<u>Exercice 4 (5 points) :</u> Pour les candidats ayant choisi l'enseignement de spécialité « Mathématiques »

<u>A REDIGER SUR FEUILLE SEPAREE</u>

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.
   b. Démontrer que le couple (d, m) est solution de l'équation (E) si et seulement si :
   $$9(d-3) = 26(m-1).$$
   c. En déduire que les solutions de l'équation (E) sont les nombres entiers relatifs de la forme :
   $$\begin{cases} d = 26k + 3 \\ m = 9k + 1 \end{cases}, \text{ avec } k \in \mathbb{Z}$$

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

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.

b. Décrypter le mot : XQGY.