TS spécialité

corrigé de du Bac blanc

Partie A

1. Quand on saisit 3 , l'algorithme affiche 3 (aucun tour de boucle)
2. Quand on saisit 55 , l'algorithme affiche 3 (deux tours de boucle, $55-26-26=3$)
3. Pour un nombre entier positif X quelconque, l'algorithme affiche l'entier positif inférieur à 26 congru à X modulo 26 , c'est-à-dire le reste de la division euclidienne de X par 26 .

Partie B

1. $\begin{pmatrix}3 & 1\\5 & 2\end{pmatrix}\begin{pmatrix}17\\4\end{pmatrix}=\begin{pmatrix}55\\93\end{pmatrix}$ puis $55-2\times26=3$ et $93-3\times26=15$.

2. a. $\begin{pmatrix}x_1\\x_2\end{pmatrix}$ est transformé en $\begin{pmatrix}z_1\\z_2\end{pmatrix}$ donc $\begin{cases}3x_1+x_2\equiv z_1(26)\\5x_1+2x_2\equiv z_2(26)\end{cases}$. De même $\begin{cases}3x'_1+x'_2\equiv z_1(26)\\5x'_1+2x'_2\equiv z_2(26)\end{cases}$ et

   donc on a $\begin{cases}3x_1+x_2\equiv 3x'_1+x'_2(26)\\5x_1+2x_2\equiv 5x'_1+2x'_2(26)\end{cases}$.

   b. $\begin{cases}3x_1+x_2\equiv 3x'_1+x'_2(26)\\5x_1+2x_2\equiv 5x'_1+2x'_2(26)\end{cases}\Rightarrow\begin{cases}6x_1+2x_2\equiv 6x'_1+2x'_2(26)\\5x_1+2x_2\equiv 5x'_1+2x'_2(26)\end{cases}$. Par différence on obtient

   $6x_1+2x_2-(5x_1+2x_2)\equiv 6x'_1+2x'_2-(5x'_1+2x'_2)(26)\Leftrightarrow x_1\equiv x'_1(26)$. De même on a

   $3(5x_1+2x_2)-5(3x_1+x_2)\equiv 3(5x'_1+2x'_2)-5(3x'_1+x'_2)(26)\Leftrightarrow x_2\equiv x'_2(26)$.

   Comme $0\le x_1<26$ et $0\le x'_1<26$ on a $-26<x_1-x'_1<26$. Or $x_1-x'_1\equiv 0(26)$ donc

   $x_1-x'_1=0\Leftrightarrow x_1=x'_1$. De même $x_2=x'_2$.

   Ceci prouve que deux blocs de deux lettres différents ne peuvent pas être codés de la même façon.

3. a. $C'C=\begin{pmatrix}2 & -1\\-5 & 3\end{pmatrix}\begin{pmatrix}3 & 1\\5 & 2\end{pmatrix}=\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}=I_2$ Donc C' est la matrice inverse de C .

   b. $\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{pmatrix}2 & -1\\-5 & 3\end{pmatrix}\begin{pmatrix}3\\15\end{pmatrix}=\begin{pmatrix}-9\\30\end{pmatrix}$

   c. $-9+26=17$ et $30-26=4$ donc $\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}17\\4\end{pmatrix}$.

   d. On peut conjectuer que la méthode de décodage est semblable à la méthode de codage mais en utilisant la matrice inverse à celle du codage.

4. a. On a $\begin{pmatrix}y'_1\\y'_2\end{pmatrix}=C'\begin{pmatrix}z_1\\z_2\end{pmatrix}$ donc $C\begin{pmatrix}y'_1\\y'_2\end{pmatrix}=CC'\begin{pmatrix}z_1\\z_2\end{pmatrix}\Leftrightarrow C\begin{pmatrix}y'_1\\y'_2\end{pmatrix}=\begin{pmatrix}z_1\\z_2\end{pmatrix}\Leftrightarrow\begin{cases}3y'_1+y'_2=z_1\\5y'_1+2y'_2=z_2\end{cases}$ et

   comme $x_1\equiv y'_1(26)$ et $x_2\equiv y'_2(26)$ on a $\begin{cases}3y'_1+y'_2\equiv 3x_1+x_2(26)\\5y'_1+2y'_2\equiv 5x_1+2x_2(26)\end{cases}\Leftrightarrow\begin{cases}3x_1+x_2\equiv z_1(26)\\5x_1+2x_2\equiv z_2(26)\end{cases}$

b. $\begin{cases} 3x_1 + x_2 \equiv z_1 (26) \\ 5x_1 + 2x_2 \equiv z_2 (26) \end{cases}$ signifie que $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ est transformé en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$. Comme il existe un unique couple transformé en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ (voir question 2), on a bien décodé $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$.

5. QC → $\begin{pmatrix} 16 \\ 2 \end{pmatrix}$ puis $C' \begin{pmatrix} 16 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 16 \\ 2 \end{pmatrix} = \begin{pmatrix} 30 \\ -74 \end{pmatrix}$. $30 - 26 = 4$ et $-74 + 3 \times 26 = 4$. On a enfin $\begin{pmatrix} 4 \\ 4 \end{pmatrix}$ → EE. Le décodage de QC est donc EE.