

## Exercice 4 (5 points) Centres étrangers Juin 2014

### Partie A : préliminaires

1. a. Soient  $n$  et  $N$  deux entiers naturels supérieurs ou égaux à 2, tels que :  $n^2 \equiv N - 1 \pmod{N}$ .

Montrer que :  $n \times n^3 \equiv 1 \pmod{N}$ .

$$n^2 \equiv N - 1 \pmod{N} \Rightarrow (n^2)^2 \equiv (N - 1)^2 \pmod{N}$$

Or  $(N - 1)^2 = N^2 - 2N + 1$  et  $N^2 \equiv 0 \pmod{N}$  et  $-2N \equiv 0 \pmod{N}$ , donc  $(N - 1)^2 \equiv 1 \pmod{N}$ .

Finalement  $n \times n^3 \equiv 1 \pmod{N}$  car  $n^4 = n \times n^3$ .

b. Dédurre de la question précédente un entier  $k_1$  tel que :  $5k_1 \equiv 1 \pmod{26}$ .

On a  $5^2 = 25 = 26 - 1$ , donc  $5^2 \equiv -1 \pmod{26}$ .

La question précédente montre que  $5 \times 5^3 \equiv 1 \pmod{26}$ .

Donc  $k_1 = 5^3 = 125$ .

On admettra que l'unique entier  $k$  tel que :  $0 \leq k \leq 25$  et  $5k \equiv 1 \pmod{26}$  vaut 21.

2. On donne les matrices :  $A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}$ ,  $B = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}$ ,  $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ ,  $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ .

a. Calculer la matrice  $6A - A^2$ .

$$6A = \begin{pmatrix} 24 & 6 \\ 18 & 12 \end{pmatrix} \text{ et } A^2 = \begin{pmatrix} 19 & 6 \\ 18 & 7 \end{pmatrix}, \text{ donc } 6A - A^2 = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = 5I \text{ (I matrice unité).}$$

b. En déduire que  $A$  est inversible et que sa matrice inverse, notée  $A^{-1}$ , peut s'écrire sous la forme  $A^{-1} = \alpha I + \beta A$ , où  $\alpha$  et  $\beta$  sont deux réels que l'on déterminera.

On a  $6A - A^2 = A(6I - A) = 5I$  ou encore  $A \times \frac{1}{5}(6I - A) = I$  : cette égalité montre que la matrice  $A$  est inversible et que son inverse est  $A^{-1} = \frac{1}{5}(6I - A) = \frac{6}{5}I - \frac{1}{5}A$ .

c. Vérifier que :  $B = 5A^{-1}$ .

$$A^{-1} = \frac{6}{5}I - \frac{1}{5}A \Leftrightarrow 5A^{-1} = 6I - A = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} = B.$$

Conclusion  $B = 5A^{-1}$ .

d. Démontrer que si  $AX = Y$ , alors  $5X = BY$ .

En partant de l'égalité précédente :

$$B = 5A^{-1} \Leftrightarrow BA = 5A^{-1}A \Leftrightarrow BA = 5I \Leftrightarrow BAX = 5IX \Leftrightarrow BY = 5X.$$

### Partie B : procédure de codage

• Le mot à coder est remplacé par la matrice  $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ , où  $x_1$  est l'entier représentant la première lettre du mot et  $x_2$  l'entier représentant la deuxième, selon le tableau de correspondance ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

• La matrice  $X$  est transformée en la matrice  $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$  telle que :  $Y = AX$ .

• La matrice  $Y$  est transformée en la matrice  $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ , où  $r_1$  est le reste de la division euclidienne de  $y_1$  par 26 et  $r_2$  le reste de la division euclidienne de  $y_2$  par 26.

• Les entiers  $r_1$  et  $r_2$  donnent les lettres du mot codé, selon le tableau de correspondance ci-dessus.

Exemple : « OU » (mot à coder) donne « YE » :

$$\text{OU} \rightarrow X = \begin{pmatrix} 14 \\ 20 \end{pmatrix} \rightarrow Y = \begin{pmatrix} 76 \\ 82 \end{pmatrix} \rightarrow R = \begin{pmatrix} 24 \\ 4 \end{pmatrix} \rightarrow \text{YE}.$$

**Question :** Coder le mot « ET », en utilisant et en détaillant la procédure de codage décrite ci-dessus.

ET est codé par la matrice  $X = \begin{pmatrix} 4 \\ 19 \end{pmatrix}$ .

Puis  $Y = AX = \begin{pmatrix} 35 \\ 50 \end{pmatrix}$ , puis  $R = \begin{pmatrix} 9 \\ 24 \end{pmatrix}$  et d'après le tableau ET est codé JY .

**Partie C : procédure de décodage** (on conserve les mêmes notations que pour le codage)

Lors du codage, la matrice  $X$  a été transformée en la matrice  $Y$  telle que :  $Y = AX$ .

1. Démontrer que : 
$$\begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_2 = -3y_1 + 4y_2 \end{cases}.$$

On a  $Y = AX \Leftrightarrow A^{-1}Y = X \Leftrightarrow 5A^{-1}Y = 5X = BY$  soit  $Y = AX \Leftrightarrow \begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_2 = -3y_1 + 4y_2 \end{cases}$

2. En utilisant la question 1. b. de la partie A, établir que : 
$$\begin{cases} x_1 \equiv 16y_1 + 5y_2 \pmod{26} \\ x_2 \equiv 15y_1 + 6y_2 \pmod{26} \end{cases}.$$

La question 1. b. de la partie A a montré que  $5 \times 21 \equiv 1 \pmod{26}$ . Donc en reprenant le système de la question précédente et en multipliant par 21, on obtient :

$$\begin{cases} 21 \times 5x_1 = 21 \times (2y_1 - y_2) \\ 21 \times 5x_2 = 21 \times (-3y_1 + 4y_2) \end{cases} \Leftrightarrow \begin{cases} 21 \times 5x_1 = 42y_1 - 21y_2 \\ 21 \times 5x_2 = -63y_1 + 84y_2 \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 16y_1 + 5y_2 \pmod{26} \\ x_2 \equiv 15y_1 + 6y_2 \pmod{26} \end{cases}$$

3. Décoder le mot « QP ».

QP est associé à la matrice  $\begin{pmatrix} 16 \\ 15 \end{pmatrix}$ .

En utilisant le résultat précédent :

$$\begin{cases} x_1 \equiv 16y_1 + 5y_2 \pmod{26} \\ x_2 \equiv 15y_1 + 6y_2 \pmod{26} \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 256 + 75 \pmod{26} \\ x_2 \equiv 240 + 90 \pmod{26} \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 331 \pmod{26} \\ x_2 \equiv 330 \pmod{26} \end{cases} \Leftrightarrow \begin{cases} x_1 = 19 \\ x_2 = 18 \end{cases}$$

Le mot décodé est donc TS .