MATRICI PĂTRATE DE ORDIN 2

I. RIDICAREA LA PUTERE A UNEI MATRICI PĂTRATE DE ORDIN 2

* În ceea ce urmează vom folosi următoarele notaţii :

$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, S=a+d , D=ad-bc , $I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; a,b,c,d$\in$ **C** (am notat cu **C** mulţimea numerelor complexe).

Presupunem cunoscută identitatea:

$\mathbf{A}^2=S\mathbf{A}-D\mathbf{I}$ (R I.1)

Oricum, se poate verifica foarte uşor. În acest capitol vom da o generalizare a relatiei (R I.1) pentru puteri naturale ale lui A .

* Înmulţind relaţia (R I.1) cu A^{n-1} obţinem $A^{n+1}=SA^n-DA^{n-1}$.
De aici rezultă că putem să considerăm identitatea

$$\begin{pmatrix} A^{n+1} \\ A^n \end{pmatrix}=\begin{pmatrix} S & -D \\ 1 & 0 \end{pmatrix}\begin{pmatrix} A^n \\ A^{n-1} \end{pmatrix} \quad \text{(R I.2)}$$

dacă definim produsul mixt

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} M \\ N \end{pmatrix}=\begin{pmatrix} xM+yN \\ zM+wN \end{pmatrix}$$

unde x,y,z,w$\in$ **C** iar M,N sunt matrici pătrate de ordin2.

Ceea ce e important pentru noi este că produsul acesta are proprietatea asociativităţii mixte următoare :

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\left\{\begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix}\begin{pmatrix} M \\ N \end{pmatrix}\right\}=\left\{\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix}\right\}\begin{pmatrix} M \\ N \end{pmatrix}$$

unde x,y,z,w,x’,y’,z’,w’$\in$ **C** iar M şi N sunt matrici pătrate de ordin 2 cu elemente numere complexe.Aceasta se poate verifica direct prin calcul.

* Dacă notăm $H=\begin{pmatrix} S & -D \\ 1 & 0 \end{pmatrix}$ din relaţia (R I.2) , prin iterare repetată şi folosind asociativitatea mixtă , rezultă :

$$\begin{pmatrix} A^{n+1} \\ A^n \end{pmatrix}=H\begin{pmatrix} A^n \\ A^{n-1} \end{pmatrix}=H\left(H\begin{pmatrix} A^{n-1} \\ A^{n-2} \end{pmatrix}\right)=(H\,H)\begin{pmatrix} A^{n-1} \\ A^{n-2} \end{pmatrix}=H^2\begin{pmatrix} A^{n-1} \\ A^{n-2} \end{pmatrix}=H^2\left(H\begin{pmatrix} A^{n-2} \\ A^{n-3} \end{pmatrix}\right)=K=H^n\begin{pmatrix} A \\ I \end{pmatrix}$$

Deci avem relatia $\begin{pmatrix} A^{n+1} \\ A^n \end{pmatrix}=H^n\begin{pmatrix} A \\ I \end{pmatrix}$ n$\geq$1 ; (R I.3)
care de altfel se poate verifica prin inducţie.

Ceea ce este remarcabil aici este că H are un element egal cu zero ; aceasta ne dă posibilitatea să calculăm H^n şi în cele din urmă A^{n+1}.

* Calculul lui H^n şi al lui A^{n+1}:

Notăm $H^n = \begin{pmatrix} x_n & y_n \\ z_n & w_n \end{pmatrix}$; atunci din relaţia $H^{n+1}=H\,H^n$ rezultă :

$\begin{pmatrix} x_{n+1} & y_{n+1} \\ z_{n+1} & w_{n+1} \end{pmatrix} = \begin{pmatrix} S & -D \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x_n & y_n \\ z_n & w_n \end{pmatrix}$. De aici rezultă :

$$\begin{array}{lcll} x_{n+1}=Sx_n-Dz_n & & x_{n+1}=Sx_n - Dx_{n-1} & \\ y_{n+1}=Sy_n-Dw_n & \Leftrightarrow & y_{n+1}=Sy_n - Dy_{n-1} & \text{(R I.4)} \\ z_{n+1}=x_n & & z_{n+1}=x_n & \\ w_{n+1}=y_n & & w_{n+1}=y_n & \end{array}$$

Fie p şi q rădăcinile ecuaţiei $\alpha^2 - S\alpha + D = 0$; presupunem că $p\neq q$.
Atunci şirurile $\mathbf{x_n=a_1p^n+b_1q^n}$ şi $\mathbf{y_n= a_2p^n+b_2q^n}$ sunt soluţii pentru relaţiile (R I.4) , ceea ce se poate verifica direct prin calcul.

Numerele a_1,b_1 şi a_2,b_2 rezultă din condiţiile iniţiale $H^0 = \begin{pmatrix} x_0 & y_0 \\ z_0 & w_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ şi

$H^1 = \begin{pmatrix} x_1 & y_1 \\ z_1 & w_1 \end{pmatrix} = \begin{pmatrix} S & -D \\ 1 & 0 \end{pmatrix}$. $H^0=I$ deoarece presupunem det $H=D\neq 0$.

Rezultă: $x_0=1$, $y_0=0$ şi $x_1=S$, $y_1= -D$. Aceasta permite să scriem relaţiile :

$$\begin{array}{ll} a_1+b_1=x_0=1 & a_2+b_2=y_0=0 \\ a_1p+b_1q=x_1=S & a_2p+b_2q=y_1= -D \end{array}$$

De aici rezultă printr-un calcul simplu că:

$a_1 = \dfrac{-p}{q-p}$, $b_1 = \dfrac{q}{q-p}$, $a_2 = \dfrac{pq}{q-p}$, $b_2 = \dfrac{-pq}{q-p}$. De aici deducem :

$$\begin{cases} x_n = \dfrac{-p^{n+1}+q^{n+1}}{q-p} \\ y_n = \dfrac{qp^{n+1}-pq^{n+1}}{q-p} = \dfrac{p^n-q^n}{q-p}D \\ z_n = \dfrac{-p^n+q^n}{q-p} \\ w_n = \dfrac{qp^n-pq^n}{q-p} = \dfrac{p^{n-1}-q^{n-1}}{q-p}D \end{cases}$$

Folosind relaţia (R I.3) putem calcula A^{n+1} ; din ea rezultă:

$$\begin{pmatrix} A^{n+1} \\ A^n \end{pmatrix} = \begin{pmatrix} x_n & y_n \\ z_n & w_n \end{pmatrix}\begin{pmatrix} A \\ I \end{pmatrix}$$

$$A^{n+1}=x_nA+y_nI= \frac{q^{n+1}-p^{n+1}}{q-p}A - \frac{q^n-p^n}{q-p}DI \qquad n\geq 1 \qquad \text{(R I.5)}$$

unde p,q sunt rădăcinile distincte ale ecuaţiei $\alpha^2 - S\alpha + D = 0$.

II GENERALIZAREA RELAȚIEI : $A^{n+1} = \frac{q^{n+1}-p^{n+1}}{q-p}A - \frac{q^n-p^n}{q-p}DI$

În determinarea relatiei (R I.5) am folosit faptul că $p \neq q$ şi că $D \neq 0$. În continuare vom găsi o formulă pentru A^n care este mai generală pentru că nu depinde de aceste condiţii .

Notăm $X_n = \frac{q^n-p^n}{q-p}$; $p+q=S$ şi $pq=D$ deoarece p,q verifică ecuaţia $\alpha^2 - S\alpha + D = 0$.

Şirul X_n verifică relaţia de recurenţă $X_{n+1}=SX_n - DX_{n-1}$: Într-adevăr $SX_n - DX_{n-1}=$

$= (p+q)\frac{q^n-p^n}{q-p} - pq\frac{q^{n-1}-p^{n-1}}{q-p} = \frac{q^{n+1}-p^{n+1}}{q-p} = X_{n+1}$.De aceea dăm o nouă definiţie pentru X_n

Definiţia 1: $\mathbf{X_{n+1}=def=SX_n - DX_{n-1}}$ cu valorile iniţiale $\mathbf{X_1=1}$ **şi** $\mathbf{X_2=S}$ şi $\mathbf{n \geq 2}$; (R II.1)

Observaţia1 : termenii $X_1, X_2, X_3, \ldots, X_n, \ldots$sunt definiţi independent de relaţiile $p \neq q$ şi $D \neq 0$
Observaţia2 :putem defini cu aceeaşi relaţie de recurenţă termenii $X_0, X_{-1}, X_{-2}, \ldots$ dacă impunem condiţia suplimentară $D \neq 0$. Într-adevăr :

n=1 implică $X_{1+1}=SX_1 - DX_0$ adică $S= S\cdot 1 - D\cdot X_0$ de unde rezultă $X_0=0$ deoarece $D \neq 0$.

n=0 implică $X_{0+1}=SX_0 - DX_{0-1}$adică $1=S\cdot 0 - D\cdot X_{-1}$ de unde rezultă $X_{-1} = -\frac{1}{D}$ deoarece $D \neq 0$.

n= -1implică $X_{-1+1}=SX_{-1} - DX_{-1-1}$ adică $X_{-2} = -\frac{S}{D^2}$ deoarece $D \neq 0$.

În general $X_{-n} = -\frac{X_n}{D^n}$, pentru $n \geq 1$ daca $D \neq 0$.

Definiţia 2 :Fie $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, S=a+d , D=ad-bc , $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $a,b,c,d \in \mathbf{C}$; definim şirul de matrici : $\mathbf{A_{n+1}=def=X_{n+1}A- X_nD\, I}$ $\mathbf{n \geq 1}$; (R II.2)

Dacă $D \neq 0$ atunci $A_{n+1}=def=X_{n+1}A- X_nD\, I$ $n \in \mathbf{Z}$ (R'II.2) este un şir de matrici definit pentru orice întreg n (vezi obs.2 din def1).
Aici şirul X_n este cel din **Definiţia 1**.

Vom demonstra ca $\mathbf{A^{n+1}=A_{n+1}}$ în 2 etape : $\mathbf{n \geq 1}$ si $\mathbf{n \leq 0}$

Teorema 1 : $\mathbf{A^{n+1}=A_{n+1}}$ pentru orice $\mathbf{n \geq 1}$.
Demonstraţia o facem prin inducţie :
n=1 ; trebuie arătat că $A^2=A_2$;dar $A_2= A_{1+1}=def2= X_{1+1}A- X_1D\, I=def1=SA-1\cdot D\, I$ =(R I.1)=A^2

Presupunem că $A^{k+1}=A_{k+1}$, unde $k \geq 1$ e fixat ; atunci :

$$A^{k+2}=A^{k+1} A =A_{k+1} A=def2= (X_{k+1} A - X_k D\, I) A = X_{k+1} A^2 - X_k D\, I A=(R\ I.1)=$$
$$=X_{k+1} (S A - D I) - X_k D A = (S X_{k+1} - D X_k) A - X_{k+1} D I =def1=$$
$$=X_{k+2} A - X_{k+1} D I=def2= A_{k+2}.$$

Rezultă :$A^{k+2}=A_{k+2}$ şi demonstraţia este completă. Deci:

$\mathbf{A^{n+1}=A_{n+1}=X_{n+1}A- X_nD\ I\ ,\ n\geq 1.}$ (R II.3)

Vom extinde teorema1 şi pentru exponenţi întregi negativi:

Teorema 2 : Dacă $\mathbf{D\neq 0}$ atunci $\mathbf{A^{n+1}=A_{n+1}}$ **pentru orice întreg n**.

Demonstraţia o facem prin inducţie descendentă pentru toate valorile întregi $\mathbf{n\leq 0}$ deoarece pentru $\mathbf{n\geq 1}$ este deja făcută. Conform obs.2 din def1, X_n este definit şi pentru orice număr $n\leq 0$ deoarece $D\neq 0$. Reţinem valorile deja determinate:

$$X_2=S \quad , \quad X_1=1 \quad , \quad X_0=0 \quad , \quad X_{-1}=-\frac{1}{D} \quad , \quad X_{-2}=-\frac{S}{D^2}$$

Dacă n=0 atunci $A_1= A_{0+1}$=def2=$X_{0+1}A- X_0D\ I=1\cdot A- 0\cdot D\ I=A=A^1$. Deci $A_1=A^1$.

Dacă n= -1 atunci $A_0=A_{-1+1}$=def2=$X_{-1+1}A- X_{-1}D\ I=0\cdot A-\left(-\frac{1}{D}\right)D\cdot I=I=A^0$. Deci $A_0=A^0$

Fie n= -2.

Deoarece det A=D≠0 există A^{-1}.Atunci din relaţia $A^2=SA-DI$ prin înmulţirea ei cu A^{-1} obţinem $A=S\ I - DA^{-1}$ de unde rezultă că

$$A^{-1}=-\frac{1}{D}A+\frac{S}{D}I$$

Dar $A_{-1}=A_{-2+1}$=def2= $X_{-2+1}A- X_{-2}D\ I=X_{-1}A- X_{-2}D\ I=$

$$=-\frac{1}{D}A-\left(-\frac{S}{D^2}\right)D\,I=-\frac{1}{D}A+\frac{S}{D}I \ \text{; rezultă:}$$

$$A_{-1}=A^{-1}=-\frac{1}{D}A+\frac{S}{D}I \quad \text{(R II.4)}$$

Presupunem $A^{k+1}=A_{k+1}$ unde $k\leq -2$ este fixat.

Atunci $A^k=A^{-1}A^{k+1}=A^{-1}A_{k+1}$=(R II.4),def2=$\left(-\frac{1}{D}A+\frac{S}{D}I\right)\left(X_{k+1}A-X_kD\,I\right)=$

$$=-\frac{1}{D}X_{k+1}A^2+X_kA+\frac{S}{D}X_{k+1}A-SX_kI=\text{def}1,(\text{R I.1})=-\frac{1}{D}\left(SX_k-DX_{k-1}\right)\left(SA-DI\right)+$$

$$+X_kA+\frac{S}{D}\left(SX_k-DX_{k-1}\right)A-SX_kI=\text{calcul}=X_kA-X_{k-1}D\,I=\text{def}\,2=A_k$$

Deci din $A^{k+1}=A_{k+1}$ rezultă $A^k=A_k$. Inducţia descendentă este probată şi teorema 2 este demonstrată.Deci :

$\mathbf{A^{n+1}=A_{n+1}=X_{n+1}A- X_nD\ I}$ **oricare ar fi n∈ Z ,** <u>dar</u> cu condiţia D≠0. (R II.5)

<u>TREBUIE REŢINUTĂ CONCLUZIA:</u>

Dacă $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ **, S=a+d , D=ad-bc , atunci rezultă că :**

1) $\mathbf{A^{n+1}=X_{n+1}A - X_nD\ I}$ **pentru orice n≥1 , unde şirul X_n este definit de relaţia $X_{n+1}=SX_n - DX_{n-1}$ cu valorile iniţiale $X_1=1$ şi $X_2=S$.**
2) **Dacă D≠0 relaţia $A^{n+1}=X_{n+1}A- X_nD\ I$ este valabilă pentru orice număr întreg n . Facem precizarea că şirul X_n este definit acum pentru orice număr întreg n cu aceeaşi relaţie $X_{n+1}=SX_n - DX_{n-1}$ şi valorile iniţiale $X_1=1$ şi $X_2=S$.**

III STUDIUL ŞIRULUI X_n ŞI CÂTEVA APLICAŢII

*Să vedem ce se întâmplă cu şirul $X_{n+1}=SX_n - DX_{n-1}$ dacă ecuaţia $\alpha^2 - S\alpha + D = 0$ are rădăcinile p şi q egale :

Teorema 1 : Dacă rădăcinile ecuaţiei $\alpha^2 - S\alpha + D = 0$ sunt egale ($q=p\neq0$) atunci soluţia recurenţei $X_{n+1}=SX_n - DX_{n-1}$ este şirul $X_n=nq^{n-1}$, $n\geq1$.

Demonstraţie: Avem relaţiile $S=2q$ şi $D=q^2$. Atunci rezultă că:
$SX_n - DX_{n-1}=2q\cdot nq^{n-1}- q^2\cdot(n-1)q^{n-2}=(n+1)q^n=X_{n+1}$.
În plus avem îndeplinite condiţiile iniţiale $X_1=1q^{1-1}=1$ şi $X_2=2q^{2-1}=2q=S$.

Consecinţă : $\mathbf{A^{n+1}}=X_{n+1}A- X_nD\, I=(n+1)q^nA- nq^{n-1}q^2\, I=\mathbf{q^n[(n+1)A- nqI\,]}$. Relaţia este valabilă şi pentru $n\leq0$ deoarece $D=q^2\neq0$.

Exemplu: $A=\begin{pmatrix}4 & -1\\ 9 & -2\end{pmatrix}$, S=2 , D=1 ; ecuaţia $\alpha^2 - 2\alpha + 1 = 0$ are soluţiile p=q=1 . Rezultă că $A^{n+1}= 1^n[(n+1)\cdot A- n\cdot1\cdot I\,]=\begin{pmatrix}3n+4 & -n-1\\ 9n+9 & -3n-2\end{pmatrix}$; deoarece $D=1\neq0$ putem considera valoarea n= -2 ; atunci obţinem : $A^{-1}=\begin{pmatrix}-2 & 1\\ -9 & 4\end{pmatrix}$.

*Acum considerăm un exemplu în care S=0 . Fie $A=\begin{pmatrix}-1 & -3\\ 2 & 1\end{pmatrix}$. Avem S=0 şi D=5.

Din $X_{n+1}=SX_n - DX_{n-1}$ rezultă :
$X_{n+1}=0\cdot X_n - 5\cdot X_{n-1}$ adică $X_{n+1}= -5X_{n-1}$; deoarece $X_1=1$ şi $X_2=S=0$ rezultă
$X_{2k}=0$ şi $X_{2k+1}=(-5)^k$; atunci avem următoarele relaţii ce rezultă din (R II.5) :

$A^{2k+1}=X_{2k+1}A- X_{2k}5\, I=(-5)^kA$ şi $A^{2k}=X_{2k}A- X_{2k-1}\cdot 5\cdot I=(-5)^kI$,

ceea ce se poate scrie condensat astfel:

$$A^n=(-5)^{[n/2]}\cdot\frac{\left(1+(-1)^n\right)\cdot I+\left(1-(-1)^n\right)\cdot A}{2}$$

Relaţia este valabilă şi pentru $n\leq1$ deoarece $D\neq0$.
Generalizarea cazului S=0 este imediată şi o lăsăm pe seama cititorului.

*Considerăm şi un exemplu în care D=0 . Fie $A=\begin{pmatrix}2 & 3\\ 4 & 6\end{pmatrix}$. Avem S=8 şi D=0.

Din $X_{n+1}=SX_n - DX_{n-1}$ rezultă $X_{n+1}=8\cdot X_n - 0\cdot X_{n-1}$. Rezultă $X_{n+1}=8^n$ iar $A^{n+1}=X_{n+1}A- X_nD\, I$ implică $A^{n+1}=8^n\cdot A- 8^{n-1}\cdot0\cdot I=8^n\cdot A$.
Generalizarea cazului D=0 este imediată şi o lăsăm pe seama cititorului.

*Dacă S=D=0 atunci din identitatea $A^2=SA-DI$ rezultă $A^2=0$. Atunci dacă $n\geq3$ rezultă $A^n=A^2\cdot A^{n-2}=0\cdot A^{n-2}=0$

*Din $X_{n+1}=SX_n - DX_{n-1}$ rezultă o formulă combinatorială pentru X_{n+1} dacă observăm şi generalizăm următoarele relaţii :

$X_1=1$
$X_2=S$
$X_3=SX_2- DX_1=S^2- D$
$X_4=SX_3- DX_2=S^3- 2SD$
$X_5=SX_4- DX_3=S^4- 3S^2D+D^2$
$X_6=SX_5- DX_4=S^5- 4S^3D+3SD^2$
$X_7=SX_6- DX_5=S^6- 5S^4D+6S^2D^2- D^3$
$X_8=SX_7- DX_6=S^7- 6S^5D+10S^3D^2- 4SD^3$

Dacă citim triunghiul lui Pascal pe diagonală de jos în sus şi de la stânga la dreapta în sensul indicat de puncte vedem chiar coeficienţii dezvoltării lui X_{n+1} :

n = 0 N 1
n = 1 N 1 1
n = 2 N 1 2 1
n = 3 N 1 3 3 1
n = 4 N 1 4 6 4 1
n = 5 N 1 5 10 10 5 1
n = 6 N 1 6 15 20 15 6 1
n = 7 N 1 7 21 35 35 21 7 1

De aceea putem presupune că termenul $S^{n-2i}D^i$ din dezvoltarea lui X_{n+1} are coeficientul $(-1)^i C_{n-i}^i$. Intuiţia nu ne înşeală pentru că se poate demonstra :

Teorema 2 :
Șirul X_{n+1} din capitolul II Definiţia 1 în cazul $n\geq 0$ admite reprezentarea următoare :

$$X_{n+1} = S^n - C_{n-1}^1 S^{n-2\cdot 1} D^1 + C_{n-2}^2 S^{n-2\cdot 2} D^2 - \ldots + (-1)^i C_{n-i}^i S^{n-2i} D^i + \ldots = \sum_{i=0}^{\left[n/2\right]} (-1)^i C_{n-i}^i S^{n-2i} D^i$$

Notăm relaţia de mai sus cu (R III.1).

Demonstraţie:

Se verifică faptul că şirul $X_{n+1} = \sum_{i=0}^{\left[n/2\right]} (-1)^i C_{n-i}^i S^{n-2i} D^i$ satisface relaţia de recurenţă $X_{n+1}=SX_n - DX_{n-1}$ şi că are aceeaşi termeni iniţiali $X_1=1$ şi $X_2=S$. Verificarea recurenţei se face analizând cazurile când n este par şi când n este impar deoarece trebuie explicitată limita de sumare $\left[n/2\right]$=partea întreagă a numarului $\frac{n}{2}$.

***Aplicaţia 1 .**

Să se determine o matrice pătrată de ordin 2 , A , astfel încât şirul de matrici A^{n+1} să fie periodic de perioadă n=3 .

Rezolvare : Fie $A=\begin{pmatrix}-2 & 3\\ -1 & 1\end{pmatrix}$. Avem S= -1 şi D=1. Ecuaţia $\alpha^2+\alpha+1=0$ are soluţiile $q=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}$ şi $p=\cos\frac{2\pi}{3}-i\sin\frac{2\pi}{3}$; atunci folosind formula lui Moivre rezultă că

$X_{n+1}=\dfrac{q^{n+1}-p^{n+1}}{q-p}=\dfrac{\sin(n+1)\frac{2\pi}{3}}{\sin\frac{2\pi}{3}}$ este un şir periodic de perioadă n=3; rezultă din (R II.5) că

şi $A^{n+1}=X_{n+1}A-X_n\cdot 1\cdot I$ este şir periodic de perioadă 3 ; avem că $A^3=X_3A-X_2I=0A-(-1)I=I$; de aceea $A^{3k}=I$; $A^{3k+1}=A$; $A^{3k+2}=A^2$.

De asemenea relaţia (R III.1) din teorema 2 implică

$X_{n+1}=\sum_{i=0}^{[n/2]}(-1)^i C_{n-i}^i(-1)^{n-2i}1^i$; de aici rezultă prin înmulţire cu $(-1)^n$ identitatea remarcabilă :

$$\sum_{i=0}^{[n/2]}(-1)^i C_{n-i}^i=(-1)^n\dfrac{\sin(n+1)\frac{2\pi}{3}}{\sin\frac{2\pi}{3}}\quad ,\ n\geq 0$$

***Aplicaţia 2.**

Să se determine o matrice pătrată de ordin 2 , A , astfel încât şirul de matrici A^{n+1} să fie periodic de perioadă n=10 .

Rezolvare: Fie $A=\begin{pmatrix}\cos\frac{\pi}{5} & 1+\cos\frac{\pi}{5}\\ -1+\cos\frac{\pi}{5} & \cos\frac{\pi}{5}\end{pmatrix}=\frac{1}{4}\begin{pmatrix}1+\sqrt{5} & 5+\sqrt{5}\\ -3+\sqrt{5} & 1+\sqrt{5}\end{pmatrix}$;avem $S=2\cos\frac{\pi}{5}$ şi D=1

iar ecuaţia $\alpha^2-2\cos\frac{\pi}{5}\alpha+1=0$ are soluţiile $q=\cos\frac{\pi}{5}+i\sin\frac{\pi}{5}$ şi $p=\cos\frac{\pi}{5}-i\sin\frac{\pi}{5}$.

Rezultă folosind din nou formula lui Moivre că $X_{n+1}=\dfrac{q^{n+1}-p^{n+1}}{q-p}=\dfrac{\sin(n+1)\frac{\pi}{5}}{\sin\frac{\pi}{5}}$; aceasta ne

arată că şirul X_{n+1} este periodic de perioadă n=10 ; rezultă din (R II.5) că şi $A^{n+1}=X_{n+1}A-X_n\cdot 1\cdot I$ este şir periodic de perioadă n=10.Se verifică uşor că $X_{10}=0$ şi $X_9=-1$; atunci $A^{10}=X_{10}A-X_9\cdot 1\cdot I=0\cdot A-(-1)\cdot 1\cdot I=I$. De aceea $A^{10k+j}=A^j$ unde $0\leq j\leq 9$.

Relaţia (R III.1) din teorema 2 conduce la identitatea:

$$X_{n+1} = \sum_{i=0}^{[n/2]} (-1)^i C_{n-i}^i \left(\frac{1+\sqrt{5}}{2}\right)^{n-2i} = \frac{\sin(n+1)\frac{\pi}{5}}{\sin\frac{\pi}{5}} \quad , \ n\geq 0 \qquad \text{(R III.2)}$$

***Aplicaţia 3 .**

Aici vom demonstra câteva proprietăţi ale şirului lui Fibonaci.
Şirul numerelor lui Fibonaci este definit de recurenţa $F_{n+1}=F_n+F_{n-1}$
şi de valorile iniţiale $F_1=F_2=1$; avem în tabelul de mai jos primii 18 termeni :

F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}	F_{14}	F_{15}	F_{16}	F_{17}	F_{18}
1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584

*Considerăm matricea $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$; vrem să calculăm A^{n+1} cu relaţia $A^{n+1}=X_{n+1}A- X_nD\, I$.

Avem S=1 , D= -1 ; relaţia $X_{n+1}=SX_n - DX_{n-1}$ devine $X_{n+1}=X_n +X_{n-1}$, valorile iniţiale fiind $X_1=1$ şi $X_2=S=1$; de aici rezultă că $X_{n+1}=F_{n+1}$.
Atunci relaţia (R II.5) devine :

$A^{n+1}=F_{n+1}A- F_n(-1)I=\begin{pmatrix} F_{n+1} & F_{n+1} \\ F_{n+1} & 0 \end{pmatrix} + \begin{pmatrix} F_n & 0 \\ 0 & F_n \end{pmatrix} = \begin{pmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{pmatrix}$;(am utilizat relaţia$F_{n+2}=F_{n+1}+F_n$)

Ultima relaţie se mai poate scrie :

$$A^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} ;$$

*Deoarece det $(A^n)=(\det A)^n$ obţinem relaţia :

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

*Din $A^{n+m}=A^n\cdot A^m$ obţinem :

$\begin{pmatrix} F_{n+m+1} & F_{n+m} \\ F_{n+m} & F_{n+m-1} \end{pmatrix} = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \cdot \begin{pmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{pmatrix}$; de aici se pot deduce patru identităţi a căror scriere o lăsăm pe seama cititorului.

*Relaţia (R III.1) devine :

$F_{n+1} = \sum_{i=0}^{[n/2]} (-1)^i C_{n-i}^i 1^{n-2i} (-1)^i$; de aici deducem identitatea remarcabilă :

$$F_{n+1} = \sum_{i=0}^{[n/2]} C_{n-i}^i = C_n^0 + C_{n-1}^1 + C_{n-2}^2 + \ldots \qquad n\geq 0 \qquad \text{(R III.3)}$$

*Rădăcinile ecuaţiei $\alpha^2 - \alpha - 1 = 0$ sunt $q = \frac{1+\sqrt{5}}{2}$, $p = \frac{1-\sqrt{5}}{2}$ de unde rezultă că recurenţa $F_{n+1}=F_n+F_{n-1}$ cu condiţiile iniţiale $F_1=F_2=1$ este verificată de şirul

$F_n = \frac{q^n - p^n}{q-p} = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$; de aici rezultă că

$$\left|\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n} - F_n\right| = \frac{1}{\sqrt{5}}\left(\frac{\sqrt{5}-1}{2}\right)^{n} \rightarrow 0 \quad ,\text{adica} \quad F_n \cong \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n} \;;$$

De aceea în relaţia (R III.2) $\sum_{i=0}^{[n/2]}(-1)^i C_{n-i}^{i}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2i} = \frac{\sin(n+1)\frac{\pi}{5}}{\sin\frac{\pi}{5}}$ este interesant să vedem

ce obţinem dacă facem înlocuirea $\left(\frac{1+\sqrt{5}}{2}\right)^{n-2i} \rightarrow F_{n-2i}$.

Prin înlocuire obţinem şirul $Y_{n+1} = \text{def} = \sum_{i=0}^{[n/2]}(-1)^i C_{n-i}^{i} F_{n-2i}$.

Am calculat cu ajutorul unui calculator de buzunar primele 18 valori ale acestui şir :

Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}	Y_{17}	Y_{18}
0	1	1	0	0	0	-1	-1	0	0	0	1	1	0	0	0	-1	-1

În calcule am folosit valoarea $F_0=0$.
Analizând aceste valori intuim că şirul Y_{n+1} este mărginit , ia doar valorile -1 , 0 , 1 şi este chiar periodic (perioada este probabil n=10) .
Nu am demonstrat deocamdată nici una din aceste afirmaţii.
Propunem aceste probleme cititorului . (Sugerăm să folosim relaţia (R III.3) ; astfel reducem totul la o problemă de combinări) .

Aplicaţia 4 .
Vom prezenta în continuare fără detalii un sistem criptografic .
*Chestiuni preliminare :
Considerăm aici că matricea A are elemente din corpul $\mathbf{Z_p}$, unde p este un număr prim mare.
Menţinem def 1 şi def 2 din cap. **II** ; în aceste condiţii au loc teoremele 1 şi 2 din cap. **II** adică
$A^{n+1}=X_{n+1}A- X_nD\,I$ (R III.4)
*Ideea de bază a cripto-sistemului :
-introducem textul pe care vrem să-l criptăm în elementele lui A sub formă binară
(de exemplu fiecare caracter al textului poate fi reprezentat pe un octet iar câteva caractere alăturate formează un număr pe care îl atribuim elementului « a » al matricii A , etc.) .
-criptarea matricii A constă în calcularea unei puteri A^{n+1} ; A^{n+1} reprezintă textul deja criptat sau criptotextul.
-cheia de decriptare este formată din perechea de numere (X_{n+1}, X_nD)

Cel care obţine în mod fraudulos criptotextul A^{n+1}, trebuie să-l ghicească pe A (ştiindu-l doar pe A^{n+1}) , ca să ajungă la textul iniţial . Aceasta este extrem de improbabil fiindcă nu deţine cheia (X_{n+1}, X_nD).

Pentru cel care deţine cheia este foarte simplu să-l obţină pe A din (R III.4) :

$A=(X_{n+1})^{-1}(A^{n+1}+X_nD\,I)$

*Dacă avem de criptat un volum mare de date procedăm astfel :

Presupunem că avem mai multe « sertare » fiecare cu cheia lui ; ca să nu purtăm după noi toate cheile încuiem în « sertarul 2 » cheia de la « sertarul 1 » , apoi încuiem în « sertarul 3 » cheia de la « sertarul 2 » şi aşa mai departe ; noi nu trebuie să păstrăm decât cheia de la ultimul « sertar ».
Sertarele conţin evident şi informatia pe care vrem să o protejăm.

Sertarele sunt un şir de matrici de forma :

$$A_{(i)} = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$$

Textul se introduce în elementele a_i şi d_i iar cheia pentru decriptare a matricii precedente se introduce în elementele b_i şi c_i ; după aceste operaţiuni se criptează matricea $A_{(i)}$ iar cheia ei de decriptare se va introduce în matricea următoare $A_{(i+1)}$.

*Trebuie evitate cazurile S=0 , D=0 , $S^2=4D$ deoarece atunci decriptarea poate deveni uşoară chiar fără cunoaşterea cheii ; de aceea vom folosi un caracter special w de un octet care nu are nici o semnificaţie în text dar prin introducerea căruia se modifică valoarea numerică a elementelor a_i şi d_i până când obţinem îndeplinirea celor trei condiţii $S\neq 0$, $D\neq 0$, $S^2\neq 4D$.

*Toate calculele se fac modulo p ; de aceea numărul de caractere care formează elementele a_i şi d_i este limitat de mărimea numărului prim p.

*Putem oricând să adăugăm la text o continuare : caracterele noi vor fi introduse în matrici noi ;avantajul evident este că lungimea cheii ultimei matrici adăugate nu depinde deloc de lungimea textului pe care l-am criptat .

*Numărul prim p trebuie să fie suficient de mare încât să descurajeze tentativa de a încerca toate cheile posibile.

Nota : Am utilizat o idee din cartea lui Isaac J. Shoenberg « Privelisti matematice » , Editura Tehnica -1989