Corrigé Bac Blanc
Spécialité

EXERCICE 4 **5 points**

Candidats ayant suivi l'enseignement de spécialité

Partie A

On considère l'algorithme suivant :

A et X sont des nombres entiers
Saisir un entier positif A
Affecter à X la valeur de A
Tant que X supérieur ou égal à 26
Affecter à X la valeur X −26
Fin du tant que
Afficher X

1. Si on saisit 3 comme valeur de A, le nombre X prend la valeur 3 qui est inférieure à 26 donc on n'entre pas dans la boucle « tant que » ; l'algorithme affiche la valeur de X donc 3.
2. Si on saisit 55 comme valeur de A, le nombre X prend d'abord la valeur 55 qui est supérieure à 26 ; la première fois qu'on entre dans la boucle, on remplace X par X−26 = 55 − 26 = 29. Le nombre 29 est encore supérieur ou égal à 26 donc on entre une seconde fois dans la boucle ; le nombre X est remplacé par X−26 = 29−26 = 3.
   Le nombre 3 est strictement plus petit que 26 donc on n'entre pas dans la boucle et on affiche la valeur de X donc 3.
3. Dans cet algorithme, on soustrait 26 autant de fois que l'on peut du nombre positif X ; on obtient un nombre entier compris entre 0 et 25 qui représente le reste de la division de X par 26 et donc le reste de la division de A par 26.

Partie B

1. Explication du codage de RE en DP, autrement dit du passage de $\begin{pmatrix}17\\4\end{pmatrix}$ à $\begin{pmatrix}3\\15\end{pmatrix}$:

   $C\times\begin{pmatrix}17\\4\end{pmatrix}=\begin{pmatrix}3&1\\5&2\end{pmatrix}\begin{pmatrix}17\\4\end{pmatrix}=\begin{pmatrix}3\times17+1\times4\\5\times17+2\times4\end{pmatrix}=\begin{pmatrix}51+4\\85+8\end{pmatrix}=\begin{pmatrix}55\\93\end{pmatrix}$

   Or $55=2\times26+3$ donc 55 a pour reste 3 dans la division par 26.
   Et $93=3\times26+15$ donc 93 a pour reste 15 dans la division par 26.
   On passe donc de $\begin{pmatrix}55\\93\end{pmatrix}$ à $\begin{pmatrix}3\\15\end{pmatrix}$, donc le codage de RE représenté par $\begin{pmatrix}17\\4\end{pmatrix}$ conduit à DP représenté par $\begin{pmatrix}3\\15\end{pmatrix}$.

2. Soient x_1, x_2, x'_1, x'_2 quatre nombres entiers compris entre 0 et 25 tels que $\begin{pmatrix}x_1\\x_2\end{pmatrix}$ et $\begin{pmatrix}x'_1\\x'_2\end{pmatrix}$ sont transformés lors du procédé de codage en $\begin{pmatrix}z_1\\z_2\end{pmatrix}$.

   a. Pour transformer $\begin{pmatrix}x_1\\x_2\end{pmatrix}$ par le procédé de codage, on calcule d'abord
   $\begin{pmatrix}3&1\\5&2\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}3x_1+x_2\\5x_1+2x_2\end{pmatrix}$; puis on détermine les restes de $3x_1+x_2$ et de $5x_1+2x_2$ dans la division par 26.
   D'après le texte, on obtient $\begin{pmatrix}z_1\\z_2\end{pmatrix}$ ce qui veut dire que z_1 est le reste de $3x_1+x_2$ dans la division par 26, et que z_2 est le reste de $5x_1+2x_2$ dans cette même division.

Or $\begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix}$ est également transformé en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$, donc z_1 est aussi le reste de $3x'_1 + x'_2$ dans la division par 26, et z_2 le reste de $5x'_1 + 2x'_2$ dans cette même division.

Les nombres $3x_1 + x_2$ et $3x'_1 + x'_2$ ont le même reste z_1 dans la division par 26 donc ils sont congrus modulo 26. Idem pour $5x_1 + 2x_2$ et $5x'_1 + 2x'_2$.

On a donc : $\begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 \quad [26] \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 \quad [26] \end{cases}$

b. $\begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 \quad [26] \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 \quad [26] \end{cases}$

donc $\begin{cases} 2(3x_1 + x_2) \equiv 2\left(3x'_1 + x'_2\right) \quad [26] \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 \quad [26] \end{cases}$

donc $\begin{cases} 6x_1 + 2x_2 \equiv 6x'_1 + 2x'_2 \quad [26] \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 \quad [26] \end{cases}$

donc $x_1 \equiv x'_1 \quad [26]$ (par soustraction).

$\begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 \quad [26] \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 \quad [26] \end{cases}$

donc $\begin{cases} 5(3x_1 + x_2) \equiv 5\left(3x'_1 + x'_2\right) \quad [26] \\ 3(5x_1 + 2x_2) \equiv 3\left(5x'_1 + 2x'_2\right) \quad [26] \end{cases}$

donc $\begin{cases} 15x_1 + 5x_2 \equiv 15x'_1 + 5x'_2 \quad [26] \\ 15x_1 + 6x_2 \equiv 15x'_1 + 6x'_2 \quad [26] \end{cases}$

donc $x_2 \equiv x'_2 \quad [26]$ (par soustraction).

Donc $x_1 \equiv x'_1 \quad [26]$ et $x_2 \equiv x'_2 \quad [26]$.

On a : $\left.\begin{array}{r} x_1 \equiv x'_1 \quad [26] \\ 0 \leqslant x_1 \leqslant 25 \\ 0 \leqslant x'_1 \leqslant 25 \end{array}\right\} \Longrightarrow x_1 = x'_1$

et $\left.\begin{array}{r} x_2 \equiv x'_2 \quad [26] \\ 0 \leqslant x_2 \leqslant 25 \\ 0 \leqslant x'_2 \leqslant 25 \end{array}\right\} \Longrightarrow x_2 = x'_2$

Il n'y a donc qu'un couple d'entiers de $[0;25]$ $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ qui se code en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$.

3. On souhaite trouver une méthode de décodage pour le bloc DP :

a. Soit la matrice $C' = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$.

$C \times C' = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} = \begin{pmatrix} 3\times 2 + 1\times(-5) & 3\times(-1) + 1\times 3 \\ 5\times 2 + 2\times(-5) & 5\times(-1) + 2\times 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Donc C est inversible et C' est la matrice inverse de C.

b. $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}\begin{pmatrix} 3 \\ 15 \end{pmatrix} = \begin{pmatrix} 2\times 3 + (-1)\times 15 \\ (-5)\times 3 + 3\times 15 \end{pmatrix} = \begin{pmatrix} -9 \\ 30 \end{pmatrix}$ donc $\begin{cases} y_1 = -9 \\ y_2 = 30 \end{cases}$

c. Soit $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ tel que $\begin{cases} x_1 \equiv y_1 \quad [26] \text{ avec } 0 \leqslant x_1 \leqslant 25 \\ x_2 \equiv y_2 \quad [26] \text{ avec } 0 \leqslant x_2 \leqslant 25 \end{cases}$

autrement dit $\begin{cases} x_1 \equiv -9 \quad [26] \text{ avec } 0 \leqslant x_1 \leqslant 25 \\ x_2 \equiv 30 \quad [26] \text{ avec } 0 \leqslant x_2 \leqslant 25 \end{cases}$

Or $\begin{cases} -9 \equiv 17 \quad (26) \text{ avec } 0 \leqslant 17 \leqslant 25 \\ 30 \equiv 4 \quad (26) \text{ avec } 0 \leqslant 4 \leqslant 25 \end{cases}$ donc $\begin{cases} x_1 = 17 \\ x_2 = 4 \end{cases}$

d. On peut penser que le décodage d'un couple de lettres se fait de la même manière que son codage en remplaçant la matrice C par la matrice C'.

4. Dans cette question nous allons généraliser ce procédé de décodage.

On considère un bloc de deux lettres et on appelle z_1 et z_2 les deux entiers compris entre 0 et 25 associés à ces lettres à l'étape 3. On cherche à trouver deux entiers x_1 et x_2 compris entre 0 et 25 qui donnent la matrice colonne $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ par les étapes 2 et 3 du procédé de codage.

Soient y'_1 et y'_2 tels que $\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix} = C' \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$

$\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 2z_1 - z_2 \\ -5z_1 + 3z_2 \end{pmatrix}$ donc $\begin{cases} y'_1 = 2z_1 - z_2 \\ y'_2 = -5z_1 + 3z_2 \end{cases}$

Soient x_1 et x_2, les nombres entiers tels que $\begin{cases} x_1 \equiv y'_1 \quad [26] \text{ avec } 0 \leqslant x_1 \leqslant 25 \\ x_2 \equiv y'_2 \quad [26] \text{ avec } 0 \leqslant x_2 \leqslant 25 \end{cases}$

$3x_1 + x_2 \equiv 3y'_1 + y'_2 \equiv 3(2z_1 - z_2) + (-5z_1 + 3z_2) \equiv 6z_1 - 3z_2 - 5z_1 + 3z_2 \equiv z_1 \quad [26]$

$5x_1 + z_2 \equiv 5y'_1 + 2y'_2 \equiv 5(2z_1 - z_2) + 2(-5z_1 + 3z_2) \equiv 10z_1 - 5z_2 - 10z_1 + 6z_2 \equiv z_2 \quad [26]$

On peut donc dire : $\begin{cases} 3x_1 + x_2 \equiv z_1 \quad [26] \\ 5x_1 + 2x_2 \equiv z_2 \quad [26] \end{cases}$

On a donc décodé la matrice colonne $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ en la multipliant par la matrice C' pour obtenir $\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix}$ puis on a pris les restes module 26 pour obtenir enfin $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

Le système obtenu $\begin{cases} 3x_1 + x_2 \equiv z_1 \quad [26] \\ 5x_1 + 2x_2 \equiv z_2 \quad [26] \end{cases}$ prouve que la matrice $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ se code bien en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ et donc que la matrice $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ se décode bien en $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

5. Les deux lettres QC correspondent à la matrice colonne $\begin{pmatrix} 16 \\ 2 \end{pmatrix}$.

On calcule $C' \times \begin{pmatrix} 16 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 16 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \times 16 + (-1) \times 2 \\ (-5) \times 16 + 3 \times 2 \end{pmatrix} = \begin{pmatrix} 32 - 2 \\ -80 + 6 \end{pmatrix} = \begin{pmatrix} 30 \\ -74 \end{pmatrix}$

$30 = 1 \times 26 + 4$ donc $30 \equiv 4 \quad [26]$ avec $0 \leqslant 4 \leqslant 25$

$74 = 3 \times 26 + 4$ donc $74 \equiv 4 \quad [26]$ avec $0 \leqslant 4 \leqslant 25$

Le nombre 4 correspond à la lettre E donc QC se décode en EE.