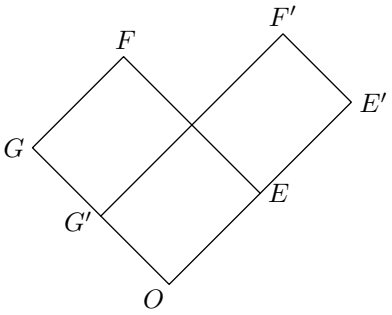
Terminale Option Experte / Annales sur les matrices

1. Matrices et suites

E.1

Un logiciel permet de transformer un élément rectangulaire d'une photographie.
Ainsi, le rectangle initial $OEFG$ est transformé en un rectangle $OE'F'G'$, appelé image de $OEFG$.



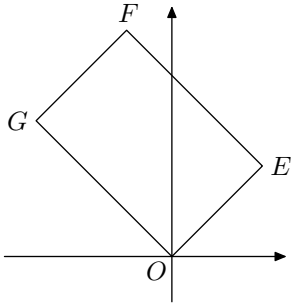
L'objet de cet exercice est d'étudier le rectangle obtenu après plusieurs transformations successives.

Partie A

Le plan est rapporté à un repère orthonormé $\left(O\,;\,\vec{i}\,;\,\vec{j}\right)$.
Les points E, F et G ont pour coordonnées respectives $(2\,;2)$, $(-1\,;5)$ et $(-3\,;3)$.

La transformation du logiciel associe à tout point $M(x\,;y)$ du plan le point $M'(x'\,;y')$, image du point M tel que :

$$\begin{cases} x' = \dfrac{5}{4}x + \dfrac{3}{4}y \\ y' = \dfrac{3}{4}x + \dfrac{5}{4}y \end{cases}$$



1 a Calculer les coordonnées E', F' et G', images des points E, F et G par cette transformation.

b Comparer les longueurs OE et OE' d'une part, OG et OG' d'autre part.
Donner la matrice carrée d'ordre 2, notée A, telle que :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

Partie B

Dans cette partie, on étudie les coordonnées des images successives du sommet F du rectangle $OEFG$ lorsqu'on applique plusieurs fois la transformation du logiciel.

1 On considère l'algorithme suivant destiné à afficher les coordonnées de ces images successives.

Une erreur a été commise.

Modifier cet algorithme pour qu'il permette d'afficher ces coordonnées :

Entrée	Saisir un entier naturel non nul N
Intialisation	Affecter à x la valeur -1 Affecter à y la valeur 5
Traitement	POUR i ALLANT DE 1 A N Affecter à a la valeur $\frac{5}{4}x+\frac{3}{4}y$ Affecter à b la valeur $\frac{3}{4}x+\frac{5}{4}y$ Affecter à x la valeur a Affecter à y la valeur b FIN POUR
Sortie	Afficher x, afficher y

2 On a obtenu le tableau suivant :

i	1	2	3	4	5	10	15
x	2,5	7,25	15,625	31,8125	63,9063	2047,9971	65535,9999
y	5,5	8,75	16,375	32,1875	64,0938	2048,0029	65536,0001

Conjecturer le comportement de la suite des images successives du point F.

Partie C

Dans cette partie, on étudie les coordonnées des images successives du sommet E du rectangle $OEFG$. On définit la suite des points $E_n(x_n\,;y_n)$ du plan par $E_0=E$ et la relation de récurrence :

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A \cdot \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

où $(x_{n+}\,;y_{n+1})$ désignent les coordonnées du point E_{n+1}.
Ainsi, $x_0=2$ et $y_0=2$.

1 On admet que, pour tout entier $n\geqslant 1$, la matrice A^n peut s'écrire sous la forme :

$$A^n = \begin{pmatrix} \alpha_n & \beta_n \\ \beta_n & \alpha_n \end{pmatrix}$$

Démontrer par récurrence que, pour tout entier naturel $n\geqslant 1$, on a :

$$\alpha_n = 2^{n-1} + \frac{1}{2^{n+1}} \quad ; \quad \beta = 2^{n-1} - \frac{1}{2^{n+1}}$$

2 a Démontrer que, pour tout entier naturel n, le point E_n est situé sur la droite d'équation $y=x$.
On pourra utiliser que, pour tout entier naturel n, les coordonnées $(x_n\,;y_n)$ du point E_n vérifient :

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \cdot \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$

b Démontrer que la longueur OE_n tend vers $+\infty$ quand n tend vers $+\infty$.

2. Matrice de transition

E.2 On étudie l'évolution dans le temps du nombre de jeunes et d'adultes d'une population d'animaux. Pour tout entier naturel n, on note j_n le nombre d'animaux jeunes après n années d'observation et a_n le nombre d'animaux adultes après n années d'observation. Il y a au début de la première année de l'étude, 200 animaux jeunes et 500 animaux adultes. Ainsi :

$j_0 = 200$ et $a_0 = 500$.

On admet que pour tout entier naturel n, on a :

$$\begin{cases} j_{n+1} = 0{,}125 \cdot j_n + 0{,}525 \cdot a_n \\ a_{n+1} = 0{,}625 \cdot j_n + 0{,}625 \cdot a_n \end{cases}$$

On introduit les matrices suivantes :

$$A = \begin{pmatrix} 0{,}125 & 0{,}525 \\ 0{,}625 & 0{,}625 \end{pmatrix} \quad ; \quad U_n = \begin{pmatrix} j_n \\ a_n \end{pmatrix}$$

1. a) Montrer que pour entier naturel n : $U_{n+1} = A \times U_n$.

   b) Calculer le nombre d'animaux jeunes et d'animaux adultes après un an d'observation, puis, après deux ans d'observation *(résultats arrondis à l'unité près par défaut)*.

   c) Pour tout entier naturel n non nul, exprimer U_n en fonction de A^n et de U_0.

2. On introduit les matrices suivantes :

$$Q = \begin{pmatrix} 7 & 3 \\ -5 & 5 \end{pmatrix} \quad ; \quad D = \begin{pmatrix} -0{,}25 & 0 \\ 0 & 1 \end{pmatrix}$$

   a) On admet que la matrice Q est inversible et que :

$$Q^{-1} = \begin{pmatrix} 0{,}1 & -0{,}06 \\ 0{,}1 & 0{,}14 \end{pmatrix}$$

   Montrer que : $Q \times D \times Q^{-1} = A$

   b) Montrer, par récurrence sur n, que pour tout entier naturel n non nul :

$$A^n = Q \times D^n \times Q^{-1}$$

   c) Pour tout entier naturel n non nul, déterminer D^n en fonction de n.

3. On admet que pour tout entier naturel n non nul,

$$A^n = \begin{pmatrix} 0{,}3 + 0{,}7 \times (-0{,}25)^n & 0{,}42 - 0{,}42 \times (-0{,}25)^n \\ 0{,}5 - 0{,}5 \times (-0{,}25)^n & 0{,}7 + 0{,}3 \times (-0{,}25)^n \end{pmatrix}$$

   a) En déduire les expressions de j_n et a_n en fonction de n. Déterminer les limites de ces deux suites.

   b) Que peut-on en conclure pour la population d'animaux étudiée?

E.3 Une espèce d'oiseau ne vit que sur deux îles A et B d'un archipel.
Au début de l'année 2013, 20 millions d'oiseaux de cette espèce sont présents sur l'île et 10 millions sur l'île B.

Des observations sur plusieurs années ont permis aux ornithologues d'estimer que, compte tenu des naissances, décès, et migrations entre les deux îles, on retrouve au début de chaque année les propositions suivantes :

- Sur l'île A : 80 % du nombre d'oiseaux présents sur l'île A au début de l'année précédente et 30 % du nombre d'oiseaux présents sur l'île B au début de l'année précédente ;
- sur l'île B : 20 % du nombre d'oiseaux présents sur l'île A au début de l'année précédente et 70 % du nombre d'oiseaux présents sur l'île B au début de l'année précédente.

Pour tout entier naturel n, on note a_n *(respectivement b_n)* le nombre d'oiseaux *(en millions)* présents sur l'île A *(respectivement B)* au début de l'année $(2013+n)$.

Partie A - Algorithmique et conjectures

On donne ci-dessous une fonction `f`, issue d'un algorithme, prenant pour argument un entier `n` supérieur ou égal à 2013 représentant l'année d'étude et renvoyant le nombre d'oiseaux vivant sur chacune des deux îles pour cette année.

```
Fonction f(n)
    a ← 20
    b ← 10
    i ← 2013
    Tant que i<n
        c ← (0,8a+0,3b)
        b ← (0,2a+0,7b)
        a ← c
    Fin Tant que
    Renvoyer (a ; b)
```

1. Le code de la fonction `f` comporte des oublis dans le traitement. Repérer ces oublis et les corriger.

2. On donne ci-dessous un tableau représentant les valeurs successivement prises par les variables de la fonction `f` lors de son exécution pas à pas lors de son appel avec la valeur 2020.

n	a	b
2013	20	10
2014	19	11
2015	18,5	11,5
2016	18,25	11,75
2017	18,125	11,875
2018	18,0425	11,9375
2019	18,03125	11,96875
2020	18,015625	11,984375

   Au vu de ces résultats, émettre des conjectures concernant le sens de variation et la convergence des suites (a_n) et (b_n).

Partie B - Étude mathématique

On note U_n la matrice colonne $\begin{pmatrix} a_n \\ b_n \end{pmatrix}$

1. Montrer que, pour tout entier naturel n :
$U_{n+1} = M \cdot U_n$
où M est une matrice carrée d'ordre 2 que l'on déterminera.

On admet alors que $U_n = M^n \cdot U_0$ pour tout entier naturel $n \geqslant 1$.

2. À l'aide d'un raisonnement par récurrence, justifier que, pour tout entier naturel $n \geqslant 1$:

$$M^n = \begin{pmatrix} 0{,}6 + 0{,}4 \times 0{,}5^n & 0{,}6 - 0{,}6 \times 0{,}5^n \\ 0{,}4 - 0{,}4 \times 0{,}5^n & 0{,}4 + 0{,}6 \times 0{,}5^n \end{pmatrix}$$

On ne détaillera le calcul que pour le premier des coefficients de la matrice M^n.

3. Exprimer a_n en fonction de n, pour tout entier naturel $n \geqslant 1$.

4. Avec ce modèle, peut-on dire qu'au bout d'un grand nombre d'années, le nombre d'oiseaux sur l'île A va se stabiliser? Si oui, préciser vers quelle valeur.

3. Matrice de transition du type : $X = AX + B$

E.4 Un opérateur téléphonique A souhaite prévoir l'évolution de nombre de ses abonnés dans une grande ville par rapport à son principal concurrent B à partir de 2013.
En 2013, les opérateurs A et B ont chacun 300 milliers d'abonnés.

Pour tout entier naturel n, on note a_n le nombre d'abonnés, en milliers, de l'opérateur A la n-ième année après 2013, et b_n le nombre d'abonnés, en milliers, de l'opérateur B la n-ième année après 2013.
Ainsi : $a_0 = 300$ et $b_0 = 300$.

Des observations, réalisées les années précédentes, conduisent à modéliser la situation par la relation suivante :

$$\begin{cases} a_{n+1} = 0{,}7a_n + 0{,}2b_n + 60 \\ b_{n+1} = 0{,}1a_n + 0{,}6b_n + 70 \end{cases}, \text{ pour tout entier } n \in \mathbb{N}.$$

On considère les matrices :

$$M = \begin{pmatrix} 0{,}7 & 0{,}2 \\ 0{,}1 & 0{,}6 \end{pmatrix} \quad ; \quad P = \begin{pmatrix} 60 \\ 70 \end{pmatrix}.$$

Pour tout entier naturel n, on note $U_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$

1. a. Déterminer U_1.
b. Vérifier que, pour tout entier naturel n :
$U_{n+1} = M \times U_n + P$.

2. On note I la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
a. Calculer : $(I - M) \times \begin{pmatrix} 4 & 2 \\ 1 & 3 \end{pmatrix}$.
b. En déduire que la matrice $I - M$ est inversible et préciser son inverse.
c. Déterminer la matrice telle que : $U = M \times U + P$

3. Pour tout entier naturel, on pose : $V_n = U_n - U$.
a. Justifier que, pour tout entier naturel n :
$V_{n+1} = M \times V_n$.
b. En déduire que, pour tout entier naturel n :
$V_n = M^n \times V_0$

4. On admet que, pour tout entier naturel n :

$$V_n = \begin{pmatrix} \frac{-100}{3} \times 0{,}8^n - \frac{140}{3} \times 0{,}5^n \\ \frac{-50}{3} \times 0{,}8^n + \frac{140}{3} \times 0{,}5^n \end{pmatrix}$$

a. Pour tout entier naturel n, exprimer U_n en fonction de n et en déduire la limite de la suite (a_n).
b. Estimer le nombre d'abonnés de l'opérateur A à long terme.

4. Matrices et arithmétique

E.5 **Partie A**

On considère la fonction `f`, extrait d'un algorithme, prenant pour argument un entier naturel `A` et revoyant en fin d'exécution la valeur de la variable `X` :

```
Fonction f(A)
    X ← A
    Tant que X supérieur ou égal à 26
        X ← X−26
    Fin Tant que
    Renvoyer X
```

1. Quelle est la valeur renvoyée par l'appel à la fonction `f` lorsque la valeur fournie en argument est le nombre 3?

2. Quelle est la valeur renvoyée par l'appel à la fonction `f` lorsque la valeur fournie en argument est le nombre 55?

3. Pour un nombre entier saisi quelconque, que représente le résultat renvoyé par cette fonction?

Partie B

On veut coder un bloc de deux lettres selon la procédure suivante *(détaillée en quatre étapes)* :

- **Étape 1** : chaque lettre du bloc est remplacée par un entier en utilisant le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

On obtient une matrice colonne $\begin{pmatrix} x_1 \\ y_2 \end{pmatrix}$ où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

- **Étape 2** : $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$ est transformé en $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ tel que :

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

La matrice $C = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$ est appelée la matrice de codage.

- **Étape 3** : $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ est transformé en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ tel que :

$$\begin{cases} z_1 \equiv y_1 \pmod{26} & \text{avec } 0 \leqslant z_1 \leqslant 25 \\ z_2 \equiv y_2 \pmod{26} & \text{avec } 0 \leqslant z_2 \leqslant 25 \end{cases}$$

- **Étape 4** : $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ est transformé en un bloc de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1

> **Exemple :**
> $\text{RE} \longmapsto \begin{pmatrix} 17 \\ 4 \end{pmatrix} \longmapsto \begin{pmatrix} 55 \\ 93 \end{pmatrix} \longmapsto \begin{pmatrix} 3 \\ 15 \end{pmatrix} \longmapsto \text{DP}$

Justifier le passage de $\begin{pmatrix} 17 \\ 4 \end{pmatrix}$ à $\begin{pmatrix} 55 \\ 93 \end{pmatrix}$, puis, à $\begin{pmatrix} 3 \\ 15 \end{pmatrix}$

(1) Soient x_1, x_2, x'_1, x'_2 quatre nombres entiers compris entre 0 et 25 tels que $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ et $\begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix}$ sont transformés lors du procédé de codage en $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$.

(a) Montrer que $\begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 \pmod{26} \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 \pmod{26} \end{cases}$

(b) En déduire $x_1 \equiv x'_1 \pmod{26}$ et $x_2 \equiv x'_2 \pmod{26}$, puis que $x_1 = x'_1$ et $x_2 = x'_2$.

(2) On souhaite trouver une méthode de décodage pour le bloc DP

(a) Vérifier que la matrice $C' = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$ est la matrice inverse de C.

(b) Calculer $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ tels que : $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ 15 \end{pmatrix}$

(c) Calculer $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ tels que :

$$\begin{cases} x_1 \equiv y_1 \pmod{26} & \text{avec } 0 \leqslant x_1 \leqslant 25 \\ x_2 \equiv y_2 \pmod{26} & \text{avec } 0 \leqslant x_2 \leqslant 25 \end{cases}$$

(d) Quel procédé général de décodage peut-on conjecturer ?

(3) Dans cette question, nous allons généraliser ce procédé de décodage.
On considère un bloc de deux lettres et on appelle z_1 et z_2 les deux entiers compris entre 0 et 25 associés à ces lettres à l'étape **3**. On cherche à trouver deux entiers x_1 et x_2 compris entre 0 et 25 qui donnent la matrice colonne $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ par les étapes **2** et **3** du procédé de codage.

Soient y'_1 et y'_2 tels que :

$$\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix} = C \cdot \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \quad \text{où} \quad C = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$$

Soient x_1 et x_2, les nombres entiers tels que :

$$\begin{cases} x_1 \equiv y'_1 \pmod{26} & \text{avec } 0 \leqslant x_1 \leqslant 25 \\ x_2 \equiv y'_2 \pmod{26} & \text{avec } 0 \leqslant x_2 \leqslant 25 \end{cases}$$

Montrer que :

$$\begin{cases} 3x_1 + x_2 \equiv z_1 \pmod{26} \\ 5x_1 + 2x_2 \equiv z_2 \pmod{26} \end{cases}$$

Conclure.

(4) Décoder QC.

5. *Exercices non-classés*

E.6 Chaque jeune parent utilise chaque mois une seule marque de petits pots pour bébé. Trois marques X, Y et Z se partagent le marché. Soit n un entier naturel.

On note :

- X_n l'événement "*la marque X est utilisée le mois n*" ;
- Y_n l'événement "*la marque Y est utilisée le mois n*" ;
- Z_n l'événement "*la marque Z est utilisée le mois n*" ;

Les probabilités des événements X_n, Y_n, Z_n sont notées respectivement x_n, y_n, z_n.
La campagne publicitaire de chaque marque fait évoluer la répartition :

- Un acheteur de la marque X le mois n a le mois suivant :
  - 50 % de chance de rester fidèle à cette marque.
  - 40 % de chance d'acheter la marque Y.
  - 10 % de chance d'acheter la marque Z.
- Un acheteur de la marque Y le mois n a le mois suivant :
  - 30 % de chance de rester fidèle à cette marque ;
  - 50 % de chance d'acheter la marque X ;
  - 20 % de chance d'acheter la marque Z.
- Un acheteur de la marque Z le mois n a le mois suivant :
  - 70 % de chance de rester fidèle à cette marque ;
  - 10 % de chance d'acheter la marque X ;
  - 20 % de chance d'acheter la marque Y.

(1) (a) Exprimer x_{n+1} en fonction de x_n, y_n et z_n.

On admet que :

$y_{n+1}=0{,}4x_n+0{,}3y_n+0{,}2z_n \quad ; \quad z_{n+1}=0{,}1x_n+0{,}2y_n+0{,}7z_n$

(b) Exprimer z_n en fonction de x_n et y_n. En déduire l'expression de x_{n+1} et y_{n+1} en fonction de x_n et y_n.

(2) On définit la suite (U_n) par $U_n=\begin{pmatrix}x_n\\y_n\end{pmatrix}$ pour tout entier naturel n.

On admet que, pour tout entier naturel n :

$U_{n+1}=A\cdot U_n+B$

où : $A=\begin{pmatrix}0{,}4 & 0{,}4\\0{,}2 & 0{,}1\end{pmatrix}$; $B=\begin{pmatrix}0{,}1\\0{,}2\end{pmatrix}$

Au début de l'étude statistique *(mois de janvier 2014 : $n=0$)*, on estime que :

$U_0=\begin{pmatrix}0{,}5\\0{,}3\end{pmatrix}$

On considère la fonction `f` de l'algorithme suivant :

```
Fonction f(n)
    i ← 0
    A ← [0,4  0,4]
        [0,2  0,1]
    B ← [0,1]
        [0,2]
    U ← [0,5]
        [0,3]
    Tant que i<n
        U ← A· U+B
        i ← i+1
    Fin de Tant que
    Renvoyer U
```

(a) Donner les valeurs renvoyées par cette fonction lorsqu'elle est appelée avec les valeurs `n=1` puis pour `n=3`.

(b) Quelle est la probabilité d'utiliser la marque X au mois d'avril?

Dans la suite de l'exercice, on cherche à déterminer une expression de U_n en fonction de n.

On note I la matrice $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ et N la matrice $I-A$.

(3) On désigne par C une matrice colonne à deux lignes.

(a) Démontrer que $C=A\cdot C+B$ équivaut à $N\cdot C=B$.

(b) On admet que N est une matrice inversible et que :

$$N^{-1}=\begin{pmatrix}\frac{45}{23} & \frac{20}{23}\\\frac{10}{23} & \frac{30}{23}\end{pmatrix}$$

En déduire que : $C=\begin{pmatrix}\frac{17}{46}\\\frac{7}{23}\end{pmatrix}$

(4) On note V_n la matrice telle que $V_n=U_n-C$ pour tout entier naturel n.

(a) Montrer que, pour tout entier naturel n :

$V_{n+1}=A\cdot V_n$

(b) On admet que : $U_n=A^n\cdot(U_0-C)+C$.

Quelles sont les probabilités d'utiliser les marques X, Y et Z au mois de mai?

E.7 Partie A : préliminaires

(1) (a) Soient n et N deux entiers naturels supérieurs ou égaux à 2, tels que : $n^2\equiv N-1 \pmod N$

Montrer que : $n\times n^3\equiv 1 \pmod N$

(b) Déduire de la question précédente un entier k_1 tel que :

$5\cdot k_1\equiv 1 \pmod{26}$

On admettra que l'unique entier k tel que :

$0\leqslant k\leqslant 25 \quad ; \quad 5\cdot k\equiv 1 \pmod{26}$

vaut 21.

(2) On donne les matrices :

$A=\begin{pmatrix}4 & 1\\3 & 2\end{pmatrix}$; $B=\begin{pmatrix}2 & -1\\-3 & 4\end{pmatrix}$; $X=\begin{pmatrix}x_1\\x_2\end{pmatrix}$; $Y=\begin{pmatrix}y_1\\y_2\end{pmatrix}$

(a) Calculer la matrice : $6A-A^2$.

(b) En déduire que A est inversible et que sa matrice inverse, notée A^{-1}, peut s'écrire sous la forme :

$A^{-1}=\alpha\cdot I+\beta\cdot A$

où α et β sont deux réels que l'on déterminera.

(c) Vérifier que : $B=5\cdot A^{-1}$

(d) Démontrer que si $A\cdot X=Y$ alors $5\cdot X=B\cdot Y$.

Partie B : procédure de codage

Coder le mot "*ET*", en utilisant la procédure de codage décrite ci-dessous.

- Le mot à coder est remplacé par la matrice $X=\begin{pmatrix}x_1\\x_2\end{pmatrix}$, où x_1 est l'entier représentant la première lettre du mot et x_2 l'entier représentant la deuxième selon le tableau de correspondance ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- La matrice X est transformée en la matrice $\begin{pmatrix}y_1\\y_2\end{pmatrix}$ telle que : $Y=A\cdot X$.
- La matrice Y est transformée en la matrice $R=\begin{pmatrix}r_1\\r_2\end{pmatrix}$, où r_1 est le reste de la division euclidienne de y_1 par 26 et r_2 le reste de la division euclidienne de y_2 par 26.
- Les entiers r_1 et r_2 donnent les lettres du mot codé, selon le tableau de correspondance ci-dessus.

Exemple :

"*Ou*" *(mot à coder)* $\rightsquigarrow X\begin{pmatrix}14\\20\end{pmatrix}\rightsquigarrow Y=\begin{pmatrix}76\\82\end{pmatrix}$

$\rightsquigarrow R=\begin{pmatrix}24\\4\end{pmatrix}\rightsquigarrow$ "*YE*" *(mot codé)*

Partie C : procédure de décodage *(on conserve les mêmes notations que pour le codage)*

Lors du codage, la matrice X a été transformée en la matrice $Y=\begin{pmatrix}y_1\\y_2\end{pmatrix}$ telle que : $Y=A\cdot X$

1. Démontrer que : $\begin{cases} 5\cdot x_1 = 2\cdot y_1 - y_2 \\ 5\cdot x_2 = -3\cdot y_1 + 4\cdot y_2 \end{cases}$

2. En utilisant la question 1 b de la partie **A**, établir que :
$$\begin{cases} x_1 \equiv 16\cdot y_1 + 5\cdot y_2 \pmod{26} \\ x_2 \equiv 15\cdot y_1 + 6\cdot y_2 \pmod{26} \end{cases}$$

3. Décoder le mot "*QP*".

E.8

Le but de cet exercice est d'étudier, sur un exemple, une méthode de chiffrement publiée en 1929 par le mathématicien et cryptologue Lester Hill. Ce chiffrement repose sur la donnée d'une matrice A, connue uniquement de l'émetteur et du destinataire.

Dans tout l'exercice, on note A la matrice définie par :
$$A = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix}$$

Partie A - Chiffrement de Hill

Voici les différentes étapes de chiffrement pour un mot comportant un nombre pair de lettres :

- **Étape 1 :**
  On divise le mot en blocs de deux lettres consécutives puis, pour chaque bloc, on effectue chacune des étapes suivantes.
- **Étape 2 :**
  On associe aux deux lettres du bloc les deux entiers x_1 et x_2 tous deux compris entre 0 et 25, qui correspondent aux deux lettres dans le même ordre, dans le tableau suivant :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **Étape 3 :**

On transforme la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ en la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ vérifiant $Y = A\cdot X$.

- **Étape 4 :**

On transforme la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ en la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$, où r_1 est le reste de la division euclidienne de y_1 par 26 et r_2 celui de la division euclidienne de y_2 par 26.

- **Étape 5 :**
  On associe aux entiers r_1 et r_2 les deux lettres correspondantes du tableau de l'étape 2.
  Le bloc chiffré est le bloc obtenu en juxtaposant ces deux lettres.

Question : utiliser la méthode de chiffrement exposée pour chiffrer le mot "*HILL*".

Partie B - Quelques outils mathématiques nécessaires au déchiffrement

1. Soit a un entier relatif premier avec 26.
   Démontrer qu'il existe un entier relatif u tel que :
   $u\times a \equiv 1 \pmod{26}$.

2. On considère la fonction `f` d'un algorithme prenant pour argument un entier naturel `a` premier avec 26.

```
Fonction f(a)
    u ← 0
    r ← 0
    Tant que  r≠ 1
        u ←  u+1
        r ← reste de la division euclidienne
                de  u× a par 26
    Fin du Tant que
    Renvoyer u
```

On appelle la fonction `f` avec la valeur du paramètre `a=21`.

a. Reproduire sur la copie et compléter le tableau suivant, avec les différentes valeurs prises par les variables `u` et `v` lors de l'appel à la fonction `f`.

u	0	1	2	...
r	0	21	...	...

b. En déduire que : $5\times 21 \equiv 1 \pmod{26}$.

3. On rappelle que A est la matrice $A = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix}$ et on note I la matrice : $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

a. Calculer la matrice : $12\cdot A - A^2$.

b. En déduire la matrice B telle que : $B\cdot A = 21\cdot I$

c. Démontrer que si $A\cdot X = Y$ alors $21\cdot X = B\cdot Y$.

Partie C - Déchiffrement

On veut déchiffrer le mot $VLUP$.

On note $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ la matrice associée, selon le tableau de correspondance, à un bloc de deux lettres avant chiffrement, et $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ la matrice définie par l'égalité :
$$Y = A\cdot X = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix}\cdot X$$

Si r_1 et r_2 sont les restes respectifs de y_1 et y_2 dans la division euclidienne par 26, le bloc de deux lettres après chiffrement est associé à la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$.

1. Démontrer que : $\begin{cases} 21\cdot x_1 = 7\cdot y_1 - 2\cdot y_2 \\ 21\cdot x_2 = -7\cdot y_1 + 5\cdot y_2 \end{cases}$

2. En utilisant la question **B** 2, établir que :
$$\begin{cases} x_1 \equiv 9\cdot r_1 + 16\cdot r_2 \pmod{26} \\ x_2 \equiv 17\cdot r_1 + 25\cdot r_2 \pmod{26} \end{cases}$$

3. Déchiffrer le mot VLUP, associé aux matrices $\begin{pmatrix} 21 \\ 11 \end{pmatrix}$ et $\begin{pmatrix} 20 \\ 15 \end{pmatrix}$.

E.9 Un fumeur décide d'arrêter de fumer. On choisit d'utiliser la modélisation suivante :

- s'il ne fume pas un jour donné, il ne fume pas le jour suivant avec une probabilité de 0,9 ;
- s'il fume un jour donné, il fume le jour suivant avec une probabilité de 0,6.

On appelle p_n la probabilité de ne pas fumer le n-ième jour après sa décision d'arrêter de fumer et q_n, la probabilité de fumer le n-ième jour après sa décision d'arrêter de fumer.

On suppose que $p_0 = 0$ et $q_0 = 1$.

1. Calculer p_1 et q_1.
2. On utilise un tableur pour automatiser le calcul des termes successifs des suites (p_n) et (q_n). Une copie d'écran de cette feuille de calcul est fournie ci-dessous :

	A	**B**	**C**	**D**
1	n	p_n	q_n	
2	0	0	1	1
3	1			
4	2			
5	3			

Dans la colonne **A** figurent les valeurs de l'entier naturel n.
Quelles formules peut-on écrire dans les cellules `B3` et `C3` de façon qu'en les recopiant vers le bas, on obtienne respectivement dans les colonnes `B` et `C` les termes successifs des suites (p_n) et (q_n) ?

3. On définit les matrices M et, pour tout entier naturel n, X_n par :

$$M = \begin{pmatrix} 0{,}9 & 0{,}4 \\ 0{,}1 & 0{,}6 \end{pmatrix} \quad \text{et} \quad X_n = \begin{pmatrix} p_n \\ q_n \end{pmatrix}.$$

On admet que $X_{n+1} = M \cdot X_n$ et que, pour tout entier naturel n, $X_n = M^n \cdot X_0$

On définit les matrices A et B par :

$$A = \begin{pmatrix} 0{,}8 & 0{,}8 \\ 0{,}2 & 0{,}2 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 0{,}2 & -0{,}8 \\ -0{,}2 & 0{,}8 \end{pmatrix}$$

a. Démontrer que : $M = A + 0{,}5 \cdot B$

b. Vérifier que $A^2 = A$ et que :

$$A \cdot B = B \cdot A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

On admet dans la suite que, pour tout entier naturel n strictement positif :
$A^n = A \quad ; \quad B^n = B$.

c. Démontrer que, pour tout entier naturel :
$M^n = A + 0{,}5^n \cdot B$

d. En déduire, que pour tout entier naturel n :
$p_n = 0{,}8 - 0{,}8 \times 0{,}5^n$

e. À long terme, peut-on affirmer avec certitude que le fumeur arrêtera de fumer ?

E.10 Asie Juin 2018