SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Vedran Batel

BROJEVNI SUSTAVI

Diplomski rad

Voditelj rada:
doc.dr.sc. Tomislav Pejković

Zagreb, rujan 2018.

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. ____________________________

Sadržaj

Uvod

Brojevni sustav u kojem smo navikli računati je dekadski sustav čije ime potječe od grčke riječi $\delta\varepsilon\kappa\alpha$ što znači deset. Najmanja moguća znamenka je 0, a najveća moguća znamenka je 9 i ukupno imamo deset znamenki. To je sustav na koji smo navikli, ali to nije jedini sustav. Osim dekadskog sustava postoje i ostali pozicijski sustavi, a najčešće se koriste binarni, oktalni i heksadekadski.

Binarni sustav je pozicijski brojevni sustav s bazom 2. To znači da u tom brojevnom sustavu za označavanje brojeva koristimo dvije znamenke i to 0 i 1. To je brojevni sustav s najmanjom bazom, a iz naziva njegove znamenke na engleskom jeziku, BInary digiT, nastalo je ime za najmanju količinu informacije BIT. Široko se koristi u tehnici, budući da je potrebno razlikovati samo dva stanja za prikaz znamenaka. Primjerice, napon od $2,4$ V do 5 V u TTL sustavima (tranzistor - tranzistorski logički sklop) označava znamenku 1, dok napon od 0 V do $2,4$ V označava 0. Tehničke pogodnosti proizlaze iz pojednostavljenja sklopova i velike razine šuma koje uređaj može neometano podnositi. Stoga danas digitalni uređaji gotovo isključivo koriste binarni sustav. Posljedično je korišten u računalima pa stoga i općenito u informatici i programiranju.

U digitalnoj tehnici koristi se i oktalni sustav koji ima osam znamenaka, od 0 do 7, a kako je $2^3 = 8$ jednostavno je pretvarati brojeve iz binarnog sustava u oktalni i obrnuto. Heksadekadski brojevni sustav je brojevni sustav s bazom šesnaest. Za predstavljanje svake znamenke potrebno je 16 različitih znakova te se u tu svrhu koristite znamenke od 0 do 9 koje imaju istu vrijednost kao i u dekadskom sustavu te slova A, B, C, D, E i F koja predstavljaju redom vrijednosti od 10 do 15. Heksadekadski sustav je naslijedio oktalni sustav kao čovjeku praktičniji prikaz brojeva koji su u svojoj prirodi binarni, dakle brojeva koji se koriste u računalima i softveru (heksadecimalni editor). Ta praktičnost je posljedica činjenice da je brojevna baza heksadekadskog sustava potencija broja dva te stoga svaka znamenka u heksadekadskom sustavu zamjenjuje četiri uzastopne znamenke binarnog sustava. Na primjer binarni broj 1111000010010110 se heksadekadski može kraće prikazati kao F096.

Navedeni su sustavi koji se najčešće koriste, ali naravno da postoji beskonačno mnogo brojevnih sustava pa nas zanima postoje li neka općenita pravila i svojstva u svim brojevnim sustavima te je to naša motivacija za ovaj rad. Također ćemo promatrati neke brojevne sustave koji nisu uobičajeni u primjenama, ali se pojavljuju u teoriji brojeva. Osnovna literatura korištena u radu je knjiga J.-P. Allouchea i J. Shallita [1].

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

Kratka povijest brojevnih sustava

Prvo ćemo se ukratko dotaknuti povijesti brojevnih sustava koristeći kao literaturu prvenstveno [2].

Prva pojava brojevnih sustava. Mezopotamija i Kina

Bilježenje brojeva postojalo je prije bilježenja riječi, u Mezopotamiji je zabilježeno u četvrtom tisućljeću prije Krista. Prvi bitan napredak bilo je uvođenje brojki oko 3500. pr. Kr. u Mezopotamiji. Tu su se iz prvotnih piktograma razvili prvi brojevni sustavi. U starim su civilizacijama najčešći bili nepozicijski brojevni sustavi s bazom 10, ali i 60, 20 te 12. Glavne karakteristike mezopotamske matematike su: praktična orijentacija, pozitivni razlomci (s nazivnikom 60), kombinacija dekadskog i seksagezimalnog sustava koji su uglavnom aditivni sustavi. Babilonski seksagezimalni sustav je prvi u povijesti bio pozicijski. Međutim, nije u potpunosti bio pozicijski zbog nedostatka znaka za nulu pa su neki znakovi mogli označavati više različitih brojeva. U perzijsko doba pojavljuje se i znak za nulu, ali se koristi samo kad je nula potrebna "usred" broja dok se ranije koristio razmak. U Kini se iza 1500.g. pr. Kr. koristio dekadski sustav.

Rimsko carstvo

Rimski je sustav primarno dekadski, ali s tzv. sekundarnom bazom 5. Suptraktivan je, tj. aditivan, osim što se u slučaju da se ispred simbola veće vrijednosti nađe simbol manje vrijednosti, ta manja oduzima od veće, primjerice IV = IIII.

Indija

Indijci su tijekom prvog tisućljeća poslije Krista razvili dekadski pozicijski sustav s nulom. Nula se pojavljuje najkasnije u 7. stoljeću. Prvo poznato korištenje posebnih simbola za decimalne znamenke uključujući i simbol za znamenku nula (mali krug) je na kamenom natpisu u hramu u Gwalioru iz 876. godine. Nulu Indijci nazivaju sunya, što znači praznina. U arapskom prijevodu to je sifr, što je u latiniziranoj verziji dalo pojam cifre, tj. znamenke.

Brahmagupta (598.–670.), najveći indijski matematičar svog doba, bitno je doprinio razvoju brojevnog sustava, uključivo korištenje nule i negativnih brojeva.

Bhaskara II iz 12. stoljeća je najveći matematičar klasičnog indijskog razdoblja. Značajan je njegov doprinos razumijevanju brojevnih sustava i općenito algebre.

Arapi

Do 10. stoljeća u arapskim su se zemljama koristila tri tipa aritmetike. Račun na prste, gdje se brojevi pišu riječima, a ovaj način računa su koristili trgovci i računovođe, seksagezimalni sustav gdje su brojevi označeni arapskim slovima, a koristio se najčešće za astronomiju. U indijskom dekadskom sustavu su znamenke negdje između 7. i 9. st. preuzete iz Indije, ali bez standardnog skupa simbola, tako da se u raznim krajevima koristilo donekle različite oblike znamenki. Ispočetka su ih koristili na prašnjavim pločama koje su omogućavale isto što i danas ploča i kreda. Al-Uqlidisi (oko 920.–980.) je opisao dekadski i seksagezimalni pozicijski sustav i pokazao kako metode prilagoditi za pero i papir. Od 7. st. korišten je i alfabetski sustav (abjad).

Novo doba

Poznato je da je Lagrange bez većih nevolja preživio razdoblje Francuske revolucije. U tom je razdoblju bio član odbora Akademije znanosti za standardizaciju mjera (1790.), koji se zalagao za metrički sustav i decimalni brojevni sustav. U toj je komisiji bilo zahtjeva za korištenjem baze 12, na što je Lagrange ironično zastupao korištenje baze 11, v. [2].

Kao što možemo vidjeti, kroz povijest su se koristili razni brojevni sustavi pa se možemo upitati zbog čega danas koristimo dekadski sustav. U principu, nema razloga zašto netko ne bi koristio pozicijski sustav s bazom različitom od 10. Odabir broja 10 kao baze brojevnog sustava je zapravo ništa drugo nego ishod određenih povijesnih procesa koji su nas mogli odvesti i u nekom drugom smjeru. Primjerice, u dobu u kojem živimo postoje jako napredna računala i strojevi koji rade u binarnom sustavu. Stoga postoje kulturalni i povijesni razlozi i za usvajanje binarnog sustava kao glavnog brojevnog sustava kojim bi se svi koristili. Međutim, ono što bi uzrokovalo probleme pri korištenju takvog sustava su dugi i nepregledni nizovi znamenaka nula i jedinica koje bi predstavljale određen broj. U tom smislu, bilo bi logičnije odabrati recimo heksadekadski sustav koji ima šesnaest znamenaka i kratke nizove za prikaz jednog broja. Suočeni s tom dilemom, možda je najbolji izbor nešto između, a to je upravo dekadski sustav koji ima pogodnost i u tome što ljudi imaju ukupno deset prstiju na rukama, v. [3].

Poglavlje 2

Osnovno o brojevim sustavima

Brojevni sustav je način prikazivanja cijelog broja (općenitije, elementa skupa S) kao konačne linearne kombinacije
$$n = \sum_{0 \le i \le r} a_i u_i.$$
Koeficijenti a_i nazivaju se znamenkama broja prikazanog u bazi s elementima iz niza u_i. Niz znamenaka $a_r a_{r-1} \cdots a_1 a_0$ je prikaz broja n. Po dogovoru pišemo prikaz počevši s najznačajnijim znamenkama.

Svaki nenegativni cijeli broj može se zapisati kao linearna kombinacija

$$\sum_{0 \le i \le r} a_i 10^i \, , 0 \le a_i < 10$$

i to je dekadski prikaz broja.

Općenito, brojevni sustav je uređena trojka

$$\mathcal{N} = (U, D, R)$$

pri čemu je $U = \{u_0, u_1, u_2, \ldots\}$ beskonačan niz elemenata skupa S zvan *bazni niz*, D je obično podskup skupa S, zovemo ga skup znamenaka i $R \subseteq D^*$ je skup valjanih prikaza brojeva. Ovdje smo s D^* označili skup svih konačnih nizova (tj. riječi) s elementima iz D. Definiramo preslikavanje $[w]_U$ iz D^* u S na sljedeći način

$$\text{Ako je } w = a_t a_{t-1} \cdots a_1 a_0, \text{tada je } [w]_U = \sum_{0 \leqslant i \leqslant t} a_i u_i$$

Kako bismo imali ispravan brojevni sustav, moraju vrijediti dva željena svojstva, a to su

a) Postoji barem jedan valjani prikaz za svaki element danog skupa S. Kažemo da je $\mathcal{N}$ *potpun*.

b) Nijedan element nema više od jednog valjanog prikaza. Kažemo da je $\mathcal{N}$ *jednoznačan*.
   Kada je $\mathcal{N}$ potpun i jednoznačan, onda kažemo da je *savršen*. U tom slučaju preslikavanje $[w]_U$ je invertibilno.

Sada se bavimo određivanjem uređene trojke $\mathcal{N}$ te dolazimo do raznih zaključaka. Naš cilj je da za dani niz U nađemo skupove D i R takve da je uređena trojka (U, D, R) savršena. Brojevni sustav može biti određen na više načina.

1) Fiksiramo skup D. Bilo koji niz znamenaka odabranih iz skupa D je dopušten ako vodeća znamenka nije nula.

2) Drugi način je odabrati U i odrediti R metodom "pohlepni algoritam" koji proizvodi "pohlepne prikaze". U svrhu konkretizacije, pretpostavimo da je S skup prirodnih brojeva i neka je $u_0 < u_1 < u_2 < \dots$ beskonačan rastući niz prirodnih brojeva. Također pretpostavimo da je $u_0 = 1$. "Pohlepni algoritam" izražava bilo koji prirodan broj N kao linearnu kombinaciju
$$\sum_{0 \leqslant i \leqslant t} a_i u_i.$$

Pogledajmo na koji način funkcionira taj algoritam.

Pohlepni(N)
$t := 0$
dok je $u_{t+1} \leqslant N$ radi
    $t := t + 1$
za $i = t$ do $i = 0$ radi
    $a_i := \lfloor N/u_i \rfloor$
    $N := N - a_i u_i$
    izlaz (a_i)

Ovdje smo sa $\lfloor x \rfloor$ označili najveće cijelo od x. Budući da je $u_0 = 1$, algoritam uvijek završava. Ako je Pohlepni(N)=$a_t a_{t-1} \cdots a_1 a_0$, tada je

$$N = \sum_{0 \leqslant i \leqslant t} a_i u_i. \tag{2.1}$$

Definirajmo sada skup valjanih prikaza s

$$R = \{\text{Pohlepni}(N) : N \geqslant 1\} \cup \{\epsilon\}$$

Ovdje smo sa ϵ označili praznu riječ, tj. niz duljine 0. U ovom slučaju, skup znamenaka D je implicitno definiran kroz izlaz algoritma. Lako je vidjeti da je $a_i < u_{i+1}/u_i$. Ako

je $c = \sup_{i\geq 0} u_{i+1}/u_i$ konačan, tada je i D konačan i možemo uzeti da je $D = \sum_{\lfloor c\rfloor+1} = \{0, 1, \ldots, \lfloor c\rfloor\}$. Zgodno svojstvo pohlepnih prikaza je očuvanje poretka, a pod time mislimo sljedeće:
Neka je w (tj. x) pohlepni prikaz od m (tj. n). Dodajmo kraćem bloku od w i x vodeće nule pa dobivamo prikaze iste duljine w' (tj. x'). Tada w' prethodi x' u leksikografskom poretku ako i samo ako je $m < n$.

Pohlepni algoritam proizvodi savršeni brojevni sustav. Ipak često je korisno naći lako izračunljiv uvjet koji točno karakterizira R. Sljedeći teorem to postiže kad je osnovni skup $\mathbb{N}$.

Teorem 2.1. *Neka je $u_0 < u_1 < u_2 < \ldots$ rastući niz cijelih brojeva takav da je $u_0 = 1$. Svaki nenegativni cijeli broj N ima točno jedan prikaz oblika $\sum_{0\leqslant i\leqslant s} a_i u_i$ gdje je $a_s \neq 0$, a za $i \geq 0$ su znamenke a_i nenegativni cijeli brojevi koji zadovoljavaju nejednakost*

$$a_0u_0 + a_1u_1 + \cdots + a_iu_i < u_{i+1}. \tag{2.2}$$

Dokaz. Za $N = 0$, rezultat je istinit budući da je tada N prikazan praznom sumom od 0 članova. Ako je $N \neq 0$, tada prvo dokazujemo da pohlepni algoritam stvara prikaz koji zadovoljava (2.2). Račun pohlepnog algoritma može biti prikazan na sljedeći način.

$$\begin{aligned}
N &= a_tu_t + r_t & &(0 \leq r_t < u_t),\\
r_t &= a_{t-1}u_{t-1} + r_{t-1} & &(0 \leq r_{t-1} < u_{t-1}),\\
r_{t-1} &= a_{t-2}u_{t-2} + r_{t-2} & &(0 \leq r_{t-2} < u_{t-2}),\\
&\vdots\\
r_2 &= a_1u_1 + r_1 & &(0 \leq r_1 < u_1),\\
r_1 &= a_0u_0.
\end{aligned}$$

Sada je lako indukcijom vidjeti da je $r_{i+1} = a_iu_i + a_{i-1}u_{i-1} + \cdots + a_0u_0$ i štoviše, imamo $r_{i+1} < u_{i+1}$ pa je (2.2) zadovoljena.
Sljedeće što dokazujemo je jedinstvenost prikaza. Pretpostavimo da N ima dva različita prikaza.

$$\begin{aligned}
N &= a_su_s + \cdots + a_0u_0\\
&= b_su_s + \cdots + b_0u_0
\end{aligned}$$

gdje su a_i i b_i nenegativni cijeli brojevi i kraći prikaz dupunjen je nulama ako je potrebno tako da prikazi imaju istu duljinu. Uočimo da s može biti odabran tako da je barem jedan od a_s, b_s različit od nule. Neka je i najveći cijeli broj takav da je $a_i \neq b_i$. Bez smanjenja općenitosti, pretpostavimo da je $a_i > b_i$. Tada je

$$u_{i+1} \leq (a_{i+1} - b_{i+1})u_{i+1} = (b_i - a_i)u_i + \cdots + (b_0 - a_0)u_0 \leq b_iu_i + \cdots + b_0u_0$$

što je u kontradikciji s (2.2). □

Kao posljedica teorema 2.1, dobivamo osnovni teorem prikaza u bazi k.
Neka je $\sum_k = \{0, 1, \ldots, k-1\}$ i definiramo C_k kao skup

$$C_k := \{\epsilon\} \cup (\textstyle\sum_k \setminus\{0\}) \sum_k^*$$

Korolar 2.2. *Neka je $k \geq 2$ cijeli broj. Tada svaki nenegativni cijeli broj ima jedinstven prikaz oblika*

$$N = \sum_{0 \leq i \leq t} a_i k^i$$

gdje je $a_t \neq 0$ i $0 \leq a_i < k$ za $0 \leq i \leq t$.

Dokaz. Ovaj prikaz dobiva se pomoću pohlepnog algoritma. Prema (2.2) i $u_i = k^i$ imamo $a_i k^i < k^{i+1}$ pa je $a_i < k$. S druge strane, svaki niz $a_r a_{r-1} \cdots a_0$ s $a_r \neq 0$ i $0 \leq a_i < k$ za $0 \leq i \leq r$ predstavlja valjani izlaz pohlepnog algoritma jer je

$$a_0 + a_1 k + \cdots + a_r k^r \leq (k-1)(1 + k + \cdots + k^r) = k^{r+1} - 1 < k^{r+1}.$$

□

Sada definiramo kanonski prikaz u bazi k. Dokazali smo da za svaki nenegativan cijeli broj N postoji jedinstveni prikaz oblika $N = \sum_{0 \leq i \leq t} a_i k^i$ s $a_t \neq 0$ i $0 \leq a_i < k$. U tom slučaju definiramo $(N)_k = a_t a_{t-1} \cdots a_1 a_0 \in C_k$. Tako je primjerice $(19)_2 = 10011$.
Definirajmo i inverznu operaciju. Za $w = b_1 b_2 \cdots b_r$, definiramo $[w]_k = \sum_{1 \leq i \leq r} b_i k^{r-i}$. Očito vrijedi $[(N)_k]_k = N$.

Iako smo definirali razvoj u bazi k pri čemu je k prirodan broj veći od 1, moguće je takav razvoj definirati i za $k = 1$. U tom slučaju imamo takozvani *unarni* prikaz u kojem je cijeli broj n prikazan nizom $1^n = \underbrace{11 \cdots 1}_{\text{n}}$, v. [1].

Poglavlje 3

Sume znamenaka

Neka je k cijeli broj takav da je $k \geq 2$. Definirajmo dvije prirodne funkcije na osnovi kanonskog prikaza nenegativnog broja u bazi k. Ako je $(n)_k = b_r b_{r-1} \cdots b_0$, definiramo $\ell_k(n) = r + 1$ što je *duljina zapisa* u bazi k. Očito imamo

$$\ell_k(n) = \begin{cases} 1 + \lfloor \log_k n \rfloor, & \text{ako je } n \geq 1, \\ 0, & \text{ako je } n = 0. \end{cases}$$

Također, definiramo $s_k(n)$ kao *sumu znamenaka* u bazi k.

$$s_k(n) := \sum_{0 \leq i \leq r} b_i.$$

Funkcije $\ell_k(n)$ i $s_k(n)$ se pojavljuju u mnogim područjima matematike, a naročito u teoriji brojeva. U ovom dijelu fokusiramo se na neka svojstva $s_k(n)$. Podsjetimo se da $\nu_k(r)$ označava eksponent najveće potencije od k koja dijeli r, npr. $\nu_2(40) = 3$.

Teorem 3.1. *Neka su k i n cijeli brojevi takvi da je $k \geq 2$ i $n \geq 0$. Tada je*

$$\sum_{1 \leq m \leq n} \nu_k(m) = \frac{n - s_k(n)}{k - 1}.$$

Dokaz. Rezultat je očito istinit za $n = 0$. Neka je m cijeli broj takav da je $m \geq 1$ i pretpostavimo da je prikaz od m u bazi k jednak $w\, c\, 0^a$ za neke $w \in \sum_k^*$, $c \in \sum_k \backslash \{0\}$ i a je nenegativni cijeli broj. Primijetimo da je $a = \nu_k(m)$. Tada je $m - 1$ prikazan u bazi k kao

$$\text{Concat}(w, (c-1), (k-1)^a),$$

gdje eksponent označava ponavljanje, a Concat spajanje riječi. Tada imamo

$$s_k(m) - s_k(m-1) = 1 - (k-1)\nu_k(m). \tag{3.1}$$

Sada, zbrajanjem obiju strana od $m = 1$ do $m = n$ dobivamo

$$s_k(n) = n - (k-1) \sum_{1 \le m \le n} \nu_k(m)$$

iz čega proizlazi traženi rezultat za $n \ge 1$. □

Kao posljedicu dobivamo klasični Legendreov rezultat

Korolar 3.2. *Neka je p prost broj. Tada za sve $n \ge 0$ imamo*

$$\nu_p(n!) = \frac{n - s_p(n)}{p - 1}$$

Dokaz. Rezultat slijedi iz teorema 3.1 i činjenice da je

$$\sum_{1 \le m \le n} \nu_p(m) = \nu_p(n!)$$

□

Funkcija $s_k(n)$ se ne ponaša lijepo, beskonačno često može biti velika kao $(k-1)\log_k(n+1)$, ili mala kao 1. S ciljem razumijevanja "prosječnog" ponašanja $s_k(n)$ kada $n \to \infty$, uvodimo sumirajuću funkciju $S_k(x)$ definiranu kao

$$S_k(x) := \sum_{0 \le i < x} s_k(i).$$

Lako je sada, promatrajući koliko puta se koja znamenka pojavljuje na pojedinoj poziciji, vidjeti da vrijedi

$$S_k(k^n) = \frac{k-1}{2} k^n n, \tag{3.2}$$

što nam sugerira da je $S_k(x) \approx \frac{k-1}{2\log k} x \log x$. To i jest istina, što nam pokazuje sljedeći teorem. Prisjetimo se da Landauova notacija $f(x) = O(g(x))$ znači da postoje konstante $c > 0$ i $x_0 \ge 0$ takve da je $f(x) \le cg(x)$ za sve $x \ge x_0$.

Teorem 3.3. *Neka je k cijeli broj za koji vrijedi $k \ge 2$. Tada je*

$$S_k(x) = \frac{k-1}{2\log k} x \log x + O(x),$$

gdje konstanta u $O(x)$ ovisi o k, ali ne o x.

Dokaz. Pretpostavimo da je $0 \leq t < k$ i $j \geq 0$. Definirajmo $\varepsilon_j^{(k)}(n)$ kao koeficijent od k^j u prikazu od n u bazi k. Tada je $\varepsilon_j^{(k)}(n) = t$ ako i samo ako postoje $m, u \geq 0$ takvi da je

$$n = mk^{j+1} + u,$$

gdje je $tk^j \leq u < (t+1)k^j$. Sada definiramo funkciju $f(x, j, t)$ kao broj prirodnih brojeva $n < x$ takvih da je $\varepsilon_j^{(k)}(n) = t$. Tada je

$$\begin{aligned} f(x, j, t) &= \sum_{\substack{m,u \geq 0 \\ mk^{j+1}+u<x \\ tk^j \leq u < (t+1)k^j}} 1 \\ &= \sum_{tk^j \leq u < (t+1)k^j} \left(\frac{x}{k^{j+1}} + O(1) \right) \\ &= \frac{x}{k} + O(k^j). \end{aligned}$$

Sada je

$$\begin{aligned} S_k(x) &= \sum_{\substack{0 \leq j < \frac{\log x}{\log k} \\ 0 \leq t < k}} t f(x, j, t) \\ &= \sum_{\substack{0 \leq j < \frac{\log x}{\log k} \\ 0 \leq t < k}} t \left(\frac{x}{k} + O(k^j) \right) \\ &= \frac{k(k-1)}{2} \left(\frac{\log x}{\log k} + O(1) \right) \frac{x}{k} + \frac{k(k-1)}{2} \sum_{0 \leq j < \frac{\log x}{\log k}} O(k^j) \\ &= \frac{k-1}{2 \log k} x \log x + O(x) + \frac{k(k-1)}{2} O\left(\frac{kx-1}{k-1} \right) \\ &= \frac{k-1}{2 \log k} x \log x + O(x). \end{aligned}$$

□

Sljedeći teorem pokazuje da je rezultat teorema 3.3 najbolji mogući.

Teorem 3.4. *Postoji beskonačni rastući niz prirodnih brojeva $(x_n)_{n \geq 1}$ i konstanta $C > 0$ takva da je*

$$\left| S_k(x_n) - \frac{k-1}{2 \log k} x_n \log x_n \right| \geq C x_n$$

za sve $n \geq 1$.

Dokaz. Neka je $x_n = (k+1)k^{n-1}$. Tada je

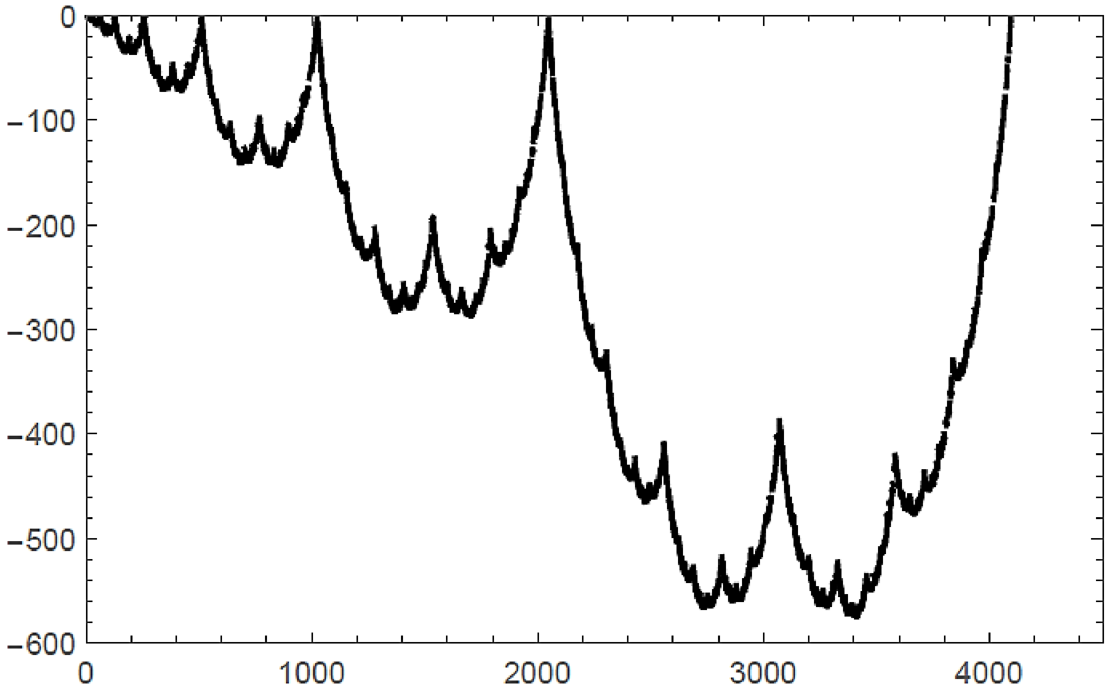
$$S_k((k+1)k^{n-1}) - S_k(k^n) = k^{n-1} + S_k(k^{n-1}),$$

a iz (3.2) znamo da je

$$S_k(k^n) = \frac{k-1}{2} \cdot k^n \cdot n.$$

Stoga je

$$S_k((k+1)k^{n-1}) = k^{n-1} + \frac{k-1}{2}k^n n + \frac{k-1}{2}k^{n-1}(n-1).$$



Slika 3.1: Graf funkcije $S_2(x) - \frac{x \log x}{2 \log 2}$ za $1 \leq x \leq 4096$

Sada definirajmo

$$C(k) = \frac{\frac{k-1}{2 \log k} x_n \log x_n - S_k(x_n)}{x_n}.$$

Vidjet ćemo da $C(k)$ ne ovisi o n. Naime, imamo

$$\begin{aligned}
C(k) &= \frac{k-1}{2\log k}\log(k^{n-1}(k+1)) - \left(\frac{k^{n-1} + \frac{k-1}{2}k^n n + \frac{k-1}{2}k^{n-1}(n-1)}{(k+1)k^{n-1}}\right) \\
&= \frac{k-1}{2}\log_k(k+1) + \frac{k-1}{2}(n-1) - \frac{nk^2 - n + 3 - k}{2(k+1)} \\
&= \frac{k-1}{2}\log_k(k+1) + \frac{(k^2-1)(n-1) - nk^2 + n - 3 + k}{2(k+1)} \\
&= \frac{1}{2}\left((k-1)\log_k(k+1) - \frac{k^2 - k + 2}{k+1}\right).
\end{aligned}$$

Provjerimo da je

$$C(k) > \frac{1}{2}(k - 1 - \frac{k^2 - k + 2}{k+1}) = \frac{k-3}{2(k+1)} = \frac{1}{2}(1 - \frac{4}{k+1}) \geq \frac{1}{2}(1 - \frac{4}{6}) = \frac{1}{6}.$$

Zato možemo uzeti $C = \frac{1}{8}$ i teorem je dokazan, v. [1]. □

Brojanje blokova i znamenački nizovi

U prošlom odjeljku smo promatrali svojstva funkcije sume znamenaka, $s_k(n)$. U slučaju kada je $k = 2$, funkcija $s_2(n)$ može se također promatrati kao brojanje pojavljivanja znamenke 1 u prikazu od n u bazi 2. To vodi k prirodnoj generalizaciji gdje brojimo pojavljivanja bilo kojeg bloka znamenaka u prikazu od n u bazi k.

Neka je $P \in \{0, 1, \ldots, k-1\}^* \setminus \{\epsilon\}$. Definirajmo $e_{k;P}(n)$ kao broj pojavljivanja od P u kanonskom prikazu broja n u bazi k. Dopuštena su preklapanja u različitim pojavama od P. Primjerice $e_{2;11}(7) = e_{2;11}(27) = 2$ jer je $(7)_2 = 111$ i $(27)_2 = 11011$. Dobiveni niz $(e_{k;P}(n))_{n\geq 0}$ ponekad se naziva *uzorački niz* za uzorak P. Ako je $P = 0^i$ za neke $i \geq 1$, kažemo da je P nul-uzorak, inače je P nenul-uzorak. Razjasnimo i slučaj kada P počinje nulom. Ako P sadrži barem jedan simbol različit od nule, tada u računanju $e_{k,P}(n)$ pretpostavljamo da prikaz od n u bazi k počinje s po volji dugim nizom nula. Tako je, primjerice, $e_{2;010}(5) = 1$. S druge strane, ako je P nul-uzorak, tj. $P = 0^i$ za neki $i \geq 1$, onda samo brojimo koliko puta se P pojavljuje u kanonskom prikazu od n u bazi k, npr. $e_{2;00}(36) = 2$.

Razmotrimo funkciju $e_{2;11}(n)$, koja broji pojavljivanja bloka 11 u prikazu od n u bazi 2. Ako za $n \geq 0$ stavimo $r_n = (-1)^{e_{2;11}(n)}$, tada dobijemo $\mathbf{r}$, poznati *Rudin-Shapirov niz*, kojemu je prvih nekoliko članova

$$\begin{array}{ccccccccccccccc}
n & = & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
r_n & = & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1
\end{array}$$

Rudin - Shapirov niz je najprije proučavan zbog zanimljivog odnosa s maksimumom nekih funkcija. Definirajmo L^2 normu funkcije

$$\|f\|_2 = \left(\frac{1}{2\pi}\int_0^{2\pi} |f(t)|^2 dt\right)^{\frac{1}{2}}$$

Sada nije teško vidjeti da, za bilo koji niz $(a_n)_{n\geq 0}$ s elementima iz $\{-1, +1\}$, vrijedi

$$\sup_{\theta\in\mathbb{R}} \left|\sum_{0\leq n<N} a_n e^{in\theta}\right| \geq \left\|\sum_{0\leq n<N} a_n e^{in\theta}\right\|_2 = \sqrt{N}.$$

S druge strane, može se pokazati da za "skoro sve" nizove $(a_n)_{n\geq 0}$ s elementima iz $\{-1, +1\}$ vrijedi

$$\sup_{\theta\in\mathbb{R}} \left|\sum_{0\leq n<N} a_n e^{in\theta}\right| = O\left(\sqrt{N\log N}\right) \tag{3.3}$$

Za Rudin - Shapirov niz imamo sljedeći rezultat.

Teorem 3.5. *Za Rudin - Shapirov niz* **r** *postoji konstanta $C \geq 0$ takva da za svaki $N \geq 0$ vrijedi*

$$\sup_{\theta\in\mathbb{R}} \left|\sum_{0\leq n<N} r_n e^{in\theta}\right| \leq C\sqrt{N}.$$

Štoviše, možemo uzeti da je $C = 2 + \sqrt{2}$.

Dokaz. Definirajmo 2-dimenzionalni vektor V_n i 2×2 matrice A_0 i A_1 s

$$V_n := \begin{pmatrix} r_n \\ r_{2n+1} \end{pmatrix}, \quad A_0 := \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad A_1 := \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}.$$

Koristeći relacije $r_{2n} = r_n$, $r_{4n+1} = r_n$ i $r_{4n+3} = -r_{2n+1}$, za sve $n \geq 0$ imamo

$$V_{2n} = A_0 V_n,$$
$$V_{2n+1} = A_1 V_n.$$

Ako sada definiramo

$$R(N,\theta) := \sum_{0\leq n<2^N} V_n e^{in\theta},$$
$$M(\theta) := A_0 + e^{i\theta} A_1,$$

lako dobivamo da je za sve $N \geq 1$

$$\begin{aligned}
R(N,\theta) &= \sum_{0\leq n<2^N} V_n e^{in\theta} \\
&= \sum_{0\leq n<2^{N-1}} V_{2n} e^{i(2n)\theta} + \sum_{0\leq n<2^{N-1}} V_{2n+1} e^{i(2n+1)\theta} \\
&= \sum_{0\leq n<2^{N-1}} A_0 V_n e^{i(2n)\theta} + \sum_{0\leq n<2^{N-1}} A_1 V_n e^{i(2n+1)\theta} \\
&= A_0 \left(\sum_{0\leq n<2^{N-1}} V_n e^{i(2n)\theta} \right) + A_1 \left(\sum_{0\leq n<2^{N-1}} V_n e^{i(2n+1)\theta} \right)
\end{aligned}$$

Dakle,

$$R(N,\theta) = A_0 R(N-1, 2\theta) + e^{i\theta} A_1 R(N-1, 2\theta) = M(\theta) R(N-1, 2\theta).$$

Ponavljanjem dobivamo

$$\begin{aligned}
R(N,\theta) &= M(\theta) R(N-1, 2\theta) \\
&= M(\theta) M(2\theta) R(N-2, 4\theta) \\
&= \cdots \\
&= M(\theta) M(2\theta) \cdots M(2^{N-1}\theta) R(0, 2^N\theta) \\
&= M(\theta) M(2\theta) \cdots M(2^{N-1}\theta) V_0.
\end{aligned} \tag{3.4}$$

Sada radimo kratku digresiju da bi rekli ponešto o normama vektora i matrica. Ako je $v = (v_1, v_2, \ldots, v_r)$ vektor realnih ili kompleksnih brojeva, tada s $||v||$ označavamo euklidsku normu $(\sum_{1\leq i\leq r} |v_i|^2)^{\frac{1}{2}}$. Neka je M kvadratna matrica dimenzije d s elementima iz $\mathbb{R}$ ili $\mathbb{C}$. S $||M||$ označavamo L^2 normu, što je matrična norma pridružena običnoj Euklidskoj normi na $\mathbb{R}^d$ ili $\mathbb{C}^d$ formulom $||M|| = \sup_{||x||=1} ||Mx||$. Ako je M matrica, tada je njezin spektralni radijus $\rho(M)$ definiran kao najveća apsolutna vrijednost njezinih svojstvenih vrijednosti. Koristit ćemo sljedeći teorem [6, str. 346].

Teorem 3.6. *Kvadrat L^2 norme od M jednak je $\rho(MM^*)$, gdje je M^* adjungirana matrica matrice M.*

Nastavak dokaza. Vratimo se sada dokazu teorema 3.5. Uzimajući L^2 normu obiju strana iz (3.4), dobivamo

$$\begin{aligned}\left|\sum_{0\le n<2^N} r_n e^{in\theta}\right| &\le \|R(N,\theta)\| = \|M(\theta)M(2\theta)\cdots M(2^{N-1})V_0\| \\ &\le \|M(\theta)M(2\theta)\cdots M(2^{N-1})\|\cdot\|V_0\| \\ &\le \left(\prod_{0\le j<2^N}\|M(2^j\theta)\|\right)\sqrt{2} = \sqrt{2}\prod_{0\le j<N}\sqrt{\rho(M(2^j\theta)M^*(2^j\theta))}.\end{aligned}$$

Jednostavni račun pokazuje da za svaki $\alpha\in\mathbb{R}$ vrijedi

$$\rho\left(\begin{pmatrix}1 & e^{i\alpha}\\ 1 & -e^{i\alpha}\end{pmatrix}\begin{pmatrix}1 & e^{i\alpha}\\ 1 & -e^{i\alpha}\end{pmatrix}^*\right) = \rho\left(\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}\right) = 2$$

tako da je

$$\left|\sum_{0\le n<2^N} r_n e^{in\theta}\right| \le \sqrt{2}(2^{N/2}).$$

Ovo daje tvrdnju teorema kad sumiramo po intervalu $[0,2^N-1]$. S ciljem omeđivanja sume

$$S(N,\theta) = \sum_{0\le n<N} r_n e^{in\theta}$$

uzimamo da je binarni zapis od N jednak $2^{N_0}+2^{N_1}+\cdots$, gdje je $N_0 > N_1 > \cdots \ge 0$. Umjesto $\sum_{a\le n<b} r_n e^{in\theta}$ kraće pišemo $\sum_{a\le n<b}$. Imamo

$$\sum_{a\le n<N} = \sum_{0\le n<2^{N_0}} + \sum_{2^{N_0}\le n<2^{N_0}+2^{N_1}} + \sum_{2^{N_0}+2^{N_1}\le n<2^{N_0}+2^{N_1}+2^{N_2}} + \cdots.$$

Svaka od ovih suma ima oblik $\sum_{K\le n<K+2^j}$, gdje 2^{J+1} dijeli K. Međutim, lako se vidi da ako je n element od $[0,2^J-1]$ i ako 2^{J+1} dijeli K, tada je $r_{n+K}=r_nr_K$ pa je

$$\sum_{K\le n<K+2^J} r_n e^{in\theta} = \sum_{0\le n<2^J} r_{n+K}e^{i(n+K)\theta} = \sum_{0\le n<2^J} r_nr_Ke^{in\theta}e^{iK\theta}.$$

Stoga je

$$\left|\sum_{K\le n<K+2^J} r_n e^{in\theta}\right| = \left|\sum_{0\le n<2^J} r_n e^{in\theta}\right| \le \sqrt{2}(2^{J/2}).$$

Vraćajući se sumi $S(N,\theta)$, imamo

$$|S(N,\theta)| \le \left|\sum_{0\le n<2^{N_0}}\right| + \left|\sum_{2^{N_0}\le n<2^{N_0}+2^{N_1}}\right| + \cdots \le \sqrt{2}(2^{N_0/2}+2^{N_1/2}+\cdots).$$

Kako bismo završili ovaj dokaz, dovoljno je pokazati da vrijedi

$$(2^{N_0/2} + 2^{N_1/2} + \cdots) \leq (1 + \sqrt{2})(2^{N_0} + 2^{N_1} + \cdots)^{1/2} = (1 + \sqrt{2})\sqrt{N}.$$

Definirajmo sada funkcije h_j s $h_j(x) := (x + 2^{N_j})^{1/2} - x^{1/2}$. Te funkcije su padajuće za $x \geq 0$ jer je $h_j'(x) < 0$. Stoga, kako je $N_0 > N_1 > \cdots$, imamo da za svaki j vrijedi

$$h_j(2^{N_j}) \leq h_j(2^{N_{j+1}} + 2^{N_{j+2}} + \cdots),$$

odnosno,

$$(2^{N_j} + 2^{N_j})^{1/2} - (2^{N_j})^{1/2} \leq (2^{N_j} + 2^{N_{j+1}} + \cdots)^{1/2} - (2^{N_{j+1}} + 2^{N_{j+2}} + \cdots)^{1/2}.$$

pa je

$$(\sqrt{2} - 1)2^{N_j/2} \leq (2^{N_j} + 2^{N_{j+1}} + \cdots)^{1/2} - (2^{N_{j+1}} + 2^{N_{j+2}} + \cdots)^{1/2}.$$

Zbrajanjem po j, dobivamo

$$(\sqrt{2} - 1)(2^{N_0/2} + 2^{N_1/2} + \cdots) \leq (2^{N_0} + 2^{N_1} + \cdots)^{1/2},$$

odnosno

$$(2^{N_0/2} + 2^{N_1/2} + \cdots) \leq (\sqrt{2} + 1)(2^{N_0} + 2^{N_1} + \cdots)^{1/2}.$$

□

Recimo sada ponešto o sumama uzoračkih nizova.

Teorem 3.7. *Neka je $(S(n))_{n\geq 0}$ niz realnih brojeva tako da je $S(0) = 0$ i neka je $k \geq 2$ cijeli broj. Tada S možemo na jedinstven način prikazati kao sumu uzoračkih nizova na sljedeći način*

$$S(n) = \sum_{i\geq 1} \hat{S}(i) e_{k;(i)_k}(n), \tag{3.5}$$

gdje su $\hat{S}(i)$ realni brojevi. Štoviše, ako S ima cjelobrojne vrijednosti, tada i niz $\hat{S}$ ima cjelobrojne vrijednosti. Preslikavanje $(S(n)) \to \left(\hat{S}(n)\right)$ zove se ***uzoračka transformacija*** *niza S.*

Dokaz. Primijetimo da je suma (3.5) dobro definirana zbog toga što za svaki n postoji samo konačan broj članova.

Kako bismo pokazali da koeficijenti $\hat{S}(i)$ postoje, možemo uzeti da je $\hat{S}(1) = S(1)$ jer je $e_{k;1}(1) = 1$. Promotrimo sada funkciju $S(n) - \hat{S}(1)e_{k;1}(n)$. Ova funkcija ima vrijednost 0 za $n = 0, 1$. Stoga možemo odabrati $\hat{S}(2)$ kao $S(2) - \hat{S}(1)e_{k;1}(2)$. Sada promotrimo $S(n) - \hat{S}(1)e_{k;1}(n) - \hat{S}(2)e_{k;(2)_k}(n)$, itd.

Kako bismo vidjeli da je zapis (3.5) jedinstven, uočimo da je $\hat{S}(1)$ potpuno određen uvrštavanjem $n = 1$. Kad je $\hat{S}(1)$ određen, $\hat{S}(2)$ je potpuno određen uvrštavanjem $n = 2$, itd.

Koeficijenti $\hat{S}(i)$ su cjelobrojni ako S sadrži cjelobrojni niz, zbog toga što u svakom koraku izvodimo operacije oduzimanja, a nikad dijeljenja. □

Sada prelazimo na pojam "znamenačkih nizova". Ako je prikaz broja n u bazi k jednak $n = \sum_{0\le i\le t} a_i k^i$, tada, kao i u dokazu teorema 3.3, definiramo $\varepsilon_i^{(k)}(n) = a_i$. (U slučaju kada je baza jasna iz konteksta, izostavit ćemo gornji indeks). Uočimo da je

$$\varepsilon_i^{(k)}(n) = \lfloor n/k^i \rfloor - k\lfloor n/k^{i+1} \rfloor.$$

Tada se za niz $(b(n))_{n\ge 0}$ kaže da je *znamenački niz* ako postoji prirodan broj r i funkcija $F : \mathbb{Z}^r \to \mathbb{C}$ takva da je $F(0, 0, \ldots, 0) = 0$ i

$$b(n) = \sum_{i\ge 0} F(\varepsilon_i(n), \ldots, \varepsilon_{i+r-1}(n)).$$

Uočimo da je suma dobro definirana jer je $F(0, 0, \ldots, 0) = 0$.

Primjer 3.8. *Niz $s_k(n)$ je znamenački. To odgovara slučaju kad je $r = 1$ i $F(x) = x$.*

Primjer 3.9. *Neka $B_k(n)$ označava broj blokova susjednih identičnih znamenki prikaza od n u bazi k. Primjerice, $B_{10}(3331000022) = 4$. Tada je $B_k(n)$ znamenački zato što možemo uzeti da je $r = 2$ i $F(x, y) = 1$ ako je $x \neq y$, a inače je 0.*

Teorem 3.10. *Niz $(b(n))_{n\ge 0}$ je znamenački ako i samo ako može biti izražen kao konačna linearna kombinacija ne-nul uzoračkih nizova.*

Dokaz. Neka je $\sum_k = \{0, 1, \ldots, k-1\}$. Pretpostavimo da je niz $(b(n))_{n\ge 0}$ znamenački. Tada je

$$b(n) = \sum_{i\ge 0} F(\varepsilon_i(n), \ldots, \varepsilon_{i+r-1}(n)).$$

Sada se lako vidi da je

$$b(n) = \sum_{(t_0,\ldots,t_{r-1})\in\sum_k^r} F(t_0, t_1, \ldots, t_{r-1}) e_{k;t_{r-1}t_{r-2}\ldots t_0}(n).$$

S druge strane, pretpostavimo da je $(b(n))_{n\ge 0}$ konačna linearna kombinacija ne-nul uzoračkih nizova, npr.

$$b(n) = \sum_{P\in\mathcal{P}} a_P e_{k;P}(n).$$

Ako je r duljina najduljeg niza u $\mathcal{P}$, pišemo

$$b(n) = \sum_{i \geq 0} F(\varepsilon_i(n), \ldots, \varepsilon_{i+r-1}(n)),$$

gdje je

$$F(t_0, t_1, \ldots, t_{r-1}) = \sum_{\substack{P \in \mathcal{P} \\ P \text{ sadrži } t_{r-1} \ldots t_1 t_0}} a_P.$$

$\square$

Poglavlje 4

Prikaz realnih brojeva

U prošlom poglavlju promatrali smo prikaz cijelih brojeva u bazi k. U ovom poglavlju kratko raspravljamo o prikazima realnih brojeva, usredotočujući se na prikaz u bazi k.

Teorem 4.1. *Neka je $k \neq 1$ prirodan broj. Svaki realni broj x može se prikazati u obliku*

$$\lfloor x \rfloor + \sum_{i \geq 1} a_i k^{-i},$$

gdje je $0 \leq a_i < k$. Ako x nije oblika b/k^r za neke cijele brojeve b i r takve da je $r \geq 0$, tada je prikaz jedinstven. Ako je x oblika b/k^r, $r \geq 0$, tada imamo dva različita prikaza, jedan u kojem je $a_i = 0$ za $i > r$ te drugi gdje je $a_i = k - 1$ za $i > r$.

Dokaz. Sljedeći algoritam osigurava jedan prikaz od x_0 u bazi k

```
    RealRep(k,x0)
a0 := ⌊x0⌋
i := 0
dok je ai ≠ xi radi
        xi+1 := k(xi − ai)
        i := i + 1
        ai := ⌊xi⌋
        izlaz(ai)
```

Ako algoritam završava na ulazu (k, x), tada je jasno da je $x = a_0 + \sum_{1 \leq i \leq r} a_i k^{-1}$ za neki $r \geq 0$. S druge strane, ako algoritam ne završava, tada je lako vidjeti da niz $(a_0 + \sum_{1 \leq i \leq r} a_i k^{-1})_{r \geq 1}$ teži u x slijeva. Stoga svaki broj ima barem jedan prikaz.

Pretpostavimo da postoje cijeli brojevi b i r takvi da je $x = b/k^r$. Tada možemo napisati da je $x = \lfloor x \rfloor + \{x\}$, gdje je $\{x\} = c/k^r$ za neki cijeli broj $c \geq 0$. Neka je $w = (c)_k$ prikaz cijelog broja c u bazi k i neka je $w' = 0^{r-|w|}w$. Tada, ako je $w' = d_1 d_2 \cdots d_r$, imamo sljedeću jednakost

$$x = a_0 + \sum_{i\geq 1} a_i k^{-1} = a'_0 + \sum_{i\geq 1} a'_i k^{-1},$$

gdje je $a_0 = \lfloor x \rfloor$, $a_i = d_i$ za $1 \leq i \leq r$, $a_i = 0$ za $i > r$, $a'_i = d_i$ za $1 \leq i < r$; $a'_r = d_r - 1$ i $a'_i = k - 1$ za $i > r$. Konačno, $a'_0 = a_0$, osim ako je $r = 0$, a u tom slučaju je $a'_0 = a_0 - 1$. Sad pretpostavimo da ne postoje cijeli brojevi b i r takvi da je $x = b/k^r$ i pretpostavimo da x ima barem dva različita prikaza. Primjerice

$$x = a_0 + \sum_{i\geq 1} a_i k^{-i}$$

i

$$x' = a'_0 + \sum_{i\geq 1} a'_i k^{-i},$$

gdje je $x = x'$. Kako se ovi prikazi razlikuju, mora postojati najmanji index $j \geq 0$ takav da je $a_j \neq a'_j$. Bez smanjenja općenitosti pretpostavimo da je $a_j < a'_j$. Tada postoji indeks $\ell > j$ takav da je $a_\ell < k - 1$, a ako ne, tada bismo imali $x = b/k^r$ za neke cijele brojeve b i r. Tada vrijedi da je $x' - x > k^{-\ell}$, što je u kontradikciji s pretpostavkom da je $x' = x$. □

Teorem 4.2. *Neka je $k \in \mathbb{Z}_{\geq 2}$ i neka je $\{x\} = 0.a_1 a_2 a_3 \ldots$ prikaz razlomljenog dijela broja x u bazi k. Tada je x racionalan broj ako i samo ako je beskonačna riječ*

$$\mathbf{a} = a_1 a_2 a_3 \ldots$$

periodična od nekog mjesta nadalje.

Dokaz. Pretpostavimo da je $\mathbf{a}$ periodična riječ. Tada možemo napisati

$$\{x\} = 0.a_1 a_2 a_3 \ldots a_r (a_{r+1} \ldots a_{r+s})^\omega$$

za neke cijele brojeve r i s takve da je $r \geq 0$ i $s > 0$. Tada je lako provjeriti da je

$$\{x\} = k^{-r}\left([a_1 a_2 \ldots a_r]_k + \frac{[a_{r+1} a_{r+2} \ldots a_{r+s}]_k}{k^s - 1}\right),$$

pa je x racionalan.

S druge strane, ako je x racionalan, tada je $\{x\} = b/c$ za cijele brojeve b i c takve da je $b \geq 0$ i $c > 0$. Svaki korak algoritma RealRep proizvodi novu znamenku a_i i x_i oblika b_i/c, takve da je $0 \leq b_i < c$. Ako je $b_i = 0$, algoritam završava, što odgovara periodičnom prikazu s periodom koji je jedna znamenka, 0. Ako algoritam ne završava, postoji najviše c različitih mogućnosti za b_i. Kad se jedna od njih pojavi po drugi put, izlaz algoritma postaje periodičan. □

Neka je $k \geq 2$ cijeli broj. Neka su $w, x \in \Sigma_k^*$ konačne riječi takve da je $w = a_1a_2 \ldots a_i$ i $x = b_1b_2 \ldots b_j$. Definiramo $[w.x]_k = [w]_k + k^{-j}[x]_k$. Slično, ako je $\mathbf{x} \in \Sigma_k^\omega$ i $\mathbf{x} = b_1b_2 \ldots$, tada definiramo $[w.\mathbf{x}]_k = \lim_{n\to\infty}([w]_k + k^{-j}[x_n]_k)$, gdje je $x_n = b_1b_2 \ldots b_n$.

Poglavlje 5

Prikaz u bazi k s drugim skupovima znamenki

U prethodnim poglavljima smo promatrali prikaze u bazi k koristeći skup znamenki $\Sigma_k = \{0, 1, \ldots, k-1\}$. Tako smo dobili brojevni sustav za nenegativne cijele brojeve gdje su valjani prikazi dani skupom $C_k = \{\epsilon\} \cup (\Sigma_k \setminus \{0\})\Sigma_k^*$. U ovom poglavlju ispitujemo korištenje alternativnih skupova znamenaka.

Počinjemo ispitivanjem skupa znamenki $E_k = \{1, 2, \ldots, k\}$. Ovaj skup znamenaka ima lijepo svojstvo izbjegavanja problema vodećih nula. Kao što sljedeći teorem pokazuje, tako dobivamo savršeni brojevni sustav za nenegativne cijele brojeve, gdje je skup valjanih prikaza jednostavno E_k^*.

Teorem 5.1. *Neka je $k \geq 2$ cijeli broj. Svaki cijeli broj $n \geq 0$ može biti na jedinstven način prikazan u obliku*

$$n = \sum_{0 \leq i \leq r} a_i k^i,$$

gdje su a_i cijeli brojevi *iz* $\{1, 2, \ldots, k\}$.

Taj prikaz naziva se bijektivni prikaz.

Dalje se okrećemo skupovima znamenaka koji uključuju pozitivne i negativne znamenke. Uključivanje negativnih znamenaka znači da postoji mogućnost prikazivanja svih cijelih brojeva, ne samo nenegativnih. Vjerojatno najpoznatiji primjer takvog tipa brojevnog sustava naziva se *uravnoteženi ternarni* sustav, koji prikazuje brojeve u bazi 3 koristeći skup znamenaka $F = \{-1, 0, 1\}$. To je savršeni brojevni sustav za skup $\mathbb{Z}$ čiji je odgovarajući skup valjanih prikaza dan s $\{\epsilon\} \cup (F \setminus \{0\})F^*$.

Nazovimo konačan skup D cjelobrojnih znamenki *osnovnim* za bazu k pri čemu je $k \geq 2$ ako je $0 \in D$ i

$$((1, k, k^2, \ldots), D, \{\epsilon\} \cup (D \setminus \{0\}))D^*)$$

je savršen brojevni sustav. Tada prirodno proizlazi sljedeće pitanje. Za danu bazu k, koji skupovi znamenaka su osnovni? Sljedeći teorem navodi odgovor.

Kažemo da je skup S *potpuni sustav ostataka* (modulo k) ako je $|S| = k$ i za sve cijele brojeve n postoji $m \in S$ takav da je $m \equiv n \pmod{k}$.

Teorem 5.2. *Neka je $k \geq 2$ cijeli broj. Tada je skup znamenaka D koji sadrži nulu osnovni za k ako i samo ako vrijede sljedeća dva uvjeta.*

(a) D čini potpuni sustav ostataka (modulo k),

(b) za sve $n \geq 1$ i sve $w \in D^n$, $[w]_k$ nije jednak niti jednom nenul višekratniku od $k^n - 1$.

Prije nego dokažemo teorem, iskazat ćemo i dokazati neke leme.

Lema 5.3. *Ako je D osnovni za k, tada je $|D| \leq k$.*

Dokaz. Pretpostavimo da je $|D| > k$. Neka je $m = \max_{d \in D} |d|$. Očito je $m \geq 1$. Razmotrimo nizove iz $S = (D \setminus \{0\})D^n$. Postoji najmanje $k(k+1)^n$ takvih nizova i ako su $w, x \in S$, moramo imati $[w]_k \neq [x]_k$, budući da je D osnovni. Ali za $w \in S$ imamo

$$|[w]_k| \leq mk^n + \cdots + mk + m \leq m(k^{n+1} - 1).$$

Stoga postoji najviše $2m(k^{n+1} - 1) + 1 \leq 2mk^{n+1}$ mogućih različitih vrijednosti za prikaze duljine točno $n+1$. Međutim, postoji $k(k+1)^n$ različitih prikaza i kako je $k(k+1)^n > 2mk^{n+1}$ za n dovoljno velik, neki broj mora imati najmanje dva prikaza. Stoga D ne može biti osnovni. □

Lema 5.4. *Ako je D osnovni za k, tada D mora biti potpuni sustav ostataka modulo k.*

Dokaz. Kako je D osnovni za k, za sve i takve da je $0 \leq i < k$ mora postojati prikaz w takav da je $[w]_k = i$. Pretpostavimo da je $w = a_r a_{r-1} \cdots a_1 a_0$. Tada je $i = a_r k^r + \cdots + a_1 k + a_0$ pa uzimajući obje strane modulo k, proizlazi da je $i \equiv a_0 \pmod{k}$. Prema lemi 5.3, D sadrži najviše k elemenata pa rezultat slijedi. □

Lema 5.5. *Ako je D baza za k, tada $j(k-1) \notin D$ za sve $j \neq 0$.*

Dokaz. Pretpostavimo da je D osnovni i pretpostavimo da postoji $j \neq 0$ takav da je $j(k-1) \in D$. Kako je D osnovni, postoji niz w takav da je $[w]_k = -j$. Neka je $w = a_r a_{r-1} \cdots a_1 a_0$. Budući da je $a_0 \equiv -j \pmod{k}$, prema lemi 5.4, imamo da je $a_0 = j(k-1)$. Stoga je

$$[a_r a_{r-1} \cdots a_1]_k = \frac{(-j) - a_0}{k} = \frac{-j - jk + j}{k} = -j$$

pa $-j$ ima dva različita prikaza, što je kontradikcija. □

Lema 5.6. *Za bilo koji cijeli broj $t \geq 1$, skup znamenaka D je osnovni za k ako i samo ako je skup znamenaka $\{[w]_k : w \in D^t\}$ osnovni za k^t.*

Dokaz prethodne leme je vrlo jednostavan. Sada smo spremni dokazati teorem 5.2.

Dokaz. Ako je D skup znamenaka koji je osnovni, tada tvrdnja (a) slijedi iz leme 5.4, a tvrdnja (b) slijedi iz kombinacije lema 5.5 i 5.6.

Sada pretpostavimo da uvjeti (a) i (b) vrijede. Želimo zaključiti da je D osnovni za k. Definirajmo $f(j) = (j - \overline{j})/k$, gdje je $\overline{j}$ jedinstveni element od D kongruentan s j modulo k. Definirajmo $f^0(j) = j$ i $f^s(j) = f(f^{s-1}(j))$ za $s \geq 1$. Očito, ako je $f^{s+1}(j) = 0$ za neki s, tada je

$$j = \overline{j} + \overline{f(j)}k + \cdots + \overline{f^s(j)}k^s.$$

Za $|j|$ dovoljno velik vrijedi $f(j) < j$. Stoga, ili postoji s takav da je $f^s(j) = 0$ ili postoje takvi $s \geq 0$ i $t \geq 1$ da je $f^s(j) = f^{s+t}(j) = a$ za neki $a \neq 0$. U prvom slučaju imamo prikaz za j koji je nužno jedinstven. U drugom slučaju imamo da je $f^t(a) = a$. Zato je

$$a = \overline{a} + \cdots + \overline{f^{t-1}(a)}k^{t-1} + ak^t$$

pa je

$$-a(k^t - 1) = \overline{a} + \cdots + \overline{f^{t-1}(a)}k^{t-1}.$$

Slijedi da je $-a(k^t - 1) \in D^t$, što je u kontradikciji s (b). □

Primjer 5.7. *Neka su k i ℓ prirodni brojevi. Brojevni sustav (k, ℓ) definiran je kao prikaz u bazi $k + \ell + 1$ koristeći skup znamenaka $\{-k, 1 - k, 2 - k, \ldots, -1, 0, 1, 2, \ldots, \ell - 1, \ell\}$. Primjerice, prije spomenuti uravnoteženi ternarni sustav je $(1, 1)$ brojevni sustav. Prema teoremu 5.2 su ovi brojevni sustavi savršeni.*

Poglavlje 6

Nestandardni prikazi

6.1 Prikaz brojeva u negativnoj bazi

Znamo da svaki broj veći od 1 može biti baza brojevnog sustava. Međutim, ono što nije baš tako poznato je to da se svi cijeli brojevi mogu prikazati u bazi s negativnim brojem. Prikaz brojeva u negativnoj bazi je pojednostavljen zbog toga što nema potrebe za posebnim znakom koji će biti pridružen svakom negativnom broju. Primjerice, broj $-326 = (-10)^3 + 7(-10)^2 + 3(-10) + 4$ pa je broj -326 prikazan kao 1734 u bazi -10. Svaki cijeli broj može se jedinstveno prikazati u negativnoj bazi. Zapravo, čak je taj prikaz "više jedinstven" nego u pozitivnoj bazi jer budući da nema predznaka, ne postoji problem da je $+0$ isto što i -0. Možemo zbrajati, oduzimati i množiti u negativnoj bazi iako možemo dobiti beskonačan niz znamenaka koje treba prenositi, no i taj problem se može savladati.

Kako bismo formalizirali negativne baze, kažemo da je N cijeli broj prikazan u bazi b ako je napisan u obliku $N = \sum_{k=0}^{m} a_k b^k$, gdje je $0 \leq a_k < |b|$. To označavamo s $N = [a_m a_{m-1} \cdots a_1 a_0]_b$. Ako je $b = 10$, izostavljamo zagrade i indeks b da dobijemo uobičajen dekadski prikaz. Bez obzira je li baza pozitivna ili negativna, znamenke a_k u prikazu se mogu izračunati na uobičajen način tako da je $q_0 = N$ i ponavljamo algoritam dijeljenja $q_k = q_{k+1} b + a_k$, gdje je $0 \leq a_k < |b|$, dok kvocijent ne postane 0. Na primjer, prikažimo broj 34 u brojevnom sustavu s bazom -2

$$\begin{aligned}
34 &= (-17)(-2) + 0 \\
-17 &= 9(-2) + 1 \\
9 &= (-4)(-2) + 1 \\
-4 &= 2(-2) + 0 \\
2 &= (-1)(-2) + 0 \\
-1 &= 1(-2) + 1 \\
1 &= 0(-2) + 1
\end{aligned}$$

i u brojevnom sustavu s bazom -10.

$$\begin{aligned} 34 &= (-3)(-10)+4 \\ -3 &= 1(-10)+7 \\ 1 &= 0(-10)+1 \end{aligned}$$

Stoga je $34 = [174]_{-10} = [1100110]_{-2}$. Možemo provjeriti naš račun.

$$[174]_{-10} = 1(-10)^2 + 7(-10) + 4 = 100 - 70 + 4 = 34,$$

$$[1100110]_{-2} = (-2)^6 + (-2)^5 + (-2)^2 + (-2) = 64 - 32 + 4 - 2 = 34.$$

Ako je baza negativan cijeli broj manji od -1, recimo $b = -s$, tada *svaki cijeli broj može biti na jedinstven način zapisan u bazi b.*

Budući da broj u negativnoj bazi nema znak za predznak, kako ćemo znati je li pozitivan ili negativan? Odgovor je jednostavan. Pozitivan je ako ima neparan broj znamenaka, a inače je negativan. Možemo znati koji je od dva broja veći uspoređujući znamenke uz najveću potenciju baze u kojima se razlikuju. Ako se počinju razlikovati u parnoj potenciji, tada je veći onaj broj s većom znamenkom. S druge strane, ako se počinju razlikovati u neparnoj potenciji baze, veći je onaj broj s manjom znamenkom. Primjerice, $[3326]_{-10} > [3354]_{-10}$ jer se počinju razlikovati u prvoj potenciji od -10. Primjenjujući to pravilo, vidimo da je $[3547]_{-10} > [3261]_{-10}$ i $[111]_{-2} > [1010]_{-2}$.

Možemo zbrajati, oduzimati i množiti brojeve u negativnoj bazi kao što to inače činimo. Međutim, prenošenje znamenaka je kompliciranije. Često se događa da se znamenke koje se pamte gomilaju i dobivamo beskonačne nizove znamenaka koje se pamte. No, iako ima beskonačno znamenaka koje se pamte, točan rezultat dobivamo u konačno mnogo koraka. Može se pokazati da ako zbrojimo dva broja s r ili manje znamenaka, tada suma sadrži najviše $r + 2$ znamenke, v. [5].

U ovom odjeljku ukratko ispitujemo prikaze svih cijelih brojeva u bazi $-k$. Prvo dokazujemo generalni rezultat o prikazima za prstene.

Neka je S komutativni prsten s jedinicom, neka je $k \in S$ i $U = (1, k, k^2, \ldots)$. Obično odredimo skup znamenaka D koji sadrži nulu i onda definiramo skup valjanih prikaza kao

$$R = \{\epsilon\} \cup (D \setminus \{0\})D^*.$$

Sada generaliziramo koncept potpunih sustava ostataka na komutativne prstenove. Kažemo da D čini *potpuni sustav ostataka* za S (modulo k) ako D zadovoljava sljedeća dva uvjeta.

(a) Za svaki $s \in S$ postoji $d \in D$ takav da je $s \equiv d \pmod{k}$.

(b) Ako su $d, d' \in D$ i $d \neq d'$, tada je $d \not\equiv d' \pmod{k}$.

Lema 6.1. *Neka je S prsten takav da je $D \subseteq S$ i $k \in S$. Neka je $\mathcal{N} = (U, D, R)$ brojevni sustav takav da je $U = (1, k, k^2, \ldots)$ i $R = \{\epsilon\} \cup (D \setminus \{0\})D^*$.*

(a) Ako je $\mathcal{N}$ potpun, tada D sadrži potpuni sustav ostataka za S (modulo k)

(b) Ako je D potpun sustav ostataka i $0 \in D$ te ako jednakost $kx = ky$ u skupu S povlači jednakost $x = y$ te ako je $\mathcal{N}$ potpun, tada je $\mathcal{N}$ jednoznačan.

Dokaz. (a) Kako je D potpun, svaki $s \in S$ ima prikaz

$$s = \sum_{0 \le i \le r} a_i k^i.$$

Tada skup svih mogućih vrijednosti za a_0 sadrži potpun sustav ostataka zato što je $s \equiv a_0 \pmod{k}$.

(b) Pretpostavimo da je D potpun sustav ostataka za S (modulo k). Neka su $s = \sum_{0 \le i \le r} a_i k^i$ i $s = \sum_{0 \le j \le r'} a'_j k^j$ dva različita prikaza za neki $s \in S$ s $a_i, a'_j \in D$ za $0 \le i \le r, 0 \le j \le r'$. Bez smanjenja općenitosti, možemo uzeti da je $r \le r'$ i da je r najmanji među svim elementima s dva različita prikaza. Tada je $s \equiv a_0 \pmod{k}$ i $s \equiv a'_0 \pmod{k}$ pa je $a_0 \equiv a'_0 \pmod{k}$ i stoga $a_0 = a'_0$. Sada promatramo $x = \sum_{1 \le i \le r} a_i k^{i-1}$ i $y = \sum_{i \le j \le r'} a'_j k^{j-1}$. Vidimo da je $kx = ky = s - a_0$, odnosno, zbog svojstva kraćenja, $x = y$. Ali tada x ima dva različita prikaza i jedan je kraći nego prije, što je kontradikcija.

□

Kao primjenu ove korisne leme dokazat ćemo sljedeći teorem.

Teorem 6.2. *Neka je $k \ge 2$ cijeli broj. Tada svaki cijeli broj N ima jedinstveni prikaz u bazi $-k$ oblika*

$$N = \sum_{0 \le i \le t} a_i(-k)^i,$$

gdje je $a_t \neq 0$ i $0 \le a_i < k$ za $0 \le i \le t$.

Dokaz. Prvo dokazujemo da svaki cijeli broj može biti prikazan u bazi $-k$ koristeći znamenke $\Sigma_k = \{0, 1, \ldots, k-1\}$. To činimo sljedećim algoritmom.

NegBaseRep (N, k)
$i := 0$
dok je $N \neq 0$ radi
  (1) $a_i := N \bmod k$
  (2) $N := (N - a_i)/(-k)$
  (3) $i := i + 1$

Lako je uočiti da ako algoritam završava, tada postoji r takav da je

$$N = \sum_{0 \le i \le r} a_i(-k)^i.$$

Preostaje vidjeti završava li algoritam NegBaseRep. To pokazujemo indukcijom po $|N|$. Lako je vidjeti da algoritam završava ako je $|N| \le 1$. Inače, u koraku (2) mijenjamo N s $N' = -(N - a_i)/k$. Sada ako $N \notin \{0, -1\}$, imamo $|N'| < |N|$ i dokaz je gotov. Da pokažemo jedinstvenost prikaza, primijenjujemo lemu 6.1. □

Ako je $N = \sum_{0 \le i \le r} a_i(-k)^i$ i $a_r \neq 0$, definiramo $(N)_{-k}$ kao niz $a_r a_{r-1} \cdots a_1 a_0$. Također, ako je $w = c_1 c_2 \cdots c_t$, pišemo $[w]_{-k}$ za cijeli broj $\Sigma_{1 \le i \le t} c_i(-k)^{t-i}$, kao što smo već rekli na početku ovog odjeljka.

6.2 Fibonaccijev prikaz

Sada krećemo ispitivati još jedan egzotični brojevni sustav, temeljen na Fibonaccijevim brojevima. Podsjetimo se da su Fibonaccijevi brojevi definirani s $F_0 = 0, F_1 = 1$ i $F_n = F_{n-1} + F_{n-2}$ za $n \ge 2$. Imamo sljedeći teorem.

Teorem 6.3. *Svaki cijeli broj $n \ge 0$ može biti jedinstveno prikazan kao*

$$n = \sum_{2 \le i \le r} a_i F_i$$

gdje je $a_i \in \Sigma_2 = \{0, 1\}, a_r \neq 0$ i $a_i a_{i+1} = 0$ za $2 \le i < r$.

Taj prikaz zove se *Fibonaccijev prikaz*.

Dokaz. Koristimo teorem 2.1 Pretpostavimo da je $a_i \in \{0, 1\}$. Dovoljno je pokazati da je $a_t F_t + a_{t-1} F_{t-1} + \cdots + a_2 F_2 < F_{t+1}$ za sve t ako i samo ako je $a_i a_{i+1} = 0$ za $2 \le i < r$.

Pretpostavimo da postoji index i takav da je $a_i a_{i+1} = 1$, odnosno $a_i = a_{i+1} = 1$. Tada je $a_{i+1} F_{i+1} + a_i F_i + \cdots a_2 F_2 \ge F_i + F_{i+1} = F_{i+2}$, što je kontradikcija za $t = i + 1$.

S druge strane, pretpostavimo da je $a_i a_{i+1} = 0$ za $2 \le i < r$. Tada se najveća moguća vrijednost od $a_t F_t + \cdots + a_2 F_2$ postiže kada je $a_t = 1, a_{t-1} = 0, a_{t-2} = 1, a_{t-3} = 0$ itd. No, lako je indukcijom dokazati da je $F_t + F_{t-2} + \cdots + F_2 = F_{t+1} - 1$ ako je t paran i da je $F_t + F_{t-2} + \cdots + F_3 = F_{t+1} - 1$ ako je t neparan broj. □

Iz ovog teorema proizlazi da postoji bijekcija između nenegativnih cijelih brojeva i prikaza oblika $\sum_{2 \le i \le r} a_i F_i$ s $a_i a_{i+1} = 0$ za $2 \le i < r$. Pišemo $(n)_F$ za $a_r a_{r-1} \cdots a_2$, Fibonaccijev prikaz od n i ako je $w = a_1 a_2 \cdots a_j \in \{0, 1\}^*$, pišemo $[w]_F = \sum_{1 \le i \le j} a_i F_{j-i+2}$. Skup svih valjanih Fibonaccijevih prikaza dan je regularnim izrazom

$$\epsilon + 1(0 + 01)^*.$$

6.3 Ostrovskijev α-brojevni sustav

Ostrovskijev brojevni sustav je dobio ime po ukrajinskom matematičaru Alexandru Ostrovskom. Postoje dva srodna brojevna sustava bazirana na verižnim razlomcima, jedan je nestandardni pozicijski brojevni sustav za prikaz cijelih brojeva, a drugi prikaz realnih brojeva gdje bazni niz sadrži necijele brojeve. Mi ćemo se ovdje baviti samo prvim brojevnim sustavom.

Podsjetimo se osnovnih definicija vezanih uz verižne razlomke, detalji i daljnji razvoj teorije mogu se naći npr. u [4]. Ostrovskijev α-brojevni sustav može se promatrati kao generalizacija Fibonaccijevog brojevnog sustava proučavanog u prošlom odjeljku.

Svaki iracionalan broj α može biti prikazan na jedinstven način kao beskonačni verižni razlomak

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}} = [a_0, a_1, a_2, \ldots]$$

gdje je a_0 cijeli broj, a a_i su prirodni brojevi za $i \geq 1$. Prethodna tvrdnja zapravo znači da je

$$\alpha = \lim_{n\to\infty} p_n/q_n,$$

tj. limes niza konvergenti

$$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}.$$

Konvergente p_n/q_n su očito racionalni brojevi čije brojnike i nazivnike možemo računati pomoću sljedećih rekurzija

$$p_{-2} = 0,\ p_{-1} = 1,\ p_n = a_n p_{n-1} + p_{n-2}$$
$$q_{-2} = 1,\ q_{-1} = 0,\ q_n = a_n q_{n-1} + q_{n-2}$$

za $n \geq 0$. Niz $(q_n)_{n\geq 0}$ nazivnika konvergenti čini bazu brojevnog sustava utemeljenog na α.

Teorem 6.4. *Neka je α iracionalan realni broj i neka je $(q_n)_{n\geq 0}$ niz nazivnika konvergenti verižnog razlomka od α. Tada svaki nenegativan broj N može biti prikazan na jedinstven način u obliku*

$$N = \sum_{0\leq i\leq j} b_i q_i,$$

gdje su b_i cijeli brojevi koji zadovoljavaju sljedeća tri uvjeta.

1. $0 \le b_0 < a_1$.

2. $0 \le b_i \le a_{i+1}$ *za* $i \ge 1$.

3. *Za* $i \ge 1$, *ako je* $b_i = a_{i+1}$, *tada je* $b_{i-1} = 0$.

Dokaz. Koristimo teorem 2.1. Dovoljno je pokazati da je nejednakost

$$b_0q_0 + b_1q_1 + \cdots + b_iq_i < q_{i+1} \tag{6.1}$$

ekvivalentna trima iskazanim uvjetima.

Pretpostavimo da nejednakost (6.1) vrijedi. Tada, kako je $q_0 = 1$ i $q_1 = a_1$, vidimo da nejednakost $b_0q_0 < q_1$ povlači uvjet 1.

Sada dokazujemo uvjet 2. Nejednakost (6.1) povlači $b_iq_i < q_{i+1} = a_{i+1}q_i + q_{i-1}$. Dijeljenjem s q_i, dobivamo $b_i < a_{i+1} + q_{i-1}/q_i$. Kako je $q_{i-1} \le q_i$, dobivamo $b_i \le a_{i+1}$.

Kako bismo dokazali uvjet 3, uočimo da ako je $b_i = a_{i+1}$ i $b_{i-1} \ge 1$, tada je

$$b_0q_0 + \cdots + b_{i-1}q_{i-1} + b_iq_i \ge a_{i+1}q_i + q_{i-1} = q_{i+1},$$

što je u kontradikciji s nejednakošću (6.1).

Preostaje pokazati da iz uvjeta (1)-(3) slijedi nejednakost (6.1). To dokazujemo indukcijom po i. Za $i = 0$ znamo iz uvjeta (1) da je $b_0 < a_1$ pa je $b_0q_0 < q_1$. Za $i = 1$ znamo po uvjetima (2) i (3) da je $b_1 \le a_2$ i $b_0 = 0$ ako je $b_1 = a_2$, stoga je $b_0q_0 + b_1q_1 = b_0 + b_1a_1 \le a_1a_2 < a_1a_2 + 1 = q_2$.

Pretpostavimo da tvrdnja vrijedi za sve $i < r$. Dokazujemo ju za $i = r$. Znamo da je $b_r \le a_{r+1}$ iz uvjeta (2). Ako je $b_r \le a_{r+1} - 1$, tada je $b_rq_r \le (a_{r+1} - 1)q_r \le q_{r+1} - q_r$. Zajedno s pretpostavkom indukcije da je $b_0q_0 + \cdots + b_{r-1}q_{r-1} < q_r$, dobivamo $b_0q_0 + \cdots + b_rq_r < q_{r+1}$.

S druge strane, ako je $b_r = a_{r+1}$, tada iz uvjeta (3) znamo da je $b_{r-1} = 0$. Slijedi da je $b_{r-1}q_{r-1} + b_rq_r = a_{r+1}q_r = q_{r+1} - q_{r-1}$, a zajedno s pretpostavkom $b_0q_0 + \cdots + b_{r-2}q_{r-2} < q_{r-1}$ to daje nejednakost $b_0q_0 + \cdots + b_rq_r < q_{r+1}$ kako smo i željeli. Primijetimo da za $\alpha = \frac{1+\sqrt{5}}{2} = [1, 1, 1, \ldots]$ Ostrovskijev brojevni sustav postaje upravo Fibonaccijev sustav iz prethodnog odjeljka. □

6.4 Prikazi u kompleksnim bazama

U ovom poglavlju promatramo Gaussove cijele brojeve

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

gdje je $i = \sqrt{-1}$. Ograničit ćemo se na bazne skupove čiji su elementi potencije jednog Gaussovog cijelog broja θ. Kao i u prethodnim poglavljima, tražimo prikaze koji su prirodni i koji prikazuju svaki cijeli broj točno jednom.

U svrhu dobivanja potpunog brojevnog sustava, trebamo skup znamenaka koji je potpun sustav ostataka. Za $\theta = d + ei$, definiramo *normu* $N(\theta) = d^2 + e^2 = \theta \cdot \overline{\theta}$.

Lema 6.5. *Neka su d i e cijeli brojevi takvi da je* $\mathrm{NZD}(d, e) = 1$. *Definirajmo $\theta = d + ei$. Neka je $\overline{d}$ takav cijeli broj da je* $d\overline{d} \equiv 1 \pmod{N(\theta)}$. *Tada za sve cijele brojeve a i b postoji jedinstveni cijeli broj c,* $0 \leq c < N(\theta)$, *takav da je* $a + bi \equiv c \pmod{d + ei}$. *Štoviše, možemo uzeti da je* $c = (a + be\overline{d}) \pmod{N(\theta)}$.

Dokaz. Lako je provjeriti da za sve $c \in \mathbb{Z}$ imamo

$$(a + bi - c)(d - ei) = (a - c)d + be + (bd + (c - a)e)i.$$

Slijedi da je

$$a + bi - c = (f + gi)(d + ei),$$

gdje je

$$f = \frac{(a - c)d + be}{d^2 + e^2}$$

i

$$g = \frac{bd + (c - a)e}{d^2 + e^2}.$$

Sada neka je $c \equiv a + be\overline{d} \pmod{d^2 + e^2}$. Za ovaj izbor c, jasno da je $f \in \mathbb{Z}$. Da utvrdimo kako je $g \in \mathbb{Z}$, uočimo da je

$$\begin{aligned} bd + (c - a)e &\equiv bd + be^2\overline{d} \pmod{d^2 + e^2} \\ &\equiv b\overline{d}(d^2 + e^2) \pmod{d^2 + e^2} \\ &\equiv 0 \pmod{d^2 + e^2}. \end{aligned}$$

Stoga je $a + bi \equiv c(\mathrm{mod} + ei)$.

Kako bismo vidjeli da je c jedinstven, pretpostavimo da za dva različita cijela broja c i c' takva da je $0 \leq c, c' < N(\theta)$ vrijedi $c \equiv c' (\mathrm{mod}\ d + ei)$. Tada, ako je $h = c - c'$, vrijedi da je $h \equiv 0 (\mathrm{mod}\ d + ei)$ i štoviše

$$1 \leq h < N(\theta). \tag{6.2}$$

Dakle, postoje cijeli brojevi r i s takvi da je $h = (r + si)(d + ei) = rd - es + (ds + er)i$. Kako je h cijeli broj, slijedi da je $ds + er = 0$. Budući da je $\mathrm{NZD}(d, e) = 1$, postoji cijeli broj k takav da je $s = -ek$ i $r = dk$. Stoga je $h = rd - es = (d^2 + e^2)k = N(\theta)k$, ali to je u kontradikciji s nejednakošću (6.2). □

Primjer 6.6. *Nađimo cijeli broj c takav da je $17 + 23i \equiv c \pmod{\theta}$, gdje je $\theta = 31 + 45i$. U ovom slučaju imamo $a = 17, b = 23, d = 31, e = 45$ i $N(\theta) = 2986$. Tada je $\overline{d} = 289$. Možemo uzeti da je $c = (a + be\overline{d}) \mod N(\theta) = 532$. Doista, imamo $a + bi - c = (-5 + 8i)(d + ei)$.*

Lema 6.7. *Neka su d i e takvi cijeli brojevi da je $\mathrm{NZD}(d, e) = \lambda > 0$. Za cijele brojeve a i b postoji jedinstveni par cijelih brojeva (x, y) sa svojstvom $0 \le x < (d^2 + e^2)/\lambda$ i $0 \le y < \lambda$ takav da je $a + bi \equiv x + yi \pmod{d + ei}$.*

Dokaz. Neka su A i B cijeli brojevi, $0 \le A, B < \lambda$ takvi da je $A \equiv a \pmod{\lambda}$ i $B \equiv b \pmod{\lambda}$. Prema lemi 6.5 postoji jedinstveni broj c takav da je $0 \le c < N(\theta)/\lambda^2$ i da je

$$\frac{a - A}{\lambda} + \frac{b - B}{\lambda} i \equiv c \pmod{\frac{d + ei}{\lambda}} \tag{6.3}$$

Množenjem s λ, dobivamo

$$a - A + (b - B)i \equiv \lambda c \pmod{d + ei}.$$

Slijedi da je

$$a + bi \equiv \lambda c + A + Bi \pmod{d + ei}$$

pa možemo uzeti da je $x = \lambda c + A$ i $y = B$. Kako je $0 \le c \le N(\theta)/\lambda^2 - 1$, slijedi da je $0 \le x < N(\theta)/\lambda$.

Za dokazivanje jedinstvenosti, pretpostavimo da su cijeli brojevi x, x', y, y', $0 \le x, x' < N(\theta)/\lambda, 0 \le y, y' < \lambda$ i $(x, y) \ne (x', y')$ takvi da je

$$x + yi \equiv x' + y'i \pmod{d + ei}.$$

Ako stavimo $m = x - x'$ i $n = y - y'$, tada postoje cijeli brojevi r i s takvi da je $m + ni = (d + ei)(r + si)$. Slijedi da je $m = dr - es$ i $n = ds + er$ te $0 \le |m| < N(\theta)/\lambda$, $0 \le |n| < \lambda$. Kako je $\lambda = \mathrm{NZD}(d, e)$, to $\lambda \mid n$ pa slijedi da je $n = 0$. Stoga je $ds = -er$ i postoji cijeli broj k takav da je $r = kd/\lambda$ i $s = -ke/\lambda$. Stoga je $m = k(d^2 + e^2)/\lambda$ i zato $k = 0$. No, to znači da je $x = x'$ i $y = y'$, što je kontradikcija. □

Time smo dokazali sljedeći rezultat.

Teorem 6.8. *Neka su d i e cijeli brojevi takvi da je $\mathrm{NZD}(d, e) = \lambda > 0$ i definirajmo $\theta = d + ei$. Tada skup*

$$\left\{x + yi : 0 \le x < \frac{N(\theta)}{\lambda},\ 0 \le y < \lambda\right\}$$

čini potpun sustav ostataka (modulo θ).

Neka je $U = (1, \theta, \theta^2, \dots)$ i $D = \{0, 1, \dots, N(\theta - 1)\}$. Sada istražujemo sljedeće prirodno pitanje. Za koje Gaussove cijele brojeve θ je brojevni sustav $(U, D, \{\epsilon\} \cup (D \setminus \{0\})D^*)$ savršen?

Teorem 6.9. *Neka je $\theta \in \mathbb{Z}[i]$. Brojevni sustav $\mathcal{N} = (U, D, \{\epsilon\} \cup (D \setminus \{0\})D^*)$, gdje je $U = \{1, \theta, \theta^2, \dots\}$ i $D = \{0, 1, \dots, N(\theta) - 1\}$, je savršen ako i samo ako je $\theta = -A \pm i$ za neki cijeli broj $A \geq 1$.*

Dokaz. Najprije pokazujemo da ako θ nije oblika $-A \pm i$, tada se neki element iz $\mathbb{Z}[i]$ ne može prikazati.

Neka je $\theta = a + bi$. Pretpostavimo da je $a \geq 1$. Tada dokazujemo da broj $\alpha := (1 - a) + bi$ nije prikaziv u $\mathcal{N}$. Pretpostavimo da jest. Tada bismo imali

$$\alpha = c_0 + c_1\theta + c_2\theta^2 + \cdots + c_k\theta^k.$$

Definirajmo $\rho := \alpha(1 - \theta) = a^2 + b^2 - 2a + 1$. Sada imamo

$$\rho = c_0 + (c_1 - c_0)\theta + \cdots + (c_k - c_{k-1})\theta^k - c_k\theta^{k+1}. \tag{6.4}$$

Slijedi da je $\rho \equiv c_0 \pmod{\theta}$. Kako je $0 \leq \rho < N(\theta)$, slijedi da je $\rho = c_0$. Sada iz jednakosti (6.4) dobivamo

$$(c_1 - c_0)\theta + \cdots + (c_k - c_{k-1})\theta^k - c_k\theta^{k+1} = 0.$$

Dijeljenjem s θ, dobivamo

$$(c_1 - c_0) + (c_2 - c_1)\theta + \cdots + (c_k - c_{k-1})\theta^{k-1} - c_k\theta^k = 0.$$

Uzimajući obje strane modulo θ, vidimo da je $c_1 \equiv c_0 \pmod{\theta}$. Stoga je $c_1 = c_0$. Slično tomu, $c_2 = c_1, \dots, c_k = c_{k-1}$ i na kraju je $c_k = 0$. Dakle, $c_0 = c_1 = c_2 = \cdots = c_k = 0$ i $\rho = 0$. Slijedi da je $\theta = 1$, što očito nije baza savršenog brojevnog sustava.

Sljedeće pokazujemo da je $b = \pm 1$. Iz binomnog teorema lako vidimo da je b djelitelj od $\operatorname{Im} \theta^j = \operatorname{Im} (a + bi)^j$ za svaki $j \geq 0$. Slijedi da ako je

$$\alpha = c_0 + c_1\theta + \cdots + c_k\theta^k,$$

tada je

$$\operatorname{Im} \alpha = c_1 \operatorname{Im} \theta + \cdots + c_k \operatorname{Im} \theta^k.$$

Dakle, $b \mid \operatorname{Im} \alpha$. Kako je α proizvoljan, moramo imati $b = \pm 1$.

Za preostalu mogućnost $\theta = \pm i$ lako je vidjeti da ne može biti baza savršenog brojevnog sustava.

Sada ostaje pokazati da ako je $\theta = -A \pm i$, tada je brojevni sustav $\mathcal{N}$ savršen. Koristeći lemu 6.7 i teorem 6.8, dovoljno je pokazati da svaki Gaussov cijeli broj ima barem jedan prikaz. Prvo promatramo slučaj gdje je $\theta = -A + i$.

Ideja dokaza je da prvo pokažemo kako izraziti bilo koji $\alpha \in \mathbb{Z}[i]$ u obliku $\sum_{0\leq i\leq r} c_i\theta^i$ gdje su c_i nenegativni cijeli brojevi koji nisu nužno manji od $N(\theta)$. Takav prikaz zovemo *nenormaliziranim*. Dalje, pokazujemo kako pretvoriti taj prikaz u normalizirani gdje znamenke c_i zadovoljavaju uvjet $0 \leq c_i < N(\theta)$ nizom koraka zvanim *algoritam sređivanja*.

Počinjemo dobivanjem nenormaliziranog prikaza. Neka je $\alpha = e + fi$ te neka je $c = e + Af$. Tada jednostavan račun pokazuje da je $c + f\theta = e + fi = \alpha$. Sada je lako vidjeti da je $\theta^2 + 2A\theta + A^2 = -1$ pa ako je $c < 0$, možemo zamijeniti c s $(-c)(\theta^2 + 2A\theta + A^2)$. Slično, ako je $f < 0$, možemo zamijeniti f sa $(-f)(\theta^2 + 2A\theta + A^2)$. Dakle, dobivamo prikaz

$$\alpha = d_0 + d_1\theta + d_2\theta^2 + d_3\theta^3$$

gdje su d_0, d_1, d_2 i d_3 nenegativni cijeli brojevi.

Ovaj prikaz možda nije normaliziran pa sada pokazujemo kako ga normalizirati nizom koraka. Svaki korak će održati svojstvo da su sve znamenke nenegativne, a neće povećavati zbroj znamenaka. Općenitije, razmotrimo prikaz

$$\alpha = d_0 + d_1\theta + \cdots + d_k\theta^k \tag{6.5}$$

gdje je $k \geq 3$ i $d_i \geq 0$ za $0 \leq i \leq k$. Definirajmo $t_0 = \sum_{0\leq j\leq k} d_j$. Tada je t_0 nenegativan cijeli broj i $t_0 = 0$ ako i samo ako je $\alpha = 0$. Prema teoremu o dijeljenju s ostatkom

$$d_0 = q(A^2 + 1) + u_0, \tag{6.6}$$

gdje je $0 \leq u_0 \leq A^2$ i $q \geq 0$. Jednostavnim računom dobivamo da je

$$A^2 + 1 = (A-1)^2\theta + (2A-1)\theta^2 + \theta^3. \tag{6.7}$$

Sada ubacimo jednakost (6.7) u jednakost (6.6) i dobijemo

$$d_0 = u_0 + q((A-1)^2\theta + (2A-1)\theta^2 + \theta^3). \tag{6.8}$$

Dobiveni izraz uvrstimo u jednakost (6.5) da dobijemo

$$\begin{aligned}\alpha &= u_0 + (d_1 + q(A-1)^2)\theta + (d_2 + q(2A-1))\theta^2 \\ &\quad + (d_3 + q)\theta^3 + d_4\theta^4 + \cdots + d_k\theta^k \\ &= d'_0 + d'_1\theta + \cdots + d'_k\theta^k.\end{aligned}$$

Ako stavimo da je $t'_0 = \sum_{0\leq j\leq k} d'_j$, tada je

$$\begin{aligned}t'_0 - t_0 &= u_0 - d_0 + q(A-1)^2 + q(2A-1) + q \\ &= q(-(A^2+1) + (A-1)^2 + (2A-1) + 1) \\ &= 0\end{aligned}$$

pa je $t'_0 = t_0$. Neka je $\alpha = d'_0 + \theta\alpha_1$. Vidimo da je

$$\alpha_1 = d'_1 + d'_2\theta + \cdots + d'_k\theta^{k-1}.$$

Ako definiramo $t_1 = d'_1 + d'_2 + \cdots + d'_k$, tada je očito $t_1 \leq t'_0 = t_0$ pri čemu jednakost vrijedi ako i samo ako je $u_0 = 0$. Sada nastavimo taj postupak. Tako dobivamo

$$\alpha = \alpha_1\theta + u_0, \quad \alpha_1 = \alpha_2\theta + u_1, \ldots$$

i odgovarajuće sume znamenaka $t_0, t_1, t_2, \ldots$ Kako navedeni niz nije ni rastući ni negativan, uočavamo da je $t_q = t_{q+1} = t_{q+2} = \cdots$ za neki $q \geq 0$. Slijedi da je $0 = u_q = u_{q+1} = u_{q+2} = \cdots$. Stoga je $\alpha_q = \alpha_{q+1}\theta, \alpha_{q+1} = \alpha_{q+2}\theta, \ldots$, iz čega slijedi da $\theta^k \mid \alpha_q$ za sve $k \geq 0$. Dakle, $\alpha_q = 0$. Time dobivamo normalizirani prikaz

$$\alpha = u_0 + u_1\theta + \cdots + u_{q-1}\theta^q,$$

što dovršava dokaz za $-A + i$.

Kako bismo riješili slučaj prikaza u bazi $(-A - i)$, jednostavno zapišimo kompleksni konjugat $\overline{\alpha}$ u bazi $(-A + i)$ kao prije. S $\theta = -A + i$ dobivamo da je

$$\overline{\alpha} = u_0 + u_1\theta + \cdots + u_{q-1}\theta^q.$$

Sada kompleksno konjugiramo obje strane da dobijemo prikaz od α u bazi $-A - i$. $\square$

Bibliografija

[1] J.-P. Allouche, J. Shallit, *Automatic sequences*, Cambridge 2003.

[2] F. M. Bruckler, *Povijest matematike*, diplomski kolegij 2017/2018., dostupno na `http://prelog.chem.pmf.hr/ fmbruckler/PovMat/povijest.html`, 2018.

[3] L. Corry, *A Brief History of Numbers*, Oxford 2015.

[4] A. Dujella, *Diofantske jednadžbe*, poslijediplomski kolegij 2006/2007., dostupno na `https://web.math.pmf.unizg.hr/~duje/dioph/dioph.pdf` (travanj 2018.)

[5] W. J. Gilbert, R. J. Green *Negative Based Number Systems*, Mathematics Magazine, Vol. 52, No. 4, (1979.) 240–244.

[6] R. A. Horn, C. R. Johnson, *Matrix Analysis*, Cambridge 2013.

Sažetak

Prvi brojevni sustavi razvili su se oko 3500. g. pr. Kr. kada su i prvi puta uvedene brojke. Stare civilizacije koristile su brojevne sustave s bazama $10, 12, 20$ i 60. Nas u ovom radu zanimaju općeniti brojevni sustavi s bazom koja je proizvoljan prirodni broj veći od 1. Za njih proučavamo funkciju sume znamenaka definiranu na prirodnim brojevima te općenitije brojanje blokova znamenki. U drugom dijelu rada promatramo prikaz u bazi k s drugim skupom znamenki te neke nestandardne prikaze poput Fibonaccijevog, Ostrovskijevog ili prikaza u negativnoj ili kompleksnoj bazi.

Summary

The first numeration systems evolved around 3500 BC. when the numbers were introduced for the first time. Old civilizations used numeration systems with bases 10, 12, 20, and 60. In this work, we are interested in general numeration systems with a base that is an arbitrary positive integer greater than one. We study the sum of digits function defined on positive integers and, more generally, functions counting blocks of digits. In the second part of this work, we examine representations in base k with alternative set of digits and some non-standard representations such as Fibonacci's, Ostrowsky's and also representations in negative or complex bases.

Životopis

Rođen sam 10. siječnja 1992. godine.

Osnovnu školu sam završio u Barbanu 2006. godine kada sam i upisao opću gimnaziju u Puli koju sam završio 2010. godine. Te godine upisao sam Prirodoslovno - matematički fakultet, matematički odsjek, nastavnički smjer te sam 2014. godine završio preddiplomski studij. Godine 2014. upisao sam diplomski studij matematike, nastavnički smjer.

Od 2015. godine sam radio u OŠ Ivana Gundulića gdje sam ostao do 2017. godine. Te godine sam dobio i certifikat za uspješno pohađanje tečaja "Teaching Math, Science And Art Outdoors" koji se održao u Švedskoj u svibnju u sklopu Erasmus+ KA1 projekta. Školske godine 2017/2018. radio sam u OŠ Don Lovre Katića i u OŠ Vjekoslava Paraća u Solinu.