Partie A : quelques résultats

1. On considère l'équation $(E) : 9d - 26m = 1$, où d et m désignent deux entiers relatifs.

a. Les nombres 9 et 26 sont premiers entre eux donc, d'après le théorème de BÉZOUT, l'équation $(E) : 9d - 26m = 1$ admet des solutions entières.
$9 \times 3 - 26 \times 1 = 1$ donc le couple $(3\ ;\ 1)$ est solution de l'équation (E).

b. Le couple $(d\ ;\ m)$ est solution de (E) si et seulement si $9d - 26m = 1$
si et seulement si $9d - 26m = 9 \times 3 - 26 \times 1$
si et seulement si $9(d-3) - 26(m-1) = 0$
si et seulement si $9(d-3) = 26(m-1)$

c. $9(d-3) = 26(m-1)$ donc 9 divise $26(m-1)$. Or 9 et 26 sont premiers entre eux donc, d'apèrs le théorème de GAUSS, 9 divise $m-1$. On peut donc écrire $m-1$ sous la forme $9k$ avec $k \in \mathbf{Z}$. Donc $m = 9k+1$ avec $k \in \mathbf{Z}$.
$9(d-3) = 26(m-1)$ et $m-1 = 9k$ donc $9(d-3) = 26 \times 9k$ ce qui équivaut à $d-3 = 26k$ ou encore $d = 26k+3$ avec $k \in \mathbf{Z}$.
Réciproquement, si $d = 26k+3$ et $m = 9k+1$ avec $k \in \mathbf{Z}$, alors
$9d - 26m = 9(26k+3) - 26(9k+1) = 9 \times 26k + 27 - 26 \times 9k - 26 = 1$ et donc le couple $(d\ ;\ m)$ est solution de (E).
Les solutions de l'équation (E) sont donc les couples $(d\ ;\ m)$ tels que

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

2. **a.** Soit n un nombre entier.
$n = 26k - 1 \iff 26k - n = 1 \iff 26k + n(-1) = 1$
Il existe donc deux entiers relatifs k et -1 tels que $26k + n(-1) = 1$ donc, d'après le théorème de BÉZOUT, les nombres n et 26 sont premiers entre eux.

b. Soit $n = 9d - 28$, avec $d = 26k+3$ et $k \in \mathbf{Z}$.
$n = 9d - 28 = 9(26k+3) - 28 = 9 \times 26k + 27 - 28 = 26(9k) - 1 = 26K - 1$ où $K \in \mathbf{Z}$
D'après la question précédente, on peut déduire que $n = 9d - 28$ et 26 sont premiers entre eux.

Partie B : cryptage et décryptage

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

1. En cryptant par cette méthode le mot « PION », on obtient « LZWH » ; on veut crypter le mot « ESPION ».
Les lettres ES correspondent à la matrice colonne $\begin{pmatrix} 4 \\ 18 \end{pmatrix}$; $\begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix} \times \begin{pmatrix} 4 \\ 18 \end{pmatrix} = \begin{pmatrix} 36+72 \\ 28+54 \end{pmatrix} = \begin{pmatrix} 108 \\ 82 \end{pmatrix}$

$108 = 4 \times 26 + 4$ donc $108 \equiv 4$ modulo 26
$82 = 3 \times 26 + 4$ donc $82 \equiv 4$ modulo 26
donc $\begin{pmatrix} 108 \\ 82 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 4 \end{pmatrix}$ modulo 26 ce qui correspond à EE.
Le mot ESPION se code donc en EELZWH.

2. Méthode de décryptage

a. $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$; $\det(A) = 9 \times 3 - 4 \times 7 = -1 \neq 0$ donc la matrice A est inversible.

On trouve son inverse à la calculatrice : $A^{-1} = \begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix}$

b. Au cryptage, une matrice colonne X correspondant à deux lettres, est d'abord transformée en la matrice Y telle que $AX = Y$. Puis on cherche la matrice Y' composée de nombres entiers entre 0 et 25 et telle que $Y' \equiv Y$ modulo 26.

Au décryptage, on cherche la matrice colonne Y correspondant aux deux lettres à décrypter. Puis on détermine la matrice X telle que $AX = Y$, autrement dit telle que $X = A^{-1}Y$. Enfin on détermine la matrice colonne X' composée des restes des éléments de X modulo 26.

Comme $X \equiv X'$ modulo 26, d'après le texte $AX \equiv AX'$ modulo 26 et donc AX et AX' correspondent à la même matrice colonne Y modulo 26 ; ce qui valide le processus de décryptage.

Pour décrypter les lettres XQ, on cherche la matrice colonne correspondant à ces deux lettres : $\begin{pmatrix} 23 \\ 16 \end{pmatrix}$ puis on multiplie à gauche par la matrice A^{-1}

$\begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix} \times \begin{pmatrix} 23 \\ 16 \end{pmatrix} = \begin{pmatrix} -3 \times 23 + 4 \times 16 \\ 7 \times 23 - 9 \times 16 \end{pmatrix} = \begin{pmatrix} -5 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 17 \end{pmatrix}$ modulo 26 ce qui correspond à VR.

On fait de même avec GY représenté par $\begin{pmatrix} 6 \\ 24 \end{pmatrix}$:

$\begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix} \times \begin{pmatrix} 6 \\ 24 \end{pmatrix} = \begin{pmatrix} -3 \times 6 + 4 \times 24 \\ 7 \times 6 - 9 \times 24 \end{pmatrix} = \begin{pmatrix} 78 \\ -174 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 8 \end{pmatrix}$ modulo 26 ce qui correspond à AI.

Le mot XQGY se décode en VRAI.