

## MATRICI PĂTRATE DE ORDIN 2

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

\* În ceea ce urmează vom folosi următoarele notații :

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

Presupunem cunoscută identitatea:

$$A^2 = SA - DI \quad (\text{R I.1})$$

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

\* Înmulțind relația (R I.1) cu  $A^{n-1}$  obținem  $A^{n+1} = SA^n - DA^{n-1}$ .

De aici rezultă că putem să considerăm identitatea

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

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} M \\ N \end{pmatrix} = \begin{pmatrix} xM + yN \\ zM + wN \end{pmatrix} \text{ unde } x,y,z,w \in \mathbf{C} \text{ iar } M,N \text{ sunt matrici pătrate de ordin 2.}$$

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

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \left\{ \begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix} \begin{pmatrix} M \\ N \end{pmatrix} \right\} = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix} \right\} \begin{pmatrix} M \\ N \end{pmatrix} \text{ unde } x,y,z,w,x',y',z',w' \in \mathbf{C} \text{ iar } M \text{ și } N$$

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 relația (R I.2) , prin iterare repetată și folosind asociativitatea mixtă , rezultă :

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

$$\text{Deci avem relația } \begin{pmatrix} A^{n+1} \\ A^n \end{pmatrix} = H^n \begin{pmatrix} A \\ I \end{pmatrix} \quad n \geq 1 \quad ; \quad (\text{R I.3})$$

care de altfel se poate verifica prin inducție.

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

\* Calculul lui  $H^n$  și al lui  $A^{n+1}$ :

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

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

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

Fie  $p$  și  $q$  rădăcinile ecuației  $\alpha^2 - S\alpha + D = 0$ ; presupunem că  $p \neq q$ .  
Atunci șirurile  $x_n = a_1 p^n + b_1 q^n$  și  $y_n = a_2 p^n + b_2 q^n$  sunt soluții pentru relațiile (R I.4), ceea ce se poate verifica direct prin calcul.

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

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

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

$$\begin{aligned} a_1 + b_1 &= x_0 = 1 & a_2 + b_2 &= y_0 = 0 \\ a_1 p + b_1 q &= x_1 = S & a_2 p + b_2 q &= y_1 = -D \end{aligned}$$

De aici rezultă printr-un calcul simplu că:

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

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

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

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

$$A^{n+1} = x_n A + y_n I = \frac{q^{n+1} - p^{n+1}}{q-p} A - \frac{q^n - p^n}{q-p} D I \quad n \geq 1 \quad (R I.5)$$

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

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

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

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

$$\begin{aligned} \text{Șirul } X_n \text{ verifică relația de recurență } X_{n+1} &= SX_n - DX_{n-1} : \text{Într-adevăr } SX_n - DX_{n-1} = \\ &= (p+q) \frac{q^n - p^n}{q-p} - pq \frac{q^{n-1} - p^{n-1}}{q-p} = \frac{q^{n+1} - p^{n+1}}{q-p} = X_{n+1}. \end{aligned}$$

De aceea dăm o nouă definiție pentru  $X_n$

**Definiția 1:**  $X_{n+1} = \text{def} = SX_n - DX_{n-1}$  cu valorile inițiale  $X_1=1$  și  $X_2=S$  și  $n \geq 2$  ; (R II.1)

Observația 1 : termenii  $X_1, X_2, X_3, \dots, X_n, \dots$  sunt definiți independent de relațiile  $p \neq q$  și  $D \neq 0$   
 Observația 2 : putem defini cu aceeași relație de recurență termenii  $X_0, X_{-1}, X_{-2}, \dots$  dacă impunem condiția suplimentară  $D \neq 0$  . Într-adevăr :

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

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

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

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

$$\text{Definiția 2 : Fie } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} , S=a+d , D=ad-bc , I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} ; a,b,c,d \in \mathbb{C} ; \text{ definim}$$

$$\text{șirul de matrici : } A_{n+1} = \text{def} = X_{n+1}A - X_n D I \quad n \geq 1 ; \quad (\text{R II.2})$$

Dacă  $D \neq 0$  atunci  $A_{n+1} = \text{def} = X_{n+1}A - X_n D I \quad n \in \mathbb{Z} \quad (\text{R'II.2})$  este un șir de matrici definit pentru orice întreg  $n$  (vezi obs.2 din def1).

Aici șirul  $X_n$  este cel din **Definiția 1**.

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

**Teorema 1 :**  $A^{n+1} = A_{n+1}$  pentru orice  $n \geq 1$ .

Demonstrația o facem prin inducție :

$$n=1 ; \text{trebuie arătat că } A^2 = A_2 ; \text{dar } A_2 = A_{1+1} = \text{def} = X_{1+1}A - X_1 D I = \text{def} = SA - 1 \cdot D I = (\text{R I.1}) = A^2$$

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

$$\begin{aligned} A^{k+2} &= A^{k+1} A = A_{k+1} A = \text{def} = (X_{k+1} A - X_k D I) A = X_{k+1} A^2 - X_k D I A = (\text{R I.1}) = \\ &= X_{k+1} (S A - D I) - X_k D A = (S X_{k+1} - D X_k) A - X_{k+1} D I = \text{def} = \\ &= X_{k+2} A - X_{k+1} D I = \text{def} = A_{k+2}. \end{aligned}$$

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

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

Vom extinde teorema 1 și pentru exponenți întregi negativi:

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

Demonstrația o facem prin inducție descendentă pentru toate valorile întregi  $n \leq 0$  deoarece pentru  $n \geq 1$  este deja făcută. Conform obs.2 din def1,  $X_n$  este definit și pentru orice număr  $n \leq 0$  deoarece  $D \neq 0$ . Reținem valorile deja determinate:

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

Dacă  $n=0$  atunci  $A_1 = A_{0+1} = \text{def } 2 = X_{0+1}A - X_0 D I = 1 \cdot A - 0 \cdot D I = A = A^1$ . Deci  $A_1 = A^1$ .

Dacă  $n = -1$  atunci  $A_0 = A_{-1+1} = \text{def } 2 = X_{-1+1}A - X_{-1} D I = 0 \cdot A - \left(-\frac{1}{D}\right) D \cdot I = I = A^0$ . Deci  $A_0 = A^0$

Fie  $n = -2$ .

Deoarece  $\det A = D \neq 0$  există  $A^{-1}$ . Atunci din relația  $A^2 = SA - DI$  prin înmulțirea ei cu  $A^{-1}$  obținem  $A = S I - DA^{-1}$  de unde rezultă că

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

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

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

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

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

Atunci  $A^k = A^{-1} A^{k+1} = A^{-1} A_{k+1} = (R II.4), \text{ def } 2 = \left(-\frac{1}{D} A + \frac{S}{D} I\right) (X_{k+1}A - X_k D I) =$

$$= -\frac{1}{D} X_{k+1} A^2 + X_k A + \frac{S}{D} X_{k+1} A - S X_k I = \text{def } 1, (R I.1) = -\frac{1}{D} (S X_k - D X_{k-1}) (SA - DI) +$$

$$+ X_k A + \frac{S}{D} (S X_k - D X_{k-1}) A - S X_k I = \text{calcul} = X_k A - X_{k-1} D I = \text{def } 2 = A_k$$

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

$$A^{n+1} = A_{n+1} = X_{n+1}A - X_n D I \text{ oricare ar fi } n \in \mathbb{Z}, \text{ dar cu condiția } D \neq 0. \quad (R II.5)$$

### TREBUIE REȚINUTĂ CONCLUZIA:

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

- 1)  $A^{n+1} = X_{n+1}A - X_n D I$  pentru orice  $n \geq 1$ , unde șirul  $X_n$  este definit de relația  $X_{n+1} = S X_n - D X_{n-1}$  cu valorile inițiale  $X_1 = 1$  și  $X_2 = S$ .
- 2) Dacă  $D \neq 0$  relația  $A^{n+1} = X_{n+1}A - X_n D I$  este valabilă pentru orice număr întreg  $n$ . Facem precizarea că șirul  $X_n$  este definit acum pentru orice număr întreg  $n$  cu aceași relație  $X_{n+1} = S X_n - D X_{n-1}$  și valorile inițiale  $X_1 = 1$  și  $X_2 = S$ .

### III STUDIUL ȘIRULUI $X_n$ ȘI CÂTEVA APLICAȚII

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

**Teorema 1** : Dacă rădăcinile ecuației  $\alpha^2 - S\alpha + D = 0$  sunt egale ( $q=p \neq 0$ ) atunci soluția recurenței  $X_{n+1}=SX_n - DX_{n-1}$  este șirul  $X_n=nq^{n-1}$ ,  $n \geq 1$ .

Demonstrație: Avem relațiile  $S=2q$  și  $D=q^2$ . 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 condițiile inițiale  $X_1=1q^{1-1}=1$  și  $X_2=2q^{2-1}=2q=S$ .

Consecință :  $A^{n+1}=X_{n+1}A - X_n D I = (n+1)q^n A - nq^{n-1} q^2 I = q^n [(n+1)A - nqI]$ . Relația este valabilă și pentru  $n \leq 0$  deoarece  $D=q^2 \neq 0$ .

Exemplu:  $A = \begin{pmatrix} 4 & -1 \\ 9 & -2 \end{pmatrix}$ ,  $S=2$ ,  $D=1$ ; ecuația  $\alpha^2 - 2\alpha + 1 = 0$  are soluțiile  $p=q=1$ . Rezultă că

$A^{n+1} = 1^n [(n+1) \cdot A - n \cdot 1 \cdot I] = \begin{pmatrix} 3n+4 & -n-1 \\ 9n+9 & -3n-2 \end{pmatrix}$ ; deoarece  $D=1 \neq 0$  putem considera valoarea

$n=-2$ ; atunci obținem :  $A^{-1} = \begin{pmatrix} -2 & 1 \\ -9 & 4 \end{pmatrix}$ .

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

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  $X_1=1$  și  $X_2=S=0$  rezultă  $X_{2k}=0$  și  $X_{2k+1}=(-5)^k$ ; atunci avem următoarele relații ce rezultă din (R II.5) :

$$A^{2k+1} = X_{2k+1}A - X_{2k}5I = (-5)^k A \quad \text{și} \quad A^{2k} = X_{2k}A - X_{2k-1} \cdot 5 \cdot I = (-5)^k I,$$

ceea ce se poate scrie condensat astfel:

$$A^n = (-5)^{\lfloor \frac{n}{2} \rfloor} \cdot \frac{(1 + (-1)^n) \cdot I + (1 - (-1)^n) \cdot A}{2}$$

Relația este valabilă și pentru  $n \leq 1$  deoarece  $D \neq 0$ .

Generalizarea cazului  $S=0$  este imediată și o lăsăm pe seama cititorului.

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

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  $A^{n+1}=X_{n+1}A - X_n D I$  implică  $A^{n+1}=8^n \cdot A - 8^{n-1} \cdot 0 \cdot I = 8^n \cdot A$ .

Generalizarea cazului  $D=0$  este imediată și o lăsăm pe seama cititorului.

\*Dacă  $S=D=0$  atunci din identitatea  $A^2=SA-DI$  rezultă  $A^2=0$ . Atunci dacă  $n \geq 3$  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 și generalizăm următoarele relații :

$$X_1=1$$

$$X_2=S$$

$$X_3=SX_2- DX_1=S^2- D$$

$$X_4=SX_3- DX_2=S^3- 2SD$$

$$X_5=SX_4- DX_3=S^4- 3S^2D+D^2$$

$$X_6=SX_5- DX_4=S^5- 4S^3D+3SD^2$$

$$X_7=SX_6- DX_5=S^6- 5S^4D+6S^2D^2- D^3$$

$$X_8=SX_7- DX_6=S^7- 6S^5D+10S^3D^2- 4SD^3$$

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

$$n = 0 \quad N \quad 1$$

$$n = 1 \quad N \quad 1 \quad 1$$

$$n = 2 \quad N \quad 1 \quad 2 \quad 1$$

$$n = 3 \quad N \quad 1 \quad 3 \quad 3 \quad 1$$

$$n = 4 \quad N \quad 1 \quad 4 \quad 6 \quad 4 \quad 1$$

$$n = 5 \quad N \quad 1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1$$

$$n = 6 \quad N \quad 1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1$$

$$n = 7 \quad N \quad 1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1$$

De aceea putem presupune că termenul  $S^{n-2i}D^i$  din dezvoltarea lui  $X_{n+1}$

are coeficientul  $(-1)^i C_{n-i}^i$ . Intuiția nu ne înșală pentru că se poate demonstra :

### **Teorema 2 :**

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

$$X_{n+1} = S^n - C_{n-1}^1 S^{n-2 \cdot 1} D^1 + C_{n-2}^2 S^{n-2 \cdot 2} D^2 - K + (-1)^i C_{n-i}^i S^{n-2i} D^i + K = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^i C_{n-i}^i S^{n-2i} D^i$$

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

Demonstrație:

Se verifică faptul că șirul  $X_{n+1} = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^i C_{n-i}^i S^{n-2i} D^i$  satisface relația de recurență

$X_{n+1}=SX_n - DX_{n-1}$  și că are aceiași termeni inițiali  $X_1=1$  și  $X_2=S$ . Verificarea recurenței se face analizând cazurile când  $n$  este par și când  $n$  este impar deoarece trebuie explicitată limita

de sumare  $\lfloor \frac{n}{2} \rfloor = \text{partea întregă a numărului } \frac{n}{2}$ .

**\*Aplicația 1.**

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

Rezolvare: Fie  $A = \begin{pmatrix} -2 & 3 \\ -1 & 1 \end{pmatrix}$ . Avem  $S = -1$  și  $D = 1$ . Ecuația  $\alpha^2 + \alpha + 1 = 0$  are soluțiile

$q = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}$  și  $p = \cos \frac{2\pi}{3} - i \sin \frac{2\pi}{3}$ ; atunci folosind formula lui Moivre rezultă că

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

și  $A^{n+1} = X_{n+1}A - X_n \cdot 1 \cdot I$  este șir 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 relația (R III.1) din teorema 2 implică

$$X_{n+1} = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^i C_{n-i}^i (-1)^{n-2i} 1^i; \text{ de aici rezultă prin înmulțire cu } (-1)^n \text{ identitatea remarcabilă:}$$

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

**\*Aplicația 2.**

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

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

iar ecuația  $\alpha^2 - 2 \cos \frac{\pi}{5} \alpha + 1 = 0$  are soluțiile  $q = \cos \frac{\pi}{5} + i \sin \frac{\pi}{5}$  și  $p = \cos \frac{\pi}{5} - i \sin \frac{\pi}{5}$ .

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

arată că șirul  $X_{n+1}$  este periodic de perioadă  $n=10$ ; rezultă din (R II.5) că și

$A^{n+1} = X_{n+1}A - X_n \cdot 1 \cdot I$  este șir periodic de perioadă  $n=10$ . Se verifică ușor că  $X_{10} = 0$  și  $X_9 = -1$ ; 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  $0 \leq j \leq 9$ .

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

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

**\*Aplicația 3.**

Aici vom demonstra câteva proprietăți ale șirului lui Fibonacci.

Șirul numerelor lui Fibonacci este definit de recurența  $F_{n+1}=F_n+F_{n-1}$

și de valorile inițiale  $F_1=F_2=1$ ; 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 relația  $A^{n+1}=X_{n+1}A - X_n D I$ .

Avem  $S=1$ ,  $D=-1$ ; relația  $X_{n+1}=SX_n - DX_{n-1}$  devine  $X_{n+1}=X_n + X_{n-1}$ , valorile inițiale fiind  $X_1=1$  și  $X_2=S=1$ ; de aici rezultă că  $X_{n+1}=F_{n+1}$ .

Atunci relația (R II.5) devine :

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

Ultima relație se mai poate scrie :

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

\*Deoarece  $\det(A^n)=(\det A)^n$  obținem relația :

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

\*Din  $A^{n+m}=A^n \cdot A^m$  obținem :

$$\begin{pmatrix} F_{n+m+1} & F_{n+m} \\ F_{n+m} & F_{n+m-1} \end{pmatrix} = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \cdot \begin{pmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{pmatrix}; \text{ de aici se pot deduce patru identități a căror}$$

scriere o lăsăm pe seama cititorului.

\*Relația (R III.1) devine :

$$F_{n+1} = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^i C_{n-i}^i 1^{n-2i} (-1)^i; \text{ de aici deducem identitatea remarcabilă :}$$

$$F_{n+1} = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} C_{n-i}^i = C_n^0 + C_{n-1}^1 + C_{n-2}^2 + \dots + K \quad n \geq 0 \quad (\text{R III.3})$$

\*Rădăcinile ecuației  $\alpha^2 - \alpha - 1 = 0$  sunt  $q = \frac{1+\sqrt{5}}{2}$ ,  $p = \frac{1-\sqrt{5}}{2}$  de unde rezultă că recurența  $F_{n+1}=F_n+F_{n-1}$  cu condițiile inițiale  $F_1=F_2=1$  este verificată de șirul

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



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

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

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

Prin înlocuire obținem șirul  $Y_{n+1} = \text{def} = \sum_{i=0}^{\lfloor n/2 \rfloor} (-1)^i C_{n-i}^i F_{n-2i}$ .

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

Y <sub>1</sub>	Y <sub>2</sub>	Y <sub>3</sub>	Y <sub>4</sub>	Y <sub>5</sub>	Y <sub>6</sub>	Y <sub>7</sub>	Y <sub>8</sub>	Y <sub>9</sub>	Y <sub>10</sub>	Y <sub>11</sub>	Y <sub>12</sub>	Y <sub>13</sub>	Y <sub>14</sub>	Y <sub>15</sub>	Y <sub>16</sub>	Y <sub>17</sub>	Y <sub>18</sub>
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 șirul  $Y_{n+1}$  este mărginit, ia doar valorile -1, 0, 1 și este chiar periodic (perioada este probabil  $n=10$ ).

Nu am demonstrat deocamdată nici una din aceste afirmații.

Propunem aceste probleme cititorului. (Sugerăm să folosim relația (R III.3); astfel reducem totul la o problemă de combinări).

#### Aplicația 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.

Menținem def 1 și def 2 din cap. II; în aceste condiții au loc teoremele 1 și 2 din cap. II adică  $A^{n+1} = X_{n+1}A - X_n D I$  (R III.4)

\*Idea 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  $(X_{n+1}, X_n D)$

Cel care obține în mod fraudulos criptotextul  $A^{n+1}$ , trebuie să-l ghicească pe A (știindu-l doar pe  $A^{n+1}$ ), ca să ajungă la textul inițial. Aceasta este extrem de improbabil fiindcă nu deține cheia  $(X_{n+1}, X_n D)$ .

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

$$A = (X_{n+1})^{-1} (A^{n+1} + X_n D I)$$

\*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 » și așa mai departe ; noi nu trebuie să păstrăm decât cheia de la ultimul « sertar ».

Sertarele conțin evident și informația pe care vrem să o protejăm.

Sertarele sunt un șir de matrici de forma :

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

Textul se introduce în elementele  $a_i$  și  $d_i$  iar cheia pentru decriptare a matricii precedente se introduce în elementele  $b_i$  și  $c_i$  ; după aceste operațiuni 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 ușoară chiar fără cunoașterea cheii ; de aceea vom folosi un caracter special  $w$  de un octet care nu are nici o semnificație în text dar prin introducerea căruia se modifică valoarea numerică a elementelor  $a_i$  și  $d_i$  până când obținem îndeplinirea celor trei condiții  $S \neq 0$  ,  $D \neq 0$  ,  $S^2 \neq 4D$ .

\*Toate calculele se fac modulo  $p$  ; de aceea numărul de caractere care formează elementele  $a_i$  și  $d_i$  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**