Fermatova četvorka

Čupić, Lovro

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Lovro Čupić

FERMATOVA čETVORKA

Diplomski rad

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. _____

Posvetu želim razdvojiti na dva dijela:

Svojim dragim roditeljima, što su me bezuvjetno trpili svih ovih godina,

i Luciji Zoretić.

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

Čovjek kojega danas zovemo ocem algebre, Diofant iz Aleksandrije (3. st.), u jednomu od povijesno najznačajnijih matematičkih udžbenika, *Aritmetici*, navodi zadatak: „Nađi četiri broja sa svojstvom da produkt svaka dva među njima uvećan za 1 daje kvadrat“. Iako ovaj zadatak i za današnje pojmove uopće nije jednostavan, on je takve brojeve uspio pronaći. Zato skup od m različitih prirodnih brojeva sa svojstvom da produkt svaka dva među njima uvećan za jedan daje kvadrat prirodnog broja danas nosi ime *Diofantova m-torka*. Sustavno proučavanje takvih skupova nastupilo je, u skladu s napretkom matematičke misli i poboljšanja notacije, tek mnogo nakon Diofantove ere. Dvojica matematičara čija imena često susrećemo, Leonhard Euler i Pierre de Fermat, gorljivo su se zanimali za takve skupove i mnogo vremena posvetili traženju što većeg diofantskog skupa, što se često svodilo na problem proširenja nekog od poznatih skupova. Fermat je pronašao da broj 120 nadopunjuje Diofantovu trojku $\{1, 3, 8\}$ do Diofantove četvorke. Zato taj skup, $\{1, 3, 8, 120\}$, danas zovemo *Fermatova četvorka*.

Što se tiče petorki, tek nedavno je dokazano da cjelobrojna Diofantova petorka ne postoji. Jedan od matematičara koji su ostavili značajan trag u utiranju puta prema tom teškom dokazu je i naš akademik Andrej Dujella, koji je dokazao da petorki ima samo konačno mnogo te da šestorka ne postoji. Pitanje proširenja usko je vezano za sustave pelovskih jednadžbi. U našem primjeru Fermatove trojke, ako je d broj koji proširuje skup $\{1, 3, 8\}$ u $\{1, 3, 8, d\}$ tako da Diofantovo svojstvo ostane zadržano, imamo:

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

odakle eliminacijom parametra d dolazimo do sustava tzv. pelovskih jednadžbi sa zajedničkom nepoznanicom x:

$$y^2 - 3x^2 = -2,\ z^2 - 8x^2 = -7.$$

Svaku od jednadžbi tog sustava možemo riješiti zasebno i rješenja u x predstaviti kao nizove. Želimo naći zajedničke elemente ovih nizova, za što je nužno pronaći (po mogućnosti, što bolje) ograde na veličine pripadnih indeksa. Tim problemom pozabavili su se Harold

Davenport i Alan Baker 1969. godine primjenjujući teoriju tzv. linearnih formi u logaritmima i algoritamsku metodu koju danas znamo kao Baker – Davenportovu redukciju. Ne ulazeći u potankosti oko svih rezultata koji su prethodili konačnom rješenju ovog problema, u ovom diplomskom radu opisujemo dokaz jedinstvenosti proširenja Fermatove četvorke prema radu Bakera i Davenporta iz 1969. ([1]).

Rad započinjemo detaljnim razmatranjem Pellove i pelovske jednadžbe, njihove rješivosti te opisujemo skup svih rješenja (ako rješenje postoji). Zanimljivo je da se rješenja nekih diofantskih jednadžbi (konkretno, pelovskih) mogu dovesti u vezu s linearnim formama u logaritmima algebarskih brojeva. Baker je 60-tih godina prošlog stoljeća razvio teoriju prema kojoj takve linearne forme ne mogu biti jako blizu nuli te našao djelotvornu donju ogradu za njih. Ti su se rezultati postupno poboljšavali u desetljećima koja su uslijedila, a mi smo za rješavanje sustava pelovskih jednadžbi primijenili Baker-Wüstholzov teorem iz 1993.

Iako je naš početni problem, proširenje Diofantovog skupa $\{1, 3, 8\}$, jednostavan za postaviti i razumjeti, njegovo rješavanje zadire u teška i ozbiljna područja teorije brojeva. U radu smo pokušali navesti, a djelomično i dokazati, sve što je potrebno za njegovo rješavanje.

Zahvaljujem mentorici Zrinki Franušić na brižnoj strpljivosti, gotovo nadnaravnoj ljubaznosti i sveopćoj susretljivosti u pripremi ovog rada koji bi, uskraćen njezinih bogatih doprinosa u sadržajnom, tehničkom i organizacijskom pogledu, zasigurno završio u plavom kontejneru za reciklažu.

Moram zahvaliti profesoru Andreju Dujelli na izvanrednom udžbeniku *Teorija brojeva*, kojim sam se iscrpno služio u stvaranju ovog rada.

Zahvalio bih i kolegici Maji Dravec na podsjetniku o formalnostima vezanim za prijavu termina diplomskog ispita.

Posljednju zahvalu, na značajnoj moralnoj podršci u trenucima kada su razlozi za optimizam bili sve, samo ne i očiti, upućujem kolegi Lovri Sindičiću.

Poglavlje 1

Pelovske jednadžbe

1.1 Pellova jednadžba

Između brojevnih skupova, najdulju povijest imaju prirodni, a zatim cijeli brojevi. Posljedično tome, jednadžbe u kojima se traže cjelobrojna rješenja neizostavan su predmet izučavanja svakoj generaciji matematičara. Prije nego se i sami uhvatimo u koštac s jednom klasom takvih jednadžbi (konkretno, pelovskom), navodimo rezultat njemačkog matematičara Dirichleta, koji će biti važan za egzistenciju rješenja tih jednadžbi. Oznaka $\|\alpha\|$ predstavlja udaljenost od α do najbližeg cijelog broja, tj. $\|\alpha\| = \min\{|\alpha - n| \ : \ n \in \mathbb{Z}\}$.

Teorem 1.1.1 (Dirichlet, 1842.)**.** *Neka su α i Q realni brojevi i $Q > 1$. Tada postoje cijeli brojevi p, q takvi da je $1 \leq q \leq Q$ i $\|\alpha q\| = |\alpha q - p| \leq \frac{1}{Q}$.*

Dokaz. Prvo ćemo dokazati tvrdnju kada je Q prirodan. Promotrimo sljedećih $Q + 1$ brojeva:

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

Svi ovi brojevi leže u segmentu $[0, 1]$ i imaju oblik $r\alpha - s$, za neke cijele brojeve r i s ($0 = 0 \cdot \alpha - 0, 1 = 0 \cdot \alpha - (-1), \{k\alpha\} = k\alpha - \lfloor k\alpha \rfloor$). Podijelimo segment $[0, 1]$ na Q disjunktnih podintervala duljine $\dfrac{1}{Q}$:

$$[0, \frac{1}{Q}\rangle, \ [\frac{1}{Q}, \frac{2}{Q}\rangle, \ \ldots \ , [\frac{Q-1}{Q}, 1].$$

Prema Dirichletovu principu, budući da imamo više brojeva nego podintervala, barem jedan podinterval sadržava dva ili više od gornjih $Q + 1$ brojeva. Uočimo da ta dva broja ne mogu biti 0 i 1. Stoga postoje cijeli brojevi r_1, r_2, s_1, s_2 takvi da je $0 \leq r_i \leq Q$, $i = 1, 2$, $r_1 \neq r_2$ i da vrijedi

$$|(r_1\alpha - s_1) - (r_2\alpha - s_2)| \leq \frac{1}{Q}.$$

Možemo pretpostaviti da je $r_1 > r_2$. Stavimo: $q = r_1 - r_2, p = s_1 - s_2$. Tada je $1 \leq q \leq Q$ i $|\alpha q - p| \leq \frac{1}{Q}$, čime je tvrdnja teorema dokazana u slučaju $Q \in \mathbb{N}$.

Pretpostavimo sada da Q nije prirodan broj. Neka je $Q' = \lfloor Q \rfloor + 1$. Prema već dokazanom, postoje cijeli brojevi p, q takvi da je $1 \leq q \leq Q'$ i $|\alpha q - p| \leq \frac{1}{Q'}$. No sada je $|\alpha q - p| < \frac{1}{Q}$, a $1 \leq q < Q'$ povlači da je $1 \leq q \leq \lfloor Q \rfloor < Q$. □

Korolar 1.1.2. *Ako je α iracionalan, onda postoji beskonačno mnogo parova p, q relativno prostih cijelih brojeva takvih da je*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{1.1}$$

Dokaz. Tvrdnja Teorema 1.1.1 očito vrijedi i ako zahtijevamo da su p i q relativno prosti (uvjeti na p i q ostaju zadovoljeni i nakon dijeljenja njihovim zajedničkim faktorom). Dakle, za $Q > 1$ postoje relativno prosti cijeli brojevi p, q takvi da je

$$|\alpha - \frac{p}{q}| \leq \frac{1}{Qq} < \frac{1}{q^2}.$$

Budući da je α iracionalan, to je $\alpha q - p \neq 0$.

Pretpostavimo da postoji samo konačno mnogo racionalnih brojeva $\frac{p}{q}$ koji zadovoljavaju (1.1). Neka su to brojevi $\frac{p_j}{q_j}, j = 1, \ldots, n$. Izaberimo prirodni broj m tako da je $\frac{1}{m} < |\alpha q_j - p_j|$ za sve za sve $j = 1, \ldots, n$. Primijenimo li Teorem 1.1.1 uz $Q = m$, dobivamo racionalni broj $\frac{p}{q}$ koji zadovoljava (1.1) i za koji vrijedi $|\alpha q - p| \leq \frac{1}{m}$. Prema tome, $\frac{p}{q}$ različit je od $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$, što je kontradikcija. □

Napomena 1.1.3. *Tvrdnja Korolara 1.1.2 ne vrijedi ako je α racionalan. Neka je $\alpha = \frac{u}{v}$. Ako je $\frac{p}{q} \neq \alpha$, onda je*

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{u}{v} - \frac{p}{q}\right| = \left|\frac{uq - vp}{vq}\right| \geq \frac{1}{vq},$$

pa (1.1) *povlači da je $q < v$, dok je p jednoznačno određen s q kao najbliži cijeli broj od αq. To znači da* (1.1) *može biti zadovoljen samo za konačno mnogo parova p, q relativno prostih cijelih brojeva.*

Općenito, potreba aproksimiranja realnih brojeva racionalnim brojevima malih nazivnika prirodno se javlja u svakodnevici, primjerice, pri sastavljanju kalendara, u arhitekturi i slikarstvu, gdje se često traži omjer zlatnog reza, glazbi, kod određivanja idealnog broja tonova u glazbenoj ljestvici, i drugdje. U grani teorije brojeva koja se naziva *diofantske aproksimacije* često se pitamo koliko dobro možemo zadani iracionalni broj aproksimirati pomoću racionalnog, tj. kolika je udaljenost iracionalnog broja α i racionalnog broja $\frac{p}{q}$,

odnosno $|\alpha - \frac{p}{q}|$. Pritom ćemo tu razliku uspoređivati s q jer za veće nazivnike očekujemo i bolje aproksimacije.

Dirichletov teorem 1.1.1 i njegov korolar zapravo su prirodno poboljšanje sljedećeg jednostavnog razmatranja. Dakle, tražimo racionalne aproksimacije realnog broja α koje zadovoljavaju $\alpha - \frac{p}{q} < \frac{1}{2q}$. Podijelimo segment $[\lfloor\alpha\rfloor, \lfloor\alpha\rfloor + 1]$ na q jednakih dijelova te pogledajmo koji je od brojeva

$$\lfloor\alpha\rfloor, \lfloor\alpha\rfloor + \frac{1}{q}, \lfloor\alpha\rfloor + \frac{2}{q}, \ldots, \lfloor\alpha\rfloor + 1$$

na brojevnom pravcu najbliži broju α. Neka je to broj $\lfloor\alpha\rfloor + \frac{k}{q} = \frac{p}{q}$. Tada vrijedi $\alpha - \frac{p}{q} < \frac{1}{2q}$. Nadalje, možemo se zapitati postoji li nejednakost bolja od (1.1), gdje bi eksponent na desnoj strani bio veći od 2. Vidjet ćemo da je eksponent 2 u nazivniku (1.1) zaista najbolji mogući. Međutim, moguće je zamijeniti jedinicu iz brojnika konstantnim faktorom $c(\alpha)$. To je motiviralo definiciju loše aproksimabilnog broja.

Definicija 1.1.4. *Za iracionalni broj α kažemo da je **loše aproksimabilan** ako postoji pozitivna konstanta $c(\alpha)$ takva da je*

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

za svaki racionalni broj p/q.

Može se pokazati da i loše aproksimabilnih i realnih brojeva koji nisu loše aproksimabilni ima neprebrojivo mnogo. Također vrijedi da omeđenost kvocijenata u razvoju iracionalnog broja u jednostavni verižni razlomak povlači lošu aproksimabilnost i obrnuto. Verižni razlomci moćan su alat za rješavanje sljedeće jednadžbe:

Definicija 1.1.5. *Diofantska jednadžba oblika*

$$x^2 - dy^2 = 1, \tag{1.2}$$

*gdje d prirodan broj koji nije potpun kvadrat nazivamo **Pellova jednadžba**.*

Diofantske jednadžbe rješavaju se u prstenu cijelih brojeva. Pellovu (i kasnije pelovsku) jednadžbu rješavat ćemo u skupu prirodnih brojeva. Pellova jednadžba uvijek ima rješenja u $\mathbb{Z}$, od kojih je $(1, 0)$ jedno (zovemo ga trivijalnim rješenjem).

Jednadžba (1.2) potvrđuje tzv. Stiglerov zakon pogrešnog imenovanja (eponymy). Naime, engleski matematičar 17. stoljeća John Pell nije doprinio rješavanju Pellove jednadžbe. Zaslugu mu je pogrješno pripisao Euler, zamijenivši ga s Pellovim suvremenikom lordom Brounckerom. Iako je na toj jednadžbi Brahmagupta radio još tisuću godina prije

njih, naziv se zadržao do danas. Jednadžba je prvotno zanimala matematičare jer pronalazak rješenja omogućava dobru racionalnu aproksimaciju korijena. Naime,

$$\sqrt{d} = \frac{\sqrt{x^2 - 1}}{y} \approx \frac{x}{y}.$$

Koristit ćemo se Korolarom 1.1.2 da dokažemo sljedeću Lemu, koja će poslužiti u dokazu Teorema 1.1.7, koji kaže da Pellova jednadžba uvijek ima rješenje.

Lema 1.1.6. *Neka je d prirodan broj koji nije potpun kvadrat. Tada postoji cijeli broj $k, 0 < |k| < 1 + 2\sqrt{d}$, sa svojstvom da jednadžba*

$$x^2 - dy^2 = k \tag{1.3}$$

ima beskonačno mnogo rješenja u prirodnim brojevima.

Dokaz. Prema Korolaru 1.1.2, postoji beskonačno mnogo parova prirodnih brojeva (x, y) sa svojstvom

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

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 svojstvom ima beskonačno, a cijelih brojeva koji su po modulu manji od $1 + 2\sqrt{d}$ samo konačno mnogo, to postoji neki cijeli broj k takav da je $|k| < 1 + 2\sqrt{d}$, za koji jednadžba (1.3) ima beskonačno mnogo rješenja. Budući da d nije potpun kvadrat, vrijedi da je $k \neq 0$. □

Teorem 1.1.7. *Neka je d prirodan broj koji nije potpun kvadrat. Postoji bar jedan par prirodnih brojeva (x, y) koji zadovoljava jednadžbu $x^2 - dy^2 = 1$.*

Dokaz. Beskonačno mnogo rješenja jednadžbe (1.3) iz Leme 1.1.6 možemo podijeliti u k^2 klasa, stavljajući rješenja (x_1, y_1) i (x_2, y_2) u istu klasu ako i samo ako je $x_1 \equiv x_2 \pmod{k}$ i $y_1 \equiv y_2 \pmod{k}$. Tada neka od tih klasa sadržava barem dva (u stvari beskonačno) različita rješenja (x_1, y_1), (x_2, y_2). Stavimo

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

("podijelimo" rješenja $x_2 + y_2\sqrt{d}$ i $x_1 + y_1\sqrt{d}$ i racionaliziramo nazivnik). Tvrdimo da je $x, y \in \mathbb{Z},\ y \neq 0$ i $x^2 - dy^2 = 1$. Imamo:

$$x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_y^2 \equiv k \equiv 0 \pmod{k},\ \ x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{k},$$

pa su $x, y \in \mathbb{Z}$. Pretpostavimo da je $y = 0$, tj. $x_1y_2 = x_2y_1$. Tada je

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

tj. $x_1^2 = x_2^2$, što je u suprotnosti s pretpostavkom da su x_1 i x_2 različiti prirodni brojevi. Naposljetku,

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

□

Za najmanje rješenje u prirodnim brojevima Pellove jednadžbe kažemo da je njezino *fundamentalno rješenje*. Označavamo ga s (x_1, y_1), a često također i s $x_1 + y_1\sqrt{d}$ (primijetimo da je zbog iracionalnosti od $\sqrt{d}$ zapis $a + b\sqrt{d}, a, b \in \mathbb{Q}$ jedinstven). Na ovaj način uvodimo uređaj na skupu rješenja. Rješenje $u + v\sqrt{d}$ veće je od $u' + v'\sqrt{d}$ ako vrijedi numerička nejednakost $u + v\sqrt{d} > u' + v'\sqrt{d}$. O rješenjima Pellove (i pelovske) jednadžbe često govorimo kao o elementima kvadratnog polja. Istaknut ćemo neke osnovne pojmove i svojstva kvadratnih polja.

Neka je $d \in \mathbb{Z}$ i d nije potpun kvadrat. Tada skup

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

uz operacije standardnog zbrajanja i množenja ima algebarsku strukturu polja, te ga nazivamo *kvadratno polje*.

Uočimo da ako za neki $k \in \mathbb{Z}, k \neq 0, k^2|d$ tj. $d = k^2d'$, onda je $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ pa možemo pretpostaviti da je d kvadratno slobodan. Svaki element kvadratnog polja $\mathbb{Q}(\sqrt{d})$ može se shvatiti kao nultočka jedinstvenog normiranog kvadratnog polinoma $x^2 + Ax + B = 0$, gdje su $A, B \in \mathbb{Q}$. Ako je element $\alpha \in \mathbb{Q}(\sqrt{d})$ nultočka kvadratnog polinoma $x^2 + Ax + B = 0$, gdje su A, B cijeli brojevi, onda se α naziva *algebarski cijeli broj* ili kraće samo *cijeli broj*.

Skup svih cijelih brojeva nekog kvadratnog polja čini prsten, tzv. *prsten cijelih brojeva* i označava se s $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. U ovisnosti o broju d, znamo precizno opisati sve elemente prstena cijelih brojeva. Naime, vrijedi

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

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

Norma elementa $\alpha = u + v\sqrt{d}$ definira se kao

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

Istaknimo neka svojstva norme:

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

Teorem 1.1.8. *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 dana formulom*

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

tj.

$$x_n = x_1^n + \binom{n}{2} d x_1^{n-2} y_1^2 + \binom{n}{4} d^2 x_1^{n-4} y_1^4 + \ldots,$$
$$y_n = n x_1^{n-1} y_1 + \binom{n}{3} d x_1^{n-3} y_1^3 + \binom{n}{5} d^2 x_1^{n-5} y_1^5 + \ldots.$$

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

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

što znači da su (x_n, y_n) zaista rješenja (i ima ih beskonačno mnogo).

Pretpostavimo sada da je (s,t) rješenje koje nije oblika (x_n, y_n) , $n \in \mathbb{N}$. Budući da je $x_1 + y_1\sqrt{d} > 1$ i $s + t\sqrt{d} > 1$, to postoji $m \in \mathbb{N}$ takav da je

$$(x_1 + y_1\sqrt{d})^m < s + t\sqrt{d} < (x_1 + y_1\sqrt{d})^{m+1}. \tag{1.5}$$

Pomnožimo li (1.5) s $(x_1 + y_1\sqrt{d})^{-m} = (x_1 - y_1\sqrt{d})^m$, dobivamo

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

Definirajmo $a, b \in \mathbb{Z}$ s $a + b\sqrt{d} = (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m$. Imamo $a^2 - db^2 = (s^2 - dt^2)(x_1^2 - dy_1^2)^m = 1$. 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. □

Indijski matematičar sedmog stoljeća Brahmagupta znao je "iskombinirati" dva rješenja Pellove jednadžbe u novo rješenje koristeći identitet koji danas nosi njegovo ime:

$$(x^2 - dy^2)(u^2 - dv^2) = (xu + dyv)^2 - d(xv + yu)^2.$$

Poseban slučaj ove formule za $d = 1$ bio je poznat još i Diofantu.

Označimo sa S skup rješenja Pellove jednadžbe takvih da je x prirodan, a y cjelobrojan, tj.

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

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

Teorem 1.1.9. *Skup S s operacijom množenja tvori cikličku grupu $(S, \cdot)$.*

Dokaz. Najprije provjerimo zatvorenost za množenje. Neka su $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ iz S. Tada je

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

Vrijedi da je

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

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

Multiplikativna jedinica 1 je iz S jer je $(1, 0)$ trivijalno rješenje. Multiplikativni inverz od $x + y\sqrt{d}$ je $x - y\sqrt{d}$, a to je element skupa S. Prema Teoremu 1.1.8 jasno je da je fundamentalno rješenje $x_1 + y_1\sqrt{d}$ generator grupe $(S, \cdot)$. □

Sljedeći teorem daje rekurzivne formule za rješenja Pellove jednadžbe.

Teorem 1.1.10. *Neka je* (x_n, y_n), $n \in \mathbb{N}$ *niz svih rješenja Pellove jednadžbe* $x^2 - dy^2 = 1$ *u prirodnim brojevima, zapisan u rastućem redoslijedu. Uzmimo da je* $(x_0, y_0) = (1, 0)$. *Tada vrijedi:*

$$x_{n+2} = 2x_1x_{n+1} - x_n, \quad y_{n+2} = 2x_1y_{n+1} - y_n, \ \ n \geq 0.$$

Dokaz. Prema Teoremu 1.1.8 vrijedi $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$. Odavde je

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

Sada imamo:

$$x_{n+2} = x_1x_{n+1} + dy_1y_{n+1},$$
$$x_n = x_1x_{n+1} - dy_1y_{n+1},$$

odakle zbrajanjem dobivamo $x_{n+2} = 2x_1x_{n+1} - x_n$. Analogno je

$$y_{n+2} = x_1y_{n+1} + y_1x_{n+1},$$
$$y_n = x_1y_{n+1} - y_1x_{n+1},$$

pa ponovno zbrajanjem dobivamo $y_{n+2} = 2x_1y_{n+1} - y_n$. □

Ove rekurzije možemo matrično prikazati na sljedeći način:

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

Pellovom jednadžbom često se nazivaju sve četiri jednadžbe $x^2 - dy^2 = \pm 1, \pm 4$. Problem pronalaženja jedinica (invertibilnih elemenata u pripadnom prstenu cijelih brojeva) u realnim kvadratnim poljima $\mathbb{Q}(\sqrt{d})$ (s $d < 0$) usko je povezan upravo s ove četiri jednadžbe. Uočimo da za razliku od obične Pellove jednadžbe jednadžba

$$x^2 - dy^2 = -1 \tag{1.6}$$

ne mora imati rješenja u cijelim brojevima. Npr. očito je da jednažba $x^2 - 3y^2 = -1$ nema rješenja (jer je lijeva strana kongruentna 0 ili 1 modulo 3). Nužan uvjet za rješivost jednadžbe (1.6) je da d nema prostih djelitelja oblika $4k + 3$ (jer -1 mora biti kvadratni ostatak modulo d). No vidjet ćemo uskoro da taj uvjet nije i dovoljan. Ako jednadžba (1.6) ima rješenja, onda najmanje njezino rješenje u prirodnim brojevima zovemo *fundamentalno rješenje*.

Teorem 1.1.11. *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 jednadžbe $x^2 - dy^2 = -1$ u prirodnim brojevima.*

Dokaz. Imamo $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, pa je $x_n^2 - dy_n^2 = (x_1^2 - dy_1^2)^n = (-1)^n$. 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 $x^2 - dy^2 = -1$. Pretpostavimo da za fundamentalno rješenje $a + b\sqrt{d}$ jednadžbe $x^2 - dy^2 = 1$ 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 $0 < -x_1 + y_1\sqrt{d} < 1$. 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 (1.6) koje je manje od fundamentalnog, što je kontradikcija.

Pretpostavimo sada da je $u + v\sqrt{d}$ neko rješenje od (1.6) koje nije sadržano u nizu $(x_{2n+1} + y_{2n+1}\sqrt{d})$. Tada postoji $n \in \mathbb{N}$ 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 s $(x_1 - y_1\sqrt{d})^{2n}$, 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 već smo dokazali da takvi σ i τ ne mogu postojati. □

Do sada smo ustanovili da je Pellova jednadžba uvijek rješiva, te opisali njezin skup rješenja. Iz svega do sada iznesenog vidi se da je najbitnije pronaći najmanje rješenje u skupu prirodnih brojeva - fundamentalno rješenje. Redom ispitivati je li broj $1 + dy^2$ potpuni kvadrat za $y = 1, 2, \ldots$. nije učinkovito, što se vidi na primjeru Pellove jednadžbe za $d = 61$ (gdje je $x_1 > 10^9$). Metoda koja se pokazuje djelotvornom koristi razvoj broja $\sqrt{d}$ u jednostavni verižni razlomak.

Teorem 1.1.12. *Neka je $(u, v) \in \mathbb{N}^2$ rješenje Pellove jednadžbe $x^2 - dy^2 = 1$. Onda je $\frac{u}{v}$ neka konvergenta razvoja $\sqrt{d}$ u verižni razlomak.*

Prije dokaza ovog teorema spomenut ćemo što su verižni razlomci i navesti nekoliko lema koje se koriste u dokazu.

Definirat ćemo polinome $p_0, q_0, p_1, q_1, p_2, q_2, \ldots$ takve da su p_n, q_n polinomi u varijablama $a_0, a_1, \ldots, a_n$. Najprije definiramo $p_0 = a_0, q_0 = 1$. Zatim, pretpostavimo da su $p_0, q_0, \ldots, p_{n-1}, q_{n-1}$ već definirani. Uz oznake $p'_k = p_k(a_1, a_2, \ldots, a_{k+1})$, $q'_k = q_k(a_1, a_2, \ldots, a_{k+1})$, definiramo

$$p_n = a_0 p'_{n-1} + q'_{n-1}, \quad q_n = p'_{n-1}.$$

Sada je $\frac{p_n}{q_n}$ racionalna funkcija od $a_0, a_1, \ldots, a_n$ i pisat ćemo

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

Posebno je $[a_0] = \frac{p_0}{q_0} = a_0$. Za $n > 0$ imamo

$$[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n} = \frac{a_0 p'_{n-1} + q'_{n-1}}{p'_{n-1}} = a_0 + \frac{1}{p'_{n-1}/q'_{n-1}} = a_0 + \frac{1}{[a_1, \ldots, a_n]}.$$

Ponavljanjem ovog postupka dobivamo

$$[a_0, a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}. \tag{1.7}$$

Racionalne funkcije ovog oblika nazivaju se *verižni* ili *neprekidni razlomci*.

Lema 1.1.13. *Za $n \geq 2$ vrijedi*

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}.$$

Lema 1.1.14. *Za $k = 1, \ldots, n$ neka je $r_k = [a_k, a_{k+1}, \ldots, a_n]$. Tada je*

$$[a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_{k-1}, [a_k, a_{k+1}, \ldots, a_n]] = \frac{p_{k-1} r_k + p_{k-2}}{q_{k-1} r_k + q_{k-2}}.$$

Dokaz. Druga jednakost slijedi izravno iz Leme 1.1.13. Prvu jednakost dokazujemo indukcijom po k. Za $k = 1$ tvrdnja leme je točna jer je

$$[a_0, a_1, \ldots, a_n] = a_0 + \frac{1}{[a_1, \ldots, a_n]} = [a_0, [a_1, \ldots, a_n]].$$

Pretpostavimo sada da tvrdnja leme vrijedi za $k - 1$, gdje je $1 < k \leq n$. Tada je

$$[a_0, a_1, \ldots, a_n] = a_0 + \frac{1}{[a_1, \ldots, a_n]} = a_0 + \frac{1}{[a_1, \ldots, a_{k-1}, [a_k, \ldots, a_n]]} = [a_0, \ldots, a_{k-1}, [a_k, \ldots, a_n]].$$

□

Lema 1.1.15. *Za $n \geq -1$ vrijedi $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$.*

Dokaz. Lemu dokazujemo indukcijom. Za $n = -1$ imamo $q_{-1}p_{-2} - p_{-1}q_{-2} = 0 \cdot 0 - 1 \cdot 1 = (-1)^{-1}$. Pretpostavimo da tvrdnja vrijedi za $n - 1$. Tada je

$$\begin{aligned} q_n p_{n-1} - p_n q_{n-1} &= (a_n q_{n-1} + q_{n-2}) p_{n-1} - (a_n p_{n-1} + p_{n-2}) q_{n-1} \\ &= -(q_{n-1} p_{n-2} - p_{n-1} q_{n-2}) = -(-1)^{n-1} = (-1)^n. \end{aligned}$$

□

Lema 1.1.16. *Neka je $\alpha = [a_0, a_1, \ldots, a_{n+1}]$. Tada je*

$$q_n \alpha - p_n = \frac{(-1)^n}{a_{n+1} q_n + q_{n-1}}.$$

Dokaz. Prema lemama 1.1.13 i 1.1.15 je

$$q_n \alpha - p_n = q_n \frac{p_{n+1}}{q_{n+1}} - p_n = \frac{-(q_{n+1} p_n - p_{n+1} q_n)}{q_{n+1}} = \frac{(-1)^n}{a_{n+1} q_n + q_{n-1}}.$$

□

Lema 1.1.17. *Neka je a_0 cijeli broj te $a_1, \ldots, a_n$ prirodni brojevi. Tada je $[a_0, a_1, \ldots, a_n]$ racionalni broj. Obrnuto, za dani racionalni broj $\frac{u}{v}$ postoji $n \geq 0$ i brojevi $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_n \in \mathbb{N}$ tako da je*

$$\frac{u}{v} = [a_0, a_1, \ldots, a_n]. \tag{1.8}$$

Nadalje, ako je $\frac{u}{v} \geq 1$, onda je $a_0 \geq 1$.

Napomena 1.1.18. *(i) Ako je r cijeli broj, onda postoje točno dva razvoja od r u jednostavni verižni razlomak: $r = [r]$ i $r = [r - 1, r]$.*

(ii) Ako je r racionalni broj, ali nije cijeli, onda r ima točno dva razvoja u jednostavni verižni razlomak: jedan je oblika $[a_0, a_1, \ldots, a_n]$ uz $a_n \geq 2$, a drugi je oblika $[a_0, a_1, \ldots, a_{n-1}, a_n - 1, 1]$.

Teorem 1.1.19 (Legendre, 1798.)**.** *Neka su p, q cijeli brojevi takvi da je $q \geq 1$ i*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}. \tag{1.9}$$

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

Dokaz. Možemo pretpostaviti da je $\alpha \neq \frac{p}{q}$; inače je tvrdnja trivijalno ispunjena. Tada možemo pisati $\alpha - \frac{p}{q} = \frac{\epsilon\theta}{q^2}$, gdje je $0 < \theta < \frac{1}{2}$ i $\epsilon = \pm 1$. Prema Lemi 1.1.17, postoji razvoj od $\frac{p}{q}$ u jednostavni verižni razlomak

$$\frac{p}{q} = [b_0, b_1, \ldots, b_{n-1}],$$

gdje je n izabran tako da vrijedi $(-1)^{n-1} = \epsilon$. Definirajmo ω s

$$\alpha = \frac{\omega p_{n-1} + p_{n-2}}{\omega q_{n-1} + q_{n-2}}, \tag{1.10}$$

tako da je $\alpha = [b_0, b_1, \ldots, b_{n-1}, \omega]$. Uočimo da je (1.10) ekvivalentno s

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

Možemo pretpostaviti da je $\alpha q_{n-1} - p_{n-1} \neq 0$ jer je inače $\alpha = \frac{p_{n-1}}{q_{n-1}} = \frac{p}{q}$.

Sada je, iz Leme 1.1.16

$$\frac{\epsilon\theta}{q^2} = \alpha - \frac{p}{q} = \frac{1}{q_{n-1}}(\alpha q_{n-1} - p_{n-1}) = \frac{1}{q_{n-1}} \cdot \frac{(-1)^{n-1}}{\omega q_{n-1} + q_{n-2}},$$

pa je $\theta = \frac{q_{n-1}}{\omega q_{n-1} + q_{n-2}}$. Rješavanjem ove jednadžbe po ω, dobivamo $\omega = \frac{1}{\theta} - \frac{q_{n-2}}{q_{n-1}}$. Odavde slijedi da je $\omega > 2 - 1 = 1$. Razvijmo ω u (konačan ili beskonačan) jednostavan verižni razlomak

$$\omega = [b_n, b_{n+1}, b_{n+2}, \ldots].$$

Budući da je $\omega > 1$, svi b_j su prirodni brojevi. Koristeći se Lemom 1.1.14 i prelazeći na limes ako je potrebno, dobivamo

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

Ovo je razvoj u jednostavni verižni razlomak od α i

$$\frac{p}{q} = \frac{p_{n-1}}{q_{n-1}} = [b_0, b_1, \ldots, b_{n-1}]$$

je konvergenta od α, što je i trebalo dokazati. □

Dokaz Teorema 1.1.12. Faktorizacijom Pellove jednadžbe imamo

$$(u - v\sqrt{d})(u + v\sqrt{d}) = 1. \tag{1.11}$$

Iz ovoga možemo zaključiti da je $u - v\sqrt{d}$ pozitivan broj i da je $\frac{u}{v} > \sqrt{d}$. Jednakost (1.11) možemo zapisati kao $u - v\sqrt{d} = \frac{1}{u+v\sqrt{d}}$. Na taj način imamo

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

Kako je $\frac{u}{v} - \sqrt{d}$ pozitivan, vrijedi $|\frac{u}{v} - \sqrt{d}| < \frac{1}{2v^2}$. Sada po Teoremu 1.9 slijedi da je $\frac{u}{v}$ konvergenta razvoja $\sqrt{d}$ u verižni razlomak. □

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

Teorem 1.1.20. *Neka je r duljina perioda u razvoju od $\sqrt{d}$ te neka su $(\frac{p_n}{q_n})$ konvergente od $\sqrt{d}$.*

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

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

Napomena 1.1.21. *Ako je r paran, onda je fundamentalno rješenje od $x^2 - dy^2 = 1$ dano s (p_{r-1}, q_{r-1}). Ako je r neparan, onda je fundamentalno rješenje od $x^2 - dy^2 = -1$ dano s (p_{r-1}, q_{r-1}), a fundamentalno rješenje od $x^2 - dy^2 = 1$ s (p_{2r-1}, q_{2r-1}).*

Iz prethodne napomene je jasno kako se dogodilo da je fundamentalno rješenje nekih Pellovih jednadžbi jako veliko za relativno mali d. Na spomenutom primjeru za $d = 61$ imamo

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

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

1.2 Pelovska jednadžba

Definicija 1.2.1. *Općenito, za N cijeli broj različit od 0, jednadžbu*

$$x^2 - dy^2 = N \tag{1.12}$$

*nazivamo **pelovskom jednadžbom**.*

Pelovska jednadžba ne mora imati cjelobrojnih rješenja, no ako ima barem jedno, onda ih ima beskonačno mnogo. Zaista, ako je $x + y\sqrt{d}$ rješenje jednadžbe (1.12), a $u + v\sqrt{d}$ rješenje pripadne Pellove jednadžbe $x^2 - dy^2 = 1$, onda je

$$(x + y\sqrt{d})(u + v\sqrt{d}) = (ux + dvy) + (uy + vx)\sqrt{d} \tag{1.13}$$

također rješenje jednadžbe (1.12) 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 (1.13) slijedi da i jednadžba (1.12) ima beskonačno rješenja (uz pretpostavku da ima barem jedno). Za dva rješenja $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ jednadžbe (1.12) kažemo da su *asocirana* ako se jedno iz drugog može dobiti množenjem s nekim rješenjem Pellove jednadžbe kao u formuli (1.13). Lako se provjerava da je na ovaj način uvedena relacija ekvivalencije na skupu svih rješenja jednadžbe (1.12) (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*. Sljedeća propozicija daje nužan i dovoljan uvjet za asociranost rješenja:

Propozicija 1.2.2. *$x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ asocirana su ako i samo ako vrijedi*

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

Neka je $\mathbf{K}$ jedna klasa rješenja te neka su njezini 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 $\mathbf{K}$. Ako vrijedi $\mathbf{K} = \overline{\mathbf{K}}$, onda kažemo da je klasa $\mathbf{K}$ *dvoznačna*.

Među svim elementima klase $\mathbf{K}$ odabrat ćemo jedan, $x^* + y^*\sqrt{d}$, koji ćemo zvati *fundamentalno rješenje jednadžbe $x^2 - dy^2 = N$ u klasi $\mathbf{K}$*. Biramo ga tako da y^* poprimi najmanju moguću nenegativnu vrijednost među svim elementima $x + y\sqrt{d}$ u klasi $\mathbf{K}$. Ovim je zahtjevom i x^* jednoznačno određen, osim u slučaju kada je $\mathbf{K}$ dvoznačna. Ako je $\mathbf{K}$ dvoznačna, onda izabiremo x^* tako da zadovolji i dodatni uvjet da je $x^* \geq 0$. Uočimo da $|x^*|$ poprima najmanju moguću vrijednost unutar klase $\mathbf{K}$. Iz sljedećeg teorema zaključit ćemo da postoji konačno mnogo klasa, odnosno konačno mnogo fundamentalnih rješenja pelovske jednadžbe $x^2 - dy^2 = N$.

Teorem 1.2.3. *Neka je $u + v\sqrt{d}$ fundamentalno rješenje Pellove jednadžbe $x^2 - dy^2 = 1$. Tada svako fundamentalno rješenje $x^* + y^*\sqrt{d}$ pelovske jednadžbe $x^2 - dy^2 = N$ zadovoljava sljedeće nejednakosti:*

$$0 \leq y^* \leq \frac{v}{\sqrt{2(u+\epsilon)}}\sqrt{|N|}, \quad |x^*| \leq \sqrt{\frac{1}{2}(u+\epsilon)|N|}, \tag{1.14}$$

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

Dokaz. Neka je

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

gdje je

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

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

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

odnosno

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

Kvadriranjem dobivamo

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

tj.

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

odakle je

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

što povlači prvu nejednakost u (1.14). Drugu nejednakost dobivamo iz

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

□

Uz male preinake, Teorem 1.1.12 može se dokazati i za sve jednadžbe oblika $x^2 - dy^2 = N$, gdje je $|N| < \sqrt{d}$:

Teorem 1.2.4. *Neka 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

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

Iz Legendreova teorema 1.9 slijedi da je $\frac{x}{y}$ neka (neparna) konvergenta od $\sqrt{d}$.

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

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

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 $\sqrt{d}$. □

Dakle, rješivost jednadžbe $x^2 - dy^2 = N$ u relativno prostim cijelim brojevima x, y ako je $|N| < \sqrt{d}$ možemo ustanoviti tako da $\sqrt{d}$ razvijemo u verižni razlomak te provjerimo zadovoljava li neka od prvih $2r$ konvergenti (gdje je r period) relaciju

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

Za rješenje $x_0 + y_0\sqrt{d}$ kažemo da je *primitivno* ako su x_0 i y_0 relativno prosti. Ako je $\text{nzd}(x_0, y_0) = g$, onda je $\frac{x_0}{g} + \frac{y_0}{g}\sqrt{d}$ primitivno rješenje jednadžbe $x^2 - dy^2 = \frac{N}{g^2}$.

Lema 1.2.5. *Ako je $x_0 + y_0\sqrt{d}$ primitivno rješenje jednadžbe $x^2 - dy^2 = N$, onda postoji cijeli broj k, $k < \frac{|N|}{2}$, sa svojstvom*

$$x_0 \equiv k y_0 \pmod{N},$$
$$k^2 \equiv d \pmod{N}.$$

U tom slučaju kažemo da rješenje $x_0 + y_0\sqrt{d}$ pripada broju k.

Dokaz. Budući da su x_0 i y_0 relativno prosti, to su i y_0 i N također relativno prosti. Stoga postoji $k \in \mathbb{Z}$ takav da je $ky_0 \equiv x_0 \pmod{N}$. Broj k možemo izabrati iz bilo kojeg potpunog skupa ostataka modulo N, pa tako i onog s najmanjim ostacima po apsolutnoj vrijednosti, koji sadržava ostatke koji su po apsolutnoj vrijednosti $\leq \frac{|N|}{2}$. Nadalje,

$$x_0^2 - dy_0^2 \equiv (k^2 - d)y_0^2 \equiv 0 \pmod{N},$$

pa je $k^2 \equiv d \pmod{N}$. □

Lema 1.2.6. *Dva primitivna rješenja jednadžbe $x^2 - dy^2 = N$, gdje je N cijeli broj različit od* 0*, asocirana su ako i samo ako pripadaju istom broju.*

Dokaz. Neka su $x_0 + y_0\sqrt{d}$ i $x_1 + y_1\sqrt{d}$ dva primitivna asocirana rješenja jednadžbe $x^2 - dy^2 = N$. Tada postoji rješenje $u + v\sqrt{d}$ jednadžbe $x^2 - dy^2 = 1$ tako da je

$$x_1 = x_0 u + d y_0 v, \quad y_1 = x_0 v + y_0 u.$$

Ako $x_0 + y_0\sqrt{d}$ pripada broju k, onda vrijedi

$$y_1 k \equiv x_0 v k + y_0 u k \equiv y_0 v k^2 + x_0 u \equiv d y_0 v + x_0 u \equiv x_1 \pmod{N},$$

pa i $x_1 + y_1\sqrt{d}$ pripada broju k. Tada je

$$x_0 x_1 \equiv k^2 y_0 y_1 \equiv d y_0 y_1 \pmod{N} \text{ i } x_0 y_1 \equiv k y_0 y_1 \equiv y_0 x_1 \pmod{N},$$

pa su rješenja asocirana. □

Teorem 1.2.7. *Neka je d prirodan broj koji nije potpuni kvadrat i N cijeli broj. Pretpostavimo da nejednadžba* (1.14) *ima rješenja* $x_i^* + y_i^* \sqrt{d}$, $i = 1, 2, \ldots, k$, *pri čemu ta rješenja predstavljaju neasocirana rješenja jednadžbe* (1.12)*. Tada su sva cjelobrojna rješenja pelovske jednadžbe* (1.12) *dana s*

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

$n \in \mathbb{Z}$, $i = 1, 2, \ldots, k$.

Napominjemo da slično kao za Pellovu jednadžbu, i za pelovsku se komponente rješenja, x i y, mogu prikazati kao rekurzivni nizovi drugog reda. Pri tom vrijede iste rekurzivne formule kao u Teoremu 1.1.10 uz odgovarajuće početne uvjete.

Poglavlje 2

Neke metode iz diofantskih aproksimacija

Teorija tzv. *diofantskih aproksimacija* razvila se na problemu aproksimacije iracionalnih brojeva racionalnima. Kako može dati gornju ogradu na veličinu rješenja diofantskih jednadžbi, često se primjenjuje u njihovu rješavanju. Dirichletov teorem 1.1.1 i njegova posljedica, Korolar 1.1.2, često se smatraju ishodišnim rezultatom teorije diofantskih aproksimacija.

2.1 Liouvilleov teorem i algebarski brojevi

Lema 2.1.1. *Neka je α iracionalni broj koji je korijen polinoma*

$$P(X) = aX^2 + bX + c, \quad a \neq 0,$$

s cjelobrojnim koeficijentima i diskriminantom $D = b^2 - 4ac > 0$. Tada za $A > \sqrt{D}$ nejednadžba

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

ima samo konačno mnogo rješenja $p, q \in \mathbb{Z}$.

Dokaz. Zapišimo $P(X)$ u obliku $P(X) = a(X - \alpha)(X - \alpha')$. Tada je $D = a^2(\alpha - \alpha')^2$. Ako je $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$, onda imamo

$$\frac{1}{q^2} \leq |P(p/q)| = \left|\alpha - \frac{p}{q}\right| \cdot \left|a\Big(\alpha' - \frac{p}{q}\Big)\right| < \frac{1}{Aq^2}\left|a\Big((\alpha' - \alpha) + (\alpha - \frac{p}{q})\Big)\right| < \frac{\sqrt{D}}{Aq^2} + \frac{|a|}{A^2q^4}.$$

Odavde je, zbog $A > \sqrt{D}$,

$$q^2 < \frac{|a|}{A^2\left(1 - \frac{\sqrt{D}}{A}\right)},$$

što očito ima samo konačno mnogo rješenja u cijelim brojevima. □

Definicija 2.1.2. *Neka je $\alpha \in \mathbb{C}$. Kažemo da je α **algebarski broj** ako postoji polinom $f(x) \in \mathbb{Q}[X]$, različit od nul-polinoma, takav da vrijedi $f(\alpha) = 0$. Ako $\alpha \in \mathbb{C}$ nije algebarski, onda kažemo da je transcendentan.*

Teorem 2.1.3. *Neka je α algebarski broj. Tada postoji jedinstven, normiran, ireducibilan polinom $P_\alpha(x) \in \mathbb{Q}[X]$ takav da vrijedi $P_\alpha(\alpha) = 0$. Nadalje, svaki polinom $Q(x) \in \mathbb{Q}[X]$ kojeg α poništava djeljiv je s $P_\alpha(x)$.*

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

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

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

Definicija 2.1.4. *Polinom $P_\alpha(x)$ opisan u Teoremu 2.1.3 naziva se **minimalni polinom algebarskog broja** α. **Stupanj algebarskog broja** α je stupanj njegovog minimalnog polinoma $P_\alpha(x)$.*

Definicija 2.1.5. *Za algebarski broj α kažemo da je **algebarski cijeli broj** ako njegov minimalni polinom ima cjelobrojne koeficijente, tj. $P_\alpha(x) \in \mathbb{Z}[X]$.*

Teorem 2.1.6 (Liouville, 1844.)**.** *Neka je α realni algebarski broj stupnja d. Tada postoji konstanta $c(\alpha) > 0$ takva da za svaki racionalan broj $\frac{p}{q} \neq \alpha$, gdje je $q > 0$, vrijedi*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}. \tag{2.1}$$

Dokaz. Neka je $P(x)$ cjelobrojni minimalni polinom od α. Tada za racionalan broj $\frac{p}{q} \neq \alpha$, $q > 0$ trivijalno vrijedi

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

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

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

gdje smo koristili $P(\alpha) = 0$. Nadalje, bez smanjenja općenitosti možemo pretpostaviti da je $\left|\alpha - \frac{p}{q}\right| \leq 1$ jer je u suprotnom jednakost (2.1) zadovoljena. Tada vrijedi

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

Nejednakost (2.1) ispunjena je za konstantu $c(\alpha)$ definiranu relacijom

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

□

Definicija 2.1.7. *Neka je α realni broj. Ako za svaki $w > 0$ postoji racionalni broj $\frac{p}{q}$ takav da je*

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^w},$$

onda kažemo da je α ***Liouvilleov broj****.*

Iz Liouvilleova teorema slijedi da je svaki Liouvilleov broj transcendentan. Budući da su brojevi $\sum_{n\geq 1} a_n 10^{-n!}$ za $a_n \in \{1, 2\}$ Liouvilleovi brojevi, imamo dokaz neprebrojivosti skupa transcendentnih brojeva.

Korolar 2.1.8. *Neka je α algebarski broj stupnja $d \geq 2$ i $\mu > d$. Liouvilleov teorem povlači da nejednadžba*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\mu} \tag{2.2}$$

ima samo konačno mnogo racionalnih rješenja $\frac{p}{q}$.

Razni matematičari poboljšali su ovaj rezultat spuštanjem ograde na μ. Donja tablica prikazuje tko je i kada poopćio nejednakost (2.2) tako da ista vrijedi i za $\mu > f(d)$:

godina	$< \mu$	Matematičar
1908.	$d/2 + 1$	Axel Thue (Nor)
1921.	$2\sqrt{d}$	Carl Ludwig Siegel (Deu)
1947.	$\sqrt{2d}$	Freeman Dyson (UK)
1952.	$\sqrt{2d}$ (neovisno)	Aleksander Gelfond (Rus)
1955.	2	Klaus Roth (Ger)

Klaus Roth je 1958. godine nagrađen Fieldsovom medaljom za postavljanje najbolje moguće ograde na μ takve da nejednadžba (2.2) ima beskonačno mnogo rješenja u racionalnim brojevima. Njegov teorem navodimo bez dokaza:

Teorem 2.1.9 (Roth, 1955.)**.** *Neka je α realni algebarski broj stupnja $d \geq 2$. Tada za svaki $\delta > 0$ nejednadžba*

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

ima samo konačno mnogo rješenja u racionalnim brojevima $\frac{p}{q}$.

2.2 Bakerova teorija

Primjenom Bakerove metode linearnih formi u logaritmima algebarskih brojeva moguće je dobiti „efektivno“ poboljšanje Liouvilleova teorema, no ono što je nama važno jest primjena na rješavanje diofantskih jednadžbi, odnosno sustava pelovskih jednadžbi.

Sustavi pelovskih jednadžbi

Želimo li riješiti sustav pelovskih jednadžbi

$$x^2 - ay^2 = c, \quad z^2 - by^2 = d,$$

možemo riješiti svaku jednadžbu zasebno i dobivena rješenja (za y) izjednačiti. Znamo da će rješenja biti oblika

$$x + y\sqrt{a} = (x^* + y^*\sqrt{a})(u + v\sqrt{a})^m,$$

odnosno

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

gdje su $u + v\sqrt{a}$ i $s + t\sqrt{b}$ fundamentalna rješenja pripadnih Pellovih jednadžbi, $x^* + y^*\sqrt{a}$ i $z' + y'\sqrt{b}$ prolaze konačnim skupom fundamentalnih rješenja promatranih pelovskih jednadžbi, a m i n prolaze skupom nenegativnih cijelih brojeva. Odavde je

$$y = \frac{1}{2\sqrt{a}}\Big((x^* + y^*\sqrt{a})(u + v\sqrt{a})^m - (x^* - y^*\sqrt{a})(u - v\sqrt{a})^m\Big),$$

odnosno

$$y = \frac{1}{2\sqrt{b}}\Big((z' + y'\sqrt{b})(s + t\sqrt{b})^n - (z' - y'\sqrt{b})(s - t\sqrt{b})^n\Big).$$

Ugrubo, imamo da je $\gamma \cdot \alpha^m \approx \delta \cdot \beta^n$, gdje su $\alpha, \beta, \gamma, \delta$ kvadratne iracionalnosti. Logaritmiranjem dobivamo

$$m \ln \alpha - n \ln \beta + \ln \frac{\gamma}{\delta} \approx 0. \tag{2.4}$$

Linearne forme u logaritmima algebarskih brojeva

Zbog dobivene relacije (2.4), smisleno je za proizvoljne algebarske brojeve $\alpha_1, \ldots, \alpha_n$, različite od 0 i 1, i racionalne brojeve $\beta_1, \ldots, \beta_n$, promatrati izraze oblika

$$\Lambda = \beta_1 \ln \alpha_1 + \ldots + \beta_n \ln \alpha_n. \tag{2.5}$$

Prethodni izraz za Λ naziva se *linearna forma u logaritmima algebarskih brojeva*. Za primjene na diofantske jednadžbe, od interesa je slučaj gdje su β_i-ovi cijeli brojevi. Nadalje, u našim primjenama, α_i-ovi će biti pozitivni realni brojevi, tako da će ln biti obična realna logaritamska funkcija (u općem slučaju, ln je glavna grana kompleksne logaritamske funkcije).

Od prvih radova Alana Bakera s kraja 60-ih godina 20. stoljeća, pa sve do danas, poznato je više rezultata koji govore o tome da linearna forma u logaritmima ne može biti jako blizu nuli. Posebno će nas zanimati rezultati koji daju eksplicitnu gornju ogradu za m i n jer ih možemo primijeniti pri rješavanju sustava pelovskih jednadžbi, a primjenjivi su i na mnoge druge diofantske probleme. Razvoj teorije linearnih formi u logaritmima motiviran je sedmim Hilbertovim problemom, koji je tražio da se dokaže da ako je α algebarski broj $\neq 0, 1$ te β algebarski i iracionalan, onda je α^β transcendentni broj. Tu su tvrdnju pokazali Gelfond i Schneider (neovisno) 1934. godine. Baker je 1966. godine poopćio taj rezultat i dokazao da ako su $\alpha_1, \ldots, \alpha_n$ algebarski brojevi $\neq 0, 1$ i $\beta_1, \ldots, \beta_n$ linearno nezavisni nad $\mathbb{Q}$, onda je broj $\alpha_1^{\beta_1} \cdot \ldots \cdot \alpha_n^{\beta_n}$ transcendentan. Dakle, ako su $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ kao gore, a α_{n+1} proizvoljan algebarski broj, onda je $\beta_1 \ln \alpha_1 + \ldots + \beta_n \ln \alpha_n \neq \alpha_{n+1}$. Štoviše, Baker je pokazao da broj

$$|\beta_1 \ln \alpha_1 + \ldots + \beta_n \ln \alpha_n - \alpha_{n+1}|$$

ne može biti jako mali.

Teorem 2.2.1. *Ako su $\alpha_1, \ldots, \alpha_n$ algebarski brojevi takvi da su $\ln \alpha_1, \ldots, \ln \alpha_n$ linearno nezavisni nad $\mathbb{Q}$, onda su $1, \ln \alpha_1, \ldots, \ln \alpha_n$ linearno nezavisni nad poljem algebarskih brojeva.*

Teorem 2.2.1 nećemo dokazivati, ali navodimo nekoliko korolara:

Korolar 2.2.2. *Svaka netrivijalna linearna kombinacija logaritama algebarskih brojeva s algebarskim koeficijentima je transcendentan broj.*

Drugim riječima, za algebarske brojeve $\alpha_1, \ldots, \alpha_n$, $\alpha_i \neq 0$ i $\beta_0, \beta_1, \ldots, \beta_n$, $\beta_0 \neq 0$ imamo

$$\beta_0 + \beta_1 \ln \alpha_1 + \ldots + \beta_n \ln \alpha_n \neq 0.$$

Ovo očito vrijedi za $n = 0$. Pretpostavimo da tvrdnja vrijedi za $n < m$, gdje je m prirodan broj. Pokazat ćemo da onda tvrdnja vrijedi i za $n = m$. Ako su $\ln\alpha_1, \ldots, \ln\alpha_m$ linearno nezavisni nad poljem racionalnih brojeva, onda tvrdnja slijedi iz Teorema 2.2.1. Prema tome, možemo pretpostaviti da postoje racionalni brojevi $\rho_1, \ldots, \rho_m$ gdje je, uzmimo, $\rho_r \neq 0$, takvi da

$$\rho_1 \ln\alpha_1 + \ldots + \rho_m \ln\alpha_m = 0.$$

Jasno je da

$$\rho_r(\beta_0 + \beta_1 \ln\alpha_1 + \ldots + \beta_m \ln\alpha_m) = \beta_0' + \beta_1' \ln\alpha_1 + \ldots + \beta_m' \ln\alpha_m,$$

gdje su

$$\beta_0' = \rho_r \beta_0, \quad \beta_j' = \rho_r \beta_j - \rho_j \beta_r \quad (1 \leq j \leq m).$$

Kako je $\beta_0' \neq 0$ i $\beta_r' = 0$, traženi rezultat slijedi indukcijom.

Korolar 2.2.3. *Broj $e^{\beta_0}\alpha_1^{\beta_1} \ldots \alpha_n^{\beta_n}$ je transcendentan za proizvoljne algebarske brojeve $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ različite od nule.*

Uistinu, ako bi $\alpha_{n+1} = e^{\beta_0}\alpha_1^{\beta_1} \ldots \alpha_n^{\beta_n}$ bio algebarski, onda bi i

$$\beta_1 \ln\alpha_1 + \ldots + \beta_n \ln\alpha_n - \alpha_{n+1} \quad (= -\beta_0)$$

bio algebarski broj različit od nule, protivno prethodnom korolaru. Sljedeći korolar pokriva slučaj $\beta_0 = 0$.

Korolar 2.2.4. *Broj $\alpha_1^{\beta_1} \ldots \alpha_n^{\beta_n}$ je transcendentan za sve $\alpha_1, \ldots, \alpha_n$ različite od* 0 *i* 1 *i sve algebarske brojeve $\beta_1, \ldots, \beta_n$ za koje su* $1, \beta_1, \ldots, \beta_n$ *linearno nezavisni nad* $\mathbb{Q}$.

Dovoljno je pokazati da za proizvoljne algebarske brojeve $\alpha_1, \ldots, \alpha_n$, različite od 0 i 1, i $\beta_1, \ldots, \beta_n$ linearno nezavisne nad $\mathbb{Q}$, vrijedi

$$\beta_1 \ln\alpha_1 + \ldots + \beta_n \ln\alpha_n \neq 0;$$

tada tvrdnja slijedi uz zamjene $n \to n+1$ i $\beta_{n+1} = -1$. Za $n = 1$, korolar trivijalno slijedi. Pretpostavimo da korolar vrijedi za $n < m$, gdje je m prirodan broj, a pokazat ćemo da tada vrijedi i za $n = m$. Ako su $\ln\alpha_1, \ldots, \ln\alpha_n$ linearno nezavisni nad racionalnim brojevima, primjenom Teorema 2.2.1 možemo pretpostaviti da postoje $\rho_1, \ldots, \rho_m$ i β_j' kao u dokazu Korolara 2.2.2, s tim da je sada $\beta_0 = \beta_0' = 0$. Jasno je da ako su $\beta_1, \ldots, \beta_m$ linearno nezavisni nad $\mathbb{Q}$, onda su također i β_j' (j nije 0 ili r) pa dokaz slijedi indukcijom.

Kao posebne slučajeve ovih korolara možemo dobiti da je $\pi + \ln\alpha$ transcendentan neovisno o izboru algebarskog broja $\alpha \neq 0$ (što znači da je i π transcendentan) te da je $e^{\alpha\pi+\beta}$ transcendentan (što znači da je i e transcendentan).

Baker–Wüstholzov teorem

Pokazuje se da ako je $\Lambda \neq 0$, onda se $|\Lambda|$ može ocijeniti odozgo ogradom koja ovisi o apsolutnim vrijednostima β_i-ova te stupnjevima i visinama α_i-ova. Navest ćemo bez dokaza Baker-Wüstholzov teorem koji ćemo koristiti u trećem poglavlju.

Definiramo visinu algebarskog broja i Mahlerovu mjeru polinoma. Neka je α algebarski broj, a $P(x)$ njegov cjelobrojni minimalni polinom

$$P(x) = a_d x^d + \cdots + a_1 x + a_0 = a_d \prod_{i=1}^{d} (x - \alpha^{(i)}).$$

Visina (naivna visina) od α je

$$H(\alpha) = \max\{|a_i| : \ i = 0, 1, \ldots, d\},$$

Mahlerova mjera $M(\alpha)$ je

$$M(\alpha) = |a_d| \prod_{i=1}^{d} \max\{|\alpha^{(i)}|, 1\},$$

a $h(\alpha) = \frac{1}{d} \ln M(\alpha)$ je *logaritamska Weilova visina*.

Teorem 2.2.5. *Neka su $\alpha_1, \ldots \alpha_n$ algebarski brojevi, $b_1, \ldots, b_n$ cijeli brojevi, Λ linearna forma* (2.5)*, te $d = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$ stupanj algebarskog proširenja polja $\mathbb{Q}$ generiranog s $\alpha_1, \ldots \alpha_n$. Ako je $\Lambda \neq 0$, onda je*

$$|\Lambda| > (3A)^{-dnB},$$

gdje je $B = \max\{|b_1|, \ldots, |b_n|, 2\}$ i $A = \max\{H(\alpha_1), \ldots, H(\alpha_n)\}$.

Ovaj teorem nećemo dokazivati (vidjeti [5], poglavlje 14.3, Propozicija 14.5). Pokazalo se da nejednakost iz ovog teorema nije dovoljno dobra za većinu primjena, no sljedeća tvrdnja vrlo je operativno primjenljiva.

Teorem 2.2.6 (Baker-Wüstholz, 1993.)**.** *Neka su $\alpha_1, \ldots \alpha_n$ algebarski brojevi, $b_1, \ldots, b_n$ cijeli brojevi, Λ linearna forma* (2.5)*, te $d = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$ stupanj algebarskog proširenja polja $\mathbb{Q}$ generiranog s $\alpha_1, \ldots \alpha_n$. Ako je $\Lambda \neq 0$, onda je*

$$\ln |\Lambda| \geq -18(n+1)! n^{n+1} (32d)^{n+2} \ln(2nd) h'(\alpha_1) \cdot \cdots \cdot h'(\alpha_n) \ln B,$$

gdje je $B = \max\{|b_1|, ..., |b_n|\}$, $h'(\alpha) = \max\{h(\alpha), \frac{1}{d}|\ln \alpha|, \frac{1}{d}\}$, a $h(\alpha)$ je logaritamska Weilova visina.

Ugrubo, Teorem 2.2.5 daje

$$\ln|\Lambda| > -C_1(n,d)\ln A \cdot B,$$

a Teorem 2.2.6 kaže da je

$$\ln|\Lambda| \geq -C(n,d)\ln A_1 \cdot \cdots \cdot \ln A_n \ln B,$$

gdje je $A_j = \max\{H(\alpha_j), 1\}$, $j = 1, \ldots, n$, a C i C_1 neke pozitivne konstante koje ovise o broju algebarskih brojeva i stupnju proširenja polja $\mathbb{Q}$ generiranog s tim istim algebarskim brojevima. Rezultat Bakera i Wüstholza malo je poboljšao Matvejev 2000. godine. Postoje i poboljšanja za slučajeve (koji su najvažniji za primjene) $n = 2$ (Laurent, Mignotte, Nesterenko, 1995.) i $n = 3$ (Mignotte, 2006.). U rješavanju našeg problema pokazuje se da je Baker-Wüstholzov teorem (u kombinaciji s metodama redukcije) sasvim dovoljan.

Poglavlje 3

Fermatova četvorka

3.1 Diofantove m-torke

Definicija 3.1.1. ***Diofantova m-torka*** *je skup od m različitih prirodnih brojeva sa svojstvom da je produkt svaka dva njegova različita elementa uvećan za jedan jednak kvadratu nekog cijelog broja.*

Napomenimo da ćemo Diofantova m-torku označavati kao skup, što onda uključuje pretpostavku da su elementi međusobno različiti. Poredak elemenata nije bitan, iako ih je uobičajeno pisati u rastućem poretku. Dakle, $\{a_1, \ldots, a_m\}$ je Diofantova m-torka ako je zadovoljeno sljedećih $m(m-1)/2$ uvjeta:

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

za neke $n_{ij} \in \mathbb{N}$.

Vjeruje se je prvu četvorku racionalnih brojeva koji zadovoljavaju svojstvo iz Definicije 3.1.1 pronašao starogrčki matematičar Diofant Aleksandrijski,

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

Zaista, vrijedi

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

Prvi primjer Diofantove četvorke pronašao je Fermat i to je bio skup

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

kojeg se često naziva *Fermatova četvorka*. Zaista,

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

Kako je $0 \cdot a_i + 1 = 1^2$, ne dozvoljavamo da 0 bude član m-torke. Također se lako uvjeriti da ne postoji Diofantova m-torka koja se sastoji od elemenata suprotnih predznaka jer je za $a_i \cdot a_j < 0, \{a_i, a_j\} \neq \{-1, 1\}$, $a_i a_j + 1 < 0$. Zato Diofantove m-torke uglavnom tražimo u skupu prirodnih brojeva. Ponekad se generalizira tako što skupove s opisanim svojstvom tražimo u polju racionalnih brojeva, kada govorimo o *racionalnoj Diofantovoj m-torci*.

Definicija 3.1.2. ***Racionalna Diofantova m-torka*** *je skup od m racionalnih brojeva različitih od 0 sa svojstvom da je produkt svaka dva njegova različita elementa uvećan za 1 jednak kvadratu nekog racionalnog broja.*

U definiciji Diofantove m-torke isključuje se zahtjev da produkt elementa sa samim sobom uvećan za jedan daje kvadrat. Očito je da u cijelim brojevima taj uvjet ne može biti zadovoljen jer jednadžba $a^2 + 1 = r^2$ nema rješenja u $\mathbb{N}$. No u skupu racionalnih brojeva nema nekog očitog razloga zašto takvi skupovi (koje bismo mogli nazvati *jake Diofantove m-torke*) ne bi postojali. Svaki element a takvog skupa trebao bi zadovoljavati da je $a^2 + 1$ kvadrat, pa je stoga $a = X/Y$, gdje je (X, Y, Z) Pitagorina trojka, tj. $X^2 + Y^2 = Z^2$. U [7] dokazano je da postoji beskonačno mnogo jakih racionalnih Diofantovih trojki (primjerice $\{1976/5607, 3780/1691, 14596/1197\}$), ali nije poznato postoji li ijedna jaka Diofantova četvorka.

Prirodno se zapitati koliko veliki takvi skupovi mogu biti, tj. koji je najveći m za kojeg postoji Diofantova m-torka. Iz primjera Fermatove četvorke, vidimo da je $m \geq 4$. Dugi niz godina pretpostavljalo se da Diofantova petorka ne postoji. U nizu radova dokazano je postojanje samo konačno mnogo petorki, no ograde na elemente bile su prevelike da bi se to učinkovito, računalom moglo provjeriti. Dujella je u [4] 2004. godine dokazao da ne postoji Diofantova šestorka, ali tek su 2019. godine He, Togbé i Ziegler uspjeli dokazati da niti petorka zaista ne postoji ([11]). S druge strane, u racionalnom slučaju pitanje je sasvim otvoreno te za sada nema ni neke opće prihvaćene slutnje o tome koliko najviše elemenata može sadržavati racionalna Diofantova m-torka.

U bliskoj vezi s problemom veličine Diofantovih skupova jest problem nadopunjavanja dane Diofantove m-torke s bar još jednim elementom. Švicarskom matematičaru Leonhardu Euleru bilo je poznato da se svaki Diofantov par $\{a, b\}$, odnosno skup za kojeg je

$$ab + 1 = r^2, \tag{3.1}$$

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 $bc_\pm + 1 = (b \pm r)^2$. Za trojku gdje je $c = a + b \pm 2r$ kažemo da je *regularna*.

Nadalje, svaka Diofantova trojka $\{a, b, c\}$ može se nadopuniti elementima

$$d_\pm = a + b + c + 2abc \pm 2rst, \tag{3.2}$$

pri čemu je

$$ab + 1 = r^2,\ ac + 1 = s^2,\ bc + 1 = t^2, \tag{3.3}$$

za $r, s, t \in \mathbb{N}$ i $d_- \neq 0$. Pokažimo da je $ad_\pm + 1 = \square$. Vrijedi

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

gdje je korišteno (3.3). Analogno se pokazuje da vrijedi

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

Ako smo počeli od regularne trojke $\{a, b, a + b + 2r\}$, element d_+ možemo prikazati kao

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

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

$$\{a, b, a + b + 2r, 4r(a + r)(b + r)\}. \tag{3.4}$$

Za četvorke ovog oblika kažemo da su *regularne*. Drugim riječima, Diofantova četvorka $\{a, b, c, d\}$ je regularna ako i samo ako vrijedi

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1). \tag{3.5}$$

Još uvijek je nedokazana slutnja da su sve Diofantove četvorke regularne. S tim u vezi spomenimo da su Cipu, Fujita i Miyazaki dokazali da se proizvoljna Diofantova trojka $\{a, b, c\}$ može proširiti do Diofantove četvorke na najviše osam različitih načina ([2]). Budući da postoji beskonačno mnogo parova međusobno različitih prirodnih brojeva za koje vrijedi (3.1), iz (3.4) možemo zaključiti da postoji beskonačno mnogo regularnih Diofantovih četvorki. Čak postoje parametarske familije cjelobrojnih Diofantovih četvorki dane s pomoću polinoma ili Fibonaccijevih brojeva:

$$\{k, k + 2, 4k + 4, 16k^3 + 48k^2 + 44k + 12\}, \tag{3.6}$$

$$\{F_{2k}, F_{2k+2}, F_{2k+4}, 4F_{2k+1}F_{2k+2}F_{2k+4}\}, \tag{3.7}$$

za $k \geq 1$. U [12] dokazano je da se broj Diofantovih četvorki s elementima $\leq N$ asimptotski približava $C\sqrt[3]{N}\ln N$, gdje je $C \approx 0.338285$. Zanimljivo je da je Euler uspio proširiti Fermatovu četvorku do racionalne petorke $\{1, 3, 8, 120, \frac{777480}{8288641}\}$. Nedavno je Stoll dokazao da je ovo proširenje jedinstveno [13]. To posebno znači da se ova petorka ne može proširiti do racionalne Diofantove šestorke. Dokaz tog rezultata koristi se modernim tehnikama za nalaženje svih racionalnih nultočaka na krivuljama genusa ≥ 2. Sljedeći teorem govori o odnosu veličina članova Diofantove trojke.

Teorem 3.1.3. *Neka je $\{a, b, c\}$ Diofantova trojka te $a < b < c$. Tada je ili $c = a + b + 2r$ ili $c > 4ab$.*

Dokaz. Neka su $d_{+,-}$ definirani kao u (3.2) (to su rješenja kvadratne jednadžbe (3.5)).Imamo da je

$$d_+d_- = a^2 + b^2 + c^2 - 2ab - 2ac - 2bc - 4 = (c - a - b)^2 - 4r^2 = (c - a - b + 2r)(c - a - b - 2r),$$

odakle vidimo da je $d_- = 0$ ako i samo ako je $c = a + b \pm 2r$. Ako je $d_- \neq 0$, onda je $\{a, b, c, d_-\}$ također jedna Diofantova četvorka. Neka je $c = \max(a, b, c)$. Tada je

$$c = a + b + d_- + 2abd_- + 2\sqrt{(ab + 1)(ad_- + 1)(bd_- + 1)} > 4ab.$$

□

Sada ćemo ugrubo skicirati neke od ideja koje su korištene u rezultatima o (ne)proširivosti Diofantovih trojki i četvorki. Problem proširenja Diofantove trojke $\{a, b, c\}, a < b < c$, do Diofantove četvorke $\{a, b, c, d\}$ dovodi nas do sustava jednadžbi

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

iz kojih eliminacijom varijable d dobivamo sustav simultanih jednadžbi pelovskog tipa

$$cx^2 - az^2 = c - a, \quad cy^2 - bz^2 = c - b. \tag{3.8}$$

Rješenja ovakvih jednadžbi opisuju se pomoću konačno mnogo binarnih rekurzivnih nizova. Stoga se polazni problem svodi na traženje presjeka tih nizova, tj. na konačno mnogo jednadžbi oblika $v_m = w_n$, gdje su (v_m) i (w_n) nizovi koji zadovoljavaju jednadžbe (3.8). U potpoglavlju 2.2 vidjeli smo kako je Bakerova teorija linearnih formi u logaritmima algebarskih brojeva iskoristiva za dobivanje gornje ograde na m, n.

Drugi način za dobivanje gornje ograde na rješenja je pomoću rezultata o simultanoj aproksimaciji kvadratnih korijena (tzv. Bennettov teorem, dobiven generalizacijom tzv. hipergeometrijske metode). Naime, ako pretpostavimo da sustav 3.8 ima neko relativno veliko rješenje (x, y, z), onda $\frac{x}{z}$ i $\frac{y}{z}$ predstavljaju vrlo dobre racionalne aproksimacije (sa zajedničkim nazivnikom) iracionalnih brojeva $\sqrt{a/c}$ i $\sqrt{b/c}$. Ako su te aproksimacije bolje od onih čije postojanje jamči Dirichletov teorem o simultanim aproksimacijama (vidjeti [5], Korolar 8.49), onda možemo očekivati da ćemo dobiti kontradikciju, što će povlačiti da rješenja ne mogu biti velika.

Kao što je već spomenuto, odnedavno je poznato da ne postoji cjelobrojna Diofantova petorka, dakle, možemo reći da je Fermat pronašao najveći mogući skup s tim svojstvom. S druge strane, u racionalnom slučaju postoje veći skupovi s Diofantovim svojstvom. Euler je dokazao da postoji beskonačno mnogo racionalnih Diofantovih petorki. No pitanje postojanja racionalnih Diofantovih šestorki ostalo je otvoreno sljedeća dva stoljeća. Prvu racionalnu Diofantovu šestorku pronašao je Gibbs 1999. godine, a to je bila šestorka

$$\{11/192, 35/192, 155/27, 512/27, 1235/48, 180873/16\},$$

dok su Dujella, Kazalicki, Mikić i Szikszai 2017. godine dokazali da postoji beskonačno mnogo racionalnih Diofantovih šestorki [8].

Nije poznat ni jedan primjer racionalne Diofantove sedmorke i otvoren je problem postoji li takva sedmorka. Poznati su primjeri „gotovo“sedmorki, tj. skupova od sedam elemenata kojima samo jedan uvjet nedostaje kako bi bili racionalne Diofantove sedmorke. Drugim riječima, postoje racionalne Diofantove petorke koje se mogu na dva različita načina proširiti do šestorke. Primjerice, petorka

$$\{243/560, 1147/5040, 1100/63, 7820/567, 95/112\}$$

može se proširiti do šestorke s $38269/6480$ ili sa $196/45$ [10].

3.2 Proširenje skupa $\{1, 3, 8\}$

Teorem 3.2.1. *Ako je* $\{1, 3, 8, d\}$ *Diofantova četvorka, onda je* $d = 120$.

Ovaj teorem može se dokazati primjenom Bakerove teorije linearnih formi u logaritmima. To su prvi učinili Baker i Davenport u [1]. S problemom ih je upoznao J. H. van Lint u ožujku 1968. godine. Van Lint je uspio dokazati teorem za $d < 10^{1\,700\,000}$.

Iz definicije Diofantove četvorke vrijedi da je

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

Eliminacijom nepoznanice d, dobivamo ekvivalentan sustav pelovskih jednadžbi sa zajedničkom nepoznanicom x:

$$y^2 - 3x^2 = -2, \tag{3.9}$$

$$z^2 - 8x^2 = -7. \tag{3.10}$$

Uočimo da je jedno rješenje ovog sustava $(x, y, z) = (1, 1, 1)$, no ono odgovara *nepravom* proširenju $d = 0$. Nadalje, rješenje $(11, 19, 31)$ odgovara proširenju $d = 120$. Istražit ćemo ima li sustav (3.9), (3.10) još rješenja. Iz sljedećeg teorema (kojeg ne dokazujemo) proizlazi da sustav ima konačno mnogo rješenja.

Teorem 3.2.2. *(Siegel, 1926.) Neka je* $f(x)$ *polinom s cjelobrojnim koeficijentima koji ima barem tri različite nultočke u* $\mathbb{C}$. *Tada jednadžba*

$$y^2 = f(x) \tag{3.11}$$

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

Uz supstituciju $t = yz$, množenjem (3.9) i (3.10) dobivamo jednadžbu

$$t^2 = (3x^2 - 2)(8x^2 - 7), \tag{3.12}$$

koja prema Teoremu 3.2.2 ima konačno mnogo cjelobrojnih rješenja. Zato je broj mogućih proširenja skupa $\{1, 3, 8\}$ konačan. Opisat ćemo korake kojima su Baker i Davenport u [1] dokazali jedinstvenost proširenja.

(i) Opisati skup svih rješenja sustava (3.9), (3.10) pomoću nizova potencija kvadratnih iracionalnosti.

(ii) Dobiti nejednakosti u kojoj se pojavljuje cjelobrojna linearna kombinacija logaritama triju algebarskih brojeva, odnosno linearna forma u logaritmima algebarskih brojeva.

(iii) Pomoću Bakerovog rezultata koji daje donju ogradu za vrijednost linearne forme odrediti $X > 0$ tako da sustav (3.9), (3.10) nema rješenja za $x > X$.

(iv) Reducirati gornju ogradu X pomoću metode izvorno opisane u [1]. Mi ćemo koristiti Lemu 3.2.7, verziju redukcije dane u [6].

Rješenja pelovskih jednadžbi

Fundamentalno rješenje Pellove jednadžbe $y^2-3x^2 = 1$, koja pripada (3.9), je $(y, x) = (2, 1)$. Prema Teoremu 1.2.3 vrijede sljedeće ocjene za fundamentalno rješenje (y^*, x^*) jednadžbe (3.9):

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

Stoga je $(y^*, x^*) \in \{(1, 1), (-1, 1)\}$. Iz Propozicije 1.2.2 slijedi da su ova dva fundamentalna rješenja asocirana, odnosno pripadaju istoj klasi. Stoga je $(y^*, x^*) = (1, 1)$ jedino fundamentalno rješenje (3.9), a sva rješenja (y, x) u skupu prirodnih brojeva nalazimo primjenom Teorema 1.2.7:

$$y + x\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^m,\ m \geq 0, \tag{3.13}$$

odakle je

$$y - x\sqrt{3} = (1 - \sqrt{3})(2 - \sqrt{3})^m,\ m \geq 0. \tag{3.14}$$

Oduzimanjem relacija (3.13) i (3.14) dobivamo

$$2x\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^m - (1 - \sqrt{3})(2 - \sqrt{3})^m,\ m \geq 0. \tag{3.15}$$

Uobičajeno je sva rješenja od (3.9) u x definirati pomoću niza $(v_m)_{m\geq 0}$:

$$v_m = \frac{1 + \sqrt{3}}{2\sqrt{3}}(2 + \sqrt{3})^m - \frac{1 - \sqrt{3}}{2\sqrt{3}}(2 + \sqrt{3})^{-m},\ m \geq 0, \tag{3.16}$$

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

Sada rješavamo jednadžbu (3.10). Fundamentalno rješenje pripadne Pellove jednadžbe $z^2 - 8x^2 = 1$ je $(u, v) = (3, 1)$. Za fundamentalno rješenje jednadžbe (3.10) pomoću Teorema 1.2.3 dobivamo ograde:

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

Dakle, $(z^*, x^*) \in \{(1,1),(-1,1)\}$. Prema Propoziciji 1.2.2 rješenja $(1,1)$ i $(-1,1)$ nisu asocirana pa su sva cjelobrojna rješenja (z,x) od (3.10) (opet prema Teoremu 1.2.7) dana s

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

odnosno

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

Kao i u prethodnom slučaju, sva rješenja od (3.10) zapisujemo pomoću nizova $(w_n^+)_{n\geq 0}$ i $(w_n^-)_{n\geq 0}$:

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

Odrediti x koji zadovoljava sustav (3.9) i (3.10) ekvivalentno je određivanju nenegativnih cijelih brojeva m i n za koje je $v_m = w_n^+$ ili $v_m = w_n^-$, odnosno traženju presjeka nizova (v_m) i $(w_n^{+,-})$. Prvih nekoliko članova nizova v i $w^{+,-}$ dani su u sljedećoj tablici:

i	v_i	w_i^+	w_i^-
0	1	1	1
1	3	4	2
2	11	23	11
3	41	134	64
4	153	781	373
5	571	4552	2174

Imamo $v_0 = w_0^{+,-} = 1$, odakle je $d = 0$ trivijalno rješenje (i predstavlja tzv. *nepravo* proširenje trojke) te $v_2 = w_2^- = 11$, odakle je $d = 11^2 - 1 = 120$. Želimo dokazati da drugih rješenja nema.

Lako se vidi da za $n > 2$ vrijedi $w_n^{+,-} > v_n$, odakle slijedi da je $m < n$.

Nizovi v i w daju se karakterizirati kao rekurzivni:

Propozicija 3.2.3. *Za $n \geq 2$, vrijedi da je*

$$w_n^+ = 6 \cdot w_{n-1}^+ - w_{n-2}^+,$$

gdje je $w_0^+ = 1$ i $w_1^+ = 4$.

Ista rekurzija vrijedi i za niz w_n^-, ali tada je $w_1^- = 2$.

Propozicija 3.2.4. *Za $n \geq 2$, vrijedi da je*

$$v_n = 4 \cdot v_{n-1} - v_{n-2},$$

gdje je $v_0 = 1$ i $v_1 = 3$.

Jednadžba $v_m = w_n^{+,-}$ svodi se na sljedeću eksponencijalnu jednadžbu:

$$\frac{(1+\sqrt{3})(2+\sqrt{3})^n - (1-\sqrt{3})(2-\sqrt{3})^n}{2\sqrt{3}} = \frac{(2\sqrt{2}\pm 1)(3+2\sqrt{2})^m + (2\sqrt{2}\mp 1)(3-2\sqrt{2})^m}{4\sqrt{2}}. \tag{3.17}$$

Linearna forma u logaritmima - *gornja ograda*

Lema 3.2.5. *Neka su $m, n > 2$ prirodni brojevi koji zadovoljavaju* (3.17)*. Tada vrijedi*

$$0 < |\Lambda| < 7.3 \cdot (2+\sqrt{3})^{-2n}, \tag{3.18}$$

gdje je

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

Dokaz. Očito je

$$v_n > \frac{(1+\sqrt{3})(2+\sqrt{3})^n}{2\sqrt{3}}, \quad w_m^{+,-} < \frac{(2\sqrt{2}+1)(3+2\sqrt{2})^m}{2\sqrt{2}},$$

pa iz $v_n = w_m^{+,-}$ slijedi

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

Kako je $(3+2\sqrt{2})^{-1} = 3-2\sqrt{2}$ i $(2+\sqrt{3})^{-1} = 2\sqrt{3}$, prethodnu nejednakost možemo zapisati kao

$$(3-2\sqrt{2})^m < \frac{(2\sqrt{2}+1)\sqrt{3}}{(\sqrt{3}+1)\sqrt{2}}(2-\sqrt{3})^n < 1.7163(2-\sqrt{3})^n. \tag{3.19}$$

Sada iz (3.17), dijeljenjem s $\frac{2\sqrt{2}\pm 1}{2\sqrt{2}} \cdot (3+2\sqrt{2})^m$, dobivamo

$$\begin{aligned}
&\left|\frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)} \cdot \frac{(2+\sqrt{3})^n}{(3+2\sqrt{2})^m} - 1\right| \\
&\leq \frac{2\sqrt{2}+1}{2\sqrt{2}-1} \cdot (3-2\sqrt{2})^{2m} + \frac{2\sqrt{2}(\sqrt{3}-1)}{\sqrt{3}(2\sqrt{2}-1)}(2-\sqrt{3})^n(3-2\sqrt{2})^m \\
&< 7.29(2-\sqrt{3})^{2n},
\end{aligned}$$

pri čemu smo u posljednjoj nejednakosti koristili (3.19).

Iskoristit ćemo sljedeću jednostavnu činjenicu: ako je $a \in \langle 0, 1\rangle$ i $0 < |X| < a$, onda je

$$|\ln(X+1)| < \frac{-\ln(1-a)}{a} \cdot |X|. \tag{3.20}$$

Zaista,

$$|\ln(X+1)| = \left| \sum_{i=1}^{\infty} \frac{(-1)^{i-1} X^i}{i} \right| < |X| \cdot \sum_{i=1}^{\infty} \frac{a^{i-1}}{i} = |X| \cdot \frac{-\ln(1-a)}{a}.$$

Primjenom nejednakosti (3.20) na

$$X = \frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2} \pm 1)} \cdot \frac{(2+\sqrt{3})^n}{(3+2\sqrt{2})^m} - 1$$

i $a = 0.0027$ ($\approx 7.29 \cdot (2-\sqrt{3})^6$), dobivamo

$$|\ln(X+1)| < 1.00135 \cdot |X|,$$

gdje je

$$\ln(X+1) = \ln \frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2} \pm 1)} \cdot \frac{(2+\sqrt{3})^n}{(3+2\sqrt{2})^m} = \Lambda.$$

Kako je $|X| < 7.29(2-\sqrt{3})^{2n}$, slijedi tražena nejednakost

$$\Lambda < 7.3 \cdot (2-\sqrt{3})^{2n}.$$

Još treba dokazati da je $\Lambda > 0$. Ako bi bilo $\Lambda = 0$, onda bismo kvadriranjem dobili da je

$$16(2+\sqrt{3})^{2n+1} = 3(9 \pm 4\sqrt{2})(3+2\sqrt{2})^{2m},$$

što je kontradikcija jer je jednakost oblika $a + b\sqrt{3} = c + d\sqrt{2}$, $a, b, c, d \in \mathbb{Q}$, moguća samo ako je $b = d = 0$. □

Primjena Baker-Wüstholzova teorema - *donja ograda*

Sada je sve spremno za primjenu Baker-Wüstholzova teorema 2.2.6 na formu Λ iz Leme 3.2.5. Imamo:

$$\begin{aligned}
\alpha_1 &= 2+\sqrt{3}, \\
\alpha_2 &= 3+2\sqrt{2}, \\
\alpha_3 &= \frac{2(4 \pm \sqrt{2})(3+\sqrt{3})}{21},
\end{aligned}$$

te

$$b_1 = n,\ b_2 = -m,\ b_3 = 1,\ d = 4,$$

jer je $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Cjelobrojni minimalni polinomi algebarskih brojeva $\alpha_1, \alpha_2, \alpha_3$ su

$$\begin{aligned} P_{\alpha_1}(x) &= x^2 - 4x + 1, \\ P_{\alpha_2}(x) &= x^2 - 6x + 1, \\ P_{\alpha_3}(x) &= 441x^4 - 2016x^3 + 2880x^2 - 1536x + 256, \end{aligned}$$

pa su visine

$$\begin{aligned} h(\alpha_1) &= \frac{1}{2}\ln(2 + \sqrt{3}) \approx 0.6585, \\ h(\alpha_2) &= \frac{1}{2}\ln(3 + 2\sqrt{2}) \approx 0.8814, \\ h(\alpha_3) &= \frac{1}{4}\ln\left(441 \cdot \frac{2(4 + \sqrt{2})(3 + \sqrt{3})}{21} \cdot \frac{2(4 - \sqrt{2})(3 + \sqrt{3})}{21}\right) \approx 1.7836. \end{aligned}$$

Dakle, Baker-Wüstholzov 2.2.6 teorem nam daje

$$\ln|\Lambda| \geq -18 \cdot 4! \cdot 3^4 \cdot (32 \cdot 4)^5 \cdot \ln 24 \cdot 0.6585 \cdot 0.8814 \cdot 1.7836 \ln n \geq -3.96 \cdot 10^{15} \ln n.$$

Usporedimo li ovo s (3.18), dobivamo nejednadžbu

$$-3.96 \cdot 10^{15} \ln n \leq \ln|\Lambda| < \ln 7.3 - 2n \ln(2 + \sqrt{3}),$$

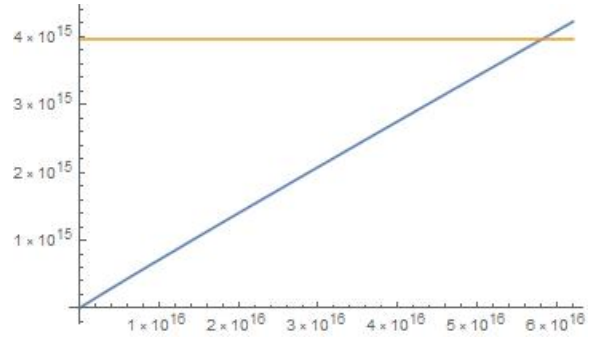
odnosno

$$3.96 \cdot 10^{15} \ln n > 2.63n - 1.99.$$

Ako prethodnu nejednakost zapišemo kao

$$f(n) = \frac{2.63n - 1.99}{\ln n} < 3.96 \cdot 10^{15} \tag{3.21}$$

možemo uočiti da smo strogo rastuću funkciju f ($f'(n) > 0$ za $n \geq 2$) ograničili s $3.96 \cdot 10^{15}$ pa ćemo za dovoljno velik n dobiti kontradikciju, kao što možemo vidjeti na grafu ispod.



Za $n = 6 \cdot 10^{16}$ dobivamo da je $f(n) > 4 \cdot 10^{15}$ što je u kontradikciji s nejednakošću (3.21). Stoga smo pokazali sljedeću tvrdnju.

Lema 3.2.6. *Ako je $v_n = w_m^{+,-}$ za $n, m \geq 2$, onda je $m < n < 6 \cdot 10^{16}$.*

Baker-Davenportova redukcija

Ograda na indekse m i n iz Leme 3.2.6 je prevelika da bismo preostale slučaje provjerili efektivno i tako dokazali Teorem 3.2.1. U tu svrhu primjenjuje se varijanta tzv. *Baker-Davenportove redukcije*. U sljedećoj lemi dana je varijanta koju su pokazali Dujella i Pethő u [6].

Lema 3.2.7. *Neka je κ iracionalni broj te N prirodni broj. Neka je $\frac{p}{q}$ konvergenta u razvoju verižnog razlomka od κ takva da je $q > 6N$ te neka su μ, A, B realni brojevi takvi da je $A > 0$ i $B > 1$. Neka je $\epsilon = ||\mu q|| - N \cdot ||\kappa q||$, gdje $||\,||$ označava udaljenost do najbližeg cijelog broja. Ako je $\epsilon > 0$, onda nejednadžba*

$$0 < n\kappa - m + \mu < A \cdot B^{-n}, \tag{3.22}$$

nema rješenja u prirodnim brojevima m i n takvima da vrijedi

$$\frac{\ln\left(\frac{Aq}{\epsilon}\right)}{\ln B} \leq n \leq N.$$

Dokaz. Pretpostavimo da je $1 \leq n \leq N$. Množenjem nejednakosti (3.22) s q i dodavanjem članova $\pm np$ imamo

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

Odavde je

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

jer je $n|\kappa q - p| < \frac{n}{q} < \frac{1}{2}$. Zaista, p/q je konvergenta od κ pa je $|\kappa - \frac{p}{q}| < \frac{1}{q^2}$ i $n < q/6$. Nadalje, kako je $|\mu q - (mq - np)| \geq ||\mu q||$, dobivamo

$$qAB^{-n} > ||\mu q|| - N||\kappa q|| = \epsilon,$$

što povlači da je

$$n < \frac{\ln\left(\frac{Aq}{\epsilon}\right)}{\ln B}.$$

□

Napomena 3.2.8. *Uvjet $q > 6N$ je donekle proizvoljan. Naime, s jedne strane želimo biti što sigurniji da će vrijediti uvjet $\epsilon > 0$, a s druge strane želimo da q bude što manji (da bi nova granica bila što manja). Iz svojstava konvergenti verižnih razlomaka, znamo da vrijedi $\|\kappa q\| < \frac{1}{q}$, dok o $\|\mu q\|$ općenito znamo samo da je $\leq \frac{1}{2}$. Zato je razumno uzeti da je barem $q > 2N$, a $q > 6N$ je eksperimentalno potvrđen kao dobar izbor.*

Napomena 3.2.9. *Ako uvjet $\epsilon > 0$ nije zadovoljen, onda možemo pokušati uzeti sljedeću konvergentu i provjeriti hoće li za nju uvjet biti zadovoljen. Čak i ako je $\epsilon < 0$, moguće je dobiti neku informaciju o n. Naime, ako označimo $r = \lfloor \mu q + \frac{1}{2} \rfloor$, onda je*

$$|np - mq + r| < qAB^{-n} + |\mu q - r| + n|\kappa q - p| \leq qAB^{-n} + \|\mu q\| + N\|\kappa q\| < qAB^{-n} + \frac{1}{2} + \frac{1}{6}.$$

Ako je $qAB^{-n} > \frac{1}{3}$, onda je $n < \frac{\ln(3Aq)}{\ln B}$. Ako je $qAB^{-n} \leq \frac{1}{3}$, onda je $np - mq + r = 0$, što znači da je $np \equiv -r \pmod q$. Ova kongruencija ima jedinstveno rješenje $n \equiv n_0 \pmod q$, pa iz $n \leq N < q$ slijedi da je $n = n_0$.

Napokon možemo dokazati Teorem 3.2.1: Primijenimo redukciju iz Leme 3.2.7 na formu Λ iz Leme 3.2.5 uz $N = 6 \cdot 10^{16}$. Prema (3.18) imamo

$$n \ln(2 + \sqrt{3}) - m \ln(3 + 2\sqrt{2}) + \ln \frac{2\sqrt{2}(1 + \sqrt{3})}{\sqrt{3}(2\sqrt{2} \pm 1)} < 7.3 \cdot (2 + \sqrt{3})^{-2n},$$

odnosno dijeljenjem s $\ln(3 + 2\sqrt{2})$

$$n \frac{\ln(2 + \sqrt{3})}{\ln(3 + 2\sqrt{2})} - m + \frac{1}{\ln(3 + 2\sqrt{2})} \ln \frac{2\sqrt{2}(1 + \sqrt{3})}{\sqrt{3}(2\sqrt{2} \pm 1)} < \frac{7.3}{\ln(3 + 2\sqrt{2})} \cdot (2 + \sqrt{3})^{-2n},$$

što je uz

$$\kappa = \frac{\ln(2 + \sqrt{3})}{\ln(3 + 2\sqrt{2})},\ \mu_{1,2} = \frac{\ln \frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)}}{\ln(3 + 2\sqrt{2})},\ A = \frac{7.3}{\ln(3 + 2\sqrt{2})},\ B = (2 + \sqrt{3})^2$$

upravo nejednakost (3.22).

Razvoj od κ u verižni razlomak je

$$[0, 1, 2, 1, 20, 1, 5, 3, 8, 5, 1, 2, 1, 1, 1, 1, 4, 3, 3, 3, 1, 6, 3, 1, 2, 22, 1, 2, 8, 2, 1, 2, 6, 3, 20, 2, 10, 3, \ldots],$$

a prva konvergenta od κ koja zadovoljava uvjet $q > 6N$ jednaka

$$\frac{p}{q} = \frac{742265900639684191}{993522360732597120}.$$

Vidjet ćemo da će za μ_1 trebati uzeti sljedeću konvergentu, pa promotrimo najprije što se dobije za μ_2. Imamo

$$\|\mu_2 q\| \approx 0.24492,\ \|\kappa q\| \cdot N \approx 0.01878,$$

pa je $\epsilon \approx 0.22614 > 0$. Stoga se traženje rješenja reducira za

$$n < \ln(\frac{Aq}{\epsilon})/(\ln B) < 16.84,$$

odnosno $n \leq 16$.

Primjenom Leme 3.2.7 za μ_1 i za gore navedene p, q, dobivamo negativan ϵ ($\|\mu_1 q\| \approx 0.007626$, $\|\kappa q\| \cdot N \approx 0.01878$). Stoga uzimamo sljedeću konvergentu

$$\frac{P}{Q} = \frac{2297570640187354392}{3075296607888933649}.$$

Dobivamo

$$\|\mu_1 Q\| \approx 0.2989,\ \|\kappa Q\| \cdot N \approx 0.002254,$$

pa je pripadni $\epsilon \approx 0.29665 > 0$ te možemo primijeniti redukciju, koja nam daje

$$n < \ln(\frac{Aq}{\epsilon})/(\ln B) < 17.17,$$

tj. $n \leq 17$.

Ponovimo li redukciju za $N = 17$, ponovno dobivamo da je odgovarajuća konvergenta

$$\frac{p'}{q'} = \frac{387}{518}$$

i redukcija nam daje $n \leq 4$.

Lako se provjerava da jednadžbe $v_n = w_m^{+,-}$ nemaju rješenja za $n = 3, 4$ i $m < n$. Tako smo dovršili dokaz tvrdnje da ako je $\{1, 3, 8, d\}$ Diofantova četvorka, onda mora biti $d = 120$.

Poglavlje 4

Biografije

4.1 Diofant

Diofant iz Aleksandrije rođen je između 201. i 215. godine. Napisao je niz knjiga o aritmetici, ali mnoge su s vremenom izgubljene. 6/13 je sačuvano, od kojih je najčuvenija *Aritmetika*. U četvrtom dijelu Aritmetike, 20. zadatak glasi:

Nađi četiri broja (kod Diofanta to je značilo pozitivna racionalna broja) *sa svojstvom da produkt svaka dva među njima uvećan za 1 daje kvadrat.*

Opisat ćemo kako je Diofant riješio taj zadatak. Dva broja s traženim svojstvom možemo dobiti tako da uzmemo $a = x$ i $b = x + 2$, pa je $ab + 1 = (x + 1)^2$. Par $\{a, b\}$ takav da je $ab + 1 = r^2$ do trojke možemo proširiti tako da uzmemo $c = a + b + 2r$. Zaista, tada je $ac + 1 = (a + r)^2$, $bc + 1 = (b + r)^2$. Tako se dobije $c = 4x + 4$. Sada istu konstrukciju primijenimo na par $\{a, c\}$ i jednakost $ac + 1 = (2x + 1)^2$. Dobivamo $d = x + (4x + 4) + 2(2x + 1) = 9x + 6$. Tako smo dobili skup $\{a, b, c, d\}$ koji zadovoljava pet od šest uvjeta iz definicije Diofantove četvorke. Jedini uvjet koji nedostaje jest da je $bd + 1$ kvadrat. Dakle, treba naći racionalno rješenje jednadžbe

$$9x^2 + 24x + 13 = y^2.$$

Diofant je znao kako riješiti jednadžbu ovakva tipa. Rješenje je tražio u obliku $y = 3x + t$, pa bi nakon uvrštavanja dobio linearnu jednadžbu u varijabli x. Pritom nije tražio opće rješenje jednadžbe, moguće i zbog poteškoća s tadašnjom matematičkom notacijom (kojoj je mnogo doprinio već uvođenjem slova za nepoznanice), već bi jednostavno uvrstio neku konkretnu vrijednost i dobio jedno rješenje. Tako je u ovom slučaju stavio $y = 3x - 4$ te dobio jednadžbu $48x = 3$ i rješenje $x = \frac{1}{16}$. Na taj način pronašao je prvi primjer onoga što danas nazivamo racionalna Diofantova četvorka

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

Čitajući Aritmetiku, Pierre de Fermat zaključuje da se jedna od jednadžbi koje Diofant razmatra ne može riješiti. Fermat je na marginama te knjige napisao "Pronašao sam briljantan dokaz ove tvrdnje, ali margine su preuske!", bez dodatnih pojašnjenja. Dakako, radi se o velikom Fermatovu teoremu kojeg je 1993. godine dokazao Andrew Wiles. O Diofantu se malo zna, ali ponešto doznajemo iz zapisa o brojevnim zagonetkama i mozgalicama grčkog povjesničara Metrodorusa iz 5. stoljeća. Jedan od zadataka, zvan Epitaf, navodno je prepisan s njegove nadgrobne ploče:

Ovdje leži Diofant, algebre div.
Koliko doživješe, kamen kaže siv:
Šestina života na dječaštvo mu pade,
Dvanaestina još dok mladost mu ne stade.
Još sedminu otpoče u bračnom zajedništvu.
Pet godina potom, obradova se sinu,
Ali to dobro biće ne bi duga vijeka,
Samo pola od očeva života dočeka.
Još četiri godine brojevima se tješio
I tako je život tog mudraca završio.

Rješenje jednadžbe $x = x/6 + x/12 + x/7 + 5 + x/2 + 4$ je $x = 84$ pa smatramo da je Diofant živio 84 godine.

4.2 Pierre de Fermat

Pierre de Fermat rođen je 1607. ili 1608. godine u malom gradu na jugu Francuske nedaleko od Toulousea. Iako je po zanimanju bio pravnik, većinu slobodnog vremena bavio se matematikom. Kako nije bio sklon pisanju, a u 17. stoljeću nije bilo znanstvenih časopisa, malo je radova objavio. U korespondenciji s uglednim matematičarima tog doba, ostavio je pozamašnu rukopisnu baštinu. Iz tih su prepiski proistekli vrijedni matematički rezultati.

Fermatov trag vidljiv je u brojnim granama matematike, a vjerojatno najviše u teoriji brojeva - kojom se bavio s posebnim zanosom otkad mu je u ruke dospjela Diofantova Aritmetika. Odlične intuicije, bio je u stanju postulirati tvrdnje čija se točnost potvrđivala desetljećima ili čak (u slučaju Velikog Fermatovog teorema) i stoljećima koja su uslijedila. Iako ga se smatra utemeljiteljem moderne teorije brojeva, njegov opus obuhvaća i vrijedne rezultate iz vjerojatnosti, geometrije i optike.

4.3 Alan Baker

Alan Baker rođen je 19. kolovoza 1939. u Londonu. Tamo pohađa srednju školu Stratford Grammar School po čijem završetku dobiva državnu stipendiju za sveučilište University College London, gdje s najvišim pohvalama ostvaruje titulu prvostupnika matematike. Godine 1961. odlazi na Trinity College Cambridge gdje postiže titulu magistra i nastavlja znanstveni rad pod mentorstvom profesora Harolda Davenporta. Doktorirao je godine 1965. na temi *Neki aspekti diofantskih aproksimacija*. Od 1964. do 1968. radi kao znanstveni novak na Cambridge-u, kada postaje voditelj matematičkog odsjeka i povremeno boravi u Sjedinjenim Državama, gdje 1970. postaje član Instituta za napredna istraživanja na Princetonu. Iste godine na kongresu matematičara u Nici dobiva najprestižnije od matematičkih priznanja, Fieldsovu medalju. Dodjelu je komentirao renomirani mađarski teoretičar brojeva Pal Turán: „Teorija transcendentnih brojeva, koju je začeo Liouville 1844., uvelike je obogaćena zadnjih godina radovima Alana Bakera, Wolfganga Schmidta i Vladimira Genadijeviča Sprindžuka, među kojima je Bakerov doprinos teoriji diofantskih jednadžbi od najvećeg značaja. Ova teorija, s poviješću duljom od tisuću godina, do početka stoljeća nije bila mnogo više od skupa izoliranih problema namijenjenih kreativnim *ad hoc* metodama. Bio je to Axel Thue koji je 1909. godine učinio proboj prema općim rezultatima dokazavši da sve diofantske jednadžbe oblika $f(x, y) = m$, gdje je m cijeli broj i f ireducibilna homogena binarna forma stupnja barem tri s cjelobrojnim koeficijentima, ima najviše konačno mnogo rješenja u cijelim brojevima."

Turán dalje navodi kako Carl Siegel i Klaus Roth nisu samo pronašli klase diofantskih jednadžbi za koje ovaj zaključak vrijedi, nego i dali ogradu za broj rješenja. Međutim, Baker je otišao korak dalje i proizveo rezultate koji bi, teoretski, mogli dovesti do potpunog rješenja te vrste problema. Dokazao je da za već opisane jednadžbe $f(x, y) = m$ postoji ograda B koja ovisi samo o m i cjelobrojnim koeficijentima od f za koju vrijedi

$$\max\{x_0, y_0\} \leq B$$

za svako rješenje (x_0, y_0). To povlači da je u principu moguće odrediti sva rješenja provjerom konačnog broja mogućnosti.

Vrijedi istaknuti i Bakerov doprinos Hilbertovom sedmom problemu, koji je pitao je li broj a^q transcendentan ako su a i q algebarski. Hilbert je očekivao da će rješenje tog problema biti kompliciranije od dokaza Riemannove slutnje. Neovisno jedan o drugome, taj su problem riješili Aleksandar Gelfond i Theodor Schneider 1934. godine. Baker je poopćio njihov rezultat (Teorem 2.2.1) stvorivši klasu prethodno nezabilježenih transcendentnih brojeva i pokazao kako se pozadinska teorija može primijeniti na rješavanje raznih diofantskih problema. Turan zaključuje sljedećim riječima: „Bakerov rad uvjerljivo naglašava dvije stvari. Prvo, bez podcjenjivanja vrijedne težnje za začećem nove teorije kako

bi se riješio neki problem, isplati se napasti konkretan težak problem izravno. Drugo, pokazuje kako se rješenje nekog problema razvija sasvim prirodno unutar zdrave teorije i brzo dolazi u plodan dodir s važnim matematičkim pitanjima."

Godine 1974. postaje profesor teorijske matematike na Cambridgeu i gostujući profesor na Stanfordu. Držao je predavanja i na drugim prestižnim sveučilištima diljem svijeta. Istaknuti Bakerovi udžbenici iz teorije brojeva su *Teorija transcendentnih brojeva* (1975), *Koncizni uvod u teoriju brojeva* (1984), (s Gisbertom Wüstholzom) *Forme u logaritmima i diofantska geometrija* (2007) i *Sveobuhvatni tečaj iz teorije brojeva* (2012). Osim Fieldsove medalje, Baker je dobitnik brojnih nagrada i priznanja, među kojima izdvajamo Adamsovu nagradu od sveučilišta u Cambridgeu (1972) i članstvo u *Royal Society of London* (1973).

Izvan matematike, Baker za svoje interese navodi fotografiju i kazalište. Preminuo je 4. veljače 2018. u Cambridgeu.

Bibliografija

[1] A. Baker, H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, The Quarterly Journal of Mathematics **20** (1969), 129–137.

[2] M. Cipu, Y. Fuita, T. Miyazaki, *On the number of extensions of a Diophantine triple*, Int. J. Number Theory **14** (2018), 899–917.

[3] A. Dujella, *Diophantine m-tuples* `https://web.math.pmf.unizg.hr/~duje/intro.html`

[4] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

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

[6] A. Dujella, A. Pethó, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) **49** (1998), 291–306.

[7] A. Dujella, V. Petričević, *Strong Diophantine triples*, Experiment. Math. **17** (2008), 83–89.

[8] A. Dujella, M. Kazalicki, M. Mikić, M. Szikszai, *There are infinitely many rational Diophantine sextuples*, Int.Math.Res.Not.IMRN **2017 (2)** (2017), 490–508.

[9] A. Filipin, Z. Franušić, *Diofantovi skupovi*, skripta, `https://web.math.pmf.unizg.hr/~fran/Diofantovi%20skupovi/DS-skripta.pdf` , 2020.

[10] P.E. Gibbs, *A survey of rational Diophantine sextuples of low height*, preprint, 2016.

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

[12] G. Martin, S. Sitar, *Erdos-Turan with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples,* Mathematika **57** (2011), 1–29.

[13] M. Stoll, *Diagonal genus 5 curves, elliptic curves over $\mathbb{Q}(t)$, and rational Diophantine quintuples*, Acta Arith. **190** (2019), 239–261.

[14] T. Prekpaljaj, I. Purgar, *Pierre de Fermat*, Seminar za kolegij Životopisi matematičara, 2013.

[15] P. Turán, *On the work of Alan Baker*, Actes du Congrès International des Mathématiciens, Nice, 1970 Vol. 1 (Paris, 1971), 3-5.

[16] Web stranica `https://mathshistory.st-andrews.ac.uk/Biographies/Baker_Alan/`

Sažetak

Fermatova četvorka je skup $\{1, 3, 8, 120\}$ sa svojstvom da je umnožak bilo koja dva njegova elementa uvećan za 1 potpuni kvadrat. Općenito, skupovi od m prirodnih brojeva s danim svojstvom nazivaju se Diofantove m-torke. U ovom radu pokazujemo da ako je $\{1, 3, 8, d\}$ Diofantova četvorka, tada je $d = 120$. To su izvorno dokazali Baker i Davenport u [1], gdje su uveli metodu osnovanu na teoriji linearnih formi u logaritmima algebarskih brojeva i metodu redukcije temeljenu na verižnim razlomcima.

Summary

Fermat's quadruple is a set $\{1, 3, 8, 120\}$ with a property that the product of any two of its elements increased by 1 is a perfect square. Generally, sets of m positive integers with the given property are called Diophantine m-tuples. In this thesis, we show that if $\{1, 3, 8, d\}$ is a Diophantine quadruple, then $d = 120$. This was originally proved by Baker and Davenport in [1], where they introduced a method based on the theory of linear forms in the logarithms of algebraic numbers and a reduction method based on continued fractions.

Životopis

Rođen sam 8. 10. 1993. u Zagrebu, gdje sam završio osnovnu i srednju školu. U drugom razredu dobivam izravan upis na PMF kao nagradu za peto mjesto na državnom natjecanju iz fizike. Od ostalih ostvarenja volim istaknuti neplaniran plasman na državna natjecanja iz kemije u prvom i trećem razredu. Fiziku upisujem 2012., a nastavnički smjer matematika - fizika 2016. godine. Sljedeće godine držim demonstrature iz tri matematička kolegija. 2020. godine radim kao nastavnik matematike u Tehničkoj školi Ruđera Boškovića, gdje sam i sada zaposlen. Od 2019. sam šahovski majstor (titula FM).