Razlomački skupovi

Crevar, Renata

Master's thesis / Diplomski rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:538998

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Renata Crevar

RAZLOMAČKI SKUPOVI

Diplomski rad

Voditelj rada:
doc. dr. sc. Tomislav Pejković

Zagreb, srpanj 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. _____

Zahvaljujem se svom mentoru doc.dr.sc. Tomislavu Pejkoviću na pruženoj pomoći te motiviranju tijekom izrade diplomskog rada. Najviše se zahvaljujem mojoj obitelji koja je cijelo moje školovanje bila uz mene i bodrila me dajući mi snagu, ljubav i podršku.Od srca vam se zahvaljujem te ovaj rad posvećujem upravo vama.

Sadržaj

Uvod

Teorija brojeva spada među najstarije grane matematike. Prvi tragovi teorije brojeva mogu se pronaći kod Babilonaca iz polovice trećeg tisućljeća prije Krista. Tijekom duge povijesti teorija brojeva često se smatrala "najčišćom" granom matematike jer je bila najdalja od bilo kakvih konkretnih primjena. Međutim, sredinom 70-ih godina 20. stoljeća nastupa bitna promjena, tako da je danas teorija brojeva jedna od najvažnijih grana matematike za primjene u kriptografiji i sigurnoj razmjeni informacija. Ona se ponajprije bavi proučavanjem svojstava skupa prirodnih brojeva $\mathbb{N}$, zatim cijelih brojeva $\mathbb{Z}$, te skupa racionalnih brojeva $\mathbb{Q}$. Prirodan problem teorije brojeva je proučavanje razlomačkih skupova u skupu realnih i u skupu p-adskih brojeva za dani prost broj p.

U ovom radu su prvo navedeni temeljni pojmovi potrebni za razumijevanje daljnjeg rada, te tvrdnje koje se upotrebljavaju u kasnijim dokazima. U drugom poglavlju se bavimo razlomačkim skupovima u skupu realnih brojeva dokazujući ono što su njihovi autori nazvali četiri dragulja, odnosno četiri zanimljiva teorema o razlomačkim skupovima. U sljedećem poglavlju promatramo razlomačke skupove u p-adskim brojevima. Tu najprije uspoređujemo situaciju u realnim i p-adskim brojevima, to jest koji uvjeti da bi skup bio razlomački gust u skupu realnih brojeva vrijede i u skupu p-adskih brojeva. Zatim smo gledali slučaj kada je skup sastavljen od suma potencija (suma kvadrata i suma kubova) pitajući se kada je razlomački skup gust u $\mathbb{Q}_p$. Nakon toga smo uspostavili rezultat za određene nizove zadane rekurzijama drugog reda što uključuje Fibonaccijeve brojeve kao poseban slučaj. Na kraju smo promatrali unije geometrijskih nizova ograničivši se na neparne proste brojeve p.

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.

Poglavlje 1

Osnovne definicije i teoremi

Na početku ćemo definirati neke osnovne pojmove i teoreme bitne za razumijevanje sljedećih poglavlja.

Definicija 1.1. *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b djeljiv sa a, to jest da a dijeli b, ako postoji cijeli broj k takav da je $b = ak$. To zapisujemo sa $a \mid b$. Ako b nije djeljiv sa a, onda pišemo $a \nmid b$.*

Teorem 1.2 (**Teorem o dijeljenju s ostatkom**). *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je $b = qa + r$, $0 \leq r < a$.*

Dokaz. Dokaz možete pronaći u [3] na stranici 2. □

Definicija 1.3. *Prirodan broj $p > 1$ nazivamo prost broj ako je djeljiv samo s 1 i sa samim sobom. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je složen.*

Teorem 1.4. *Ako je p prost i $p \mid ab$, onda $p \mid a$ ili $p \mid b$.*

Dokaz. Dostupno u [3] na stranici 7. □

Definicija 1.5. *Neka su b i c cijeli brojevi. Cijeli broj a zovemo zajednički djelitelj od b i c ako $a \mid b$ i $a \mid c$. Ako je barem jedan od brojeva b i c različit od nule, onda postoji samo konačno mnogo zajedničkih djelitelja od b i c. Najveći među njima zove se najveći zajednički djelitelj od b i c i označava se s* $\mathrm{nzd}(b, c)$. *Slično se definira najveći zajednički djelitelj brojeva $b_1, b_2, \ldots, b_n$ koji nisu svi jednaki nuli, te se označava s* $\mathrm{nzd}(b_1, b_2, \ldots, b_n)$.

Definicija 1.6. *Reći ćemo da su cijeli brojevi a i b relativno prosti ako je* $\mathrm{nzd}(a, b) = 1$. *Za cijele brojeve $a_1, a_2, \ldots, a_n$ reći ćemo da su relativno prosti ako je* $\mathrm{nzd}(a_1, a_2, \ldots, a_n) = 1$, *a da su u parovima relativno prosti ako je* $\mathrm{nzd}(a_i, a_j) = 1$ *za sve $1 \leq i, j \leq n, i \neq j$*

Definicija 1.7. *Ako cijeli broj $m \neq 0$ dijeli razliku $a - b$, onda kažemo da je a kongruentan b modulo m i pišemo $a \equiv b \pmod{m}$. U protivnom, kažemo da a nije kongruentan b modulo m i pišemo $a \not\equiv b \pmod{m}$.*

Teorem 1.8. *Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$.*

Dokaz. Dokaz se nalazi u [3] na stranici 12. □

Definicija 1.9. *Skup $\{x_1, \ldots, x_m\}$ zove se potpuni sustav ostataka modulo m ako za svaki $y \in \mathbb{Z}$ postoji točno jedan x_j takav da je $y \equiv x_j \pmod{m}$. Drugim riječima, potpuni sustav ostataka dobivamo tako da iz svake klase ekvivalencije modulo m uzmemo po jedan član.*

Teorem 1.10. *Neka su a i m prirodni, te b cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ ima rješenja ako i samo ako $d = \text{nzd}(a, m)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo m.*

Dokaz. Dokaz se nalazi u [3] na stranici 14. □

Teorem 1.11 (**Kineski teorem o ostatcima).** *Neka su $m_1, m_2, \ldots, m_r$ u parovima relativno prosti prirodni brojevi, te neka su $a_1, a_2, \ldots, a_r$ cijeli brojevi. Tada sustav kongruencija*

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2}, \ldots,\ x \equiv a_r \pmod{m_r} \tag{1.1}$$

ima rješenja. Ako je x_0 jedno rješenje, onda su sva rješenja od (1.1) dana sa $x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$.

Dokaz. Dokaz se nalazi u [3] na stranici 15. □

Definicija 1.12. *Reducirani sustav ostataka modulo m je skup cijelih brojeva r_i sa svojstvom da je $\text{nzd}(r_i, m) = 1, r_i \not\equiv r_j \pmod{m}$ za $i \neq j$, te da za svaki cijeli broj x takav da je $\text{nzd}(x, m) = 1$ postoji r_i takav da je $x \equiv r_i \pmod{m}$. Jedan reducirani sustav ostataka modulo m je skup svih brojeva $a \in \{1, 2, \ldots, m\}$ takvih da je $\text{nzd}(a, m) = 1$. Svi reducirani sustavi ostataka modulo m imaju isti broj elemenata. Taj broj označavamo sa $\varphi(m)$, a funkciju $\varphi(m)$ zovemo Eulerova funkcija.*

Teorem 1.13. *Eulerova funkcija φ je multiplikativna, tj. $\varphi(1) = 1$ i za svaka dva relativno prosta prirodna broja a i b je $\varphi(ab) = \varphi(a)\varphi(b)$. Nadalje, za svaki prirodan broj $n > 1$ vrijedi $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ gdje umnožak ide po svim prostim brojevima koji dijele n.*

Dokaz. Dokaz se nalazi u [3] na stranici 18. □

Teorem 1.14 (**Eulerov teorem).** *Ako je* $\text{nzd}(a, m) = 1$, *tada je* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Dokaz. Dokaz se nalazi u [3] na stranici 18. □

Teorem 1.15 (**Mali Fermatov teorem).** *Neka je p prost broj. Ako* $p \nmid a$, *onda je* $a^{p-1} \equiv 1 \pmod{p}$. *Za svaki cijeli broj a vrijedi* $a^p \equiv a \pmod{p}$.

Dokaz. Dokaz dobivamo direktno iz prethodna dva teorema. □

Definicija 1.16. *Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je* $a^d \equiv 1 \pmod{n}$ *zove se red od a modulo n. Još se kaže da a pripada eksponentu d modulo n.*

Definicija 1.17. *Ako je red od a modulo n jednak* $\varphi(n)$, *onda se a zove primitivni korijen modulo n.*

Teorem 1.18. *Za prirodan broj n postoji primitivni korijen modulo n ako i samo ako je* $n = 2, 4, p^j$ *ili* $2p^j$, *gdje je p neparan prost broj.*

Dokaz. Dokaz se nalazi u [3] na stranici 25. □

Definicija 1.19. *Neka je* $\text{nzd}(a, m) = 1$. *Ako kongruencija* $x^2 \equiv a \pmod{m}$ *ima rješenja, onda kažemo da je a kvadratni ostatak modulo m. U protivnom kažemo da je a kvadratni neostatak modulo m.*

Teorem 1.20. *Neka je p prost broj. Tada kongruencija* $x^2 \equiv -1 \pmod{p}$ *ima rješenja ako i samo ako je* $p = 2$ *ili* $p \equiv 1 \pmod{4}$.

Dokaz. Dokaz se nalazi u [3] na stranici 21. □

Teorem 1.21 (**Fermatov teorem).** *Prirodan broj n se može prikazati u obliku* $n = x^2 + y^2$, $x, y \in \mathbb{Z}$ *ako i samo ako se u rastavu broja n na proste faktore svaki prosti faktor p za koji je* $p \equiv 3 \pmod{4}$ *javlja s parnom potencijom.*

Dokaz. Dokaz se nalazi u [3] na stranici 43. □

Teorem 1.22 (**Lagrangeov teorem o četiri kvadrata).** *Svaki prirodan broj n može se prikazati u obliku sume četiri cijela broja, to jest u obliku* $n = x^2 + y^2 + z^2 + w^2$, $x, y, z, w \in \mathbb{Z}$.

Dokaz. Dokaz se nalazi u [3] na stranici 45. □

Sada se prisjetimo definicije apsolutne vrijednosti.

Definicija 1.23. *Neka je K polje. Funkcija* $|\cdot| : K \to \mathbb{R}$ *se zove apsolutna vrijednost ako za sve* $x, y \in K$ *vrijedi:*

1) $|x| \geq 0$, $|x| = 0$ *ako i samo ako* $x = 0$.

2) $|xy| = |x||y|$.

3) $|x + y| \leq |x| + |y|$ *(nejednakost trokuta)*

Definicija 1.24. *Za apsolutnu vrijednost* $|\cdot|$ *na* K *kažemo da je nearhimedska ako uz nejednakost trokuta vrijedi i jača nejednakost*

$$|x + y| \leq max\{|x|, |y|\},$$

za svaki $x, y \in K$.

Ako apsolutna vrijednost nije nearhimedska, kažemo da je arhimedska.

Poznajemo standardnu apsolutnu vrijednost na $\mathbb{Q}$, odnosno $\mathbb{R}$ koja je arhimedska. No, na $\mathbb{Q}$ se mogu definirati i neke nearhimedske apsolutne vrijednosti. Neka je p prost broj. Tada svaki $x \in \mathbb{Q}, x \neq 0$, ima jedinstven prikaz u obliku

$$x = \frac{a}{b} \cdot p^{v_p(x)}, \quad p \nmid ab, \quad v_p(x) \in \mathbb{Z}$$

Funkcija $x \longmapsto v_p(x)$ naziva se *p-adska valuacija*, a funkcija

$$|x|_p = \begin{cases} p^{-v_p(x)}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

p-adska norma i nije teško provjeriti da je to nearhimedska apsolutna vrijednost koju zovemo *p-adska apsolutna vrijednost*.

Ako je $|\cdot|$ apsolutna vrijednost, tada je i $|\cdot|^\alpha$ apsolutna vrijednost za svaki $\alpha \in \mathbb{R}^\times$. Takve dvije apsolutne vrijednosti induciraju istu topologiju na K pa kažemo da su ekvivalentne. Trivijalna apsolutna vrijednost na K definirana je sa

$$|x| = \begin{cases} 0, & \text{ako je } x = 0 \\ 1, & \text{ako je } x \neq 0 \end{cases}$$

Teorem 1.25 (Teorem Ostrowskog za polje $\mathbb{Q}$). *Svaka netrivijalna apsolutna vrijednost na* $\mathbb{Q}$ *je ekvivalentna običnoj apsolutnoj vrijednosti ili p-adskoj apsolutnoj vrijednosti za neki prost broj p.*

Dokaz. Neka je $|\cdot|$ netrivijalna apsolutna vrijednost na $\mathbb{Q}$. Postoje dva moguća slučaja.

1.slučaj. Pretpostavimo da je $|\cdot|$ arhimedska apsolutna vrijednost. Želimo pokazati da je ekvivalentna s "običnom" (∞-adskom) apsolutnom vrijednosti. Neka je n_0 najmanji prirodan broj za koji je $|n_0| > 1$ (postoji takav jer bi u protivnom apsolutna vrijednost $|\cdot|$ bila nearhimedska). Sada možemo pronaći pozitivan realan broj α takav da vrijedi

$$|n_0| = n_0^\alpha.$$

Uzmimo sada proizvoljan cijeli broj n i napišemo ga u obliku

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k,$$

za $0 \leq a_i \leq n_0 - 1, a_k \neq 0$. Primijetimo da je k određen s $n_0^k \leq n < n_0^{k+1}$ iz čega slijedi

$$k = \left\lfloor \frac{\log n}{\log n_0} \right\rfloor.$$

Sada djelujemo s apsolutnom vrijednošću na n i dobivamo

$$|n| = |a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k| \leq |a_0| + |a_1| n_0^\alpha + |a_2| n_0^{2\alpha} + \cdots + |a_k| n_0^{k\alpha}.$$

Kako smo odabrali n_0 kao najmanji prirodan broj čija je apsolutna vrijednost veća od 1, znamo da je $|a_i| \leq 1$ te dobivamo da je

$$|n| \leq 1 + n_0^\alpha + n_0^{2\alpha} + \cdots + n_0^{k\alpha} = n_0^{k\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-k\alpha}) \leq n_0^{k\alpha} \sum_{i=0}^{\infty} n_0^{-i\alpha} = n_0^{k\alpha} \frac{n_0^\alpha}{n_0^\alpha - 1}.$$

Uvedimo supstituciju $C = \frac{n_0^\alpha}{n_0^\alpha - 1}$, pa prethodna nejednakost izgleda

$$|n| \leq C n_0^{k\alpha} \leq C n^\alpha.$$

Ova nejednakost vrijedi za svaki n (budući da smo ga odabrali proizvoljno) i sada uzmemo neki veliki N te primijenimo nejednakost na n^N i dobivamo

$$|n^N| \leq C n^{N\alpha}.$$

Uzimajući N-ti korijen, slijedi

$$|n| \leq \sqrt[N]{C} n^\alpha.$$

Pustimo $N \to \infty$ pa je $\sqrt[N]{C} \to 1$ te tako dobivamo nejednakost $|n| \leq n^\alpha$.

Sada želimo pokazati da vrijedi $|n| \geq n^\alpha$. Iz zapisa za n i iz $n_0^{k+1} > n \geq n_0^k$ dobivamo

$$n_0^{(k+1)\alpha} = |n_0^{k+1}| = |n + n_0^{k+1} - n| \leq |n| + |n_0^{k+1} - n|.$$

Iskoristimo dobivenu gornju ogradu $|n_0^{k+1} - n| \leq (n_0^{k+1} - n)^\alpha$ i $n \geq n_0^k$ da dobijemo

$$|n| \geq n_0^{(k+1)\alpha} - \left(n_0^{k+1} - n\right)^\alpha = n_0^{(k+1)\alpha} \left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right) = C' n_0^{(k+1)\alpha} \geq C' n^\alpha,$$

gdje je $C' = 1 - \left(1 - \frac{1}{n_0}\right)^\alpha$ pozitivan broj koji ne ovisi o n. Sada kao maloprije umjesto n promatramo n^N, uzmemo N-ti korijen i pustimo da $N \to \infty$ te dobivamo traženu nejednakost $|n| \geq n^\alpha$. Dakle, $|n| = n^\alpha$. Jasno je da je $|x| = |x|_\infty^\alpha$ za svaki $x \in \mathbb{Q}$. To dokazuje da je $|\cdot|$ ekvivalentna običnoj apsolutnoj vrijednosti.

2.slučaj. Neka je $|\cdot|$ nearhimedska apsolutna vrijednost. Kako je $|\cdot|$ netrivijalna, mora postojati najmanji cijeli broj n_0 takav da je $|n_0| < 1$. Prvo moramo provjeriti da je n_0 prost broj. Pretpostavimo da je $n_0 = a \cdot b$ gdje su a, b manji od n_0. Po našem izboru za n_0, imali bismo $|a| = |b| = 1$ i $|n_0| < 1$, što ne može vrijediti. Dakle, n_0 je prost broj i označavamo ga s p. Želimo pokazati da je $|\cdot|$ ekvivalentna p-adskoj apsolutnoj vrijednosti. Ako n nije djeljiv s p, tada je $|n| = 1$. Naime, ako n podijelimo s p, imat ćemo $n = rp + s$ gdje je $0 < s < p$, te su $r, s \in \mathbb{Z}$. S obzirom na minimalnost broja p, slijedi $|s| = 1$. Također, $|rp| < 1$ jer je $|r| \leq 1$ ($|\cdot|$ je nearhimedska) i $|p| < 1$ (po konstrukciji). Dakle, $|n| = 1$. Konačno, svaki $n \in \mathbb{Z}$ zapisujemo kao $n = p^v n'$ za $p \nmid n'$. Tada je

$$|n| = |p^v n'| = |p^v||n'| = |p|^v = c^{-v},$$

gdje je $c = |p|^{-1} > 1$. Dakle, $|\cdot|$ je ekvivalentna p-adskoj apsolutnoj vrijednosti. □

Polje s metrikom naziva se potpunim ako svaki Cauchyjev niz u njemu konvergira. Neka je $\mathcal{R} = \{(a_n)_n : (a_n)_n$ je Cauchyjev niz u $\mathbb{Q}$ s obzirom na standardnu apsolutnu vrijednost$\}$. Lako se vidi da je $\mathcal{R}$ zatvoren na operacije zbrajanja i množenja:

$$(x_n)_n + (y_n)_n = (x_n + y_n)_n$$
$$(x_n)_n \cdot (y_n)_n = (x_n y_n)_n$$

Kažemo da su dva niza $(x_n), (y_n) \in \mathcal{R}$ ekvivalentna i pišemo $(x_n)_n \sim (y_n)_n$ ako je $\lim_{n\to\infty}(x_n - y_n) = 0$. Neka je $\mathbb{R} = \mathcal{R}/\sim$ skup klasa ekvivalencije Cauchyjevih nizova. Može se provjeriti da $\mathbb{R}$ uz operacija zbrajanja i množenja te prirodni uređaj zadovoljava aksiome polja realnih brojeva. Ovaj postupak konstrukcije polja $\mathbb{R}$ iz polja $\mathbb{Q}$ se naziva upotpunjenje polja $\mathbb{Q}$ u odnosnu na standardnu apsolutnu vrijednost.

Analogno se provodi upotpunjenje i za ostale apsolutne vrijednosti na $\mathbb{Q}$. Kako polje $\mathbb{Q}$ nije potpuno u odnosu na normu $|\cdot|_p$, njegovim upotpunjenjem dobivamo polje $\mathbb{Q}_p$. To znači da se norma $|\cdot|_p$ može proširiti sa $\mathbb{Q}$ na $\mathbb{Q}_p$. Takav $\mathbb{Q}_p$ je potpun u odnosu na $|\cdot|_p$ i $\mathbb{Q}$ je gust u $\mathbb{Q}_p$. Svaki $\alpha \in \mathbb{Q}_p$ se može na jedinstven način zapisati u obliku

$$\alpha = \sum_{k \geq v_p(\alpha)} a_k p^k,$$

gdje je $v_p(\alpha) \in \mathbb{Z}$, a za znamenke a_k vrijedi $0 \leq a_k < p$.

Elemente od $\mathbb{Q}_p$ zovemo *p-adski brojevi*, a elemente za koje je $|\alpha|_p \leq 1$, zovemo *p-adski cijeli brojevi* i skup svih takvih elemenata označavamo sa $\mathbb{Z}_p$.

Poglavlje 2

Razlomački skupovi u realnim brojevima

Razlomački skup je skup kojeg dobivamo kada uzmemo kvocijent svakog para elemenata danog podskupa skupa prirodnih brojeva. Neka je $A \subseteq \mathbb{N}$ podskup skupa prirodnih brojeva. Tada je $R(A) = \{a/b : a, b \in A\}$ njemu pridruženi *razlomački skup* (odnosno kvocijentni skup).

Neka je $A(x) = A \cap [1, x]$ tako da $|A(x)|$ predstavlja broj elemenata u skupu A koji su $\leq x$. *Donja asimptotska gustoća* od A je broj

$$\underline{d}(A) = \liminf_{n\to\infty} \frac{|A(n)|}{n}$$

koji očito zadovoljava $0 \leq \underline{d}(A) \leq 1$. Kažemo da je A *razlomački gust* ako je zatvarač od $R(A)$ u $\mathbb{R}$ jednak $[0, \infty)$, to jest ako je $R(A)$ gust u $[0, \infty)$.
Dokazat ćemo četiri zanimljiva teorema o razlomačkim skupovima.

1. Skup svih prirodnih brojeva čiji prikaz u bazi b započinje znamenkom 1 je razlomački gust za $b = 2, 3, 4$, ali nije razlomački gust za $b \geq 5$.

2. Za svaki $\delta \in [0, \frac{1}{2})$ postoji skup $A \subset \mathbb{N}$ takav da je $\underline{d}(A) = \delta$, ali A nije razlomački gust. S druge strane, ako je $\underline{d}(A) \geq \frac{1}{2}$, onda A mora biti razlomački gust.

3. Možemo particionirati $\mathbb{N}$ u tri skupa tako da nijedan od njih nije razlomački gust. No, nemoguća je takva particija u samo dva skupa.

4. Postoje podskupovi od $\mathbb{N}$ koji sadrže proizvoljno duge artimetičke nizove, a ipak nisu razlomački gusti. S druge strane, postoji razlomački gust skup koji ne sadrži aritmetički niz duljine ≥ 3.

2.1 Prvi teorem

Teorem 2.1. *Skup svih prirodnih brojeva čiji prikaz u bazi b započinje znamenkom* 1 *je razlomački gust za* $b = 2, 3, 4$, *ali nije razlomački gust za* $b \geq 5$.

Da bismo dokazali ovaj teorem, potrebna nam je sljedeća tvrdnja.

Propozicija 2.2. *Neka* $1 < a \leq b$. *Skup*

$$A = \bigcup_{k=0}^{\infty} [b^k, ab^k) \cap \mathbb{N} \tag{2.1}$$

je razlomački gust ako i samo ako je $b \leq a^2$. *Nadalje, imamo* $\underline{d}(A) = \frac{a-1}{b-1}$.

Dokaz. Prvo ćemo izračunati $\underline{d}(A)$. Budući da je brojeća funkcija $|A(x)|$ neopadajuća na svakom intervalu $[b^k, ab^k)$ i konstantna na svakom intervalu $[ab^k, b^{k+1})$, slijedi

$$\begin{aligned} \liminf_{n\to\infty} \frac{|A(n)|}{n} &= \liminf_{n\to\infty} \frac{1}{b^n} \sum_{k=0}^{n-1} \left|[b^k, ab^k) \cap \mathbb{N}\right| \\ &= \lim_{n\to\infty} \frac{1}{b^n} \sum_{k=0}^{n-1} (a-1)b^k \\ &= \lim_{n\to\infty} \frac{(a-1)\,(b^n-1)}{b^n(b-1)} \\ &= \frac{a-1}{b-1} \end{aligned} \tag{2.2}$$

Koristili smo činjenicu da je razlika između $ab^k - b^k$ i $|[b^k, ab^k) \cap \mathbb{N}|$ manja ili jednaka 1. Sada kad smo izračunali $\underline{d}\,(A)$, promatramo razlomačku gustoću.

1. *slučaj.* Pretpostavimo da je $a^2 < b$. Po konstrukciji, svaki kvocijent elemenata od A pripada intervalu oblika $I_\ell = (a^{-1}b^\ell, ab^\ell)$ za neki cijeli broj ℓ. Ako je $j < k$, onda je $a^2 < b^{k-j}$ odakle slijedi $ab^j < a^{-1}b^k$ tako da je svaki element iz I_ℓ strogo manji od svakog elementa iz I_k. Stoga $R(A)$ ne sadrži elemente ni iz jednog intervala oblika $[ab^\ell, a^{-1}b^{\ell+1}]$, a svaki od tih intervala je neprazan zbog $a^2 < b$. Dakle, A nije razlomački gust.

2. *slučaj.* Neka je sada $b \leq a^2$. Primijetimo da je

$$(0, \infty) = \bigcup_{j\in\mathbb{Z}} \left[\frac{b^j}{a}, b^j\right) \cup [b^j, ab^j).$$

Pretpostavimo da ξ pripada intervalu $[b^j, ab^j)$ za neki cijeli broj j. Za $\epsilon > 0$ neka je k dovoljno velik tako da vrijedi $1 < b^k\epsilon$ te uočimo

$$b^{j+k} \leq b^k\xi < ab^{j+k}.$$

Neka je ℓ jedinstveni prirodni broj koji zadovoljava

$$b^{j+k} + \ell \leq b^k\xi < b^{j+k} + \ell + 1 \tag{2.3}$$

i

$$0 \leq \ell \leq (a-1)b^{j+k} - 1. \tag{2.4}$$

Iz (2.3) vidimo

$$0 \leq b^k\xi - \left(b^{j+k} + \ell\right) < 1$$

iz čega slijedi

$$0 \leq \xi - \frac{b^{j+k} + \ell}{b^k} < \epsilon.$$

Budući da (2.4) osigurava da $b^{k+j}+\ell$ pripada intervalu $[b^{j+k}, ab^{j+k})$, zaključujemo da $\frac{b^{j+k}+\ell}{b^k}$ pripada $R(A)$. Sličan argument se primjenjuje ako ξ pripada intervalu $\left[\frac{b^j}{a}, b^j\right)$. Uzevši sve u obzir, zaključujemo da je A razlomački gust. □

Propozicija 2.2 povlači naš prvi teorem o razlomačkim skupovima tako da za $a = 2$ i cijeli broj $b \geq 2$, definiramo skup

$$A = \bigcup_{k=0}^{\infty} [b^k, ab^k) \cap \mathbb{N}.$$

To je upravo skup svih prirodnih brojeva čiji prikaz u bazi b započinje znamenkom 1. Nejednakost $b \leq a^2$ vrijedi upravo za baze $b = 2, 3, 4$, ali ne vrijedi za $b \geq 5$.

2.2 Drugi teorem

Vidjeli smo da postoje skupovi koji nisu razlomački gusti, iako im je donja asimptotska gustoća pozitivna. Stoga se postavlja pitanje postoji li kritična vrijednost $0 < \kappa < 1$ takva da $\kappa \leq \underline{d}(A)$ nužno povlači da je A razlomački gust. Sljedeći rezultat pokazuje da postoji takva kritična vrijednost i jednaka je $\kappa = \frac{1}{2}$.

Teorem 2.3. *Za svaki $\delta \in [0, \frac{1}{2})$ postoji skup $A \subset \mathbb{N}$ takav da je $\underline{d}(A) = \delta$, ali A nije razlomački gust. S druge strane, ako je $\underline{d}(A) \geq \frac{1}{2}$, onda A mora biti razlomački gust.*

Ako je $0 \leq \delta < \frac{1}{2}$, onda možemo pisati $\delta = \frac{1}{2+\epsilon}$ gdje je $\epsilon > 0$. Neka su sada $a = 1 + \frac{\epsilon}{2}$ i $b = 1 + \epsilon + \frac{1}{2}\epsilon^2$ pa vrijedi $1 < a^2 < b$. Za ove parametre, Propozicija 2.2 kaže da skup A definiran s (2.1) zadovoljava $\underline{d}(A) = \delta$ i nije razlomački gust. Ako je $\delta = 0$, tada vidimo da skup $A = \{2^n : n \in \mathbb{N}\}$ nije razlomački gust i za njega vrijedi $\underline{d}(A) = 0$.

Dakle, možemo konstruirati skupove koji imaju donju asimptotsku gustoću po volji blizu $\frac{1}{2}$, ali koji nisu razlomački gusti. S druge strane, jasno je da postoje razlomački gusti skupovi takvi da je $\underline{d}(A) = \frac{1}{2}$, primjerice skup parnih brojeva $A = \{2, 4, 6, ..\}$. Međutim, pitanje može li skup koji nije razlomački gust imati donju asimptotsku gustoću *jednaku* kritičnoj vrijednosti $\frac{1}{2}$ je mnogo teže.

U kasnim šezdesetim godinama 20. stoljeća, slovački matematičkar Tibor Šalát je predložio primjer skupa $A \subset \mathbb{N}$ koji nije razlomački gust, ali je $\underline{d}(A) = \frac{1}{2}$. Međutim, njegov primjer nije bio ispravan što je istaknuto u ispravku istog rada objavljenom godinu dana kasnije.

Godine 1998. Strauch i Tóth pokazali su općenitiji rezultat koji povlači da skup koji zadovoljava $\underline{d}(A) \geq \frac{1}{2}$ mora biti razlomački gust. Za $\underline{d}(A) > \frac{1}{2}$ razlomačka gustoća od A proizlazi i iz sofisticiranog rezultata koji pripada metričkoj teoriji brojeva. Sljedeći teorem koji pokriva kritični slučaj $\underline{d}(A) = \frac{1}{2}$ u osnovi su dokazali Strauch i Tóth.

Teorem 2.4. *Ako je* $\underline{d}(A) \geq \frac{1}{2}$*, onda je* A razlomački gust.

Dokaz. Neka je $\underline{d}(A) \geq \frac{1}{2}$ i pretpostavimo suprotno, to jest da za neke $0 < \alpha < \beta \leq 1$ imamo $R(A) \cap (\alpha, \beta) = \varnothing$. Primjećujemo da A mora biti beskonačan, te elemente od A poredamo u rastućem nizu $a_1 < a_2 < ....$ Neka je k prirodni broj dovoljno velik da vrijedi $k\alpha > 1$ i neka je $0 < \theta < 1$. Za svaki $m, n \in \mathbb{N}$, neka je

$$J_m^n = \left(\alpha a_{k(\lfloor \theta n \rfloor + m)}, \alpha \left(a_{k(\lfloor \theta n \rfloor + m)} + k\right)\right).$$

Tvrdimo da su za svaki $n \in \mathbb{N}$ intervali

$$J_0^n, J_1^n, \ldots, J_{n-\lfloor \theta n \rfloor - 1}^n, (\alpha a_{kn}, \beta a_{kn}) \tag{2.5}$$

koje koristimo u nastavku dokaza u parovima disjunktni. Doista, budući da su a_i prirodni brojevi, slijedi da je

$$\alpha \left(a_{k(\lfloor \theta n \rfloor + m)} + k\right) \leq \alpha \left(a_{k(\lfloor \theta n \rfloor + m) + k}\right) = \alpha \left(a_{k(\lfloor \theta n \rfloor + m + 1)}\right)$$

tako da je desni rub od J_m^n manji ili jednak lijevom rubu intervala J_{m+1}^n. Sličan argument pokazuje da je desni rub od $J_{n-\lfloor \theta n \rfloor - 1}^n$ manji ili jednak od αa_{kn}.

Zatim, neka je n dovoljno velik tako da je $\lfloor \theta n \rfloor \geq \frac{\alpha}{\beta - \alpha}$. Tvrdimo da je

$$J_m^n \subseteq (\alpha a_{k(\lfloor \theta n \rfloor + m)}, \beta a_{k(\lfloor \theta n \rfloor + m)}) \tag{2.6}$$

za svaki $m = 0, 1, \ldots, n - \lfloor \theta n \rfloor - 1$. Da bismo ovo dokazali, primijetimo

$$\frac{k\alpha}{\beta - \alpha} \leq k\lfloor \theta n \rfloor \leq a_{k\lfloor \theta n \rfloor} < a_{k\lfloor \theta n \rfloor + m}$$

što povlači da je $\alpha\left(a_{k(\lfloor \theta n \rfloor + m)} + k\right) \leq \beta a_{k(\lfloor \theta n \rfloor + m)}$ pa vrijedi (2.6)

Budući da je $(\alpha a_n, \beta a_n) \cap A = \varnothing$ po pretpostavci, slijedi da su intervali (2.5) sadržani u komplementu $[0, \infty) \setminus A$. Označimo $B = \mathbb{N} \setminus A$ te imamo

$$|B\left(\beta a_{kn}\right)| \geq ((\beta - \alpha)a_{kn} - 1) + (n - \lfloor \theta n \rfloor)(k\alpha - 1).$$

Podijelimo s βa_{kn} te uzimajući limes superior, dobivamo

$$\begin{aligned}
1 - \underline{d}(A) &= \limsup_{n\to\infty} \frac{|B(n)|}{n} \\
&\geq \limsup_{n\to\infty} \frac{|B\left(\beta a_{kn}\right)|}{\beta a_{kn}} \\
&\geq \limsup_{n\to\infty} \left(\frac{(\beta - \alpha)a_{kn} - 1}{\beta a_{kn}} + \frac{(n - \lfloor \theta n \rfloor)(k\alpha - 1)}{\beta a_{kn}} \right) \\
&\geq \frac{\beta - \alpha}{\beta} + \liminf_{n\to\infty} \frac{(n - \lfloor \theta n \rfloor)(k\alpha - 1)}{\beta a_{kn}} \\
&\geq 1 - \frac{\alpha}{\beta} + (1 - \theta) \liminf_{n\to\infty} \frac{\alpha k n - n}{\beta a_{kn}} \\
&\geq 1 - \frac{\alpha}{\beta} + (1 - \theta) \left(\frac{\alpha}{\beta} \liminf_{n\to\infty} \frac{kn}{a_{kn}} - \frac{1}{\beta k} \limsup_{n\to\infty} \frac{kn}{a_{kn}} \right) \\
&\geq 1 - \frac{\alpha}{\beta} + (1 - \theta) \left(\frac{\alpha}{\beta} \underline{d}(A) - \frac{1}{\beta k} \right)
\end{aligned}$$

.

Kada $\theta \to 0$ i $k \to \infty$, dobivamo

$$\left(1 + \frac{\alpha}{\beta}\right) \underline{d}(A) \leq \frac{\alpha}{\beta} \tag{2.7}$$

Ako je $\underline{d}(A) \geq \frac{1}{2}$, tada prethodna nejednakost povlači da je $\beta \leq \alpha$ što je kontradikcija. □

Zapravo smo pokazali da ako imamo $R(A) \cap (\alpha, \beta) = \varnothing$, onda mora vrijediti (2.7). U stvari, nije teško pokazati da je

$$\underline{d}(A) \leq \frac{\alpha}{\beta} \min\{\overline{d}(A), 1 - \overline{d}(A)\}$$

i $\overline{d}(A) \leq 1 - (\beta - \alpha)$, gdje

$$\overline{d}(A) = \limsup_{n\to\infty} \frac{|A(n)|}{n}$$

označava *gornju asimptotsku gustoću* od A [1]. Poznato je kako $\underline{d}(A) + \overline{d}(A) \geq 1$ povlači da je A razlomački gust.

2.3 Treći teorem

Jasno je da je $\mathbb{N}$ razlomački gust budući da je $R(\mathbb{N}) = \mathbb{Q} \cap (0, \infty)$ skup pozitivnih racionalnih brojeva. Sada se postavlja zanimljivo pitanje: ako je $\mathbb{N}$ particioniran na konačan broj disjunktnih podskupova, mora li ijedan od tih podskupova biti razlomački gust? Odgovor nam daje sljedeći teorem.

Teorem 2.5. *Možemo particionirati $\mathbb{N}$ u tri skupa tako da nijedan od njih nije razlomački gust. No, nemoguća je takva particija u samo dva skupa.*

Ovaj teorem se temelji na radu Bukora, Šaláta i Tótha. Oni su zajedno s mađarskim matematičarem P. Erdősom generalizirali drugu tvrdnju pokazujući da ako je skup A prikazan kao rastući niz $a_1 < a_2 < \ldots$ koji zadovoljava $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = 1$, tada je za svaki $B \subseteq A$ skup B ili skup $A \setminus B$ razlomački gust. Dokaz Teorema 2.5 je sadržan u sljedeća dva rezultata.

Propozicija 2.6. *Postoje disjunktni skupovi $A, B, C \subset \mathbb{N}$ koji nisu razlomački gusti i vrijedi $\mathbb{N} = A \cup B \cup C$.*

Dokaz. Neka je

$$A = \bigcup_{k=0}^{\infty} [5^k, 2 \cdot 5^k) \cap \mathbb{N}$$

$$B = \bigcup_{k=0}^{\infty} [2 \cdot 5^k, 3 \cdot 5^k) \cap \mathbb{N}$$

$$C = \bigcup_{k=0}^{\infty} [3 \cdot 5^k, 5 \cdot 5^k) \cap \mathbb{N}$$

tako da se A, B i C sastoje od onih prirodnih brojeva čiji prikaz u bazi 5 započinje redom sa 1, sa 2 i sa 3 ili 4. Ovdje promatramo samo C, ostala dva slučajeva su slična (za skup A tvrdnja slijedi iz Propozicije 2.2). Uočimo da je svaki kvocijent dvaju elemenata iz C sadržan u intervalu oblika $I_\ell = \left(\frac{3}{5}5^\ell, \frac{5}{3}5^\ell\right)$ za neki cijeli broj ℓ. Ako je $j < k$ onda je svaki element iz I_j strogo manji od svakog elementa iz I_k budući da je $\frac{5}{3} \cdot 5^j < \frac{3}{5} \cdot 5^k$ ekvivalentno $\frac{25}{9} < 5^{k-j}$. Stoga je $R(C) \cap [\frac{5}{3}5^\ell, \frac{3}{5}5^{\ell+1}] = \varnothing$ za svaki cijeli broj ℓ, pa C nije razlomački gust. □

Teorem 2.7. *Ako su A i B disjunktni skupovi takvi da je $\mathbb{N} = A \cup B$, tada je barem jedan od njih* razlomački gust.

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da su A i B beskonačni skupovi. Pretpostavimo suprotno, to jest da ni A ni B nisu razlomački gusti. Dakle, postoje $\alpha, \beta > 1$ i $\epsilon > 0$ takvi da su $R(A) \cap (\alpha - \epsilon, \alpha + \epsilon)$ i $R(B) \cap (\beta - \epsilon, \beta + \epsilon)$ oba prazni skupovi. Neka je sada $n_0 \in \mathbb{N}$ takav da je

$$\frac{1 + \alpha + \beta + 2\alpha\beta}{n_0} < \epsilon.$$

Budući da su A i B oba beskonačni, postoji $n > \alpha\beta(n_0 + 1)$ takav da je $n \in A$ i $n + 1 \in B$. Ako $s = \lfloor \frac{n}{\alpha\beta} \rfloor - 1$ pripada A, onda za $t = \lfloor \alpha s \rfloor$ dobivamo

$$\left| \frac{t}{s} - \alpha \right| = \left| \frac{\lfloor \alpha s \rfloor - \alpha s}{s} \right| < \frac{1}{s} \leq \frac{1}{n_0} < \epsilon. \tag{2.8}$$

Budući da je $R(A) \cap (\alpha - \epsilon, \alpha + \epsilon) = \varnothing$, zaključujemo da t pripada B. Primijetimo da je

$$\begin{aligned} \left| \frac{n+1}{t} - \beta \right| &= \frac{n + 1 - \beta \lfloor \alpha s \rfloor}{t} \\ &< \frac{n + 1 - \beta(\alpha s - 1)}{t} \\ &= \frac{1 + \beta + \alpha\beta + n - \alpha\beta \left\lfloor \frac{n}{\alpha\beta} \right\rfloor}{t} \\ &< \frac{1 + \beta + 2\alpha\beta}{t} \\ &\leq \frac{1 + \alpha + \beta + 2\alpha\beta}{n_0} \\ &< \epsilon. \end{aligned}$$

Stoga, $\frac{n+1}{t}$ leži u $R(B) \cap (\beta - \epsilon, \beta + \epsilon)$ što je kontradikcija. Dakle, s mora pripadati skupu B.

Uzimamo sada da $s = \left\lfloor \frac{n}{\alpha\beta} \right\rfloor - 1$ pripada B i da je $t = \lfloor \beta s \rfloor$. Radeći kao u (2.8)

vidimo da je $|\frac{t}{s} - \beta| < \epsilon$ i stoga t leži u skupu A. Nadalje,

$$\begin{aligned}\left|\frac{n}{t} - \alpha\right| &= \left|\frac{n - \alpha\lfloor\beta s\rfloor}{t}\right| \\ &< \frac{n - \alpha(\beta s - 1)}{t} \\ &= \frac{\alpha + n - \alpha\beta s}{t} \\ &= \frac{\alpha + n - \alpha\beta\left(\left\lfloor\frac{n}{\alpha\beta}\right\rfloor - 1\right)}{t} \\ &= \frac{\alpha + \alpha\beta + \left(n - \alpha\beta\left\lfloor\frac{n}{\alpha\beta}\right\rfloor\right)}{t} \\ &< \frac{\alpha + 2\alpha\beta}{n_0} \\ &< \epsilon.\end{aligned}$$

Stoga, $\frac{n}{t}$ pripada $R(A) \cap (\alpha - \epsilon, \alpha + \epsilon)$ što je kontradikcija koja povlači da s ne pripada ni A ni B. To je nemoguće jer je $\mathbb{N} = A \cup B$. □

Primijetimo da se donja asimptotska gustoća ne odnosi na prethodni rezultat budući da je moguće particionirati $\mathbb{N}$ na dva podskupa tako da oba imaju donju asimptotsku gustoću 0.

Propozicija 2.8. *Postoje disjunktni skupovi $A, B \subset \mathbb{N}$ takvi da je $\mathbb{N} = A \cup B$, te $\underline{d}(A) = \underline{d}(B) = 0$ i $\overline{d}(A) = \overline{d}(B) = 1$.*

Dokaz. U dokazu nam je potreban Stolz–Cesàroov teorem koji govori da ako su x_n i y_n dva rastuća, neograničena niza realnih brojeva, tada

$$\lim_{n\to\infty} \frac{x_{n+1} - x_n}{y_{n+1} - y_n} = L \quad \Longrightarrow \quad \lim_{n\to\infty} \frac{x_n}{y_n} = L.$$

Stavimo prvih 1! prirodnih brojeva u A, zatim sljedećih 2! u B, pa sljedećih 3! u A i tako dalje, te dobivamo skupove

$$A = \{1, 4, 5, 6, 7, 8, 9, 34, \ldots\}, \quad B = \{2, 3, 10, 11, 12, \ldots, 32, 33, 154, 155, \ldots\}.$$

Po konstrukciji je $A \cap B = \varnothing$ i $\mathbb{N} = A \cup B$. Neka je $x_n = \sum_{k=1}^{2n-1} k!$ i $y_n = \sum_{k=1}^{2n} k!$, te vrijedi $|A(x_n)| = |A(y_n)| = \sum_{k=1}^{n}(2k-1)!$. Zbog

$$\frac{|A\,(y_{n+1})| - |A\,(y_n)|}{y_{n+1} - y_n} = \frac{(2n+1)!}{(2n+2)! + (2n+1)!} = \frac{1}{2n+3} \to 0$$

i

$$\frac{|A(x_{n+1})| - |A(x_n)|}{x_{n+1} - x_n} = \frac{(2n+1)!}{(2n+1)! + (2n)!} = \frac{1}{1 + \frac{1}{2n+1}} \to 1$$

iz Stolz–Cesàroova teorema slijedi da je $\underline{d}(A) = 0$ i $\overline{d}(A) = 1$. Analogan argument za nizove $x_n = \sum_{k=1}^{2n} k!$ i $y_n = \sum_{k=1}^{2n+1} k!$ daje da je $\underline{d}(B) = 0$ i $\overline{d}(B) = 1$. □

2.4 Četvrti teorem

Podsjetimo se da je aritmetički niz s razlikom b i duljinom n niz oblika $a, a+b, a+2b, \ldots, a+(n-1)b$. Podskupovi skupa prirodnih brojeva koji sadrže proizvoljno duge aritmetičke nizove često se smatraju "gusti" u nekom smislu.

Teorem 2.9. *Postoje podskupovi od $\mathbb{N}$ koji sadrže proizvoljno duge artimetičke nizove, a ipak nisu razlomački gusti. S druge strane, postoji razlomački gust skup koji ne sadrži aritmetički niz duljine ≥ 3.*

Uočimo da je prva tvrdnja ovog teorema već dokazana. Iz Propozicije 2.2 dobivamo skupove koji nisu razlomački gusti i koji sadrže proizvoljno duge blokove uzastopnih prirodnih brojeva. Stoga, trebamo samo konstruirati razlomački gust skup koji ne sadrži aritmetički niz duljine tri.

Propozicija 2.10. *Skup $A = \{2^j : j \geq 2\} \cup \{3^k : k \geq 2\}$ je razlomački gust i ne sadrži aritmetički niz duljine tri.*

Dokaz. Prvo se podsjetimo da Kroneckerov teorem iz diofantskih aproksimacija kaže da ako je $\beta > 0$ iracionalan, $\alpha \in \mathbb{R}$ i $\delta > 0$, onda postoje $m, n \in \mathbb{N}$ takvi da je $|n\beta - \alpha - m| < \delta$. Neka su $\xi, \epsilon > 0$ i primijetimo da je $\beta = \log_2 3 > 0$ iracionalan. Zbog neprekidnosti od $f(x) = 2^x$ u $\log_2 \xi$, postoji $\delta > 0$ takav da vrijedi

$$|\log_2 x - \log_2 \xi| < \delta \quad \Longrightarrow \quad |x - \xi| < \epsilon. \tag{2.9}$$

Kroneckerov teorem za $\beta = \log_2 3$ i $\alpha = \log_2 \xi$ daje $n, m \in \mathbb{N}$ takve da vrijedi

$$\left| \log_2 \left(\frac{3^n}{2^m} \right) - \log_2 \xi \right| = \left| n \log_2 3 - \log_2 \xi - m \right| < \delta.$$

Iz (2.9) slijedi $\left| \frac{3^n}{2^m} - \xi \right| < \epsilon$, odakle vidimo da je A razlomački gust.

Sada ćemo pokazati da A ne sadrži aritmetički niz duljine tri. Pretpostavimo suprotno, to jest da postoji takav aritmetički niz. Po definiciji od A, prvi član tog niza je potencija od 2 ili potencija od 3. Slučajeve ćemo razmotriti odvojeno.

1.slučaj. Prepostavimo da 2^j, $2^j + b$ i $2^j + 2b$ pripadaju skupu A. Budući da je $2^j + 2b$ paran i pripada A, mora biti oblika 2^k za neki $k > j$, odakle slijedi da

je $b = 2^{k-1} - 2^{j-1}$ paran zbog $j \geq 2$. Stoga, $2^j + b$ također mora biti oblika 2^ℓ za neki $\ell > j$ tako da vrijedi

$$2^\ell = 2^j + b = 2^j + (2^{k-1} - 2^{j-1}) = 2^{j-1}(2^{k-j} + 1).$$

Dijeljenjem prethodne jednakosti s 2^{j-1}, dobivamo kontradikciju.

2.slučaj. Pretpostavimo da je 3^j, $3^j + b$, $3^j + 2b$ aritmetički niz u A duljine tri koji započinje sa 3^j. U tom slučaju, $3^j + 2b$ je neparan, pa mora biti oblika 3^k za neki $k > j$. Dakle,

$$b = \frac{3^k - 3^j}{2} = 3^j \frac{\left(3^{k-j} - 1\right)}{2},$$

pa je $3^j + b$ u našem nizu djeljiv s 3^j. Stoga je $3^j + b = 3^\ell$ za neki $\ell > j$ iz čega slijedi

$$3^\ell = 3^j + b = 3^j + 3^j \frac{\left(3^{k-j} - 1\right)}{2}.$$

Budući da to povlači da je $2 \cdot 3^{\ell-j} = 2 + \left(3^{k-j} - 1\right)$, a to modulo 3 ne vrijedi, zaključujemo da A ne sadrži aritmetički niz duljine 3. □

Poglavlje 3

Razlomački skupovi u p-adskim brojevima

U prošlom poglavlju smo promatrali kada je za podskup $A \subseteq \mathbb{N}$ njemu pridruženi razlomački skup $R(A)$ gust u skupu pozitivnih realnih brojeva, a sada ćemo istražiti uvjete kada je $R(A)$ gust u skupu p-adskih brojeva. Budući da je $R(A)$ podskup skupa racionalnih brojeva $\mathbb{Q}$, postoje i druge metrike koje možemo promatrati osim one inducirane strandardnom aposlutnom vrijednošću. Prisjetimo se p-adske metrike.

Fiksiramo prost broj p i primijetimo da svaki racionalni broj različit od nule ima jedinstveni prikaz oblika $r = \pm\frac{p^k a}{b}$ gdje je $k \in \mathbb{Z}$, $a, b \in \mathbb{N}$ i $\text{nzd}(a, p) = \text{nzd}(b, p) = \text{nzd}(a, b) = 1$. *P-adska valuacija* takvog r je dana s $v_p(r) = k$, a njegova *p-adska apsolutna vrijednost* je $|r|_p = p^{-k}$. Dogovorom stavljamo $v_p(0) = \infty$ i $|0|_p = 0$. *P-adska metrika* na $\mathbb{Q}$ je dana s $d(x, y) = |x - y|_p$.

Garcia i Luca su dokazali da je razlomački skup za Fibonaccijeve brojeve gust u $\mathbb{Q}_p$ za svaki p. Njihov rezultat je proširio Sanna koji je dokazao da je razlomački skup k-generaliziranih Fibonaccijevih brojeva gust u $\mathbb{Q}_p$ za sve cijele brojeve $k \geq 2$ i proste brojeve p. U ovom ćemo poglavlju pobliže objasniti i istražiti razlomačke skupove u p-adskim brojevima. Slijedi nekoliko osnovnih lema koje će biti korisne u nastavku.

Lema 3.1. *Ako je S gust u $\mathbb{Q}_p$, tada za svaku konačnu vrijednost p-adske valuacije postoji element iz S s tom valuacijom.*

Dokaz. Ako se $q \in \mathbb{Q}_p^\times$ može proizvoljno dobro aproksimirati s elementima iz S, tada postoji niz $s_n \in S$ takav da vrijedi $|p^{-v_p(s_n)} - p^{-v_p(q)}| = ||s_n|_p - |q|_p| \leq |s_n - q|_p \to 0$. Na $\mathbb{Q}^\times$ p-adska valuacija poprima samo cjelobrojne vrijednosti, pa je $v_p(s_n)$ od nekog n nadalje jednak $v_p(q)$. □

Obrat ove leme ne vrijedi što vidimo promatrajući skup $S = \{p^k : k \in \mathbb{Z}\}$. Općenitije, imamo sljedeći rezultat.

Lema 3.2. *Ako je A geometrijski niz u $\mathbb{Z}$, tada $R(A)$ nije gust ni u jednom $\mathbb{Q}_p$.*

Dokaz. Ako je $A = \{cr^n : n \geq 0\}$ za cijele brojeve c i r različite od nule, tada je $R(A) = \{r^n : n \in \mathbb{Z}\}$. Neka je p prost broj. Ako $p \nmid r$, tada $R(A)$ nije gust u $\mathbb{Q}_p$ po prethodnoj Lemi 3.1. Ako $p \mid r$, tada $r^k \equiv -1 \pmod{p^2}$ ne može vrijediti zbog toga što je -1 invertibilno modulo p. Dakle, $R(A)$ se ne približava -1 u $\mathbb{Q}_p$ po volji blizu. □

U nastavku se često pozivamo na *"tranzitivnost gustoće"*, to jest ako je X gust u Y i Y gust u Z, onda je X gust u Z. Tu činjenicu koristimo zajedno sa sljedećom lemom.

Lema 3.3. *Neka je $A \subseteq \mathbb{N}$.*

(a) Ako je A p-adski gust u $\mathbb{N}$, tada je $R(A)$ gust u $\mathbb{Q}_p$.

(b) Ako je $R(A)$ p-adski gust u $\mathbb{N}$, tada je $R(A)$ gust u $\mathbb{Q}_p$.

Dokaz.

(a) Ako je A p-adski gust u $\mathbb{N}$, tada je p-adski gust i u $\mathbb{Z}$ jer je $\mathbb{N}$ p-adski gust u $\mathbb{Z}$. Funkcija $x \longmapsto \frac{1}{x}$ je neprekidna na $\mathbb{Q}_p^\times$, pa je $R(A)$ p-adski gust u $\mathbb{Q}$ koji je gust u $\mathbb{Q}_p$.

(b) Pretpostavimo da je $R(A)$ p-adski gust u $\mathbb{N}$. Budući da je funkcija $x \longmapsto \frac{1}{x}$ neprekidna na $\mathbb{Q}_p^\times$, zaključak slijedi iz činjenice da je $\mathbb{N}$ p-adski gust u skupu $\{x \in \mathbb{Q} : v_p(x) \geq 0\}$. □

Iako uvjet iz (a) povlači uvjet iz (b), iskazali smo ih odvojeno budući da uvjet iz (a) nije nužan da bi $R(A)$ bio gust u $\mathbb{Q}_p$. Ako je A skup parnih brojeva, tada je $R(A) = \mathbb{Q}$ gust u $\mathbb{Q}_p$ za svaki p, ali A nije 2-adski gust u $\mathbb{N}$. Sljedeća lema se odnosi na općenitije aritmetičke nizove.

Lema 3.4. *Neka je $A = \{an + b : n \geq 0\}$.*

(a) Ako $p \nmid a$, tada je $R(A)$ gust u $\mathbb{Q}_p$.

(b) Ako $p \mid a$ i $p \nmid b$, tada $R(A)$ nije gust u $\mathbb{Q}_p$.

Dokaz.

(a) Neka $p \nmid a$ i neka je $n \in \mathbb{N}$ proizvoljan. Ako je $r \geq 1$, neka je $i \equiv a^{-1}(n - b) \pmod{p^r}$ tako da je $ai + b \equiv n \pmod{p^r}$. Stoga je A p-adski gust u $\mathbb{N}$, pa je po Lemi 3.3 $R(A)$ gust u $\mathbb{Q}_p$.

(b) Ako $p \mid a$ i $p \nmid b$, tada je $v_p(an + b) = 0$ za svaki n. Zato, po Lemi 3.1 $R(A)$ nije gust u $\mathbb{Q}_p$. □

3.1 Usporedba realnog i p-adskog slučaja

Mnogi radovi posvećeni su proučavanju razlomačkih skupova u realnim brojevima, odnosno proučavali su se uvjeti na skup A za koje je $R(A)$ gust u $\mathbb{R}_+ = (0, +\infty)$. Želimo vidjeti koji uvjeti koji daju da je skup razlomački gust u skupu realnih brojeva vrijede i u skupu p-adskih brojeva.

Nezavisnost od realnog slučaja

Ponašanje razlomačkih skupova u p-adskim brojevima je u suštini nezavisno od ponašanja u realnim brojevima. Preciznije, postoji konkretan primjer za svaku od četiri tvrdnje oblika "$R(A)$ (je gust / nije gust) u svakom $\mathbb{Q}_p$ i (gust je / nije gust) u $\mathbb{R}_+$".

(a) Neka je $A = \mathbb{N}$. Tada je $R(A)$ gust u svakom $\mathbb{Q}_p$ i gust u $\mathbb{R}_+$.

(b) Neka je $F = \{1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots\}$ skup Fibonaccijevih brojeva. Tada je $R(F)$ gust u svakom $\mathbb{Q}_p$ kao što ćemo vidjeti u Korolaru 3.15. S druge strane, Binetova formula jamči da $R(F)$ ima gomilišta samo u cjelobrojnim potencijama zlatnog omjera te stoga $R(F)$ nije gust u $\mathbb{R}_+$.

(c) Neka je $A = \{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}$ skup prostih brojeva. P-adska valuacija kvocijenata prostih brojeva pripada skupu $\{-1, 0, 1\}$, pa Lema 3.1 jamči da $R(A)$ nije gust ni u jednom $\mathbb{Q}_p$. Gustoća od $R(A)$ u $\mathbb{R}_+$ je posljedica Teorema o prostim brojevima što je dokazao Schinzel.

(d) Neka je $A = \{2, 6, 30, 210, \ldots\}$ skup primorijela. Za prirodan broj n je n-ti primorijel definiran kao produkt prvih n prostih brojeva. P-adska valuacija kvocijenata primorijela pripada skupu $\{-1, 0, 1\}$, pa Lema 3.1 jamči da $R(A)$ nije gust ni u jednom $\mathbb{Q}_p$. Nadalje, $R(A) \cap [1, \infty) \subseteq \mathbb{N}$, pa $R(A)$ nije gust u $\mathbb{R}_+$.

Nezavisnost po različitim prostim brojevima

Teorem 3.5. *Za svaki skup P prostih brojeva, postoji $A \subseteq \mathbb{N}$ takav da je $R(A)$ gust u $\mathbb{Q}_p$ ako i samo ako je $p \in P$.*

Dokaz. Neka je P skup prostih brojeva, neka je Q skup prostih brojeva koji nisu u P i neka je $A = \{a \in \mathbb{N} : v_q(a) \leq 1 \text{ za svaki } q \in Q\}$. Lema 3.1 osigurava da $R(A)$ nije gust u $\mathbb{Q}_q$ za svaki $q \in Q$. Za fiksirani $p \in P$, neka je $\ell \geq 0$ i neka je $n = p^k m \in \mathbb{N}$ takav da $p \nmid m$. Dirichletov teorem o prostim brojevima u aritmetičkim nizovima daje prost broj oblika $r = p^\ell j + m$. Tada je $p^k r \in A$ i $p^k r \equiv p^k(p^\ell j + m) \equiv p^k m \equiv n \pmod{p^\ell}$. Budući da je n bio proizvoljan, po Lemi 3.3 slijedi da je $R(A)$ gust u $\mathbb{Q}_p$. □

Aritmetički nizovi

Vidjeli smo ranije da postoji skup $A \subseteq \mathbb{N}$ koji sadrži proizvoljno duge aritmetičke nizove tako da $R(A)$ nije gust u $\mathbb{R}_+$. S druge strane, također smo vidjeli da postoji skup A koji ne sadrži artimetički niz duljine tri, a $R(A)$ je gust u $\mathbb{R}_+$. Isti rezultati vrijede, s različitim primjerima, za p-adske brojeve.

Primjer 3.6 (Proizvoljno dugi aritmetički nizovi). *Teorem Greena i Taoa kaže da skup prostih brojeva sadrži proizvoljno duge aritmetičke nizove. Međutim, njegov razlomački skup nije gust ni u jednom $\mathbb{Q}_p$ kako smo maloprije pokazali.*

Skup bez dugih aritmetičkih nizova može imati razlomački skup koji je gust u nekom $\mathbb{Q}_p$. Promotrimo skup $A = \{2^n : n \geq 0\} \cup \{3^n : n \geq 0\}$ koji ne sadrži artimetičke nizove duljine tri kako smo dokazali u Propoziciji 2.10. Može se pokazati da je $R(A)$ gust u $\mathbb{Q}_p$ ako i samo ako je $p = 3$. No, možemo naći i puno bolji primjer.

Teorem 3.7. *Postoji skup $A \subseteq \mathbb{N}$ koji ne sadrži artimetički niz duljine tri i koji je gust u svakom $\mathbb{Q}_p$.*

Dokaz. Neka je (q_n, r_n) enumeracija skupa svih parova (q, r), gdje je q potencija prostog broja i $0 \leq r < q$. Primijetimo da se svaki od parova $(q, 0), (q, 1), \ldots, (q, q-1)$ pojavljuje točno jednom u ovom prebrajanju. Konstruiramo skup A koji je u početku prazan. Stavimo prvi prirodni broj a_1 takav da je $a_1 \equiv r_1 \pmod{q_1}$. Zatim mu dodamo a_2 takav da je $a_2 > a_1$ i $a_2 \equiv r_2 \pmod{q_2}$. Izaberemo $a_3 > a_2$ za koji je $a_3 \equiv r_3 \pmod{q_3}$ i tako da a_1, a_2, a_3 nije aritmetički niz duljine tri. Nastavljamo ovim postupkom tako da se prirodan broj $a_n > a_{n-1}$ dobiva u n-tom koraku tako da je $a_n \equiv r_n \pmod{q_n}$ i $a_1, a_2, \ldots, a_n$ ne sadrži aritmetički niz duljine tri. Budući da $A = \{a_n : n \geq 1\}$ sadrži potpuni skup ostataka modulo svaka potencija svakog prostog broja, vrijedi da je p-adski gust u $\mathbb{N}$ za svaki prost broj p. Stoga je $R(A)$ gust u svakom $\mathbb{Q}_p$ po Lemi 3.3. Po konstrukciji A ne sadrži artimetički niz duljine tri. □

Asimptotska gustoća

U prošlom poglavlju smo promatrali asimptotsku gustoću za razlomačke skupove u realnim brojevima te smo definirali donju i gornju asimptotsku gustoću. Ako je $\underline{d}(A) = \overline{d}(A)$ za $A \subseteq \mathbb{N}$, tada je njihova zajednička vrijednost označena s $d(A)$ i zove se *asimptotska gustoća* (ili prirodna gustoća) od A. Dakle,

$$d(A) = \lim_{n\to\infty} \frac{|A(n)|}{n}.$$

U Teoremu 2.4 smo promatrali kritični prag za donju asimptotsku gustoću koji garantira da je odgovarajući skup razlomački gust u $\mathbb{R}_+$. S druge strane, u p-adskom slučaju je kritični prag jednak 1.

Teorem 3.8.

(a) Ako je $\overline{d}(A) = 1$*, tada je* $R(A)$ *gust u svakom* $\mathbb{Q}_p$*.*

(b) Za svaki $\alpha \in [0, 1)$ *postoji* $A \subseteq \mathbb{N}$ *takav da* $R(A)$ *nije gust ni u jednom* $\mathbb{Q}_p$ *i* $\underline{d}(A) \geq \alpha$*.*

Dokaz.

(a) Pretpostavimo da je $\overline{d}(A) = 1$. Ako A ne sadrži nijednog predstavnika iz neke klase kongruencije modulo proste potencije p^r, tada je $\overline{d}(A) \leq 1 - \frac{1}{p^r} < 1$, što je kontradikcija. Stoga A sadrži predstavnika iz svake klase kongruencije modulo svaka potencija p^r svakog prostog broja p. Neka su $n, r \in \mathbb{N}$ i uzmimo $a, b \in A$ tako da je $a \equiv n \pmod{p^r}$ i $b \equiv 1 \pmod{p^r}$. Tada je $a \equiv bn \pmod{p^r}$ i stoga vrijedi da je $v_p(\frac{a}{b} - n) = v_p(a - bn) \geq r$. Dakle, po Lemi 3.3 je $R(A)$ gust u $\mathbb{Q}_p$.

(b) Neka je $\alpha \in (0, 1)$, neka p_n označava n-ti prost broj i neka je r_n dovoljno velik tako da vrijedi $2^n \leq (1 - \alpha)p_n^{r_n}$ za $n \geq 1$. Ako je

$$A = \{a \in \mathbb{N} : v_{p_n}(a) \leq r_n \quad \text{za svaki n}\},$$

tada $R(A)$ nije gust ni u jednom $\mathbb{Q}_p$ po Lemi 3.1. Budući da A ne sadrži upravo višekratnike od $p_n^{r_n}$, imamo

$$\underline{d}(A) \geqslant 1 - \sum_{n=1}^{\infty} \frac{1}{p_n^{r_n}} \geqslant 1 - \sum_{n=1}^{\infty} \frac{(1 - \alpha)}{2^n} = \alpha \qquad \square.$$

Drugi ekstremni primjer dan je u sljedećem teoremu.

Teorem 3.9. *Postoji* $A \subseteq \mathbb{N}$ *za koji je* $d(A) = 0$*, a* $R(A)$ *je gust u svakom* $\mathbb{Q}_p$*.*

Dokaz. Neka je q_n rastući niz $2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, \ldots$ prostih potencija. Konstruirajmo A prema sljedećem postupku. Stavimo prvih q_1 brojeva u A $(1, 2 \in A)$ i preskočimo sljedećih $q_1!$ brojeva $(3, 4 \notin A)$. Stavimo sada sljedećih q_2 brojeva u A $(5, 6, 7 \in A)$ i preskočimo sljedećih $q_2!$ brojeva $(8, 9, 10, 11, 12, 13 \notin A)$. Brzorastuće veličine razmaka između uzastopnih blokova elemenata od A jamče da je $d(A) = 0$. Budući da A sadrži proizvoljno duge blokove uzastopnih cijelih brojeva, sadrži i potpun skup ostataka modulo svaki q_n. Stoga je A p-adski gust u $\mathbb{N}$ za svaki prost broj p, pa je $R(A)$ gust u svakom $\mathbb{Q}_p$ po Lemi 3.3. $\square$

Particije od $\mathbb{N}$

Vidjeli smo ranije u Teoremu 2.5 da ako je $\mathbb{N} = A \cup B$, tada je barem jedan od $R(A)$ i $R(B)$ gust u $\mathbb{R}_+$, ali postoji i particija $\mathbb{N} = A \cup B \cup C$, takva da nijedan od $R(A)$, $R(B)$ i $R(C)$ nije gust u $\mathbb{R}_+$. U p-adskom slučaju, situacija je drugačija.

Primjer 3.10. *Fiksiramo prost broj p i neka je*

$$A = \{p^j n \in \mathbb{N} : j \text{ paran }, \text{nzd}(n, p) = 1\}$$

i

$$B = \{p^j n \in \mathbb{N} : j \text{ neparan }, \text{nzd}(n, p) = 1\}.$$

Tada je $A \cap B = \varnothing$ i $A \cup B = \mathbb{N}$, ali ni $R(A)$ ni $R(B)$ nije gust u $\mathbb{Q}_p$ po Lemi 3.1.

3.2 Suma potencija

Prikazivanje prirodnih brojeva kao sume kvadrata datira još iz doba antike, iako je ovo istraživanje uistinu procvalo u djelima Fermata, Lagrangea i Legendrea. Kasniji su autori proučavali općenitije kvadratne forme i prikaze prirodnih brojeva kao sume viših potencija. Neka je

$$A = \{a \in \mathbb{N} : a = x_1^n + x_2^n + \cdots + x_m^n, \quad x_i \geq 0\}.$$

Za koje m, n i p je $R(A)$ gust u $\mathbb{Q}_p$?

Za kvadrate i kubove idući teoremi daju potpuni odgovor, dok je za više potencije pitanje još otvoreno.

Teorem 3.11. *Neka je $S_n = \{a \in \mathbb{N} : a$ je suma n kvadrata cijelih brojeva, pri čemu je 0 dozvoljeno$\}$.*

(a) $R(S_1)$ nije gust ni u jednom $\mathbb{Q}_p$.

(b) $R(S_2)$ je gust u $\mathbb{Q}_p$ ako i samo ako je $p \equiv 1 \pmod 4$.

(c) $R(S_n)$ je gust u $\mathbb{Q}_p$ za sve p kada je $n \geq 3$.

Dokaz.

(a) Neka je p prost broj. Tada $2 \mid v_p(s)$ za svaki $s \in S_1$ i stoga $R(S_1)$ nije gust ni u jednom $\mathbb{Q}_p$ po Lemi 3.1.

(b) Postoje tri slučaja: (b1) $p = 2$; (b2) $p \equiv 1 \pmod 4$; (b3) $p \equiv 3 \pmod 4$.

(b1) Budući da je $v_2(3) = 0$, za svaki element $\frac{a}{b} \in R(S_2)$ koji je u $\mathbb{Q}_2$ dovoljno blizu 3 mora vrijediti $v_2(a) = v_2(b)$. Bez smanjenja općenitosti možemo pretpostaviti da su a i b neparni. Tada vrijedi $a \equiv b \equiv 1 \pmod 4$ budući da su $a, b \in S_2$, pa je $a \equiv 3b \pmod 4$ nemoguće. Stoga se $R(S_2)$ ne približava po volji blizu 3 u $\mathbb{Q}_2$.

(b2) Neka je $p \equiv 1 \pmod 4$. Po Lemi 3.3 dovoljno je pokazati da za svaki $n \geq 0$ i $r \geq 1$ kongruencija $x^2 + y^2 \equiv n \pmod{p^r}$ ima rješenje sa $p \nmid x$. Dokazujemo indukcijom po r. Budući da postoji točno $(p+1)/2$ kvadratnih ostataka modulo p, to skupovi $\{x^2 : x \in \mathbb{Z}/p\mathbb{Z}\}$ i $\{n - y^2 : y \in \mathbb{Z}/p\mathbb{Z}\}$ imaju neprazni presjek. Stoga, $x^2 + y^2 \equiv n \pmod p$ ima rješenje. Ako $p \nmid n$, tada p ne može dijeliti i x i y, pa u tom slučaju možemo pretpostaviti da $p \nmid x$. Ako $p \mid n$, neka je $x = 1$ i $y^2 \equiv -1 \pmod p$. Takav y postoji jer je $p \equiv 1 \pmod 4$. Time je pokazana baza indukcije za $r = 1$.

Pretpostavimo da je $x^2 + y^2 \equiv n \pmod{p^r}$ i $p \nmid x$. Tada je $x^2 + y^2 = n + mp^r$ za neki $m \in \mathbb{Z}$. Neka je $i \equiv -2^{-1}x^{-1}m \pmod p$ tako da vrijedi $p \mid (2ix + m)$. Tada je

$$\begin{aligned}(x + ip^r)^2 + y^2 &= x^2 + 2ixp^r + i^2p^{2r} + y^2 \\ &\equiv n + (2ix + m)p^r \pmod{p^{r+1}} \\ &\equiv n \pmod{p^{r+1}}.\end{aligned}$$

Time je induktivni dokaz završen.

(b3) Neka je $p \equiv 3 \pmod 4$. Ako su $a, b \in S_2$, tada Teorem 1.21 osigurava da su i $v_p(a)$ i $v_p(b)$ parni. Stoga je $v_p(a) - v_p(b) = v_p(a/b) \neq 1 = v_p(p)$ za svaki $a, b \in S_2$. Dakle, $R(S_2)$ se ne približava p u $\mathbb{Q}_p$ po volji.

(c) Lagrangeov teorem o četiri kvadrata kaže da je $S_n = \mathbb{N}$ za $n \geq 4$, pa je $R(S_n) = \mathbb{Q}$ gust u $\mathbb{Q}_p$ za $n \geq 4$. Stoga, promatramo samo $n = 3$ i iz toga proizlaze tri slučaja: (c1) $p = 2$; (c2) $p \equiv 1 \pmod 4$; (c3) $p \equiv 3 \pmod 4$.

(c1) Podsjetimo se da Legendreov teorem o tri kvadrata kaže da se prirodni broj nalazi u S_3 ako i samo ako nije oblika $4^i(8j + 7)$ za neke $i, j \geq 0$. Dakle, ako je 2-adska valuacija prirodnog broja neparna, tada je on suma tri kvadrata. Neka je $n \in \mathbb{N}$ neparan i neka je $k \in \mathbb{N}_0$. Ako je k neparan, neka je $a = 2^k n$ i $b = 1$, a ako je k paran, neka je $a = 2^{k+1}n$ i $b = 2$. Tada je $a = 2^k nb$ i $a, b \in S_3$ budući da je $v_2(a)$ neparan. Dakle, $a \equiv 2^k nb \pmod{2^r}$ za svaki $r \in \mathbb{N}$, pa je $R(S_3)$ 2-adski gust u $\mathbb{N}$. Po Lemi 3.3 je $R(S_3)$ gust u $\mathbb{Q}_2$.

(c2) Ako je $p \equiv 1 \pmod 4$, tada $R(S_3)$ sadrži $R(S_2)$ koji je gust u $\mathbb{Q}_p$, po (b2).

(c3) Neka je $p \equiv 3 \pmod 4$. Budući da je $4^j(8k + 7)$ kongruentno $0, 4$ ili 7 modulo 8, slijedi da S_3 sadrži beskonačni aritmetički niz $A = \{8k + 1 : k \geq 0\}$. Po Lemi 3.4 slijedi da je $R(A)$ gust u $\mathbb{Q}_p$, pa je zato i $R(S_3)$ gust u $\mathbb{Q}_p$. □

Teorem 3.12. *Neka je $C_n = \{a \in \mathbb{N} : a$ je suma n kubova nenegativnih cijelih brojeva, pri čemu je 0 dozvoljeno$\}$.*

(a) $R(C_1)$ nije gust ni u jednom $\mathbb{Q}_p$.

(b) $R(C_2)$ je gust u $\mathbb{Q}_p$ ako i samo ako je $p \neq 3$.

(c) $R(C_n)$ je gust u svakom $\mathbb{Q}_p$ za sve p kada je $n \geq 3$.

Dokaz.

(a) Neka je p prost broj. Tada $3 \mid v_p(c)$ za svaki $c \in C_1$, pa po Lemi 3.1 slijedi da $R(C_1)$ nije gust ni u jednom $\mathbb{Q}_p$.

(b) Promatramo tri slučaja: (b1) $p \neq 3, 7$; (b2) $p = 3$; (b3) $p = 7$.

(b1) Kongruencija $x^3 + y^3 \equiv n \pmod{m}$ ima rješenje za svaki n ako i samo ako $7 \nmid m$ i $9 \nmid m$. To je rezultat K.A. Broughana iz 2003. Dakle, C_2 je p-adski gust u $\mathbb{N}$ ako je $p \neq 3, 7$, pa je $R(C_2)$ gust u $\mathbb{Q}_p$ za $p \neq 3, 7$ po Lemi 3.3.

(b2) Ako je $x/y \in R(C_2)$ dovoljno blizu 3 u $\mathbb{Q}_3$, tada je $v_3(x) = v_3(y) + 1$. Bez smanjenja općenitosti možemo pretpostaviti da je $v_3(x) = 1$ i $v_3(y) = 0$. Suma dva kuba modulo 9 mora biti među brojevima $0, 1, 2, 7, 8$ tako da $v_3(x) = 1$ nije moguća za $x \in C_2$. Stoga $R(C_2)$ nije gust u $\mathbb{Q}_3$.

(b3) Neka je $p = 7$. Za svaki cijeli broj m kongruentan s $0, 1, 2, 5$ ili 6 modulo 7 i svaki $r \geq 1$, koristimo indukciju po r da bi pokazali kako $x^3 + y^3 \equiv m \pmod{7^r}$ ima rješenje sa $7 \nmid x$. Kubovi modulo 7 su $0, 1$ i 6 i stoga je svaka od klasa ostataka $0, 1, 2, 5, 6$ suma dva kuba modulo 7, od kojih je barem jedan različit od nule. Ovo je baza indukcije. Pretpostavimo da je m kongruentan $0, 1, 2, 5$ ili 6 modulo 7 i da je $x^3 + y^3 \equiv m \pmod{7^r}$ pri čemu $7 \nmid x$. Tada je $x^3 + y^3 = m + 7^r\ell$ za neki $\ell \in \mathbb{Z}$. Neka je $i \equiv -5\ell x^{-2} \pmod 7$ tako da vrijedi $7 \mid (3ix^2 + \ell)$. Tada je

$$\begin{aligned}(x + 7^r i)^3 + y^3 &\equiv x^3 + y^3 + 3x^2 \cdot 7^r i \pmod{7^{r+1}} \\ &\equiv m + 7^r(3ix^2 + \ell) \pmod{7^{r+1}} \\ &\equiv m \pmod{7^{r+1}}.\end{aligned}$$

Budući da $7 \nmid x$, slijedi da $7 \nmid (x + 7^r i)$. Tu završavamo s indukcijom.

Inverzi od $1, 2, 5$ i 6 modulo 7 su $1, 4, 3$ i 6 tim redom. Dakle, za svaki m kongruentan $1, 3, 4$ ili 6 modulo 7, kongruencija $(x^3 + y^3)^{-1} \equiv m \pmod{7^r}$ ima rješenje sa $7 \nmid x$. Svaka klasa ostataka modulo 7 je produkt elementa iz skupa $\{0, 1, 2, 5, 6\}$ s elementom iz $\{1, 3, 4, 6\}$. Za dani prirodni broj n i $r \geq 0$ zapišemo $n \equiv m_1 m_2 \pmod{7^r}$ gdje je m_1 modulo 7 u $\{0, 1, 2, 5, 6\}$, a m_2 modulo 7 je u $\{1, 3, 4, 6\}$. Tada postoje $c_1, c_2 \in C_2$ tako da vrijedi $c_1 c_2^{-1} \equiv m_1 m_2 \equiv n \pmod{7^r}$. Po Lemi 3.3 vrijedi da je $R(C_2)$ gust u $\mathbb{Q}_7$.

(c) Treba promatrati dva slučaja: (c1) $n \geq 4$; (c2) $n = 3$ i $p = 3$.

(c1) Gotovo svaki prirodan broj, u smislu asimptotske gustoće, je suma četiri kuba. To je Davenportov rezultat iz 1939. Za svaku prostu potenciju p^r i za svaki $n \in \mathbb{N}$, kongruencija $x \equiv n \pmod{p^r}$ mora imati rješenje $x \in C_4$ jer bi u suprotnom asimptotska gustoća od C_4 bila najviše $1 - 1/p^r$. Po Lemi 3.3 dobivamo da je $R(C_4)$ gust u $\mathbb{Q}_p$.

(c2) Modulo 9 je skup suma tri kuba $\{0, 1, 2, 3, 6, 7, 8\}$. Budući da je $4 \cdot 7 \equiv 5 \cdot 2 \equiv 1 \pmod 9$, svaki element iz $\{1, 4, 5, 8\}$ je modulo 9 inverz klase ostataka koja je suma tri kuba. Argument s podizanjem sličan onome u dokazu (b3) pokazuje za $m \equiv 0, 1, 2, 3, 6, 7, 8 \pmod 9$, kongruencija $x^3 + y^3 + z^3 \equiv m \pmod{3^r}$ ima rješenje sa $3 \nmid x$ za svaki $r \geq 2$. Stoga za $m \equiv 1, 4, 5, 8 \pmod 9$ kongruencija $(x^3 + y^3 + z^3)^{-1} \equiv m \pmod{3^r}$ ima rješenje sa $3 \nmid x$ za svaki $r \geq 2$.

Svaka klasa ostataka modulo 9 je produkt elementa iz skupa $\{0, 1, 2, 3, 6, 7, 8\}$ i elementa iz $\{1, 4, 5, 8\}$. Za dani prirodni broj n i $r \geq 2$ napišimo $n \equiv m_1 m_2 \pmod{3^r}$, gdje je m_1 modulo 9 u $\{0, 1, 2, 3, 6, 7, 8\}$, a m_2 modulo 9 je u $\{1, 4, 5, 8\}$. Tada postoje $c_1, c_2 \in C_3$ takvi da vrijedi $c_1 c_2^{-1} \equiv m_1 m_2 \equiv n \pmod{3^r}$. Po Lemi 3.3 imamo da je $R(C_2)$ gust u $\mathbb{Q}_3$. □

3.3 Rekurzije drugog reda

Garcia i Luca su pokazali da je skup kvocijenata Fibonaccijevih brojeva gust u $\mathbb{Q}_p$ za svaki p. Dokaz je koristio malu količinu algebarske teorije brojeva i neke relativno nepoznate rezultate o Fibonaccijevim brojevima. Prosti brojevi $p = 2$ i $p = 5$ su zahtijevali poseban pristup. Ovaj rezultat je proširio Sanna koji je dokazao da je razlomački skup k-generaliziranih Fibonaccijevih brojeva gust u $\mathbb{Q}_p$ za sve cijele brojeve $k \geq 2$ i za sve proste brojeve p. U ovom ćemo odjeljku pokazati rezultat za određene rekurzije drugog reda koje uključuju Fibonaccijeve brojeve kao poseban slučaj.

Fiksiramo cijele brojeve r i s i neka je $(a_n)_{n\geq 0}$ definiran s

$$a_0 = 0, \quad a_1 = 1, \quad a_{n+2} = ra_{n+1} + sa_n$$

te neka je $(b_n)_{n\geq 0}$ definiran s

$$b_0 = 2, \quad b_1 = r, \quad b_{n+2} = rb_{n+1} + sb_n.$$

Nizove $(a_n)_{n\geq 0}$ i $(b_n)_{n\geq 0}$ zovemo *Lucasovi nizovi prve vrste*, odnosno *druge vrste*. Pretpostavljamo da karakteristični polinom $x^2 - rx - s$ ima dva korijena različita od nule $\alpha, \beta \in \mathbb{C}$ takva da α/β nije korijen iz jedinice. Posebno, α i β su različiti, pa je tada lako dobiti

$$a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

i

$$b_n = \alpha^n + \beta^n,$$

za sve cijele brojeve $n \geq 0$ te je $a_n, b_n \neq 0$ za sve $n \geq 1$. Za svaki prost broj p takav da $p \nmid s$, neka je $\tau(p)$ najmanji prirodan broj k takav da $p \mid a_k$ (zna se da takav k postoji).

Vezano uz p-adsku valuaciju od $(a_n)_{n\geq 0}$ navodimo idući teorem bez dokaza.

Teorem 3.13. *Ako $p \nmid s$, tada je*

$$v_p(a_n) = \begin{cases} v_p(n) + v_p(a_p) - 1 & ako\ p \mid \Delta, p \mid n \\ 0 & ako\ p \mid \Delta, p \nmid n \\ v_p(n) + v_p(a_{p\tau(p)}) - 1 & ako\ p \nmid \Delta, \tau(p) \mid n, p \mid n \\ v_p(a_{\tau(p)}) & ako\ p \nmid \Delta, \tau(p) \mid n, p \nmid n \\ 0 & ako\ p \nmid \Delta, \tau(p) \nmid n \end{cases}$$

za sve prirodne brojeve n, pri čemu je $\Delta = r^2 + 4s$.

Dokazat ćemo sljedeći rezultat.

Teorem 3.14. *Neka je $A_n = \{a_n : n \geq 1\}$ i $B_n = \{b_n : n \geq 1\}$.*

(a) Ako $p \mid s$ i $p \nmid r$, tada $R(A)$ nije gust u $\mathbb{Q}_p$.

(b) Ako $p \nmid s$, tada je $R(A)$ gust u $\mathbb{Q}_p$.

(c) Za sve neparne proste brojeve p je $R(B)$ gust u $\mathbb{Q}_p$ ako i samo ako postoji prirodan broj n takav da $p \mid b_n$.

Dokaz.

(a) Ako $p \mid s$ i $p \nmid r$, tada se induktivno vidi $a_n \equiv r^{n-1} \pmod{p}$ tako da je $v_p(a_n) = 0$ za $n \geq 0$. Stoga, $R(A)$ nije gust u $\mathbb{Q}_p$ po Lemi 3.1.

(b) Prepostavimo da $p \nmid s$. Iz Teorema 3.13 slijedi da za svaki cijeli broj $j \geq 1$ postoji cijeli broj $m \geq 1$ tako da je $v_p(a_m) \geq j$. Stoga je

$$a_m = \frac{\alpha^m - \beta^m}{\alpha - \beta} \equiv 0 \pmod{p^j}$$

tako da je

$$\alpha^m \equiv \beta^m \pmod{p^j}, \tag{3.1}$$

gdje sa $x \equiv y \pmod{t}$, označavamo da je $(x - y)/t$ algebarski cijeli broj. Neka je $k = 2mp^{j-1}(p-1)$, pa po (3.1) slijedi

$$\alpha^k \equiv \beta^k \equiv (\alpha^m\beta^m)^{p^{j-1}(p-1)} \equiv (-s)^{mp^{j-1}(p-1)} \equiv 1 \pmod{p^j},$$

budući da je $\alpha\beta = -s$, $p \nmid s$ i zahvaljujući Eulerovom teoremu. Zato je

$$\begin{aligned} \frac{a_{kn}}{a_k} &= \frac{\left(\alpha^k\right)^n - \left(\beta^k\right)^n}{\alpha^k - \beta^k} \\ &= \left(\alpha^k\right)^{n-1} + \left(\alpha^k\right)^{n-2}\left(\beta^k\right) + \cdots + \left(\beta^k\right)^{n-1} \\ &\equiv n \pmod{p^j}, \end{aligned}$$

za sve prirodne brojeve n. Budući da su n i j bili proizvoljni, po Lemi 3.3 slijedi da je $R(A)$ gust u $\mathbb{Q}_p$.

(c) ($\Rightarrow$) Dokazujemo obrat po kontrapoziciji. Ako $p \nmid b_n$ za sve $n \geq 1$, tada je $v_p(b_n) = 0$ za sve $n \geq 1$. Tada $R(B)$ nije gust u $\mathbb{Q}_p$ po Lemi 3.1.

(c) ($\Leftarrow$) Pretpostavimo da je p neparan prost broj koji dijeli b_n za neki $n \geq 1$. Budući da je $b_n = a_{2n}/a_n$, imamo

$$v_p(b_n) = v_p(a_{2n}) - v_p(a_n).$$

Stoga je $v_p(a_{2n}) > v_p(a_n)$. Kako je p neparan, po Teoremu 3.13 slijedi

$$p \nmid \Delta, \quad \tau(p) \nmid n, \quad \tau(p) \mid 2n, \tag{3.2}$$

što povlači

$$v_2(\tau(p)) = v_2(n) + 1. \tag{3.3}$$

Za cijeli broj $j \geq 1$ neka je

$$k = p^{j+1} \cdot \frac{p-1}{2^{v_2(p-1)}} \cdot n.$$

S jedne strane, po (3.3) imamo da $\tau(p) \nmid k$, pa Teorem 3.13 daje $v_p(a_k) = 0$. S druge strane, $\tau(p) \mid 2k$ i $p \mid 2k$. Stoga, po Teoremu 3.13 imamo

$$v_p(a_{2k}) = v_p(2k) + v_p(a_{p\tau(p)}) - 1 \geq j.$$

Dakle,

$$v_p(b_k) = v_p(a_{2k}) - v_p(a_k) \geq j,$$

tako da je

$$\alpha^k \equiv -\beta^k \pmod{p^j}.$$

Označimo $h = 2^{v_2(p-1)}$, pa imamo

$$\begin{aligned}(\alpha^k)^{2h} &\equiv (\alpha^k)^h(\alpha^k)^h \equiv (\alpha^k)^h(-\beta^k)^h \\ &\equiv (\alpha^k)^h(\beta^k)^h \equiv (-s)^{p^{j+1}(p-1)n} \equiv 1 \pmod{p^j},\end{aligned}$$

budući da je $\alpha\beta = -s$, $p \nmid s$ i zahvaljujući Eulerovom teoremu. Uočimo da su $2h$ i p^j relativno prosti, pa po Kineskom teoremu o ostatcima za svaki prirodan broj m možemo odabrati prirodan broj ℓ tako da je

$$\ell \equiv m \pmod{p^j} \quad \text{i} \quad \ell \equiv 1 \pmod{2h}.$$

Kako je ℓ neparan, slijedi

$$\begin{aligned}\frac{b_{k\ell}}{b_k} &= \frac{(\alpha^k)^\ell + (\beta^k)^\ell}{(\alpha^k) + (\beta^k)} \\ &= (\alpha^k)^{\ell-1} + (\alpha^k)^{\ell-2}(-\beta^k) + \cdots + (-\beta^k)^{\ell-1} \\ &\equiv \ell(\alpha^k)^{\ell-1} \equiv m \pmod{p^j}.\end{aligned}$$

Budući da su j i m bili proizvoljni, po Lemi 3.3 znamo da je $R(B)$ gust u $\mathbb{Q}_p$. $\square$

Korolar 3.15. *Neka je $(F_n)_{n\geq 0}$ niz Fibonaccijevih brojeva i neka je $(L_n)_{n\geq 0}$ niz Lucasovih brojeva. Neka je $F = \{F_n : n \geq 1\}$ i $L = \{L_n : n \geq 1\}$*

(a) $R(F)$ je gust u $\mathbb{Q}_p$ za svaki p.

(b) $R(L)$ je gust u $\mathbb{Q}_p$ ako i samo ako je $p \neq 2$ i $p \mid L_n$ za neki $n \geq 1$.

Dokaz. Uzmimo $r = s = 1$.

(a) Slijedi iz (b) dijela Teorema 3.14.

(b) Za neparne p tvrdnja je posljedica (c) dijela Teorema 3.14. Za $p = 2$, dovoljno je primijetiti da je $(L_n)_{n\geq 0}$ periodički modulo 8 i $8 \nmid L_n$ za svaki $n \geq 1$. Stoga, tvrdnja slijedi iz Leme 3.1. □

Zna se da skup prostih brojeva koji dijele barem jedan Lucasov broj L_n ima gustoću $\frac{2}{3}$ kao podskup svih prostih brojeva. U Teoremu 3.14 (a-b) dio je oštar u smislu da ako $p \mid s$ i $p \mid r$, tada $R(A)$ može ili ne mora biti gust u $\mathbb{Q}_p$.

Primjer 3.16. *Neka je $p = 3$, $r = 15$ i $s = -54$. Uočimo da $p \mid s$ i $p \mid r$. Tada je $\alpha = 9$ i $\beta = 6$, pa je*

$$a_n = \frac{9^n - 6^n}{9 - 6} = 3^{n-1}(3^n - 2^n).$$

Tvrdimo da $R(A)$ nije gust u $\mathbb{Q}_3$. Budući da je $v_3(3) = 1$ i $v_3(a_m/a_n) = (m-1) - (n-1) = m - n$ za $m, n \geq 0$, svaki element iz $R(A)$ koji je dovoljno blizu 3 u $\mathbb{Q}_3$ mora biti oblika a_{n+1}/a_n za neki $n \geq 1$. Međutim,

$$\begin{aligned} v_3\left(\frac{a_{n+1}}{a_n} - 3\right) &= v_3\left(\frac{3^n(3^{n+1} - 2^{n+1})}{3^{n-1}(3^n - 2^n)} - 3\right) \\ &= 1 + v_3\left(\frac{3^{n+1} - 2^{n+1}}{3^n - 2^n} - 1\right) \\ &= 1 + v_3(3^{n+1} - 2^{n+1} - 3^n + 2^n) \\ &= 1 + v_3(3^n(3-1) - 2^n(2-1)) \\ &= 1 + v_3(2 \cdot 3^n - 2^n) = 1 + v_3(3^n - 2^{n-1}) = 1, \end{aligned}$$

pa se $R(A)$ ne približava 3 u $\mathbb{Q}_3$ po volji blizu.

Primjer 3.17. *Neka je $p = 5$, $r = 20$ i $s = -75$. Uočimo da $p \mid s$ i $p \mid r$. Tada je $\alpha = 15$ i $\beta = 5$, pa je*

$$a_n = \frac{15^n - 5^n}{15 - 5} = 5^{n-1}\frac{3^n - 1}{2}.$$

Tvrdimo da je $R(A)$ gust u $\mathbb{Q}_5$. Neka je $N \in \mathbb{N}$ i pišemo $N = 5^t N_0$, za $5 \nmid N_0$. Neka je $r \geq t$ dovoljno velik takav da $r \not\equiv t - 1 \pmod 4$. Budući da je $\phi(5^{r+1}) = 4 \cdot 5^r$, zbog Eulerovog teorema možemo pisati

$$3^{4\cdot 5^r} - 1 = 5^{r+1}\ell, \quad 5 \nmid \ell. \tag{3.4}$$

Neka $m \geq 1$ zadovoljava

$$m \equiv \ell^{-1} N_0 (3^{r-t+1} - 1) \pmod{5^{r+1}}. \tag{3.5}$$

Eulerov teorem jamči da $5 \nmid m$ budući da $4 \nmid (r - t + 1)$. Ako je $n = 4 \cdot 5^r m$, tada je

$$\begin{aligned}
&(3^{n+r-t+1} - 1)\frac{a_n}{a_{n+r-t+1}} \\
&= 5^{n-1}\left(\frac{3^n - 1}{2}\right)\left(\frac{2}{5^{n+r-t}}\right) \\
&= 5^{-r+t-1}(3^{4\cdot 5^r m} - 1) \\
&= 5^t \left(\frac{3^{4\cdot 5^r m} - 1}{3^{4\cdot 5^r} - 1}\right)\left(\frac{3^{4\cdot 5^r} - 1}{5^{r+1}}\right) \\
&= 5^t \left(\frac{\left(3^{4\cdot 5^r}\right)^m - 1}{3^{4\cdot 5^r} - 1}\right)\ell \qquad (po\ (3.4)) \\
&= 5^t \left((3^{4\cdot 5^r})^{m-1} + (3^{4\cdot 5^r})^{m-2} + \cdots + 1\right)\ell \\
&\equiv 5^t m\ell \pmod{5^{r+1}} \qquad (\textit{budući da je } \phi(5^{r+1}) = 4 \cdot 5^r) \\
&\equiv 5^t N_0 \left(3^{r-t+1} - 1\right) \pmod{5^{r+1}} \qquad (\textit{po } (3.5)) \\
&\equiv N\left(3^{r-t+1} - 1\right) \pmod{5^{r+1}} \qquad (\textit{budući da je } N = 5^t N_0) \\
&\equiv N\left(3^{n+r-t+1} - 1\right) \pmod{5^{r+1}} \qquad (\textit{budući da } \phi(5^{r+1}) \mid n)
\end{aligned}$$

Budući da $4 \mid n$ i $4 \nmid (r - t + 1)$, slijedi da $5 \nmid (3^{n+r-t+1} - 1)$ i stoga

$$v_5\left(\frac{a_n}{a_{n+r-t+1}} - N\right) \geqslant r + 1.$$

Stoga je $R(A)$ 5-adski gust u $\mathbb{N}$, pa je gust i u $\mathbb{Q}_5$ po Lemi 3.3.

Pretpostavimo da $p \mid s$ i $p \mid r$. Tada je $d = \text{nzd}(r, s)$ djeljiv s p. Indukcijom slijedi da $d^{\lfloor n/2 \rfloor}$ dijeli a_n za $n \geq 0$. Preciznije

$$a_n = \sum_{k=0}^{n-1} \binom{n-1-k}{k} r^{\max\{n-1-2k,0\}} s^{\max\{\lfloor \frac{2k+1}{2} \rfloor, 0\}}$$

i stoga je teško točno odrediti $v_p(a_n)$. Prema tome, trenutno ne možemo potpuno karakterizirati kada je $R(A)$ gust u $\mathbb{Q}_p$ ako $p \mid s$ i $p \mid r$. No, u nekim slučajevima možemo upotrijebiti ad hoc metode. Razmotrimo sljedeći primjer.

Primjer 3.18. *Cjelobrojni niz*

$$0, 1, 2, -1, -12, -19, 22, 139, 168, -359, -1558, -1321, 5148, \ldots$$

je generiran rekurzijom

$$a_0 = 0, \quad a_1 = 1, \quad a_{n+2} = 2a_{n+1} - 5a_n, \quad n \geq 0.$$

U ovom slučaju su $\alpha = 1 + 2i$ *i* $\beta = 1 - 2i$ *kompleksni. Neka je* $A = \{a_n : n \geq 1\}$ *i indukcijom se pokaže da* $5 \nmid a_n$ *za sve* $n \geq 1$. *Po Lemi 3.1 i Teoremu 3.14 vrijedi da je* $R(A)$ *gust u* $\mathbb{Q}_p$ *ako i samo ako* $p \neq 5$.

3.4 Unije geometrijskih nizova

Razlomački skup od $A = \{2^n : n \in \mathbb{N}\} \cup \{3^n : n \in \mathbb{N}\}$ je gust u $\mathbb{R}_+$ kako smo pokazali u Propoziciji 2.10. Cijeli broj g se zove *primitivan korijen modulo* m ako je g generator multiplikativne grupe $(\mathbb{Z}/m\mathbb{Z})^\times$. Gauss je dokazao da primitivni korijeni postoje samo za module $2, 4, p^k$ i $2p^k$ gdje je p neparan prost broj.

Ograničit ćemo se na neparne proste brojeve.

Teorem 3.19. *Neka je* p *neparan prost broj, neka je* b *cijeli broj različit od nule i neka je*

$$A = \{p^j : j \in \mathbb{N}\} \cup \{b^j : j \in \mathbb{N}\}.$$

Tada je $R(A)$ *gust u* $\mathbb{Q}_p$ *ako i samo ako je* b *primitivan korijen modulo* p^2.

Dokaz. ($\Rightarrow$) Pretpostavimo da je $R(A)$ gust u $\mathbb{Q}_p$. Tvrdimo da je b primitivan korijen modulo p. Ako nije, tada postoji $m \in \{2, 3, \ldots, p-1\}$ takav da vrijedi $b^j \not\equiv m \pmod{p}$ za sve $j \in \mathbb{Z}$. Tada se $R(A)$ ne približava m u $\mathbb{Q}_p$ po volji blizu što je kontradikcija. Stoga, b mora biti primitivan korijen modulo p.

Pretpostavimo sada da b nije primitivan korijen modulo p^2. Budući da je b primitivan korijen modulo p, red od b modulo p^2 je barem $p - 1$. S druge strane taj red dijeli $\varphi(p^2) = p(p-1)$. Budući da je p prost broj, slijedi da b modulo p^2 mora biti $p - 1$. Stoga je $b^{p-1} \equiv 1 \pmod{p^2}$.

Ako je $b^n \equiv p+1 \pmod{p^2}$, tada je $b^n \equiv 1 \pmod{p}$ i zato je n višekratnik od $p - 1$. Tada je $b^n \equiv 1 \pmod{p^2}$ što je kontradikcija. Stoga se $R(A)$ ne približava $p + 1$ u $\mathbb{Q}_p$ po volji blizu te b mora biti primitivan korijen modulo p^2.

($\Leftarrow$) Neka je $r \geq 1$ i neka je $n = p^k m \in \mathbb{N}$ za $p \nmid m$. Budući da je b primitivan korijen modulo p^2, tada je i primitivan korijen modulo $p^3, p^4, \ldots$, pa postoji j takav da je $b^j m \equiv 1 \pmod{p^r}$. Stoga je

$$v_p\left(n - \frac{p^k}{b^j}\right) = k + v_p\left(m - \frac{1}{b^j}\right) \geq v_p(b^j m - 1) \geq r,$$

pa je $R(A)$ gust u $\mathbb{Q}_p$ po Lemi 3.3. □

Primitivni korijen modulo p nije nužno primitivni korijen modulo p^2. Primjerice, 1 je primitivni korijen modulo 2, ali nije modulo 4. Ili, ako je $p = 37$, tada je 18 primitivni korijen modulo p, ali nije modulo p^2.

Primjer 3.20. *Neka je $p = 5$ i $q = 7$. Vrijedi da je 5 primitivni korijen modulo 7 i obrnuto. Međutim, 5 je primitivni korijen modulo 7^2, ali 7 nije primitivni korijen modulo 5^2. Neka je*

$$A = \{5, 7, 25, 49, 125, 343, 625, 2401, 3125, \ldots\} = \{5^j : j \geq 0\} \cup \{7^j : j \geq 0\}$$

Tada Teorem 3.19 povlači da je $R(A)$ gust u $\mathbb{Q}_7$, ali nije u $\mathbb{Q}_5$.

Sljedeći nam teorem govori da postoji beskonačno mnogo takvih parova prostih brojeva. Dokaz je znatno složeniji od materijala koje smo do sad radili, pa ga izostavljamo.

Teorem 3.21. *Postoji beskonačno mnogo parova (p, q) prostih brojeva tako da p nije primitivni korijen modulo q, a q je primitivni korijen modulo p^2.*

Korolar 3.22. *Postoji beskonačno mnogo parova (p, q) prostih brojeva takvih da je razlomački skup od $\{p^j : j \geq 0\} \cup \{q^k : k \geq 0\}$ gust u $\mathbb{Q}_p$, ali nije u $\mathbb{Q}_q$.*

Neka $a \prec b$ označava "a je primitivni korijen modulo b" (s tim da je primitivni korijen modulo p^2 automatski i primitivni korijen modulo p). Sljedeća tablica pokazuje nekoliko mogućnosti, pri čemu smo sa I označili istinitu, a sa N neistinitu tvrdnju.

p	q	$p \prec q$	$q \prec p$	$p \prec q^2$	$q \prec p^2$
3	5	I	I	I	I
5	7	I	I	I	N
3	7	I	N	I	N
5	11	N	N	N	N
7	19	N	I	N	N

Bibliografija

[1] Bryan Brown, Michael Dairyko, Stephan Ramon Garcia, Bob Lutz, Michael Someck, *Four Quotient Set Gems* The American Mathematical Monthly, Vol. 121, No. 7 (August–September), pp. 590-598

[2] Andrej Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[3] Andrej Dujella, *Uvod u teoriju brojeva*, dostupno na `https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf` (srpanj 2019.)

[4] Stephan Ramon Garcia, Yu Xuan Hong, Florian Luca, Elena Pinsker, Carlo Sanna, Evan Schechter, Adam Starr, *p-adic quotient sets*, dostupno na `https://arxiv.org/abs/1607.07951` (siječanj 2018.)

[5] Neal Koblitz, *p-adic Numbers, p -adic Analysis, and Zeta -Functions* , Second Edition, Springer, New York, 1984.

Sažetak

Razlomački skup je skup kojeg dobivamo kada uzmemo kvocijent svakog para elemenata danog podskupa skupa prirodnih brojeva. Neka je $A \subseteq \mathbb{N}$ podskup skupa prirodnih brojeva. Tada je $R(A) = \{a/b : a, b \in A\}$ njemu pridruženi razlomački skup.

Ovaj diplomski rad sadrži tri poglavlja. U prvom poglavlju izlažemo osnovne pojmove i rezultate iz teorije brojeva koji se koriste u nastavku rada. U drugom poglavlju iskazujemo i dokazujemo četiri zanimljiva teorema o razlomačkim skupovima u realnim brojevima. U zadnjem poglavlju ovog rada promatramo razlomačke skupove u p-adskim brojevima, gdje je p neki prost broj.

Summary

A quotient set is the set we get when we take the quotient of each pair of the elements of a given subset of a set of positive integers. Let $A \subseteq \mathbb{N}$ be a subset of the set of positive integers. Then $R(A) = \{a/b : a, b \in A\}$ denotes the corresponding quotient set.

This graduate thesis is divided into three chapters. In the first chapter we give some of the fundamental terms and results from the theory of numbers used throughout the rest of the thesis. In the second chapter we state and prove four interesting theorems about quotient sets in real numbers. In the last chapter of this thesis, we study quotient sets in p-adic numbers, where p is some prime number.

Životopis

Rođena sam 1. ožujka 1996. godine u Šibeniku. Osnovnoškolsko obrazovanje započela sam 2002. godine u Osnovnoj školi Tina Ujevića. Nakon završene osnovne škole, upisala sam Prirodoslovno-matematičku gimnaziju Antuna Vrančića u Šibeniku. U srpnju 2014. godine upisala sam nastavnički smjer studija matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Nakon završenog preddiplomskog studija, upisala sam 2017. godine diplomski studij matematike, smjer Matematička statistika na istom fakultetu.