Homogene linearne rekurzije

Karlović, Luka

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Luka Karlović

HOMOGENE LINEARNE REKURZIJE

Diplomski rad

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

Zagreb, 2022.

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. _____

Ocu Antunu i majci Senki koji su neprestano bili uz mene i podupirali me financijski i moralno. Djevojci Teni, svim prijateljima i prijateljicama s kojima dijelim mnogo lijepih iskustava, događaja i doživljaja, a koji su bili uz mene i kroz manje lijepe periode. Svima koji su me poticali da ostvarim sve svoje velike i male ciljeve te nisu nikada posumnjali u mene, čak i kada ja jesam. Učiteljima, nastavnicima i profesorima koji su me poučili mnogim stvarima, a posebno izv. prof. dr. sc. Zrinki Franušić koja me vodila kroz mnogo kolegija i ovaj diplomski rad.

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

Sadržaj

Uvod

Nizove u kojima se članovi određuju pomoću svojih prethodnika zovemo rekurzivnim. U prvom poglavlju rada definirani su nizovi zadani linearnom homogenom rekurzijom s konstantinim koeficijentima te je pokazano da skup svih takvih kompleksnih nizova čini kompleksni vektorski prostor. Nadalje, zanima nas kako odrediti opći član rekurzivno zadanog niza, to jest kako riješiti rekurziju. Opisujemo dvije metode za rješavanje rekurzije. Jedna metoda koristi alate iz linearne algebre kao što su račun svojstvenih vrijednosti i svojstvenih vektora matrice, a druga se zasniva na rješavanju karakteristične jednadžbe rekurzije. Metode su potkrijepljene rješavanjem primjera linearnih homogenih rekurzija reda 2 i reda 3.

Drugo poglavlje rada posvećeno je modularnim rekurzijama, odnosno linearnim homogenim rekurzijama s konstantnim cjelobrojnim koeficijentima i cjelobrojnim početnim uvjetima modulo neki fiksni prirodni broj. Modularne rekurzije su periodične pa je stoga najprije proučena periodičnost nizova dobivenih iteracijama, odnosno kompozicijama zadane funkcije. Detaljnije su obrađene modularne rekurzije prvog i drugog reda.

Poglavlje 1

Linearne homogene rekurzivne relacije

Niz brojeva je funkcija čija je domena skup prirodnih brojeva $\mathbb{N}$ (ili $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$), a kodomena neki skup brojeva. Niz $a : \mathbb{N} \to S$ kraće označavamo s (a_n), pri čemu je $a_n = a(n)$, $n \in \mathbb{N}$, tzv. **opći** ili n-**član niza**. U ovisnosti o kodomeni, koja je najčešće $\mathbb{Z}$, $\mathbb{R}$ ili $\mathbb{C}$, govorimo o *nizu cijelih brojeva*, *nizu realnih brojeva* ili *nizu kompleksnih brojeva*. Jedan od načina zadavanja niza jest pomoću *rekurzivnih formula* u kojem se članovi niza određuju pomoću svojih prethodnika. Takve nizove nazivamo **rekurzivnim nizovima**. Primjer rekurzivno zadanog niza je poznati **Fibonaccijev niz** (ili **niz Fibonaccijevih brojeva**) (F_n) kojemu je svaki član, izuzevši prva dva, jednak zbroju prethodna dva člana niza. Konkretno,

$$F_1 = 1,\ F_2 = 1,$$

su *početne vrijednosti* niza, a svaki sljedeći član niza definira se *rekurzivnom relacijom*

$$F_n = F_{n-1} + F_{n-2},\ n \geq 3,$$

pa dobivamo

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, \ldots$$

Rekurzivna relacija kojom je zadan Fibonaccijev niz spada u tzv. **linearne homogene rekurzivne relacije** ili kraće **linearne homogene rekurzije**.

U ovom poglavlju bavit ćemo se problemom eksplicitnog određivanja općeg člana rekurzivnog niza, odnosno tzv. **rješavanjem rekurzije**. Jedna od metoda za rješavanje rekurzije koristi matričnu reprezentaciju rekurzivnog niza, a druga uključuje karakterističnu jednadžbu. Obje metode potkrijepit ćemo i odgovarajućim primjerima.

1.1 Definicija niza zadanog linearnom homogenom rekurzijom

Definicija 1.1.1. *Neka je* $k \in \mathbb{N}$, $a_0, a_1, a_2, \ldots, a_{k-1} \in \mathbb{C}$ *te* $c_1, c_2, \ldots, c_k \in \mathbb{C}$, $c_k \neq 0$. *Kažemo da je niz* (a_n) ***zadan linearnom homogenom rekurzijom reda*** k ***s konstantnim koeficijentima*** *ako je*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}, \tag{1.1}$$

za sve $n \geq k$. *Prvih* k *članova niza* (a_n) *nazivaju se* ***početni uvjeti****.*

Prema prethodnoj definiciji Fibonaccijev niz zadovoljava linearnu homogenu rekurziju reda 2 s koeficijentima $c_1 = c_2 = 1$ uz početne uvjete $F_1 = F_2 = 1$ (ili $F_0 = 0$, $F_1 = 1$). U radu ćemo se baviti samo rekurzijama s konstantim koeficijentima.

Naziv *linearne* rekurzije proizlazi iz činjenice da su nizovi zadani relacijom (1.1) zatvoren na zbrajanje nizova i množenje nizova skalarom što ćemo pokazati u sljedećoj tvrdnji.

Propozicija 1.1.2. *Neka je* $\mathcal{LH}$ *skup svih kompleksnih nizova zadanih linearnom homogenom rekurzijom reda* k *s konstantnim koeficijentima* (1.1)*. Tada je* $\mathcal{LH}$ *kompleksan vektorski prostor.*

Dokaz. Prostor svih kompleksnih nizova, u oznaci $\mathbb{C}^{\mathbb{N}}$, čini kompleksan vektorski prostor uz operacije zbrajanje nizova i množenje nizova skalarom koje se definiraju po elementima niza (odnosno po točkama jer je niz po definiciji funkcija s domenom $\mathbb{N}$ ili $\mathbb{N}_0$). Stoga ćemo pokazati da je skup

$$\mathcal{LH} = \{(a_n) \in \mathbb{C}^{\mathbb{N}} : a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},\ n \geq k\}.$$

potprostor od $\mathbb{C}^{\mathbb{N}}$.

Neka su $(a'_n), (a''_n) \in \mathcal{LH}$ te $\lambda, \mu \in \mathbb{C}$. Tada za sve $n \geq k$ vrijedi

$$a'_n = c_1 a'_{n-1} + c_2 a'_{n-2} + \cdots + c_k a'_{n-k}, \tag{1.2}$$

$$a''_n = c_1 a''_{n-1} + c_2 a''_{n-2} + \cdots + c_k a''_{n-k}. \tag{1.3}$$

Množenjem (1.2) s $\lambda \in \mathbb{C}$ te (1.3) s $\mu \in \mathbb{C}$ dobivamo

$$\lambda a'_n = \lambda c_1 a'_{n-1} + \lambda c_2 a'_{n-2} + \cdots + \lambda c_k a'_{n-k}, \tag{1.4}$$

$$\mu a''_n = \mu c_1 a''_{n-1} + \mu c_2 a''_{n-2} + \cdots + \mu c_k a''_{n-k}. \tag{1.5}$$

Zbrajanjem (1.4) i (1.5) te izlučivanjem konstanti $c_1, c_2, \ldots, c_k$ dobivamo

$$\lambda a'_n + \mu a''_n = c_1 \left(\lambda a'_{n-1} + \mu a''_{n-1}\right) + c_2 \left(\lambda a'_{n-2} + \mu a''_{n-2}\right) + \cdots + c_k \left(\lambda a'_{n-k} + \mu a''_{n-k}\right). \tag{1.6}$$

Iz (1.6) slijedi da i linearna kombinacija nizova (a'_n) i (a''_n), tj. da niz

$$\lambda(a'_n) + \mu(a''_n) = (\lambda a'_n + \mu a''_n)$$

zadovoljava relaciju (1.1) uz početne uvjete

$$\lambda a'_0 + \mu a'_0, \ldots, \lambda a'_{k-1} + \mu a'_{k-1}.$$

Dakle, $\mathcal{LH}$ je zatvoren na zbrajanje nizova i množenje nizova skalarom pa je $\mathcal{LH}$ potprostor od $\mathbb{C}^{\mathbb{N}}$. □

Jasno je da je skup svih realnih nizova zadan istom linearnom homogenom rekurzijom s konstantnim koeficijentima realan vektorski prostor, tj. potprostor od $\mathbb{R}^{\mathbb{N}}$.

1.2 Matrični prikaz niza zadanog linearnom homogenom rekurzijom

Pretpostavimo da je niz (a_n) zadan početnim uvjetima

$$a_0, a_1, \ldots, a_{k-1},$$

te relacijom (1.1) za sve $n \geq k$. S obzirom da je svaki član rekurzije k-tog reda određen s k neposredno prethodećih članova, možemo promatrati funkciju koja djeluje na uređene k-torke uzastopnih članova:

$$\begin{array}{c}
(a_{k-1}, a_{k-2}, \ldots, a_0) \\
\downarrow \\
(\underbrace{c_1 a_{k-1} + c_2 a_k + \cdots + c_k a_0}_{=a_k}, a_{k-1}, \ldots, a_1) \\
\downarrow \\
(\underbrace{c_1 a_k + c_2 a_{k-1} + \cdots + c_k a_1}_{=a_{k+1}}, a_k, \ldots, a_2) \\
\downarrow \\
\vdots \\
\downarrow \\
(\underbrace{c_1 a_{n+k-2} + c_2 a_{n+k-3} + \cdots + c_k a_{n-1}}_{=a_{n+k-1}}, a_{n+k-2}, \ldots, a_n) \\
\downarrow \\
(\underbrace{c_1 a_{n+k-1} + c_2 a_{n+k-2} + \cdots + c_k a_n}_{=a_{n+k}}, a_{n+k-1}, \ldots, a_{n+1}) \\
\downarrow \\
\vdots
\end{array} \tag{1.7}$$

Na taj način definirana je funkcija $f : \mathbb{C}^k \to \mathbb{C}^k$,

$$f(x_1, x_2, \ldots, x_k) = (c_1x_1 + c_2x_2 + \cdots + c_kx_k, x_1, \ldots, x_{k-1}), \tag{1.8}$$

štoviše linearan operator $\mathbb{C}^k \to \mathbb{C}^k$. Njegov matrični zapis u kanonskoj bazi prostora $\mathbb{C}^k$, $(e) = ((1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1))$, je kvadratna matrica reda k:

$$B = \begin{pmatrix} c_1 & c_2 & \ldots & c_{k-1} & c_k \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}. \tag{1.9}$$

Ako uzastopne k-torke niza (a_n) „smjestimo" u jednostupčanu matricu

$$A_n = \begin{pmatrix} a_{n+k-1} \\ a_{n+k-2} \\ \vdots \\ a_{n+1} \\ a_n \end{pmatrix}, \tag{1.10}$$

za sve $n \geq 0$, relacije iz (1.7) možemo zapisati kao

$$\begin{array}{c} A_0 \\ \downarrow \\ BA_0 = A_1 \\ \downarrow \\ BA_1 = A_2 \\ \downarrow \\ \vdots \\ \downarrow \\ BA_{n-1} = A_n \\ \downarrow \\ BA_n = A_{n+1} \\ \downarrow \\ \vdots \end{array}$$

Stoga, možemo zaključiti da za sve $n \in \mathbb{N}$ vrijedi:

$$A_n = BA_{n-1} = B(BA_{n-2}) = B^2A_{n-2} = B^2(BA_{n-3}) = B^3A_{n-3} = \cdots = B^nA_0.$$

Zbog toga ćemo matricu B danu s (1.9) zvati **matrica pridružena rekurziji** (1.1) ili samo **matrica rekurzije**.

Zahvaljući dobivenoj relaciji $A_n = B^n A_0$ možemo eksplicitno odrediti n-ti član rekurzivnog niza (a_n), odnosno *riješiti rekurziju*. Za to nam je potrebno izračunati n-tu potenciju kvadratne matrice B, što nije jednostavno osim u slučaju nekih specijalnih oblika matrice. Npr. ako je matrica A dijagonalna, tj. $A = \text{diag}(\alpha_1, \ldots, \alpha_k)$, n-ta potencija matrice A je $A^n = \text{diag}(\alpha_1^n, \ldots, \alpha_k^n)$. No matrica rekurzije ne može biti dijagonalna. Ipak u slučaju da je B *dijagonalizabilna* matrica, njenu potenciju isto možemo relativno lako odrediti.

Kažemo da je matrica $A \in M_n(\mathbb{C})$ *dijagonalizabilna* nad poljem kompleksnih brojeva ako je *slična* nekoj dijagonalnoj matrici $D \in M_n(\mathbb{C})$, tj. ako postoji regularna matrica $P \in M_n(\mathbb{C})$ takva da je $D = P^{-1}AP$. Matrica P je *matrica prijelaza* između dviju baza vektorskog prostora u kojima je linearnom operatoru pridružena matrica A, odnosno matrica D.

Neka je D dijagonalna matrica i $D = P^{-1}AP$. Tada je $A = PDP^{-1}$ te

$$A^n = (PDP^{-1})(PDP^{-1}) \ldots (PDP^{-1}).$$

Asocijativnost množenja matrica omogućava nam da premjestimo zagrade pa imamo

$$A^n = PD(P^{-1}P)D(P^{-1}P) \cdots (P^{-1}P)DP^{-1}.$$

S obzirom na to da svi susjedni faktori P^{-1} i P u umnošku daju jediničnu matricu I, dobivamo

$$A^n = PD^nP^{-1},$$

što se zbog već spomenute n-te potencije dijagonalne matrice računa relativno lako.

Za određivanje dijagonalne matrice D i regularne matrice P potrebno je riješiti tzv. *spektralni problem* matrice A koji uključuje određivanje svojstvenih vrijednosti matrice (– nultočaka karakteristične jednadžbe $\det(A - \lambda I) = 0$) te pripadnih svojstvenih vektora od kojih se formira matrica P.

Ako B ima n različitih svojstvenih vrijednosti, onda je B dijagonalizabilna. Matrica koja ima manje od n različitih svojstvenih vrijednosti može, ali i ne mora biti dijagonalizabilna. Ako B nije dijagonalizabilna, koristi se takozvana Jordanova forma matrice (no u ovom radu se s tim slučajem nećemo baviti).

Primjer 1.2.1. *Riješimo homogenu linearnu rekurziju drugog reda*

$$a_0 = 2,\ a_1 = 3, a_{n+2} = 3a_{n+1} - 2a_n,\ n \in \mathbb{N}_0, \tag{1.11}$$

koristeći matricu pridruženu rekurziji.

Rješenje. Iščitavamo matricu pridruženu ovoj rekurziji:

$$B = \begin{pmatrix} 3 & -2 \\ 1 & 0 \end{pmatrix}.$$

Svojstveni polinom matrice B bit će

$$k_B(\lambda) = \begin{vmatrix} 3-\lambda & -2 \\ 1 & 0-\lambda \end{vmatrix} = (3-\lambda)(-\lambda) - (-2)\cdot 1 = \lambda^2 - 3\lambda + 2.$$

Nultočke polinoma $\lambda^2 - 3\lambda + 2 = (\lambda - 1)(\lambda - 2)$ su 1 i 2. Svojstvene vrijednosti matrice B su stoga 1 i 2 pa je matrica B dijagonalizabilna. Kako bismo pronašli svojstvene vektore, rješavamo matrične jednadžbe

$$(B - 2I)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \text{ i } (B - 1I)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

gdje je $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (jedinična matrica). Rješenje prve matrične jednadžbe je $(x\ y)^T = (2y\ y)^T = y(2\ 1)^T$, a druge $(x\ y)^T = (x\ x)^T = x(1\ 1)^T$. Od svojstvenih vektora

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

formiramo matricu prijelaza:

$$P = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

Inverz ove matrice nalazimo standardnim postupkom:

$$\left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 1 & -1 \\ 1 & 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \end{array}\right).$$

Dakle,

$$P^{-1} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}.$$

Stoga je $B = PDP^{-1}$, odnosno i $B^n = PD^nP^{-1}$ gdje je

$$D = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

Dakle,

$$\begin{aligned} B^n &= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2^n & 0 \\ 0 & 1^n \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 2^{n+1} & 1 \\ 2^n & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 2^{n+1} - 1 & -2^{n+1} + 2 \\ 2^n - 1 & -2^n + 2 \end{pmatrix} \end{aligned}$$

te

$$\begin{aligned} A_n = B^n A_0 &= \begin{pmatrix} 2^{n+1} - 1 & -2^{n+1} + 2 \\ 2^n - 1 & -2^n + 2 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \\ &= \begin{pmatrix} 3 \cdot 2^{n+1} - 3 - 2 \cdot 2^{n+1} + 4 \\ 3 \cdot 2^n - 3 - 2 \cdot 2^n + 4 \end{pmatrix} \\ &= \begin{pmatrix} 2^{n+1} + 1 \\ 2^n + 1 \end{pmatrix}. \end{aligned}$$

Konačno, opći član niza zadanog rekurzijom i početnim uvjetima (1.11) glasi

$$a_n = 2^n + 1.$$

□

Primijetimo da postupak rješavanja rekurzije ne ovisi o početnim uvjetima. Konkretno, opći član rekurzivnog niza zadan rekurzijom (1.11) i s početnim uvjetima a_0, a_1 glasi:

$$a_n = \begin{pmatrix} 2^n - 1 & -2^n + 2 \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_0 \end{pmatrix} = a_1 (2^n - 1) - a_0 (2^n - 2)$$

Opišimo postupak koji smo proveli u primjeru 1.2.1:

Neka je niz (a_n) zadan početnim uvjetima $a_0, \ldots, a_{k-1} \in \mathbb{C}$ te homogenom linearnom rekurzijom s konstantnim koeficijentima k-tog reda

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}, \ n \geq k,$$

pri čemu su $c_1, \ldots, c_k \in \mathbb{C}$ i $c_k \neq 0$.

1. Označimo matricu rekurzije i početni vektor

$$B = \begin{pmatrix} c_1 & c_2 & \dots & c_{k-1} & c_k \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}_{k\times k}, \quad A_0 = \begin{pmatrix} a_{k-1} \\ a_{k-2} \\ \vdots \\ a_1 \\ a_0 \end{pmatrix}_{k\times 1}.$$

   Pretpostavka: Matrica B je dijagonalizabilna.

2. Odredimo svojstvene vrijednosti matrice B rješavanjem karakteristične jednadžbe

$$\det(B - \lambda I) = 0.$$

   Neka su $\lambda_1, \lambda_2, \dots, \lambda_k$ svojstvene vrijednosti od B (pri čemu svojstvene vrijednosti ne moraju biti međusobno različite).

3. Rješavanjem matričnih jednadžbi

$$BX = \lambda_i X,$$

   za sve $i = 1, \dots, k$, odredimo bazu za $\mathbb{C}^k$ koja se sastoji od svojstvenih vektora matrice B: $\{v_1, \dots, v_k\}$.

4. Formiramo dijagonalnu matricu

$$D = \operatorname{diag}(\lambda_1, \dots, \lambda_k),$$

   i matricu prijelaza čiji su stupci svojstveni vektori matrice B, tj. $P = (v_1\ v_2\ \dots v_k)$ te izračunamo

$$B^n = PD^nP^{-1}.$$

5. Rješenje rekurzije je

$$A_n = B^n A_0.$$

   (Opći član niza a_n možemo dobiti množenjem zadnjeg retka matrice B^n sa jednostupčanom matricom početnih uvjeta A_0.)

1.3 Karakteristična jednadžba rekurzije

Neka je homogenom linearnom rekurzijom (1.1) s konstantnim koeficijentima $c_1, \ldots, c_k \in \mathbb{C}$, $c_k \neq 0$ zadan niz (a_n). Objasnit ćemo postupak za rješavanje ove rekurzije pomoću tzv. karakteristične jednadžbe.

U relaciju (1.1) uvrštavamo $a_n = x^n$, tj. koristimo tzv. Eulerovu supstituciju jer pretpostavljamo da je rješenje od (1.1) linearna kombinacija rješenja oblika x^n. Stoga iz

$$x^n = c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_k x^{n-k}$$

kraćenjem s x^{n-k} (jer nas ne zanima trivijalno rješenje $x = 0$) dobivamo jednadžbu

$$x^k = c_1 x^{k-1} + c_2 x^{k-2} + \cdots + c_k \tag{1.12}$$

koja se naziva **karakteristična jednadžba** rekurzivne relacije (1.1). Označavamo

$$p(x) = x^k - c_1 x^{k-1} - c_2 x^{k-2} - \cdots - c_k.$$

Svaki *korijen karakteristične jednadžbe* (1.12) (odnosno nultočka polinoma p) rješenje je rekurzije (1.1) pa s obzirom na to da je $\mathcal{LH}$ (skup svih kompleksnih nizova zadanih linearnom homogenom rekurzijom reda k s konstantnim koeficijentima) vektorski prostor (propozicija 1.1.2) slijedi da je i linearna kombinacija tih rješenja također rješenje rekurzije (1.1). Konkretno, ako je $p(x) = (x - x_1) \cdots (x - x_k)$, odnosno ako su

$$x_1, \ldots, x_k \in \mathbb{C}$$

korijeni jednadžbe (1.12), tada su

$$x_1^n, \ldots, x_k^n$$

rješenja rekurzije (1.1) pa je i

$$a_n = \alpha_1 x_1^n + \cdots + \alpha_k x_k^n,\ n \geq k, \tag{1.13}$$

rješenje rekurzije (1.1) za proizvoljan izbor konstanti $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$. Rješenje (1.13) naziva se **opće rješenje** rekurzije. Uočimo da su svi korijeni jednadžbe (1.12) različiti od nule zbog pretpostavke da je $c_k \neq 0$.

Pretpostavimo da je $x_1 \in \mathbb{C}$ višestruki korijen kratnosti $r > 1$ jednadžbe (1.12), tj. neka je

$$p(x) = (x - x_1)^r q(x),\ q(x_1) \neq 0.$$

Tada je

$$a_n = n^j x_1^n,\ n \geq k, \tag{1.14}$$

rješenje rekurzije (1.1) za sve $j = 0, 1, \ldots, r-1$. Zaista, najprije uočimo da je x_1 i r-struka nultočka polinoma

$$p_n(x) = x^{n-k}p(x) = x^{n-k}(x-x_1)^r q(x) = x^n - c_1x^{n-1} - c_2x^{n-2} - \cdots - c_kx^{n-k},$$

ali i nultočka prve derivacije polinoma p_n, tj. $p_n'(x_1) = 0$ što možemo zapisati kao

$$nx_1^{n-1} - c_1(n-1)x_1^{n-2} - c_2(n-2)x_1^{n-3} - \cdots - c_k(n-k)x_1^{n-k-1} = 0.$$

Množenjem prethodne jednakosti s x_1 slijedi da je

$$nx_1^n - c_1(n-1)x_1^{n-1} - c_2(n-2)x_1^{n-2} - \cdots - c_k(n-k)x_1^{n-k} = 0,$$

iz čega vidimo da je

$$a_n = nx_1^n$$

rješenje rekurzije (1.1).

Sada ustanovimo da je x_1 nultočka derivacije polinoma

$$xp_n'(x) = nx^n - c_1(n-1)x^{n-1} - c_2(n-2)x^{n-2} - \cdots - c_k(n-k)x^{n-k}.$$

Zaista,

$$xp_n'(x) = x((n-k)x^{n-k-1}(x-x_1)^r q(x) + x^{n-k}r(x-x_1)^{r-1}q(x) + x^{n-k}(x-x_1)^r q'(x)),$$

pa je $xp_n'(x) = (x-x_1)^{r-1}q_1(x)$, a $\frac{\mathrm{d}}{\mathrm{d}x}(xp_n'(x)) = (x-x_1)^{r-2}q_2(x)$. S druge strane,

$$\frac{\mathrm{d}}{\mathrm{d}x}(xp_n'(x)) = n^2x^{n-1} - c_1(n-1)^2x^{n-2} - c_2(n-2)^2x^{n-3} - \cdots - c_k(n-k)^2x^{n-k-1}$$

te uvršavanjem x_1 u prethodni izraz dobivamo

$$n^2x_1^{n-1} - c_1(n-1)^2x_1^{n-2} - c_2(n-2)^2x_1^{n-3} - \cdots - c_k(n-k)^2x_1^{n-k-1} = 0.$$

Ponovo, množenjem prethodne jednakosti s x_1 zaključujemo i da je

$$a_n = n^2x_1^n$$

rješenje rekurzije (1.1). Opisani postupak možemo ponoviti još točno $(r-1)-2$ puta što pokazuje da su (1.14) rješenja rekurzije (1.1).

Zbog svega navedenog razlikujemo dva slučaja za rješavanje homogene linearne rekurzije:

Slučaj I. Karakteristična jednadžba ima k različitih korijena, tj.

$$p(x) = (x - x_1)(x - x_2) \cdots (x - x_k),$$

gdje je $x_i \neq x_j$ za $1 \leq i < j \leq k$.

Slučaj II. Karakteristična jednadžba ima korijene višestruke kratnosti, tj.

$$p(x) = (x - x_1)^{r_1}(x - x_2)^{r_2} \cdots (x - x_l)^{r_l},$$

pri čemu vrijedi $l < k$, $x_i \neq x_j$ za $1 \leq i < j \leq l$ i $r_1 + \cdots + r_l = k$.

Teorem 1.3.1. *Neka su $c_1, c_2, \ldots, c_k \in \mathbb{C}$, $c_k \neq 0$ te neka je niz (a_n) zadan rekurzijom*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},\ n \geq k$$

s početnim uvjetima $a_0, a_1, \ldots, a_{k-1} \in \mathbb{C}$.

I. Ako su $x_1, x_2, \ldots, x_k \in \mathbb{C}$ različiti korijeni karakteristične jednadžbe (1.12)*, onda postoje jedinstveni $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{C}$ takvi da je*

$$a_n = \alpha_1 x_1^n + \cdots + \alpha_k x_k^n, \tag{1.15}$$

za sve $n \in \mathbb{N}_0$.

II. Ako su $x_1, x_2, \ldots, x_l \in \mathbb{C}$ različiti korijeni karakteristične jednadžbe (1.12) *s kratnostima $r_1, r_2, \ldots, r_l$, onda postoje jedinstveni $\alpha_{1,1}, \ldots, \alpha_{1,r_1}, \ldots, \alpha_{l,1}, \ldots, \alpha_{l,r_l} \in \mathbb{C}$ takvi da je*

$$a_n = (\alpha_{1,1} + \alpha_{1,2} n + \cdots + \alpha_{1,r_1} n^{r_1 - 1}) x_1^n + \cdots + (\alpha_{l,1} + \alpha_{l,2} n + \cdots + \alpha_{l,r_l} n^{r_l - 1}) x_l^n, \tag{1.16}$$

za sve $n \in \mathbb{N}_0$.

Dokaz. Pokazali smo da (1.15) i (1.16) zadovoljavaju rekurziju za bilo koji izbor konstanti α_i, odnosno α_{ij}. Još samo preostaje pokazati da su te konstante potpuno određene početnim uvjetima $a_0, a_1, \ldots, a_{k-1}$.

I. U (1.15) uvrštavamo $n = 0$ pa $n = 1$ i tako sve do $n = k - 1$ te dobivamo sustav od k linearnih jednadžbi s k nepoznanica

$$\begin{aligned} \alpha_1 + \alpha_2 + \cdots + \alpha_k &= a_0, \\ x_1\alpha_1 + x_2\alpha_2 + \cdots + x_k\alpha_k &= a_1, \\ &\vdots \\ x_1^{k-1}\alpha_1 + x_2^{k-1}\alpha_2 + \cdots + x_k^{k-1}\alpha_k &= a_{k-1}. \end{aligned}$$

Matrica ovog sustava naziva se Vandermondeova matrica

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_k \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{k-1} & x_2^{k-1} & \dots & x_k^{k-1} \end{pmatrix}$$

te je determinanta Vandermondeove matrice (takozvana Vandermondeova determinanta)

$$\det V = \prod_{1 \le i < j \le k} (x_j - x_i) \tag{1.17}$$

različita od nule jer je $x_i \neq x_j$ za $1 \le i < j \le k$ prema pretpostavci. Dakle, determinanata sustava V je regularna matrica pa zaključujemo da sustav ima jedinstveno rješenje u $\alpha_1, \alpha_2, \dots, \alpha_k$.

II. U ovom se slučaju je matrica sustava u nepoznanicama α_{ij} tzv. poopćena ili generalizirana Vandermondeova matrica i regularna je zbog $x_i \neq x_j$ za $1 \le i < j \le l$. Stoga vrijedi analogan rezultat kao u I. □

Napomena 1.3.2. *Karakteristična jednadžba* (1.12) *rekurzivne relacije* (1.1) *jednaka je upravo karakterističnoj jednadžbi matrice rekurzije B koja je dana s* (1.9) *. Zaista,*

$$\det(B - xI) = \begin{vmatrix} c_1 - x & c_2 & \dots & c_{k-1} & c_k \\ 1 & -x & \dots & 0 & 0 \\ 0 & 1 & & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & -x \end{vmatrix}_{k\times k}$$

$$= (c_1 - x)(-x)^{k-1} - \begin{vmatrix} c_2 & c_3 & \dots & c_{k-1} & c_k \\ 1 & -x & \dots & 0 & 0 \\ 0 & 1 & & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & -x \end{vmatrix}_{(k-1)\times(k-1)}$$

$$= (-1)^k x^k + (-1)^{k-1} c_1 x^{k-1} - c_2 (-x)^{k-2} + \begin{vmatrix} c_3 & c_4 & \dots & c_{k-1} & c_k \\ 1 & -x & \dots & 0 & 0 \\ 0 & 1 & & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & -x \end{vmatrix}_{(k-2)\times(k-2)}$$

$$= \dots = (-1)^k (x^k - c_1 x^{k-1} - c_2 x^{k-2} - \dots - c_k)$$

Primjer 1.3.3. *Riješimo homogenu linearnu rekurziju iz primjera 1.2.1 drugog reda*

$$a_0 = 2, a_1 = 3, a_{n+2} = 3a_{n+1} - 2a_n, n \geq 0,$$

koristeći njenu karakterističnu jednadžbu.

Rješenje. Korijeni karakteristične jednadžbe $x^2 - 3x + 2 = 0$ su $x_1 = 1$ i $x_2 = 2$. Stoga je opće rješenje prema teoremu 1.3.1:

$$a_n = \alpha_1 \cdot 1 + \alpha_2 \cdot 2^n$$

Iz početnih uvjeta slijedi

$$\begin{aligned} \alpha_1 + \alpha_2 &= 2, \\ \alpha_1 + 2\alpha_2 &= 3. \end{aligned} \tag{1.18}$$

Rješenje ovog sustava je $(\alpha_1, \alpha_2) = (1, 1)$ pa je opći član niza dan s

$$a_n = 1 + 2^n.$$

1.4 Primjeri

Primjer 1.4.1. *Riješimo rekurziju kojom je određen Fibonaccijev niz*

$$F_{n+2} = F_{n+1} + F_n, \ n \geq 0,$$

uz početne uvjete $F_0 = 0, F_1 = 1$.

Rješenje. I. način: Pomoću problema svojstvenih vrijednosti matrice rekurzije,

$$B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Svojstvene vrijednosti matrice B su nultočke karakterističnog polinoma

$$k_B(\lambda) = \begin{vmatrix} 1 - \lambda & 1 \\ 1 & 0 - \lambda \end{vmatrix} = \lambda^2 - \lambda - 1.$$

Dakle, svojstvene vrijednosti od B su

$$\alpha = \frac{1 + \sqrt{5}}{2}, \ \beta = \frac{1 - \sqrt{5}}{2}$$

pa se B može dijagonalizirati u bazi svojstvenih vektora: $\{(\alpha, 1), (\beta, 1)\}$, tj.

$$B = PDP^{-1} = P \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} P^{-1},$$

gdje su

$$P = \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix}, P^{-1} = \begin{pmatrix} \frac{1}{\sqrt{5}} & -\frac{1}{\sqrt{5}}\beta \\ -\frac{1}{\sqrt{5}} & \frac{1}{\sqrt{5}}\alpha \end{pmatrix}.$$

Računamo

$$A_n = B^n A_0 = PD^n P^{-1} A_0 = \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{5}} & -\frac{1}{\sqrt{5}}\beta \\ -\frac{1}{\sqrt{5}} & \frac{1}{\sqrt{5}}\alpha \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$= \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha^{n+1} & \beta^{n+1} \\ \alpha^n & \beta^n \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha^{n+1} - \beta^{n+1} \\ \alpha^n - \beta^n \end{pmatrix}.$$

Dakle,

$$F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n) = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n, \ n \geq 0.$$

II. način: Karakteristična jednadžba $x^2 - x - 1 = 0$ ima dva različita korijena: α i β pa je stoga

$$F_n = C \cdot \alpha^n + D \cdot \beta^n.$$

Konstante C, D odredimo pomoću početnih uvjeta $F_0 = 0$, $F_1 = 1$:

$$C + D = 0, \ C\alpha + D\beta = 1.$$

Otuda je

$$C(\alpha - \beta) = 1,$$

odnosno

$$C = \frac{1}{\sqrt{5}}, \ D = -\frac{1}{\sqrt{5}}.$$

□

Primjer 1.4.2. *Riješimo rekurziju zadanu s*

$$a_0 = -1, a_1 = 2, a_2 = 4, \ a_{n+3} = 4a_{n+2} - a_{n+1} - 6a_n, \ n \in \mathbb{N}_0.$$

Rješenje. I. način: Matrica rekurzije je

$$B = \begin{pmatrix} 4 & -1 & -6 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Svojstveni polinom matrice B je

$$k_B(\lambda) = \begin{vmatrix} 4 - \lambda & -1 & -6 \\ 1 & -\lambda & 0 \\ 0 & 1 & -\lambda \end{vmatrix} = -\lambda^3 + 4\lambda^2 - \lambda - 6.$$

Vrijedi

$$-\lambda^3 + 4\lambda^2 - \lambda - 6 = (\lambda + 1)(\lambda - 2)(\lambda - 3),$$

iz čega slijedi da su nultočke svojstvenog polinoma $-1, 2$ i 3. Svojstvene vrijednosti matrice B su stoga $-1, 2$ i 3. Kako bismo pronašli svojstvene vektore, rješavamo

$$(B + I)\begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0,\ (B - 2I)\begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0 \text{ te } (B - 3I)\begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0, \text{ gdje je } I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Rješenje prve matrične jednadžbe je $(x\ y\ z)^T = (x\ \ -x\ \ x)^T = x(1\ \ -1\ \ 1)^T$, druge $(x\ y\ z)^T = (4z\ 2z\ z)^T = y(2\ \ 1)^T$ i treće $(x\ y\ z)^T = (9z\ 3z\ z)^T = z(9\ \ 3\ \ 1)^T$. Stoga su svojstveni vektori

$$\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 9 \\ 3 \\ 1 \end{pmatrix}.$$

Matrica prijelaza glasi

$$P = \begin{pmatrix} 1 & 4 & 9 \\ -1 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix}.$$

Inverz matrice prijelaza je

$$P^{-1} = \begin{pmatrix} \frac{1}{12} & \frac{-5}{12} & \frac{1}{2} \\ \frac{-1}{3} & \frac{2}{3} & 1 \\ \frac{1}{4} & \frac{-1}{4} & \frac{-1}{2} \end{pmatrix}.$$

Za

$$D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

i matricu P vrijedi $B = PDP^{-1}$, stoga vrijedi i $B^n = PD^nP^{-1}$. Budući da je $A_0 = (4\ 2\ -1)^T$, slijedi

$$\begin{aligned} A_n = B^nA_0 &= \begin{pmatrix} 1 & 4 & 9 \\ -1 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} (-1)^n & 0 & 0 \\ 0 & 2^n & 0 \\ 0 & 0 & 3^n \end{pmatrix}\begin{pmatrix} \frac{1}{12} & \frac{-5}{12} & \frac{1}{2} \\ \frac{-1}{3} & \frac{2}{3} & 1 \\ \frac{1}{4} & \frac{-1}{4} & \frac{-1}{2} \end{pmatrix}\begin{pmatrix} 4 \\ 2 \\ -1 \end{pmatrix} \\ &= \begin{pmatrix} -(-1)^n + 3^{n+2} - 2^{n+2} \\ (-1)^n + 3^{n+1} - 2^{n+1} \\ -(-1)^n + 3^n - 2^n \end{pmatrix}. \end{aligned}$$

Dakle, rješenje rekurzije s danim početnim uvjetima je $a_n = -(-1)^n + 3^n - 2^n$.

II. način: Rješenja karakteristične jednadžbe

$$x^3 - 4x^2 + x + 6 = 0$$

su $-1, 2, 3$ pa je opće rješenje rekurzije oblika

$$a_n = \alpha_1 \cdot (-1)^n + \alpha_2 \cdot 3^n + \alpha_3 \cdot 2^n,$$

za neke $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$. Početni uvjeti daju nam sustav tri linearne jednadžbe s tri nepoznanice

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= -1, \\ -\alpha_1 + 3\alpha_2 + 2\alpha_3 &= 2, \\ \alpha_1 + 9\alpha_2 + 4\alpha_3 &= 4, \end{aligned}$$

čije je rješenje $(\alpha_1, \alpha_2\alpha_3) = (-1, 1, -1)$. Dakle, opći član niza je

$$a_n = -(-1)^n + 3^n - 2^n, \ n \geq 0.$$

□

Primjer 1.4.3. *Odredimo opći član niza zadan rekurzijom*

$$s_{n+3} = 3s_{n+2} - 3s_{n+1} + s_n, \ n \geq 0,$$

i početnim uvjetima $s_0 = 0$, $s_1 = 1$, $s_2 = 3$.

Rješenje. Karakteristična jednadžba

$$x^3 - 3x^2 + 3x - 1 = (x-1)^3 = 0$$

ima trostruki korijen $x_1 = 1$ pa je prema teoremu 1.3.1 opće rješenje rekurzije dano s

$$s_n = \alpha_1 + \alpha_2 \cdot n + \alpha_3 \cdot n^2,$$

a konstante $\alpha_1, \alpha_2, \alpha_3$ dobivamo rješavanjem sustava

$$\alpha_1 = 0, \ \alpha_1 + \alpha_2 + \alpha_3 = 1, \ \alpha_1 + 2\alpha_2 + 4\alpha_3 = 3.$$

Kako je $(\alpha_1, \alpha_2, \alpha_3) = (0, \frac{1}{2}, \frac{1}{2})$ slijedi

$$s_n = \frac{1}{2} \cdot n + \frac{1}{2} \cdot n^2 = \frac{1}{2} n(n+1).$$

Dakle, niz (s_n) je niz tzv. *trokutastih brojeva*.
Matrica ove rekurzije nije dijagonalizabilna, no može se prijeći na Jordanovu formu. □

Poglavlje 2

Modularne rekurzije

Ovo poglavlje posvećeno je proučavanju modularnih rekurzija, to jest linearnih rekurzija 1.1.1 zadanih s cjelobrojnim koeficijentima te cjelobrojnim početnim uvjetima modulo neki fiksni prirodni broj.

Prije nego što krenemo u razmatranje periodičnosti modularnih rekurzija, navedimo neke oznake koje ćemo rabiti. Za prirodan broj m skup najmanjih nenegativnih ostataka modulo m označavamo sa

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Skup $\mathbb{Z}_m$ je komutativni prsten s jedinicom s obzirom na operacije zbrajanja i množenja modulo m. Ako je $m = p$ prosti broj, $\mathbb{Z}_p$ je polje.

Za $a \in \mathbb{Z}$ najmanji nenegativan ostatak pri dijeljenju s m označit ćemo s $a \mod m$. To znači da je $a \mod m \in \mathbb{Z}_m$ i kongruentan je broju a modulo m.

2.1 Periodičnost

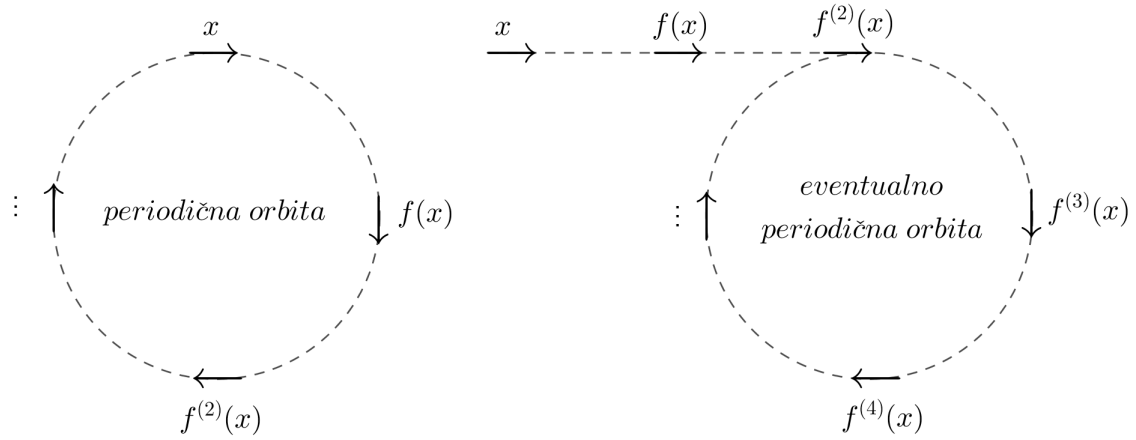
Primjer 2.1.1. *Pogledajmo prvih tridesetak članova Fibonaccijevog niza modulo* 6*:*

$$\underbrace{1, 1, 2, 3, 5, 2, 1, 3, 4, 1, 5, 0, 5, 5, 4, 3, 1, 4, 5, 3, 2, 5, 1, 0}_{24 \text{ člana niza}}, 1, 1, 2, 3, 5, 2, 1, 3, \ldots$$

Primjećujemo da su se početni uvjeti $1, 1$ *ponovili nakon nekog vremena, a budući da je riječ je o rekurziji drugog reda članovi niza će se ponoviti kada se početni uvjeti ponove.*

Ovo smo mogli zaključiti i bez da smo popisali elemente niza jer postoji 36 različitih uređenih parova brojeva modulo 6. Stoga smo sigurni da će se u prvih 37 članova niza pojaviti barem jedno ponavljanje nekog para brojeva.

Periodičnost uočena u primjeru 2.1.1 motivacija je za sljedeću definiciju.



Slika 2.1: Periodična i eventualno periodična orbita

Definicija 2.1.2. *Neka je X neprazan skup. Za funkciju $f : X \to X$ definiramo* ***n-tu iteraciju*** *od f kao*

$$f^{(n)} = \overbrace{f \circ f \circ f \circ \cdots \circ f}^{n \text{ puta}}.$$

Za $x \in X$ niz

$$x, f^{(1)}(x), f^{(2)}(x), f^{(3)}(x), f^{(4)}(x), \ldots \tag{2.1}$$

zovemo ***orbita*** *od x (s obzirom na funkciju f).*

Ako postoji $n > 0$ takav da $f^{(n)}(x) = x$, kažemo da je orbita od x ***periodična****. Ako je orbita od x periodična, njen* ***period*** *je najmanji prirodni broj t za koji vrijedi $f^{(t)}(x) = x$. U slučaju kada je $t = 1$, niz (2.1) je stacionaran i kažemo da je x* ***fiksna točka****.*

Nadalje, kažemo da je orbita od x ***eventualno periodična*** *ako postoji prirodni broj t takav da je $f^{(n+t)}(x) = f^{(n)}(x)$ za sve dovoljno velike n. Najmanji takav $t \in \mathbb{N}$ zvat ćemo* ***period*** *eventualno periodične orbite.*

Primijetimo da je prema definiciji svaka periodična orbita ujedno i eventualno periodična. Na slici 2.1 ilustrirana je ideja periodične orbite kao zatvorene petlje koja se vraća u početnu točku nakon n iteracija od f. Jasno, kod eventualno periodične orbite zatvorena petlja se pojavljuje tek nakon nekoliko početnih iteracija i ona se ostvaruje bez vraćanja u točku x. Definirane pojmove ilustriramo sljedećim primjerom.

Primjer 2.1.3. *Zadana je funkcija* $f : \mathbb{Z} \to \mathbb{Z},\ f(x) = -x^2 + 3x + 1$. *Vrijedi:*

$$f(0) = 1, f^{(2)}(0) = f(f(0)) = f(1) = 3,\ f^{(3)}(0) = f(f^{(2)}(0)) = f(3) = 1, \ldots$$

Orbita od $x = 0$ *je niz* $0, 1, 3, 1, 3, 1, 3, \ldots$, *tj. orbita od* $x = 0$ *je eventualno periodična s periodom dva.*

Teorem 2.1.4. *Neka je* X *konačan skup i* $f : X \to X$. *Tada je orbita od* x *eventualno periodična za svaki* $x \in X$. *Period svake orbite manji je ili jednak broju elemenata skupa* X.

Dokaz. Ako skup X sadrži n elemenata, onda skup

$$\left\{x, f(x), f^{(2)}(x), \ldots, f^{(n)}(x)\right\} \tag{2.2}$$

sadrži $n + 1$ elemenata koji su svi iz skupa X. Stoga moraju postojati dva elementa u skupu (2.2) koji su jednaki. Pretpostavimo da su to

$$f^{(i)}(x) = f^{(j)}(x)$$

za neke $0 \leq i < j \leq n$. Vrijedi

$$\begin{aligned}
f^{(i+1)}(x) =& f(f^{(i)}(x)) = f(f^{(j)}(x)) = f^{(j+1)}(x),\\
f^{(i+2)}(x) =& f(f(f^{(i)}(x))) = f(f(f^{(j)}(x))) = f^{(j+2)}(x),\\
&\vdots\\
f^{(i+k)}(x) =& f^{(j+k)}(x),\ \text{ za sve } k \geq 0.
\end{aligned}$$

Dakle, za $m \geq i$ imamo

$$f^{(m+(j-i))}(x) = f^{(j+(m-i))}(x) = f^{(i+(m-i))}(x) = f^{(m)}(x),$$

zbog čega je orbita od x eventualno periodična i period joj je najviše $j - i$. Zbog $j \leq n$ i $i \geq 0$ slijedi $j - i \leq n$ čime je tvrdnja teorema dokazana. □

Teorem 2.1.5. *Neka je funkcija* $f : X \to X$ *injekcija, pri čemu* X *nije nužno konačan skup. Ako je orbita od* $x \in X$ *eventualno periodična, onda je ona periodična.*

Dokaz. Neka je period orbite od $x \in X$ jednak t te neka N najmanji nenegativan cijeli broj za koji vrijedi

$$f^{(n+t)}(x) = f^{(n)}(x),$$

za sve $n \geq N$. Orbita od x je periodična ako je $N = 0$, tj, ako je

$$f^{(t)}(x) = x.$$

Pretpostavimo suprotno, to jest $N \neq 0$. Tada imamo

$$f(f^{(N-1)}(x)) = f^{(N)}(x) = f^{(N+t)}(x) = f(f^{(N+t-1)}(x)).$$

Budući da je f injekcija, slijedi

$$f^{(N-1)}(x) = f^{(N-1+t)}(x).$$

Međutim, to je u kontradikciji s minimalnošću od N pa zaključujemo da je $N = 0$, tj. orbita od x je periodična. □

Korolar 2.1.6. *Neka je X konačan skup i $f : X \to X$ injektivna funkcija. Tada je orbita svakog elementa skupa X periodična.*

Dokaz. Prema teoremu 2.1.4 je orbita svakog elementa skupa X eventualno periodična jer je X konačan skup, a teorem 2.1.5 povlači da je orbita i periodična (jer je f injekcija). □

Već smo proučili Fibonaccijev niz modulo 6 i uočili da mu je period 24. Promotrimo sada niz Fibonaccijevih brojeva modulo 2, 3, 4 te 12.

- Fibonaccijev niz modulo 2:

  $$1, 1, 0, 1, 1, 0, \ldots$$

  Period je 3.

- Fibonaccijev niz modulo 3:

  $$1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2 \ldots$$

  Period je 8.

- Fibonaccijev niz modulo 4:

  $$1, 1, 2, 3, 1, 0, 1, 1, 2 \ldots$$

  Period je 6.

- Fibonaccijev niz modulo 12:

  $$1, 1, 2, 3, 5, 8, 1, 9, 10, 7, 5, 0, 5, 5, 10, 3, 1, 4, 5, 9, 2, 11, 1, 0, 1, 1, 2 \ldots$$

  Period je 24.

modul	2	3	4	6	12
period	3	8	6	24	24

Tablica 2.1: Periodičnost Fibonaccijevog modularnog niza

Ukratko rezultate istraživanja periodičnosti Fibonaccijevog niza modulo $m \in \{2, 3, 4, 6, 12\}$ prikazujemo u Tablici 2.1.

Primjećujemo period Fibonaccijevog niza modulo modulo $6 = 2 \cdot 3$ jednak 8, odnosno jednak umnošku perioda za modulo 2 i perioda za modulo 3, no za period modulo $12 = 3 \cdot 4$ to ne vrijedi ($24 \neq 8 \cdot 6$), ali ipak $24 \mid 8 \cdot 6$. Sljedeći teorem otkriva zbog čega je to tako.

Napomenimo da za cjelobrojnu funkciju $f : \mathbb{Z} \to \mathbb{Z}$, $f \mod m$ će označavati funkciju definiranu s $(f \mod m)(x) = f(x) \mod m$. Tada je za svaki $x \in \mathbb{Z}$ orbita od x eventualno periodična s obzirom na funkciju $f \mod m$ jer je $f^{(k)} \in \mathbb{Z}_m$ za sve $k \in \mathbb{N}$.

Teorem 2.1.7. *Neka je $f : \mathbb{Z} \to \mathbb{Z}$, $x \in \mathbb{Z}$ te $m_1, m_2 \in \mathbb{N}$. Ako je orbita od x periodična s periodom t_1 s obzirom na funkciju $f \mod m_1$ i periodična s periodom t_2 s obzirom na funkciju $f \mod m_2$, onda je orbita od x periodična s periodom $\mathrm{nzv}(t_1, t_2)$[1] s obzirom na funkciju $f \mod \mathrm{nzv}(m_1, m_2)$.*

Dokaz. Neka je $m = \mathrm{nzv}(m_1, m_2)$ i $T = \mathrm{nzv}(t_1, t_2)$. Prema pretpostavci teorema postoje nenegativni cijeli brojevi N_1 i N_2 za koje je

$$f^{(n+t_i)}(x) \equiv f^{(n)}(x) \pmod{m_i}, \tag{2.3}$$

za sve $n \geq N_i$, $i = 1, 2$. Odatle je

$$f^{(n+T)}(x) \equiv f^{(n)}(x) \pmod{m_i},$$

za sve $n \geq \max\{N_1, N_2\}$. Nadalje, s obzirom na to da ako $m_1 \mid a$ i $m_2 \mid a$, onda $\mathrm{nzv}(m_1, m_2) \mid a$, dobivamo da

$$f^{(n+T)}(x) \equiv f^{(n)}(x) \pmod{m}, \tag{2.4}$$

za sve $n \geq \max\{N_1, N_2\}$.

S druge strane pretpostavimo da je orbita od x periodična s periodom t s obzirom na funkciju $f \mod m$. Dakle, postoji nenegativni cijeli broj N za koji je

$$f^{(n+t)}(x) \equiv f^{(n)}(x) \pmod{m}, \tag{2.5}$$

za sve $n \geq N$.

Trebamo pokazati da je $t = T$.

[1] Najmanji zajednički višekratnik brojeva t_1 i t_2.

$\boxed{t \leq T}$: Direktno iz relacija (2.4) i (2.6). Naime, t je period, tj. najmanji prirodan broj za koji vrijedi (2.6).

$\boxed{T \leq t}$: Iz (2.6) slijedi da je

$$f^{(n+t)}(x) \equiv f^{(n)}(x) \pmod{m_i}, \tag{2.6}$$

za sve $n \geq N$, $i = 1, 2$. Zbog (2.3) mora vrijediti da $t_1 \mid t$ i $t_2 \mid t$ pa stoga i $T = \text{nzv}(t_1, t_2) \mid t$. □

Svaki prirodni broj $m > 1$ možemo prikazati u obliku

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

gdje su $p_1, p_2, \dots, p_s$ različiti prosti brojevi, a $\alpha_1, \alpha_2, \dots, \alpha_s$ su prirodni brojevi. Takav prikaz prirodnog broja $m > 1$ zovemo *kanonski rastav broja m na proste faktore*. Induktivnom primjenom teorema 2.1.7 dobivamo sljedeću tvrdnju.

Korolar 2.1.8. *Neka je $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ kanonski rastav broja m na proste faktore te t_i period orbite od $x \in X$ s obzirom na $f \mod p_i^{\alpha_i}$, $i = 1, 2, \dots, s$. Tada je period orbite od x s obzirom na $f \mod m$ jednak* $\text{nzv}(t_1, t_2, \dots, t_s)$.

2.2 Periodičnost modularnih linearnih rekurzija

U odjeljku 1.2 definirali smo funkciju $f : \mathbb{C}^k \to \mathbb{C}^k$ pravilom preslikavanja (1.8). Sada ćemo promatrati funkcije $f : \mathbb{Z}_m^k \to \mathbb{Z}_m^k$ sa sličnim pravilom preslikavanja

$$f(x_1, x_2, \dots, x_k) = (x_2, \dots, x_k, (c_k x_1 + c_{k-1} x_2 + \dots + c_1 x_k) \mod m), \tag{2.7}$$

gdje su $c_1, \dots, c_k \in \mathbb{Z}_m$ i $c_k \neq 0$.

Napomenimo još da ćemo elemente prstena $\mathbb{Z}_m$ koji imaju multiplikativni inverz modulo m zvati kratko *invertibilnima*. (Pritom ne bi trebalo doći do zabune oko toga s obzirom na koju operaciju mislimo jer svaki element iz Z_m ima aditivni inverz, tj. suprotni element.) Element $a \in \mathbb{Z}_m$ je invertibilan ako i samo ako je a relativno prost s m, tj. $\text{nzd}(a, m) = 1$[2].

Lema 2.2.1. *Funkcija $f : \mathbb{Z}_m^k \to \mathbb{Z}_m^k$ s pravilom preslikavanja* (2.7) *je injekcija ako i samo ako c_k ima multiplikativni inverz modulo m.*

[2]Najveći zajednički djelitelj brojeva a i m.

Dokaz. Pretpostavimo da je

$$f(x_1, x_2, \ldots, x_k) = f(y_1, y_2, \ldots, y_k),$$

za neke $(x_1, x_2, \ldots, x_k), (y_1, y_2, \ldots, y_k) \in \mathbb{Z}_m^k$. Iz (2.7) slijedi

$$\begin{aligned} x_2 &= y_2, \\ &\vdots \\ x_k &= y_k, \\ (c_1 x_k + c_2 x_{k-1} + \cdots + c_k x_1) \mod m &= (c_1 y_k + c_2 y_{k-1} + \cdots + c_k y_1) \mod m, \end{aligned}$$

pa je stoga

$$c_k x_1 \mod m = c_k y_1 \mod m,$$

odnosno

$$c_k x_1 \equiv c_k y_1 \pmod{m}.$$

Prethodna relacija ekvivalentna je s

$$x_1 \equiv y_1 \pmod{m}$$

ako i samo ako je $\text{nzd}(c_k, m) = 1$, tj. ako i samo ako c_k ima multiplikativni inverz modulo m. Budući da su $x_1, y_1 \in \mathbb{Z}_m^k$, zaključujemo da je $x_1 = y_1$ ako i samo ako je c_k invertibilan u $\mathbb{Z}_m^k$. Dakle, $f(x_1, x_2, \ldots, x_k) = f(y_1, y_2, \ldots, y_k)$ povlači da je $(x_1, x_2, \ldots, x_k) = (y_1, y_2, \ldots, y_k)$ ako i samo ako c_k ima multiplikativni inverz modulo m. □

Teorem 2.2.2. *Neka je zadana funkcija $f : \mathbb{Z}_m^k \to \mathbb{Z}_m^k$ s pravilom preslikavanja* (2.7)*. Orbita svake uređene k-torke $(a_0, a_1, \ldots, a_{k-1}) \in \mathbb{Z}_m^k$ je eventualno periodična. Dodatno, ako c_k ima multiplikativni inverz modulo m, orbita svake uređene k-torke $(a_0, a_1, \ldots, a_{k-1}) \in \mathbb{Z}_m^k$ je periodična.*

Dokaz. Zbog toga što je $\mathbb{Z}_m^k$ konačan skup prema teoremu 2.1.4 vrijedi da je orbita svake uređene k-torke $(a_0, a_1, \ldots, a_{k-1})$ eventualno periodična.
Dodatno, lema 2.2.1 garantira nam da je f injekcija jer c_k prema pretpostavci ima multiplikativni inverz modulo m. Teorem 2.1.5 pokazuje da je svaka eventualno periodična orbita od $(a_0, a_1, \ldots, a_{k-1})$ ujedno i periodična zbog čega vrijedi tvrdnja. □

Budući da je c_k invertibilan ako i samo ako je relativno prost s m, imamo sljedeću posljedicu prethodnih tvrdnji.

Korolar 2.2.3. *Neka je $f : \mathbb{Z}_m^k \to \mathbb{Z}_m^k$ dana pravilom preslikavanja* (2.7)*. Ako je* $\text{nzd}(c_k, m) = 1$*, orbita svakog elementa skupa $\mathbb{Z}_m^k$ je periodična.*

Ako je p prosti broj, $\mathbb{Z}_p$ je polje pa je svaki $c_k \in \mathbb{Z}_p\backslash\{0\}$ invertibilan. Stoga vrijedi sljedeća tvrdnja.

Korolar 2.2.4. *Neka je p prosti broj i $f : \mathbb{Z}_p^k \to \mathbb{Z}_p^k$ funkcija dana pravilom preslikavanja* (2.7). *Tada je orbita svakog elementa skupa $\mathbb{Z}_p^k$ periodična.*

2.3 Modularne rekurzije prvog reda

Zanima nas periodičnost modularnih rekurzija prvog reda, tj. rekurzija zadanih s

$$a_n = ca_{n-1}, n \in \mathbb{N}, \tag{2.8}$$

gdje je $c \in \mathbb{Z}\backslash\{0\}$ i $a_0 \in \mathbb{Z}$ (početni uvjet). Riječ je zapravo o geometrijskom nizu čiji je opći član dan s

$$a_n = c^n a_0.$$

Funkcija (2.7) u ovom slučaju je $f : \mathbb{Z}_m \to \mathbb{Z}_m$,

$$f(x) = cx \mod m.$$

Najprije odbacimo trivijalne slučajeve: $a_0 = 0$ (jer je tada $a_n = 0$ za sve $n \in \mathbb{N}$) i $c = 1$ (jer je $a_n = a_0$, za sve $n \in \mathbb{N}$). Dakle, pretpostavljamo da je $a_0 \neq 0$ i $c \neq 1$.

Prije nego što kažemo nešto o periodu ovog modularnog niza, prisjetit ćemo se da je **red** broja a modulo m, pri čemu su a i m relativno prosti, najmanji prirodan broj d za koji vrijedi

$$a^d \equiv 1 \pmod{m}.$$

Označit ćemo ga s $\mathrm{ord}_m(a)$. Eulerov teorem kaže da je

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

za sve $a \in \mathbb{Z}$ i $m \in \mathbb{N}$ takve da je $\mathrm{nzd}(a, m) = 1$ te za posljedicu ima da

$$\mathrm{ord}_m(a) \mid \varphi(m),$$

pri čemu je φ Eulerova funkcija.

Prema korolaru 2.2.3 za niz (2.8), ako je c invertibilan u $\mathbb{Z}_m$, tj. $\mathrm{nzd}(c, m) = 1$, onda je orbita svakog elementa iz $\mathbb{Z}_m$ je periodična. Stoga pretpostavimo da je $\mathrm{nzd}(c, m) = 1$ i da je t period orbite od a_0,

$$f^{(t)}(a_0) = a_0,$$

odnosno

$$a_0 c^t \equiv a_0 \pmod{m}.$$

Prethodna kongruencija ekvivalentna je s

$$c^t \equiv 1 \pmod{\frac{m}{\text{nzd}(a_0, m)}}.$$

Stoga je period t jednak redu broja c modulo $\frac{m}{\text{nzd}(a_0, m)}$.

Pretpostavimo da je $\text{nzd}(c, m) > 1$ i $\text{nzd}(a_0, m) = 1$. Tada orbita od a_0 nije periodična. Zaista, ako je orbita od a_0 periodična s periodom t, onda je

$$a_0 c^t \equiv a_0 \pmod{m},$$

što je ekvivalentno s

$$c^t \equiv 1 \pmod{m}$$

pa c invertibilan element, što nije moguće. No pokažimo da postoje $t, \ell \in \mathbb{N}$ za koje je

$$a_0 c^{t+\ell} \equiv a_0 c^{\ell} \pmod{m}.$$

Neka je ℓ najmanji prirodan broj za koji su brojevi c i $\frac{m}{\text{nzd}(c^\ell, m)}$ relativno prosti. Tada je prethodna kongruencija ekvivalentna kongruenciji

$$c^t \equiv 1 \pmod{\frac{m}{\text{nzd}(c^\ell, m)}},$$

što znači da je orbita od a_0 eventualno periodična s periodom

$$t = \text{ord}_k(c),\ k = \frac{m}{\text{nzd}(c^\ell, m)}.$$

Na kraju pretpostavimo da je $\text{nzd}(c, m) > 1$ i $\text{nzd}(a_0, m) > 1$. Tu razlikujemo dva podslučaja:

- c je relativno prost s n,
- c nije relativno prost s n,

gdje je $n = \frac{m}{\text{nzd}(a_0, m)}$. Ako je $\text{nzd}(c, n) = 1$, onda je kongruencija

$$a_0 c^t \equiv a_0 \pmod{m},$$

ekvivalentna s

$$c^t \equiv 1 \pmod{n}, \tag{2.9}$$

pa je orbita od a_0 periodična s periodom $\text{ord}_n(c)$.

Ako je $\text{nzd}(c, n) > 1$, onda (2.9) ne može vrijediti, no vrijedi

$$c^{t+\ell} \equiv c^{\ell} \pmod{n},$$

što znači da je orbita od a_0 eventualno periodična s periodom $\text{ord}_k(c)$ za $k = \dfrac{n}{\text{nzd}(c^{\ell}, n)}$ gdje je ℓ najmanji prirodan broj za koji su c i k relativno prosti.

Ovime smo dokazali sljedeći teorem.

Teorem 2.3.1. *Neka je $m \in \mathbb{N}$, $a_0, c \in \mathbb{Z}_m \setminus \{0\}$ te $f : \mathbb{Z}_m \to \mathbb{Z}_m$ zadana s $f(x) = cx \mod m$. Nadalje, neka je $n = \dfrac{m}{\text{nzd}(a_0, m)}$. Tada vrijedi:*

1. *Ako je $\text{nzd}(c, n) = 1$, onda je orbita od a_0 periodična s periodom*

$$t = \text{ord}_n(c).$$

2. *Ako je $\text{nzd}(c, n) > 1$, onda orbita od a_0 nije periodična već eventualno periodična s periodom*

$$t = \text{ord}_k(c),$$

gdje je $k = \dfrac{n}{\text{nzd}(c^{\ell}, n)}$, a ℓ je najmanji prirodan broj za koji su c i k relativno prosti.

Primjer 2.3.2. *Zadan je rekurzivni niz*

$$a_n = 12a_{n-1},\ n \geq 1.$$

Proučit ćemo ovaj niz varijajući različite početne uvjete a_0 i module m.

(a) $a_0 = 1$, $m = 13$,

$$a_n \mod 13 : \quad 1, 12, 1, 12, 1, \ldots$$

Period je 2. Naime,

$$\text{nzd}(c, \frac{m}{\text{nzd}(a_0, m)}) = \text{nzd}(c, m) = \text{nzd}(12, 13) = 1,$$

a period je jednak redu broja 12 modulo 13, što je 2 jer je $12^2 \equiv 1 \pmod{13}$.

(b) $a_0 = 1$, $m = 17$,

$$a_n \mod 17 : \quad 1, 1, 12, 8, 11, 13, 3, 2, 7, 16, 5, 9, 6, 4, 14, 15, 10, 1, 12, 8, \ldots$$

Zadovoljeni su isti uvjeti kao u prethodnom slučaju, ali period je maksimalan jer je 12 primitivni korijen modulo 17[3], tj. $t = \text{ord}_{17}(12) = 16$.

[3] Ako je red od c modulo m jednak $\varphi(m)$, onda se c naziva primitivni korijen modulo m.

(c) $a_0 = 3$, $m = 21$,

$$a_n \mod 21: \quad 3, 15, 12, 18, 6, 9, 3, 15, 12, \ldots$$

Vrijedi da je

$$\text{nzd}(c, \frac{m}{\text{nzd}(a_0, m)}) = \text{nzd}(12, 7) = 1$$

pa je period jednak redu broja 12 *modulo* 7*, što je* $t = 6$*.*

(d) $a_0 = 3$, $m = 16$,

$$a_n \mod 16: \quad 3, 4, 0, 0, \ldots$$

Vrijedi da je

$$\text{nzd}(c, m) = \text{nzd}(12, 16) = 4,$$

a to znači da je orbita eventualno periodična. Najmanji prirodan broj ℓ *za koji su* $c = 12$ *i* $\frac{m}{\text{nzd}(c^\ell, m)} = \frac{16}{\text{nzd}(12^\ell, 16)}$ *relativno prosti je* $\ell = 2$*. Taj broj nam kaže da će niz biti periodičan od trećeg člana niza nadalje.*

Sada treba naći najmanji prirodni broj t (period) za koji vrijedi

$$3 \cdot 12^{t+2} \equiv 3 \cdot 12^2 \pmod{16},$$

odnosno ekvivalentna kongruencija

$$12^t \equiv 1 \pmod{1}.$$

što znači da je $t = 1$ *(tj.* $t = \text{ord}_1(12) = 1$*).*

(e) $a_0 = 3$, $m = 120$,

$$a_n \mod 120: \quad 3, 36, 72, 24, 48, 96, 72, 24, \ldots$$

Navedeni modularni niz je eventualno periodičan jer je

$$\text{nzd}(c, \frac{m}{\text{nzd}(m, a_0)}) = \text{nzd}(12, 40) = 4 > 1.$$

Analogno kao u primjeru (d), dobivamo da je $\ell = 2$ *jer su* $c = 12$ *i* $\frac{m}{\text{nzd}(c^\ell, m)} = \frac{120}{\text{nzd}(12^\ell, 120)}$ *relativno prosti za* $\ell = 2$ *pa se niz počinje ponavljati nakon drugog člana. Period t određujemo pomoću kongruencije*

$$3 \cdot 12^{t+2} \equiv 3 \cdot 12^2 \pmod{120},$$

odnosno njoj ekvivalentne

$$12^t \equiv 1 \pmod{5}.$$

Dakle, $t = \text{ord}_5(12) = 4$*.*

2.4 Modularne rekurzije drugog reda

Proučili smo modularne rekurzije prvog reda. Prelazimo na modularne rekurzije drugog reda. Neka su c_1 i c_2 cijeli brojevi koji nisu jednaki nuli. Pretpostavimo da je niz (x_n) zadan rekurzijom

$$x_{n+2} = c_1 x_{n+1} + c_2 x_n,\ n \in \mathbb{N}_0, \tag{2.10}$$

te početnim uvjetima $x_0, x_1 \in \mathbb{Z}$. Za dani modul $m \in \mathbb{N}$, $m > 1$, promatramo cjelobrojni niz $(a_n) \subset \mathbb{Z}_m$ zadan s

$$a_n = x_n \mod m.$$

Bez smanjenja općenitosti možemo uzeti da su $c_1, c_2 \in \mathbb{Z}_m$, $c_1 \neq 0$. Nadalje, pretpostavljamo da je $\text{nzd}(c_2, m) = 1$, odnosno da je c_2 invertibilan element prstena $\mathbb{Z}_m$. Umjesto (2.10) možemo pisati

$$a_{n+2} = c_1 a_{n+1} + c_2 a_n \mod m,\ n \in \mathbb{N}_0, \tag{2.11}$$

uz početne uvjete $a_0, a_1 \in \mathbb{Z}_m$.

Kao u odjeljku 1.2, rekurziju (2.11) možemo matrično zapisati kao

$$A_n = B^n A_{n-1},\ n \in \mathbb{N}_0 \tag{2.12}$$

gdje je

$$A_n = \begin{pmatrix} a_{n+1} \\ a_n \end{pmatrix},$$

a B je matrica pridružena rekurziji (2.11):

$$B = \begin{pmatrix} c_1 & c_2 \\ 1 & 0 \end{pmatrix}. \tag{2.13}$$

Napominjemo da u (2.12) koristimo operaciju modularnog množenje matrica. Nadalje, vrijedi

$$A_n = B^n A_0,\ n \in \mathbb{N}_0. \tag{2.14}$$

Skup svih matrica reda 2 s elementima iz $\mathbb{Z}_m$, u oznaci $M_2(\mathbb{Z}_m)$, čini monoid s obzirom na množenje matrica modulo m. Podskup svih invertibilnih matrica u $M_2(\mathbb{Z}_m)$ ima strukturu grupe. Tu grupu možemo označiti s $\text{GL}(\mathbb{Z}_m, 2)$. Uočimo da je matrica B element grupe $\text{GL}(\mathbb{Z}_m, 2)$. Zaista, budući da je c_2 invertibilan element u $\mathbb{Z}_m$, lako pronalazimo inverz matrice B standardnim postupkom:

$$\left(\begin{array}{cc|cc} c_1 & c_2 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} c_1c_2^{-1} & 1 & c_2^{-1} & 0 \\ 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 0 & 1 & c_2^{-1} & -c_1c_2^{-1} \\ 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 1 & c_2^{-1} & -c_1c_2^{-1} \end{array}\right).$$

Dakle, vrijedi

$$B^{-1} = \begin{pmatrix} 0 & 1 \\ c_2^{-1} & -c_1 c_2^{-1} \end{pmatrix}. \tag{2.15}$$

Nadalje, $\mathrm{GL}(\mathbb{Z}_m, 2)$ je grupa konačnog reda (tj. ima konačno mnogo elemenata) pa je i svaki element te grupe *konačnog reda*. Odnosno za svaku matricu $A \in \mathrm{GL}(\mathbb{Z}_m, 2)$ postoji najmanji prirodni broj k za koju je $A^k = I$, gdje je I jedinična matrica reda 2. Stoga za B postoji najmanji prirodni broj r – *red* matrice B za koji je

$$B^r = I.$$

Zbog prethodne jednakosti i (2.14) slijedi da je

$$A_r = B^r A_0 = IA_0 = A_0,$$

a to znači da je r višekratnik perioda niza (a_n). No može li r biti jednak periodu niza (a_n)? Odgovor na pitanje daje sljedeći teorem.

Teorem 2.4.1. *Neka je niz* (a_n) *iz* $\mathbb{Z}_m$ *zadan rekuzivnom relacijom* (2.11) *uz početne uvjete* $a_0, a_1 \in \mathbb{Z}_m$. *Tada period niza* (a_n) *dijeli red matrice pridružene rekurziji* (2.11).

Nadalje, ako skup $\{(a_1, a_0), (a_2, a_1)\}$ *razapinje modul*[4] $\mathbb{Z}_m^2$, *period niza* (a_n) *jednak je r.*

Dokaz. Prva tvrdnja argumentirana je u raspravi prije teorema.

Prelazimo na matrične zapise:

$$A_0 = \begin{pmatrix} a_1 \\ a_0 \end{pmatrix}, A_1 = \begin{pmatrix} a_2 \\ a_1 \end{pmatrix}$$

te pretpostavljamo da $\{A_0, A_1\}$ razapinje modul $M_{2,1}(\mathbb{Z}_m)$ – modul matrica tipa 2×1 s elementima iz prstena $\mathbb{Z}_m$. Dakle, svaka matrica $X \in M_{2,1}(\mathbb{Z}_m)$ se prikazuje kao

$$X = \alpha_0 A_0 + \alpha_1 A_1,$$

za neke $\alpha_0, \alpha_1 \in \mathbb{Z}_m$. Pretpostavimo da je period niza (a_n) jednak $r_0 \in \mathbb{N}$ i $r_0 < r$. Tada je

$$B^{r_0} A_0 = A_0,\ B^{r_0} A_1 = B^{r_0}(BA_0) = B(B^{r_0} A_0) = A_1,$$

pri čemu je B matrica pridružena rekurziji (2.11) dana s (2.13). Nadalje, jasno je

$$B^{r_0} X = B^{r_0}(\alpha_0 A_0 + \alpha_1 A_1) = \alpha_0 A_0 + \alpha_1 A_1 = X,$$

za sve $X \in M_{2,1}(\mathbb{Z}_m)$. Stoga je nužno $(B^{r_0} - I)X = 0$, za sve $X \in M_{2,1}(\mathbb{Z}_m)$, odnosno $B^{r_0} = I$, a to je u kondradikciji s pretpostavkom da je r red matrice B. Dakle, $r_0 = r$. □

Dokaz teorema 2.4.1 temeljio se samo na invertibilnosti matrice B pa se analogon tog teorema može dokazati za rekurzije k-tog reda.

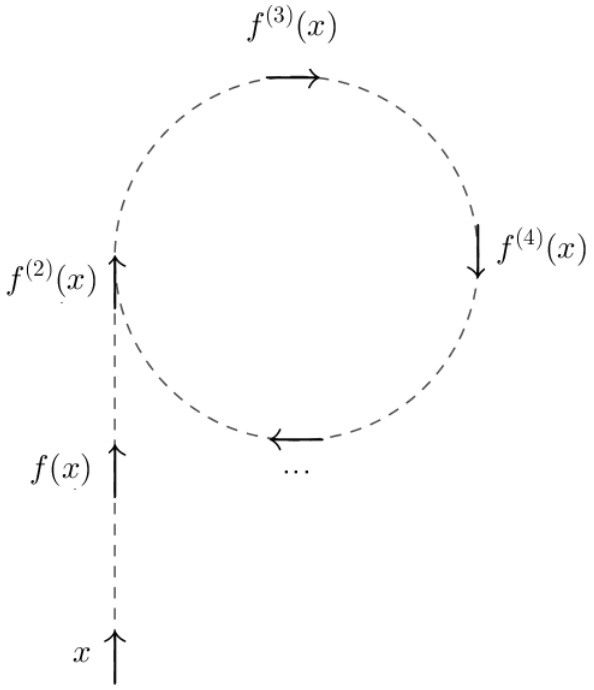
[4] Modul je generalizacija pojma vektorskog prostora, pri čemu je polje skalara zamijenjeno prstenom.

2.5 Primjene

Pseudonasumični brojevi

Nasumični brojevi često su potrebni u primjerice znanstvenom računanju, kriptografiji te videoigrama. Pojam **nasumičan niz** odnosi se na onaj niz koji zadovoljava određene statističke zahtjeve. Primjer jednostavnog zahtjeva za nizove u $\mathbb{Z}_{10}$ je da se svaka znamenka pojavljuje otprilike jednak broj puta tako da je za svaku znamenku vjerojatnost da ju u dovoljno dugim nizovima nasumično odaberemo otprilike jednaka jednoj desetini. Nasumičan niz možemo dobiti mehanički ili iz nekog fizikalnog procesa. Međutim, za nizove dobivene modularnim rekurzijama može se *dokazati* da zadovoljavaju tražene zahtjeve. Jasno, niz ne može zadovoljavati *sve* statističke zahtjeve. To je razlog zašto se brojevi dobiveni ovakvim načinom nazivaju **pseudonasumični**.

Faktorizacija



Slika 2.2: Eventualno periodična orbita u obliku grčkog slova ρ

Jedna od najjednostavnijih metoda rastava na proste faktore je **Pollardova ρ metoda**[5]. Pritom se koristi orbitama polinoma modulo m. Polinom je najčešće kvadratni jer se pokazuje da linearni polinomi ne zadovoljavaju potrebne statističke zahtjeve. Naziv metode proizaći će iz činjenice da dobivamo eventualno periodičnu orbitu koju smo ilustrirali na slici 2.1. Zarotiramo li sliku za 90 stupnjeva u smjeru suprotnom od smjera kazaljke na satu, dobivamo oblik slova ρ kao što možemo vidjeti na slici 2.2. Ova metoda se zasniva na tome da ako je p neki prosti djelitelj od n, onda će p dijeliti i razliku članova niza (generiranog npr. kvadratnim polinomom) modulo p. No kako je p nepoznat, računa se, kroz više iteracija, najveći zajednički djelitelj razlike članova niza modulo n i broja n. Ako je ta vrijednost netrivijalna (tj. različita od n i različita od 1), onda smo dobili djelitelja od n.

[5]John Pollard, britanski matematičar rođen 1941. godine, svoju ρ metodu je izumio 1975. godine.

Bibliografija

[1] D. Bakić, *Linearna algebra i primjene*, Školska knjiga, 2021.

[2] P. Cull, M. Flahive, R. Robson, *Difference Equations: From Rabbits to Chaos*, Springer, 2005.

[3] A. Dujella, *Algoritmi u teoriji brojeva*, skripta, `https://web.math.pmf.unizg.hr/~duje/algortb/algortb.pdf` (lipanj 2022.)

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

[5] A. Dujella, *Uvod u teoriju brojeva*, skripta, `https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf` (srpanj 2022.)

[6] Z. Franušić, J. Šiftar, *Linearna algebra*, skripta, `https://web.math.pmf.unizg.hr/~fran/LA.pdf` (lipanj 2022.)

[7] D. Jukić, *Rekurzivne relacije i potencije kvadratnih matrica*, Ekon. vjesnik, 1 (6), 133–136, 1992.

[8] Z. Kurnik, *Metoda rekurzije*, Matematika i škola, 24, 148–155, 2004.

[9] D. W. Robinson, *A Note on Linear Recurrent Sequences Modulo m*, The American Mathematical Monthly, Vol. 73, No. 6 (1966), 619–621

[10] D. Veljan, *Kombinatorna i diskretna matematika*, Algoritam, Zagreb 2001.

[11] A. Vince, *Period of a linear recurrence*, Acta Arithmetica, XXXIX, 303–301, 1981.

[12] *John Pollard (mathematician)*, `https://en.wikipedia.org/wiki/John_Pollard_(mathematician)` (lipanj 2022.)

Sažetak

Kažemo da niz $(a_n)_{n\geq 0}$ zadovoljava *linearnu homogenu rekurzivnu relaciju s konstantnim koeficijentima reda k* ako vrijedi

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

za sve $n \geq k$, pri čemu su $c_1, c_2, \ldots, c_k \in \mathbb{C}$ konstante, a prvih k članova niza $a_0, a_1, \ldots, a_{k-1}$ su početni uvjeti. U radu je opisana metoda eksplicitnog određivanja općeg člana rekurzivno zadanog niza koja se koristi alatima iz linearne algebre kao što je račun svojstvenih vrijednosti i vektora matrice, te metoda koja koristi karakterističnu jednadžbu rekurzije. Nadalje, proučavale su se i takozvane *modularne rekurzije*, odnosno linearne homogene rekurzije modulo neki fiksni prirodni broj. Njihovo glavno svojstvo je periodičnost uz kojeg se veže problem određivanja perioda.

Summary

A sequence $(a_n)_{n\geq 0}$ is said to satisfy a *linear homogeneous recurrence relation with constant coefficients* if

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

is true for all $n \geq k$, where $c_1, c_2, \ldots, c_k \in \mathbb{C}$, and the first k terms $a_0, a_1, \ldots, a_{k-1}$ are called initial values. In this thesis a method using techniques from linear algebra, such as eigenvalues and eigenvectors of a matrix, is described and applied to determine the general term of sequences satisfying these types of recurrence relations. A method using the characteristic equation of such sequences is also described. Moreover, modular recurrences, which are linear homogeneous recurrences modulo a fixed positive integer, are analysed. Their main property is periodicity, alongside which comes the problem of determining the period.

Životopis

Luka Karlović rođen je 6.10.1998. u Varaždinu u Republici Hrvatskoj. Pohađa VI. osnovnu školu Varaždin nakon čega upisuje Drugu gimnaziju Varaždin gdje pohađa program opće gimnazije. 2017. godine upisuje studijski program Matematika i fizika; smjer: nastavnički na Prirodoslovno-matematičkom fakultetu Sveučilišta u Zagrebu. Tijekom studija radi za Photomath (srpanj-rujan 2020.), kao učitelj matematike u Osnovnoj školi Ivana Filipovića Zagreb (veljača 2021.) te kao demonstrator na kolegijima Elementarna teorija brojeva (2021.) i Uvod u opću fiziku (2022.) na PMF-u Sveučilišta u Zagrebu. Volonterski održava znanstvene radionice iz područja matematike i fizike na Ljetnoj tvornici znanosti (2018.-2022.), dok na PMF-u Sveučilišta u Zagrebu održava radionice iz fizike za srednjoškolce povodom Međunarodnog dana svjetlosti te matematičke radionice za učenike razredne nastave u sklopu Udruge Primus.