<u>Correction Exercice 4:</u> Pour les candidats ayant choisi l'enseignement de spécialité « Mathématiques »

L'objet du problème est l'étude d'une méthode de cryptage, dite « chiffrement de Hill », dans un cas particulier.

Cette méthode nécessite une matrice de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, dont les coefficients sont des nombres entiers choisis entre 0 et 25, et tels que $ad - bc$ soit premier avec 26.

Cette matrice est connue seulement de l'émetteur et du destinataire.

Les deux parties de cet exercice sont indépendantes

Partie A : quelques résultats

1. On considère l'équation (E): $9d - 26m = 1$, où d et m désignent deux entiers relatifs.
   a. Donner une solution simple de cette équation, de sorte que d et m soient des nombres entiers compris entre 0 et 3.

$$\mathbf{9 \times 3 - 26 \times 1 = 27 - 26 = 1}$$

Le couple $(3; 1)$ est une solution particulière de l'équation (E).

   b. Démontrer que le couple (d, m) est solution de l'équation (E) si et seulement si :

$$9(d - 3) = 26(m - 1).$$

$(d ; m)$ solution de $(E) \Leftrightarrow 9d - 26m = 1$ (1)

$(3; 1)$ solution de $(E) \Leftrightarrow 9 \times 3 - 26 \times 1 = 1$ (2)

On soustrait membre à membre (1) et (2).

On obtient alors : $9(d - 3) - 26(m - 1) = 0 \Leftrightarrow 9(d - 3) = 26(m - 1)$ (E')

Si $(d; m)$ solution de l'équation (E') alors : $9d - 27 = 26m - 26$ donc $9d - 26 = 27 - 26 = 1$.

Donc $(d; m)$ est solution de l'équation (E).

   c. En déduire que les solutions de l'équation (E) sont les nombres entiers relatifs de la forme :

$$\begin{cases} d = 26k + 3 \\ m = 9k + 1 \end{cases}, \text{ avec } k \in \mathbb{Z}$$

D'après l'équation (E') 9 divise $26(m-1)$, or 9 et 26 sont premiers entre eux, d'après le théorème de Gauss 9 divise $m-1$.

$9 \mid m-1 \Leftrightarrow \exists\, k \in \mathbb{Z}$ tel que $m-1=9k$

Donc $m=9k+1$.

On remplace $m-1$ dans l'équation (E') :

$$9(d-3)=26\times 9k \Leftrightarrow d-3=26k$$

Donc $d=26k+3$.

Réciproquement si $\begin{cases} d=26k+3 \\ m=9k+1 \end{cases}$ solution de (E') alors :

$$9(26k+3)-26(9k+1)=234k+27-234k-26=1$$

Donc $(d;m)$ solution de (E).

Les solutions de (E) sont de la forme : $\begin{cases} d=26k+3 \\ m=9k+1 \end{cases}$, $k \in \mathbb{Z}$.

2. a. Soit n un nombre entier. Démontrer que si $n=26k-1$, avec k entier relatif, alors n et 26 sont premiers entre eux.

$$n=26k+1 \Leftrightarrow -n+26k=1$$

Donc $n\times(-1)+26\times k=1 \Leftrightarrow n\times u+26\times v=1$

On a alors $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$, d'après le théorème de Bézout les nombres n et 26 sont premiers entre eux.

b. En déduire que les nombres $9d-28$, avec $d=26k+3$ et $k \in \mathbb{Z}$, sont premiers avec 26.

$$9d-28=9(26k+3)-28$$

$$9d-28=9\times 26k+27-28$$

$$9d-28=9\times 26k-1$$

On pose $9k=k' \in \mathbb{Z}$ alors $9d-28=26k'-1$.
D'après la question précédente, $26k'-1$ et 26 sont premiers entre eux, donc les nombres $9d-28$ sont premiers avec 26.

PARTIE B : cryptage et décryptage

On considère la matrice $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$.

On utilisera le tableau suivant pour la correspondance entre les lettres et les nombres.

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

Méthode de cryptage (pour un mot comportant un nombre pair de lettres)	**Exemple : avec le mot MATH**	
1. On regroupe les lettres par paires.	MA	TH
2. On remplace les lettres par les valeurs associées à l'aide du tableau précédent, et on place les couples de nombres obtenus dans des matrices colonne.	$C_1 = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$	$C_2 = \begin{pmatrix} 19 \\ 7 \end{pmatrix}$
3. On multiplie les matrices colonne par la gauche par la matrice $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$	$AC_1 = \begin{pmatrix} 108 \\ 84 \end{pmatrix}$	$AC_2 = \begin{pmatrix} 199 \\ 154 \end{pmatrix}$
4. On remplace chaque coefficient des matrices colonne obtenues par leur reste dans la division euclidienne par 26.	$108 = 4 \times 26 + 4$ $84 = 3 \times 26 + 6$ On obtient : $\begin{pmatrix} 4 \\ 6 \end{pmatrix}$	$\begin{pmatrix} 17 \\ 24 \end{pmatrix}$
5. On utilise le tableau de correspondance entre lettres et nombres pour obtenir le mot crypté.	EGRY	

1. En cryptant par cette méthode le mot « PION », on obtient « LZWH ». En détaillant les étapes pour les lettres « ES », crypter le mot « ESPION ».

- **E correspond au nombre 4**.

S correspond au nombre 18.

Donc $\boldsymbol{C_1 = \begin{pmatrix} 4 \\ 18 \end{pmatrix}}$.

- **On calcule** $\boldsymbol{AC_1 = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix} \times \begin{pmatrix} 4 \\ 18 \end{pmatrix} = \begin{pmatrix} 9 \times 4 + 4 \times 18 \\ 7 \times 4 + 3 \times 18 \end{pmatrix} = \begin{pmatrix} 108 \\ 82 \end{pmatrix}}$

On effectue les divisions euclidiennes de ces coefficients par 26.

- $\mathbf{108 = 4 \times 26 + 4}$ **donc** $\mathbf{108 \equiv 4\ (26)}$

et $\mathbf{82 = 3 \times 26 + 4}$ **donc** $\mathbf{82 \equiv 4\ (26)}$

On obtient alors la matrice $\begin{pmatrix}\mathbf{4}\\\mathbf{4}\end{pmatrix}$**.**

4 correspond à la lettre E.

- **« ESPION » est crypté par le mot « EELZWH »**

2. Méthode de décryptage

Notation : lorsqu'on manipule des matrices de nombres entiers relatifs, on peut utiliser la notation « ≡ » pour parler de congruence coefficient par coefficient. Par exemple, on peut écrire :

$$\begin{pmatrix}108\\84\end{pmatrix} \equiv \begin{pmatrix}4\\6\end{pmatrix} \text{ modulo 26 car } 108 \equiv 4 \text{ modulo 26 et } 84 \equiv 6 \text{ modulo 26.}$$

Soient a, b, x, y, x' et y' des nombres entiers relatifs.
On sait que si $x \equiv x'$ modulo 26 et $y \equiv y'$ modulo 26 alors :
$ax + by \equiv ax' + by'$ modulo 26.

Ce résultat permet d'écrire que, si A est une matrice 2×2, et B et C sont deux matrices colonne 2×1, alors :

$$B \equiv C \text{ modulo 26 implique } AB \equiv AC \text{ modulo 26.}$$

a. Etablir que la matrice A est inversible et déterminer son inverse.

On calcule le déterminant de la matrice A.

Det(A)= $\mathbf{9 \times 3 - 7 \times 4 = 1 \neq 0}$

Donc la matrice A est inversible. A la calculatrice on obtient : $\boldsymbol{A^{-1} = \begin{pmatrix}-3 & 4\\7 & -9\end{pmatrix}}$

On vérifie : $\begin{pmatrix}\mathbf{9} & \mathbf{4}\\\mathbf{7} & \mathbf{3}\end{pmatrix} \times \begin{pmatrix}\mathbf{-3} & \mathbf{4}\\\mathbf{7} & \mathbf{-9}\end{pmatrix} = \boldsymbol{I_2}$

b. Décrypter le mot : XQGY.

- **X correspond au nombre 23**.

Q correspond au nombre 16.

On obtient alors la matrice $\begin{pmatrix}23\\16\end{pmatrix}$.

- **On calcule $A^{-1}\times\begin{pmatrix}23\\16\end{pmatrix}=\begin{pmatrix}-3 & 4\\7 & -9\end{pmatrix}\times\begin{pmatrix}23\\16\end{pmatrix}=\begin{pmatrix}-3\times23+4\times16\\7\times23-9\times16\end{pmatrix}=\begin{pmatrix}-5\\17\end{pmatrix}$**

$\begin{pmatrix}-5\\17\end{pmatrix}\equiv\begin{pmatrix}21\\17\end{pmatrix}$ modulo 26

Donc 21 correspond à la lettre V et 17 correspond à la lettre R.

- **G correspond au nombre 6.**

Y correspond au nombre 24.

On obtient alors la matrice $\begin{pmatrix}6\\24\end{pmatrix}$.

- **On calcule $A^{-1}\times\begin{pmatrix}6\\24\end{pmatrix}=\begin{pmatrix}-3 & 4\\7 & -9\end{pmatrix}\times\begin{pmatrix}6\\24\end{pmatrix}=\begin{pmatrix}-3\times6+4\times24\\7\times6-9\times24\end{pmatrix}=\begin{pmatrix}78\\-174\end{pmatrix}$**

$\begin{pmatrix}78\\-174\end{pmatrix}\equiv\begin{pmatrix}0\\8\end{pmatrix}$ modulo 26

Donc 0 correspond à la lettre A et 8 correspond à la lettre I.

- **XQGY est décrypté par le mot VRAI.**