

Un exemple de codage avec des matrices congruentes

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ sont deux matrices.

On dit que $A \equiv A' [5]$ si $a \equiv a' [5]$; $b \equiv b' [5]$; $c \equiv c' [5]$ et $d \equiv d' [5]$.

1/ a/ A et A' sont deux matrices carrées d'ordre 2 telles que $A \equiv A' [5]$.

Z et Z' sont deux matrices à deux ligne et une colonne telles que $Z \equiv Z' [5]$.

Montrer que $A Z \equiv A' Z' [5]$.

b/ A et A' sont deux matrices carrées d'ordre 2 telles que $A \equiv A' [5]$.

B et B' sont deux matrices carrées d'ordre 2 telles que $B \equiv B' [5]$.

Montrer que $A B \equiv A' B' [5]$.

Chaque lettre de l'alphabet est représentée par une matrice colonne déduite de ce tableau :

	0	1	2	3	4
0	A	B	C	D	E
1	F	G	H	I	J
2	K	L	M	N	O
3	P	Q	R	S	T
4	U	V	X	Y	Z

Par exemple, la lettre R est représentée par la matrice $X = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$.

La lettre W est remplacée par deux lettres V.

Pour coder la lettre R, on choisit une matrice carrée, par exemple la matrice $M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, on effectue le produit $M X = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 8 \\ 18 \end{pmatrix}$ puis on calcule, pour chaque terme le reste de la division euclidienne par 5. La lettre R est ainsi codée par la matrice $Y = \begin{pmatrix} 3 \\ 3 \end{pmatrix}$ qui représente la lettre S.

La lettre R est codée par la lettre S.

2 a/ On donne les matrices $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $P = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$. Montrer que $P M \equiv I [5]$.

b/ Une lettre est représentée par la matrice colonne X puis codée par la matrice $Y = M X$.

Montrer que $X \equiv PY [5]$.

À partir de la forme codée Y de la lettre S , on retrouve ainsi la représentation X de la lettre R .

On dit donc que la matrice P permet de décoder un message.

c/ Coder puis décoder le message « D ».

d/ Pour coder un message de plusieurs lettres, par exemple le message « TRUC », on peut utiliser la matrice $\begin{pmatrix} 4 & 2 & 0 & 2 \\ 3 & 3 & 4 & 0 \end{pmatrix}$.

Coder puis décoder le message « OUI ».

3/ On va montrer que la matrice $M = \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}$ ne permet pas de coder le message « L ».

Le message « L » est représenté par la matrice $X = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

a/ Montrer que $MX \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} [5]$.

b/ Montrer par l'absurde qu'il n'existe pas de matrice carrée P qui permette de décoder le message « L » (c'est-à-dire une matrice PM telle que $PM \equiv I [5]$).

Corrigé

$$1/ a/ A Z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

$$A' Z' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a'x' + b'y' \\ c'x' + d'y' \end{pmatrix}.$$

$$a \equiv a' [5] \text{ et } x \equiv x' [5] \text{ donc } ax \equiv a'x' [5].$$

$$\text{On montre de même que } by \equiv b'y' [5], \text{ que } ax + by \equiv a'x' + b'y' [5] \text{ et que } cx + dy \equiv c'x' + d'y' [5]$$

$$\text{On a donc montré que } A Z \equiv A' Z' [5].$$

$$2/ a/ P M = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 10 & 16 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} [5].$$

$$b/ MX = Y \text{ donc } MX \equiv Y [5], \text{ donc } PMX \equiv PY [5], \text{ donc } X \equiv PY [5].$$

$$c/ \text{ La lettre D est représentée par la matrice } X = \begin{pmatrix} 3 \\ 0 \end{pmatrix}.$$

$$\text{La lettre D est codée par la matrice } Y = M X = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 9 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 4 \end{pmatrix} [5].$$

La lettre D est donc codée par la lettre Y.

Maintenant, décodons : $PY = PMX = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 13 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 0 \end{pmatrix} [5]$.

On retrouve la représentation de la lettre D. On a donc décodé la lettre D.

d/ Le message « OUI » est représenté par la matrice $X = \begin{pmatrix} 4 & 0 & 3 \\ 2 & 4 & 1 \end{pmatrix}$.

Le message « OUI » est codé par la matrice $Y = M X = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 4 & 0 & 3 \\ 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 8 & 8 & 5 \\ 20 & 16 & 13 \end{pmatrix} \equiv \begin{pmatrix} 3 & 3 & 0 \\ 0 & 1 & 3 \end{pmatrix} [5]$.

Le message « OUI » est donc codé par le message « DIP ».

Maintenant, décodons : $PMX = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 3 & 3 & 0 \\ 0 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 9 & 10 & 3 \\ 12 & 14 & 6 \end{pmatrix} \equiv \begin{pmatrix} 4 & 0 & 3 \\ 2 & 4 & 1 \end{pmatrix} [5]$.

On retrouve la représentation du message « OUI ».

3/ a/ $MX = \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 5 \\ 10 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} [5]$.

b/ Supposons qu'il existe une matrice P qui permette de décoder la lettre L,

dans ce cas $PMX \equiv X [5]$

donc $PMX \equiv \begin{pmatrix} 1 \\ 2 \end{pmatrix} [5]$.

Ceci est absurde car $MX \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} [5]$ donc $PMX \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} [5]$.