Contrôle du 3-5-2017
Spécialité mathématiques (1 heure)

Une copie préparée à compléter et à rendre est jointe au sujet.

I. (13 points)

On dispose de trois boules indiscernables au toucher numérotées 1, 2, 3 placées dans une urne et de deux pièces équilibrées A et B. Un jeu consiste à tirer plusieurs fois une boule dans l'urne en la remettant chaque fois dans l'urne.
Après chaque tirage, si l'on obtient la boule portant le numéro 1, alors on retourne la pièce A, si l'on obtient la boule portant le numéro 2, alors on retourne la pièce B et si l'on on obtient la boule portant le numéro 3, alors on ne retourne aucune des deux pièces. Au début du jeu, les deux pièces sont du côté face.

Partie 1 (2 points : 1°) 1 point ; 2°) 1 point)

Dans l'algorithme ci-dessous, 0 code le côté face d'une pièce et 1 code le côté pile. Si a code le côté de la pièce A à un instant donné, alors $1-a$ code le côté de la pièce A après l'avoir retournée.
Les variables a, b, n, i, r, s sont des entiers naturels. De plus, la valeur de n saisie en entrée doit être supérieure ou égale à 1.

Entrée :
Saisir n

Initialisation :
a prend la valeur 0
b prend la valeur 0

Traitement :
Pour i allant de 1 à n **Faire**
  r prend la valeur d'un entier aléatoire compris entre 1 et 3 (au sens large)
  Si $r=1$
    Alors a prend la valeur $1-a$
  FinSi
  Si $r=2$
    Alors b prend la valeur $1-b$
  FinSi
FinPour

Sortie :
s prend la valeur $a+b$
Afficher s

1°) On exécute cet algorithme en saisissant la valeur 3 pour n en entrée et en supposant que les valeurs aléatoires générées successivement pour r sont 2, 3 et 1.
Quelle est la valeur de s affichée en sortie ?
On pourra recopier et compléter le tableau donné ci-contre contenant l'état des variables i, r, a, b au cours de l'exécution de l'algorithme (il est demandé de ne rien écrire dans le tableau ci-contre).

variables	i	r	a	b
initialisation			0	0
1er passage dans la boucle				
2e passage dans la boucle				
3e passage dans la boucle				

2°) Cet algorithme permet-il de décider si à la fin les deux pièces sont du côté pile ? Répondre par oui ou non sans justifier.

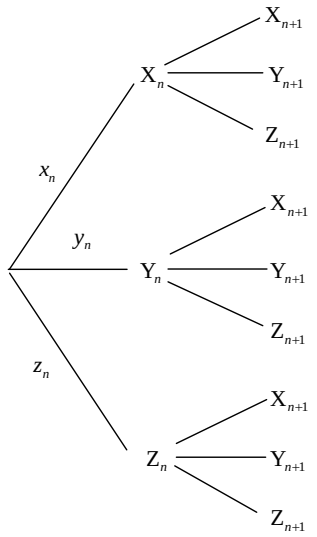
Partie 2 (11 points : 1°) 3 points ; 2°) 2 points ; 3°) 3 points ; 4°) 2 points ; 5°) 1 point)

Pour tout entier naturel n, on note :
- X_n l'événement : « À l'issue de n tirages dans l'urne, les deux pièces sont du côté face » ;
- Y_n l'événement : « À l'issue de n tirages dans l'urne, une pièce est du côté pile et l'autre est du côté face » ;
- Z_n l'événement : « À l'issue de n tirages dans l'urne, les deux pièces sont du côté pile ».

De plus, on note x_n, y_n, z_n les probabilités respectives des événements X_n, Y_n et Z_n. Ainsi, $x_0=1$, $y_0=0$ et $z_0=0$.

On note U_n la matrice colonne $\begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix}$. On a : $U_0=\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

1°) Compléter l'arbre de probabilités ci-dessous en écrivant les probabilités conditionnelles sur les branches partant de X_n, Y_n, Z_n (certaines probabilités peuvent être nulles).



Exprimer x_{n+1} en fonction de x_n, y_n, z_n.
Exprimer y_{n+1} en fonction de x_n, y_n, z_n.
Exprimer z_{n+1} en fonction de x_n, y_n, z_n.

2°) Donner sans explication la matrice M carrée d'ordre 3 telle que pour tout entier naturel n, $U_{n+1} = MU_n$.

3°) On admet que pour tout entier naturel n, on a :

$$M^n = \frac{1}{4}\begin{pmatrix} 1+2\times\left(\frac{1}{3}\right)^n+\left(-\frac{1}{3}\right)^n & 1-\left(-\frac{1}{3}\right)^n & 1-2\times\left(\frac{1}{3}\right)^n+\left(-\frac{1}{3}\right)^n \\ 2-2\times\left(-\frac{1}{3}\right)^n & 2+2\times\left(-\frac{1}{3}\right)^n & 2-2\times\left(-\frac{1}{3}\right)^n \\ 1-2\times\left(\frac{1}{3}\right)^n+\left(-\frac{1}{3}\right)^n & 1-\left(-\frac{1}{3}\right)^n & 1+2\times\left(\frac{1}{3}\right)^n+\left(-\frac{1}{3}\right)^n \end{pmatrix}.$$

Donner les expressions de x_n, y_n, z_n en fonction de n.

4°) Donner les limites de x_n, y_n, z_n lorsque n tend vers $+\infty$.
On justifiera avec soin la limite de x_n et l'on donnera les limites y_n et z_n sans justifier.

5°) Exprimer en fonction de n la probabilité de l'événement E_n : « À l'issue de n tirages dans l'urne, au moins une pièce est du côté pile ».

II. (4 points : 1°) 2 points ; 2°) 2 points)

Un mobile peut occuper deux positions A et B. À chaque seconde, il peut soit rester dans la position dans laquelle il se trouve, soit en changer.
On suppose que :
- si le mobile est dans la position A il y reste avec la probabilité 0,3 et il passe dans la position B avec la probabilité 0,7 ;
- si le mobile est dans la position B il y reste avec la probabilité 0,2 et il passe dans la position A avec la probabilité 0,8.

Faire au brouillon le graphe probabiliste G permettant de modéliser la situation.

1°) Écrire sans justifier la matrice de transition en colonnes M du graphe G.

2°) Vrai ou faux ?

« Après 4 secondes, le mobile a autant de chances d'être dans la position A que d'être dans la position B. »

Répondre sans justifier. On discutera suivant la position initiale du mobile.

III. (4 points : 1°) 1 point ; 2°) a) 1 point ; b) 1 point ; c) 1 point)

On s'intéresse à un procédé de codage qui utilise la matrice $A = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}$.
Cette matrice est connue seulement de l'émetteur et du destinataire.

1°) **Procédure de codage**

Pour coder un mot de deux lettres à l'aide de la matrice A on utilise la procédure ci-après :

Étape 1 : On associe au mot la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ où x_1 est l'entier correspondant à la première lettre du mot et x_2 l'entier correspondant à la deuxième lettre du mot selon le tableau de correspondance ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Étape 2 : La matrice X est transformée en la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ telle que $Y = AX$.

Étape 3 : La matrice Y est transformée en la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ telle que 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.

Étape 4 : À la matrice R on associe un mot de deux lettres selon le tableau de correspondance de l'étape 1.

Exemple : JE $\rightarrow X = \begin{pmatrix} 9 \\ 4 \end{pmatrix} \rightarrow Y = \begin{pmatrix} 66 \\ 57 \end{pmatrix} \rightarrow R = \begin{pmatrix} 14 \\ 5 \end{pmatrix}$ $\rightarrow$ OF.
Le mot JE est codé en le mot OF.

Coder le mot DO. On détaillera les étapes nécessaires au codage.

2°) **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 telle que $Y = AX$.

On pose $B = \begin{pmatrix} 1 & -1 \\ 7 & 2 \end{pmatrix}$.

a) Démontrer que $BA \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (mod. 26).

b) En observant que $AX \equiv R$ (mod. 26), démontrer que $X \equiv BY$ (mod. 26).

c) Décoder le mot SG. On détaillera les étapes nécessaires au décodage.

TS spé **Prénom :** ……..… **Nom :** …… **Note :**

I. (13 points)

Partie 1 (2 points : 1°) 1 point ; 2°) 1 point)

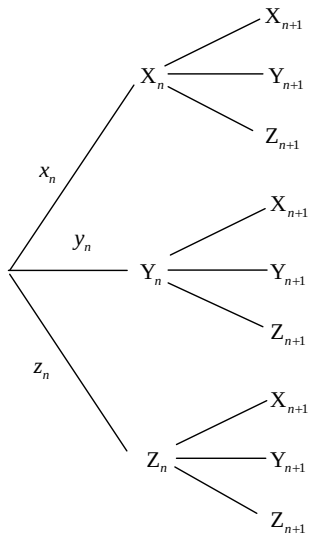
1°) La valeur de *s* affichée en sortie est …….. .

variables	*i*	*r*	*a*	*b*	*s*
initialisation			0	0	
1er passage dans la boucle					
2e passage dans la boucle					
3e passage dans la boucle					

2°) ……

Partie 2 (11 points : 1°) 3 points ; 2°) 2 points ; 3°) 3 points ; 4°) 2 points ; 5°) 1 point)

1°)



Écrire ci-contre une égalité par ligne.

……

……

……

2°)

3°) Écrire une égalité par ligne.

……

……

……

4°) ……

……

……

……

……

……

……

……

……

……

5°) …… (une seule égalité)

II. (4 points : 1°) 2 points ; 2°) 2 points)

1°) 2°) ……

III. (4 points : 1°) 1 point ; 2°) a) 1 point ; b) 1 point ; c) 1 point)

1°) ……

……

……

……

……

……

……

……

……

……

2°)

a) ……

……

……

……

……

……

b) ……

……

……

……

……

……

……

……

c) ……

……

……

……

……

……

……

……

……

Corrigé du contrôle du 3-5-2017
Partie spécialité

I.

On dispose de trois boules indiscernables au toucher numérotées 1, 2, 3 placées dans une urne et de deux pièces équilibrées A et B. Un jeu consiste à tirer plusieurs fois une boule dans l'urne en la remettant chaque fois dans l'urne.
Après chaque tirage, si l'on obtient la boule portant le numéro 1, alors on retourne la pièce A, si l'on obtient la boule portant le numéro 2, alors on retourne la pièce B et si l'on on obtient la boule portant le numéro 3, alors on ne retourne aucune des deux pièces. Au début du jeu, les deux pièces sont du côté face.

Partie 1

Dans l'algorithme ci-dessous, 0 code le côté face d'une pièce et 1 code le côté pile. Si a code le côté de la pièce A à un instant donné, alors $1-a$ code le côté de la pièce A après l'avoir retournée.
Les variables a, b, n, i, r, s sont des entiers naturels. De plus, la valeur de n saisie en entrée doit être supérieure ou égale à 1.

Entrée :
Saisir n

Initialisation :
a prend la valeur 0
b prend la valeur 0

Traitement :
Pour i allant de 1 à n **Faire**
  r prend la valeur d'un entier aléatoire compris entre 1 et 3 (au sens large)
  Si $r=1$
    Alors a prend la valeur $1-a$
  FinSi
  Si $r=2$
    Alors b prend la valeur $1-b$
  FinSi
FinPour

Sortie :
s prend la valeur $a+b$
Afficher s

1°) On exécute cet algorithme en saisissant la valeur 3 pour n en entrée et en supposant que les valeurs aléatoires générées successivement pour r sont 2, 3 et 1.
Quelle est la valeur de s affichée en sortie ?
On pourra recopier et compléter le tableau donné ci-contre contenant l'état des variables i, r, a, b au cours de l'exécution de l'algorithme (il est demandé de ne rien écrire dans le tableau ci-contre).

variables	i	r	a	b
initialisation			0	0
1er passage dans la boucle				
2e passage dans la boucle				
3e passage dans la boucle				

La valeur de s affichée en sortie est 2.

variables	i	r	a	b
initialisation			0	0
1er passage dans la boucle	1	2	0	1
2e passage dans la boucle	2	3	0	1
3e passage dans la boucle	3	1	1	1

2°) Cet algorithme permet-il de décider si à la fin les deux pièces sont du côté pile ? Répondre par oui ou non sans justifier.

oui

À l'issue des tirages, les deux pièces sont du côté pile si et seulement si $s=2$.

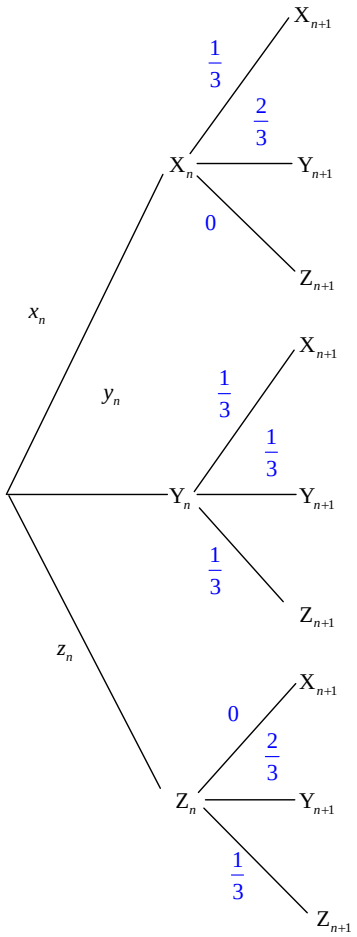
Partie 2

Pour tout entier naturel n, on note :
- X_n l'événement : « À l'issue de n tirages dans l'urne, les deux pièces sont du côté face » ;
- Y_n l'événement : « À l'issue de n tirages dans l'urne, une pièce est du côté pile et l'autre est du côté face » ;
- Z_n l'événement : « À l'issue de n tirages dans l'urne, les deux pièces sont du côté pile ».

De plus, on note x_n, y_n, z_n les probabilités respectives des événements X_n, Y_n et Z_n. Ainsi, $x_0=1$, $y_0=0$ et $z_0=0$.

On note U_n la matrice colonne $\begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix}$. On a : $U_0=\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

1°) Compléter l'arbre de probabilités ci-dessous en écrivant les probabilités conditionnelles sur les branches partant de X_n, Y_n, Z_n (certaines probabilités peuvent être nulles).



Exprimer x_{n+1} en fonction de x_n, y_n, z_n.
Exprimer y_{n+1} en fonction de x_n, y_n, z_n.
Exprimer z_{n+1} en fonction de x_n, y_n, z_n.

X_{n+1} est l'événement « À l'issue de $n+1$ tirages dans l'urne, les deux pièces sont du côté face ».
On cherche donc la probabilité que, à l'issue de $n+1$ lancers, les deux pièces soient du côté face sachant qu'à l'issue de n tirages elles étaient déjà les deux du côté face. Il faut donc qu'il n'y ait aucun retournement de pièce lors du $(n+1)$-ième tirage, c'est-à-dire qu'il faut tirer la boule portant le numéro 3.

La probabilité de l'événement « obtenir la boule portant le numéro 3 » est $\frac{1}{3}$ puisqu'il y a trois boules dans l'urne indiscernables au toucher et donc qu'il y a équiprobabilité.

On en déduit que $P(X_{n+1}/X_n)=\frac{1}{3}$.

On fait de même dans les autres cas.

X_n, Y_n, Z_n forment un système complet d'événements donc d'après la formule des probabilités totales, on a :

$$P(X_{n+1})=P(X_{n+1}\cap X_n)+P(X_{n+1}\cap Y_n)+P(X_{n+1}\cap Z_n)$$
$$P(Y_{n+1})=P(Y_{n+1}\cap X_n)+P(Y_{n+1}\cap Y_n)+P(Y_{n+1}\cap Z_n)$$
$$P(Z_{n+1})=P(Z_{n+1}\cap X_n)+P(Z_{n+1}\cap Y_n)+P(Z_{n+1}\cap Z_n)$$

Ces égalités donnent :

$$x_{n+1}=P(X_n)\times P(X_{n+1}/X_n)+P(Y_n)\times P(X_{n+1}/Y_n)+P(Z_n)\times P(X_{n+1}/Z_n)$$

$$y_{n+1}=P(X_n)\times P(Y_{n+1}/X_n)+P(Y_n)\times P(Y_{n+1}/Y_n)+P(Z_n)\times P(Y_{n+1}/Z_n)$$

$$z_{n+1}=P(X_n)\times P(Z_{n+1}/X_n)+P(Y_n)\times P(Z_{n+1}/Y_n)+P(Z_n)\times P(Z_{n+1}/Z_n)$$

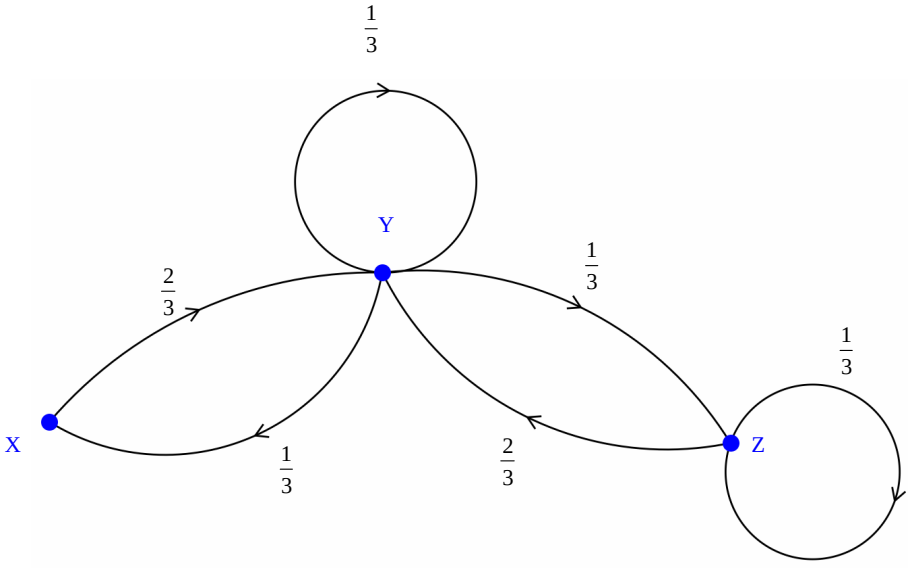
En remplaçant les probabilités conditionnelles par leurs valeurs (lues dans l'arbre de probabilités), on obtient immédiatement les égalités suivantes :

$$x_{n+1}=\frac{x_n}{3}+\frac{y_n}{3}$$
$$y_{n+1}=\frac{2x_n}{3}+\frac{y_n}{3}+\frac{2z_n}{3}$$
$$z_{n+1}=\frac{y_n}{3}+\frac{z_n}{3}$$

On peut aussi écrire ces trois relations sous la forme :

$$x_{n+1}=\frac{x_n+y_n}{3}$$
$$y_{n+1}=\frac{2x_n+y_n+2z_n}{3}$$
$$z_{n+1}=\frac{y_n+z_n}{3}$$

On peut aussi représenter la situation par un graphe probabiliste.
On note X l'état : « Les deux pièces sont du côté face », Y l'état : « Les deux pièces ne sont pas du même côté » et Z l'état : « Les deux pièces sont du côté pile ».



2°) Donner sans explication la matrice M carrée d'ordre 3 telle que pour tout entier naturel n, $U_{n+1} = MU_n$.

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

On peut vérifier le résultat de cette question grâce au résultat admis dans la question suivante où l'on donne l'expression de la matrice M^n en fonction de n. Il suffit de remplacer n par 1.

3°) On admet que pour tout entier naturel n, on a :

$$M^n = \frac{1}{4}\begin{pmatrix} 1+2\times\left(\frac{1}{3}\right)^n+\left(-\frac{1}{3}\right)^n & 1-\left(-\frac{1}{3}\right)^n & 1-2\times\left(\frac{1}{3}\right)^n+\left(-\frac{1}{3}\right)^n \\ 2-2\times\left(-\frac{1}{3}\right)^n & 2+2\times\left(-\frac{1}{3}\right)^n & 2-2\times\left(-\frac{1}{3}\right)^n \\ 1-2\times\left(\frac{1}{3}\right)^n+\left(-\frac{1}{3}\right)^n & 1-\left(-\frac{1}{3}\right)^n & 1+2\times\left(\frac{1}{3}\right)^n+\left(-\frac{1}{3}\right)^n \end{pmatrix}.$$

Donner les expressions de x_n, y_n, z_n en fonction de n.

D'après les questions précédentes, $\forall n \in \mathbb{N} \quad U_n = M^n U_0$.

Or $U_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

En effectuant les calculs, on obtient :

$$x_n = \frac{1}{4}\times\left[1+2\times\left(\frac{1}{3}\right)^n+\left(-\frac{1}{3}\right)^n\right]$$

$$y_n = \frac{1}{4}\times\left[2-2\times\left(-\frac{1}{3}\right)^n\right]$$

$$z_n = \frac{1}{4}\times\left[1-2\times\left(\frac{1}{3}\right)^n+\left(-\frac{1}{3}\right)^n\right]$$

On peut vérifier en effectuant le calcul que l'on a bien $x_n + y_n + z_n = 1$ pour tout entier naturel n.

4°) Donner les limites de x_n, y_n, z_n lorsque n tend vers $+\infty$.
On justifiera avec soin la limite de x_n et l'on donnera les limites y_n et z_n sans justifier.

On a : $\lim\limits_{n\to+\infty}\left(\frac{1}{3}\right)^n = 0$ car $-1<\frac{1}{3}<1$ et $\lim\limits_{n\to+\infty}\left(-\frac{1}{3}\right)^n = 0$ car $-1<-\frac{1}{3}<1$.

On en déduit que $\lim\limits_{n\to+\infty} x_n = \frac{1}{4}$.

On démontre de même que $\lim\limits_{n\to+\infty} y_n = \frac{1}{2}$ et $\lim\limits_{n\to+\infty} z_n = \frac{1}{4}$.

5°) Exprimer en fonction de n la probabilité de l'événement E_n : « À l'issue de n tirages dans l'urne, au moins une pièce est du côté pile ».

$$P(E_n) = \frac{1}{4}\times\left[3-2\times\left(\frac{1}{3}\right)^n-\left(-\frac{1}{3}\right)^n\right]$$

E_n est la réunion des événements Y_n et Z_n.

Comme Y_n et Z_n sont incompatibles, on a $P(E_n) = P(Y_n) + P(Z_n)$ soit $P(E_n) = y_n + z_n$.

On reprend ensuite les expressions de y_n et z_n en fonction de n obtenues à la question précédente.

$$P(E_n) = \frac{1}{4}\times\left[2-2\times\left(-\frac{1}{3}\right)^n\right]+\frac{1}{4}\times\left[1-2\times\left(\frac{1}{3}\right)^n+\left(-\frac{1}{3}\right)^n\right]$$

$$= \frac{1}{4}\times\left[3-2\times\left(\frac{1}{3}\right)^n-\left(-\frac{1}{3}\right)^n\right]$$

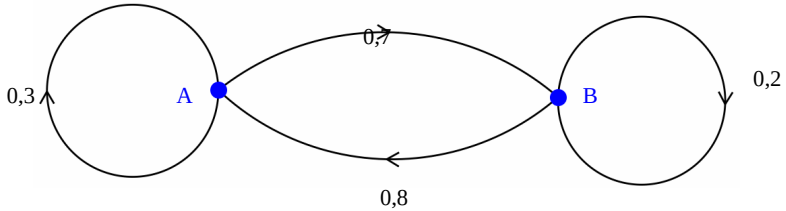
II.

Un mobile peut occuper deux positions A et B. À chaque seconde, il peut soit rester dans la position dans laquelle il se trouve, soit en changer.
On suppose que :
- si le mobile est dans la position A il y reste avec la probabilité 0,3 et il passe dans la position B avec la probabilité 0,7 ;
- si le mobile est dans la position B il y reste avec la probabilité 0,2 et il passe dans la position A avec la probabilité 0,8.

Faire au brouillon le graphe probabiliste *G* permettant de modéliser la situation.

1°) Écrire sans justifier la matrice de transition M en colonnes du graphe *G*.

$$M = \begin{pmatrix} 0,3 & 0,8 \\ 0,7 & 0,2 \end{pmatrix}$$



La matrice M est écrite en prenant les sommets du graphe dans l'ordre logique A-B.

2°) Vrai ou faux ?

« Après 4 secondes, le mobile a autant de chances d'être dans la position A que d'être dans la position B. »

Répondre sans justifier. On discutera suivant la position initiale du mobile.

Pour tout entier naturel *n*, on note P_n la matrice colonne donnant l'état probabiliste au bout de *n* secondes avec la probabilité que le mobile soit en A (coefficient de la première ligne) et la probabilité que le mobile soit en B (coefficient de la deuxième ligne).

On sait que $\forall n \in \mathbb{N} \quad P_n = M^n P_0$.

Donc $P_4 = M^4 P_0 \quad (1)$.

On calcule la matrice M^4 avec la calculatrice.

On obtient $M^4 = \begin{pmatrix} 0,5625 & 0,5 \\ 0,4375 & 0,5 \end{pmatrix}$.

1er cas : Le mobile est initialement dans la position A.

On a donc $P_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

L'égalité (1) donne alors : $P_4 = \begin{pmatrix} 0,5625 \\ 0,4375 \end{pmatrix}$.

Dans ce cas, l'affirmation est donc fausse.

2e cas : Le mobile est initialement dans la position B.

On a donc $P_0 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

L'égalité (1) donne alors : $P_4 = \begin{pmatrix} 0,5 \\ 0,5 \end{pmatrix}$.

Dans ce cas, l'affirmation est donc vraie.

Une élève a essayé de faire un arbre de probabilités à 4 niveaux. Cette méthode est inextricable du point de vue des calculs.

III.

On s'intéresse à un procédé de codage qui utilise la matrice $A = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}$.

Cette matrice est connue seulement de l'émetteur et du destinataire.

1°) **Procédure de codage**

Pour coder un mot de deux lettres à l'aide de la matrice A on utilise la procédure ci-après :

Étape 1 : On associe au mot la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ où x_1 est l'entier correspondant à la première lettre du mot et x_2 l'entier correspondant à la deuxième lettre du mot selon le tableau de correspondance ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Étape 2 : La matrice X est transformée en la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ telle que $Y = AX$.

Étape 3 : La matrice Y est transformée en la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ telle que 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.

Étape 4 : À la matrice R on associe un mot de deux lettres selon le tableau de correspondance de l'étape 1.

Exemple : JE $\rightarrow X = \begin{pmatrix} 9 \\ 4 \end{pmatrix} \rightarrow Y = \begin{pmatrix} 66 \\ 57 \end{pmatrix} \rightarrow R = \begin{pmatrix} 14 \\ 5 \end{pmatrix} \rightarrow$ OF.

Le mot JE est codé en le mot OF.

Coder le mot DO. On détaillera les étapes nécessaires au codage.

Étape 1 : On associe au mot DO la matrice $X = \begin{pmatrix} 3 \\ 14 \end{pmatrix}$ (car la lettre D correspond au nombre 3 et la lettre O correspond au nombre 14).

Étape 2 :

$$\begin{aligned} Y &= AX \\ &= \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} 3 \\ 14 \end{pmatrix} \\ &= \begin{pmatrix} 6\times 3+3\times 14 \\ 5\times 3+3\times 14 \end{pmatrix} \\ &= \begin{pmatrix} 60 \\ 57 \end{pmatrix} \end{aligned}$$

Étape 3 : $60 = 2\times 26+8$ et $57 = 2\times 26+5$

$R = \begin{pmatrix} 8 \\ 5 \end{pmatrix}$

Étape 4 : Le mot DO est codé en IF.

On peut aussi adopter la présentation plus rapide suivante :

$$\text{DO} \rightarrow X = \begin{pmatrix} 3 \\ 14 \end{pmatrix} \rightarrow Y = \begin{pmatrix} 60 \\ 57 \end{pmatrix} \rightarrow R = \begin{pmatrix} 8 \\ 5 \end{pmatrix} \rightarrow \text{IF.}$$

2°) **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 telle que $Y = AX$.

On pose $B = \begin{pmatrix} 1 & -1 \\ 7 & 2 \end{pmatrix}$.

a) Démontrer que $BA \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (mod. 26).

$$\begin{aligned} BA &= \begin{pmatrix} 1 & -1 \\ 7 & 2 \end{pmatrix}\begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 52 & 27 \end{pmatrix} \end{aligned}$$

On a : $1 \equiv 1$ (mod. 26) ; $0 \equiv 0$ (mod. 26) ; $52 \equiv 0$ (mod. 26) ; $27 \equiv 1$ (mod. 26).
On en déduit que $BA \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (mod. 26).

Variante (un peu moins bien) :

$$BA - I_2 = \begin{pmatrix} 1 & 0 \\ 52 & 27 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 26 & 0 \\ 26 & 0 \end{pmatrix}$$

26 divise tous les coefficients de $BA - I_2$ donc $BA \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (mod. 26).

Mise en garde :

On notera que B est l'inverse de la matrice A modulo 26 mais n'est pas l'inverse de A au sens usuel.

On ne peut donc pas l'écrire A^{-1}.

b) En observant que $AX \equiv R$ (mod. 26), démontrer que $X \equiv BY$ (mod. 26).

On considère la relation $AX \equiv R$ (mod. 26) (1).

On utilise les propriétés de la relation de congruence modulo 26 pour les matrices à coefficients entiers relatifs.

$(1) \Leftrightarrow BAX \equiv BR$ (mod.26)

$\Leftrightarrow I_2X \equiv BR$ (mod. 26)

$\Leftrightarrow X \equiv BR$ (mod. 26)

$\Leftrightarrow X \equiv BY$ (mod. 26) (car $R \equiv Y$ (mod. 26))

c) Décoder le mot SG. On détaillera les étapes nécessaires au décodage.

Le mot codé est MI.

La matrice colonne correspondant au mot SG est $Y = \begin{pmatrix} 18 \\ 6 \end{pmatrix}$.

On calcule $BY = \begin{pmatrix} 1 & -1 \\ 7 & 2 \end{pmatrix}\begin{pmatrix} 18 \\ 6 \end{pmatrix} = \begin{pmatrix} 12 \\ 138 \end{pmatrix}$.

En effectuant la division euclidienne de 138 par 26, on obtient aisément $BY \equiv \begin{pmatrix} 12 \\ 8 \end{pmatrix}$ (mod. 26).

Or on a démontré à la question précédente que $X \equiv BY$ (mod. 26).

Donc $X \equiv \begin{pmatrix} 12 \\ 8 \end{pmatrix}$ (mod. 26).

Comme les coefficients de X sont des entiers naturels compris entre 0 et 25 au sens large, on en déduit que $X = \begin{pmatrix} 12 \\ 8 \end{pmatrix}$.

Par suite, le mot cherché est MI.