



Annales 2016 - Spécialité

I Sujet : Bac S – Pondichery – 22 avril 2016

Partie A

On considère les matrices M de la forme $M = \begin{pmatrix} a & b \\ 5 & 3 \end{pmatrix}$ où a et b sont des nombres entiers.

Le nombre $3a - 5b$ est appelé le déterminant de M . On le note $\det(M)$.

Ainsi $\det(M) = 3a - 5b$.

1. Dans cette question on suppose que $\det(M) \neq 0$ et on pose $N = \frac{1}{\det(M)} \begin{pmatrix} 3 & -b \\ -5 & a \end{pmatrix}$.

Justifier que N est l'inverse de M .

2. On considère l'équation (E) : $\det(M) = 3$.

On souhaite déterminer tous les couples d'entiers $(a ; b)$ solutions de l'équation (E).

(a) Vérifier que le couple $(6 ; 3)$ est une solution de (E).

(b) Montrer que le couple d'entiers $(a ; b)$ est solution de (E) si et seulement si $3(a - 6) = 5(b - 3)$.

En déduire l'ensemble des solutions de l'équation (E).

Partie B

1. On pose $Q = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}$.

En utilisant la partie A, déterminer la matrice inverse de Q .

2. Codage avec la matrice Q

Pour coder un mot de deux lettres à l'aide de la matrice $Q = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}$ 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

$$Y = QX.$$

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 est le reste de la division euclidienne de y_2 par 26.

Étape 4 : À la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ on associe un mot de deux lettres selon le tableau de correspondance de l'étape 1.

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

Le mot JE est codé en le mot OF .

Coder le mot DO .

3. 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

$$Y = QX.$$

- (a) Démontrer que $3X = 3Q^{-1}Y$ puis que
$$\begin{cases} 3x_1 \equiv 3r_1 - 3r_2 & [26] \\ 3x_2 \equiv -5r_1 + 6r_2 & [26] \end{cases}$$
- (b) En remarquant que $9 \times 3 \equiv 1 \quad [26]$, montrer que
$$\begin{cases} x_1 \equiv r_1 - r_2 & [26] \\ x_2 \equiv 7r_1 + 2r_2 & [26] \end{cases}$$
- (c) Décoder le mot SG .



II Sujet : Bac S – Liban – 31 mai 2016

Pour chacune des affirmations suivantes, dire si elle est vraie ou fausse en justifiant la réponse. Un point est attribué par réponse exacte justifiée. Une réponse non justifiée ne sera pas prise en compte et l'absence de réponse n'est pas pénalisée.

- On considère le système
$$\begin{cases} n \equiv 1 & [5] \\ n \equiv 3 & [4] \end{cases}$$
 d'inconnue n entier relatif.

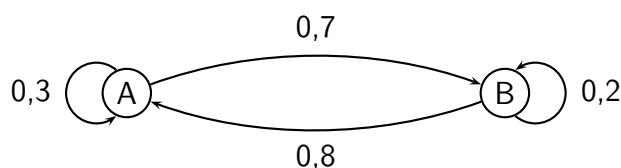
Affirmation 1 : Si n est solution de ce système alors $n - 11$ est divisible par 4 et par 5.

Affirmation 2 : Pour tout entier relatif k , l'entier $11 + 20k$ est solution du système.

Affirmation 3 : Si un entier relatif n est solution du système alors il existe un entier relatif k tel que $n = 11 + 20k$.

- Un automate peut se trouver dans deux états A ou B. À chaque seconde il peut soit rester dans l'état où il se trouve, soit en changer, avec des probabilités données par le graphe probabiliste ci-dessous.

Pour tout entier naturel n , on note a_n la probabilité que l'automate se trouve dans l'état A après n secondes et b_n la probabilité que l'automate se trouve dans l'état B après n secondes. Au départ, l'automate est dans l'état B.



On considère l'algorithme suivant :

Variables :	a et b sont des réels
Initialisation :	a prend la valeur 0 b prend la valeur 1
Traitement :	Pour k allant de 1 à 10 a prend la valeur $0,8a + 0,3b$ b prend la valeur $1 - a$ Fin Pour
Sortie :	Afficher a Afficher b

Affirmation 4 : En sortie, cet algorithme affiche les valeurs de a_{10} et b_{10} .

Affirmation 3 : Après 4 secondes, l'automate a autant de chances d'être dans l'état A que d'être dans l'état B.



III Sujet : Bac S – Amérique du Nord – 1 juin 2016

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 : $P_{(X_n=0)}(X_{n+1}=1)$, $P_{(X_n=1)}(X_{n+1}=1)$ 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 : $R_n = (P(X_n=0) \quad P(X_n=1) \quad P(X_n=2))$

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

On note R_0 la matrice ligne $(0 \quad 0 \quad 1)$.

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 : $P = \frac{1}{6} \begin{pmatrix} 2 & 3 & 1 \\ -1 & 0 & 1 \\ 2 & -3 & 1 \end{pmatrix}$, $D = \begin{pmatrix} -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ 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 $\lim_{n \rightarrow +\infty} P(X_n=0)$, $\lim_{n \rightarrow +\infty} P(X_n=1)$ et $\lim_{n \rightarrow +\infty} P(X_n=2)$.

Interpréter ces résultats.



IV Sujet : Bac S – Centres étrangers – 8 juin 2016

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	<div>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 :</div> <table><tr><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td></tr><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr><tr><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr><tr><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr></table>	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	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 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 $Y = AX$.																																																				
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 $u \times a \equiv 1 \text{ modulo } 26$.

2. On considère l'algorithme suivant :



VARIABLES :	a, u , et r sont des nombres (a est naturel et premier avec 26)
TRAITEMENT :	Lire a u prend la valeur 0, et r prend la valeur 0 Tant que $r \neq 1$ u prend la valeur $u + 1$ r prend la valeur du reste de la division euclidienne de $u \times a$ par 26 Fin du Tant que
SORTIE	Afficher u

On entre la valeur $a = 21$ dans cet algorithme.

(a) Reproduire sur la copie et compléter le tableau suivant, jusqu'à l'arrêt de l'algorithme.

u	0	1	2	...
r	0	21

(b) En déduire que $5 \times 21 \equiv 1$ modulo 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 $12A - A^2$.

(b) En déduire la matrice B telle que $BA = 21I$.

(c) Démontrer que si $AX = Y$, alors $21X = BY$.

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 : $Y = AX = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} X$.

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 :
$$\begin{cases} 21x_1 &= 7y_1 - 2y_2 \\ 21x_2 &= -7y_1 + 5y_2 \end{cases}$$

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

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



V Sujet : Bac S – Polynésie – 10 juin 2016

Pour chacune des cinq propositions suivantes, indiquer si elle est vraie ou fausse et justifier la réponse choisie. Il est attribué un point par réponse exacte correctement justifiée. Une réponse non justifiée n'est pas prise en compte. Une absence de réponse n'est pas pénalisée.

1. Proposition 1

Pour tout entier naturel n , le chiffre des unités de $n^2 + n$ n'est jamais égal à 4.

2. On considère la suite u définie, pour $n \geq 1$, par

$$u_n = \frac{1}{n} \text{pgcd}(20 ; n).$$

Proposition 2

La suite (u_n) est convergente.

3. Proposition 3

Pour toutes matrices A et B carrées de dimension 2, on a $A \times B = B \times A$.

4. Un mobile peut occuper deux positions A et B. À chaque étape, il peut soit rester dans la position dans laquelle il se trouve, soit en changer.

Pour tout entier naturel n , on note :

- A_n l'évènement « le mobile se trouve dans la position A à l'étape n » et a_n sa probabilité.
- B_n l'évènement « le mobile se trouve dans la position B à l'étape n » et b_n sa probabilité.
- X_n la matrice colonne $\begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

On admet que, pour tout entier naturel n , $X_{n+1} = M \times X_n$ avec $M = \begin{pmatrix} 0,55 & 0,3 \\ 0,45 & 0,7 \end{pmatrix}$.

Proposition 4

La probabilité $P_{A_n}(B_{n+1})$ vaut 0,45.

Proposition 5

Il existe un état initial $X_0 = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$ tel que la probabilité d'être en B à l'étape 1 est trois fois plus grande que celle d'être en A à l'étape 1, autrement dit tel que $b_1 = 3a_1$.



VI Sujet : Bac S – Métropole – 20 juin 2016

Pour tout couple d'entiers relatifs non nuls (a, b) , on note $\text{pgcd}(a, b)$ le plus grand diviseur commun de a et b . Le plan est muni d'un repère $(0; \vec{i}, \vec{j})$.

1. Exemple. Soit Δ_1 la droite d'équation $y = \frac{5}{4}x - \frac{2}{3}$.

- (a) Montrer que si (x, y) est un couple d'entiers relatifs alors l'entier $15x - 12y$ est divisible par 3.
- (b) Existe-il au moins un point de la droite Δ_1 dont les coordonnées sont deux entiers relatifs ? Justifier.

Généralisation

On considère désormais une droite Δ d'équation (E) : $y = \frac{m}{n}x - \frac{p}{q}$ où m, n, p et q sont des entiers relatifs non nuls tels que $\text{pgcd}(m, n) = \text{pgcd}(p, q) = 1$.

Ainsi, les coefficients de l'équation (E) sont des fractions irréductibles et on dit que Δ est une droite rationnelle.

Le but de l'exercice est de déterminer une condition nécessaire et suffisante sur m, n, p et q pour qu'une droite rationnelle Δ comporte au moins un point dont les coordonnées sont deux entiers relatifs.

2. On suppose ici que la droite Δ comporte un point de coordonnées (x_0, y_0) où x_0 et y_0 sont des entiers relatifs.
 - (a) En remarquant que le nombre $ny_0 - mx_0$ est un entier relatif, démontrer que q divise le produit np .
 - (b) En déduire que q divise n .
3. Réciproquement, on suppose que q divise n , et on souhaite trouver un couple (x_0, y_0) d'entiers relatifs tels que $y_0 = \frac{m}{n}x_0 - \frac{p}{q}$.
 - (a) On pose $n = qr$, où r est un entier relatif non nul. Démontrer qu'on peut trouver deux entiers relatifs u et v tels que $qru - mv = 1$.
 - (b) En déduire qu'il existe un couple (x_0, y_0) d'entiers relatifs tels que $y_0 = \frac{m}{n}x_0 - \frac{p}{q}$.
4. Soit Δ la droite d'équation $y = \frac{3}{8}x - \frac{7}{4}$. Cette droite possède-t-elle un point dont les coordonnées sont des entiers relatifs ? Justifier.
5. On donne l'algorithme suivant :



Variables : M, N, P, Q : entiers relatifs non nuls, tels que $\text{pgcd}(M, N) = \text{pgcd}(P, Q) = 1$
 X : entier naturel

Entrées : Saisir les valeurs de M, N, P, Q

Traitement et sorties :

```

Si Q divise N alors
    X prend la valeur 0
    Tant que  $\left(\frac{M}{N}X - \frac{P}{Q}\right)$  n'est pas entier
    et  $\left(-\frac{M}{N}X - \frac{P}{Q}\right)$  n'est pas entier faire
        X prend la valeur X + 1
    Fin tant que
    Si  $\frac{M}{N}X - \frac{P}{Q}$  est entier alors
        Afficher X,  $\frac{M}{N}X - \frac{P}{Q}$ 
    Sinon
        Afficher  $-X, -\frac{M}{N}X - \frac{P}{Q}$ 
    Fin Si
Sinon
    Afficher « Pas de solution »
Fin Si
  
```

- (a) Justifier que cet algorithme se termine pour toute entrée de M, N, P, Q , entiers relatifs non nuls tels que $\text{pgcd}(M, N) = \text{pgcd}(P, Q) = 1$.
- (b) Que permet-il d'obtenir ?



VII Sujet : Bac S – Antilles-Guyane – 20 juin 2016

Les parties A et B sont indépendantes

Partie A

On considère l'équation suivante d'inconnues x et y entiers relatifs : E : $7x - 3y = 1$.

- Un algorithme incomplet est donné ci-dessous. Le recopier et le compléter, en écrivant ses lignes manquantes (1) et (2) de manière à ce qu'il donne les solutions entières $(x ; y)$ de l'équation (E) vérifiant $-5 \leq x \leq 10$ et $-5 \leq y \leq 10$.

```

Variables :  X est un nombre entier
              Y est un nombre entier

Début :      Pour X variant de -5 à 10
              (1) .....
              (2) .....
              Alors Afficher X et Y
              Fin Si
              Fin Pour
              Fin Pour
Fin
  
```

- Donner une solution particulière de l'équation (E).
 - Déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E).
 - Déterminer l'ensemble des couples $(x ; y)$ d'entiers relatifs solutions de l'équation (E) tels que $-5 \leq x \leq 10$ et $-5 \leq y \leq 10$.

Partie B

Le plan complexe est rapporté à un repère orthonormé $(O; \vec{u}, \vec{v})$.

On considère la droite \mathcal{D} d'équation

$$7x - 3y - 1 = 0$$

On définit la suite (A_n) de points du plan de coordonnées $(x_n ; y_n)$ vérifiant pour tout n entier naturel :

$$\begin{cases} x_0 = 1 \\ y_0 = 2 \end{cases} \quad \text{et} \quad \begin{cases} x_{n+1} = -\frac{13}{2}x_n + 3y_n \\ y_{n+1} = -\frac{35}{2}x_n + 8y_n \end{cases}$$



1. On note M la matrice $\begin{pmatrix} -13 & 3 \\ 2 & 8 \end{pmatrix}$. Pour tout entier naturel n , on pose

$$X_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}.$$

- (a) Montrer que, pour tout entier naturel n , $X_{n+1} = MX_n$.
- (b) Sans justifier, exprimer pour tout entier naturel n , X_n en fonction de M^n et X_0 .
2. On considère la matrice $P = \begin{pmatrix} -2 & -3 \\ -5 & -7 \end{pmatrix}$ et on admet que la matrice inverse de P , notée P^{-1} , est définie

$$\text{par } P^{-1} = \begin{pmatrix} 7 & -3 \\ -5 & 2 \end{pmatrix}.$$

- (a) Vérifier que $P^{-1}MP$ est une matrice diagonale D que l'on précisera.
- (b) Pour tout entier naturel n , donner D^n sans justification.
- (c) Démontrer par récurrence que, pour tout entier naturel n , $M^n = PD^nP^{-1}$.
3. On admet que, pour tout entier naturel n , $M^n = \begin{pmatrix} -14 + \frac{15}{2^n} & 6 - \frac{6}{2^n} \\ -35 + \frac{35}{2^n} & 15 - \frac{14}{2^n} \end{pmatrix}$.

En déduire que, pour tout entier naturel n , une expression de x_n et y_n en fonction de n .

4. Montrer que, pour tout entier naturel n , le point A_n appartient à la droite \mathcal{D} .



VIII Sujet : Bac S – Asie – 23 juin 2016

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

- On considère l'équation (E) : $9d - 26m = 1$, où d et m désignent deux entiers relatifs.
 - Donner une solution simple de cette équation, de sorte que d et m soient des nombres entiers compris entre 0 et 3.
 - Démontrer que le couple (d, m) est solution de l'équation (E) si et seulement si :

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

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

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

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

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

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 :

$$ax + by \equiv ax' + by' \text{ modulo } 26.$$



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

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

- (a) Établir que la matrice A est inversible, et déterminer son inverse.
- (b) Décrypter le mot : XQGY.



IX Sujet : Bac S – Métropole – 12 septembre 2016

On dispose d'un dé équilibré à 6 faces numérotées de 1 à 6 et de 3 pièces A, B et C ayant chacune un côté pile et un côté face.

Un jeu consiste à lancer une ou plusieurs fois le dé.

Après chaque lancer de dé, si l'on obtient 1 ou 2, alors on retourne la pièce A, si l'on obtient 3 ou 4, alors on retourne la pièce B et si l'on obtient 5 ou 6, alors on retourne la pièce C.

Au début du jeu, les 3 pièces sont toutes du côté face.

1. Dans l'algorithme ci-dessous, 0 code le côté face et 1 code le côté pile. Si a code un côté de la pièce A, alors $1 - a$ code l'autre côté de la pièce A.

Variables :	a, b, c, d, s sont des entiers naturels i, n sont des entiers supérieurs ou égaux à 1
Initialisation :	a prend la valeur 0 b prend la valeur 0 c prend la valeur 0 Saisir n
Traitement :	Pour i allant de 1 à n faire d prend la valeur d'un entier aléatoire compris entre 1 et 6 Si $d \leq 2$ alors a prend la valeur $1 - a$ sinon Si $d \leq 4$ alors b prend la valeur $1 - b$ sinon c prend la valeur $1 - c$ FinSi FinSi s prend la valeur $a + b + c$ FinPour
Sortie :	Afficher s

- (a) On exécute cet algorithme en saisissant $n = 3$ et en supposant que les valeurs aléatoires générées successivement pour d sont 1 ; 4 et 2. Recopier et compléter le tableau donné ci-dessous contenant l'état des variables au cours de l'exécution de l'algorithme :



variables	i	d	a	b	c	s
initialisation						
1 ^{er} passage boucle Pour						
2 ^e passage boucle Pour						
3 ^e passage boucle Pour						

(b) Cet algorithme permet-il de savoir si, après une exécution de n tirages, les trois pièces sont du côté pile ?

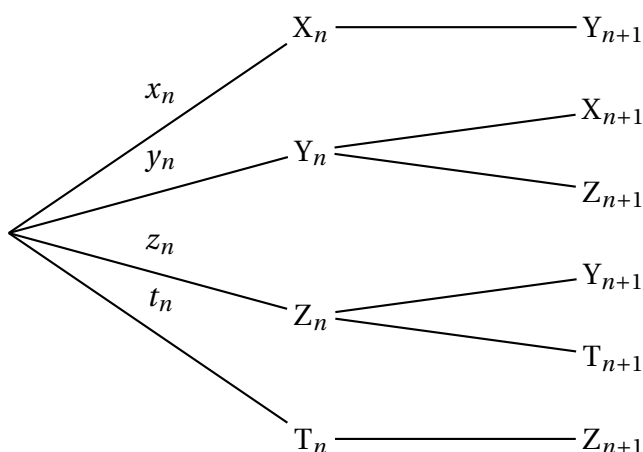
2. Pour tout entier naturel n , on note :

- X_n l'évènement : « À l'issue de n lancers de dés, les trois pièces sont du côté face »
- Y_n l'évènement : « À l'issue de n lancers de dés, une seule pièce est du côté pile et les autres sont du côté face »
- Z_n l'évènement : « À l'issue de n lancers de dés, exactement deux pièces sont du côté pile et l'autre est du côté face »
- T_n l'évènement : « À l'issue de n lancers de dés, les trois pièces sont du côté pile ».

De plus on note, $x_n = p(X_n)$; $y_n = p(Y_n)$; $z_n = p(Z_n)$ et $t_n = p(T_n)$ les probabilités respectives des évènements X_n , Y_n , Z_n et T_n .

(a) Donner les probabilités x_0 , y_0 , z_0 et t_0 respectives qu'au début du jeu il y ait 0, 1, 2 ou 3 pièces du côté pile.

(b) Recopier l'arbre ci-dessous et compléter les probabilités sur ses branches :



3. Pour tout entier naturel n , on note U_n la matrice ligne $(x_n y_n z_n t_n)$.

(a) Donner la matrice U_0 .

(b) À l'aide de l'arbre précédemment rempli, déterminer la matrice carrée M telle que, pour tout entier naturel n , $U_{n+1} = U_n \times M$.

4. Démontrer que, pour tout entier naturel n , $U_n = U_0 \times M^n$.



5. On admet que, pour tout entier $n \geq 1$,

$$\begin{aligned}x_n &= \frac{(-1)^n + 3 \times \left(-\frac{1}{3}\right)^n + 3 \times \left(\frac{1}{3}\right)^n + 1}{8}; \\y_n &= \frac{-3 \times \left(-\frac{1}{3}\right)^n + 3 \times \left(\frac{1}{3}\right)^n - (-1)^n \times 3 + 3}{8}; \\z_n &= \frac{-3 \times \left(-\frac{1}{3}\right)^n - 3 \times \left(\frac{1}{3}\right)^n + (-1)^n \times 3 + 3}{8}; \\t_n &= \frac{-(-1)^n + 3 \times \left(-\frac{1}{3}\right)^n - 3 \times \left(\frac{1}{3}\right)^n + 1}{8}.\end{aligned}$$

- (a) Calculer la probabilité, arrondie à 10^{-3} près, qu'au bout de 5 lancers de dés, une seule des trois pièces soit du côté pile.
- (b) Préciser si les affirmations suivantes sont vraies ou fausses. Une réponse non justifiée n'est pas prise en compte
- Première affirmation :
« À l'issue d'un nombre pair de lancers de dés, les pièces peuvent être toutes les trois du côté pile ».
 - Deuxième affirmation :
« Au cours du jeu, la probabilité que les pièces soient toutes les trois du côté pile peut être supérieure ou égale à $\frac{1}{4}$ ».
 - Troisième affirmation :
« Au cours du jeu, la probabilité que les pièces soient toutes les trois du côté pile peut être supérieure ou égale à 0,249 ».



X Sujet : Bac S – Antilles-Guyane – septembre 2016

Parmi les ordinateurs d'un parc informatique, 60 % présentent des failles de sécurité. Afin de pallier ce problème, on demande à un technicien d'intervenir chaque jour pour traiter les défaillances.

On estime que chaque jour, il remet en état 7 % des ordinateurs défaillants, tandis que de nouvelles failles apparaissent chez 3 % des ordinateurs sains. On suppose de plus que le nombre d'ordinateurs est constant sur la période étudiée.

Pour tout entier naturel n , on note a_n la proportion d'ordinateurs sains de ce parc informatique au bout de n jours d'intervention, et b_n la proportion d'ordinateurs défaillants au bout de n jours.

Ainsi $a_0 = 0,4$ et $b_0 = 0,6$.

Partie A

1. Décrire la situation précédente à l'aide d'un graphe ou d'un arbre pondéré.
2. Déterminer a_1 et b_1 .
3. Pour tout entier naturel n , exprimer a_{n+1} et b_{n+1} en fonction de a_n et b_n .
4. Soit la matrice $A = \begin{pmatrix} 0,97 & 0,07 \\ 0,03 & 0,93 \end{pmatrix}$. On pose $X_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.
 - (a) Justifier que pour tout entier naturel n , $X_{n+1} = AX_n$.
 - (b) Montrer, par récurrence, que pour tout entier naturel n , $X_n = A^n X_0$.
 - (c) Calculer, à l'aide de la calculatrice, X_{30} . En donner une interprétation concrète (les coefficients seront arrondis au millièmme).

Partie B

1. On pose $D = \begin{pmatrix} 0,9 & 0 \\ 0 & 0,9 \end{pmatrix}$ et $B = \begin{pmatrix} 0,07 \\ 0,03 \end{pmatrix}$.
 - (a) Justifier que, pour tout entier naturel n , $a_{n+1} + b_{n+1} = 1$.
 - (b) Montrer que, pour tout entier naturel n ,

$$X_{n+1} = DX_n + B.$$

2. On pose, pour tout entier naturel n , $Y_n = X_n - 10B$.
 - (a) Montrer que pour tout entier naturel n , $Y_{n+1} = DY_n$.
 - (b) On admet que pour tout entier naturel n , $Y_n = D^n Y_0$.
En déduire que pour tout entier naturel n , $X_n = D^n (X_0 - 10B) + 10B$.
 - (c) Donner l'expression de D^n puis en déduire a_{n+1} et b_{n+1} en fonction de n .
3. Selon cette étude, que peut-on dire de la proportion d'ordinateurs défaillants sur le long terme ?



XI Sujet : Bac S – Nouvelle Calédonie – 19 novembre 2016

On observe la taille d'une colonie de fourmis tous les jours.

Pour tout entier naturel n non nul, on note u_n le nombre de fourmis, exprimé en milliers, dans cette population au bout du n -ième jour.

Au début de l'étude la colonie compte 5 000 fourmis et au bout d'un jour elle compte 5 100 fourmis. Ainsi, on a $u_0 = 5$ et $u_1 = 5,1$.

On suppose que l'accroissement de la taille de la colonie d'un jour sur l'autre diminue de 10 % chaque jour.

En d'autres termes, pour tout entier naturel n , $u_{n+2} - u_{n+1} = 0,9(u_{n+1} - u_n)$.

1. Démontrer, dans ces conditions, que $u_2 = 5,19$.

2. Pour tout entier naturel n , on pose $V_n = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$ et $A = \begin{pmatrix} 1,9 & -0,9 \\ 1 & 0 \end{pmatrix}$.

(a) Démontrer que, pour tout entier naturel n , on a $V_{n+1} = AV_n$.

On admet alors que, pour tout entier naturel n , $V_n = A^n V_0$.

(b) On pose $P = \begin{pmatrix} 0,9 & 1 \\ 1 & 1 \end{pmatrix}$. On admet que la matrice P est inversible.

À l'aide de la calculatrice, déterminer la matrice P^{-1} .

En détaillant les calculs, déterminer la matrice D définie par $D = P^{-1}AP$.

(c) Démontrer par récurrence que, pour tout entier naturel n , on a

$$A^n = PD^nP^{-1}.$$

Pour tout entier naturel n , on admet que

$$A^n = \begin{pmatrix} -10 \times 0,9^{n+1} + 10 & 10 \times 0,9^{n+1} - 9 \\ -10 \times 0,9^n + 10 & 10 \times 0,9^n - 9 \end{pmatrix}.$$

(d) En déduire que, pour tout entier naturel n , $u_n = 6 - 0,9^n$.

3. Calculer la taille de la colonie au bout du 10^{e} jour. On arrondira le résultat à une fourmi près.

4. Calculer la limite de la suite (u_n) . Interpréter ce résultat dans le contexte.



XII Sujet : Bac S – Amérique du Sud – 22 novembre 2016

Les entiers naturels 1, 11, 111, 1 111, ... sont des rep-units. On appelle ainsi les entiers naturels ne s'écrivant qu'avec des 1.

Pour tout entier naturel p non nul, on note N_p le rep-unit s'écrivant avec p fois le chiffre 1 :

$$N_p = \underbrace{11\dots1}_{\substack{p \text{ répétitions} \\ \text{du chiffre 1}}} = \sum_{k=0}^{p-1} 10^k.$$

Dans tout l'exercice, p désigne un entier naturel non nul.

L'objet de cet exercice est d'étudier quelques propriétés des rep-units.

Partie A : divisibilité des rep-units dans quelques cas particuliers

1. Montrer que N_p n'est divisible ni par 2 ni par 5.
2. Dans cette question, on étudie la divisibilité de N_p par 3.
 - (a) Prouver que, pour tout entier naturel j , $10^j \equiv 1 \pmod{3}$.
 - (b) En déduire que $N_p \equiv p \pmod{3}$.
 - (c) Déterminer une condition nécessaire et suffisante pour que le rep-unit N_p soit divisible par 3.
3. Dans cette question, on étudie la divisibilité de N_p par 7.
 - (a) Recopier et compléter le tableau de congruences ci-dessous, où a est l'unique entier relatif appartenant à $\{-3 ; -2 ; -1 ; 0 ; 1 ; 2 ; 3\}$ tel que $10^m \equiv a \pmod{7}$.

On ne demande pas de justification.

m	0	1	2	3	4	5	6
a							

- (b) Soit p un entier naturel non nul.
Montrer que $10^p \equiv 1 \pmod{7}$ si et seulement si p est un multiple de 6.
On pourra utiliser la division euclidienne de p par 6.
- (c) Justifier que, pour tout entier naturel p non nul, $N_p = \frac{10^p - 1}{9}$.
- (d) Démontrer que « 7 divise N_p » est équivalent à « 7 divise $9N_p$ ».
- (e) En déduire que N_p est divisible par 7 si et seulement si p est un multiple de 6.

Partie B : un rep-unit strictement supérieur à 1 n'est jamais un carré parfait



1. Soit n un entier naturel supérieur ou égal à 2.

On suppose que l'écriture décimale de n^2 se termine par le chiffre 1, c'est-à-dire $n^2 \equiv 1 \pmod{10}$.

(a) Recopier et compléter le tableau de congruences ci-dessous.

$n \equiv \dots \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$n^2 \equiv \dots \pmod{10}$										

(b) En déduire qu'il existe un entier naturel m tel que : $n = 10m + 1$ ou

$$n = 10m - 1.$$

(c) Conclure que $n^2 \equiv 1 \pmod{20}$.

2. Soit p un entier naturel supérieur ou égal à 2.

Quel est le reste de la division euclidienne de N_p par 20 ?

3. En déduire que, pour p entier naturel supérieur ou égal à 2, le rep-unit N_p n'est pas le carré d'un entier.



Correction : Bac S – Pondichery – 22 avril 2016

Partie A

On considère les matrices M de la forme $M = \begin{pmatrix} a & b \\ 5 & 3 \end{pmatrix}$ où a et b sont des nombres entiers.

Le nombre $3a - 5b$ est appelé le déterminant de M . On le note $\det(M)$; ainsi $\det(M) = 3a - 5b$.

1. Dans cette question on suppose que $\det(M) \neq 0$ et on pose $N = \frac{1}{\det(M)} \begin{pmatrix} 3 & -b \\ -5 & a \end{pmatrix}$.

$$MN = \begin{pmatrix} a & b \\ 5 & 3 \end{pmatrix} \times \frac{1}{\det(M)} \begin{pmatrix} 3 & -b \\ -5 & a \end{pmatrix} = \frac{1}{3a-5b} \begin{pmatrix} 3a-5b & -ab+ab \\ 15-15 & -5b+3a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$NM = \frac{1}{\det(M)} \begin{pmatrix} 3 & -b \\ -5 & a \end{pmatrix} \times \begin{pmatrix} a & b \\ 5 & 3 \end{pmatrix} = \frac{1}{3a-5b} \begin{pmatrix} 3a-5b & 3b-3b \\ -5a+5a & -5b+3a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Donc N est la matrice inverse de la matrice M .

2. On considère l'équation (E) : $\det(M) = 3$.

(a) $\det(M) = 3 \iff 3a - 5b = 3$

$3 \times 6 - 5 \times 3 = 18 - 15 = 3$ donc le couple $(6 ; 3)$ est une solution de (E).

- (b) ■ On suppose que le couple $(a ; b)$ est solution de (E).

$$3a - 5b = 3$$

$$(6 ; 3) \text{ est solution } \quad 3 \times 6 - 5 \times 3 = 3$$

par soustraction $3(a-6) - 5(b-3) = 0 \iff 3(a-6) = 5(b-3)$

- Réciproquement, si $(a ; b)$ vérifie $3(a-6) = 5(b-3)$ alors :

$$3a - 18 = 5b - 15 \iff 3a - 5b = 3 \text{ donc } (a ; b) \text{ est solution de (E).}$$

Donc $(a ; b)$ est solution de (E) si et seulement si $3(a-6) = 5(b-3)$.

On cherche les solutions de l'équation (E).

- Si $3(a-6) = 5(b-3)$, alors 3 divise $5(b-3)$; or 3 et 5 sont premiers entre eux, donc d'après le théorème de GAUSS, 3 divise $b-3$. Cela veut dire que $b-3$ s'écrit $3k$ avec k entier relatif.

$$3(a-6) = 5(b-3) \text{ et } b-3 = 3k \text{ donc } 3(a-6) = 5 \times 3k \text{ ce qui équivaut à } a-6 = 5k$$

$$a-6 = 5k \iff a = 6+5k \text{ et } b-3 = 3k \iff b = 3+3k \text{ où } k \in \mathbb{Z}$$

Les solutions de (E) sont donc dans l'ensemble $\{(6+5k ; 3+3k)\}_{k \in \mathbb{Z}}$

- Réciproquement, si $a = 6+5k$ et $b = 3+3k$ avec $k \in \mathbb{Z}$, $3a - 5b = 3(6+5k) - 5(3+3k) = 18 + 15k - 15 - 15k = 3$ donc $(a ; b)$ est solution de (E).

L'ensemble solution de (E) est $\{(6+5k ; 3+3k)\}_{k \in \mathbb{Z}}$

Partie B



1. On pose $Q = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}$.

$\det(Q) = 6 \times 3 - 5 \times 3 = 18 - 15 = 3 \neq 0$ donc la matrice Q admet pour inverse la matrice

$$Q^{-1} = \frac{1}{\det(Q)} \begin{pmatrix} 3 & -3 \\ -5 & 6 \end{pmatrix} = \frac{1}{3} \begin{pmatrix} 3 & -3 \\ -5 & 6 \end{pmatrix}.$$

2. Codage avec la matrice Q

On code le mot DO en utilisant le procédé décrit dans le texte :

$$DO \rightarrow X = \begin{pmatrix} 3 \\ 14 \end{pmatrix} \rightarrow Y = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ 14 \end{pmatrix} = \begin{pmatrix} 6 \times 3 + 3 \times 14 \\ 5 \times 3 + 3 \times 14 \end{pmatrix} = \begin{pmatrix} 60 \\ 57 \end{pmatrix} \rightarrow R = \begin{pmatrix} 8 \\ 5 \end{pmatrix} \rightarrow \text{IF}$$

3. Procédure de décodage

Lors du codage, la matrice X a été transformée en la matrice Y telle que

$$Y = QX.$$

(a) $Y = QX \Rightarrow Q^{-1}Y = Q^{-1}QX \Leftrightarrow Q^{-1}Y = X \Leftrightarrow 3Q^{-1}Y = 3X \Leftrightarrow 3X = 3Q^{-1}Y$

$$X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}, Q^{-1} = \frac{1}{3} \begin{pmatrix} 3 & -3 \\ -5 & 6 \end{pmatrix} \text{ donc } 3Q^{-1} = \begin{pmatrix} 3 & -3 \\ -5 & 6 \end{pmatrix}$$

$$3X = 3Q^{-1}Y \Leftrightarrow 3 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 & -3 \\ -5 & 6 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \Leftrightarrow \begin{pmatrix} 3x_1 \\ 3x_2 \end{pmatrix} = \begin{pmatrix} 3y_1 - 3y_2 \\ -5y_1 + 6y_2 \end{pmatrix} \Leftrightarrow \begin{cases} 3x_1 = 3y_1 - 3y_2 \\ x_2 = -5y_1 + 6y_2 \end{cases}$$

Or $y_1 \equiv r_1 \quad [26]$ et $y_2 \equiv r_2 \quad [26]$ donc on en déduit que $\begin{cases} 3x_1 \equiv 3r_1 - 3r_2 \quad [26] \\ 3x_2 \equiv -5r_1 + 6r_2 \quad [26] \end{cases}$

(b) $9 \times 3 = 27$ et $27 \equiv 1 \quad [26]$ donc $9 \times 3 \equiv 1 \quad [26]$

$$\begin{cases} 3x_1 \equiv 3r_1 - 3r_2 \quad [26] \\ 3x_2 \equiv -5r_1 + 6r_2 \quad [26] \end{cases} \Rightarrow \begin{cases} 9 \times 3x_1 \equiv 9 \times 3r_1 - 9 \times 3r_2 \quad [26] \\ 9 \times 3x_2 \equiv 9 \times (-5)r_1 + 9 \times 6r_2 \quad [26] \end{cases}$$

$$\Leftrightarrow \begin{cases} x_1 \equiv r_1 - r_2 \quad [26] \\ x_2 \equiv -45r_1 + 54r_2 \quad [26] \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv r_1 - r_2 \quad [26] \\ x_2 \equiv 7r_1 + 2r_2 \quad [26] \end{cases}$$

car $-45 \equiv -2 \times 26 + 7 \equiv 7 \quad [26]$ et $54 \equiv 2 \times 26 + 2 \equiv 2 \quad [26]$

(c) Le mot SG correspond à $R = \begin{pmatrix} 18 \\ 6 \end{pmatrix}$ donc $\begin{cases} r_1 = 18 \\ r_2 = 6 \end{cases}$

$$\begin{cases} x_1 \equiv r_1 - r_2 \quad [26] \\ x_2 \equiv 7r_1 + 2r_2 \quad [26] \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 12 \quad [26] \\ x_2 \equiv 138 \quad [26] \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 12 \quad [26] \\ x_2 \equiv 8 \quad [26] \end{cases}$$

qui correspond au mot MI.



Correction : Bac S – Liban – 31 mai 2016

Pour chacune des affirmations suivantes, dire si elle est vraie ou fausse en justifiant la réponse. Un point est attribué par réponse exacte justifiée. Une réponse non justifiée ne sera pas prise en compte et l'absence de réponse n'est pas pénalisée.

- On considère le système
$$\begin{cases} n \equiv 1 \pmod{5} \\ n \equiv 3 \pmod{4} \end{cases}$$
 d'inconnue n entier relatif.

Affirmation 1 : Si n est solution de ce système alors $n - 11$ est divisible par 4 et par 5.

- Si n est solution du système, alors $n \equiv 1 \pmod{5}$; donc $n - 11 \equiv -10 \pmod{5}$. Or $-10 = 5 \times (-2) \equiv 0 \pmod{5}$, donc $n - 11 \equiv 0 \pmod{5}$, donc $n - 11$ est divisible par 5.
- Si n est solution du système, alors $n \equiv 3 \pmod{4}$; donc $n - 11 \equiv -8 \pmod{4}$. Or $-8 = 4 \times (-2) \equiv 0 \pmod{4}$, donc $n - 11 \equiv 0 \pmod{4}$, donc $n - 11$ est divisible par 4.

On a donc démontré que si n est solution du système, alors $n - 11$ est divisible par 4 et par 5.

Affirmation 1 vraie

Affirmation 2 : Pour tout entier relatif k , l'entier $11 + 20k$ est solution du système.

- $11 = 2 \times 5 + 1$ donc $11 \equiv 1 \pmod{5}$; $20k = 5(4k) \equiv 0 \pmod{5}$. Par somme, on peut dire que $11 + 20k \equiv 1 \pmod{5}$.
- $11 = 2 \times 4 + 3$ donc $11 \equiv 3 \pmod{4}$; $20k = 4(5k) \equiv 0 \pmod{4}$. Par somme, on peut dire que $11 + 20k \equiv 3 \pmod{4}$.

$11 + 20k \equiv 1 \pmod{5}$ et $11 + 20k \equiv 3 \pmod{4}$ donc $11 + 20k$ est solution du système.

Affirmation 2 vraie

Affirmation 3 : Si un entier relatif n est solution du système alors il existe un entier relatif k tel que $n = 11 + 20k$.

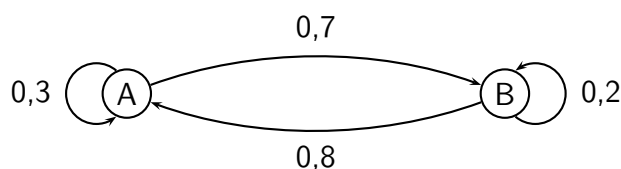
On a vu que si n est solution du système, alors $n - 11$ était divisible à la fois par 4 et par 5. Or 4 et 5 sont premiers entre eux donc, d'après le théorème de Gauss, le nombre $n - 11$ est divisible par $4 \times 5 = 20$; donc il existe un entier relatif k tel que $n - 11 = 20k$.

Affirmation 3 vraie

On a démontré que l'ensemble solution du système est $\{11 + 20k\}_{k \in \mathbb{Z}}$.

- Un automate peut se trouver dans deux états A ou B. À chaque seconde il peut soit rester dans l'état où il se trouve, soit en changer, avec des probabilités données par le graphe probabiliste ci-dessous.

Pour tout entier naturel n , on note a_n la probabilité que l'automate se trouve dans l'état A après n secondes et b_n la probabilité que l'automate se trouve dans l'état B après n secondes. Au départ, l'automate est dans l'état B.



On considère l'algorithme suivant :

Variables :	a et b sont des réels
Initialisation :	a prend la valeur 0 b prend la valeur 1
Traitement :	Pour k allant de 1 à 10 a prend la valeur $0,8a + 0,3b$ b prend la valeur $1 - a$ Fin Pour
Sortie :	Afficher a Afficher b

Affirmation 4 : En sortie, cet algorithme affiche les valeurs de a_{10} et b_{10} .

D'après le graphe, on peut dire que $\begin{cases} a_{n+1} = 0,3a + 0,8b \\ b_{n+1} = 0,7a + 0,2b \end{cases}$ avec $\begin{cases} a_0 = 0 \\ b_1 = 1 \end{cases}$

Dans l'algorithme, on a « a prend la valeur $0,8a + 0,3b$ » et il faudrait avoir « a prend la valeur $0,3a + 0,8b$ ».

Affirmation 4 fausse

Affirmation 5 : Après 4 secondes, l'automate a autant de chances d'être dans l'état A que d'être dans l'état B.

On cherche a_4 :

$$\begin{cases} a_1 = 0,3a_0 + 0,8b_0 = 0,3 \times 0 + 0,8 \times 1 = 0,8 \\ b_1 = 1 - a_1 = 0,2 \end{cases} \quad \begin{cases} a_2 = 0,3a_1 + 0,8b_1 = 0,3 \times 0,8 + 0,8 \times 0,2 = 0,4 \\ b_2 = 1 - a_2 = 0,6 \end{cases}$$

$$\begin{cases} a_3 = 0,3a_2 + 0,8b_2 = 0,3 \times 0,4 + 0,8 \times 0,6 = 0,6 \\ b_3 = 1 - a_3 = 0,4 \end{cases} \quad \begin{cases} a_4 = 0,3a_3 + 0,8b_3 = 0,3 \times 0,6 + 0,8 \times 0,4 = 0,5 \\ b_4 = 1 - a_4 = 0,5 \end{cases}$$

$a_4 = 0,5$ donc après 4 secondes, l'automate a autant de chances d'être dans l'état A que dans l'état B.

Affirmation 5 vraie



Correction : Bac S – Amérique du Nord – 1 juin 2016

1. (a) $P_{(X_n=1)}(X_{n+1}=1)$ est la probabilité qu'il y ait exactement une blanche dans l'urne U après le $(n+1)$ -ième tirage sachant qu'il y en avait exactement une au n -ième tirage

$P_{(X_n=1)}(X_{n+1}=1) = \frac{1}{2}$ car il s'agit de choisir une blanche dans chaque urne avec une probabilité $\frac{1}{4}$ ou de choisir une boule noire dans chaque urne avec une probabilité de $\frac{1}{4}$ pour que la situation reste inchangée.

$P_{(X_n=0)}(X_{n+1}=1) = 1$ car cela signifie que U ne contient que des boules noires et que l'on cherche la probabilité que l'urne V nous redonne une blanche (probabilité = 1 car V ne contient que des blanches)

$P_{(X_n=2)}(X_{n+1}=1) = 1$ car cela signifie que U ne contient que des boules blanches et que l'on cherche la probabilité que l'urne V nous redonne une noire (probabilité = 1 car V ne contient que des noires)

- (b) $(X_n=0)$, $(X_n=1)$ et $(X_n=2)$ forment une partition de l'univers de départ du $(n+1)$ -ième tirage on a donc

$$P(X_{n+1}=1) = P((X_{n+1}=1) \cap (X_n=0)) + P((X_{n+1}=1) \cap (X_n=1)) + P((X_{n+1}=1) \cap (X_n=2))$$

$$= P_{(X_n=0)}(X_{n+1}=1) \times P(X_n=0) + P_{(X_n=1)}(X_{n+1}=1) \times P(X_n=1) + P_{(X_n=2)}(X_{n+1}=1) \times P(X_n=2)$$

$$= P(X_n=0) + \frac{1}{2}P(X_n=1) + P(X_n=2)$$

$$2. R_1 = R_0 \times M = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}$$

Démonstration par récurrence de $\forall n \in \mathbb{N}, R_n = R_0 \times M^n$

Initialisation : $M^0 = I_3$ et $R_0 \times I_3 = R_0$

Hérédité : supposons que pour n entier naturel on ait $R_n = R_0 \times M^n$

Alors $R_{n+1} = R_n \times M = R_0 \times M^n \times M = R_0 \times M^{n+1}$

la propriété est vraie au rang 0 donc et si elle vraie au rang $n \geq 0$ elle l'est aussi au rang $n+1$ donc d'après le principe de récurrence : $\forall n \in \mathbb{N}, R_n = R_0 \times M^n$

3. *Initialisation* : $M^0 = I_3$ et $P \times D^0 \times P^{-1} = P \times I_3 \times P = P \times P^{-1} = I_3$

Hérédité : supposons que pour tout entier naturel k , on ait $M^k = P \times D^k \times P^{-1}$

Alors $M^{k+1} = M^k \times M = R_k \times M = P \times D^k \times P^{-1} \times M = P \times D^k \times P^{-1} \times P \times D \times P^{-1} = P \times D^k \times D \times P^{-1} = P \times D^{k+1} \times P^{-1}$.



La propriété est donc héréditaire à partir du rang 0 et vraie au rang 0 donc on a bien d'après le principe de récurrence :

$$\forall n \in \mathbb{N}, M^n = P \times D^n \times P^{-1}$$

$$4. \quad (a) \quad D^n \times P^{-1} = \begin{pmatrix} \left(-\frac{1}{2}\right)^n & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & -2 & 1 \\ 1 & 0 & -1 \\ 1 & 4 & 1 \end{pmatrix} = \begin{pmatrix} \left(-\frac{1}{2}\right)^n & \left(-\frac{1}{2}\right)^{n-1} & \left(-\frac{1}{2}\right)^n \\ 0 & 0 & 0 \\ 1 & 4 & 1 \end{pmatrix}$$

$$(b) \quad \forall n \in \mathbb{N}, R_n = R_0 \times M^n = R_0 \times P \times D^n \times P^{-1} =$$

$$\begin{pmatrix} \frac{1}{3} & -\frac{1}{2} & \frac{1}{6} \end{pmatrix} \times \begin{pmatrix} \left(-\frac{1}{2}\right)^n & \left(-\frac{1}{2}\right)^{n-1} & \left(-\frac{1}{2}\right)^n \\ 0 & 0 & 0 \\ 1 & 4 & 1 \end{pmatrix}$$

$$\text{On a donc } R_n = \begin{pmatrix} \frac{1}{3} \left(-\frac{1}{2}\right)^n + \frac{1}{6} & \frac{1}{3} \left(-\frac{1}{2}\right)^{n-1} + \frac{2}{3} & \frac{1}{3} \left(-\frac{1}{2}\right)^n + \frac{1}{6} \end{pmatrix}$$

$$5. \quad \lim_{n \rightarrow +\infty} \left(-\frac{1}{2}\right)^n = \lim_{n \rightarrow +\infty} \left(-\frac{1}{2}\right)^{n+1} = 0$$

$$\text{Donc par produit et somme } \lim_{n \rightarrow +\infty} P(X_n = 0) = \lim_{n \rightarrow +\infty} P(X_n = 2) = \frac{1}{6} \text{ et}$$

$$\lim_{n \rightarrow +\infty} P(X_n = 1) = \frac{2}{3}$$

Cela signifie que la probabilité que les urnes se retrouvent dans la situation initiale se stabilise vers $\frac{1}{6}$ quand n devient grand la probabilité que les urnes soient « monochrome » se stabilise vers $\frac{1}{3}$:
 $\left(\frac{1}{6} \text{ pour chaque couleur}\right)$



Correction : Bac S – Centres étrangers – 8 juin 2016

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

HI donne $X = \begin{pmatrix} 7 \\ 8 \end{pmatrix}$

$$AX = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} 51 \\ 105 \end{pmatrix}$$

Mais $51 \equiv 25[26]$ et $105 \equiv 1[26]$.

On en déduit que HI est codé par $Y = \begin{pmatrix} 25 \\ 1 \end{pmatrix}$, c'est à dire ZB.



$$\text{LL donne } X = \begin{pmatrix} 11 \\ 11 \end{pmatrix}$$

$$AX = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} \begin{pmatrix} 11 \\ 11 \end{pmatrix} = \begin{pmatrix} 77 \\ 154 \end{pmatrix}$$

Mais $77 \equiv 25[26]$ et $154 \equiv 24[26]$.

On en déduit que LL est codé par $Y = \begin{pmatrix} 25 \\ 24 \end{pmatrix}$, c'est à dire ZY.

On en déduit que HILL est codé ZBZY.

Partie B - Quelques outils mathématiques nécessaires au déchiffrement

1. Soit a un entier relatif premier avec 26.

Démontrons qu'il existe un entier relatif u tel que $u \times a \equiv 1 \text{ modulo } 26$.

Comme a un entier relatif premier avec 26, d'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $au + 26v = 1$ et alors $au \equiv 1[26]$

2. On considère l'algorithme suivant :

VARIABLES :	a, u , et r sont des nombres (a est naturel et premier avec 26)
TRAITEMENT :	<p>Lire a</p> <p>u prend la valeur 0, et r prend la valeur 0</p> <p>Tant que $r \neq 1$</p> <p style="padding-left: 40px;">u prend la valeur $u + 1$</p> <p style="padding-left: 40px;">r prend la valeur du reste de la division euclidienne de $u \times a$ par 26</p> <p>Fin du Tant que</p>
SORTIE	Afficher u

On entre la valeur $a = 21$ dans cet algorithme.

(a) On a : étape 1 $u=1$; $ua=21$; $r=21$

étape 2 $u=2$; $ua=42$; $r=16$

étape 3 $u=3$; $ua=63$; $r=11$

étape 4 $u=4$; $ua=84$; $r=6$

étape 5 $u=5$; $ua=105$; $r=1$

On a le tableau suivant, jusqu'à l'arrêt de l'algorithme.

u	0	1	2	3	4	5
r	0	21	16	11	6	1

(b) En déduire que $5 \times 21 \equiv 1 \text{ modulo } 26$.



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

$$(a) \quad 12A - A^2 = 12 \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} - \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} = \begin{pmatrix} 60 & 24 \\ 84 & 84 \end{pmatrix} - \begin{pmatrix} 39 & 24 \\ 84 & 63 \end{pmatrix} = \begin{pmatrix} 21 & 0 \\ 0 & 21 \end{pmatrix} = 21I.$$

(b) On vient de voir que $12A - A^2 = 21I$.

$$\text{Mais } 12A - A^2 = (12I - A) \times A$$

$$\text{En posant } B = 12I - A = 12 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} = \begin{pmatrix} 7 & -2 \\ -7 & 5 \end{pmatrix} \text{ on a } BA = 21I.$$

(c) Démontrons que si $AX = Y$, alors $21X = BY$.

$$AX = Y \Rightarrow BAX = BY \Rightarrow 21IX = BY \Rightarrow 21X = BY$$

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 : $Y = AX = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} X$.

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 $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$.

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

On vient de voir que si $AX = Y$, alors $21X = BY$.

$$\text{Or } X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, B = \begin{pmatrix} 7 & -2 \\ -7 & 5 \end{pmatrix} \text{ et } Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

$$\text{Si } 21X = BY \text{ alors } 21 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 7 & -2 \\ -7 & 5 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \text{ ou encore}$$

$$\begin{cases} 21x_1 = 7y_1 - 2y_2 \\ 21x_2 = -7y_1 + 5y_2 \end{cases}$$

$$2. \begin{cases} 21x_1 = 7y_1 - 2y_2 \\ 21x_2 = -7y_1 + 5y_2 \end{cases} \Rightarrow \begin{cases} 5 \times 21x_1 = 35y_1 - 10y_2 \\ 5 \times 21x_2 = -35y_1 + 25y_2 \end{cases}$$

Mais d'après 2 : $21 \times 5 \equiv 1[26]$.

$$35 \equiv 9[26]$$

$$-10 \equiv 16[26]$$

$$-35 \equiv 17[26]$$



$$25 \equiv 25[26]$$

$$y_1 \equiv r_1 [26]$$

$$y_2 \equiv r_2 [26]$$

$$\begin{cases} 21x_1 = 7y_1 - 2y_2 \\ 21x_2 = -7y_1 + 5y_2 \end{cases} \Rightarrow \begin{cases} x_1 \equiv 9r_1 + 16r_2 [26] \\ x_2 \equiv 17r_1 + 25r_2 [26] \end{cases}$$

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

Pour VL associé à la matrice $\begin{pmatrix} 21 \\ 11 \end{pmatrix}$.

On a : $y_1 = 21 = r_1$ et $y_2 = 11 = r_2$. On en déduit :

$$\begin{cases} x_1 \equiv 9 \times 21 + 16 \times 11 [26] \\ x_2 \equiv 17 \times 21 + 25 \times 11 [26] \end{cases} \Rightarrow \begin{cases} x_1 \equiv 1 [26] \\ x_2 \equiv 8 [26] \end{cases}$$

VL était le code BI

Pour UP associé à la matrice $\begin{pmatrix} 20 \\ 15 \end{pmatrix}$.

On a : $y_1 = 20 = r_1$ et $y_2 = 15 = r_2$. On en déduit :

$$\begin{cases} x_1 \equiv 9 \times 20 + 16 \times 15 [26] \\ x_2 \equiv 17 \times 20 + 25 \times 15 [26] \end{cases} \Rightarrow \begin{cases} x_1 \equiv 4 [26] \\ x_2 \equiv 13 [26] \end{cases}$$

UP était le code EN

VLUP est le code de BIEN.



Correction : Bac S – Polynésie – 10 juin 2016

1. **Proposition 1 : VRAI** On a $n^2 + n = n(n+1)$

dernier chiffre de n	dernier chiffre de $n+1$	dernier chiffre de $n(n+1)$
0	1	0
1	2	2
2	3	6
3	4	2
4	5	0
5	6	0
6	7	2
7	8	6
8	9	2
9	0	0

2. **Proposition 2 : VRAI**

$$\forall n \in \mathbb{N}^*, 1 \leq \text{pgcd}(20; n) \leq 20 \text{ donc } \forall n \in \mathbb{N}^*, \frac{1}{n} \leq u_n \leq \frac{20}{n}$$

$$\text{or } \lim_{n \rightarrow +\infty} \frac{1}{n} = 0 \text{ et } \lim_{n \rightarrow +\infty} \frac{20}{n} = 0$$

donc d'après le théorème des gendarmes, $\lim_{n \rightarrow +\infty} u_n = 0$ donc (u_n) converge vers 0.

3. **Proposition 3 : FAUX**

$$\text{Exemple : si } A = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ alors } A \times B = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix} \text{ et } B \times A = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

4. **Proposition 4 : VRAI**

$$\forall n \in \mathbb{N}, X_{n+1} = M \times X_n \text{ donc } \begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} 0,55 & 0,3 \\ 0,45 & 0,7 \end{pmatrix} \times \begin{pmatrix} a_n \\ b_n \end{pmatrix}$$

$$\text{donc } P(B_{n+1}) = b_{n+1} = 0,45 \times a_n + 0,7 \times b_n = 0,45 \times P(A_n) + 0,7 \times P(B_n)$$

$$\text{or d'après les probabilités totales, } P(B_{n+1}) = P_{A_n}(B_{n+1}) \times P(A_n) + P_{B_n}(B_{n+1}) \times P(B_n)$$

$$\text{On a donc } P_{A_n}(B_{n+1}) = 0,45$$

Proposition 5 : FAUX

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = X_1 = M \times X_0 = \begin{pmatrix} 0,55 \times a_0 + 0,3 \times b_0 \\ 0,45 \times a_0 + 0,7 \times b_0 \end{pmatrix}$$

$$b_1 = 3a_1 \iff 0,45 \times a_0 + 0,7 \times b_0 = 3(0,55 \times a_0 + 0,3 \times b_0) \iff 0,45 \times a_0 + 0,7 \times b_0 = 1,65 \times a_0 + 0,9 \times b_0$$

$$\text{donc } b_1 = 3a_1 \iff 1,2a_0 = -0,2b_0$$

Ce résultat est absurde puisque a_0 et b_0 sont des probabilités donc des nombres positifs.



Sujet : Bac S – Métropole – 20 juin 2016

1. (a) Soit (x, y) un couple d'entiers relatifs. On a $15x - 12y = 3(5x - 4y)$

$5x$ et $4y$ sont deux entiers.

La différence de deux entiers étant un entier, $5x - 4y$ est un entier, et $3(5x - 4y)$ est ainsi un multiple de 3 :

Si x et y sont deux entiers relatifs, alors l'entier $15x - 12y$ est divisible par 3

- (b) Supposons qu'existe un point de la droite Δ_1 dont les coordonnées (x_0, y_0) sont entières.

On a alors $y_0 = \frac{5}{4}x_0 - \frac{2}{3}$ Soit : $15x_0 - 8 = 12y_0$

Ou encore : $15x_0 - 12y_0 = 8$

D'après la question précédente, $15x_0 - 12y_0$ est un multiple de 3.

Or $15x_0 - 12y_0$ est égal à 8. Comme 8 n'est pas un multiple de 3

Aucun point de la droite Δ_1 n'a ses coordonnées entières.

2. (a) Puisque le point de coordonnées (x_0, y_0) appartient à Δ , on en déduit : $y_0 = \frac{m}{n}x_0 - \frac{p}{q}$ Soit : $nqy_0 = mx_0 - pn$

Ou encore : $q(mx_0 - ny_0) = np$

Puisque x_0, y_0, m et n sont des entiers,

alors $mx_0 - ny_0$ est un entier : $q(mx_0 - ny_0)$ est donc un multiple de q

Puisque $np = q(mx_0 - ny_0)$, alors **q divise np**

- (b) D'après la question précédente, q divise np .

Comme, par hypothèse, q et p sont premiers entre eux, on en déduit, d'après le théorème de Gauss, que q divise n .

Donc **q divise n**

3. (a) Puisque n et m sont premiers entre eux, alors, en vertu du théorème de Bézout, il existe deux entiers relatifs u et v' tels que $nu + mv' = 1$

Puisque $n = qr$, l'égalité précédente s'écrit : $qru - m(-v') = 1$

soit, en posant $v = -v'$: $qru - mv = 1$

Il existe deux entiers u et v tels que $qru - mv = 1$

- (b) L'égalité $y_0 = \frac{m}{n}x_0 - \frac{p}{q}$ est équivalente, d'après la question 2.a, à l'égalité $q(mx_0 - ny_0) = np$

soit : $q(mx_0 - ny_0) = qrp$

Puisque $q \neq 0$, cette dernière égalité est équivalente à l'égalité : $mx_0 - ny_0 = rp$ (1)

D'après la question précédente, on sait qu'il existe deux entiers relatifs u et v tels que $nu - mv = 1$

Multiplions chacun des deux membres de cette égalité par rp . On obtient alors : $nurp - mvrp = rp$



soit : $m(-vrp) - n(-urp) = rp$ (2)

En comparant les égalités (1) et (2),

on en déduit : **Le point de coordonnées $(-vrp, -urp)$ est un point de Δ**

4. Les questions 2 et 3 permettent d'énoncer le résultat suivant :

Soit Δ la droite d'équation $y = \frac{m}{n}x - \frac{p}{q}$ où m, n, p et q sont des entiers relatifs non nuls tels que $\text{pgcd}(n, m) = \text{pgcd}(p, q) = 1$.

Alors il existe un point de Δ dont les coordonnées sont des entiers *si et seulement si* q divise n .

Dans le cas présent Δ est la droite d'équation $y = \frac{3}{8}x - \frac{7}{4}$.

Puisque $\text{pgcd}(3, 8) = \text{pgcd}(7, 4) = 1$ et 4 divise 8,

alors **Il existe un point de Δ dont les coordonnées sont des entiers**

5. Soit Δ la droite d'équation $y = \frac{M}{N}x - \frac{P}{Q}$.

On applique le résultat énoncé au début de la question précédente :

- (a) ■ Si Q ne divise pas N , alors l'algorithme affiche "pas de solution" : il se termine donc.
- Si Q divise N , on sait qu'il existe un point de Δ à coordonnées entières. Autrement dit, il existe un couple d'entiers (x_0, y_0) tel que $y_0 = \frac{M}{N}x_0 - \frac{P}{Q}$

Il est clair qu'un tel couple existe si et seulement si il existe un entier *relatif* x_0 tel que $\frac{M}{N}x_0 - \frac{P}{Q}$ est un entier.

Lorsque X parcourt \mathbb{N} (i.e prend les valeurs $0, 1, 2, \dots$), il existe donc un entier naturel X_0 tel que $\frac{M}{N}X_0 - \frac{P}{Q}$ ou $-\frac{M}{N}X_0 - \frac{P}{Q}$ est un entier *relatif* : l'algorithme se termine donc.

L'algorithme se termine

- (b) **L'algorithme affiche les coordonnées du point de la droite d'équation $y = \frac{M}{N}x - \frac{P}{Q}$ dont l'abscisse a la plus petite valeur absolue.**



Sujet : Bac S – Antilles-Guyane – 20 juin 2016

Les parties A et B sont indépendantes

Partie A

On considère l'équation suivante d'inconnues x et y entiers relatifs :

$$7x - 3y = 1. \quad (E)$$

1. Un algorithme incomplet est donné ci-dessous. Le recopier et le compléter, en écrivant ses lignes manquantes (1) et (2) de manière à ce qu'il donne les solutions entières $(x ; y)$ de l'équation (E) vérifiant $-5 \leq x \leq 10$ et $-5 \leq y \leq 10$.

```

Variables :  X est un nombre entier
              Y est un nombre entier
Début :      Pour X variant de -5 à 10
                (1) Pour Y variant de -5 à 10
                  (2) Si 7X-3Y=1
                    Alors Afficher X et Y
                  Fin Si
                Fin Pour
              Fin Pour
            Fin
  
```

2. (a) $7 \times 1 - 3 \times 2 = 7 - 6 = 1$ donc $(1 ; 2)$ est une solution particulière de (E).
- (b) Soit $(x ; y)$ un couple solution quelconque de (E).
 On a alors : $7x - 3y = 7 \times 1 - 3 \times 2 \iff 7(x - 1) = 3(y - 2)$.
 7 divise $7(x - 1)$ donc 7 divise $3(y - 2)$.
 7 et 3 sont premiers entre eux. D'après le théorème de Gauss, 7 divise $y - 2$ donc $y - 2 = 7k$ d'où $y = 2 + 7k$, $k \in \mathbb{Z}$.
 On remplace y par $2 + 7k$: on trouve $x = 7(x - 1) = 3 \times 7k$ d'où $x - 1 = 3k$ donc $x = 1 + 3k$.
 L'ensemble des solutions est donc $\mathcal{S} = \{(1 + 3k ; 2 + 7k), k \in \mathbb{Z}\}$.
- (c) On veut que $-5 \leq 1 + 3k \leq 10$ et $-5 \leq 2 + 7k \leq 10$ Soit $-6 \leq 3k \leq 9$ et $-7 \leq 7k \leq 8$ D'où $-2 \leq k \leq 3$ et $-1 \leq k \leq \frac{8}{7}$

Partie B

Le plan complexe est rapporté à un repère orthonormé $(0; \vec{u}, \vec{v})$



On considère la droite \mathcal{D} d'équation

$$7x - 3y - 1 = 0$$

On définit la suite (A_n) de points du plan de coordonnées $(x_n : y_n)$ vérifiant pour tout n entier naturel :

$$\begin{cases} x_0 = 1 \\ y_0 = 2 \end{cases} \quad \text{et} \quad \begin{cases} x_{n+1} = -\frac{13}{2}x_n + 3y_n \\ y_{n+1} = -\frac{35}{2}x_n + 8y_n \end{cases}$$

1. On note M la matrice $\begin{pmatrix} -\frac{13}{2} & 3 \\ -\frac{35}{2} & 8 \end{pmatrix}$. Pour tout entier naturel n , on pose

$$X_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}.$$

(a) $MX_n = \begin{pmatrix} -\frac{13}{2}x_n + 3y_n \\ -\frac{35}{2}x_n + 8y_n \end{pmatrix} = X_{n+1}$ donc $X_{n+1} = MX_n$.

(b) Pour tout n , on a : $X_n = M^n X_0$.

2. On considère la matrice $P = \begin{pmatrix} -2 & -3 \\ -5 & -7 \end{pmatrix}$ et on admet que la matrice inverse de P , notée P^{-1} , est définie

par $P^{-1} = \begin{pmatrix} 7 & -3 \\ -5 & 2 \end{pmatrix}$.

(a) $P^{-1}MP = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$ donc $D = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$ qui est bien une matrice diagonale.

(b) Pour tout n , $D^n = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2^n} \end{pmatrix}$.

(c) i. *Initialisation* : Pour $n = 0$, $M^0 = I_2$ (matrice identité) et $PD^0P^{-1} = I_2$ donc c'est vrai.

ii. *Hérédité* : supposons que pour $n \in \mathbb{N}$ quelconque, on ait $M^n = PD^nP^{-1}$, alors

$$M^{n+1} = M^n \times M = PD^nP^{-1} \times M = PD^nP^{-1} \times PDP^{-1} = PD^{n+1}P^{-1}.$$

La propriété est donc héréditaire.

La propriété étant vraie au rang 0 et la propriété étant héréditaire à tout rang, d'après l'axiome de récurrence, la propriété est vraie pour tout n .

3. On admet que, pour tout entier naturel n , $M^n = \begin{pmatrix} -14 + \frac{15}{2^n} & 6 - \frac{6}{2^n} \\ -35 + \frac{35}{2^n} & 15 - \frac{14}{2^n} \end{pmatrix}$.



On a $X_n = M^n X_0$ donc $\begin{cases} x_n = -14 + \frac{15}{2^n} + 12 - \frac{12}{2^n} \\ y_n = -35 + \frac{35}{2^n} + 30 - \frac{25}{2^n} \end{cases}$ donc :

$$\begin{aligned} x_n &= -2 + \frac{36}{2^n} \\ y_n &= -5 + \frac{7}{2^n} \end{aligned}$$

.

4. Pour tout n , $7x_n - 3y_n - 1 = -14 + \frac{21}{2^n} + 15 - \frac{21}{2^n} - 1 = 1 - 1 = 0$ donc A_n appartient à la droite \mathcal{D} .



Correction : Bac S – Asie – 23 juin 2016

Partie A : quelques résultats

1. On considère l'équation (E) : $9d - 26m = 1$, où d et m désignent deux entiers relatifs.
 - (a) Les nombres 9 et 26 sont premiers entre eux donc, d'après le théorème de BÉZOUT, l'équation (E) : $9d - 26m = 1$ admet des solutions entières.
 $9 \times 3 - 26 \times 1 = 1$ donc le couple $(3 ; 1)$ est solution de l'équation (E).
 - (b) Le couple $(d ; m)$ est solution de (E) si et seulement si $9d - 26m = 1$
 si et seulement si $9d - 26m = 9 \times 3 - 26 \times 1$
 si et seulement si $9(d - 3) - 26(m - 1) = 0$
 si et seulement si $9(d - 3) = 26(m - 1)$
 - (c) $9(d - 3) = 26(m - 1)$ donc 9 divise $26(m - 1)$. Or 9 et 26 sont premiers entre eux donc, d'après le théorème de GAUSS, 9 divise $m - 1$. On peut donc écrire $m - 1$ sous la forme $9k$ avec $k \in \mathbb{Z}$. Donc $m = 9k + 1$ avec $k \in \mathbb{Z}$.
 $9(d - 3) = 26(m - 1)$ et $m - 1 = 9k$ donc $9(d - 3) = 26 \times 9k$ ce qui équivaut à $d - 3 = 26k$ ou encore $d = 26k + 3$ avec $k \in \mathbb{Z}$.
 Réciproquement, si $d = 26k + 3$ et $m = 9k + 1$ avec $k \in \mathbb{Z}$, alors
 $9d - 26m = 9(26k + 3) - 26(9k + 1) = 9 \times 26k + 27 - 26 \times 9k - 26 = 1$ et donc le couple $(d ; m)$ est solution de (E).
 Les solutions de l'équation (E) sont donc les couples $(d ; m)$ tels que

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

2. (a) Soit n un nombre entier.
 $n = 26k - 1 \iff 26k - n = 1 \iff 26k + n(-1) = 1$
 Il existe donc deux entiers relatifs k et -1 tels que $26k + n(-1) = 1$ donc, d'après le théorème de BÉZOUT, les nombres n et 26 sont premiers entre eux.
- (b) Soit $n = 9d - 28$, avec $d = 26k + 3$ et $k \in \mathbb{Z}$.
 $n = 9d - 28 = 9(26k + 3) - 28 = 9 \times 26k + 27 - 28 = 26(9k) - 1 = 26K - 1$ où $K \in \mathbb{Z}$
 D'après la question précédente, on peut déduire que $n = 9d - 28$ et 26 sont premiers entre eux.

Partie B : cryptage et décryptage

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



1. En cryptant par cette méthode le mot « PION », on obtient « LZWH » ; on veut crypter le mot « ESPION ».

Les lettres ES correspondent à la matrice colonne $\begin{pmatrix} 4 \\ 18 \end{pmatrix}$; $\begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix} \times \begin{pmatrix} 4 \\ 18 \end{pmatrix} = \begin{pmatrix} 36+72 \\ 28+54 \end{pmatrix} = \begin{pmatrix} 108 \\ 82 \end{pmatrix}$

$\left. \begin{array}{l} 108 = 4 \times 26 + 4 \text{ donc } 108 \equiv 4 \text{ modulo } 26 \\ 82 = 3 \times 26 + 4 \text{ donc } 82 \equiv 4 \text{ modulo } 26 \end{array} \right\} \text{ donc } \begin{pmatrix} 108 \\ 82 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 4 \end{pmatrix} \text{ modulo } 26 \text{ ce qui correspond à EE.}$

Le mot ESPION se code donc en EELZWH.

2. Méthode de décryptage

- (a) $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$; $\det(A) = 9 \times 3 - 4 \times 7 = -1 \neq 0$ donc la matrice A est inversible.

On trouve son inverse à la calculatrice : $A^{-1} = \begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix}$

- (b) Au cryptage, une matrice colonne X correspondant à deux lettres, est d'abord transformée en la matrice Y telle que $AX = Y$. Puis on cherche la matrice Y' composée de nombres entiers entre 0 et 25 et telle que $Y' \equiv Y \text{ modulo } 26$.

Au décryptage, on cherche la matrice colonne Y correspondant aux deux lettres à décrypter. Puis on détermine la matrice X telle que $AX = Y$, autrement dit telle que $X = A^{-1}Y$. Enfin on détermine la matrice colonne X' composée des restes des éléments de X modulo 26.

Comme $X \equiv X' \text{ modulo } 26$, d'après le texte $AX \equiv AX' \text{ modulo } 26$ et donc AX et AX' correspondent à la même matrice colonne Y modulo 26 ; ce qui valide le processus de décryptage.

Pour décrypter les lettres XQ, on cherche la matrice colonne correspondant à ces deux lettres : $\begin{pmatrix} 23 \\ 16 \end{pmatrix}$

puis on multiplie à gauche par la matrice A^{-1}

$$\begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix} \times \begin{pmatrix} 23 \\ 16 \end{pmatrix} = \begin{pmatrix} -3 \times 23 + 4 \times 16 \\ 7 \times 23 - 9 \times 16 \end{pmatrix} = \begin{pmatrix} -5 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 17 \end{pmatrix} \text{ modulo } 26 \text{ ce qui correspond à VR.}$$

On fait de même avec GY représenté par $\begin{pmatrix} 6 \\ 24 \end{pmatrix}$:

$$\begin{pmatrix} -3 & 4 \\ 7 & -9 \end{pmatrix} \times \begin{pmatrix} 6 \\ 24 \end{pmatrix} = \begin{pmatrix} -3 \times 6 + 4 \times 24 \\ 7 \times 6 - 9 \times 24 \end{pmatrix} = \begin{pmatrix} 78 \\ -174 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 8 \end{pmatrix} \text{ modulo } 26 \text{ ce qui correspond à AI.}$$

Le mot XQGY se décode en VRAl.



Sujet : Bac S – Métropole – 12 septembre 2016

On dispose d'un dé équilibré à 6 faces numérotées de 1 à 6 et de 3 pièces A, B et C ayant chacune un côté pile et un côté face.

Un jeu consiste à lancer une ou plusieurs fois le dé.

Après chaque lancer de dé, si l'on obtient 1 ou 2, alors on retourne la pièce A, si l'on obtient 3 ou 4, alors on retourne la pièce B et si l'on obtient 5 ou 6, alors on retourne la pièce C.

Au début du jeu, les 3 pièces sont toutes du côté face.

1. Dans l'algorithme ci-dessous, 0 code le côté face et 1 code le côté pile. Si a code un côté de la pièce A, alors $1 - a$ code l'autre côté de la pièce A.

Variables :	a, b, c, d, s sont des entiers naturels i, n sont des entiers supérieurs ou égaux à 1
Initialisation :	a prend la valeur 0 b prend la valeur 0 c prend la valeur 0 Saisir n
Traitement :	Pour i allant de 1 à n faire d prend la valeur d'un entier aléatoire compris entre 1 et 6 Si $d \leq 2$ alors a prend la valeur $1 - a$ sinon Si $d \leq 4$ alors b prend la valeur $1 - b$ sinon c prend la valeur $1 - c$ FinSi FinSi s prend la valeur $a + b + c$ FinPour
Sortie :	Afficher s

- (a) On exécute cet algorithme en saisissant $n = 3$ et en supposant que les valeurs aléatoires générées successivement pour d sont 1 ; 4 et 2.

On complète le tableau :



variables	i	d	a	b	c	s
initialisation			0	0	0	
1 ^{er} passage boucle Pour	1	1	1	0	0	1
2 ^e passage boucle Pour	2	4	1	1	0	2
3 ^e passage boucle Pour	3	2	0	1	0	1

(b) Les variables a , b et c sont à 0 ou 1 selon que la pièce montre le côté face ou le côté pile ; la variable $s = a + b + c$ donne donc le nombre de pièces qui sont du côté pile.

Après une exécution de n tirages, les trois pièces sont du côté pile si $s = 3$.

2. Pour tout entier naturel n , on note :

- X_n l'évènement : « À l'issue de n lancers de dés, les trois pièces sont du côté face »
- Y_n l'évènement : « À l'issue de n lancers de dés, une seule pièce est du côté pile et les autres sont du côté face »
- Z_n l'évènement : « À l'issue de n lancers de dés, exactement deux pièces sont du côté pile et l'autre est du côté face »
- T_n l'évènement : « À l'issue de n lancers de dés, les trois pièces sont du côté pile ».

De plus on note, $x_n = p(X_n)$; $y_n = p(Y_n)$; $z_n = p(Z_n)$ et $t_n = p(T_n)$ les probabilités respectives des évènements X_n , Y_n , Z_n et T_n .

(a) Au début du jeu, les trois pièces sont du côté face donc $x_0 = 1$, $y_0 = 0$, $z_0 = 0$ et $t_0 = 0$.

(b) ■ À chaque tirage, on retourne une pièce et une seule ; donc si les trois pièces sont du côté face après le n -ième tirage, il y aura une et une seule pièce du côté pile après le $n + 1$ -ième tirage. On en déduit que $P_{X_n}(Y_{n+1}) = 1$.

■ Par un raisonnement analogue, on démontre que $P_{T_n}(Z_{n+1}) = 1$.

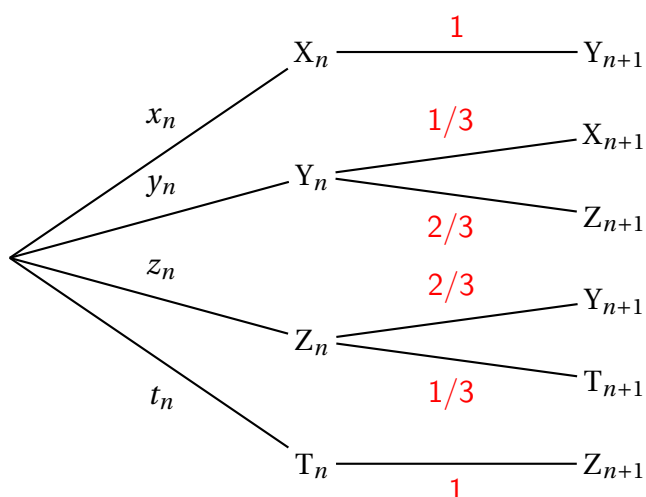
■ Si après le n -ième tirage, il y a une seule pièce du côté pile, il y a deux possibilités :

◦ c'est cette pièce qui est retournée lors du $n + 1$ -ième tirage, avec une probabilité de $\frac{1}{3}$, et donc $P_{Y_n}(X_{n+1}) = \frac{1}{3}$;

◦ c'est une des deux autres pièces qui est retournée, avec une probabilité de $\frac{2}{3}$, et donc $P_{Y_n}(Z_{n+1}) = \frac{2}{3}$.

■ Par un raisonnement analogue, on démontre que $P_{Z_n}(Y_{n+1}) = \frac{2}{3}$ et que $P_{Z_n}(T_{n+1}) = \frac{1}{3}$.

On peut donc compléter l'arbre proposé :



3. Pour tout entier naturel n , on note U_n la matrice ligne $(x_n \ y_n \ z_n \ t_n)$.

(a) $U_0 = (x_0 \ y_0 \ z_0 \ t_0) = (1 \ 0 \ 0 \ 0)$.

(b) On cherche la matrice carrée M telle que, pour tout entier naturel n , $U_{n+1} = U_n \times M$.

D'après l'arbre et le théorème des probabilités totales, on peut dire que :

$$\begin{cases} x_{n+1} = & \frac{1}{3}y_n \\ y_{n+1} = x_n & + \frac{2}{3}z_n \\ z_{n+1} = & \frac{2}{3}y_n & + t_n \\ t_{n+1} = & \frac{1}{3}z_n \end{cases}$$

Cela s'écrit sous forme matricielle :

$$(x_{n+1} \ y_{n+1} \ z_{n+1} \ t_{n+1}) = (x_n \ y_n \ z_n \ t_n) \times \begin{pmatrix} 0 & 1 & 0 & 0 \\ \frac{1}{3} & 0 & \frac{2}{3} & 0 \\ 0 & \frac{2}{3} & 0 & \frac{1}{3} \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

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



4. On va démontrer par récurrence que, pour tout entier naturel n , $U_n = U_0 \times M^n$.

Soit \mathcal{P}_n la propriété $U_n = U_0 \times M^n$.

▪ **Initialisation**

Pour $n = 0$, $M^0 = I_4$ la matrice identité d'ordre 4.

$U_0 \times M^0 = U_0 \times I_4 = U_0$ donc la propriété est vraie au rang 0.

▪ **Hérédité**

On suppose la propriété vraie pour un rang $p \geq 0$, c'est-à-dire $U_p = U_0 \times M^p$.

$U_{p+1} = U_p \times M = U_0 \times M^p \times M = U_0 \times M^{p+1}$ donc la propriété est vraie au rang $p + 1$; elle est donc héréditaire.

▪ **Conclusion**

La propriété est vraie au rang 0 et elle est héréditaire, donc elle est vraie pour tout $n \geq 0$.

On a donc démontré que, pour tout n , $U_n = U_0 \times M^n$.

5. On admet que, pour tout entier $n \geq 1$,

$$x_n = \frac{(-1)^n + 3 \times \left(-\frac{1}{3}\right)^n + 3 \times \left(\frac{1}{3}\right)^n + 1}{8};$$

$$y_n = \frac{-3 \times \left(-\frac{1}{3}\right)^n + 3 \times \left(\frac{1}{3}\right)^n - (-1)^n \times 3 + 3}{8}$$

$$z_n = \frac{-3 \times \left(-\frac{1}{3}\right)^n - 3 \times \left(\frac{1}{3}\right)^n + (-1)^n \times 3 + 3}{8};$$

$$t_n = \frac{-(-1)^n + 3 \times \left(-\frac{1}{3}\right)^n - 3 \times \left(\frac{1}{3}\right)^n + 1}{8}$$

(a) La probabilité qu'au bout de 5 lancers de dés, une seule des trois pièces soit du côté pile est y_5 .

$$y_5 = \frac{-3 \times \left(-\frac{1}{3}\right)^5 + 3 \times \left(\frac{1}{3}\right)^5 - (-1)^5 \times 3 + 3}{8} = \frac{61}{81} \approx 0,753.$$

(b) ▪ **Première affirmation**

« À l'issue d'un nombre pair de lancers de dés, les pièces peuvent être toutes les trois du côté pile ».

On veut savoir si, à l'issue d'un nombre pair de lancers, on peut avoir $t_n = 1$.

Si n est pair, alors $(-1)^n = 1$ et $\left(-\frac{1}{3}\right)^n = \left(\frac{1}{3}\right)^n$; on en déduit que $t_n = 0$.

Donc l'affirmation est **fausse**.

▪ **Deuxième affirmation**

« Au cours du jeu, la probabilité que les pièces soient toutes les trois du côté pile peut être supérieure ou égale à $\frac{1}{4}$ ».

On a vu que si n était pair, t_n valait 0 qui est inférieur à $\frac{1}{4}$.

Si n est impair, $(-1)^n = -1$ et $\left(-\frac{1}{3}\right)^n = -\left(\frac{1}{3}\right)^n$.



$$\text{Donc } t_n = \frac{1 - 3 \times \left(\frac{1}{3}\right)^n - 3 \times \left(\frac{1}{3}\right)^n + 1}{8} = \frac{2 - 6 \times \left(\frac{1}{3}\right)^n}{8} = \frac{1}{4} - \frac{3}{4} \times \left(\frac{1}{3}\right)^n < \frac{1}{4}$$

Donc l'affirmation est **fausse**.

■ Troisième affirmation

« Au cours du jeu, la probabilité que les pièces soient toutes les trois du côté pile peut être supérieure ou égale à 0,249 ».

On calcule t_n pour quelques valeurs de n :

n	1	2	3	4	5	6	7
t_n	0	0	0,222 22	0	0,246 91	0	0,249 65

$t_7 > 0,249$ donc l'affirmation est **vraie**.

Remarque

On a vu plus haut que, pour n impair, $t_n = \frac{1}{4} - \frac{3}{4} \times \left(\frac{1}{3}\right)^n$.

La suite (u_n) définie sur \mathbb{N} par $u_n = \frac{1}{4} - \frac{3}{4} \times \left(\frac{1}{3}\right)^n$ est convergente et a pour limite $\frac{1}{4}$.

Donc il existe un rang n_0 à partir duquel $u_n > 0,249$.

La suite (t_n) coïncide avec la suite (u_n) pour tous les n impairs.

Donc si n_0 est impair, $t_{n_0} = u_{n_0} > 0,249$.

Et si n_0 est pair, on prend $n_1 = n_0 + 1$ et $t_{n_1} = u_{n_1} > 0,249$.

Les suites extraites ne sont certes pas au programme de terminale S mais cet exemple est assez facile à comprendre pour un élève attentif. Et puis, c'est tellement plus joli qu'avec la calculatrice !

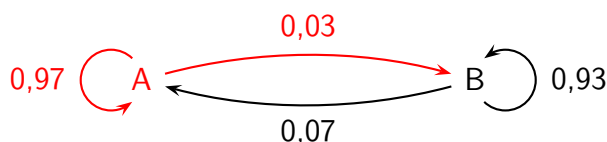
Enfin ce raisonnement permet de dire qu'il existe un rang à partir duquel $t_n > 0,249999$.



Sujet : Bac S – Antilles-Guyane – septembre 2016

Partie A

1. On décrit la situation précédente à l'aide d'un graphe en appelant A l'état « être sain » et B l'état « être défaillant » :



2. $a_1 = 0,97a_0 + 0,07b_0 = 0,97 \times 0,4 + 0,07 \times 0,6 = 0,43$

$b_1 = 0,03a_0 + 0,93b_0 = 0,03 \times 0,4 + 0,93 \times 0,6 = 0,57$

3. D'après le texte, on peut dire que
$$\begin{cases} a_{n+1} = 0,97a_n + 0,07b_n \\ b_{n+1} = 0,03a_n + 0,93b_n \end{cases}$$

4. Soit la matrice $A = \begin{pmatrix} 0,97 & 0,07 \\ 0,03 & 0,93 \end{pmatrix}$. On pose $X_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

(a) La traduction matricielle du système précédent, est :

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} 0,97 & 0,07 \\ 0,03 & 0,93 \end{pmatrix} \begin{pmatrix} a_n \\ b_n \end{pmatrix}$$

ou encore $X_{n+1} = AX_n$.

(b) Soit \mathcal{P}_n la propriété $X_n = A^n X_0$.

■ Initialisation

Pour $n = 0$, $A^n = A^0 = I_2$ la matrice identité d'ordre 2.

$A^0 \times X_0 = I_2 \times X_0 = X_0$ donc la propriété est vraie pour $n = 0$.

■ Hérédité

On suppose la propriété vraie à un rang $p \geq 0$; on va démontrer qu'elle est vraie au rang $p + 1$.

On a comme hypothèse que $X_p = A^p X_0$.

$$X_{p+1} = A \times X_p = A \times (A^p X_0) = (A \times A^p) \times X_0 = A^{p+1} X_0$$

Donc la propriété est démontrée pour le rang $p + 1$.

■ Conclusion

La propriété est vraie au rang 0 et elle est héréditaire, donc elle est vraie pour tout n .

On a donc démontré que, pour tout entier naturel n , $X_n = A^n X_0$.

(c) $X_{30} = A^{30} X_0 \approx \begin{pmatrix} 0,687 \\ 0,313 \end{pmatrix}$

Au bout de 30 jours, il y a 68,7% d'appareils sains, et 31,3% d'appareils défectueux.



Partie B

1. On pose $D = \begin{pmatrix} 0,9 & 0 \\ 0 & 0,9 \end{pmatrix}$ et $B = \begin{pmatrix} 0,07 \\ 0,03 \end{pmatrix}$.

(a) Au bout de $n+1$ jours, un appareil est soit sain soit défectueux ; la proportion d'appareils sains est a_{n+1} et la proportion d'appareil défectueux est b_{n+1} donc $a_{n+1} + b_{n+1} = 1$.

(b) On a vu que

$$\begin{cases} a_{n+1} = 0,97 a_n + 0,07 b_n \\ b_{n+1} = 0,03 a_n + 0,93 b_n \end{cases} ;$$

or, pour tout n , $a_n + b_n = 1$, donc $\begin{cases} a_{n+1} = 0,97 a_n + 0,07 (1 - a_n) \\ b_{n+1} = 0,03 (1 - b_n) + 0,93 b_n \end{cases}$

ce qui équivaut à $\begin{cases} a_{n+1} = 0,9 a_n + 0,07 \\ b_{n+1} = 0,9 b_n + 0,03 \end{cases}$

$$DX_n + B = \begin{pmatrix} 0,9 & 0 \\ 0 & 0,9 \end{pmatrix} \times \begin{pmatrix} a_n \\ b_n \end{pmatrix} + \begin{pmatrix} 0,07 \\ 0,03 \end{pmatrix} = \begin{pmatrix} 0,9 a_n \\ 0,9 b_n \end{pmatrix} + \begin{pmatrix} 0,07 \\ 0,03 \end{pmatrix} = \begin{pmatrix} 0,9 a_n + 0,07 \\ 0,9 b_n + 0,03 \end{pmatrix} = \begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = X_{n+1}$$

2. On pose, pour tout entier naturel n , $Y_n = X_n - 10B$, donc $X_n = Y_n + 10B$.

(a) $Y_{n+1} = X_{n+1} - 10B = DX_n + B - 10B = D(Y_n + 10B) - 9B = DY_n + 10DB - 9B$

$$10D = \begin{pmatrix} 9 & 0 \\ 0 & 9 \end{pmatrix} = 9I_2 \text{ donc } 10DB - 9B = 9I_2B - 9B = 9B - 9B = 0$$

Donc $Y_{n+1} = DY_n$.

(b) On admet que pour tout entier naturel n , $Y_n = D^n Y_0$.

Donc $X_n = Y_n + 10B = D^n Y_0 + 10B = D^n (X_0 - 10B) + 10B$.

(c) $D = \begin{pmatrix} 0,9 & 0 \\ 0 & 0,9 \end{pmatrix}$ donc $D = 0,9I_2$;

on a donc $D^n = 0,9^n I_2^n = 0,9^n I_2 = \begin{pmatrix} 0,9^n & 0 \\ 0 & 0,9^n \end{pmatrix}$

$X_0 = \begin{pmatrix} 0,4 \\ 0,6 \end{pmatrix}$ et $B = \begin{pmatrix} 0,07 \\ 0,03 \end{pmatrix}$ donc $10B = \begin{pmatrix} 0,7 \\ 0,3 \end{pmatrix}$

$$X_n = D^n (X_0 - 10B) + 10B \iff X_n = \begin{pmatrix} 0,9^n & 0 \\ 0 & 0,9^n \end{pmatrix} \times \left[\begin{pmatrix} 0,4 \\ 0,6 \end{pmatrix} - \begin{pmatrix} 0,7 \\ 0,3 \end{pmatrix} \right] + \begin{pmatrix} 0,7 \\ 0,3 \end{pmatrix}$$

$$\iff X_n = \begin{pmatrix} 0,9^n & 0 \\ 0 & 0,9^n \end{pmatrix} \times \begin{pmatrix} -0,3 \\ 0,3 \end{pmatrix} + \begin{pmatrix} 0,7 \\ 0,3 \end{pmatrix}$$

$$\iff X_n = \begin{pmatrix} -0,3 \times 0,9^n \\ 0,3 \times 0,9^n \end{pmatrix} + \begin{pmatrix} 0,7 \\ 0,3 \end{pmatrix}$$

$$\iff X_n = \begin{pmatrix} -0,3 \times 0,9^n + 0,7 \\ 0,3 \times 0,9^n + 0,3 \end{pmatrix}$$



$$\Leftrightarrow \begin{cases} a_n = -0,3 \times 0,9^n + 0,7 \\ b_n = 0,3 \times 0,9^n + 0,3 \end{cases}$$

3. La proportion d'ordinateurs défectueux est b_n et on cherche $\lim_{n \rightarrow +\infty} b_n$.

Or $-1 < 0,9 < 1$ donc $\lim_{n \rightarrow +\infty} 0,9^n = 0$ et on en déduit que $\lim_{n \rightarrow +\infty} b_n = 0,3$.

Sur le long terme, on peut dire que la proportion d'ordinateurs défectueux va tendre vers 30 %.



Sujet : Bac S – Nouvelle Calédonie – 19 novembre 2016

On observe la taille d'une colonie de fourmis tous les jours.

Pour tout entier naturel n non nul, on note u_n le nombre de fourmis, exprimé en milliers dans cette population au bout du n -ième jour.

Au début de l'étude la colonie compte 5 000 fourmis et au bout d'un jour elle compte 5 100 fourmis. Ainsi, on a $u_0 = 5$ et $u_1 = 5,1$.

On suppose que l'accroissement de la taille de la colonie d'un jour sur l'autre diminue de 10 % chaque jour.

En d'autres termes, pour tout entier naturel n , $u_{n+2} - u_{n+1} = 0,9(u_{n+1} - u_n)$.

1. D'après le texte, $u_2 - u_1 = 0,9(u_1 - u_0)$ donc

$$u_2 = 0,9(5,1 - 5) + 5,1 = 0,9 \times 0,1 + 5,1 = 0,09 + 5,1 = 5,19$$

2. Pour tout entier naturel n , on pose $V_n = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$ et $A = \begin{pmatrix} 1,9 & -0,9 \\ 1 & 0 \end{pmatrix}$.

$$(a) \quad u_{n+2} - u_{n+1} = 0,9(u_{n+1} - u_n) \iff u_{n+2} = 0,9u_{n+1} - 0,9u_n + u_{n+1} \iff u_{n+2} = 1,9u_{n+1} - 0,9u_n$$

On a :
$$\begin{cases} u_{n+2} = 1,9u_{n+1} - 0,9u_n \\ u_{n+1} = u_{n+1} + 0 \times u_n \end{cases}, \text{ système qui s'écrit sous la forme matricielle :}$$

$$\begin{pmatrix} u_{n+2} \\ u_{n+1} \end{pmatrix} = \begin{pmatrix} 1,9 & -0,9 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} \iff V_{n+1} = AV_n, \text{ avec } A = \begin{pmatrix} 1,9 & -0,9 \\ 1 & 0 \end{pmatrix}.$$

On admet alors que, pour tout entier naturel n , $V_n = A^n V_0$.

- (b) On pose $P = \begin{pmatrix} 0,9 & 1 \\ 1 & 1 \end{pmatrix}$. On admet que la matrice P est inversible. Avec la calculatrice, on trouve

$$P^{-1} = \begin{pmatrix} -10 & 10 \\ 10 & -9 \end{pmatrix}.$$

$$P^{-1}A = \begin{pmatrix} -10 & 10 \\ 10 & -9 \end{pmatrix} \begin{pmatrix} 1,9 & -0,9 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -10 \times 1,9 + 10 \times 1 & -10 \times (-0,9) + 10 \times 0 \\ 10 \times 1,9 - 9 \times 1 & 10 \times (-0,9) - 9 \times 0 \end{pmatrix} = \begin{pmatrix} -9 & 9 \\ 10 & -9 \end{pmatrix}$$

$$P^{-1}AP = \begin{pmatrix} -9 & 9 \\ 10 & -9 \end{pmatrix} \begin{pmatrix} 0,9 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -9 \times 0,9 + 9 \times 1 & -9 \times 1 + 9 \times 1 \\ 10 \times 0,9 - 9 \times 1 & 10 \times 1 - 9 \times 1 \end{pmatrix} = \begin{pmatrix} 0,9 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{Donc } D = \begin{pmatrix} 0,9 & 0 \\ 0 & 1 \end{pmatrix}.$$

- (c) Soit \mathcal{P}_n la propriété $A^n = PD^nP^{-1}$.

■ Initialisation

On appelle I_2 la matrice identité d'ordre 2 : $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

$$A^0 = I_2 \text{ et } D^0 = I_2 \text{ donc } PD^0P^{-1} = PI_2P^{-1} = PP^{-1} = I_2$$

Donc la propriété \mathcal{P}_0 est vérifiée.



■ Hérité

Soit n un entier naturel quelconque ; supposons que la propriété est vraie au rang n , c'est-à-dire que $A^n = PD^nP^{-1}$ (hypothèse de récurrence).

On veut démontrer que la propriété est vraie au rang $n+1$.

$$A^{n+1} = A \times A^n = (PDP^{-1})(PD^nP^{-1}) = PD(P^{-1}P)D^nP^{-1} = PD^{n+1}P^{-1}$$

La propriété est donc vraie au rang $n+1$.

On a démontré que, pour tout n , $P_n \Rightarrow P_{n+1}$.

La propriété est donc héréditaire à partir du rang 0.

■ Conclusion

La propriété est vraie au rang 0 ; elle est héréditaire à partir du rang 0, donc, d'après le principe de récurrence, elle est vraie pour tout entier naturel n .

On a donc démontré que, pour tout entier naturel n , $A^n = PD^nP^{-1}$.

Pour tout entier naturel n , on admet que $A^n = \begin{pmatrix} -10 \times 0,9^{n+1} + 10 & 10 \times 0,9^{n+1} - 9 \\ -10 \times 0,9^n + 10 & 10 \times 0,9^n - 9 \end{pmatrix}$.

(d) Pour tout entier n , on a $V^n = A^n V_0$ c'est-à-dire $\begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = A^n \begin{pmatrix} u_1 \\ u_0 \end{pmatrix}$.

$$\begin{aligned} \text{D'où : } u_n &= (-10 \times 0,9^n + 10) \times u_1 + (10 \times 0,9^n - 9) \times u_0 \\ &= (-10 \times 0,9^n + 10) \times 5,1 + (10 \times 0,9^n - 9) \times 5 \\ &= -52 \times 0,9^n + 51 + 50 \times 0,9^n - 45 \\ &= 6 - 0,9^n \end{aligned}$$

3. La taille de la colonie au bout du 10^e jour est $u_{10} = 6 - 0,9^{10} \approx 5,651$.

Au bout du dixième jour, il y aura donc environ 5 651 fourmis.

4. Comme $0 < 0,9 < 1$, $\lim_{n \rightarrow +\infty} 0,9^n = 0$.

D'après les théorèmes sur les limites de suites, la suite (u_n) converge donc vers 6.

Le nombre de fourmis dans la colonie tendra 6000 individus.



Correction : Bac S – Amérique du Sud – 22 novembre 2016

Les entiers naturels 1, 11, 111, 1 111, ... sont des rep-units. On appelle ainsi les entiers naturels ne s'écrivant qu'avec des 1.

Pour tout entier naturel p non nul, on note N_p le rep-unit s'écrivant avec p fois le chiffre 1 :

$$N_p = \underbrace{11\dots 1}_{\substack{p \text{ répétitions} \\ \text{du chiffre 1}}} = \sum_{k=0}^{p-1} 10^k.$$

Partie A : divisibilité des rep-units dans quelques cas particuliers

1. Le chiffre des unités de N_p est 1 donc N_p est impair donc il n'est pas divisible par 2.
Et comme le chiffre des unités n'est ni 0 ni 5, le nombre N_p n'est pas divisible par 5.
2. Dans cette question, on étudie la divisibilité de N_p par 3.
 - (a) $10 = 3 \times 3 + 1 \equiv 1 \pmod{3}$ et donc, pour tout j de \mathbb{N} , $10^j \equiv 1^j \pmod{3}$ donc $10^j \equiv 1 \pmod{3}$.
 - (b) N_p est la somme de p termes de la forme 10^j avec $j \in \mathbb{N}$, et pour tout j de \mathbb{N} , $10^j \equiv 1 \pmod{3}$.
Donc $N_p \equiv p \pmod{3}$.
 - (c) On peut donc dire que N_p est divisible par 3 si et seulement si p est divisible par 3.
3. Dans cette question, on étudie la divisibilité de N_p par 7.
 - (a) On complète le tableau de congruences ci-dessous, où a est l'unique entier relatif appartenant à $\{-3 ; -2 ; -1 ; 0 ; 1 ; 2 ; 3\}$ tel que $10^m \equiv a \pmod{7}$:

m	0	1	2	3	4	5	6
a	1	3	2	-1	-3	-2	1

- (b) Soit p un entier naturel non nul.

La division euclidienne de p par 6 permet d'écrire $p = 6q + r$ avec $q \in \mathbb{N}$ et $r \in \{0 ; 1 ; 2 ; 3 ; 4 ; 5\}$.

$$10^p = 10^{6q+r} = 10^{6q} \times 10^r = (10^6)^q \times 10^r$$

Or d'après la question précédente, $10^6 \equiv 1 \pmod{7}$ donc $(10^6)^q \equiv 1^q \pmod{7}$ et donc $10^{6q} \equiv 1 \pmod{7}$.

On en déduit que $10^p \equiv 10^r \pmod{7}$.

- Si p est un multiple de 6, alors $r = 0$ et $10^r = 10^0 \equiv 1 \pmod{7}$. Donc $10^p \equiv 1 \pmod{7}$.
- Si p vérifie $10^p \equiv 1 \pmod{7}$, alors $10^r \equiv 1 \pmod{7}$ où r est le reste de la division de p par 6.

D'après le tableau de la question précédente, la seule valeur possible de r dans $\{0 ; 1 ; 2 ; 3 ; 4 ; 5\}$ pour que $10^r \equiv 1 \pmod{7}$ est $r = 0$. On en déduit que p est un multiple de 6.



On a donc démontré que $10^p \equiv 1 \pmod{7}$ si et seulement si p est un multiple de 6.

- (c) $N_p = \sum_{k=0}^{p-1} 10^k = 1 + 10 + 10^2 + \dots + 10^{p-1}$ est la somme des p premiers termes de la suite géométrique de premier terme 1 et de raison 10.

$$\text{Donc } N_p = \text{premier terme} \times \frac{1 - \text{raison}^{\text{nombre de termes}}}{1 - \text{raison}} = 1 \times \frac{1 - 10^p}{1 - 10} = \frac{10^p - 1}{9}.$$

- (d) ■ Si 7 divise N_p , alors 7 divise tout multiple de N_p donc 7 divise $9N_p$.
 ■ On suppose que 7 divise $9N_p$.

On sait que 7 et 9 sont premiers entre eux ; donc, d'après le théorème de Gauss, 7 divise N_p .

On a démontré que « 7 divise N_p » est équivalent à « 7 divise $9N_p$ ».

- (e) On a vu dans une question précédente que $N_p = \frac{10^p - 1}{9}$ ce qui équivaut à $9N_p = 10^p - 1$.

N_p est divisible par 7 $\iff 9N_p$ est divisible par 7 (question d.)

$$\iff 9N_p \equiv 0 \pmod{7}$$

$$\iff 10^p - 1 \equiv 0 \pmod{7}$$

$$\iff 10^p \equiv 1 \pmod{7}$$

$$\iff p \text{ est multiple de 6} \quad (\text{question b.})$$

Partie B : un rep-unit strictement supérieur à 1 n'est jamais un carré parfait

1. Soit n un entier naturel supérieur ou égal à 2.

On suppose que l'écriture décimale de n^2 se termine par le chiffre 1, c'est-à-dire $n^2 \equiv 1 \pmod{10}$.

- (a) On complète le tableau de congruences ci-dessous :

$n \equiv \dots \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$n^2 \equiv \dots \pmod{10}$	0	1	4	9	6	5	6	9	4	1

- (b) D'après le tableau de la question précédente, pour avoir $n^2 \equiv 1 \pmod{10}$ il faut

- soit $n \equiv 1 \pmod{10}$ donc $n = 10m + 1$ avec $m \in \mathbb{N}$;
- soit $n \equiv 9 \pmod{10}$ donc $n = 10m' + 9$ ou $n = 10m - 1$ avec $m \in \mathbb{N}$.

- (c) ■ Si $n = 10m + 1$, alors $n^2 = 100m^2 + 20m + 1 = 20(5m^2 + m) + 1 \equiv 1 \pmod{20}$;
 ■ Si $n = 10m - 1$, alors $n^2 = 100m^2 - 20m + 1 = 20(5m^2 - m) + 1 \equiv 1 \pmod{20}$.

2. Soit p un entier naturel supérieur ou égal à 2. On sait que $N_p = \sum_{k=0}^{p-1} 10^k$.

Pour tout $k \geq 2$, $10^k = 100 \times 10^{k-2} = 20(5 \times 10^{k-2}) \equiv 0 \pmod{20}$. Donc $\sum_{k \geq 2} 10^k \equiv 0 \pmod{20}$.

Donc $N_p \equiv 1 + 10 \pmod{20}$ c'est-à-dire $N_p \equiv 11 \pmod{20}$.



3. On a vu que $n^2 \equiv 1 \pmod{10} \implies n^2 \equiv 1 \pmod{20}$; donc tout nombre qui a pour reste 1 dans la division par 10 et qui est un carré parfait, a pour reste 1 dans la division par 20.

Le nombre N_p a pour reste 1 dans la division par 10 et pour reste 11 dans la division par 20.

Donc N_p ne peut pas être le carré d'un entier.