

**EXERCICE 1**

**Partie A**

1) Le nombre de groupes différents de 5 coureurs est encore le nombre de tirages simultanés de 5 numéros de dossards parmi 50 numéros. Ce nombre est

$$\binom{50}{5} = \frac{50 \times 49 \times 48 \times 47 \times 46}{5 \times 4 \times 3 \times 2 \times 1} = 10 \times 49 \times 2 \times 47 \times 46 = 2\,118\,760.$$

2) (a) L'algorithme démarre avec 5 nombres égaux à 0 puis, tant que les 5 nombres ne sont pas deux à deux distincts, il génère 5 nombres au hasard entre 1 et 50. L'algorithme s'arrête quand les 5 nombres générés sont deux à deux distincts. Par suite, l'algorithme peut fournir les ensembles  $L_2$  et  $L_4$  mais pas les ensembles  $L_1$  et  $L_3$ .

(b) L'algorithme permet de tirer au sort 5 coureurs parmi les 50 pour subir un contrôle anti-dopage.

3) Il y a 50 choix possibles de 1 coureur parmi 50 et 5 choix de 1 coureur parmi les 5 qui subissent un contrôle. La probabilité qu'un coureur subisse un contrôle est donc

$$p = \frac{5}{50} = 0,1.$$

4) (a) La variable aléatoire  $X$  est régie par un schéma de BERNOULLI. En effet,

- 10 expériences identiques et indépendantes sont effectuées ;
- chaque expérience a deux issues : « le coureur subit un contrôle » avec une probabilité  $p = 0,1$  ou « le coureur ne subit pas de contrôle » avec une probabilité  $1 - p = 0,9$ .

La variable aléatoire  $X$  suit donc une loi binomiale de paramètres  $n = 10$  et  $p = 0,1$ .

On sait alors que pour tout entier  $k$  tel que  $0 \leq k \leq 10$ ,

$$p(X = k) = \binom{10}{k} (0,1)^k (0,9)^{10-k}.$$

(b) •  $p(X = 5) = \binom{10}{5} (0,1)^5 (0,9)^5 = \frac{10 \times 9 \times 8 \times 7 \times 6}{5 \times 4 \times 3 \times 2 \times 1} (0,09)^5 = 3 \times 2 \times 7 \times 6 \times (0,09)^5 = 0,0015$  arrondie au dix millième.

La probabilité que le coureur soit contrôlé 5 fois exactement est 0,0015 arrondie au dix millième.

•  $p(X = 0) = \binom{10}{0} (0,1)^0 (0,9)^{10} = (0,9)^{10} = 0,3487$  arrondie au dix millième.

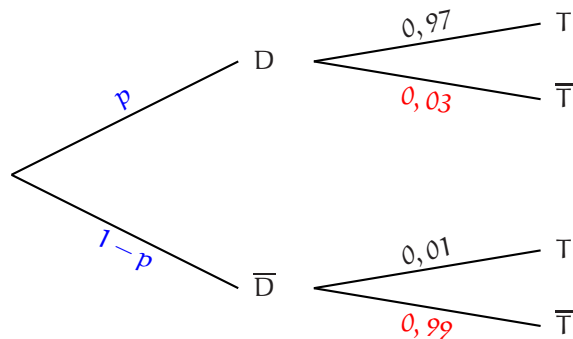
La probabilité que le coureur ne soit pas contrôlé est 0,3487 arrondie au dix millième.

•  $p(X \geq 1) = 1 - p(X = 0) = 1 - (0,9)^{10} = 0,6513$  arrondie au dix millième.

La probabilité que le coureur soit contrôlé au moins une fois est 0,6513 arrondie au dix millième.

## Partie B

1) L'énoncé fournit  $p(T) = 0,05$ ,  $p_D(T) = 0,97$  et  $p_{\overline{D}}(T) = 0,01$ . Posons  $p(D) = p$ . Représentons la situation par un arbre :



La formule des probabilités totales fournit :

$$p(T) = p(D \cap T) + p(\overline{D} \cap T) = p(D) \times p_D(T) + p(\overline{D}) \times p_{\overline{D}}(T),$$

et donc  $0,97p + 0,01(1 - p) = 0,05$  puis  $0,96p = 0,04$  et finalement

$$p(D) = \frac{0,04}{0,96} = \frac{4}{96} = \frac{1}{24}.$$

$$p(D) = \frac{1}{24}.$$

2) La probabilité demandée est  $p_T(\overline{D})$ .

$$p_T(\overline{D}) = \frac{p(T \cap \overline{D})}{p(T)} = \frac{p(\overline{D}) \times p_{\overline{D}}(T)}{p(T)} = \frac{\left(1 - \frac{1}{24}\right) \times \frac{1}{100}}{\frac{5}{100}} = \frac{23}{24} \times \frac{1}{100} \times \frac{100}{5} = \frac{23}{120}.$$

$$p_T(\overline{D}) = \frac{23}{120}.$$

## EXERCICE 2

**Proposition 1.**      **VRAI**

**Proposition 2.**      **FAUX**

**Proposition 3.**      **VRAI**

**Proposition 4.**      **VRAI**

**Justification 1** Un vecteur directeur de la droite  $\mathcal{D}$  est le vecteur  $\vec{u}$  de coordonnées  $(-2, 2, 2)$ . Un vecteur normal au plan  $\mathcal{P}$  est le vecteur  $\vec{n}$  de coordonnées  $(1, -1, -1)$ . On remarque que  $\vec{u} = -2\vec{n}$  et en particulier  $\vec{u}$  est colinéaire à  $\vec{n}$ . On en déduit que la droite  $\mathcal{D}$  est orthogonale au plan  $\mathcal{P}$ . La proposition 1 est vraie.

**Justification 2** La distance du centre O de la sphère  $\mathcal{S}$  au plan  $\mathcal{P}$  est

$$d = \frac{|0 - 0 - 0 - 2|}{\sqrt{1^2 + (-1)^2 + (-1)^2}} = \frac{2}{\sqrt{3}}.$$

La distance  $d$  n'est pas égale au rayon de la sphère  $\mathcal{S}$  et donc la sphère  $\mathcal{S}$  n'est pas tangente au plan  $\mathcal{P}$ . La proposition 2 est fautive.

**Justification 3** Un vecteur normal au plan  $\mathcal{P}'$  est le vecteur  $\vec{n}'$  de coordonnées  $(1, 1, 3)$ . Les vecteurs  $\vec{n}$  et  $\vec{n}'$  ne sont pas colinéaires car s'il existe un réel  $k$  tel que  $\vec{n}' = k\vec{n}$  alors  $k = 1$  et aussi  $k = -1$  ce qui est impossible.

On en déduit que les plans  $\mathcal{P}$  et  $\mathcal{P}'$  ne sont pas parallèles et donc que  $\mathcal{P}$  et  $\mathcal{P}'$  sont sécants en une droite  $\Delta$ .

Notons  $\Delta'$  la droite de représentation paramétrique 
$$\begin{cases} x = 1 - t' \\ y = -1 - 2t' \\ z = t' \end{cases}, t' \in \mathbb{R}.$$

Pour tout réel  $t'$ ,

$$(1 - t') - (-1 - 2t') - (t') - 2 = 0 \text{ et } (1 - t') + (-1 - 2t') + 3(t') = 0.$$

Donc tout point de la droite  $\Delta'$  appartient au plan  $\mathcal{P}$  et au plan  $\mathcal{P}'$  ou encore la droite  $\Delta'$  est contenue dans le plan  $\mathcal{P}$  et dans le plan  $\mathcal{P}'$ . Finalement,  $\Delta'$  est la droite  $\Delta$  d'intersection des plans  $\mathcal{P}$  et  $\mathcal{P}'$  ou encore un système d'équations

paramétriques de  $\Delta$  est 
$$\begin{cases} x = 1 - t' \\ y = -1 - 2t' \\ z = t' \end{cases}, t' \in \mathbb{R}.$$
 La proposition 3 est vraie.

**Justification 4** Un vecteur directeur de  $\Delta$  est le vecteur  $\vec{u}'$  de coordonnées  $(-1, -2, 1)$ . Les vecteurs  $\vec{u}$  et  $\vec{u}'$  ne sont pas colinéaires et donc les droites  $\mathcal{D}$  et  $\Delta$  ne sont pas parallèles. On en déduit que les droites  $\mathcal{D}$  et  $\Delta$  sont sécantes ou non coplanaires.

Déterminons alors l'intersection de  $\mathcal{D}$  et  $\Delta$ . Soient  $M(-3 - 2t, 2t, 1 + 2t)$ ,  $t \in \mathbb{R}$ , un point de  $\mathcal{D}$  et  $M'(1 - t', -1 - 2t', t')$ ,  $t' \in \mathbb{R}$ , un point de  $\Delta$ .

$$M = M' \Leftrightarrow \begin{cases} -3 - 2t = 1 - t' \\ 2t = -1 - 2t' \\ 1 + 2t = t' \end{cases} \Leftrightarrow \begin{cases} t' = 1 + 2t \text{ (*)} \\ -3 - 2t = 1 - (1 + 2t) \\ 2t = -1 - 2(1 + 2t) \end{cases} \Leftrightarrow \begin{cases} t' = 1 + 2t \\ -3 = 0 \\ 2t = -1 - 2(1 + 2t) \end{cases}$$

Ce système n'a pas de solution et donc  $\mathcal{D}$  et  $\Delta$  n'ont aucun point commun. Finalement, les droites  $\mathcal{D}$  et  $\Delta$  sont non coplanaires. La proposition 4 est vraie.

### EXERCICE 3

1) (a) Soit  $n \in \mathbb{N}$ . La fonction  $f_n$  est continue et positive sur  $[0, 1]$ . Donc,  $I_n$  est l'aire du domaine du plan  $\mathcal{D}_n$  délimité par les droites d'équations respectives  $x = 0$  et  $x = 1$  d'une part, l'axe des abscisses et la courbe représentative de la fonction  $f_n$  d'autre part.

Il semble que pour chaque entier naturel  $n$ , le graphe de  $f_n$  soit au-dessus du graphe de  $f_{n+1}$  sur  $[0, 1]$  et donc que l'aire du domaine  $\mathcal{D}_n$  soit plus grande que l'aire du domaine  $\mathcal{D}_{n+1}$ . En résumé, il semble que pour tout entier naturel  $n$ ,  $I_{n+1} \leq I_n$  ou encore, il semble que la suite  $(I_n)$  soit décroissante.

(b) Soit  $n \in \mathbb{N}$ .

$$\begin{aligned} I_n - I_{n+1} &= \int_0^1 \frac{e^{-nx}}{1+x} dx - \int_0^1 \frac{e^{-(n+1)x}}{1+x} dx = \int_0^1 \left( \frac{e^{-nx}}{1+x} - \frac{e^{-(n+1)x}}{1+x} \right) dx \quad (\text{par linéarité de l'intégrale}) \\ &= \int_0^1 \frac{e^{-nx} - e^{-(n+1)x}}{1+x} dx = \int_0^1 \frac{e^{-nx}(1 - e^{-x})}{1+x} dx. \end{aligned}$$

Soit  $x \in [0, 1]$ . On a  $e^{-nx} \geq 0$  et  $\frac{1}{1+x} \geq 0$ . Ensuite,  $-x \leq 0$  et donc  $e^{-x} \leq 1$  puis  $1 - e^{-x} \geq 0$ . Finalement,

$$\frac{e^{-nx}(1 - e^{-x})}{1+x} \geq 0.$$

Ainsi, pour tout réel  $x$  de  $[0, 1]$ ,  $\frac{e^{-nx}(1 - e^{-x})}{1+x} \geq 0$ . Par positivité de l'intégrale, on en déduit que  $\int_0^1 \frac{e^{-nx}(1 - e^{-x})}{1+x} dx \geq 0$  ou encore que  $I_n - I_{n+1} \geq 0$  ou enfin que  $I_{n+1} \leq I_n$ .

On a montré que pour tout entier naturel  $n$ ,  $I_{n+1} \leq I_n$  et donc que

la suite  $(I_n)$  est décroissante.

2) (a) Soit  $n \in \mathbb{N}$ . Soit  $x \in [0, 1]$ . Alors  $1+x \geq 1$  puis  $\frac{1}{1+x} \leq 1$ . En multipliant les membres de cette inégalité par le réel positif  $e^{-nx}$ , on obtient

$$\frac{e^{-nx}}{1+x} \leq e^{-nx}.$$

En multipliant les deux membres de l'inégalité  $\frac{1}{1+x} \leq 1$  par le réel positif  $\frac{e^{-nx}}{1+x}$ , on obtient aussi

$$\frac{e^{-nx}}{(1+x)^2} \leq \frac{e^{-nx}}{1+x}.$$

Enfin,  $\frac{e^{-nx}}{(1+x)^2} \geq 0$  et on a montré que

Pour tout  $n \in \mathbb{N}$  et tout  $x \in [0, 1]$ ,  $0 \leq \frac{e^{-nx}}{(1+x)^2} \leq \frac{e^{-nx}}{1+x} \leq e^{-nx}$ .

(b) D'après la question précédente et par positivité et croissance de l'intégrale, pour tout entier naturel  $n$  on a

$$0 \leq \int_0^1 \frac{e^{-nx}}{(1+x)^2} dx \leq \int_0^1 \frac{e^{-nx}}{1+x} dx \leq \int_0^1 e^{-nx} dx. \quad (*)$$

Mais pour tout entier naturel non nul  $n$ ,

$$\int_0^1 e^{-nx} dx = \left[ \frac{e^{-nx}}{-n} \right]_0^1 = \frac{e^{-n}}{-n} - \frac{1}{-n} = \frac{1 - e^{-n}}{n}.$$

On sait que  $\lim_{n \rightarrow +\infty} e^{-n} = 0$  et d'autre part,  $\lim_{n \rightarrow +\infty} \frac{1}{n} = 0$ . Par suite,  $\lim_{n \rightarrow +\infty} \frac{1}{n}(1 - e^{-n}) = 0 \times (1 - 0) = 0$ .

Les inégalités (\*) montrent que pour tout entier naturel non nul  $n$ , on a  $0 \leq I_n \leq \frac{1}{n}(1 - e^{-n})$ . Le théorème des gendarmes permet alors d'affirmer que la suite  $(I_n)$  converge et que

$$\lim_{n \rightarrow +\infty} I_n = 0.$$

Les inégalités (\*) montrent aussi que pour tout entier naturel non nul  $n$ , on a  $0 \leq J_n \leq I_n$ . Le théorème des gendarmes permet alors d'affirmer que la suite  $(J_n)$  converge et que

$$\lim_{n \rightarrow +\infty} J_n = 0.$$

**3) (a)** Soit  $n \geq 1$ . Pour  $x$  dans  $[0, 1]$ , posons  $u(x) = \frac{1}{1+x}$  et  $v(x) = \frac{e^{-nx}}{-n}$ . Les fonctions  $u$  et  $v$  sont dérivables sur  $[0, 1]$  et pour  $x$  dans  $[0, 1]$ , on a

$$\begin{aligned} u(x) &= \frac{1}{1+x} & v(x) &= \frac{e^{-nx}}{-n} \\ u'(x) &= -\frac{1}{(1+x)^2} & v'(x) &= e^{-nx} \end{aligned}$$

De plus, les fonctions  $u'$  et  $v'$  sont continues sur  $[0, 1]$ . On peut donc effectuer une intégration par parties et on obtient

$$\begin{aligned} I_n &= \int_0^1 \frac{1}{1+x} \times e^{-nx} \, dx = \left[ \frac{1}{1+x} \times \frac{e^{-nx}}{-n} \right]_0^1 - \int_0^1 \frac{-1}{(1+x)^2} \times \frac{e^{-nx}}{-n} \, dx \\ &= \frac{1}{2} \times \frac{e^{-n}}{-n} - 1 \times \frac{e^0}{-n} - \frac{1}{n} \int_0^1 \frac{e^{-nx}}{(1+x)^2} \, dx \quad (\text{par linéarité de l'intégrale}) \\ &= \frac{1}{n} - \frac{e^{-n}}{2n} - \frac{1}{n} J_n \\ &= \frac{1}{n} \left( 1 - \frac{e^{-n}}{2} - J_n \right). \end{aligned}$$

On a montré que

$$\text{pour tout entier naturel non nul } n, I_n = \frac{1}{n} \left( 1 - \frac{e^{-n}}{2} - J_n \right).$$

**(b)** Pour tout entier naturel non nul,  $nI_n = 1 - \frac{e^{-n}}{2} - J_n$ . Puisque  $\lim_{n \rightarrow +\infty} e^{-n} = 0$  et  $\lim_{n \rightarrow +\infty} J_n = 0$ , on en déduit que

$$\lim_{n \rightarrow +\infty} nI_n = 1.$$

## EXERCICE 4

### Partie A Restitution organisée de connaissances

Puisque  $a \equiv b \pmod{n}$  et  $c \equiv d \pmod{n}$ , il existe deux entiers relatifs  $k$  et  $k'$  tels que  $b = a + kn$  et  $d = c + k'n$ . Mais alors,

$$bd = (a + kn)(c + k'n) = ac + ak'n + ckn + kk'n^2 = ac + (ak' + ck + kk'n)n$$

Posons  $K = ak' + ck + kk'n$ .  $K$  est un entier relatif tel que  $bd = ac + Kn$  et on a donc montré que  $ac \equiv bd \pmod{n}$ .

### Partie B Inverse de 23 modulo 26

1)  $23 \times (-9) - 26 \times (-8) = -207 + 208 = 1$ . Donc le couple  $(-9, -8)$  est solution de l'équation (E).

2) Posons  $(x_0, y_0) = (-9, -8)$ . Soient  $x$  et  $y$  deux entiers relatifs.

$$(x, y) \text{ solution de (E)} \Leftrightarrow 23x - 26y = 1 \Leftrightarrow 23x - 26y = 23x_0 - 26y_0 \Leftrightarrow 23(x - x_0) = 26(y - y_0).$$

Si  $(x, y)$  est solution de (E), alors l'entier 26 divise l'entier  $26(y - y_0) = 23(x - x_0)$ . D'autre part, la question précédente montre qu'il existe deux entiers relatifs  $u$  et  $v$  tels que  $23u + 26v = 1$ . Le théorème de BÉZOUT permet alors d'affirmer que les entiers 23 et 26 sont premiers entre eux.

Ainsi, 26 divise  $23(x - x_0)$  et 26 est premier à 23. D'après le théorème de GAUSS, 26 divise  $x - x_0$ . Par suite, il existe un entier relatif  $k$  tel que  $x - x_0 = 26k$  ou encore tel que  $x = -9 + 26k$ . De même, il existe un entier relatif  $k'$  tel que  $y = -8 + 23k'$ .

En résumé, si  $(x, y)$  est solution de (E), il existe deux entiers relatifs  $k$  et  $k'$  tels que  $x = -9 + 26k$  et  $y = -8 + 23k'$ . Réciproquement, soient  $k$  et  $k'$  deux entiers relatifs puis  $x = -9 + 26k$  et  $y = -8 + 23k'$ .

$$(x, y) \text{ est solution de (E)} \Leftrightarrow 23(-9 + 26k) - 26(-8 + 23k') = 1 \Leftrightarrow 1 + 23 \times 26 \times (k - k') = 1 \Leftrightarrow k = k'.$$

Les solutions de (E) sont les couples d'entiers relatifs de la forme  $(-9 + 26k, -8 + 23k)$ ,  $k \in \mathbb{Z}$ .

3) Soit  $a$  un entier relatif.  $23a \equiv 1 \pmod{26}$  si et seulement si il existe un entier relatif  $y$  tel que  $23a - 26y = 1$ . D'après la question précédente, ceci impose l'existence d'un entier relatif  $k$  tel que  $a = -9 + 26k$ . Ensuite,

$$0 \leq a \leq 25 \Leftrightarrow 0 \leq -9 + 26k \leq 25 \Leftrightarrow 9 \leq 26k \leq 34 \Leftrightarrow \frac{9}{26} \leq k \leq \frac{34}{26} \Leftrightarrow k = 1.$$

Pour  $k = 1$ , on obtient  $a = -9 + 26 = 17$ . Réciproquement, puisque  $17 \times 23 = 391 = 1 + 15 \times 26$ , l'entier  $a = 17$  est un entier tel que  $0 \leq a \leq 25$  et  $23a \equiv 1 \pmod{26}$ .

$$\boxed{a = 17.}$$

### Partie C Chiffrement de Hill

1) **Etape 1.** ST correspond à  $(x_1, x_2) = (18, 19)$ .

**Etape 2.** •  $11x_1 + 3x_2 = 11 \times 18 + 3 \times 19 = 198 + 57 = 255$ .  $y_1$  est alors le reste de la division euclidienne de 255 par 26. Comme  $255 = 21 + 234 = 21 + 9 \times 26$  et que  $0 \leq 21 \leq 25$ , on en déduit que  $y_1 = 21$ .

•  $7x_1 + 4x_2 = 7 \times 18 + 4 \times 19 = 126 + 76 = 202$ . Comme  $202 = 20 + 182 = 20 + 7 \times 26$  et que  $0 \leq 20 \leq 25$ , on en déduit que  $y_2 = 20$ .

**Etape 3.** Le couple  $(21, 20)$  correspond au mot VU et donc

$$\boxed{\text{le mot ST se code en VU.}}$$

2) (a) Soient  $x_1, x_2, y_1$  et  $y_2$  quatre entiers.

$$\begin{aligned} \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} &\Rightarrow \begin{cases} 4y_1 + 23y_2 \equiv (4 \times 11 + 23 \times 7)x_1 + (4 \times 3 + 23 \times 4)x_2 \pmod{26} \\ 19y_1 + 11y_2 \equiv (19 \times 11 + 11 \times 7)x_1 + (19 \times 3 + 11 \times 4)x_2 \pmod{26} \end{cases} \\ &\Rightarrow \begin{cases} 4y_1 + 23y_2 \equiv 205x_1 + 104x_2 \pmod{26} \\ 19y_1 + 11y_2 \equiv 286x_1 + 101x_2 \pmod{26} \end{cases} \\ &\Rightarrow \begin{cases} 4y_1 + 23y_2 \equiv 23x_1 \pmod{26} \\ 19y_1 + 11y_2 \equiv 23x_2 \pmod{26} \end{cases} \end{aligned}$$

car  $205 = 23 + 7 \times 26$ ,  $104 = 4 \times 26$ ,  $286 = 11 \times 26$  et  $101 = 23 + 3 \times 26$  et donc  $205 \equiv 23 \pmod{26}$ ,  $104 \equiv 0 \pmod{26}$ ,  $286 \equiv 0 \pmod{26}$  et  $101 \equiv 23 \pmod{26}$ .

(b) On multiplie alors les deux membres de chaque congruence écrite par 17. D'après la question 3) de la partie A, on a  $23 \times 17 \equiv 1 \pmod{26}$  et donc on obtient

$$\begin{aligned} \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \pmod{26} \\ 23x_2 \equiv 19y_1 + 11y_2 \pmod{26} \end{cases} &\Rightarrow \begin{cases} x_1 \equiv 4 \times 17y_1 + 23 \times 17y_2 \pmod{26} \\ x_2 \equiv 19 \times 17y_1 + 11 \times 17y_2 \pmod{26} \end{cases} \\ &\Rightarrow \begin{cases} x_1 \equiv 68y_1 + 391y_2 \pmod{26} \\ x_2 \equiv 323y_1 + 187y_2 \pmod{26} \end{cases} \Rightarrow \begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases} \end{aligned}$$

car  $68 = 16 + 2 \times 26$ ,  $391 = 1 + 15 \times 26$ ,  $323 = 11 + 12 \times 26$  et  $187 = 5 + 7 \times 26$  et donc  $68 \equiv 16 \pmod{26}$ ,  $391 \equiv 1 \pmod{26}$ ,  $323 \equiv 11 \pmod{26}$  et  $187 \equiv 5 \pmod{26}$ .

(c) Réciproquement,

$$\begin{aligned} \begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases} &\Rightarrow \begin{cases} 11x_1 + 3x_2 \equiv 209y_1 + 26y_2 \pmod{26} \\ 7x_1 + 4x_2 \equiv 156y_1 + 27y_2 \pmod{26} \end{cases} \\ &\Rightarrow \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \end{aligned}$$

car  $209 = 1 + 8 \times 26$ ,  $26 = 0 + 1 \times 26$ ,  $156 = 0 + 6 \times 26$  et  $27 = 1 + 1 \times 26$  et donc  $209 \equiv 1 \pmod{26}$ ,  $26 \equiv 0 \pmod{26}$ ,  $156 \equiv 0 \pmod{26}$  et  $27 \equiv 1 \pmod{26}$ . En résumé,

$$\boxed{\begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases} .}$$

(d) • Le mot **YJ** correspond au couple  $(y_1, y_2) = (24, 9)$ .

•  $16y_1 + y_2 = 16 \times 24 + 9 = 393 = 3 + 15 \times 26$  et donc  $x_1 = 3$ .

$11y_1 + 5y_2 = 11 \times 24 + 5 \times 9 = 309 = 23 + 11 \times 26$  et donc  $x_2 = 23$ .

• Le couple  $(3, 23)$  correspond au mot **DX** et donc

le mot **YJ** se décode en **DX**.