Neke diofantske jednadžbe drugog stupnja

Jozinović, Ivana

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Ivana Jozinović

Neke diofantske jednadžbe drugog stupnja

Završni rad

Osijek, 2019.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Ivana Jozinović

Neke diofantske jednadžbe drugog stupnja

Završni rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2019.

Sažetak

U ovom završnom radu proučavat ćemo diofantske jednadžbe drugog stupnja. Definirat ćemo Pitagorinu jednadžbu i pokazati neke načine traženja njenih rješenja. Zatim ćemo pručavati pellovske jednadžbe i iskazati tvrdnje potrebne za njihovo rješavanje.

Ključne riječi

Diofantske jednadžbe drugog stupnja, Pellove jednadžbe, verižni razlomci

Some diophantine equations of the second degree

Summary

In this final paper we will study some diophantine equations of the second degree. We will define Pythagorean equation and show a several ways to solve it. Then we will study the Pell's equations and state the claims related to finding its solutions.

Key words

Diophantine equations of the second degree, Pell's equatinos, continued fractions

Sadržaj

1 Zbrojevi kvadrata **1**

1.1 Jednadžba oblika $x^2 + y^2 = z^2$ 1

1.2 Jednadžba oblika $x^2 + y^2 + z^2 = t^2$ 6

2 Pellovske jednadžbe **8**

2.1 Jednadžbe oblika $x^2 - dy^2 = \pm 1$ 8

2.2 Pellove jednadžbe i verižni razlomci 13

2.3 Jednadžbe oblika $x^2 - dy^2 = N$ 16

Uvod

U ovom radu proučavat ćemo osnovna svojstva i oblike diofantskih jednadžbi drugog stupnja, te neke metode njihova rješavanja. Na početku ćemo općenito definirati diofantske jednadžbe. Diofantske jednadžbe dobile su naziv po grčkom matematičaru Diofantu koji je živio u 3. stoljeću prije Krista i bavio se problemima vezanim uz jednadžbe toga tipa.

Definicija 1 *Diofantskom jednadžbom nazivamo algebarsku (poliomnu) jednadžbu s dvjema ili više nepoznanica s cijelobrojnim koeficijentima kojoj se traže cjelobrojna ili racionalna rješenja. Polinomna jednadžba je jednadžba kojoj je rješenje polinom.*

Primjer 1 *Jednadžba*

$$7x - 5y^2 = 3$$

je diofantska jednadžba s dvije nepoznanice.
Jednadžba

$$5x^2 - 4y + 5z^3 + t = 28$$

je diofantska jednadžba s 4 nepoznanice.

Definicija 2 *Polinom f je realna ili kompleksna funkcija realne ili kompleksne varijable x koju možemo zapisati u obliku:*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

pri čemu je $n \in \mathbb{N}$, $a_n \neq 0$. Realne ili kompleksne brojeve $a_0, a_1, \ldots, a_n$ zovemo koeficijenti polinoma f, broj a_0 slobodni koeficijent, a broj a_n vodeći koefcijent. Broj n zovemo stupanj polinoma f.

Primjer 2 *Funkcija*

$$f(x) = 2x^3 + 5x^2 - 8x + 3$$

je polinom 3. stupnja. Vodeći koeficijent je $a_3 = 2$, a $a_0 = 3$ je slobodni koeficijent.

Definicija 3 *Linearnom diofantskom jednadžbom s n nepoznanica nazivamo jednadžbu oblika:*

$$a_1 x_1 + a_2 x_2 + ... + a_n x_n = b$$

gdje su $x_1.,.x_n$ nepoznanice, te $a_1, .., a_n, b$ cjelobrojni koeficijenti.Sve diofantske jednadžbe koje nisu linearne nazivamo nelinearnim diofantskim jednadžbam. U njima se nepoznanice pojavljuju u članovima višeg reda. Diofantske jednadžbe drugog reda su nelinearne diofantske jednadžbe u kojima su nepoznanice drugog reda.

Primjer 3 *Jednadžba $2x_1 - 4x_2 + x_3 = 15$ je linearna diofantska jednadžba s nepoznanicama x_1, x_2, x_3 i koeficijentima $a_1 = 2, a_2 = 4$ i $a_3 = 1$.*
Jednadžba $x^2 + 3y^2 = 4$ je diofantska jednadžba drugog reda.

Neke od najpoznatijih diofantskih jednadžbi drugog reda su jednadžbe oblika $x^2 + y^2 = z^2$, gdje su $x, y, z \in \mathbb{N}$ i rješenje (x, y, z) nazivamo Pitagorina trojka o kojima ćemo govoriti u prvom poglavlju. Uz to još ćemo iskazati algoritam za rješavanje jednadžbe $x^2 + y^2 + z^2 = t^2$.

U drugom dijelu ćemo proučavati Pellove i pellovske jednadžbe, njihova rješenja i brojnost rješenja navedenih jednadžbi.

1 Zbrojevi kvadrata

U ovom poglavlju bavit ćemo se jednadžbom oblika $x^2 + y^2 = z^2$ koja je poznata i pod imenom Pitagorina jednadžba jer njezina rješenja (x, y, z) čine Pitagorinu trojku, tj. predstavljaju duljinu kateta i hipotenuze pravokutnog trokuta. Također ćemo proučavati jednadžbe oblika $x^2 + y^2 + z^2 = t^2$ i pokazati algoritam za njezino rješavanje.

1.1 Jednadžba oblika $x^2 + y^2 = z^2$

Diofantska jednadžba oblika

$$x^2 + y^2 = z^2 \tag{1}$$

poznata je i pod nazivom Pitagorina jednadžba, a rješenja ove jednadžbe (x, y, z) Pitagorina trojka. Ova jednadžba je posebno važna u trigonometriji i analitičkoj geometriji. Njen poseban slučaj, za $x = y$, povezan je s najjednostavnijim dokazom postojanja iracionalnih brojeva. Pronaći ćemo sva cjelobrojna rješenja jednadžbe (1). Isključujemo očita rješenja u kojima je jedan od brojeva x, y jednak nuli. Ako su brojevi x, y, z prirodni i zadovoljavaju jednadžbu (1), onda kažemo da je (x, y, z) pitagorejski trokut. Rješenje jednadžbe (1) naziva se primitivnim rješenjem ako su brojevi x, y, z prirodni i nemaju zajednički djelitelj veći od jedinice, odnosno ako su relativno prosti što pišemo u obliku $(x, y, z) = 1$.

Ako su x_1, y_1, z_1 primitivna rješenja jednadžbe (1) i d prirodan broj, onda su $x = dx_1, y = dy_1, z = dz_1$ također rješenje od (1). Ako je

$$x_1^2 + y_1^2 = z_1^2$$

onda množenjem obje strane s d^2 dobijemo jednadžbu (1). Obratno, ako su x, y, z rješenja jednadžbe (1) u prirodnim brojevima, onda zamjenom $(x, y, z) = d$ imamo
$x = dx_1,\ y = dy_1,\ z = dz_1$ gdje je $(x_1, y_1, z_1) = 1$. Tada imamo

$$(dx_1)^2 + (dy_1)^2 = (dz_1)^2.$$

Dijeljenjem ove jednadžbe s d^2 vidimo da su prirodni brojevi x_1, y_1, z_1 primitivno rješenje jednadžbe (1). Kažemo da rješenje jednadžbe (1) u prirodnim brojevima x, y, z pripada d-toj klasi ako je $(x, y, z) = d$. Pretpostavimo da je x, y, z primitivno rješenje jednadžbe (1). Dokazat ćemo da je jedan od brojeva x, y paran, a drugi neparan. Pretpostavimo suprotno, tj. neka su oba ili parna ili neparna.
U prvom slučaju, ako bi x i y bili parni, onda trojka ne bi bila primitivna jer bi imali najmanjeg zajedničkog djelitelja 2, što je u kontradikciji s pretpostavkom.
Kako bismo dokazali da je i drugi slučaj nemoguć dokazujemo da dijeljenjem kvadrata neparnog prirodnog broja s 8 dobijemo ostatak 1. Neparni prirodan broj zapisujemo kao $2k - 1$, gdje je k prirodan broj. Nadalje,

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

Jedan od brojeva k i $k-1$ mora biti paran, pa je umnožak sigurno djeljiv s 2 te je $4k(k-1)$ djeljivo s 8. Stoga, podijelimo li $(2k-1)^2$ s 8, dobijemo ostatak 1. Dakle, ako bi x i y bili neparni, onda bi imali $x^2+y^2 \equiv 2 \pmod 4$. To pokazuje da suma kvadrata dva neparna broja nije kvadrat neparnog broja. Ne može biti ni kvadrat parnog broja, jer bi suma u tom slučaju bila djeljiva s 4, pa bi ostatak pri djeljenju s 8 bio 0 ili 4, što je kontradikcija s prethodno dokazanom tvrdnjom. Obično se uzima za x neparan, a za y paran prirodan broj.

Teorem 1 (Euklidova formula, [1, Teorem 7.3.])
Sve primitivne Pitagorine trojke (x, y, z) u kojima je y paran, dane su formulama

$$x = m^2 - n^2,\ y = 2mn,\ z = m^2 + n^2 \tag{2}$$

gdje je $m < n$ i m, n su relativno prosti prirodni brojevi različte parnosti.

Dokaz:

Iz jednadžbe (1) slijedi da je $y^2 = z^2 - x^2$. Tada y^2 možemo pisati u obliku $y^2 = (z+x)(z-x)$. Zbog parnosti, y možemo zapisati kao $y = 2c, c \in \mathbb{N}$. Budući da su po pretpostavci x i z neparni, brojevi $(z+x)$ i $(z-x)$ su parni kao suma i razlika neparnih brojeva, pa postoje prirodni brojevi a i b takvi da je $z+x = 2a$, $z-x = 2b$. Sada je

$$c^2 = ab.$$

Zbrajanjem i oduzimanjem prethodne dvije jednadžbe dobijamo

$$z = a+b,\ x = a-b.$$

Nadalje, pretpostavimo da je $(a,b) > 1$, tj. da a i b nisu relativno prosti. Tada postoji zajednički djelitelj $d > 1$ tako da vrijedi $x = kd$, $z = ld$, gdje su k i l neki prirodni brojevi, te je $y^2 = x^2 - z^2 = (k^2 - l^2)d^2$. No, to je u kontradikciji s primitivnošću od x, y, z. Slijedi da je $(a,b) = 1$. Dakle, postoje $m, n \in \mathbb{N}$, $(m,n) = 1$, takvi da je $a = m^2,\ b = n^2$.
Odavde je

$$x = m^2 - n^2,\ z = m^2 + n^2,\ y = 2mn.$$

Brojevi m i n moraju biti različite parnosti jer je broj $x = m^2 - n^2$ neparan. Zaista, $(m^2-n^2)^2 + (2mn)^2 = m^4 + 2m^2n^2 + n^4 = (m^2+n^2)^2$. Treba još provjeriti da su relativno prosti. Pretpostavimo da je $(x,z) = d > 1$. Tada je d neparan,

$$d \mid (m^2+n^2) + (m^2-n^2) = 2m^2$$

i

$$d \mid (m^2+n^2) - (m^2-n^2) = 2n^2.$$

No, ovo je u kontradikciji s pretpostavkom da su m i n relativno prosti, pa stoga i m^2 i n^2, relativno prosti. □

Iz Teorema 1 slijedi da su sve Pitagorine trojke dane identitetom:

$$[d(m^2-n^2)]^2 + [2dmn]^2 = [d(m^2+n^2)]^2. \tag{3}$$

Primjer 4 *Nađite sve Pitagorine trojke kojima je jedna stranica jednaka 21.*

Rješenje: Budući da d mora dijeliti duljinu stranice, u našem slučaju imamo tri mogućnosti, a to su $d = 1$, $d = 3$, i $d = 7$. S obzirom da je $2mn \neq 21$ uvijek, razmatramo samo preostale dvije stranice.
Neka je $d = 1$. Jer je $m^2 + n^2 \neq 21$, mora biti $m^2 - n^2 = (m-n)(m+n) = 15$. Odavde je $m - n = 1$, $m + n = 15$ ili $m - n = 3$, $m + n = 5$ što povlači da je $m = 11$, $n = 10$ ili $m = 5$, $n = 2$. Tada su Pitagorine trojke $(21, 220, 221)$ i $(21, 20, 29)$.
Neka je $d = 3$. Moguće je samo $m^2 - n^2 = 7$, što povlači da je $m = 4$, $n = 3$. Pitagorina trojka je $(21, 72, 75)$.
Ako je $d = 7$, moguć je samo slučaj $m^2 - n^2 = 3$ i tada je $m = 2$, $n = 1$. Pitagorina trojka je $(21, 28, 35)$.

Primjer 5 *Prikažimo tablicu prvih 20 primitivnih rješenja jednadžbe $x^2 + y^2 = z^2$ koristeći formulu (3).*

Rješenje:

m	n	x	y	z
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61
7	2	45	28	53
7	4	33	56	65
7	6	13	84	85
8	1	63	16	65
8	3	55	48	73
8	5	39	80	89
8	7	15	112	113
9	2	77	36	85
9	4	65	72	97
9	8	17	144	145
10	1	99	20	101
10	3	91	60	109

Tablica 1: *Prvih 20 primitivnih Pitagorinih trojki*

Sada ćemo promotriti rješenja jednadžbe (1) za koju su dva broja u nizu x, y, z uzastopni prirodni brojevi. Jasno je da su rješenja koja pripadaju ovoj klasi primitivna. Stoga je z neparan broj, pa $z - y = 1$ može biti samo ako je y paran. Prema tome, po formuli (2),

$$m^2 + n^2 - 2mn = z - y = 1,$$

ili ekvivalentno, $(m-n)^2 = 1$, budući da $m > n$, slijedi da je $m - n = 1$, tj. $m = n+1$. Dakle, $x = m^2 - n^2 = (n+1)^2 - n^2 = 2n+1$, $y = 2n(n+1)$, $z = y+1 = 2n(n+1)+1$. Tako su sva rješenja jednadžbe (1) u prirodnim brojevima x, y, z za $z - y = 1$ dana formulama

$$x = 2n+1,\ y = 2n(n+1),\ z = 2n(n+1)+1, \text{ za } n \in \mathbb{N}.$$

Primjer 6 *Navedimo prvih 5 Pitagorinih trojki za slučaj kada je $z - y = 1$.*

Rješenje:

N	x	y	z
1	3	4	5
2	5	12	13
3	7	24	25
4	9	40	41
5	11	60	61

Tablica 2: *Prvih 5 primitivnih Pitagorinih trojki za koje vrijedi $z - y = 1$*

Promotrimo sada slučaj ako za rješenja jednadžbe $x^2 + y^2 = z^2$ vrijedi $x \pm y = 1$. Jednostavno je dokazati da postoje beskonačno mnogo takvih rješenja. Ovo slijedi odmah iz činjenice da prirodni brojevi x i z zadovoljavaju jednakost $x^2 + (x+1)^2 = z^2$, a zatim $(3x+2z+1)^2 + (3x+2z+2)^2 = (4x+3z+2)^2$.

Lema 1 ([5, Chapter 2, Lemma.])
Ako prirodni brojevi x, z zadovoljavaju jednadžbu

$$x^2 + (x+1)^2 = z^2 \tag{4}$$

i $x > 3$, tada prirodni brojevi

$$x_o = 3x - 2z + 1 \tag{5}$$
$$z_o = 3z - 4x - 2 \tag{6}$$

zadovoljavaju jednadžbu

$$x_0^2 + (x_0+1)^2 = z_0^2 \tag{7}$$

i $z_0 < z$.

Dokaz: Uvrštavanjem (5) i (6) u jednadžbu (4) dobivamo:

$$x_0^2 + (x_0+1)^2 = 2x_0^2 + 2x_0 + 1 = 18x^2 + 8z^2 - 24xz + 18x - 12z + 5,$$
$$z_0^2 = 16x^2 + 9z^2 - 24xz + 16x - 12z + 4.$$

Ako izjednačimo desne strane predhodnih dviju jednadžbi, tj.

$$16x^2 + 9z^2 - 24xz + 16x - 12z + 4 = 8z^2 + 18x^2 - 24xz + 18x - 12z + 5$$

dobijemo $z^2 = 2x^2 + 2x + 1$ što znamo da vrijedi iz jednadžbe (4). Trebamo još pokazati da su x_0 i z_0 prirodni i da je $z_0 < z$. To je ekvivalentno dokazivanju da vrijedi

$$3x - 2z + 1 > 0 \quad \text{i} \quad 0 < 3z - 4x - 2 < z$$

tj. ekvivalentno tvrdnjama

$$2z < 3x + 1,\ 3z > 4x + 2 \quad \text{i} \quad z < 2x + 1.$$

Budući da je $x > 3$ slijedi da je

$$x^2 > 3x = 2x + x > 2x + 3.$$

Ako uvrstimo u jednadžbu (4) dobijemo

$$\begin{aligned} 4z^2 &= 8x^2 + 8x + 4 = 9x^2 + 8x + 4 - x^2 \\ &< 9x^2 + 8x + 4 - (2x + 3) \\ &= 9x^2 + 6x + 1 = (3x + 1)^2. \end{aligned}$$

To povlači da je $2z < 3x + 1$. Zbrajanjem te jednadžbe sa $x > 0$ dobivamo $2z < 4x + 1$; pa je i $z < 2x + 1$. Uvrštavanjem nejednakosti $x > 0$ u jednadžbu (4) dobijemo

$$9z^2 = 18x^2 + 18x + 9 > 16x^2 + 16x + 4 = (4x + 2)^2,$$

odakle je $3z > 4x + 2$. Time je tvrdnja leme dokazana. □

Primjer 7 *Pronađimo prvih nekoliko rješenja jednadžbe* $x^2 + (x + 1)^2 = z^2$.

Rješenje:
Prva takva trojka nam je već poznata, tj. $(x_1, y_1, z_1) = (3, 4, 5)$. Drugu trojku dobivamo na sljedeći način:

$$\begin{aligned} x_2 &= 3x_1 + 2z_1 + 1 = 3 \cdot 3 + 2 \cdot 5 + 1 = 20 \\ y_2 &= x_2 + 1 = 20 + 1 = 21 \\ z_2 &= 4x_1 + 3z_1 + 2 = 4 \cdot 3 + 3 \cdot 5 + 2 = 29. \end{aligned}$$

Lako se pokaže da (x_2, y_2, z_2) zadovoljavaju uvjete jednadžbe. Analogno dobijemo (x_3, y_3, z_3).

x	y	z
3	4	5
20	21	29
119	120	169
696	697	985

Tablica 3: *Prva 4 rješenja jednadžbe* $x^2 + (x + 1)^2 = z^2$

1.2 Jednadžba oblika $x^2 + y^2 + z^2 = t^2$

Pronaći ćemo sva prirodna rješenja jednadžbe

$$x^2 + y^2 + z^2 = t^2. \tag{8}$$

Najprije primjetimo da barem dva broja od brojeva x, y i z moraju biti parni. Pretpostavimo suprotno, tj. neka su sva tri broja x, y i z neparni. Tada je t^2 , koji je suma kvadrata brojeva x, y i z, broj oblika $8k + 3$. Dijeleći kvadrat svakog neparnog broja x, y, z sa 8 dobivamo ostatak 1. Ali primjenjujući tu činjenicu i na t^2 , koji je također kvadrat neparnog broja, dolazimo do kontradikcije. Ako je samo jedan od brojeva x, y i z paran tada bi zbroj $x^2 + y^2 + z^2 = t^2$ bio oblika $4k + 2$ što je nemoguće jer je kvadrat parnog broja oblika $4k$.
Pretpostavimo da su y i z parni, tj.

$$y = 2l,\ z = 2m,$$

gdje su $l, m \in \mathbb{N}$. Iz (8) vidimo da je $t > x$. Označimo $t - x = u$ koji je također prirodan broj. Uvrstimo li prethodne jednakosti u jednadžbu (8) imamo

$$(x + u)^2 = x^2 + 4l^2 + 4m^2,$$

iz čega sređvanjem dobivamo $2xu + u^2 = 4l^2 + 4m^2$ i dalje

$$u^2 = 4l^2 + 4m^2 - 2xu. \tag{9}$$

Vidimo da je desna strana jednakosti (9) suma parnih brojeva pa je zato i u^2 paran broj. Tada je u također paran. Uvrstimo sada $u = 2n$, $n \in \mathbb{N}$ u jednadžbu (9) i dobijemo

$$n^2 = l^2 + m^2 - nx.$$

Iz posljednje jednadžbe imamo

$$x = \frac{l^2 + m^2 - n^2}{n}. \tag{10}$$

Kako je $t - x = u$, slijedi

$$t = x + u = x + 2n = \frac{l^2 + m^2 + n^2}{n}.$$

Štoviše, budući da je x prirodni broj, iz (10) zaključujemo da je $n^2 < l^2 + m^2$. Dakle, sva rješenja jednadžbe (8) u prirodnim brojevima x, y, z, t, z, mogu se dobiti iz formula

$$x = \frac{l^2 + m^2 - n^2}{n},\ y = 2l,\ z = 2m,\ t = \frac{l^2 + m^2 + n^2}{n}, \tag{11}$$

gdje su $m, n \in \mathbb{N}$ i $n < \sqrt{l^2 + m^2}$.
Obratno, ako $l, m, n \in \mathbb{N}$ zadovoljavaju gore navedene uvjete, tada brojevi x, y, z, dobiveni iz (11) tvore rješenje jednadžbe (8) u prirodnim brojevima. To se može zaključiti iz (11). Kako bismo vidjeli da oni zadovoljavaju jednadžbu (8) koristimo identitet

$$\left(\frac{l^2 + m^2 - n^2}{n}\right)^2 + (2l)^2 + (2m)^2 = \left(\frac{l^2 + m^2 + n^2}{n}\right)^2.$$

Lako se pokaže da se svako rješenje jednadžbe (8) u prirodnim brojevima x, y, z, t dobiva točno jedanput pomoću formule (11). Po (11) imamo

$$l = \frac{y}{2},\ m = \frac{z}{2},\ n = \frac{t - x}{2}$$

te su tako brojevi l, m i n jedinstveno definirani pomoću brojeva x, y, z i t. Tako smo dokazali sljedeći teorem.

Teorem 2 ([3, Chapter 2.10, Theorem 5])
Sva rješenja jednadžbe

$$x^2 + y^2 + z^2 = t^2$$

u prirodnim brojevima x, y, z, t, gdje su y i z parni, dana su formulama

$$x = \frac{l^2 + m^2 - n^2}{n},\ y = 2l,\ z = 2m,\ t = \frac{l^2 + m^2 + n^2}{n}$$

gdje su l, m proizvoljni prirodni brojevi i $n | l^2 + m^2,\ n < \sqrt{l^2 + m^2}$.

Primjer 8 (Vidi [3])
Pronađimo prvih nekoliko rješenja jednadžbe $x^2 + y^2 + z^2 = t^2$ koristeći prethodnu formulu.

Rješenje: Neka je $l = m = 1$, tada je $l^2 + m^2 = 2$, kako po uvjetu teorema 2 $n | l^2 + m^2$, $n < \sqrt{l^2 + m^2}$ slijedi da je $n = 1$. Uvrštavanjem u formulu dobivamo:

$$x = \frac{l^2 + m^2 - n^2}{n} = \frac{1 + 1 - 1}{2} = 2$$
$$y = 2l = 2,\ z = 2m = 2$$
$$t = \frac{l^2 + m^2 + n^2}{n} = \frac{1 + 1 + 1}{3} = 3.$$

Prikažimo nekoliko rješenja u tablici:

l	m	l^2+m^2	n	x	y	z	t
1	1	2	1	1	2	2	3
2	2	8	1	7	4	4	9
3	1	10	1	9	6	2	11
3	1	10	2	3	6	2	7
3	3	18	1	17	6	6	19
3	3	18	2	7	6	6	11
3	3	18	3	3	6	6	9

Tablica 4: *Prvih 7 rješenja jednadžbe* $x^2+y^2+z^2=t^2$

Primjer 9 *Odredimo rješenje jednadžbe* $x^2+y^2+z^2=t^2$ *koristeći Teorem 2 ako je* $l=3$ *i* $m=4$.

Rješenje: Rješenje jednadžbe $x^2+y^2+z^2=t^2$ dobivamo iz formula

$$x=\frac{l^2+m^2-n^2}{n},\ y=2l,\ z=2m,\ t=\frac{l^2+m^2+n^2}{n}.$$

Za zadane $l=3$ i $m=4$ najprije izračunajmo n. Po Teoremu 2 imamo $n|3^2+4^2=25$ i $n<\sqrt{25}=5$ iz čega dobivamo $n=1$.
Sada uvrstimo brojeve $l=3, m=4$ i $n=1$ u formule (11). Dobijemo $x=24, y=6, z=8$ i $t=26$. Provjerimo još da brojevi $(x,y,z,t)=(24,6,8,26)$ zadovoljavaju jednadžbu (8). Zaista je $24^2+6^2+8^2=676=26^2$.

2 Pellovske jednadžbe

Jednadžbe su dobile ime po engleskom matematičaru Johnu Pellu, kojem je Euler, po svemu sudeći pogrešno, pripisao zasluge za njezino rješavanje. Neke pojedinačne jednadžbe ovog tipa nalaze se u tekstovima starogrčkih matematičara (Arhimed, Diofant), no prvi su ih sustavno proučavali srednjevjekovni indijski matematičari (Brahmagupta, Bhaskara II). Od europskih matematičara, metode za rješavanje Pellovih jednadžbi dali su Brouncher, Fermat, Euler i Lagrange.

2.1 Jednadžbe oblika $x^2-dy^2=\pm 1$

Definicija 4 *Diofantska jednadžba*

$$x^2-dy^2=1, \tag{12}$$

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

U ovom poglavlju promotrit ćemo i jednadžbu oblika

$$x^2-dy^2=-1 \tag{13}$$

koja se zove pellovska jednadžba. Općenitu definiciju takvih jednadžbi navest ćemo u idućem potpoglavlju.
Ako je d cijeli broj takav da je $d < 0$ ili je d potpun kvadrat, onda jednadžbe (12) i (13) imaju konačno mnogo rješenja, a to su $(x,y) = (1,0)$ za jednadžbu (12) i $(x,y) = (-1,0)$ za jednadžbu (13). Kao prvi korak u proučavanju Pellove jednadžbe, dokazat ćemo, koristeći Dirichletov teorem, da ona ima beskonačno mnogo rješenja u prirodnim brojevima.

Teorem 3 (Dirichletov teorem, [1, Teorem 6.1])
Neka su α i Q realni brojevi i $Q > 1$. Tada postoje cijeli brojevi p i q takvi da je $1 \leq q < Q$ i $||\alpha q|| = |\alpha q - p| \leq \frac{1}{Q}$.

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

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

Svi ovi brojevi leže na segmentu $[0,1]$. Podijelimo segment $[0,1]$ na Q disjunktnih podintervala duljine $1/Q$:

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

Prema Dirichletovom principu, barem jedan podinterval sadrži dva (ili više) od gornjih $Q+1$ brojeva. Uočimo da broj $\{r\alpha\}$ ima oblik $r\alpha - s, r, s \in \mathbb{Z}$, a brojevi 0 i 1 se također mogu zapisati u tom obliku (uz $r = 0$). Dakle, postoje cijeli brojevi r_1, r_2, s_1, s_2 takvi da je $0 \leq r_i < Q$, $i = 1,2$, $r_1 \neq r_2$ i da vrijedi $|(r_1\alpha - s_1) - (r_2\alpha - s_2)| \leq 1/Q$. Možemo pretpostaviti da je $r_1 > r_2$. Stavimo: $q = r_1 - r_2$, $p = s_1 - s_2$. Tada je $1 \leq q < Q$ i $|\alpha q - p| \leq 1/Q$, čime je tvrdnja teorema dokazana u slučaju $Q \in \mathbb{N}$. □

Lema 2 ([2, Lema 1.1]) *Neka je d prirodan broj koji nije potpun kvadrat. Tada postoji cijeli broj k, $|k| < 1 + 2\sqrt{d}$, sa svojstvom da jednadžba*

$$x^2 - dy^2 = k \tag{14}$$

ima beskonačno mnogo rješenja u prirodnim brojevima.

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

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

Za svaki takav par (x,y) vrijedi

$$|x + y\sqrt{d}| = |x - y\sqrt{d} + 2y\sqrt{d}| < \frac{1}{y} + 2y\sqrt{d} \leq (1 + 2\sqrt{d})y$$

pa je

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

Budući da parova (x, y) s navedenim svostvo ima beskonačno, a cijelih brojeva koji su po modulu manji od $1 + 2\sqrt{d}$ samo konačno, to postoji neki cijeli broj k, takav da je $|k| < 1 + 2\sqrt{d}$, za kojeg jednadžba (14) ima beskonačno mnogo rješenja. □

Teorem 4 ([2, Teorem 1.1])
Pellova jednadžba $x^2 - dy^2 = 1$ ima barem jedno rješenje u prirodnim brojevima x i y.

Dokaz:
Beskonačno mnogo rješenja jednadžbe (14) možemo podijeliti u k^2 klasa, stavljajući rješenja (x_1, y_1) i (x_2, y_2) u istu klasu akko je $x_1 \equiv x_2 \pmod{k}$ i $y_1 \equiv y_2 \pmod{k}$. Tada neka od tih klasa sadrži barem dva (u stvari beskonačno) različitih rješenja (x_1, y_1), (x_2, y_2). Stavimo

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

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

$$k = x_2^2 - dy_2^2 = x_2^2 - d\frac{x_2^2y_1^2}{x_1^2} = \frac{x_2^2}{x_1^2}(x_1^2 - dy_1^2) = \frac{x_2^2}{x_1^2}k,$$

tj. $x_1 = x_2$, što je u suprotnosti s pretpostavkom da su x_1 i x_2 različiti prirodni brojevi.
Imamo:

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

Definicija 5 *Za najmanji $x \in \mathbb{N}$ rješenje (x, y) u prirodnim brojevima Pellove jednadžbe* (12) *kažemo da je njezino fundamentalno rješenje i označavamo ga sa (x_1, y_1), a često i sa $x_1 + y_1\sqrt{d}$.*

Teorem 5 ([2, Teorem 1.2])
Pellova jednadžba $x^2 - dy^2 = 1$ ima beskonačno mnogo rješenja. Ako je (x_1, y_1) fundamentalno rješenje, onda su sva rješenja (u prirodnim brojevima) ove jednadžbe dana formulom

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n,\ n \in \mathbb{N}. \tag{15}$$

Dokaz:
Iz (15) slijedi $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$ pa je

$$x_n^2 - y_n^2d = (x_1^2 - y_1^2d)^n = 1$$

što znači da su (x_n, y_n) zaista rješenja. Pretpostavimo sada da je (s,t) rješenje koje se ne nalazi u familiji $\{(x_n, y_n) : n \in \mathbb{N}\}$. Budući da je $x_1 + y_1\sqrt{d} > 1 is + t\sqrt{d} > 1$, to postoji $m \in \mathbb{N}$ takav da je

$$(x_1 + y_1\sqrt{d})^m < s + t\sqrt{d} < (x_1 + y_1\sqrt{d})^{m+1}. \tag{16}$$

Pomnožimo li (16) sa $(x_1 - y_1\sqrt{d})^m$, dobivamo

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

Definirajmo $a, b \in \mathbb{Z}$ s $a + b\sqrt{d} = (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m$
Imamo $a^2 - db^2 = (s^2 - dt^2)(x_1^2 - y_1^2 d)^n = 1$. Iz $a + b\sqrt{d} > 1$ slijedi $0 < a - b\sqrt{d} < 1$, pa je $a > 0$ i $b > 0$. Stoga je (a, b) rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$ i $a + b\sqrt{d} < x_1 + y_1\sqrt{d}$, što je kontradikcija. □

Primjer 10 *Odredimo sva cjelobrojna rješenja jednadžbe* $x^2 - 7y^2 = 1$.

Rješenje: Fundamentalno rješenje jednadžbe $x^2 - 7y^2 = 1$ je $8 - 3\sqrt{7}$, tj. $(x_1, y_1) = (8, 3)$. Tada su prema Teoremu 5 sva rješenja jednadžbe $x^2 - 7y^2 = 1$ dana formulom $x_n + y_n\sqrt{7} = (8 + 3\sqrt{7})^n$, $n \in \mathbb{N}$.

U nastavku ćemo reći nešto o jednadžbi (13) i njezinom rješenju. Za razliku od obične Pellove jednadžbe (12), jednadžba (13) ne mora imati rješenja u cijelim brojevima. Ako jednadžba (13) ima rješenja, onda najmanje njezino rješenje u prirodnim brojevima također zovemo fundamentalno rješenje.

Teorem 6 ([2,Teorem 1.3])
Pretpostavimo da jednadžba $x^2 - dy^2 = -1$ *ima rješenja, te da joj je* $x_1 + y_1\sqrt{d}$ *fundamentalno rješenje. Tada je* $(x_1 + y_1\sqrt{d})^2$ *fundamentalno rješenje jednadžbe* $x^2 - dy^2 = 1$. *Ako definiramo* $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$, *tada su* $x_{2n} + y_{2n}\sqrt{d}$ *sva rješenja jednadžbe* $x^2 - dy^2 = 1$, *a* $x_{2n+1} + y_{2n+1}\sqrt{d}$ *sva rješenja jednandžbe* $x^2 - dy^2 = -1$ *u prirodnim brojevima.*

Dokaz:
Imamo

$$x_n - y_n\sqrt{d} = (x_1 - y1\sqrt{d})^n,$$

pa je

$$x_n^2 - y_n^2 d = (x_1^2 - y_1^2 d)^n = (-1)^n.$$

Dakle, zaista je $x_{2n} + y_{2n}\sqrt{d}$ rješenje od $x^2 - dy^2 = 1$, a $x_{2n+1} + y_{2n+1}\sqrt{d}$ rješenje od $x^2 - y^2 = -1$. Pretpostavimo da za fundamentalno rješenje $a + b\sqrt{d}$ jednadžbe (12) vrijedi

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

Iz $(x_1 + y_1\sqrt{d})(-x_1 + y_1\sqrt{d}) = 1$, slijedi da $0 < (-x_1 + y_1\sqrt{d}) < 1$. Stoga je

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

gdje je $s = -ax_1 + dby_1$, $t = ay_1 - bx_1$ i vrijedi $s^2 - dt^2 = -1$. Zbog $s + t\sqrt{d} > 0$ i $s - t\sqrt{d} < 0$, jasno je da je $t > 0$. Ako je $s < 0$, onda iz $-x_1 + y_1\sqrt{d} < s + t\sqrt{d}$ dobivamo $x_1 + y_1\sqrt{d} > -s + t\sqrt{d}$. Prema tome, zaključujemo da je $|s| + t\sqrt{d}$ rješenje od (12), koje je manje od fundamentalnog, što je kontradikcija. Pretpostavimo sada da je $u + v\sqrt{d}$ neko rješenje od (13) koje nije sadržano u nizu $(x_{2n+1} + y_{2n+1}\sqrt{d})$. Tada postoji $m \in \mathbb{N}$ takav da je

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

Množeći ove nejednakosti sa $(x_1 - y_1\sqrt{d})^{2n}$ dobivamo

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

gdje je $\sigma^2 - d\tau^2 = -1$. No takvi σ, τ ne mogu postojati. □

Propozicija 1 ([2, Propozicija 1.2])
Ako je p prost broj i $p \equiv 1 \pmod 4$, *onda jednažba* $x^2 - py^2 = -1$ *ima rješenja.*

Dokaz:
Neka je (x_1, y_1) fundamentalno rješenje jednadžbe $x^2 - py^2 = 1$. Tada je $x_1^2 - y_1^2 \equiv 1 \pmod 4$, pa je x_1 neparan, a y_1 paran. Iz

$$\frac{x_1 - 1}{2} \cdot \frac{x_1 + 1}{2} = p\left(\frac{y_1}{2}\right)^2, \ \left(\frac{x_1 - 2}{2}, \frac{x_1 + 1}{2}\right) = 1$$

slijedi da postoje $u, v \in \mathbb{N}$ takvi da je

$$\frac{x_1 \pm 1}{2} = pu^2, \ \ \frac{x_1 \mp 1}{2} = v^2 \ \ \frac{y_1}{2} = uv.$$

Odavde je $v^2 - pu^2 = \mp 1$. No, iz $u < y_1$ i minimalnosti od (x_1, y_1), slijedi da ovdje ne možemo imati predznak $+$, tj da vrijedi $v^2 - pu^2 = -1$. Uočimo da je po Teoremu 6, $u + v\sqrt{p}$ fundamentalno rješenje od $x^2 - py^2 = -1$ i vrijedi

$$(u + v\sqrt{p})^2 = u^2 + pv^2 + 2uv\sqrt{p} = x_1 + y_1\sqrt{dp}.$$

□

Primjer 11 ([2, Primjer 1.1])
Pokažimo da jednadžba $x^2 - 34y^2 = -1$ *nema pozitivnih cjelobrojnih rješenja.*

Rješenje:
Fundamentalno rješenje $x^2 - 34y^2 = 1$ je $35 + 6\sqrt{34}$. Ako bi ova jednadžba bila rješiva, za njezino fundamentalno rješenje $x_1 + y_1\sqrt{34}$, pi po Teoremu 6, trebalo vrijediti

$$x_1^2 + 34y_1^2 = 35, \ \ 2x_1y_1 = 6.$$

Iz druge jednadžbe sustava, $2x_1y_1 = 6$, slijedi da su jedina moguća rješenja sustava $(x_1, y_1) = (1, 3)$ i $(x_1, y_1) = (3, 1)$, no ta rješenja ne zadovoljavaju prvu jednadžbu sustava, pa sustav nema rješenja.

Primjer 12 *Odredimo sva cjelobrojna rješenja jednadžbi* $x^2 - 13y^2 = \pm 1$.

Rješenje: Fundamentalno rješenje jednadžbe $x^2 - 13y^2 = -1$ je $18 + 5\sqrt{13}$. Po Teoremu 6 je tada $(18 + 5\sqrt{13})^2 = 649 + 180\sqrt{13}$ fundamentalno rješenje jednadžbe $x^2 - 13y^2 = 1$. Sva cjelobrojna rješenja jednadžbi $x^2 - 13y^2 = \pm 1$ dana su sa

$$x_n + y_n\sqrt{13} = (18 + 5\sqrt{13})^n.$$

Prema Teoremu 6, za parni n dobivamo rješenja jednadžbe $x^2 - 13y^2 = 1$, dok za neparni n slijede rješenja jednadžbe $x^2 - 13y^2 = -1$.

2.2 Pellove jednadžbe i verižni razlomci

Jedan relativno efikasan algoritam za nalaženje fundamentalog rješenja Pellovih jednadžbi dobit ćemo iz njihove veze s diofantskim aproksimacijama, te preko njih s verižnim razlomcima.

Neka je α proizvoljan realan broj. Stavimo: $a_0 = \lfloor \alpha \rfloor$. Ako je $a_0 \neq \alpha$ onda zapišimo α u obliku $\alpha = a_0 + \frac{1}{\alpha_1}$ tako da je $\alpha_1 > 1$ i stavimo $a_1 = \lfloor \alpha_1 \rfloor$. Ako je $a_1 \neq \alpha_1$, onda α_1 zapišimo u obliku $\alpha_1 = a_1 + \frac{1}{\alpha_2}$ tako da je $\alpha_2 > 1$ i stavimo $a_2 = \lfloor \alpha_2 \rfloor$. Ovaj proces možemo nastaviti u nedogled, ukoliko nije $a_n = \alpha_n$ za neki n. Jasno je da ako je $a_n = \alpha_n$ za neki n, onda je α racionalan broj. Naime, tada je

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

Ovo ćemo kraće zapisivati u obliku $\alpha = [a_0, a_1, \ldots, a_n]$. Pretpostavimo sada da je $a_n \neq \alpha_n$ za sve prirodne brojeve n. Definirajmo racionalne brojeve $\frac{p_n}{q_n}$ sa

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

Definicija 6 *Ako je a_0 cijeli broj, $a_1, \ldots, a_n$ prirodni brojevi te ako je $\alpha = [a_0, a_1 \ldots, a_n]$, onda ovaj izraz zovemo razvoj broja α u konačni jednostavni verižni (neprekidni) razlomak.*
Broj $\frac{p_i}{q_i} = [a_0, a_1, \ldots, a_i]$ je i-ta konvergenta od α, a_i je i-ti parcijalni kvocijent od α, a $\alpha_i = [a_i, a_{i+1}, \ldots, a_n]$ je i-ti potpuni kvocijent od α. Ako je α iracionalan broj, onda uvodimo oznaku $\lim_{n\to\infty}[a_0, a_1, \ldots, a_n] = [a_0, a_1, a_2, \ldots]$. Ako je $\alpha = [a_0, a_1, a_2, \ldots]$, onda ovaj izraz zovemo razvoj od α u (beskonačni) jednostavni verižni razlomak. Broj $\frac{p_i}{q_i} = [a_0, a_1, \ldots, a_i]$ je i-ta konvergenta od α, a_i je i-ti parcijalni kvocijent od α, a $\alpha_i = [a_i, a_{i+1}, \ldots]$ je i-ti potpuni kvocijent od α.

Brojnici i nazivnici konvergenti zadovoljavaju sljedeće rekurzije:

$$\begin{aligned} p_{n+2} &= a_{n+2} + p_{n+1} + p_n \\ p_0 &= a_0 \\ p_1 &= a_0 a_1 + 1, \quad p_{-1} = 1, p_{-2} = 0 \\ q &= a_{n+2} q_{n+1} + q_n \\ q_0 &= 1,\ q_1 = a_1, \quad q_{-1} = 0, q_{-2} = 1. \end{aligned}$$

Može se pokazati da za svako rješenje Pellove jednadžbe $x^2 - dy^2 = 1$ vrijedi da je $\frac{x}{y}$ neka konvergenta u razvoju od $\sqrt{d}$ u verižni razlomak (vidi [1, 2]). Broj $\sqrt{d}$ je kvadratna iracionalnost, pa mu je razvoj periodičan i ima razvoj oblika $\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{l-1}, 2a_0}]$ gdje je $a_0 = \lfloor \sqrt{d} \rfloor$. Također vrijedi tzv. palindromno svojstvo, tj. $a_1 = a_{l-1},\ a_2 = a_{l-2}$.

Sada ćemo navesti algoritam za razvoj kvadratnih iracionalnosti u verižni razlomak. Neka je α kvadratna iracionalnost. Prikažimo je u obliku $\alpha = \frac{s_0 + \sqrt{d}}{t_0}$, gdje su $d, s_0, t_0 \in \mathbb{Z}, t_0 \neq 0,\ d$ nije potpun kvadrat i $t_0 | (d - s_0^2)$. Ako je $\alpha = \sqrt{d}$ onda je $s_0 = 0,\ t_0 = 1$. Sada brojeve a_i računamo rekurzivno na sljedeći način

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

Uočimo da, iako je α iracionalan broj, ovaj algoritam radi samo s cijelim brojevima.

Primjer 13 *Odredimo razvoj sljedećih kvadratnih iracionalnosti u verižni razlomak:*
a) $\sqrt{31}$
b) $(1 + \sqrt{3})/2$

Rješenje: a) Za razvoj broja $\sqrt{31}$ u verižni razlomak koristit ćemo gore navedenu rekurziju.
$a_0 = \lfloor \sqrt{31} \rfloor = 5,$
$s_1 = 5 * 1 - 0 = 5,\ t_1 = \frac{31-25}{1} = 6,\ a_1 = \lfloor \frac{5+5}{6} \rfloor = 1,$
$s_2 = 1 * 6 - 5 = 1,\ t_2 = \frac{31-1}{6} = 5,\ a_2 = \lfloor \frac{1+5}{5} \rfloor = 1,$
$s_3 = 5 - 1 = 4,\ t_3 = \frac{31-16}{5} = 3,\ a_3 = \lfloor \frac{4+5}{3} \rfloor = 3,$
$s_4 = 9 - 4 = 5,\ t_4 = \frac{31-25}{3} = 2,\ a_4 = \lfloor \frac{5+5}{2} \rfloor = 5,$
$s_5 = 10 - 5 = 5,\ t_5 = \frac{31-25}{2} = 3,\ a_5 = \lfloor \frac{5+5}{3} \rfloor = 3,$
$s_6 = 9 - 5 = 4,\ t_6 = \frac{31-16}{3} = 5,\ a_6 = \lfloor \frac{4+3}{5} \rfloor = 1,$
$s_7 = 5 - 4 = 1,\ t_7 = \frac{31-1}{5} = 6,\ a_7 = \lfloor \frac{1+5}{6} \rfloor = 1,$
$s_8 = 6 - 1 = 5,\ t_8 = \frac{31-25}{6} = 1,\ a_8 = \lfloor \frac{5+5}{1} \rfloor = 10,$
$s_9 = 10 - 5 = 5,\ t_9 = \frac{31-25}{1} = 6,\ a_9 = \lfloor \frac{5+5}{6} \rfloor = 1.$
Dakle, $\sqrt{31} = [5; \overline{1, 1, 3, 5, 3, 1, 1, 10}]$.
b) Za razvoj broja $\frac{1+\sqrt{3}}{2}$ koristit ćemo gore navedenu rekurziju.
Imamo $\alpha = \frac{s_0 + \sqrt{d}}{t_0} = \frac{1+\sqrt{3}}{2}$ pa je $d = 3, s_0 = 1$ i $t_0 = 2$. Slijedi da je $a_0 = \lfloor \frac{1+\sqrt{3}}{2} \rfloor = 1,$
$s_1 = 1 * 2 - 1 = 1,\ t_1 = \frac{3-1}{2} = 1,\ a_1 = \lfloor \frac{1+1}{1} \rfloor = 2,$
$s_2 = 2 * 1 - 1 = 1,\ t_2 = \frac{3-1}{1} = 2,\ a_2 = \lfloor \frac{1+2}{2} \rfloor = 1,$

$s_3 = 1 * 2 - 1 = 1$, $t_3 = \frac{3-1}{2} = 1$, $a_3 = \lfloor \frac{1+1}{1} \rfloor = 2$.
Dakle, $\frac{1+\sqrt{3}}{2} = [1; \overline{2,1}]$.
Pokazuje se da su nizovi (s_i) i (t_i) ograničeni. Preciznije, dobije se da za dovoljno velike indekse i vrijedi $0 < s_i < \sqrt{d}$, $0 < t_i < s_i + \sqrt{d} < 2\sqrt{d}$. Na taj način se upravo i zaključuje da razvoj mora biti periodičan. Odavde direktno dobivamo ocjenu za duljinu perioda u razvoju od $\sqrt{d}$, tj. $l(d) < \sqrt{d} \cdot 2\sqrt{d} = 2d$. Preciznijom analizom odnosa između s_i i t_i (posebno kongruencije $s_i^2 \equiv d (\mathrm{mod}\ t_i)$), dobije se ocjena $l(d) = O(\sqrt{d}\ln d$.
Izjednačavanjem racionalnih i iracionalnih dijelova u jednakosti

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

dobiva se relacija

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

Ona nam pokazuje da rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ odgovaraju onim n-ovima za koje je $(-1)^{n+1} t_{n+1} = 1$. Nije teško za vidjeti da je $t_i = 1$ ako i samo ako $l | i$ (l je duljina perioda). Zato vrijedi

Teorem 7 ([2, Teorem 1.7]) *Neka je l duljina perioda u razvoju od $\sqrt{d}$. Ako je l paran, onda jednadžba $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja od $x^2 - dy^2 = 1$ su dana sa $(x, y) = (p_{nl-1}, q_{nl-1}), n \in \mathbb{N}$. Posebno, fundamentalno rješenje je (p_{l-1}, q_{l-1}). Ako je l neparan, onda su sva rješenja jednadžbe $x^2 - dy^2 = -1$ dana sa $(x, y) = (p_{(2n-1)l-1}, q_{(2n-1)l-1})$, a sva rješenja jednadžbe $x^2 - dy^2 = 1$ sa $(x, y) = (p_{2nl-1}, q_{2nl-1}), n \in \mathbb{N}$. Posebno, fundamentalno rješenje od $x^2 - dy^2 = 1$ je (p_{2l-1}, q_{2l-1}).*

Primjer 14 *Nadite 2 najmanja rješenja u prirodnim brojevima jednadžbe $x^2 - 31y^2 = \pm 1$.*

Rješenje:
Razvojem broja $\sqrt{31}$ u verižni razlomak, koji smo pokazali u prethodnom primjeru, dobili smo $\sqrt{31} = [5; \overline{1,1,3,5,3,1,1,10}]$. Period $l = 8$ je paran pa po Teoremu 7 jednadžba $x^2 - 31y^2 = -1$ nema rješenja, a najmanje rješenje od jednadžbe $x^2 - 31y^2 = 1$ dano je sa $(x_1, y_1) = (p_7, q_7)$, $(x_2, y_2) = (p_15, q_15)$.

n	-1	0	1	2	3	4	5	6	7	8	9	10	11
a_n		5	1	1	3	5	3	1	1	10	1	1	3
p_n	1	5	6	11	39	206	657	863	1520	16063	17583	33646	118521
q_n	0	1	1	2	7	37	118	155	273	2885	3158	6043	21287

n	12	13	14	15
a_n	5	3	1	1
p_n	626251	3876027	4502278	8378305
q_n	112478	358721	471199	829920

Dakle, $(x_1, y_1) = (p_7, q_7) = (1520, 273), (x_2, y_2) = (p_15, q_15) = (8378305, 829920)$.

2.3 Jednadžbe oblika $x^2 - dy^2 = N$

Diofantska jednadžba oblika

$$x^2 - dy^2 = N, \tag{17}$$

gdje je d prirodan broj koji nije potpun kvadrat i N cijeli broj različit od 0, naziva se pellovska jednadžba. Jasno je da ovakva jednadžba ne mora imati cjelobrojnih rješenja. No, ukoliko ima barem jedno rješenje, onda ih ima beskonačno mnogo. Zaista, ako je $x + y\sqrt{d}$ rjšenje jednadžbe (17), a $u + v\sqrt{d}$ rješenje pripadne Pellove jednadžbe $x^2 - dy^2 = 1$, onda je

$$(x + y\sqrt{d})(u + v\sqrt{d}) = (ux + dvy)(uy + vx)\sqrt{d} \tag{18}$$

takoder rješenje jednadžbe (17), jer je

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

Budući da Pellova jednadžba ima beskonačno mnogo rješenja, to iz (18) slijedi da i jednadžba (17) ima beskonačno rješenja (uz pretpostavku da ima barem jedno). Za dva rješenja $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ jednadžbe (17) kažemo da su asocirana ako se jedno iz drugog može dobiti množenjem s nekim rješenjem Pellove jednadžbe kao u formuli (18). Lako se provjerava da je na ovaj način uvedena relacija ekvivalencije na skupu svih rješenja jednadžbe (17) (podsjetimo se da je $(u + v\sqrt{d})^{-1} = u - v\sqrt{d}$, što povlači simetričnost). Reći ćemo da međusobno asocirana rješenja tvore jednu klasu rješenja. Nije teško za vidjeti da su $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ asocirani ako i samo ako vrijedi $xx' \equiv dyy' \pmod{N}$, $xy' \equiv x'y \pmod{N}$.
Neka je **K** jedna klasa rješenja, te neka su njeni elementi $x_i + y_i\sqrt{d}$, $i = 1, 2, 3, \ldots$. Tada klasu koja se sastoji od rješenja $x_i - y_i\sqrt{d}$ označavamo s $\overline{\mathbf{K}}$ i kažemo da je konjugirana klasi **K**. Ako vrijedi da je $\mathbf{K} = \overline{\mathbf{K}}$, onda kažemo da je klasa **K** dvoznačna. Među svim elementima klase **K** odabrat ćemo jedan, $x^* + y^*\sqrt{d}$, kojeg ćemo zvati fundamentalno rješenje jednadžbe $x^2 - dy^2 = N$ u klasi **K**. Biramo ga tako da y^* poprimi najmanju moguću nenegativnu vrijednost medu svim elementima $x + y\sqrt{d}$ u klasi **K**. Ovim je zahtjevom i x^* jednoznačno određen, osim u slučaju kada je **K** dvoznačna. Ako je **K** dvoznačna, onda izabiremo x^* tako da zadovolji i dodatni uvjet da je $x^* \geq 0$. Uočimo da $|x^*|$ poprima najmanju moguću vrijednost unutar klase **K**.
Sada ćemo navesti teorem koji nam govori kako odrediti fundamentalno rješenje jednadžbe (17).

Teorem 8 ([2, Teorem 1.8])
Neka je $u + v\sqrt{d}$ fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$. Tada za svako fundamentalno rješenje $x^* + y^*\sqrt{d}$ jednadžbe $x^2 - dy^2 = N$ vrijede nejednakosti:

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

gdje je $\varepsilon = 1$ ako je $N > 0$, a $\varepsilon = -1$ ako je $N < 0$. Posebno, fundamentalnih (pa i klasa rješenja) ima konačno mnogo.

Dokaz:
Dokazat ćemo tvrdnju za $N < 0$. Dokaz za $N > 0$ je analogan. Definirajmo cijele brojeve x', y' sa $x' + y'\sqrt{d} = (x^* + y^*\sqrt{d})(u + \delta v\sqrt{d})$, gdje je $\delta = 1$ ako je $x^* \leq 0$, a $\delta = -1$ ako je $x^* < 0$. Tada $x' + y'\sqrt{d}$ pripada istoj klasi kao i $x^* + y^*\sqrt{d}$, pa zbog minimalnosti od y^* zaključujemo da je

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

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

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

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

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

□

Propozicija 2 ([2, Propozicija 1.4])
Pretpostavimo da je $|N| < \sqrt{d}$. Ako je $x + y\sqrt{d}$ rješenje jednadžbe $x^2 - dy^2 = N$, onda je $\frac{x}{y}$ neka konvergenta u razvoju u verižni razlomak od $\sqrt{d}$.

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

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

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

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

Zaključujemo da je $\frac{y}{x}$ neka konvergenta od $\frac{1}{\sqrt{d}}$. No ako je $\frac{y}{x}$ i-ta konvergenta od $\frac{1}{\sqrt{d}}$, onda je $\frac{x}{y}$ $(i-1)$-va konvergenta od $\sqrt{d}$. □

Primjer 15 *Odredimo sva cjelobrojna rješenja jednadžbe $x^2 - 13y^2 = 4$.*

Rješenje: Prema Primjeru 11 fundamentalno rješenje jednadžbe $x^2 - 13y^2 = 1$ je $649 + 180\sqrt{13}$. Tada po Teoremu 8 za svako fundamentalno rješenje $x^* + y^*\sqrt{13}$ jednadžbe $x^2 - 13y^2 = 4$ vrijede nejednakosti:

$$0 \leq y^* \leq \frac{180}{\sqrt{2(649+1)}}\sqrt{|4|} \leq 9,\ |x^*| \leq \sqrt{\frac{1}{2}(649+1)|4|} \leq 25.$$

Jedina rješenja koja zadovoljavaju te nejednakosti su $11+3\sqrt{13}$ i $-11+3\sqrt{13}$. Sva rješenja su dana sa

$$x+y\sqrt{13}=\pm(11+3\sqrt{13})(649+180\sqrt{13})^n$$

i

$$x+y\sqrt{13}=\pm(-11+3\sqrt{13})(649+180\sqrt{13})^n,$$

gdje je n cijeli broj.

Literatura

[1] A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu, skripta.

[2] A. Dujella, *Diofantske jednadžbe*, dostupno na `https://web.math.pmf.unizg.hr/~duje/dioph/dioph.pdf`

[3] W. Sierpinski, *Elementay theory of numbers*, North-Holland, Amsterdam, 1988.

[4] G.H. Hardy, E.M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, 1960.

[5] K. Irleand, M. Rosen, *A classical introduction to modern number theory*, Springer science+business media, LLC, 1990.