

Centres étrangers 2014. Enseignement de Spécialité

EXERCICE 4 (5 points) (candidats ayant suivi l'enseignement de spécialité)

Partie A : préliminaires

1) a) $n \times n^3 = n^4 = (n^2)^2$. Par hypothèse, $n^2 \equiv N - 1$ modulo N ou encore $n^2 \equiv -1$ modulo N . Par suite, $(n^2)^2 \equiv (-1)^2$ modulo N ou encore

$$n \times n^3 \equiv 1 \text{ modulo } N.$$

b) On applique le résultat précédent à $n = 5$ et $N = 26$. On a $n^2 = 25$ avec $25 \equiv 26 - 1$ modulo 26.

D'après la question précédente, si on prend $k_1 = n^3$, alors $5k_1 = n \times n^3 \equiv 1$ modulo 26. L'entier $k_1 = 125$ convient.

2) a) $6A - A^2 = 6 \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} - \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 24 & 6 \\ 18 & 12 \end{pmatrix} - \begin{pmatrix} 19 & 6 \\ 18 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = 5I_2.$

b) Par suite, $A \times (6I - A) = (6I - A) \times A = 5I_2$ ou encore $A \times \frac{1}{5}(6I - A) = \frac{1}{5}(6I - A) \times A = I_2$. On en déduit que la matrice A est inversible et que

$$A^{-1} = \frac{6}{5}I - \frac{1}{5}A.$$

c) $5A^{-1} = 6I - A = 6 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} = B.$

d) $AX = Y \Rightarrow 5A^{-1}AX = 5A^{-1}Y \Rightarrow 5I_2X = BY \Rightarrow 5X = BY.$

Partie B : procédure et codage

• Le mot « ET » est remplacé par la matrice $X = \begin{pmatrix} 4 \\ 19 \end{pmatrix}$.

• La matrice X est transformée en la matrice

$$Y = AX = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 4 \\ 19 \end{pmatrix} = \begin{pmatrix} 35 \\ 50 \end{pmatrix}.$$

• $35 = 1 \times 26 + 9$ avec $0 \leq 9 \leq 25$ et $50 = 1 \times 26 + 24$ avec $0 \leq 24 \leq 25$. Donc $r_1 = 9$ et $r_2 = 24$ ou encore $R = Y = \begin{pmatrix} 9 \\ 24 \end{pmatrix}$.

• Le vecteur colonne R est associé au mot « JY ».

$$\text{Le mot « ET » est codé en le mot « JY ».$$

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

1) D'après la question 2)d) de la partie A, on a $5X = BY$ et donc

$$\begin{pmatrix} 5x_1 \\ 5x_2 \end{pmatrix} = 5X = BY = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2y_1 - y_2 \\ -3y_1 + 4y_2 \end{pmatrix},$$

et donc $\begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_2 = -3y_1 + 4y_2 \end{cases}$.

2) On multiplie chacune des deux égalités précédentes par l'entier $k = 21$. Puisque $5k \equiv 1$ modulo 26 la question 1)b) de la partie A, on obtient

$$\begin{cases} x_1 \equiv 42y_1 - 21y_2 \\ x_2 \equiv -63y_1 + 84y_2 \end{cases} \text{ modulo } 26 \quad (*).$$

D'autre part, $42 = 1 \times 26 + 16$ et donc $42 \equiv 16$ modulo 26. Ensuite, $-21 = (-1) \times 26 + 5$ et donc $-21 \equiv 5$ modulo 26. Ensuite, $-63 = (-3) \times 26 + 15$ et donc $-63 \equiv 15$ modulo 26. Enfin, $84 = 3 \times 26 + 6$ et donc $84 \equiv 6$ modulo 26. (*) peut donc encore s'écrire

$$\begin{cases} x_1 \equiv 16y_1 + 5y_2 \\ x_2 \equiv 15y_1 + 6y_2 \end{cases} \text{ modulo } 26.$$

3) Le mot « QP » est associé au vecteur $Y = \begin{pmatrix} 16 \\ 15 \end{pmatrix}$. D'après la question précédente, modulo 26 $x_1 \equiv 16 \times 16 + 5 \times 15$ ou encore $x_1 \equiv 331$. Puisque $331 = 12 \times 26 + 19$, on a encore $x_1 \equiv 19$ modulo 26 et finalement $x_1 = 19$.

De même, $x_2 \equiv 15 \times 16 + 6 \times 15$ ou encore $x_2 \equiv 330$ puis $x_2 \equiv 18$ modulo 26 et finalement $x_2 = 18$.

Le vecteur $X = \begin{pmatrix} 19 \\ 18 \end{pmatrix}$ est associé au mot « TS » et donc

Le mot « QP » code le mot « TS ».