

Durée : 4 heures

∞ Baccalauréat S Antilles-Guyane ∞  
11 septembre 2013 - Corrigé

EXERCICE 1

5 points

Commun à tous les candidats

Partie A

Restitution organisée de connaissances

Partie B

1. **Affirmation 1** :  $\Delta$  est orthogonale à toute droite du plan P.  $\Delta$  a pour vecteur directeur  $\delta(1; 3; -2)$

La droite (AB) a pour vecteur directeur  $\overrightarrow{AB}(4; -2; -1)$ .

La droite (AC) a pour vecteur directeur  $\overrightarrow{AC}(-1; -1; -2)$ .

Or  $\delta \cdot \overrightarrow{AB} = 4 - 6 + 2 = 0$  et  $\delta \cdot \overrightarrow{AC} = -1 - 3 + 4 = 0$ .

Donc  $\Delta$  est orthogonale à deux droites (AB) et (AC) sécantes du plan P : elle est orthogonale à ce plan. **VRAIE**.

2. **Affirmation 2** : les droites  $\Delta$  et (AB) sont coplanaires.

On a vu que  $\Delta$  et (AB) étaient orthogonales, donc elles ne sont pas parallèles.

Si elles sont coplanaires elles sont donc sécantes en un point.

En traduisant l'égalité vectorielle  $\overrightarrow{AM} = t' \overrightarrow{AB}$ , on obtient une équation car-

tésienne de la droite (AB) : 
$$\begin{cases} x = 4t' \\ y = -2t' - 1 \\ z = -t' + 1 \end{cases}$$
 avec  $t'$  appartenant à  $\mathbb{R}$ .

S'il existe un point commun aux deux droites ses coordonnées vérifient le système :

$$\begin{cases} t = 4t' \\ 3t - 1 = -2t' - 1 \\ -2t + 8 = -t' + 1 \end{cases} \iff \begin{cases} t = 4t' \\ 12t' = -2t' \\ -8t' = -t' - 7 \end{cases}$$
 système qui n'a manifestement pas de solution. **FAUSSE**

3. **Affirmation 3** : Le plan P a pour équation cartésienne  $x + 3y - 2z + 5 = 0$ .

On a  $4 + 3 \times (-3) - 2 \times 0 + 5 = 0 \iff -5 = 0$ , qui signifie que les coordonnées de B ne vérifient pas cette équation de plan. **FAUSSE**

4. On appelle D la droite passant par l'origine et de vecteur directeur  $\vec{u}(11; -1; 4)$ .

**Affirmation 4** : La droite D est strictement parallèle au plan d'équation  $x + 3y - 2z + 5 = 0$ .

O n'appartient pas au plan : si la droite D est parallèle au plan, elle est orthogonale au vecteur  $\vec{n}(1; 3; -2)$  normal au plan.

Or  $\vec{u} \cdot \vec{n} = 11 - 3 - 8 = 0$ . Les vecteurs sont bien orthogonaux, la droite D est strictement parallèle au plan d'équation  $x + 3y - 2z + 5 = 0$ . **VRAIE**

EXERCICE 2

6 points

Commun à tous les candidats

Partie A : Étude du cas  $k = 1$

$$f_1(x) = xe^{-x}.$$

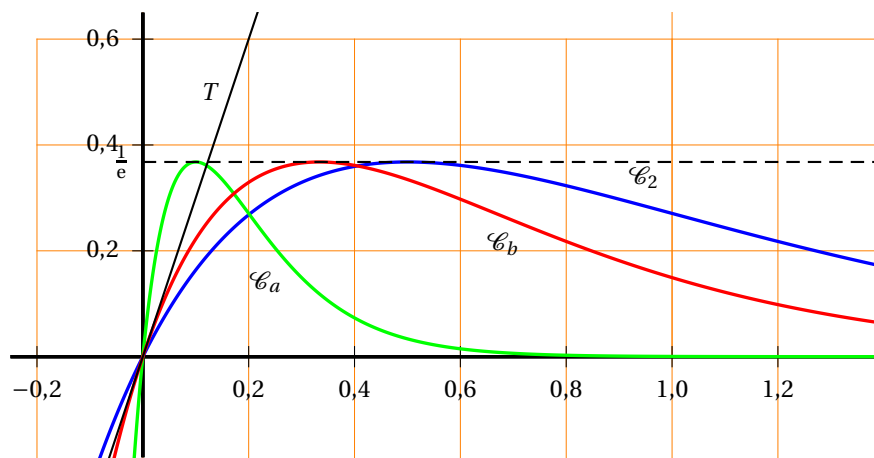
- Comme  $\lim_{x \rightarrow -\infty} e^{-x} = +\infty$ , on a  $\lim_{x \rightarrow -\infty} f_1(x) = -\infty$ .  
 $f_1(x) = \frac{x}{e^x}$ . On sait que  $\lim_{x \rightarrow +\infty} \frac{e^x}{x} = +\infty$  donc  $\lim_{x \rightarrow +\infty} f_1(x) = 0$ .  
 Donc l'axe des abscisses est asymptote horizontale à  $\mathcal{C}_1$  en  $+\infty$ .
- $f_1$  produit de fonctions dérivables sur  $\mathbb{R}$  est dérivable sur  $\mathbb{R}$  :  
 $f_1'(x) = e^{-x} - xe^{-x} = e^{-x}(1-x)$ .  
 Comme  $e^{-x} > 0$  sur  $\mathbb{R}$ , le signe de  $f_1'(x)$  est celui de  $1-x$ .  
 Donc  $f_1'(x) > 0$  si  $x < 1$  et  $f_1'(x) < 0$  si  $x > 1$ . D'où le tableau de variations :

$x$	$-\infty$	$1$	$+\infty$
$f_1'(x)$	$+$	$0$	$-$
$f(x)$	$-\infty$	$e^{-1}$	$0$

- $g_1(x) = -(x+1)e^{-x}$   
 $g_1$  étant dérivable, on a pour tout réel,  
 $g_1'(x) = -1e^{-x} - 1 \times [-(x+1)e^{-x}] = -e^{-x} + (x+1)e^{-x} = xe^{-x} = f_1(x)$ .  
 Donc  $g_1$  est bien une primitive de la fonction  $f_1$  sur  $\mathbb{R}$ .
- Comme pour tout réel  $x$ ,  $e^x > 0$ ,  $f_1(x) = 0 \iff x = 0$ .  
 Le tableau de variations ci-dessus montre donc que  $f_1(x) < 0$  sur  $] -\infty; 0[$  et  $f_1(x) > 0$  sur  $] 0; +\infty[$ .
- Comme la fonction est positive sur  $] 0; +\infty[$ , elle l'est aussi sur  $] 0; \ln 10[$ , donc l'aire cherchée est en unités d'aire égale à l'intégrale :  
 $\int_0^{\ln 10} f_1(x) dx = [g_1(x)]_0^{\ln 10} = g_1(\ln 10) - g_1(0) = -(\ln 10 + 1)e^{-\ln 10} + e^0$ .  
 Comme  $e^{-\ln 10} = \frac{1}{e^{\ln 10}} = \frac{1}{10}$ , l'aire est égale à :  
 $1 - \frac{1 + \ln 10}{10} = \frac{9}{10} - \frac{\ln 10}{10} \approx 0,67$  u. a.

**Partie B : Propriétés graphiques**

On a représenté sur le graphique ci-dessous les courbes  $\mathcal{C}_2$ ,  $\mathcal{C}_a$  et  $\mathcal{C}_b$  où  $a$  et  $b$  sont des réels strictement positifs fixés et T la tangente à  $\mathcal{C}_b$  au point O origine du repère.



- De façon évidente  $f_k(0) = k \times 0 \times e^0 = 0$ , donc les courbes  $\mathcal{C}_k$  passent par l'origine.

2. a. Produit de fonctions dérivables sur  $\mathbb{R}$ , la fonction  $f_k$  l'est aussi et :
- $$f'_k(x) = ke^{-kx} - k \times kxe^{-kx} = ke^{-kx}(1 - kx).$$
- b.  $k$  strictement positif, et  $e^{-kx} > 0$ , pour tout réel  $x$ , donc le signe de la dérivée  $f'_k(x)$  est celui de  $1 - kx$ .
- Or  $1 - kx < 0 \iff \frac{1}{k} < x$ ;  $1 - kx > 0 \iff \frac{1}{k} > x$ ;  $1 - kx = 0 \iff \frac{1}{k} = x$ .
- Il en résulte que la fonction  $f_k$  est :
- croissante sur  $\left] -\infty ; \frac{1}{k} \right[$ , et décroissante sur  $\left] \frac{1}{k} ; +\infty \right[$ ;
- elle admet donc un maximum en  $\frac{1}{k}$  :
- $$f_k\left(\frac{1}{k}\right) = k \times \frac{1}{k} \times e^{-k \times \frac{1}{k}} = 1e^{-1} = \frac{1}{e} \approx 0,368.$$
- Conclusion : toutes les fonctions ont le même maximum  $e^{-1}$  pour  $x = \frac{1}{k}$ .
- c. Le maximum pour  $k = 2$  est obtenu pour  $x = \frac{1}{2} = 0,5$ , donc le maximum pour  $f_a$  est obtenue pour une valeur  $\frac{1}{a}$  inférieure à 0,5 donc  $a > 2$ .
- Note : en fait on peut penser que l'abscisse du minimum est à peu près égale à 0,1, ce qui correspond à  $a = 10$ .*
- d. Une équation de cette tangente est :
- $$y = f'_k(0)(x - 0) + f_k(0) \iff y = k(1 - 0)e^0x + 0 \iff y = kx.$$
- e. Le coefficient directeur de la droite  $(T)$  est égal à  $\frac{0,6}{0,2} = 3$ .
- Donc la courbe  $\mathcal{C}_b$  correspond à la valeur  $b = 3$ .

**EXERCICE 3****4 points****Commun à tous les candidats**

- $p_1 = P(\mu_1 - 3\sigma_1 \leq X \leq \mu_1 + 3\sigma_1) = P(35,4 \leq X \leq 36,6) \approx 0,997$ .
- $p_2 = P(5,88 \leq Y \leq 6,12) = P(Y \leq 6,12) - P(Y \leq 5,88) \approx 0,984$ .
- a. Les deux événements  $D$  et  $L$  étant indépendants on a :  
 $P(D \cap L) = P(D) \times P(L) \approx 0,981$ .  
 La probabilité qu'une pièce ne soit pas acceptée est donc  $1 - 0,981 \approx 0,02$  arrondi à  $10^{-2}$ .
- b.  $D$  et  $L$  sont indépendants donc  $D$  et  $\bar{L}$  le sont aussi d'après le cours.  
 On a donc :  $P_{\bar{L}}(D) = P(D) = p_2$ .

**EXERCICE 4****5 points****Candidats n'ayant pas suivi l'enseignement de spécialité****Partie A : modélisation et simulation**

- $(-1 ; 1)$  : non car  $x < 0$  ce qui n'est pas possible ;  
 $(10 ; 0)$  : oui par exemple en choisissant 10 fois la valeur 0 pour  $y$  ;  
 $(2 ; 4)$  : non car  $y > 2$  ;  
 $(10 ; 2)$  : oui par exemple en choisissant dans cet ordre 8 fois la valeur 0 puis deux fois la valeur 1 pour  $y$ .
- Pour que Tom ait réussi la traversée, il faut qu'il soit arrivé au bout des 10 étapes, c'est-à-dire que  $x = 10$  et qu'il ne tombe pas lors de cette dernière étape, ce qui est encore possible si sa position à l'étape précédente était  $(9 ; 1)$  ou  $(9 ; -1)$  ; il faut donc tester également si  $y$  n'est pas plus grand que 1 ou plus petit que  $-1$  en fin d'algorithme.

On remplace dans l'algorithme la ligne :

```

| Afficher « la position de Tom est » (x; y)
par :
| Si x = 10 et y ≥ -1 et y ≤ 1
|   alors Afficher « Tom a réussi la traversée »
|   sinon Afficher « Tom est tombé »
| Fin du si
    
```

**Partie B**

Pour tout  $n$  entier naturel compris entre 0 et 10, on note :

$A_n$  l'évènement « après  $n$  déplacements, Tom se trouve sur un point d'ordonnée  $-1$  ».

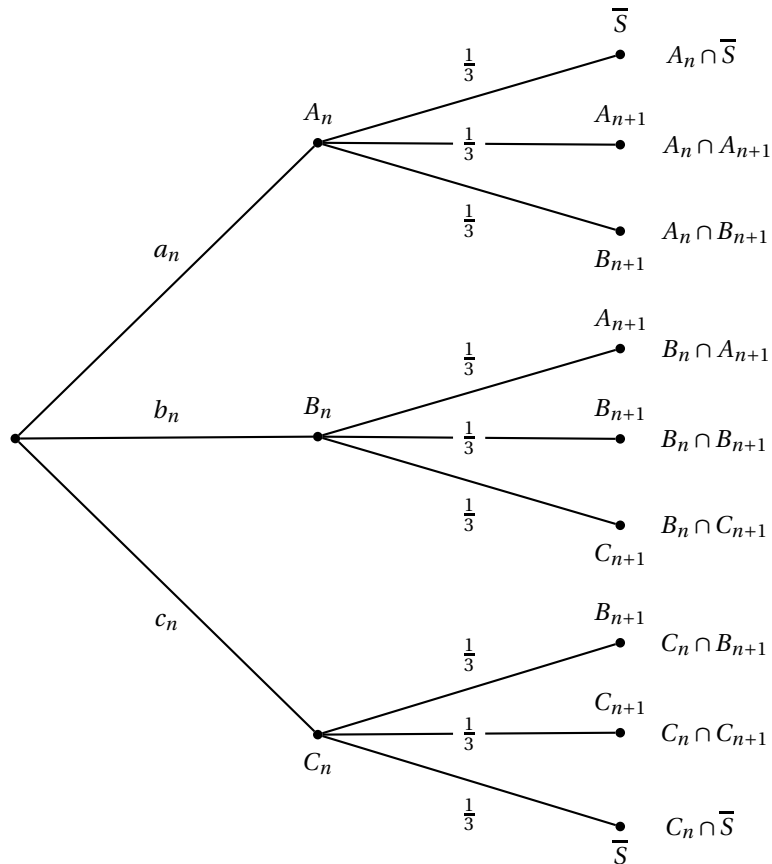
$B_n$  l'évènement « après  $n$  déplacements, Tom se trouve sur un point d'ordonnée  $0$  ».

$C_n$  l'évènement « après  $n$  déplacements, Tom se trouve sur un point d'ordonnée  $1$  ».

On note  $a_n, b_n, c_n$  les probabilités respectives des évènements  $A_n, B_n, C_n$ .

1. Au départ, Tom se trouve à l'origine  $O$  donc son ordonnée est  $0$ ; donc l'évènement  $B_0$  est réalisé :  $a_0 = 0, b_0 = 1$  et  $c_0 = 0$ .
2. On va représenter sur un arbre pondéré le passage de l'état  $n$  à l'état  $n + 1$ ; une branche vers le haut signifie que le nombre choisi au hasard est  $-1$ , une branche du milieu signifie que le nombre est  $0$  et une branche vers le bas signifie que ce nombre vaut  $1$ .

Il est dit dans le texte que  $S$  représente l'évènement « Tom traverse le pont » donc  $\bar{S}$  désigne l'évènement « Tom est tombé à l'eau ».



D'après la formule des probabilités totales :

$$a_{n+1} = P(A_{n+1}) = P(A_n \cap A_{n+1}) + P(B_n \cap A_{n+1}) \\ = P(A_n) \times P_{A_n}(A_{n+1}) + P(B_n) \times P_{B_n}(A_{n+1}) = a_n \times \frac{1}{3} + b_n \times \frac{1}{3} = \frac{a_n + b_n}{3}$$

De même  $b_{n+1} = P(B_{n+1}) = a_n \times \frac{1}{3} + b_n \times \frac{1}{3} + c_n \times \frac{1}{3} = \frac{a_n + b_n + c_n}{3}$

et  $c_{n+1} = P(C_{n+1}) = b_n \times \frac{1}{3} + c_n \times \frac{1}{3} = \frac{b_n + c_n}{3}$

3.  $P(A_1) = a_1 = \frac{a_0 + b_0}{3} = \frac{1}{3}$  ;  $P(B_1) = b_1 = \frac{a_0 + b_0 + c_0}{3} = \frac{1}{3}$  ;

$P(C_1) = c_1 = \frac{b_0 + c_0}{3} = \frac{1}{3}$ .

4. Tom se trouve sur le pont au bout de deux déplacements si l'ordonnée  $y$  de sa position vaut  $-1, 0$  ou  $1$ , autrement dit dans le cas de l'événement  $A_2 \cup B_2 \cup C_2$ . Les trois événements  $A_2, B_2$  et  $C_2$  sont incompatibles donc  $P(A_2 \cup B_2 \cup C_2) = P(A_2) + P(B_2) + P(C_2)$ .

$$a_2 = \frac{a_1 + b_1}{3} = \frac{\frac{1}{3} + \frac{1}{3}}{3} = \frac{2}{9} ; b_2 = \frac{a_1 + b_1 + c_1}{3} = \frac{\frac{1}{3} + \frac{1}{3} + \frac{1}{3}}{3} = \frac{1}{3} ;$$

$$c_2 = \frac{b_1 + c_1}{3} = \frac{\frac{1}{3} + \frac{1}{3}}{3} = \frac{2}{9}.$$

$$P(A_2 \cup B_2 \cup C_2) = P(A_2) + P(B_2) + P(C_2) = a_2 + b_2 + c_2 = \frac{2}{9} + \frac{1}{3} + \frac{2}{9} = \frac{7}{9}.$$

La probabilité que Tom se trouve sur le pont après deux déplacements est  $\frac{7}{9}$ .

5. Pour la même raison que dans la question précédente, la probabilité que Tom traverse le pont est  $P(A_{10} \cup B_{10} \cup C_{10}) = P(A_{10}) + P(B_{10}) + P(C_{10}) = a_{10} + b_{10} + c_{10} \approx 0,040272 + 0,056953 + 0,040272 \approx 0,137497$  (d'après le tableau fourni).

Une valeur approchée à 0,001 près de la probabilité que Tom traverse le pont est 0,137.

**EXERCICE 4**

**5 points**

**Candidats ayant suivi l'enseignement de spécialité**

**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. Si on saisit 3 comme valeur de A, le nombre X prend la valeur 3 qui est inférieure à 26 donc on n'entre pas dans la boucle « tant que » ; l'algorithme affiche la valeur de X donc 3.

2. Si on saisit 55 comme valeur de A, le nombre X prend d'abord la valeur 55 qui est supérieure à 26 ; la première fois qu'on entre dans la boucle, on remplace X par  $X - 26 = 55 - 26 = 29$ . Le nombre 29 est encore supérieur ou égal à 26 donc on entre une seconde fois dans la boucle ; le nombre X est remplacé par  $X - 26 = 29 - 26 = 3$ .

Le nombre 3 est strictement plus petit que 26 donc on n'entre pas dans la boucle et on affiche la valeur de X donc 3.

3. Dans cet algorithme, on soustrait 26 autant de fois que l'on peut du nombre positif X; on obtient un nombre entier compris entre 0 et 25 qui représente le reste de la division de X par 26 et donc le reste de la division de A par 26.

**Partie B**

Explication du codage de RE en DP, autrement dit du passage de  $\begin{pmatrix} 17 \\ 4 \end{pmatrix}$  à  $\begin{pmatrix} 3 \\ 15 \end{pmatrix}$ :

$$C \times \begin{pmatrix} 17 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 17 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 \times 17 + 1 \times 4 \\ 5 \times 17 + 2 \times 4 \end{pmatrix} = \begin{pmatrix} 51 + 4 \\ 85 + 8 \end{pmatrix} = \begin{pmatrix} 55 \\ 93 \end{pmatrix}$$

Or  $55 = 2 \times 26 + 3$  donc 55 a pour reste 3 dans la division par 26.

Et  $93 = 3 \times 26 + 15$  donc 93 a pour reste 15 dans la division par 26.

On passe donc de  $\begin{pmatrix} 55 \\ 93 \end{pmatrix}$  à  $\begin{pmatrix} 3 \\ 15 \end{pmatrix}$ , donc le codage de RE représenté par  $\begin{pmatrix} 17 \\ 4 \end{pmatrix}$  conduit à

DP représenté par  $\begin{pmatrix} 3 \\ 15 \end{pmatrix}$ .

1. Soient  $x_1, x_2, x'_1, x'_2$  quatre nombres entiers compris entre 0 et 25 tels que  $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$

et  $\begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix}$  sont transformés lors du procédé de codage en  $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ .

- a. Pour transformer  $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$  par le procédé de codage, on calcule d'abord

$$\begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3x_1 + x_2 \\ 5x_1 + 2x_2 \end{pmatrix}; \text{ puis on détermine les restes de } 3x_1 + x_2 \text{ et de } 5x_1 + 2x_2 \text{ dans la division par 26.}$$

D'après le texte, on obtient  $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$  ce qui veut dire que  $z_1$  est le reste de  $3x_1 + x_2$  dans la division par 26, et que  $z_2$  est le reste de  $5x_1 + 2x_2$  dans cette même division.

Or  $\begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix}$  est également transformé en  $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ , donc  $z_1$  est aussi le reste de  $3x'_1 + x'_2$  dans la division par 26, et  $z_2$  le reste de  $5x'_1 + 2x'_2$  dans cette même division.

Les nombres  $3x_1 + x_2$  et  $3x'_1 + x'_2$  ont le même reste  $z_1$  dans la division par 26 donc ils sont congrus modulo 26. Idem pour  $5x_1 + 2x_2$  et  $5x'_1 + 2x'_2$ .

$$\text{On a donc : } \begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 & (26) \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 & (26) \end{cases}$$

$$\text{b. } \begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 & (26) \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 & (26) \end{cases} \Rightarrow \begin{cases} 2(3x_1 + x_2) \equiv 2(3x'_1 + x'_2) & (26) \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 & (26) \end{cases} \Rightarrow$$

$$\begin{cases} 6x_1 + 2x_2 \equiv 6x'_1 + 2x'_2 & (26) \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 & (26) \end{cases} \Rightarrow x_1 \equiv x'_1 \quad (26) \text{ (par soustraction).}$$

$$\begin{cases} 3x_1 + x_2 \equiv 3x'_1 + x'_2 & (26) \\ 5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 & (26) \end{cases} \Rightarrow \begin{cases} 5(3x_1 + x_2) \equiv 5(3x'_1 + x'_2) & (26) \\ 3(5x_1 + 2x_2) \equiv 3(5x'_1 + 2x'_2) & (26) \end{cases} \Rightarrow$$

$$\begin{cases} 15x_1 + 5x_2 \equiv 15x'_1 + 5x'_2 & (26) \\ 15x_1 + 6x_2 \equiv 15x'_1 + 6x'_2 & (26) \end{cases} \Rightarrow x_2 \equiv x'_2 \quad (26) \text{ (par soustraction).}$$

Donc  $x_1 \equiv x'_1 \quad (26)$  et  $x_2 \equiv x'_2 \quad (26)$ .

$$\text{On a : } \left. \begin{matrix} x_1 \equiv x'_1 & (26) \\ 0 \leq x_1 \leq 25 \\ 0 \leq x'_1 \leq 25 \end{matrix} \right\} \Rightarrow x_1 = x'_1 \text{ et } \left. \begin{matrix} x_2 \equiv x'_2 & (26) \\ 0 \leq x_2 \leq 25 \\ 0 \leq x'_2 \leq 25 \end{matrix} \right\} \Rightarrow x_2 = x'_2$$

Il n'y a donc qu'un couple d'entiers de  $[0; 25]$   $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$  qui se code en  $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ .

2. On souhaite trouver une méthode de décodage pour le bloc DP :

a. Soit la matrice  $C' = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$ .

$$C \times C' = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} = \begin{pmatrix} 3 \times 2 + 1 \times (-5) & 3 \times (-1) + 1 \times 3 \\ 5 \times 2 + 2 \times (-5) & 5 \times (-1) + 2 \times 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$C' \times C = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} = \begin{pmatrix} 2 \times 3 + (-1) \times 5 & 2 \times 1 + (-1) \times 2 \\ (-5) \times 3 + 3 \times 5 & (-5) \times 1 + 3 \times 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Donc  $C'$  est la matrice inverse de  $C$ .

b.  $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ 15 \end{pmatrix} = \begin{pmatrix} 2 \times 3 + (-1) \times 15 \\ (-5) \times 3 + 3 \times 15 \end{pmatrix} = \begin{pmatrix} -9 \\ 30 \end{pmatrix}$  donc  $\begin{cases} y_1 = -9 \\ y_2 = 30 \end{cases}$

c. Soit  $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$  tel que  $\begin{cases} x_1 \equiv y_1 \pmod{26} \text{ avec } 0 \leq x_1 \leq 25 \\ x_2 \equiv y_2 \pmod{26} \text{ avec } 0 \leq x_2 \leq 25 \end{cases}$

autrement dit  $\begin{cases} x_1 \equiv -9 \pmod{26} \text{ avec } 0 \leq x_1 \leq 25 \\ x_2 \equiv 30 \pmod{26} \text{ avec } 0 \leq x_2 \leq 25 \end{cases}$

Or  $\begin{cases} -9 \equiv 17 \pmod{26} \text{ avec } 0 \leq 17 \leq 25 \\ 30 \equiv 4 \pmod{26} \text{ avec } 0 \leq 4 \leq 25 \end{cases}$  donc  $\begin{cases} x_1 = 17 \\ x_2 = 4 \end{cases}$

d. On peut penser que le décodage d'un couple de lettres se fait de la même manière que son codage en remplaçant la matrice  $C$  par la matrice  $C'$ .

3. Dans cette question nous allons généraliser ce procédé de décodage.

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

Soient  $y'_1$  et  $y'_2$  tels que  $\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix} = C' \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$

$$\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 2z_1 - z_2 \\ -5z_1 + 3z_2 \end{pmatrix} \text{ donc } \begin{cases} y'_1 = 2z_1 - z_2 \\ y'_2 = -5z_1 + 3z_2 \end{cases}$$

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

$$3x_1 + x_2 \equiv 3y'_1 + y'_2 \equiv 3(2z_1 - z_2) + (-5z_1 + 3z_2) \equiv 6z_1 - 3z_2 - 5z_1 + 3z_2 \equiv z_1 \pmod{26}$$

$$5x_1 + z_2 \equiv 5y'_1 + 2y'_2 \equiv 5(2z_1 - z_2) + 2(-5z_1 + 3z_2) \equiv 10z_1 - 5z_2 - 10z_1 + 6z_2 \equiv z_2 \pmod{26}$$

On peut donc dire :  $\begin{cases} 3x_1 + x_2 \equiv z_1 \pmod{26} \\ 5x_1 + 2x_2 \equiv z_2 \pmod{26} \end{cases}$

On a donc décodé la matrice colonne  $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$  en la multipliant par la matrice  $C'$

pour obtenir  $\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix}$  puis on a pris les restes module 26 pour obtenir enfin  $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ .

Le système obtenu  $\begin{cases} 3x_1 + x_2 \equiv z_1 \pmod{26} \\ 5x_1 + 2x_2 \equiv z_2 \pmod{26} \end{cases}$  prouve que la matrice  $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$  se code bien en  $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$  et donc que la matrice  $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$  se décode bien en  $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ .

4. Les deux lettres QC correspondent à la matrice colonne  $\begin{pmatrix} 16 \\ 2 \end{pmatrix}$ .

$$\text{On calcule } C' \times \begin{pmatrix} 16 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 16 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \times 16 + (-1) \times 2 \\ (-5) \times 16 + 3 \times 2 \end{pmatrix} = \begin{pmatrix} 32 - 2 \\ -80 + 6 \end{pmatrix} = \begin{pmatrix} 30 \\ -74 \end{pmatrix}$$

$$\begin{cases} 30 = 1 \times 26 + 4 \implies 30 \equiv 4 \pmod{26} \text{ avec } 0 \leq 4 \leq 25 \\ -74 = -3 \times 26 + 4 \implies -74 \equiv 4 \pmod{26} \text{ avec } 0 \leq 4 \leq 25 \end{cases}$$

Le nombre 4 correspond à la lettre E donc QC se décode en EE.