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 !

Éléments de correction

1. Coder « MATH »

« MA » est codé « KM ». « TH » : $X = \begin{pmatrix}19\\7\end{pmatrix}$, $AX = \begin{pmatrix}57+35\\19+14\end{pmatrix} = \begin{pmatrix}92\\33\end{pmatrix}$; $92 = 3\times 26+14$ et $33 = 26+7$, donc $Y = \begin{pmatrix}14\\7\end{pmatrix}$: « OH ». **« MATH » est codé « KMOH ».**

2. Décoder « YEDL »

Il faut « remonter » de Y à X. $\det A = 3\times 2 - 5\times 1 = 1$, donc A est inversible et $A^{-1} = \begin{pmatrix}2 & -5\\-1 & 3\end{pmatrix}$, à coefficients entiers. Si $AX \equiv Y$ (modulo 26 coefficient par coefficient), alors $X = A^{-1}AX \equiv A^{-1}Y$.

— « YE » : $Y = \begin{pmatrix}24\\4\end{pmatrix}$, $A^{-1}Y = \begin{pmatrix}48-20\\-24+12\end{pmatrix} = \begin{pmatrix}28\\-12\end{pmatrix} \equiv \begin{pmatrix}2\\14\end{pmatrix}$: « CO ».

— « DL » : $Y = \begin{pmatrix}3\\11\end{pmatrix}$, $A^{-1}Y = \begin{pmatrix}6-55\\-3+33\end{pmatrix} = \begin{pmatrix}-49\\30\end{pmatrix} \equiv \begin{pmatrix}3\\4\end{pmatrix}$: « DE ».

Le message est **« CODE »** (on vérifie en le recodant).

3. La matrice B

$\det B = 6-4 = 2$. Cherchons deux blocs codés de la même façon : pour $X = \begin{pmatrix}13\\13\end{pmatrix}$ (« NN »), $BX = \begin{pmatrix}78\\52\end{pmatrix} \equiv \begin{pmatrix}0\\0\end{pmatrix}$, comme pour « AA ». Deux blocs différents ayant le même code, **le décodage est impossible** : B est une mauvaise idée.

Pour aller plus loin (enrichissement)

On peut décoder si et seulement si le déterminant $ad-bc$ est inversible modulo 26, c'est-à-dire premier avec 26 : $ad-bc$ doit être **impair et non divisible par 13**. Dans ce cas, A^{-1} s'obtient modulo 26 en multipliant par un inverse de $ad-bc$ modulo 26. C'est le principe du chiffre de Hill (1929).

Ce qu'on a utilisé du chapitre

— Produit d'une matrice par une matrice colonne ; inverse d'une matrice 2×2, déterminant.

— Congruences modulo 26 (chapitre d'arithmétique).