Ce travail est à rendre pour le Mardi 2 Mai. Vous pouvez vous grouper en binômes.

Exercice I

Un pisciculteur dispose de deux bassins A et B pour l'élevage de ses poissons. Tous les ans à la même période :

— il vide le bassin B et vend tous les poissons qu'il contenait et transfère tous les poissons du bassin A dans le bassin B ;

— la vente de chaque poisson permet l'achat de deux petits poissons destinés au bassin A.
Par ailleurs, le pisciculteur achète en plus 200 poissons pour le bassin A et 100 poissons pour le bassin B.

Pour tout entier naturel supérieur ou égal à 1, on note respectivement a_n et b_n les effectifs de poissons des bassins A et B au bout de n années.
En début de première année, le nombre de poissons du bassin A est $a_0 = 200$ et celui du bassin B est $b_0 = 100$.

1. Justifier que $a_1 = 400$ et $b_1 = 300$ puis calculer a_2 et b_2.

2. On désigne par A et B les matrices telles que $A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 200 \\ 100 \end{pmatrix}$ et pour tout entier naturel n, on pose $X_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

a. Expliquer pourquoi pour tout entier naturel n, $X_{n+1} = AX_n + B$.

b. Déterminer les réels x et y tels que $\begin{pmatrix} x \\ y \end{pmatrix} = A\begin{pmatrix} x \\ y \end{pmatrix} + B$.

c. Pour tout entier naturel n, on pose $Y_n = \begin{pmatrix} a_n + 400 \\ b_n + 300 \end{pmatrix}$.
Démontrer que pour tout entier naturel n, $Y_{n+1} = AY_n$.

3. Pour tout entier naturel n, on pose $Z_n = Y_{2n}$.

a. Démontrer que pour tout entier naturel n, $Z_{n+1} = A^2 Z_n$. En déduire que pour tout entier naturel n, $Z_{n+1} = 2Z_n$.

b. On admet que cette relation de récurrence permet de conclure que pour tout entier naturel n,

$$Y_{2n} = 2^n Y_0.$$

En déduire que $Y_{2n+1} = 2^n Y_1$ puis démontrer que pour tout entier naturel n,

$$a_{2n} = 600 \times 2^n - 400 \quad \text{et} \quad a_{2n+1} = 800 \times 2^n - 400.$$

4. Le bassin A a une capacité limitée à 10 000 poissons.

a. On donne l'algorithme suivant.

Variables :	a, p et n sont des entiers naturels.
Initialisation :	Demander à l'utilisateur la valeur de p.
Traitement :	Si p est pair
	Affecter à n la valeur $\frac{p}{2}$
	Affecter à a la valeur $600 \times 2^n - 400$.
	Sinon
	Affecter à n la valeur $\frac{p-1}{2}$
	Affecter à a la valeur $800 \times 2^n - 400$.
	Fin de Si.
Sortie :	Afficher a.

Que fait cet algorithme ? Justifier la réponse.

b. Écrire un algorithme qui affiche le nombre d'années pendant lesquelles le pisciculteur pourra utiliser le bassin A.

Exercice II

On dispose de deux urnes U et V contenant chacune deux boules. Au départ, l'urne U contient deux boules blanches et l'urne V contient deux boules noires.
On effectue des tirages successifs dans ces urnes de la façon suivante : chaque tirage consiste à prendre au hasard, de manière simultanée, une boule dans chaque urne et à la mettre dans l'autre urne.
Pour tout entier naturel n non nul, on note X_n la variable aléatoire égale au nombre de boules blanches que contient l'urne U à la fin du n-ième tirage.

1. a. Traduire par une phrase la probabilité $P_{(X_n=1)}(X_{n+1}=1)$ puis déterminer les probabilités conditionnelles suivantes :

$$P_{(X_n=0)}(X_{n+1}=1), P_{(X_n=1)}(X_{n+1}=1) \text{ et } P_{(X_n=2)}(X_{n+1}=1).$$

b. Exprimer $P(X_{n+1}=1)$ en fonction de $P(X_n=0)$, $P(X_n=1)$ et $P(X_n=2)$.

2. Pour tout entier naturel n non nul, on note R_n la matrice ligne définie par :

$$R_n = \begin{pmatrix} P(X_n=0) & P(X_n=1) & P(X_n=2) \end{pmatrix}$$

et on considère M la matrice $\begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ 0 & 1 & 0 \end{pmatrix}$.

On note R_0 la matrice ligne $\begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$.

On admettra par la suite que, pour tout entier naturel n, $R_{n+1} = R_n \times M$.

Déterminer R_1 et justifier que, pour tout entier naturel n, $R_n = R_0 \times M^n$.

3. On admet que $M = P \times D \times P^{-1}$ avec :

$$P = \frac{1}{6}\begin{pmatrix} 2 & 3 & 1 \\ -1 & 0 & 1 \\ 2 & -3 & 1 \end{pmatrix},\ D = \begin{pmatrix} -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } P^{-1} = \begin{pmatrix} 1 & -2 & 1 \\ 1 & 0 & -1 \\ 1 & 4 & 1 \end{pmatrix}.$$

Établir que, pour tout entier naturel n, $M^n = P \times D^n \times P^{-1}$.

On admettra que, pour tout entier naturel n, $D^n = \begin{pmatrix} \left(-\frac{1}{2}\right)^n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

4. **a.** Calculer $D^n \times P^{-1}$ en fonction de n.

   b. Sachant que $R_0 P = \begin{pmatrix} \frac{1}{3} & -\frac{1}{2} & \frac{1}{6} \end{pmatrix}$, déterminer les coefficients de R_n en fonction de n.

5. Déterminer $\lim\limits_{n \to +\infty} P(X_n = 0)$, $\lim\limits_{n \to +\infty} P(X_n = 1)$ et $\lim\limits_{n \to +\infty} P(X_n = 2)$.
   Interpréter ces résultats.*

Exercice III

L'objet du problème est l'étude d'une méthode de cryptage, dite « chiffrement de Hill », dans un cas particulier. Cette méthode nécessite une matrice de la forme $\begin{pmatrix} a & b \\ c & s \end{pmatrix}$, dont les coefficients sont des nombres entiers choisis entre 0 et 25, et tels que $ad - bc$ soit premier avec 26.
Cette matrice est connue seulement de l'émetteur et du destinataire.

Les deux parties de cet exercice sont indépendantes

Partie A : quelques résultats

1. On considère l'équation $(E) : 9d - 26m = 1$, où d et m désignent deux entiers relatifs.

   a. Donner une solution simple de cette équation, de sorte que d et m soient des nombres entiers compris entre 0 et 3.

   b. Démontrer que le couple (d, m) est solution de l'équation (E) si et seulement si :

$$9(d-3) = 26(m-1).$$

c. En déduire que les solutions de l'équation (E) sont les nombres entiers relatifs de la forme :

$$\begin{cases} d &= 26k+3 \\ m &= 9k+1 \end{cases}, \quad \text{avec } k \in \mathbb{Z}.$$

2. a. Soit n un nombre entier. Démontrer que si $n = 26k-1$, avec k entier relatif, alors n et 26 sont premiers entre eux.

b. En déduire que les nombres $9d-28$, avec $d = 26k+3$ et $k \in \mathbb{Z}$, sont premiers avec 26.

Partie B : cryptage et décryptage

On considère la matrice $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$.

On utilisera le tableau suivant pour la correspondance entre les lettres et les nombres.

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

Méthode de cryptage (pour un mot comportant un nombre pair de lettres)	**Exemple : avec le mot MATH**	
1. On regroupe les lettres par paires.	MA	TH
2. On remplace les lettres par les valeurs associées à l'aide du tableau précédent, et on place les couples de nombres obtenus dans des matrices colonne.	$C_1 = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$	$C_2 = \begin{pmatrix} 19 \\ 7 \end{pmatrix}$
3. On multiplie les matrices colonne par la gauche par la matrice $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$	$AC_1 = \begin{pmatrix} 108 \\ 84 \end{pmatrix}$	$AC_2 = \begin{pmatrix} 199 \\ 154 \end{pmatrix}$
4. On remplace chaque coefficient des matrices colonne obtenues par leur reste dans la division euclidienne par 26.	$108 = 4 \times 26 + 4$ $84 = 3 \times 26 + 6$ On obtient : $\begin{pmatrix} 4 \\ 6 \end{pmatrix}$	$\begin{pmatrix} 17 \\ 24 \end{pmatrix}$
5. On utilise le tableau de correspondance entre lettres et nombres pour obtenir le mot crypté.	EGRY	

1. En cryptant par cette méthode le mot « PION », on obtient « LZWH ». En détaillant les étapes pour les lettres « ES », crypter le mot « ESPION ».

2. Méthode de décryptage

Notation : lorsqu'on manipule des matrices de nombres entiers relatifs, on peut utiliser la notation « $\equiv$ »pour parler de congruence coefficient par coefficient. Par exemple, on peut écrire :

$$\begin{pmatrix} 108 \\ 84 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 6 \end{pmatrix} \text{ modulo 26 car } 108 \equiv 4 \text{ modulo 26 et } 84 \equiv 6 \text{ modulo 26.}$$

Soient a, b, x, y, x' et y' des nombres entiers relatifs.
On sait que si $x \equiv x'$ modulo 26 et $y \equiv y'$ modulo 26 alors :
$ax + by \equiv ax' + by'$ modulo 26.

Ce résultat permet d'écrire que, si A est une matrice 2×2, et B et C sont deux matrices colonne 2×1, alors :

$$B \equiv C \text{ modulo 26 implique } AB \equiv AC \text{ modulo 26.}$$

a. Établir que la matrice A est inversible, et déterminer son inverse.

b. Décrypter le mot : XQGY.