EXERCICES SUR LES MATRICES ET SUR L'ARITHMÉTIQUES
RÉVISION POUR LE BAC

I. Arithmétique et Matrice

Chiffrement de Hill

Le principe :

On choisit quatre entiers a, b, c et d constituant la **clé** du chiffrement. Les lettres de l'alphabet sont codées de 0 à 25 grâce au tableau suivant : A chaque lettre de l'alphabet, on associe, grâce au tableau ci-dessous, un nombre entier m compris entre 0 et 25.

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

A un bloc de deux lettres correspondent un couple $(x;y)$ d'entiers compris entre 0 et 25. On calcule les codes du message chiffré en associant au couple $(x;y)$ le couple $(x';y')$ tel que :

$$\begin{cases} x' \equiv ax+by \quad (26) \\ y' \equiv cx+dy \quad (26) \end{cases}$$

On souhaite chiffrer le mot DREAM.

On partage le mot en blocs de 2 lettres : DR- EA - MA (le dernier bloc est complété au hasard).

Choisissons $a=5$, $b=7$, $c=2$ et $d=3$, le système de chiffrement est donc :

$$\begin{cases} x' \equiv 7x+3y \quad (26) \\ y' \equiv 5x+8y \quad (26) \end{cases}$$

1. Chiffrer le mot DREAM.
2. On considère la matrice $\mathrm{A} = \begin{pmatrix} 7 & 3 \\ 5 & 8 \end{pmatrix}$.
   (a) Montrer que la matrice A est inversible puis déterminer B telle que $\mathrm{A}^{-1} = \dfrac{1}{41}\mathrm{B}$.
   (b) Montrer qu'il existe un unique entier m compris entre 0 et 25 tel que $41m \equiv 1[26]$. Déterminer m.
   (c) Montrer que la matrice mB est une matrice vérifiant :
   $$m\mathrm{B} \times \begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{pmatrix} x \\ y \end{pmatrix} [26]$$
   (*Cette congruence sur les matrices colonnes signifie la congruence des coefficients de chaque ligne.)*
   (d) Déterminer alors quatre entiers A, B, C et D compris entre 0 et 25 tels que :
   $$\begin{pmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{C} & \mathrm{D} \end{pmatrix} \times \begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{pmatrix} x \\ y \end{pmatrix} [26]$$

(e) En déduire un algorithme de décodage de ce chiffrement de Hill et déchiffrer le message :

« XZEQGCXWCO »

3. Dans le chiffrement précédent, quelle condition particulière sur 41 et 26 permet de répondre à la question 2.(b)
4. On souhaite adopter le chiffrement de Hill donné par le procédé :

$$\begin{cases} x' & \equiv & 6x+2y \quad (26) \\ y' & \equiv & 7x+3y \quad (26) \end{cases}$$

Soit A la matrice associé à ce chiffrement. Calculer le PGCD de detA et de 26.

5. Comparer les produits $\begin{pmatrix} 6 & 2 \\ 7 & 3 \end{pmatrix} \times \begin{pmatrix} x+13 \\ y+13 \end{pmatrix}$ avec $\begin{pmatrix} 6 & 2 \\ 7 & 3 \end{pmatrix} \times \begin{pmatrix} x \\ y \end{pmatrix}$. Le procédé de codage est-il satisfaisant ? Justifier.

Antilles Guyanne 2013

Exercice 1. PARTIE A.

On considère l'algorithme suivant :

```
A et X sont des nombres entiers
Saisir un entier positif A
Affecter à X la valeur de A
Tant que X supérieur ou égal à 26
        Affecter à X la valeur X - 26
Fin du tant que
Afficher X
```

1. Qu'affiche cet algorithme quand on saisit le nombre 3 ?
2. Qu'affiche cet algorithme quand on saisit le nombre 55 ?
3. Pour un nombre entier saisi quelconque, que représente le résultat fourni par cet algorithme ?

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
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

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

• **Étape 2** : $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ est transformé en $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ tel que

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

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

$$\begin{cases} z_1 \equiv y_1 \,(26) \quad \text{avec } 0 \leqslant z_1 \leqslant 25 \\ z_2 \equiv y_2 \,(26) \quad \text{avec } 0 \leqslant z_2 \leqslant 25 \end{cases}$$

• **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 :

$$\text{RE} \to \begin{pmatrix} 17 \\ 4 \end{pmatrix} \to \begin{pmatrix} 55 \\ 93 \end{pmatrix} \to \begin{pmatrix} 3 \\ 15 \end{pmatrix} \to \text{DP}$$

Le bloc RE est donc codé en DP

1. Justifier le passage de $\begin{pmatrix} 17 \\ 4 \end{pmatrix}$ à $\begin{pmatrix} 55 \\ 93 \end{pmatrix}$ puis à $\begin{pmatrix} 3 \\ 15 \end{pmatrix}$.
2. 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 $\begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 \quad (26) \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 \quad (26). \end{cases}$
   (b) En déduire que $x_1 \equiv x'_1 \quad (26)$ et $x_2 \equiv x'_2 \quad (26)$ puis que $x_1 = x'_1$ et $x_2 = x'_2$.
3. 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 $\begin{cases} x_1 \equiv y_1 \quad (26) \text{ avec } 0 \leqslant x_1 \leqslant 25 \\ x_2 \equiv y_2 \quad (26) \text{ avec } 0 \leqslant x_2 \leqslant 25 \end{cases}$

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

4. 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 $\begin{pmatrix} y'_1 \\ y_2 \end{pmatrix} = \text{C}' \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ où $\text{C}' = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$.

   Soient x_1 et x_2, les nombres entiers tels que $\begin{cases} x_1 \equiv y'_1 \quad (26) \text{ avec } 0 \leqslant x_1 \leqslant 25 \\ x_2 \equiv y'_2 \quad (26) \text{ avec } 0 \leqslant x_2 \leqslant 25 \end{cases}$

   Montrer que $\begin{cases} 3x_1 + x_2 \equiv z_1 \quad (26) \\ 5x_1 + 2x_2 \equiv z_2 \quad (26). \end{cases}$.

   Conclure.
5. Décoder QC.

II. Matrice

Exercice 2.

1. Soit $A = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$ et $B = \begin{pmatrix} -2,5 & 1,5 \\ 2 & -1 \end{pmatrix}$. Montrer que B est la matrice inverse de A.
2. Soit $M = \begin{pmatrix} 3 & 3 \\ 4 & 6 \end{pmatrix}$ et $N = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.
   Déterminer la matrice colonne X vérifiant $MX = X + N$

Exercice 3. Soit la matrice carrée $A = \begin{pmatrix} 5 & 1 \\ 3 & 4 \end{pmatrix}$

1. Montrer que A est une matrice inversible.
2. Déterminer la matrice inverse de A.
3. Vérifier votre résultat à l'aide de la calculatrice.

Exercice 4. Soit la matrice $A = \begin{pmatrix} 6,25 & -9 \\ 4,5 & -6,5 \end{pmatrix}$

1. Vérifier que la matrice A est égale au produit des matrices $P \times D \times P^{-1}$ où D désigne la matrice diagonale $D = \begin{pmatrix} 0,25 & 0 \\ 0 & -0,5 \end{pmatrix}$ et où P désigne la matrice inversible $P = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$
2. En déduire les coefficients de la matrice A^n pour tout $n \geq 0$.

Exercice 5. Soit $A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix}$ On souhaite calculer A^n pour n entier naturel.

1. Calculer les premières puissances de A à l'aide d'un logiciel ou d'une calculatrice. Quelle forme particulière remarque-t-on pour ces matrices ?
2. (a) Écrire A sous la forme $2B - I_3$, où I_3 est la matrice identité d'ordre 3 et B une matrice à préciser.
   (b) Montrer que $B^2 = 3B$.
   (c) En déduire A^2 en fonction de B et I_3, puis A^3.
3. Démontrer par récurrence que pour tout n de $\mathbb{N}^*$ on a :

$$A^n = (-1)^n I_3 + \frac{1}{3}\left(5^n - (-1)^n\right) B$$

.

4. Écrire A_n avec tous ces coefficients en fonction de n pour $n \in \mathbb{N}^*$.

Exercice 6. Un complexe industriel est constitué d'une centrale électrique au fioul et d'une raffinerie de pétrole. La centrale utilise pour 1 € d'électricité produite :

- 0.10€ de sa propre consommation d'électricité ;
- 0.40€ de fioul produit par la raffinerie.

La raffinerie utilise pour 1 € de fioul produit :

- 0,30€ d'électricité produite par la centrale ;
- 0,20€ de sa propre production de fioul.

Ces consommations internes empêchent de vendre la totalité des productions d'électricité et de fioul.

But

L'objectif de l'exercice est d'évaluer les productions totales d'électricité et de fioul pour satisfaire une commande de 72000€ d'électricité et de 24000€ de fioul.

1. Notons respectivement p_e et p_f les productions totales (en euros) d'électricité et de fioul. On obtient la matrice colonne des productions $\begin{pmatrix} p_e \\ p_f \end{pmatrix}$.
   On note c_e et c_f respectivement les consommations internes (en euros) d'électricité et de fioul. On obtient la matrice colonne des consommations internes $\begin{pmatrix} c_e \\ c_f \end{pmatrix}$.
   Vérifier que C = LP avec L $\begin{pmatrix} 0.1 & 0.3 \\ 0.4 & 0.2 \end{pmatrix}$
2. Supposons que la production totale est de 80000€ d'électricité et de 50000€ de fioul.
   (a) En utilisant la question 1., calculer la matrice des consommations internes.
   (b) Déduisez-en les productions nettes, c'est-à-dire disponibles pour la vente.
   (c) Cet exemple permet-il de répondre à la question initiale posée dans l'énoncé ?
3. Il s'agit désormais de répondre à la question posée. Notons $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
   (a) La matrice associée à la production nette visée est notée N et donc N = $\begin{pmatrix} 72000 \\ 24000 \end{pmatrix}$.
   Justifier que la matrice P répondant à la question initiale posée vérifie l'égalité $(I_2 - L)P = N$.
   (b) Vérifiez que $I_2 - L = \begin{pmatrix} 0.9 & -0.3 \\ -0.4 & 0.8 \end{pmatrix}$.
   On note $A = \frac{1}{6}\begin{pmatrix} 8 & 3 \\ 4 & 9 \end{pmatrix}$. Calculer $A(I_2 - L)$. Que représente la matrice A pour la matrice $(I_2 - L)$?
   (c) En déduire la matrice P cherchée.

Exercice 7. **Pondichéry 2014**

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'évènement « la marque X est utilisée le mois n »,

Y_n l'évènement « la marque Y est utilisée le mois n »,

Z_n l'évènement « la marque Z est utilisée le mois n ».

Les probabilités des évènements 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 :
   $y_{n+1} = 0,4x_n + 0,3y_n + 0,2z_n$ et que $z_{n+1} = 0,1x_n + 0,2y_n + 0,7z_n$.
   (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, $U_{n+1} = A \times U_n + B$ où $A = \begin{pmatrix} 0,4 & 0,4 \\ 0,2 & 0,1 \end{pmatrix}$ et $B = \begin{pmatrix} 0,1 \\ 0,2 \end{pmatrix}$.

   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 l'algorithme suivant :

Variables	n et i des entiers naturels. A, B et U des matrices
Entrée et initialisation	Demander la valeur de n i prend la valeur 0 A prend la valeur $\begin{pmatrix} 0,4 & 0,4 \\ 0,2 & 0,1 \end{pmatrix}$ B prend la valeur $\begin{pmatrix} 0,1 \\ 0,2 \end{pmatrix}$ U prend la valeur $\begin{pmatrix} 0,5 \\ 0,3 \end{pmatrix}$
Traitement	Tant que $i < n$ U prend la valeur A × U + B i prend la valeur $i+1$ Fin de Tant que
Sortie	Afficher U

(a) Donner les résultats affichés par cet algorithme pour $n = 1$ 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 × C + B équivaut à N × 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, $V_{n+1} = A \times V_n$.

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

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

Exercice 8. **Amérique du sud 2013**

Le gestionnaire d'un site web, composé de trois pages web numérotées de 1 à 3 et reliées entre elles par des liens hypertextes, désire prévoir la fréquence de connexion sur chacune de ses pages web.

Des études statistiques lui ont permis de s'apercevoir que :

- Si un internaute est sur la page 1, alors il ira, soit sur la page 2 avec la probabilité $\frac{1}{4}$, soit sur la page 3 avec la probabilité $\frac{3}{4}$.
- Si un internaute est sur la page 2, alors, soit il ira sur la page 1 avec la probabilité $\frac{1}{2}$ soit il restera sur la page 2 avec la probabilité $\frac{1}{4}$, soit il ira sur la page 3 avec la probabilité $\frac{1}{4}$.
- Si un internaute est sur la page 3, alors, soit il ira sur la page 1 avec la probabilité $\frac{1}{2}$, soit il ira sur la page 2 avec la probabilité $\frac{1}{4}$,soit il restera sur la page 3 avec la probabilité $\frac{1}{4}$.

Pour tout entier naturel n, on définit les évènements et les probabilités suivants :
A_n : « Après la n-ième navigation, l'internaute est sur la page 1 » et on note $a_n = P(A_n)$.
B_n : « Après la n-ième navigation, l'internaute est sur la page 2 » et on note $b_n = P(B_n)$.
C_n : « Après la n-ième navigation, l'internaute est sur la page 3 » et on note $c_n = P(C_n)$.

1. Montrer que, pour tout entier naturel n, on a $a_{n+1} = \frac{1}{2}b_n + \frac{1}{2}c_n$.

   On admet que, de même, $b_{n+1} = \frac{1}{4}a_n + \frac{1}{4}b_n + \frac{1}{4}c_n$ et $c_{n+1} = \frac{3}{4}a_n + \frac{1}{4}b_n + \frac{1}{4}c_n$.

   Ainsi :

$$\begin{cases} a_{n+1} &= \frac{1}{2}b_n + \frac{1}{2}c_n \\ b_{n+1} &= \frac{1}{4}a_n + \frac{1}{4}b_n + \frac{1}{4}c_n \\ c_{n+1} &= \frac{3}{4}a_n + \frac{1}{4}b_n + \frac{1}{4}c_n \end{cases}$$

2. Pour tout entier naturel n, on pose $U_n = \begin{pmatrix} a_n \\ b_n \\ c_n \end{pmatrix}$.

   $U_0 = \begin{pmatrix} a_0 \\ b_0 \\ c_0 \end{pmatrix}$ représente la situation initiale, avec $a_0 + b_0 + c_0 = 1$.

   Montrer que, pour tout entier naturel n, $U_{n+1} = MU_n$ où M est une matrice 3×3 que l'on précisera.

   En déduire que, pour tout entier naturel n, $U_n = M^n U_0$.

3. Montrer qu'il existe une seule matrice colonne $U = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ telle que : $x + y + z = 1$ et $MU = U$.

4. Un logiciel de calcul formel a permis d'obtenir l'expression de M^n, n étant un entier naturel non nul :

$$M^n = \begin{pmatrix} \frac{1}{3} + \frac{\left(\frac{-1}{2}\right)^n \times 2}{3} & \frac{1}{3} + \frac{\left(\frac{-1}{2}\right)^n}{-3} & \frac{1}{3} + \frac{\left(\frac{-1}{2}\right)^n}{-3} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{5}{12} + \frac{\left(-\left(\frac{-1}{2}\right)^n\right) \times 2}{3} & \frac{5}{12} + \frac{-\left(\frac{-1}{2}\right)^n}{-3} & \frac{5}{12} + \frac{-\left(\frac{-1}{2}\right)^n}{-3} \end{pmatrix}$$

Pour tout entier naturel n non nul, exprimer a_n, b_n et c_n en fonction de n. En déduire que les suites (a_n), (b_n) et (c_n) convergent vers des limites que l'on précisera.

5. Interpréter les résultats obtenus et donner une estimation des pourcentages de fréquentation du site à long terme.

Exercice 9. **Métropole 2013**

On étudie la population d'une région imaginaire. Le 1^{er} janvier 2013, cette région comptait 250000 habitants dont 70 % résidaient à la campagne et 30 % en ville.

L'examen des données statistiques recueillies au cours de plusieurs années amène à choisir de modéliser l'évolution de la population pour les années à venir de la façon suivante :

- l'effectif de la population est globalement constant,
- chaque année, 5 % de ceux qui résident en ville décident d'aller s'installer à la campagne et 1 % de ceux qui résident à la campagne choisissent d'aller habiter en ville.

Pour tout entier naturel n, on note v_n le nombre d'habitants de cette région qui résident en ville au 1^{er} janvier de l'année $(2013+n)$ et c_n le nombre de ceux qui habitent à la campagne à la même date.

1. Pour tout entier naturel n, exprimer v_{n+1} et c_{n+1} en fonction de v_n et c_n.
2. Soit la matrice $A = \begin{pmatrix} 0,95 & 0,01 \\ 0,05 & 0,99 \end{pmatrix}$.

   On pose $X = \begin{pmatrix} a \\ b \end{pmatrix}$ où a, b sont deux réels fixés et $Y = AX$.

   Déterminer, en fonction de a et b, les réels c et d tels que $Y = \begin{pmatrix} c \\ d \end{pmatrix}$.

Les résultats précédents permettent d'écrire que pour tout entier naturel n,

$X_{n+1} = AX_n$ où $X_n = \begin{pmatrix} v_n \\ c_n \end{pmatrix}$. On peut donc en déduire que pour tout entier naturel n, $X_n = A^n X_0$.

3. Soient les matrices $P = \begin{pmatrix} 1 & -1 \\ 5 & 1 \end{pmatrix}$ et $Q = \begin{pmatrix} 1 & 1 \\ -5 & 1 \end{pmatrix}$.

(a) Calculer PQ et QP. En déduire la matrice P^{-1} en fonction de Q.

(b) Vérifier que la matrice $P^{-1}AP$ est une matrice diagonale D que l'on précisera.

(c) Démontrer que pour tout entier naturel n supérieur ou égal à 1, $A^n = PD^nP^{-1}$.

4. Les résultats des questions précédentes permettent d'établir que

$$v_n = \frac{1}{6}\left(1 + 5 \times 0,94^n\right) v_0 + \frac{1}{6}\left(1 - 0,94^n\right) c_0.$$

Quelles informations peut-on en déduire pour la répartition de la population de cette région à long terme ?

Exercice 10. **Polynésie 2013**

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 :

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

On considère les matrices $\text{M} = \begin{pmatrix} 0,7 & 0,2 \\ 0,1 & 0,6 \end{pmatrix}$ et $\text{P} = \begin{pmatrix} 60 \\ 70 \end{pmatrix}$.

Pour tout entier naturel n, on note $\text{U}_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

1. (a) Déterminer U_1.
   (b) Vérifier que, pour tout entier naturel n, $\text{U}_{n+1} = \text{M} \times \text{U}_n + \text{P}$.
2. On note I la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
   (a) Calculer $(\text{I} - \text{M}) \times \begin{pmatrix} 4 & 2 \\ 1 & 3 \end{pmatrix}$.
   (b) En déduire que la matrice $\text{I} - \text{M}$ est inversible et préciser son inverse.
   (c) Déterminer la matrice U telle que $\text{U} = \text{M} \times \text{U} + \text{P}$.
3. Pour tout entier naturel, on pose $\text{V}_n = \text{U}_n - \text{U}$.
   (a) Justifier que, pour tout entier naturel n, $\text{V}_{n+1} = \text{M} \times \text{V}_n$.
   (b) En déduire que, pour tout entier naturel n, $\text{V}_n = \text{M}^n \times \text{V}_0$.
4. On admet que, pour tout entier naturel n,

$$\text{V}_n = \begin{pmatrix} \dfrac{-100}{3} \times 0,8^n - \dfrac{140}{3} \times 0,5^n \\ \dfrac{-50}{3} \times 0,8^n + \dfrac{140}{3} \times 0,5^n \end{pmatrix}$$

   (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.

III. Arithmétique

Exercice 11.

Principe Général

1. Alice génère deux gros nombres premiers p et q, ainsi qu'un gros nombre d premier avec $\varphi(n)$.
2. Alice calcule $n = pq$ et cherche e tel que $de \equiv 1[\varphi(n)]$.
3. Alice diffuse n et e, garde en mémoire d et oublie $\varphi(n)$.
4. Bernard crypte un message M par $\mathrm{M} \longmapsto \mathrm{M}^e[n]$ et envoie le résultat à Alice.
5. Alice décode alors le message crypté par $\mathrm{C} \longmapsto \mathrm{C}^d[n]$.

Le but du protocole est bien sûr qu'Alice retrouve le message d'origine. Démontrons que c'est bien le cas. Les transformations appliquées au message sont :

$$\mathrm{M} \longmapsto \mathrm{M}^e[n] \longmapsto \left(\mathrm{M}^e[n]\right)^d[n]$$

On veut donc montrer que $\left(\mathrm{M}^e[n]\right)^d[n] = \mathrm{M}$ c'est-à-dire que :

$$\left(\mathrm{M}^e\right)^d \equiv \mathrm{M}[n] \Longleftrightarrow \mathrm{M}^{de} \equiv \mathrm{M}[n]$$

1. Montrer qu'il existe un entier relatif k tel que : $de = 1 + k\varphi(n)$ En déduire que l'on souhaite démontrer que : $\mathrm{M} \times \mathrm{M}^{k\varphi(n)} \equiv \mathrm{M}[n]$
2. **On suppose que** M **est premier avec** n**.**
   En utilisant le théorème 2 montrer que
   $$\mathrm{M} \times \mathrm{M}^{k\varphi(n)} \equiv \mathrm{M}[n]$$
3. **On suppose que** M **n'est pas premier avec** n**.**
   (a) Donner la liste des diviseurs positifs de n.
   (b) En déduire que M est un multiple de p ou de q.
   Dans le cas où M est un multiple de q on peut écrire que :
   $$\mathrm{M} = p^\alpha m \qquad \text{avec } \alpha \text{ un entier naturel et } m \text{ un entier non multiple de } p$$
   (c) Montrer que m est premier avec n.
   En déduire que $m^{de} \equiv m[n]$.
   (d) Montrer que :
   $$\mathrm{M}^{de} \equiv p^{\alpha de} \times m[n]$$
   Il nous reste à démontrer que $p^{\alpha de} \equiv p^\alpha(n)$.
   (e) Montrer que $p^{\alpha de} \equiv p^\alpha(n)$ est un multiple de p.
   (f) Montrer que
   $$p^{de} = p \times p^{k(p-1)(q-1)}$$
   En déduire en utilisant le petit théorème de Fermat (ou le théorème 2, ce qui revient au même) que :
   $$p^{de} \equiv p[q]$$
   (g) En déduire que $p^{\alpha de} - p^\alpha$ est un multiple de q.
   (h) En déduire, en utilisant Gauss que $p^{\alpha de} - p^\alpha$ est un multiple de n puis conclure.

Exercice 12. Nouvelle-Calédonie mars 2007

Pour coder un message, on procède de la manière suivante : à chacune des 26 lettres de l'alphabet, on commence par associer un entier n de l'ensemble $\Omega = \{0\ ;\ 1\ ;\ 2\ ;\ \ldots\ ;\ 24\ ;\ 25\}$ selon le tableau 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

a et b étant deux entiers naturels donnés, on associe à tout entier n de Ω le reste de la division euclidienne de $(an+b)$ par 26 ; ce reste est alors associé à la lettre correspondante.

Exemple : pour coder la lettre P avec $a = 2$ et $b = 3$, on procède de la manière suivante :

étape 1 : on lui associe l'entier $n = 15$.
étape 2 : le reste de la division de $2 \times 15 + 3 = 33$ par 26 est 7.
étape 3 : on associe 7 à H. Donc P est codé par la lettre H.

1. Que dire alors du codage obtenu lorsque l'on prend $a = 0$?
2. Montrer que les lettres A et C sont codées par la même lettre lorsque l'on choisit $a = 13$.
3. *Dans toute la suite de l'exercice*, on prend $a = 5$ et $b = 2$.
   (a) On considère deux lettres de l'alphabet associées respectivement aux entiers n et p. Montrer, que si $5n+2$ et $5p+2$ ont le même reste dans la division par 26 alors $n - p$ est un multiple de 26. En déduire que $n = p$.
   (b) Coder le mot AMI.
4. On se propose de décoder l a lettre E.
   Montrer que décoder la lettre E revient à déterminer l'élément n de Ω tel que $5n - 26y = 2$, où y est un entier.

Exercice 13. France septembre 2005

1. (a) QCM : On considère dans l'ensemble des entiers relatifs l'équation :

$$x^2 - x + 4 \equiv 0 \quad (6)$$

   A : toutes les solutions sont des entiers pairs.
   B : il n'y a aucune solution.
   C : les solutions vérifient $x \equiv 2 \quad (6)$.
   D : les solutions vérifient $x \equiv 2 \quad (6)$ ou $x \equiv 5 \quad (6)$.

   (b) On considère les deux nombres $n = 1789$ et $p = 1789^{2005}$. On a alors :
   A : $n \equiv 4 \quad (17)$ et $p \equiv 0 \quad (17)$.
   B : p est un nombre premier.
   C : $p \equiv 4 \quad (17)$.
   D : $p \equiv 1 \quad (17)$.

Exercice 14.

1. **R.O.C** : On rappelle que :
   m est un entier naturel non nul. $a \equiv b(m)$ équivaut à $a - b = km$, $k \in \mathbb{Z}$.
   Démontrer que si $a \equiv b(m)$ et si $a' \equiv b'(m)$, alors

$$a + a' \equiv b + b'(m) \qquad \text{et} aa' \equiv bb'(m)$$

2. **Application** : x et y sont deux entiers relatifs. On se propose de résoudre le système :

$$\begin{cases} 3x+y & \equiv & 1 & (6) \\ x-y & \equiv & 3 & (6) \end{cases}$$

(a) i. Démontrer que $4x \equiv 4(m)$.

ii. Déduisez-en, à l'aide d'un tableau donnant les restes modulo 6 que $4x \equiv 4(6) \Longleftrightarrow x \equiv 1(6)$ ou $x \equiv 4(6)$.

(b) En tenant-compte de $y \equiv x-3(6)$, déduisez-en les couples $(x;y)$ solutions du système.

Exercice 15. **Pondichéry 2012**

Partie A Restitution organisée de connaissance

Soit a, b, c, d des entiers relatifs et n un entier naturel non nul.
Montrer que si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $ac \equiv bd \pmod{n}$.

Partie B Inverse de 23 modulo 26

On considère l'équation

$$(\text{E}) : \quad 23x - 26y = 1,$$

où x et y désignent deux entiers relatifs.

1. Vérifier que le couple $(-9\ ;\ -8)$ est solution de l'équation (E).
2. Résoudre alors l'équation (E).
3. En déduire un entier a tel que $0 \leqslant a \leqslant 25$ et $23a \equiv 1 \pmod{26}$.

Partie C Chiffrement de Hill

On veut coder un mot de deux lettres selon la procédure suivante :

Étape 1 Chaque lettre du mot 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 un couple d'entiers $(x_1\ ;\ x_2)$ où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.
Étape 2 $(x_1\ ;\ x_2)$ est transformé en $\left(y_1\ ;\ y_2\right)$ tel que :

$$(\text{S}_1) \begin{cases} y_1 & \equiv & 11x_1+3x_2 & \pmod{26} \\ y_2 & \equiv & 7x_1+4x_2 & \pmod{26} \end{cases} \quad \text{avec } 0 \leqslant y_1 \leqslant 25 \text{ et } 0 \leqslant y_2 \leqslant 25.$$

Étape 3 $\left(y_1\ ;\ y_2\right)$ est transformé en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

Exemple : $\underbrace{\text{TE}}_{\text{mot en clair}} \overset{\text{étape1}}{\Longrightarrow} (19,4) \overset{\text{étape2}}{\Longrightarrow} (13,19) \overset{\text{étape3}}{\Longrightarrow} \underbrace{\text{NT}}_{\text{mot codé}}$

1. Coder le mot ST.
2. On veut maintenant déterminer la procédure de décodage :

(a) Montrer que tout couple $(x_1\,;\,x_2)$ vérifiant les équations du système (S_1), vérifie les équations du système :

$$(S_2)\begin{cases} 23x_1 \equiv 4y_1+23y_2 \pmod{26} \\ 23x_2 \equiv 19y_1+11y_2 \pmod{26} \end{cases}$$

(b) À l'aide de la partie B, montrer que tout couple $(x_1\,;\,x_2)$ vérifiant les équations du système (S_2), vérifie les équations du système

$$(S_3)\begin{cases} x_1 \equiv 16y_1+y_2 \pmod{26} \\ x_2 \equiv 11y_1+5y_2 \pmod{26} \end{cases}$$

(c) Montrer que tout couple $(x_1\,;\,x_2)$ vérifiant les équations du système (S_3), vérifie les équations du système (S_1)

(d) Décoder le mot **YJ**.

Exercice 16. (**Antilles-Guyanne 2012**)

Les trois questions sont indépendantes.

1. (a) Vérifier que le couple $(4\,;6)$ est une solution de l'équation

$$(E) \qquad 11x-5y=14.$$

(b) Déterminer tous les couples d'entiers relatifs (x ; y) vérifiant l'équation (E).

2. (a) Démontrer que, pour tout entier naturel n,

$$2^{3n} \equiv 1 \mod 7.$$

(b) Déterminer le reste de la division euclidienne de 2011^{2012} par 7.

3.

4. On considère l'algorithme suivant où $\text{Ent}\left(\frac{A}{N}\right)$ désigne la partie entière de $\frac{A}{N}$.

A et N sont des entiers naturels Saisir A N prend la valeur 1 Tant que $N \leqslant \sqrt{A}$ Si $\frac{A}{N} - \text{Ent}\left(\frac{A}{N}\right) = 0$ alors Afficher N et $\frac{A}{N}$ Fin si N prend la valeur N + 1 Fin Tant que.

Quels résultats affiche cet algorithme pour A = 12 ?

Que donne cet algorithme dans le cas général ?

Exercice 17. **Polynésie 2012**

PARTIE A.

On considère l'équation (E) : $25x - 108y = 1$ où x et y sont des entiers relatifs.

1. Vérifier que le couple (13 ; 3) est solution de cette équation.
2. Déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E).

PARTIE B.

Dans cette partie, a désigne un entier naturel et les nombres c et g sont des entiers naturels vérifiant la relation $25g - 108c = 1$.

On rappelle le petit théorème de Fermat :

Si p est un nombre premier et a un entier non divisible par p, alors a^{p-1} est congru à 1 modulo p que l'on note $a^{p-1} \equiv 1\ [p]$.

1. Soit x un entier naturel.
   Démontrer que si $x \equiv a\ [7]$ et $x \equiv a\ [19]$, alors $x \equiv a\ [133]$.
2. (a) On suppose que a n'est pas un multiple de 7.
   Démontrer que $a^6 \equiv 1\ [7]$ puis que $a^{108} \equiv 1\ [7]$.
   En déduire que $\left(a^{25}\right)^g \equiv a\ [7]$.
   (b) On suppose que a est un multiple de 7.
   Démontrer que $\left(a^{25}\right)^g \equiv a\ [7]$.
   (c) On admet que pour tout entier naturel a, $\left(a^{25}\right)^g \equiv a\ [19]$.
   Démontrer que $\left(a^{25}\right)^g \equiv a\ [133]$.

PARTIE C.

On note A l'ensemble des entiers naturels a tels que : $1 \leqslant a \leqslant 26$.
Un message, constitué d'entiers appartenant à A, est codé puis décodé.
La phase de codage consiste à associer, à chaque entier a de A, l'entier r tel que $a^{25} \equiv r\ [133]$ avec $0 \leqslant r < 133$.
La phase de décodage consiste à associer à r , l'entier r_1 tel que $r^{13} \equiv r_1\ [133]$ avec $0 \leqslant r_1 < 133$.

1. Justifier que $r_1 \equiv a\ [133]$.
2. Un message codé conduit à la suite des deux entiers suivants : 128 59.
   Décoder ce message.