojno ako je l neparan. Stoga jednadžba (2.1) za $N = 4l+2$, tj. $2m(2k+1)+1 = 8l+5$ ima rješenje $(m,k) = (2,l)$. Prema (1.31) dobivamo skup

$$\{2, 18l^2+14l+2, 18l^2+26l+10, 72l^2+80l+22\} \tag{2.3}$$

ima svojstvom $D(8l+5)$.

Da bismo potpuno riješili slučaj “neparnog” n, preostaje nam slučaj kada je $N = 4l$, odnosno $n = 8l + 1$. Tada je jednadžba (2.1) ekvivalentna jednadžbi

$$m(2k + 1) = 4l.$$

Za fiksan $m = 4$, rješenje prethodne jednadžbe je $k = \dfrac{l-1}{2}$. Iako k nije cjelobrojan formula (1.31) daje skup s cjelobrojnim elementima

$$\{4, 9l^2 - 5l, 9l^2 + 7l + 2, 36l^2 + 4l\} \tag{2.4}$$

i sa svojstvom $D(8l + 1)$.

Zaključimo, ako je n neparan broj, onda postoji skup sa svojstvom $D(n)$. Budući da želimo naći $D(n)$-četvorke, još bi isključiti one vrijednosti parametra l za koje skupovi (2.2)-(2.4) imaju barem dva ista elementa ili neki od elemenata jednak nuli. To ćemo analizirati u 3. etapi dokaza. U sljedećem koraku nalazimo skupove za cijele brojeve n koji su djeljivi s 4.

II) Neka je $n = 4N$ za $N \in \mathbb{Z}$. Trebamo naći neka rješenja jednadžbe

$$2m(2k + 1) + 1 = 4N. \tag{2.5}$$

Jasno je da ne postoje cjelobrojna rješenja jer s lijeva strana prethodne relacije predstavlja neparan broj a desna paran. Stoga elementi skupa (1.31) ne će biti cjelobrojni. Ovu situaciju ćemo pokušati “izvući” primjenom Propozicije 1.1.5 koja kaže da množenjem elemenata skupa sa svojstvom $D(n)$ s nekim w dobivamo skup sa svojstvom $D(nw^2)$. Dakle, za $m = 1/2$, iz (2.5) dobivamo da je

$$k = 2N - 1.$$

Stavimo da je $l = 2N$. Uvrštavanjem $(m, k) = \left(\dfrac{1}{2}, l - 1\right)$ u (1.31) dobivamo skup

$$\left\{\frac{1}{2}, \frac{9l^2}{2} - 4l, \frac{9l^2}{2} - l + \frac{1}{2}, 18l^2 - 10l + \frac{1}{2}\right\} \tag{2.6}$$

sa svojstvom $D(2l)$. Skup (2.7) očito nema cjelobrojne elemente, ali pomnožimo li ih s 2 dobit ćemo skup s cjelobrojnim elementima

$$\{1, 9l^2 - 8l, 9l^2 - 2l + 1, 36l^2 - 20l + 1\} \tag{2.7}$$

i sa svojstvom $D(8l)$ (prema Propoziciji 1.1.5).

Preostaje nam još slučaj $n = 8l+4$. Kako je $8l+4 = 4(2l+1)$, pokušat ćemo kombinirati slučajeve iz I) s Propozicijom 1.1.5. Množenjem elemenata skupa (2.2) s 2 dobivamo skup

$$\{2, 18l^2 + 16l + 2, 18l^2 + 28l + 12, 72l^2 + 88l + 26\} \tag{2.8}$$

sa svojstvom $D(16l + 12)$.

Stoga nam do zaključivanja ovog slučaja još preostaje podslučaj $n = 16l+4 = 4(4l+1)$. Tražimo m i k za koje

$$2m(2k + 1) + 1 = 4l + 1.$$

Prethodna jednadžba je zadovoljena za $(m, k) = \left(2, \frac{l-1}{2}\right)$ pa iz (1.31) dobivamo skup

$$\left\{2, \frac{9l^2}{2} - 2l - \frac{1}{2}, \frac{9l^2}{2} + 4l + \frac{3}{2}, 18l^2 + 4l\right\}$$

sa svojstvom $D(4l + 1)$. Množenjem elemenata tog skupa s 2 dobivamo skup

$$\{4, 9l^2 - 4l - 1, 9l^2 + 8l + 3, 36l^2 + 8l\} \tag{2.9}$$

sa svojstvom $D(16l + 4)$.

Dakle, pokazali smo da ako je $n \equiv 0 \pmod 4$, onda postoji skup sa svojstvom $D(n)$.

III) U ovom koraku dokazu pronalazimo sve vrijednosti $l \in \mathbb{Z}$ za koje skupovi (2.2), (2.3), (2.4), (2.7), (2.8), (2.9) reprezentiraju $D(n)$-četvorke, $n = f(l)$. Pokažimo to na pa primjeru skupa (2.2). Najprije tražimo sve $l \in \mathbb{Z}$ za koje je neki od elemenata od (2.2) jednak nuli. Znači ispitujemo imaju li sljedeći polinomi (koji korespondiraju 2., 3. i 4. elementu skupa) cjelobrojnih nultočaka:

$$\begin{aligned} p_2(l) &= 9l^2 + 8l + 1, \\ p_3(l) &= 9l^2 + 14l + 6, \\ p_4(l) &= 36l^2 + 44l + 13 \end{aligned}$$

Niti jedan od prethodnih polinoma nema cjelobrojnih nultočki. Još preostaje za provjeriti daje li formula (2.2) ze neke l dva ista elementa. Dakle, uz oznaku $p_1(l) = 1$, treba ispitati je li

$$p_i(l) = p_j(l), \ 1 \le i < j \le 4,$$

za neke $l \in \mathbb{Z}$. Dakle, provjerom nultočaka sljedećih 6 polinoma

$$\begin{aligned}
(p_2 - p_1)(l) &= 9l^2 + 8l,\\
(p_3 - p_1)(l) &= 9l^2 + 14l + 5,\\
(p_4 - p_1)(l) &= 36l^2 + 44l + 12,\\
(p_3 - p_2)(l) &= 6l + 5,\\
(p_4 - p_2)(l) &= 27l^2 + 36l + 12,\\
(p_4 - p_3)(l) &= 27l^2 + 30l + 7,
\end{aligned}$$

dobivamo da je

$$(p_2 - p_1)(0) = 0,\ (p_3 - p_1)(-1) = 0.$$

Dakle, za $l = 0$ i pripadni $n = 3$ imamo skup kojem su prva dva elementa jednaka

$$\{1, 1, 6, 13\},$$

te za $l = -1$ i pripadni $n = -1$ skup kojem su prvi i treći elementi jednaki

$$\{1, 2, 1, 5\}.$$

Ispitujući mogućnosti za ostale skupove dobit ćemo sljedeće izuzetke:

$$\{-12, -7, -4, -3, -1, 0, 1, 3, 4, 5, 8, 9, 12, 20\}.$$

Slučaj $n = 1$ je riješen (jer postoji beskonačno mnogo Diofantovih četvorki). Skupovi $\{1, 12, 28, 76\}$ i $\{1, 8, 11, 16\}$ su $D(-12)$ i $D(-7)$-četvorke, redom. Nadalje, postoji beskonačno mnogo $D(0)$-četvorki. Zaista, $\{a^2, b^2, c^2, d^2\}$ je $D(0)$-četvorka za bilo koja 4 cijela broja a, b, c, d koji su različiti od nule. Nadalje, za n koji je jednak potpunom kvadratu postoji beskonačno mnogo $D(n)$-četvorki (Korolar 1.1.7) pa možemo eliminirati slučajeve $n = 4, 9$. Stoga, nismo pronašli $D(n)$-četvorku samo za $n \in \{-4, -3, -1, 3, 5, 8, 12, 20\}$. $\square$

Preglednost radi rezultate dobivene u dokazu prethodnog teorema ističemo u sljedećem korolaru.

Korolar 2.2.2. *Neka je $k \in \mathbb{Z}$. Tada za n danog oblika, uz konačno mnogo navedenih izuzetaka, sljedeći skupovi predstavljaju $D(n)$-četvorke:*

- $n = 4k + 3$:
$$\{1, 9k^2 + 8k + 1, 9k^2 + 14k + 6, 36k^2 + 44k + 13\}, \tag{2.10}$$
za $k \neq 0, -1$ tj. $n \neq 3, -1$,

- $n = 8k + 1$:
$$\{4, 9k^2 - 5k, 9k^2 + 7k + 2, 36k^2 + 4k\}, \tag{2.11}$$
za $k \neq 0, 1, -1$, *tj.* $n \neq 1, 9, -7$,

- $n = 8k + 5$:
$$\{2, 18k^2 + 14k + 2, 18k^2 + 26k + 10, 72k^2 + 80k + 22\}, \tag{2.12}$$
za $k \neq 0, -1$, *tj.* $n \neq 5, -3$,

- $n = 8k$:
$$\{1, 9k^2 - 8k, 9k^2 - 2k + 1, 36k^2 - 20k + 1\}, \tag{2.13}$$
za $k \neq 0, 1$, *tj.* $n \neq 0, 8$,

- $n = 16k + 4$:
$$\{4, 9k^2 - 4k - 1, 9k^2 + 8k + 3, 36k^2 + 8k\}, \tag{2.14}$$
za $k \neq 0, 1, -1$, *tj.* $n \neq 4, 20, -12$,

- $n = 16k + 12$:
$$\{2, 18k^2 + 16k + 2, 18k^2 + 28k + 12, 72k^2 + 88k + 26\}, \tag{2.15}$$
za $k \neq 0, -1$, *tj.* $n \neq 12, -4$.

Korolar 2.2.3. *Za svaki racionalan broj q postoji četveročlan skup racionalnih brojeva sa svojstvom da je produkt svaka dva različita elementa tog skupa, uvećan za q, kvadrat racionalnog broja.*

Dokaz. Neka je $q = \frac{m}{n}, m \in \mathbb{Z}, n \in \mathbb{N}$. Tada za $k = 100n^2q$ vrijedi: $k \in \mathbb{Z}, k \equiv 0 \pmod 4$ i $|x| \geq 100$ pa po Teoremu 2.2.1 postoji Diofantova četvorka $\{a_1, a_2, a_3, a_4\}$ sa svojstvom $D(k)$. Slijedi da skup $\left\{\frac{a_1}{10n}, \frac{a_2}{10n}, \frac{a_3}{10n}, \frac{a_4}{10n}\right\}$ ima svojstvo $D(q)$. □

Teorem 2.2.4. *Ako cijeli broj n nije oblika* $4k + 2$ *i* $n \notin S \cup T$, *gdje je skup S definiran u Teoremu 2.2.1, a*
$$T = \{-15, -12, -7, 7, 13, 15, 21, 24, 28, 32, 48, 60, 84\},$$
onda postoje barem dvije različite Diofantove četvorke sa svojstvom $D(n)$.

Dokaz. Analogno dokazu Teorema 2.2.1, iz (1.30) dobivamo sljedeće skupove sa svojstvom $D(n)$:

- $n = 4k + 3$:
$$\{1, k^2 - 2k - 2, k^2 + 1, 4k^2 - 4k - 3\}, \tag{2.16}$$

- $n = 8k + 1$:
$$\{4, k^2 - 3k, k^2 + k + 2, 4k^2 - 4k\}, \tag{2.17}$$

- $n = 8k + 5$:
$$\{2, 2k^2 - 2k - 2, 2k^2 + 2k + 2, 8k^2 - 2\}, \tag{2.18}$$

- $n = 8k$:
$$\{1, k^2 - 6k + 1, k^2 - 4k + 4, 4k^2 - 20k + 9\}, \tag{2.19}$$

- $n = 16k + 4$:
$$\{4, k^2 - 4k - 1, k^2 + 3, 4k^2 - 8k\}, \tag{2.20}$$

- $n = 16k + 12$:
$$\{2, 2k^2 - 4k - 4, 2k^2 + 2, 8k^2 - 8k - 6\}. \tag{2.21}$$

Ponovno trebamo ispitati za koje vrijednosti cijelog broja k će gornji skupovi imati jednake elemente ili neki od elemenata jednak nuli. To vrijedi za sljedeće vrijednosti parametra k:

- $k \in \{-1, 0, 1, 2, 3\}$, tj. $n \in \{-1, 3, 7, 11, 15\}$ za skup (2.16),
- $k \in \{-2, -1, 0, 1, 2, 3, 4\}$, tj. $n \in \{-15, -7, 1, 9, 17, 25, 33\}$ za skup (2.17),
- $k \in \{-1, 0, 1, 2\}$, tj. $n \in \{-3, 5, 13, 21\}$ za skup (2.18),
- $k \in \{0, 1, 2, 3, 4, 5, 6\}$, tj. $n \in \{0, 8, 16, 24, 32, 40, 48\}$ za skup (2.19),
- $k \in \{-1, 0, 1, 2, 3, 5\}$, tj. $n \in \{-12, 4, 20, 36, 52, 84\}$ za skup (2.20),
- $k \in \{-1, 0, 1, 2, 3\}$, tj. $n \in \{-4, 12, 28, 44, 60\}$ za skup (2.21).

Dakle, formule (2.16)-(2.21) ne predstavljaju Diofantove četvorke sa svojstvom $D(n)$ ako je n element skupa

$$\{-15, -12, -7, -4, -3, -1, 0, 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15,$$
$$16, 17, 20, 21, 24, 25, 28, 32, 33, 36, 40, 44, 48, 52, 60, 84\}.$$

Kao što smo već obrazložili u dokazu Teorema 2.2.1, za $n = 0, 1$ te ako je n jednak potpunom kvadratu nekog prirodnog broja, postoji beskonačno mnogo $D(n)$-četvorki. Nadalje, može se provjeriti da skupovi

$$\{2, 7, 19, 35\},\ \{1, 8, 19, 208\},\ \{8, 51, 101, 296\},\ \{1, 24, 41, 129\},\ \{1, 12, 477, 23052\}$$

imaju redom svojstva $D(11), D(17), D(33), D(40), D(52)$. Jasno, ni slučaj $n = 44 = 11 \cdot 2^2$ nije izuzetak. Stoga su izuzetci pobrojani u sljedećem skupu

$$\{-15, -12, -7, -4, -3, -1, 3, 5, 7, 8, 12, 13, 15, 20, 21, 24, 28, 32, 48, 60, 84\} = S \cup T.$$

□

2.3 Veza $D(n)$-četvorki i *razlike kvadrata*

Teorem 2.3.1. *Cijeli broj n može se prikazati kao razlika kvadrata dva cijela broja ako i samo* $n \not\equiv 2 \pmod 4$.

Dokaz. Neka je $n = x^2 - y^2,\ x, y \in \mathbb{Z}$. Budući da kvadrat cijelog broja daje ostatak 0 ili 1 pri dijeljenju s 4, sijedi da broj n daje ostatak 0, 1 ili 3 pri dijeljenju s 4.

Obratno, pretpostavimo li $n \not\equiv 2 \pmod 4$ slijedi da je $n = 4k$ ili $n = 4k+1$ ili $n = 4k+3$ za neki $k \in \mathbb{Z}$. U prvom slučaju imamo

$$4k = (k+1)^2 - (k-1)^2,$$

u drugom

$$4k + 1 = (2k+1)^2 - (2k)^2$$

a u trećem

$$4k + 3 = (2k+2)^2 - (2k+1)^2.$$

Stoga se svaki n takav da $n \not\equiv 2 \pmod 4$ može prikazati kao razlika kvadrata dva cijela broja. □

Na temelju onoga što se pokazalo u prethodnim odsječcima vrijedi:

Teorem 2.3.2. *Neka je* $n \in \mathbb{Z}$, $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$. *Diofantova četvorka sa svojstvom* $D(n)$ *postoji ako i samo ako se n može prikazati kao razlika kvadrata dva cijela broja*

Za elemente skupa S nije poznato postoji li $D(n)$-četvorka. Posebno se težak pokazao slučaj $D(-1)$-četvorke o kojem postoji niz članaka.

Slutnja 2.3.3. *Ne postoji* $D(n)$*-četvorka za* $n \in \{-4, -3, -1, 3, 5, 8, 12, 20\}$.

Zanimljivo je napomenuti da karakterizaciju $D(n)$-četvorke pomoću prikazivosti broja n kao razlike kvadrata dva cijela broj ne možemo dokazi direktno već korištenjem polinomijalnih formula za skupove sa svojstvom $D(n)$ iz Teorema 1.2.1, no ipak izravno možemo dokazati sljedeću tvrdnju.

Propozicija 2.3.4. *Ako je $n = k^2 - a^2$, onda za svaki cijeli broj m četvorka*

$$(a, a, (m^2 + 1)a + 2mk, (m^2 + 2m + 2)a + 2(m + 1)k)$$

ima svojstvo da je produkt svaka dva među njima uvećan za n potpun kvadrat.

Dokaz. Dokaz slijedi direktno iz sljedećih relacija:

- $$a \cdot a + n = k^2$$
- $$a[(m^2 + 1)a + 2mk] + n = (am + k)^2$$
- $$a[(m^2 + 2m + 2)a + 2k(m + 1)] + n = [a(m + 1) + k]^2$$
- $$[(m^2 + 1)a + 2mk][(m^2 + 2m + 2)a + 2k(m + 1)] + n = [a(m^2 + m + 1) + k(2m + 1)]^2$$

□

2.4 Diofantove četvorke sa svojstvom $D(l^2)$

Neka su a i b prirodni brojevi takvi da je $a < b$ i $\{a, b\}$ Diofantov par sa svojstvom $D(l^2)$ za neki $l \in \mathbb{N}$. Tada postoji $k \in \mathbb{N}$ takav da je

$$ab + l^2 = k^2. \tag{2.22}$$

Ako $D(l^2)$-par želimo proširiti s još jednim prirodnim brojem x tako da skup $\{a, b, x\}$ bude Diofantova trojka sa svojstvom $D(l^2)$, onda trebaju biti ispunjena sljedeća dva uvjeta

$$\begin{aligned} ax + l^2 &= y^2, \\ bx + l^2 &= z^2, \end{aligned} \tag{2.23}$$

za neke $y, z \in \mathbb{N}$. Odnosno ekvivalentno, tražimo rješenje jednadžbe tzv. *pellovskog tipa*

$$by^2 - az^2 = l^2(b - a), \tag{2.24}$$

u nepoznanicama y i z. Lako se provjerava da je prethodna jednadžba uvijek rješiva. Naime,

$$(y, z) = (l, l), \ (y, z) = (k + a, k + b)$$

zadovoljavaju jednadžbu (2.24). Može se pokazati da će nizovi rješenja koji su generirani s ovim početnim rješenjima dati nadopunjenja $D(l^2)$-para $\{a, b\}$. Metodu nadopunjavanja opisat ćemo na konkretnom primjeru. Prije nego što izložimo taj primjer, navedimo neke osnovne činjenice o Pellovim i pellovskim jednadžbama koje će nam trebati za rješavanje jednadžbe (2.24).

Definicija 2.4.1. *Neka je d prirodni broj koji nije potpuni kvadrat. Diofantska jednadžba oblika*

$$x^2 - dy^2 = 1 \tag{2.25}$$

zove se Pellova jednadžba.

Jednadžba oblika

$$x^2 - dy^2 = N \tag{2.26}$$

gdje je N cijeli broj, naziva se pellovska jednadžba.

Teorem 2.4.2. *Neka je* $x_1 + y_1\sqrt{d}$ *fundamentalno rješenje Pellove jednadžbe* (2.25). *Tada su sva rješenja u skupu prirodnih brojeva dana formulom*

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

Konkretno, vrijedi

$$x_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} x_1^{n-2k} y_1^{2k} d^k$$

$$y_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k+1} x_1^{n-2k-1} y_1^{2k+1} d^k$$

Teorem 2.4.3. *Rješenja Pellove jednadžbe* (2.25) *u skupu prirodnih brojeva* (x_n, y_n) *zadovoljavaju rekurzivne relacije*

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

$$y_n = y_1x_{n-1} + x_1y_{n-1}, n \geq 1,$$

pri čemu je (x_1, y_1) *fundamentalno, a* $(x_0, y_0) = (1, 0)$ *trivijalno rješenje od* (2.25).

Nadalje, uz iste početne uvjete vrijede i relacije

$$x_n = 2x_1x_{n-1} - x_{n-2},$$

$$y_n = 2x_1y_{n-1} - y_{n-2}, n \geq 2.$$

Propozicija 2.4.4. *Neka je* (x_1, y_1) *neko rješenje pellovske jednadžbe* (2.26)*, a* (u, v) *rješenje Pellove jednadžbe* (2.25)*. Tada je*

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

rješenje jednadžbe (2.26)*.*

Dokaz. Direktnim uvrštavanjem $(x_2, y_2) = (x_1u + y_1vd, x_1v + y_1u)$ u (2.26). □

Korolar 2.4.5. *Neka su* $a, b \in \mathbb{N}$ *i* a, b, ab *nisu potpuni kvadrati. Ako je* (x_1, y_1) *rješenje jednadžbe*

$$ax^2 - by^2 = N, \tag{2.27}$$

(u, v) *rješenje Pellove jednadžbe* $x^2 - aby^2 = 1$*,*

$$x_2\sqrt{a} + y_2\sqrt{b} = (x_1\sqrt{a} + y_1\sqrt{b})(u + v\sqrt{ab})$$

onda je (x_2, y_2) *rješenje jednadžbe* (2.27)*.*

Dokaz. Očito je (x^*, y^*) rješenje jednadžbe (2.27) ako i samo ako je (ax^*, y^*) rješenje pellovske jednadžbe $x^2 - aby^2 = aN$. Prema Propoziciji 2.4.4, (ax_2, y_2) je rješenje od $x^2 - aby^2 = aN$ pa slijedi tvrdnja. □

Vratimo se sada na rješavanje jednadžbe (2.24). Njoj pridružena Pellova jednadžba glasi

$$y^2 - abz^2 = 1,$$

te označimo fundamentalno rješenje sa (s, t). Dakle,

$$s^2 - abt^2 = 1. \tag{2.28}$$

Prema Teoremu 2.4.2 i Korolaru 2.4.5 vrijedi da su

$$y_n\sqrt{b} + z_n\sqrt{a} = (l\sqrt{b} + l\sqrt{a})(s + t\sqrt{ab})^n,$$

$$y'_n\sqrt{b} + z'_n\sqrt{a} = ((k + a)\sqrt{b} + (k + b)\sqrt{a})(s + t\sqrt{ab})^n,$$

rješenja od (2.24) za $n \in \mathbb{N}_0$. Nizovi (y_n) i (y'_n) su binarni rekurzivni nizovi potpuno analogni onima za Pellovu jednadžbu (Teorem 2.4.3). Dakle, vrijedi

$$y_n = 2sy_{n-1} - y_{n-2},\ n \geq 2 \tag{2.29}$$

uz početne uvjete $y_0 = l$ i $y_1 = (s + at)l$, te

$$y'_n = 2sy'_{n-1} - y'_{n-2},\ n \geq 2$$

uz početne uvjete $y'_0 = k + a$ i $y'_1 = s(k + a) + at(k + b)$. Prema definiramo pripadne nizove (x_n) i (x'_n):

$$x_n = \frac{y_n^2 - l^2}{a},\ x'_n = \frac{{y'_n}^2 - l^2}{a}. \tag{2.30}$$

Jasno je da su $\{a, b, x_n\}$ i $\{a, b, x'_n\}$ Diofantovi skupovi sa svojstvom $D(l^2)$, no trebamo pokazati da su x_x, x'_n cjelobrojno za svaki $n \in \mathbb{N}_0$.

Propozicija 2.4.6. *Nizovi* (x_n) *i* (x'_n) *definirani relacijama u* (2.30) *su cjelobrojni.*

Dokaz. Pokažimo da $a \mid y_n^2 - l^2$, za svaki $n \in \mathbb{N}_0$. Tvrdnju ćemo dokazati pomoću matematičke indukcije.

1. Baza: $n = 0$ i $n = 1$,

$$y_0^2 - l^2 = 0,$$

$$y_1^2 - l^2 = (s + at)^2 l^2 - l^2 = l^2(s^2 + 2sat + a^2t^2 - 1) = l^2 \underbrace{(abt^2 + 2sat + a^2t^2)}_{a|}. \tag{2.31}$$

   pri čemu smo posljednju jednakost dobili prema (2.28).

2. Pretpostavimo da za neki $n \in \mathbb{N}$, a dijeli $y_i^2 - l^2$ za sve $i \leq n$.

3. Prema rekurziji (2.29) imamo

$$y_{n+1}^2 - l^2 = (2sy_n - y_{n-1})^2 - l^2 = 4s^2y_n^2 - 4sy_ny_{n-1} + \underbrace{y_{n-1}^2 - l^2}_{a|}. \tag{2.32}$$

   Sada, ponovno matematičkom indukcijom, pokazujemo da $a \mid sy_n - y_{n-1}$.

   a) Baza: $n = 1$,

$$\begin{aligned} sy_1 - y_0 &= s(s + at)l - l = l(s^2 - sat - 1) \\ &= l(abt + sat) = a(lbt + lst). \end{aligned}$$

   b) Neka je $n \in \mathbb{N}$. Pretpostavimo da $a \mid sy_i - y_{i-1}$ za sve $i \leq n$, tj. $sy_i - y_{i-1} = ak, k \in \mathbb{Z}$.

   c) Provjerimo vrijedi li tvrdnja za $n + 1$. Koristeći rekurziju (2.29) dobivamo

$$\begin{aligned} sy_{n+1} - y_n &= s(2sy_n - y_{n-1}) - y_n = s(sy_n + ak) - y_n \\ &= s^2y_n + aks - y_n = y_n(s^2 - 1) + aks \\ &= y_n \cdot abt + aks = a(y_nbt + ks). \end{aligned}$$

Dobili smo da $a \mid sy_{n+1} - y_n$ iz čega slijedi da je relacija (2.32) djeljiva s a pa početna pretpostavka vrijedi za sve $n \in \mathbb{N}_0$, tj. niz (x_n) je cjelobrojan.

Pokažimo sada analognu tvrdnju za niz (x'_n) opet koristeći princip matematičke indukcije. Budući da nizovi (y_n) i (y'_n) zadovoljavaju istu rekurziju dovoljno je provjeriti bazu indukcije.

1. Baza: $n = 0$ i $n = 1$. Vrijedi

$$y_0'^2 - l^2 = (k+a)^2 - l^2 = k^2 + 2ak + a^2 - l^2 = ab + 2ak + a^2 = a(a+b+2k),$$

gdje smo primijenili (2.22). Nadalje,

$$\begin{aligned} y_1'^2 - l^2 &= (s(k+a) + at(k+b))^2 - l^2 \\ &= s^2(k+a)^2 + a^2t^2(k+b)^2 + 2sat(a+k)(b+k) - l^2 \\ &= (abt^2+1)(k+a)^2 + a^2t^2(k+b)^2 + 2sat(a+k)(b+k) - l^2 \\ &= abt^2(k+a)^2 + k^2 + 2ak + a^2 + a^2t^2(k+b)^2 + 2sat(a+k)(b+k) - l^2 \\ &= abt^2(k+a)^2 + ab + 2ak + a^2 + a^2t^2(k+b)^2 + 2sat(a+k)(b+k), \end{aligned}$$

pri čemu smo koristili (2.22) i (2.28). Očito, $a \mid y_1'^2 - l^2$.

Treba još dokazati da $a \mid sy'_n - y'_{n-1}$ za što je ponovo dovoljno pokazati bazu indukcije.

a) $n = 1$

$$\begin{aligned} sy'_1 - y'_0 &= s(s(k+a) + at(k+b)) - (k+a) \\ &= (s^2-1)(k+a) + at(k+b) \\ &= abt^2(k+a) + at(k+b) \\ &= a(bt^2(k+a) + t(k+b)). \end{aligned}$$

□

U [1] je Dujella pokazao da je

$$x_n x'_n + l^2 = \left(\frac{y_n y'_y - lk}{a}\right)^2,$$

za sve $n \in \mathbb{N}_0$. Dokaz je tehnički složen i zahtijevao bi uvođenje još nizova koji zadovoljavaju jednadžbu (2.24). Drugim riječima vrijedi sljedeća tvrdnja.

Teorem 2.4.7. *Neka je $l \in \mathbb{Z}$ i $\{a, b\}$ Diofantov par sa svojstvom $D(l^2)$. Tada je*

$$\{a, b, x_n, x'_n\}$$

skup sa svojstvom $D(l^2)$ za sve $n \in \mathbb{N}$.

Na konkretnom primjeru demonstrirat ćemo opisanu metodu kojom neki Diofantov par sa svojstvom $D(l^2)$ možemo nadopuniti, na beskonačno mnogo načina, do Diofantove četvorke sa svojstvom $D(l^2)$.

Primjer 2.4.8. *Zadan je Diofantov par* $\{4, 5\}$ *sa svojstvom* $D(16)$. *Dakle, zadane su sljedeće vrijednosti parametara:*

$$a = 4, b = 5, l = 4, k = 6.$$

Da bismo odredili nizove (x_n) *i* (x'_n) *trebamo najprije odrediti nizove* (y_n) *i* (y'_n) *koji su rješenja pellovske jednadžbe* $5y^2 - 4z^2 = 16$. *Za to nam je potrebno fundamentalno rješenje pripadne Pellove jednadžbe* $y^2 - 20z^2 = 1$. *Lako se provjeri da je to* $(s, t) = (9, 2)$. *Početne vrijednosti nizova* (y_n) *i* (y'_n) *su*

$$y_0 = l = 4, \; y_1 = (s + at)l = 68,$$

$$y'_0 = k + a = 10, \; y'_1 = s(k + a) + at(k + b) = 178.$$

Kako je $x_0 = 0$, $\{a, b, x_0, x'_0\}$ *ne predstavlja pravo proširenje. Nadalje,*

$$x_1 = \frac{y_1^2 - l^2}{a} = 1152, \; x'_1 = \frac{{y'_1}^2 - l^2}{a} = 7917,$$

dat će pravo proširenje. Zaista, $\{4, 5, 1152, 7917\}$ *je Diofantova četvorka sa svojstvom* $D(4^2)$. *U to se možemo i eksplicitno uvjeriti:*

$$\begin{aligned} 4 \cdot 5 + 16 &= 6^2, \\ 4 \cdot 1152 + 16 &= 68^2, \\ 4 \cdot 7917 + 16 &= 178^2, \\ 5 \cdot 1152 + 16 &= 76^2, \\ 5 \cdot 7917 + 16 &= 199^2, \\ 1152 \cdot 7917 + 16 &= 3020^2. \end{aligned}$$

Za $n = 2, 3, 4, \ldots$ *dobivamo skupove:*

$$\begin{aligned} &\{4, 5, 372096, 2553600\}, \\ &\{4, 5, 119814912, 822255621\}, \\ &\{4, 5, 38580030720, 264763760700\}, \ldots \end{aligned}$$

Pomoću opisane konstrukcije za nadopunjavanje $D(l^2)$-para do četvorke može se doći do zanimljivih primjera čiji su elementi Fibonaccijevi i Lucasovi brojevi. *Niz Fibonaccijevih brojeva* definira se rekurzivnom relacijom

$$F_{n+1} = F_n + F_{n-1},\ n \geq 1,$$

s početnim uvjetima $F_0 = 1,\ F_1 = 1$. Niz Lucasovih brojeva u oznaci (L_n) dan je relacijom

$$L_n = F_{n+1} + F_{n-1}, n \in \mathbb{N},$$

odnosno

$$L_{n+1} = L_n + L_{n-1},\ n \leq 1,$$

s početnim uvjetima $L_0 = 2,\ L_1 = 1$.

Teorem 2.4.9. *Za sve prirodne brojeve $n \geq 2$, skupovi*

$$\{2F_{n-1}, 2F_{n+1}, 2F_n^3 F_{n+1} F_{n+2}, 2F_{n+1} F_{n+2} F_{n+3}(2F_{n+1}^2 - F_n^2)\}, \tag{2.33}$$

$$\{F_{n-1}, 4F_{n+1}, F_n^3 F_{n+2} F_{n+3}, F_{n+1} F_{n+2} F_{n+4}[F_{n+2}^2 + 2(-1)^n]\}, \tag{2.34}$$

$$\{4F_{n-1}, F_{n+1}, F_n^3 L_n L_{n+1}, F_{n+1} F_{2n+4}(F_{2n+2} + 2(-1)^n)\} \tag{2.35}$$

imaju svojstvo $D(F_n^2)$.

Za sve prirodne brojeve $n \geq 3$, skupovi

$$\{2F_{n-1}, 2F_{n+1}, 2F_{n-2} F_{n-1} F_n^3, 2F_n^3 F_{n+1} F_{n+2}\}, \tag{2.36}$$

$$\{F_{n-1}, 4F_{n+1}, F_{n-2} F_{n-1} F_{n+1}(2F_n^2 - F_{n-1}^2), F_n^3 F_{n+2} F_{n+3}\}, \tag{2.37}$$

$$\{4F_{n-1}, F_{n+1}, F_{n-2} F_{2n-2} F_{2n-1}, F_n^3 L_n L_{n+1}\} \tag{2.38}$$

imaju svojstvo $D(F_n^2)$

Teorem 2.4.9 može se dokazati direktnom provjerom. Pokažimo to na primjeru skupa (2.34):

$$F_{n-1} \cdot 4F_{n+1} + F_n^2 = L_n^2,$$

$$F_{n-1} \cdot F_n^3 F_{n+2} F_{n+3} + F_n^2 = (F_n F_{n+1}^2)^2,$$

$$F_{n-1} \cdot F_{n+1} F_{n+2} F_{n+4}[F_{n+2}^2 + 2(-1)^n] + F_n^2 = [F_{n+1} F_{n+2}^2 + (-1)^n F_{n+3}]^2,$$

$$4F_{n+1} \cdot F_n^3 F_{n+2} F_{n+3} + F_n^2 = \{F_n[2F_{n+1} F_{n+2} - (-1)^n]\}^2,$$

$$4F_{n+1} \cdot F_{n+1} F_{n+2} F_{n+4}[F_{n+2}^2 + 2(-1)^n] + F_n^2 = \{F_{n+3}[2F_{n+1} F_{n+2} + (-1)^n]\}^2,$$

$$F_n^3 F_{n+2} F_{n+3} \cdot F_{n+1} F_{n+2} F_{n+4}[F_{n+2}^2 + 2(-1)^n] + F_n^2 = \{F_n[F_{n+2}^4 + (-1)^n F_{n+2}^2 - 1]\}^2.$$

Već smo na samom početku zaključili da postoji beskonačno mnogo $D(l^2)$-četvorki u prstenu cijelih brojeva. No, to ne vrijedi za cijeli broj n koji nije jednak potpunom kvadratu. Zato je postavljena sljedeća slutnja.

Slutnja 2.4.10. *Neka je $n \in \mathbb{Z}$, $n \neq l^2$ za sve $l \in \mathbb{Z}$. Tada postoji najviše konačno mnogo $D(n)$-četvorki.*

Bibliografija

[1] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arith. **65** (1993), 15–27.

[2] A. Dujella, *Diophantine quadruples for squares of Fibonacci and Lucas numbers*, Portugaliae Math. **52** (1995), 305-318.

[3] A. Dujella, *Some polynomial formulas for Diophantine quadruples*, Grazer Math. Ber. **328** (1996), 25–30.

[4] A. Dujella, *Generalizirani Diofant-Davenportov problem*, doktorska disertacija, Sveučilište u Zagrebu, 1996.

[5] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[6] Z. Franušić, *Pellove jednadžba*, `https://web.math.pmf.unizg.hr/nastava/etb/materijali/pellova-web.pdf`

[7] B. He, A. Togbé and V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. **371** (2019), 6665–6709.

Sažetak

Neka je n cijeli broj. Skup cijelih brojeva različitih od nule $\{a_1, a_2, a_3, a_4\}$ je Diofantova četvorka sa svojstvom $D(n)$ ako je umnožak bilo koja dva elementa tog skupa uvećan za cijeli broj n jednak potpunom kvadratu. Dva važna povijesna primjera takvih skupova su $\{1, 33, 68, 105\}$ - $D(256)$-četvorka (koju je dobio grčki matematičar Diofant Aleksandrijski) te$\{1, 3, 8, 120\}$ - $D(1)$-četvorka (koju je pronašao je francuski matematičar Pierre de Fermat)

U ovom radu razmatramo problem postojanja Diofantove četvorke za proizvoljni cijeli broj n. Pokazujemo da Diofantova četvorka sa svojstvom $D(n)$ postoji ako i samo ako je $n \not\equiv 2 \pmod 4$, tj. ako i samo ako se n može prikazati kao razlika kvadrata dva cijela broja, do na konačno mnogo izuzetaka.

Summary

Let n be an integer. A set of four nonzero integers $\{a_1, a_2, a_3, a_4\}$ is a *Diophantine quadruple with the property* $D(n)$, or just a $D(n)$*-quadruple* if the product of its any two distinct elements increased by n is a perfect square. Two significant historical examples of such sets are $\{1, 33, 68, 105\}$ - a $D(256)$-quadruple (obtained by the Greek mathematician Diophantus of Alexandria) and $\{1, 3, 8, 120\}$ - a $D(1)$-quadruple (found by the French mathematician Pierre de Fermat).

In this thesis, we consider the problem of existence of Diophantine quadruples for an arbitrary integer n. We show that there exists a Diophantine quadruple with the property $D(n)$ if and only if $n \not\equiv 2 \pmod 4$, i.e. if and only if n can be represented as a difference of squares of two integers, up to finitely many exceptions.

Životopis

Rođena sam 4. kolovoza 1995. godine u Dubrovniku. Osnovnu školu završila sam u OŠ Ston (PO Ponikve) na poluotoku Pelješcu. Srednjoškolsko obrazovanje stekla sam u Općoj Gimnaziji Dubrovnik nakon čega sam 2014. godine upisala Preddiplomski sveučilišni studij Matematike, nastavnički smjer, na Prirodoslovno - matematičkom fakultetu u Zagrebu. Nakon završenog preddiplomskog studija, 2017. godine upisala sam Diplomski sveučilišni studij Matematičke statistike na istom fakultetu. Tijekom prve godine studiranja matematičke statistike u meni je rasla velika želja za poučavanjem pa se sam 2018. godine prebacila na Diplomski sveučilišni studij Matematike, nastavnički smjer.