Matrices et calcul matriciel
Problème de recherche : le message codé

On numérote les lettres de l'alphabet de 0 à 25 : A= 0, B= 1, …, Z= 25. Pour coder un message, on le découpe en blocs de deux lettres. Chaque bloc de nombres $X = \begin{pmatrix} x \\ y \end{pmatrix}$ est remplacé par le bloc $Y = \begin{pmatrix} x' \\ y' \end{pmatrix}$ où x' et y' sont les restes dans la division par 26 des coefficients de

$$AX \qquad \text{avec} \qquad A = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}.$$

Par exemple, le bloc « MA » donne $X = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$, $AX = \begin{pmatrix} 36 \\ 12 \end{pmatrix}$, donc $Y = \begin{pmatrix} 10 \\ 12 \end{pmatrix}$: « MA » est codé « KM ».

La mission

1. Coder le mot « MATH ».
2. Vous recevez le message « YEDL ». Le décoder.
3. Un camarade propose de coder avec la matrice $B = \begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix}$. Est-ce une bonne idée ?

Pour aller plus loin

À quelle condition sur une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients entiers peut-on espérer décoder les messages ?

Coups de pouce

Bloqué ? Des indices progressifs sont disponibles en ligne. N'en ouvrir qu'un à la fois, et seulement après avoir cherché !