Corrigé

Exercice 4

freemaths.fr

LES MATHÉMATIQUES

AU BACCALAURÉAT S

ARITHMÉTIQUE ET MATRICES, BAC S

- Arithmétique
- PGCD
- Congruence
- Théorème de Gauss
- Théorème de Bézout
- Nombres premiers
- Matrice inversible
- Matrice identité I_2
- Matrice diagonale D
- Matrice inverse P^{-1}
- $M = PDP^{-1}$

EXERCICE 4

[Amérique du Nord 2019]

1. a. a1. Montrons que la lettre " T " est codée par la lettre " U " :

Nous savons que : • la lettre T du message initial correspond à la matrice colonne $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$;

• $M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$.

Dans ces conditions : $\begin{pmatrix} x' \\ y' \end{pmatrix} = M \begin{pmatrix} 4 \\ 3 \end{pmatrix}$ **cad** : $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 10 \\ 24 \end{pmatrix}$.

Or : • le reste de la division euclidienne de x' par 5 est : $r' = 0$;

• le reste de la division euclidienne de y' par 5 est : $t' = 4$.

En utilisant le tableau, nous obtenons comme nouvelle lettre correspondante à la matrice $\begin{pmatrix} r' \\ t' \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \end{pmatrix}$: **la lettre U**.

Ainsi : **oui**, la lettre " T " est bien codée par la lettre " U ".

1. a. a2. Codons le message " TE " :

T correspond à la matrice colonne $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$ et E correspond à la matrice colonne $\begin{pmatrix} 4 \\ 0 \end{pmatrix}$.

Dans ces conditions: • $\begin{pmatrix} x' \\ y' \end{pmatrix} = M \begin{pmatrix} 4 \\ 3 \end{pmatrix}$ **cad**: $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 10 \\ 24 \end{pmatrix}$;

• $\begin{pmatrix} x'' \\ y'' \end{pmatrix} = M \begin{pmatrix} 4 \\ 0 \end{pmatrix}$ **cad**: $\begin{pmatrix} x'' \\ y'' \end{pmatrix} = \begin{pmatrix} 4 \\ 12 \end{pmatrix}$.

Or: • le reste de la division euclidienne de x' par 5 est: $r' = 0$;

• le reste de la division euclidienne de y' par 5 est: $t' = 4$;

• le reste de la division euclidienne de x'' par 5 est: $r'' = 4$;

• le reste de la division euclidienne de y'' par 5 est: $t'' = 2$.

En utilisant le tableau, nous obtenons comme nouveau message correspondant à la matrice carrée $\begin{pmatrix} r' & r'' \\ t' & t'' \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 4 & 2 \end{pmatrix}$: **le message UO**.

Au total après codage, le message " TE " devient: UO.

1. b. Montrons que les matrices PM et $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ sont congrues modulo 5:

$PM = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 10 & 16 \end{pmatrix}$.

Or: • $6 \equiv 1\,[\,5\,]$,

• $10 \equiv 0\,[\,5\,]$,

• $10 \equiv 0\,[\,5\,]$,

• $16 \equiv 1\,[\,5\,]$.

Dans ces conditions: $PM \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} [\,5\,]$.

Et donc: les matrices PM et I sont bien congrues modulo 5.

1. c. Montrons alors que les matrices AZ et A'Z' sont congrues modulo 5:

Nous avons: • $AZ = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$;

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

Alors: $\begin{cases} a \equiv a'\,[\,5\,] \text{ et } x \equiv x'\,[\,5\,] \Rightarrow ax \equiv a'x'\,[\,5\,] \\ b \equiv b'\,[\,5\,] \text{ et } y \equiv y'\,[\,5\,] \Rightarrow by \equiv b'y'\,[\,5\,] \end{cases} \Rightarrow \begin{array}{c} ax + by \\ \equiv \\ a'x' + b'y'. \end{array}$

et: $\begin{cases} c \equiv c'\,[\,5\,] \text{ et } x \equiv x'\,[\,5\,] \Rightarrow cx \equiv c'x'\,[\,5\,] \\ d \equiv d'\,[\,5\,] \text{ et } y \equiv y'\,[\,5\,] \Rightarrow dy \equiv d'y'\,[\,5\,] \end{cases} \Rightarrow \begin{array}{c} cx + dy \\ \equiv \\ c'x' + d'y'. \end{array}$

Donc: les matrices AZ et A'Z' sont bien congrues modulo 5.

1. d. Montrons que si MX et Y sont congrues modulo 5 alors les matrices X et PY sont congrues modulo 5:

Supposons: $MX \equiv Y\,[\,5\,]$

=> $PMX \equiv PY\,[\,5\,]$, d'après les hypothèses de l'énoncé

=> $IX \equiv PY\,[\,5\,]$, car: $PM = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

=> $X \equiv PY\,[\,5\,]$.

Ainsi: si MX et Y sont congrues modulo 5 alors les matrices X et PY sont congrues modulo 5.

1. e. Décodons alors la lettre " D ":

La lettre " D " correspond à la matrice colonne: $Y = \begin{pmatrix} 3 \\ 0 \end{pmatrix}$.

Dans ces conditions, le décodage de la lettre " D " donne: $X = PY$

$$= \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 0 \end{pmatrix}$$

cad: $X = \begin{pmatrix} 9 \\ 12 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 2 \end{pmatrix} [\,5\,]$.

Or $\begin{pmatrix} 4 \\ 2 \end{pmatrix}$ correspond à la lettre " O ", donc: la lettre " D " du message codé est décodée par la lettre " O ".

2. a. Vérifions que $RS \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [\,5\,]$:

Nous avons: $RS = \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 4 & 4 \end{pmatrix} = \begin{pmatrix} 10 & 10 \\ 20 & 20 \end{pmatrix}$.

Or: $10 \equiv 0\,[5]$ et $20 \equiv 0\,[5]$.

D'où: $RS \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5]$.

2. b. Montrons que si c'est le cas alors les matrices TRS et S sont congrues modulo 5:

D'après les propriétés admises à la question **1. c.**, nous pouvons écrire:

$\begin{cases} TR \text{ congrue à } I \text{ modulo } 5 \\ S \text{ congrue à } S \text{ modulo } 5 \end{cases}$ => TRS congrue à IS modulo 5

=> **TRS congrue à S modulo 5**.

Au total si c'est le cas, alors: **oui**, $TRS \equiv S\,[5]$.

2. c. Déduisons-en qu'un message codé par la matrice R ne peut être décodé:

Supposons qu'un message codé par la matrice R peut être décodé.

Alors les matrices TRS et S sont congrues modulo 5: $\mathbf{TRS \equiv S\,[5]}$.

Or: $RS \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5]$, d'après la question **2. a.**

Donc, nous pouvons écrire: $\begin{cases} RS \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5] \\ T \equiv T\,[5] \end{cases}$ => $TRS \equiv T \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5]$

$$\Rightarrow \ TRS \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5].$$

Et nous pouvons conclure par:

$$\begin{cases} TRS \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5] \\ TRS \equiv S [5] \end{cases} \Rightarrow \ S \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} [5].$$

En conclusion, comme $S = \begin{pmatrix} 2 & 2 \\ 4 & 4 \end{pmatrix}$ n'est pas congrue à $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ modulo 5:

effectivement, un message codé par la matrice R ne peut être décodé.