EXERCICE 1 (6 points) Commun à tous les candidats

Les deux parties sont indépendantes.

Partie A

Un groupe de 50 coureurs ; portant des dossards numérotés de 1 à 50 ; participe à une course cycliste qui comprend 10 étapes ; et au cours de laquelle aucun abandon n'est constaté.

À la fin de chaque étape ; un groupe de 5 coureurs est choisi au hasard pour subir un contrôle antidopage. Ces désignations de 5 coureurs à l'issue de chacune des étapes sont indépendantes. Un même coureur peut donc être contrôlé à l'issue de plusieurs étapes.

1. À l'issue de chaque étape, combien peut-on former de groupes différents de 5 coureurs ?
2. On considère l'algorithme ci-dessous dans lequel

- *a* rand(1, 50) » permet d'obtenir un nombre entier aléatoire appartenant à l'intervalle [1 ; 50]
- l'écriture *a* *x* := *y* » désigne l'affectation d'une valeur *y* à une variable *x*.

Variables	*a*, *b*, *c*, *d*, e sont des variables du type entier
Initialisation	*a*: = 0 ; *b*: = 0 ; *c*: = 0 ; *d*: = 0 ; *e*: = 0
Traitement	Tant que (*a* = *b*) ou (*a* = *c*) ou (*a* = *d*) ou (*a* = *e*) ou (*b* = *c*) ou (*b* = *d*) ou (*b* = *e*) ou (*c* = *d*) ou (*c* = *e*) ou (*d* = *e*)
	Début du tant que
	a := rand(1, 50) ; *b* := rand(1, 50) ; *c* := rand(1, 50) ; *d* := rand(1, 50) ; *e*:= rand(1, 50)
	Fin du tant que
Sortie	Afficher *a*, *b*, *c*, *d*, *e*

a. Parmi les ensembles de nombres suivants, lesquels ont pu être obtenus avec cet algorithme

$L_1 = \{2, 11, 44, 2, 15\}$; $L_2 = \{8, 17, 41, 34, 6\}$;

$L_3 = \{12, 17, 23, 17, 50\}$; $L_4 = \{45, 19, 43, 21, 18\}$?

b. Que permet de réaliser cet algorithme concernant la course cycliste ?

3. À l'issue d'une étape, on choisit au hasard un coureur parmi les 50 participants. Établir que la probabilité pour qu'il subisse le contrôle prévu pour cette étape est égale à 0,1.

4. On note X la variable aléatoire qui comptabilise le nombre de contrôles subis par un coureur sur l'ensemble des 10 étapes de la course.

a. Quelle est la loi de probabilité de la variable aléatoire X ? Préciser ses paramètres.

b. On choisit au hasard un coureur à l'arrivée de la course. Calculer, sous forme décimale arrondie au dix-millième, les probabilités des événements suivants

- il a été contrôlé 5 fois exactement ;
- il n'a pas été contrôlé ;
- il a été contrôlé au moins une fois.

Partie B

Dans cette partie, toute trace de recherche même incomplète, ou d'*initiative même non fructueuse, sera prise en compte dans* l'*évaluation.*

On donnera les résultats sous forme de fraction irréductible.

Pour un coureur choisi au hasard dans l'ensemble des 50 coureurs, on appelle T l'événement « le contrôle est positif », et d'après des statistiques, on admet que P(T) = 0,05.

On appelle D l'événement : « le coureur est dopé ».

Le contrôle anti-dopage n'étant pas fiable à 100 %, on sait que :

- si un coureur est dopé, le contrôle est positif dans 97 % des cas ;
- si un coureur n'est pas dopé, le contrôle est positif dans 1 % des cas.

1. Calculer P(D).
2. Un coureur a un contrôle positif. Quelle est la probabilité qu'il ne soit pas dopé ?

EXERCICE 2 (4 points) Commun à tous les candidats

Dans le repère orthonormé $(O ; \vec{i}, \vec{j}, \vec{k})$ de l'espace, on considère :

- les plans $\mathcal{P}$ et $\mathcal{P}'$ d'équations $\mathcal{P} : x - y - z - 2 = 0$ et $\mathcal{P}' : x + y + 3z = 0$.
- la droite $\mathcal{D}$ ayant pour représentation paramétrique $\begin{cases} x = -3 - 2t \\ y = 2t \\ z = 1 + 2t \end{cases} \quad t \in \mathbb{R}$.

Pour chacune des propositions suivantes, indiquer si elle est vraie ou fausse, et justifier la réponse. Une justification est attendue pour chaque réponse.

Proposition 1 : La droite $\mathcal{D}$ est orthogonale au plan $\mathcal{P}$.

Proposition 2 : La sphère $\mathcal{S}$ de centre O et de rayon 2 est tangente au plan $\mathcal{P}$.

Proposition 3 : L'intersection des plans $\mathcal{P}$ et $\mathcal{P}'$ est la droite Δ dont une représentation paramétrique est $\begin{cases} x = 1 - t' \\ y = -1 - 2t' \\ z = t' \end{cases}$; $t' \in \mathbb{R}$.

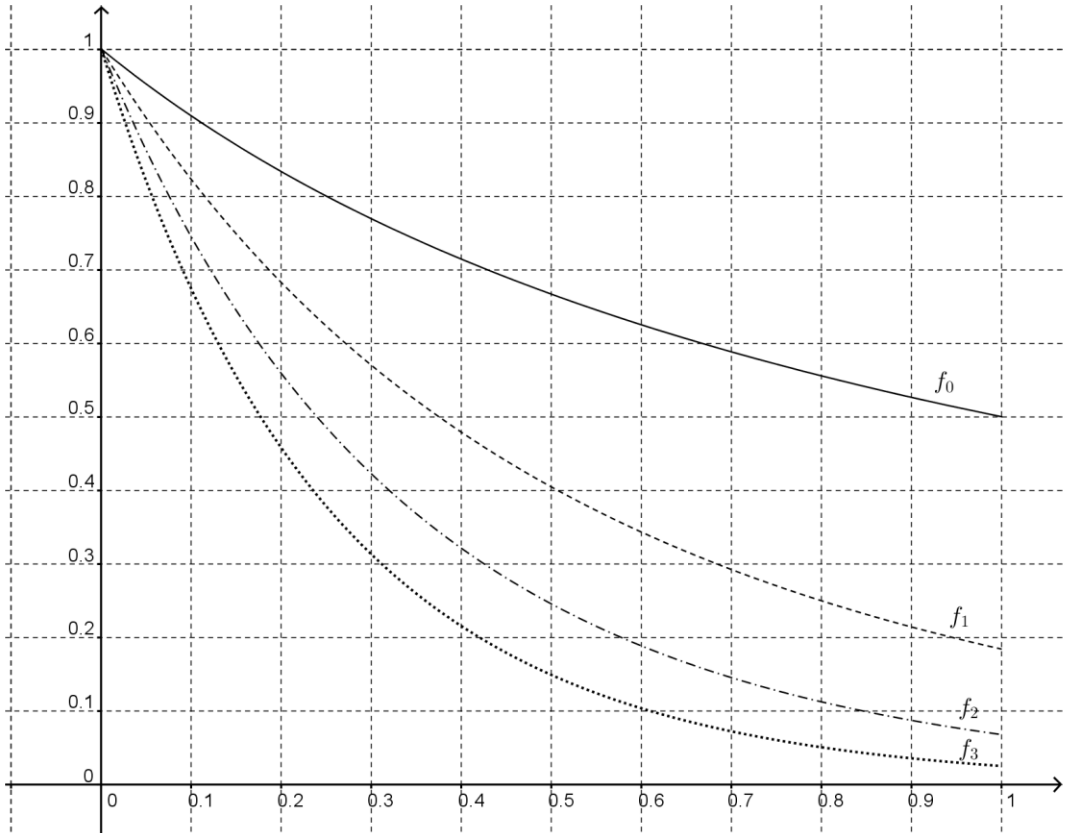
Proposition 4 : Les droites $\mathcal{D}$ et Δ sont coplanaires.

EXERCICE 3 (5 points) Commun à tous les candidats

On considère les suites (I_n) et (J_n) définies pour tout entier naturel n par :

$$I_n = \int_0^1 \frac{e^{-nx}}{1+x}\,dx \quad \text{et } J_n = \int_0^1 \frac{e^{-nx}}{(1+x)^2}\,dx$$

1. Sont représentées ci-dessous les fonctions f_n définies sur l'intervalle [0 ; 1] par $f_n(x) = \dfrac{e^{-nx}}{1+x}$ pour différentes valeurs de n.



a. Formuler une conjecture sur le sens de variation de la suite (I_n) en expliquant la démarche.

b. Démontrer cette conjecture.

2. *a*. Montrer que pour tout entier $n > 0$ et pour tout nombre réel x de l'intervalle [0 ; 1]

$$0 \leq \frac{e^{-nx}}{(1+x)^2} \leq \frac{e^{-nx}}{1+x} \leq e^{-nx}$$

b. Montrer que les suites (I_n) et (J_n) sont convergentes et déterminer leur limite.

3. *a*. Montrer, en effectuant une intégration par parties, que pour tout entier $n \geq 1$: $I_n = \dfrac{1}{n}\left(1 - \dfrac{e^{-n}}{2} - J_n\right)$

b. En déduire $\lim\limits_{n \to +\infty} n\, I_n$

EXERCICE 4 (5 points) Candidats ayant suivi l'enseignement de spécialité

Partie A Restitution organisée de connaissance

Soit a, b, c, d des entiers relatifs et n un entier naturel non nul.

Montrer que si $a \equiv b \pmod n$ et $c \equiv d \pmod n$ alors $a\,c \equiv b\,d \pmod n$.

Partie B Inverse de 23 modulo 26

On considère l'équation (E) : $23\,x - 26\,y = 1$, où x et y désignent deux entiers relatifs.

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

Partie C Chiffrement de Hill

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

Étape1 Chaque lettre du mot est remplacée par un entier en utilisant le tableau ci-dessous

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

On obtient un couple d'entiers (x_1, x_2) où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

Étape 2 (x_1, x_2) est transformé en (y_1, y_2) tel que (S_1) $\begin{cases} y_1 \equiv 11\,x_1 + 3\,x_2 \mod 26 \\ y_2 \equiv 7\,x_1 + 4\,x_2 \mod 26 \end{cases}$ avec $0 \leq y_1 \leq 25$ et $0 \leq y_2 \leq 25$.

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

Exemple : $\underset{\text{mot en clair}}{\mathrm{TE}} \xrightarrow{\text{étape 1}} (19, 4) \xrightarrow{\text{étape 2}} (13, 19) \xrightarrow{\text{étape 3}} \underset{\text{mot codé}}{\mathrm{NT}}$

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

a. Montrer que tout couple (x_1, x_2) vérifiant les équations du système (S_1), vérifie les équations du système

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

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

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

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

d. Décoder le mot YJ.

EXERCICE 4 (5 points) Candidats n'ayant pas suivi l'enseignement de spécialité

Partie A Restitution organisée de connaissances

Soit z un nombre complexe. On rappelle que $\bar{z}$ est le conjugué de z et que $|z|$ est le module de z. On admet l'égalité : $|z|^2 = z\,\bar{z}$.

Montrer que, si z_1 et z_2 sont deux nombres complexes, alors $|z_1\,z_2| = |z_1|\,|z_2|$.

Partie B Étude d'une transformation particulière

Dans le plan complexe rapporté au repère orthonormal direct $(O\,; \vec{u}, \vec{v})$ on désigne par A et B les points d'affixes respectives 1 et – 1.

Soit f la transformation du plan qui à tout point M d'affixe $z \neq 1$, associe le point M' d'affixe z' tel que $z' = \dfrac{1 - \bar{z}}{z - 1}$.

1. Soit C le point d'affixe $z_C = -2 + \mathrm{i}$.

a. Calculer l'affixe $z_{C'}$ du point C' image de C par la transformation f, et placer les points C et C' dans le repère donné en annexe.

b. Montrer que le point C' appartient au cercle $\mathscr{C}$ de centre O et de rayon 1.

c. Montrer que les points A, C et C' sont alignés.

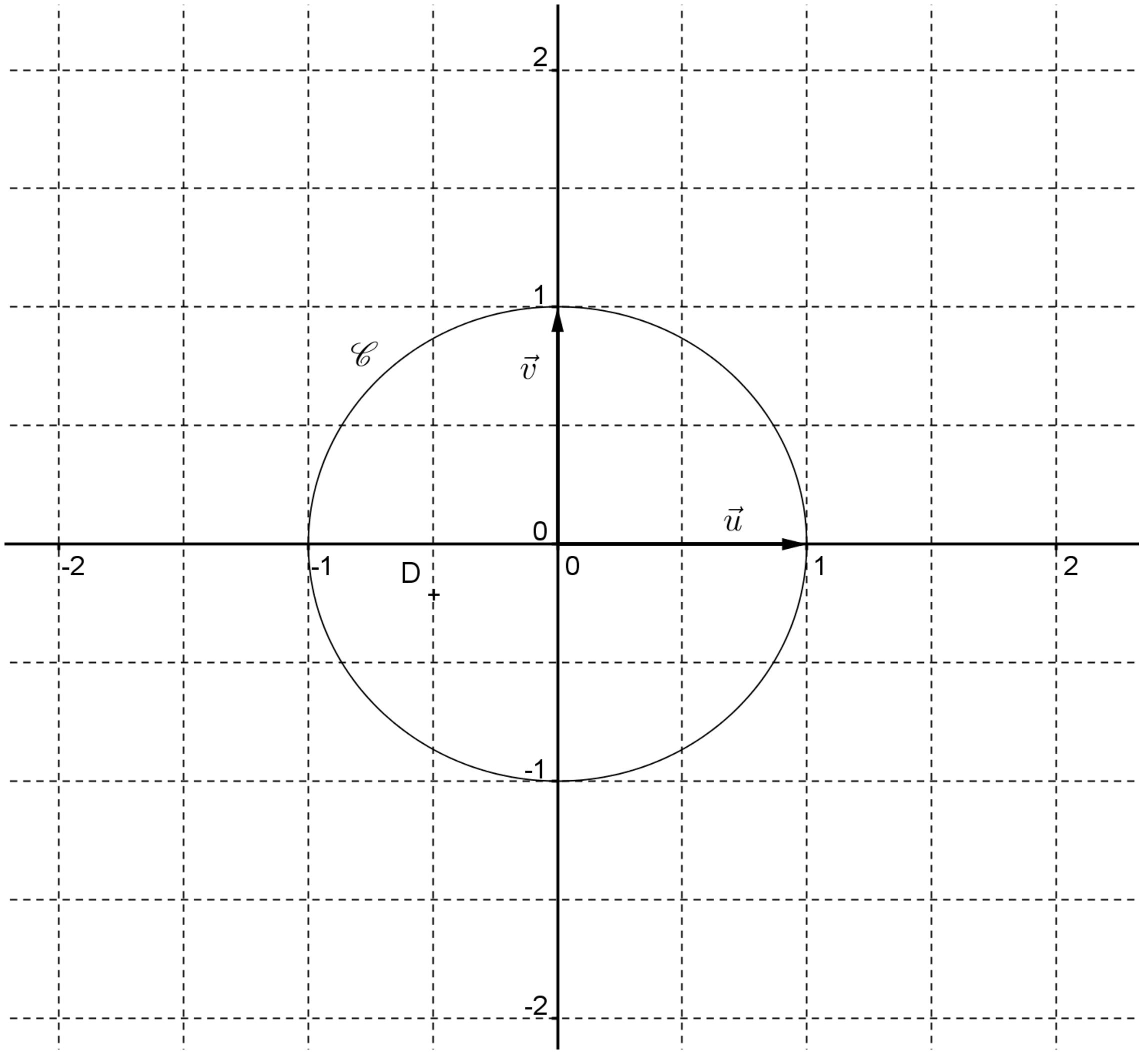
2. Déterminer et représenter sur la figure donnée en annexe l'ensemble Δ des points du plan qui ont le point A pour image par la transformation f.
3. Montrer que, pour tout point M distinct de A ; le point M' appartient au cercle $\mathscr{C}$.
4. Montrer que, pour tout nombre complexe $z \neq 1$; $\dfrac{z' - 1}{z - 1}$ est réel.

Que peut-on en déduire pour les points A, M et M' ?

5. On a placé un point D sur la figure donnée en annexe. Construire son image D' par la transformation f.

Annexe à rendre avec la copie

EXERCICE 4



CORRECTION

EXERCICE 1

Partie A

1. Il faut choisir au hasard sans ordre ni répétition 5 coureurs parmi 50 donc à l'issue de chaque étape, on peut former de $\binom{50}{5}$ soit 211 8760 groupes différents de 5 coureurs.

2. *a*. $L_1 = \{2, 11, 44, 2, 15\}$; exclu ($a = d$)
$L_2 = \{8, 17, 41, 34, 6\}$; possible : 5 nombres deux à deux distincts compris entre 1 et 50
$L_3 = \{12, 17, 23, 17, 50\}$; exclu ($b = d$)
$L_4 = \{45, 19, 43, 21, 18\}$ possible : 5 nombres deux à deux distincts compris entre 1 et 50
b. L'algorithme consiste à choisir 5 numéros deux à deux distincts pris entre 1 et 50 donc à choisir les dossards des cyclistes qui subiront un test anti-dopage.

3. A l'issue de chaque étape, on peut former de $\binom{50}{5}$ groupes différents de 5 coureurs.

On choisit au hasard un coureur parmi les 50 participants, on peut former $\binom{49}{4}$ groupes différents de 5 coureurs dans lesquels figure le coureur choisi donc la probabilité qu'il subisse le contrôle prévu pour cette étape est égale $\dfrac{\binom{49}{4}}{\binom{50}{5}} = \dfrac{49\,!}{4\,!\,45\,!} \times \dfrac{5\,!\,45\,!}{50\,!} = \dfrac{5}{50}$ soit 0,1.

4. *a*. On a une succession de 10 expériences aléatoires identiques et indépendantes, chacune d'elles a deux issues :

- réussite : le coureur est contrôlé ($p = 0,1$)
- échec : le coureur n'est pas contrôlé ($q = 1 - p = 0,9$)

donc la variable aléatoire X qui compte le nombre de sachets défectueux achetés, suit une loi binomiale de paramètres (10 ; 0,1).

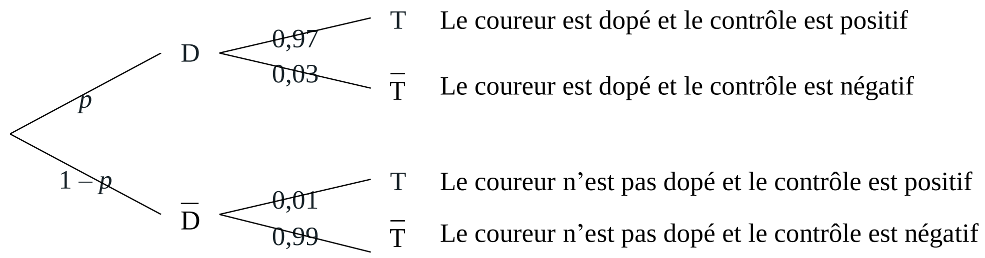
$p(X = k) = \binom{10}{k} \times 0,1^{\,k} \times 0,9^{\,10-k}$ avec $0 \leq k \leq 10$.

b. $P(X = 5) = \binom{10}{5} \times 0,1^{\,5} \times 0,9^{\,5} = 0,0015$

$P(X = 0) = 0,9^{\,10} = 0,3487$

$P(X \geq 1) = 1 - P(X = 0) = 0,6513$

Partie B



1. $P(T) = P(D \cap T) + P(\overline{D} \cap T) = p \times 0,97 + (1 - p) \times 0,01 = 0,01 + 0,96\,p$

$P(T) = 0,05$ donc $0,01 + 0,96\,p = 0,05$ donc $0,96\,p = 0,04$ donc $p = \dfrac{0,04}{0,96} = \dfrac{1}{24}$

2. $P(\overline{D} \cap T) = (1 - p) \times 0,01 = \dfrac{0,23}{24}$ donc $P(\overline{D} / T) = \dfrac{P(\overline{D} \cap T)}{P(T)} = \dfrac{\frac{0,23}{24}}{0,05} = \dfrac{0,23}{24} \times \dfrac{1}{0,05} = \dfrac{23}{120}$.

EXERCICE 2

Proposition 1 : VRAIE

Un vecteur normal au plan $\mathcal{P}$ est $\vec{n}\,(1\ ;\ -1\ ;\ -1)$, un vecteur directeur de $\mathcal{D}$ est $\vec{u}\,(-2\ ;\ 2\ ;\ 2)$, $\vec{u} = 2\,\vec{n}$ donc la droite $\mathcal{D}$ est orthogonale au plan $\mathcal{P}$.

Proposition 2 : FAUSSE

La distance de O à P est égale à $\dfrac{|0-0-0-2|}{\sqrt{1^2+(-1)^2+(-1)^2}} = \dfrac{2}{\sqrt{3}}$, cette distance est inférieure au rayon de la sphère donc la sphère $\mathcal{S}$ de centre O et de rayon 2 n'est pas tangente au plan $\mathcal{P}$, le plan $\mathcal{P}$ coupe la sphère suivant un cercle.

Proposition 3 :VRAIE

Les plans $\mathcal{P}$ et $\mathcal{P}'$ ne sont pas parallèles donc se coupent suivant une droite *d*.
Si $t = 0$, le point A de Δ a pour coordonnées $(1\ ;\ -1\ ;\ 0)$; or $1-(-1)-0-2=0$ donc $A \in \mathcal{P}$ et $1-1+3\times 0=0$ donc $A \in \mathcal{P}'$.
Si $t = 1$, le point B de Δ a pour coordonnées $(0\ ;\ -3\ ;\ 1)$; or $0-(-3)-1-2=0$ donc $B \in \mathcal{P}$ et $0-3+3\times 1=0$ donc $B \in \mathcal{P}'$.
L'intersection des plans $\mathcal{P}$ et $\mathcal{P}'$ est la droite (AB) donc la droite Δ.

L'intersection des plans $\mathcal{P}$ et $\mathcal{P}'$ est la droite Δ dont une représentation paramétrique est $\begin{cases} x = 1 - t' \\ y = -1 - 2t' \\ z = t' \end{cases}$ $t' \in \mathbb{R}$.

Proposition 4 : FAUSSE

Un vecteur directeur de $\mathcal{D}$ est $\vec{u}\,(-2\ ;\ 2\ ;\ 2)$, un vecteur directeur de Δ est $\vec{v}\,(-1\ ;\ -2\ ;\ 1)$, les coordonnées de ces vecteurs ne sont pas proportionnelles donc les droites $\mathcal{D}$ et Δ ne sont pas parallèles donc elles sont coplanaires si et seulement si elles sont sécantes.

Cherchons s'il existe *t* et t' tels que $\begin{cases} x = -3-2t = 1-t' \\ y = 2t = -1-2t' \\ z = 1+2t = t' \end{cases} \Leftrightarrow \begin{cases} -2t+t' = 4 \\ 2t+2t' = -1 \\ 2t-t' = 1 \end{cases}$

La première condition et la troisième ne sont pas compatibles : $-2t + t' = 4$ et $2t - t' = 1 \Leftrightarrow 0 = 5$! donc le système n'a pas de solution, les droites $\mathcal{D}$ et Δ ne sont pas coplanaires.

EXERCICE 3 (5 points) Commun à tous les candidats

On considère les suites (I_n) et (J_n) définies pour tout entier naturel n par :

$$\mathrm{I}_n = \int_0^1 \frac{\mathrm{e}^{-nx}}{1+x}\,\mathrm{d}x \quad \text{et } \mathrm{J}_n = \int_0^1 \frac{\mathrm{e}^{-nx}}{(1+x)^2}\,\mathrm{d}x$$

1. *a*. I_0 est l'aire comprise entre la courbe f_0, l'axe des abscisses et les droites d'équation $x = 0$ et $x = 1$
I_1 est l'aire comprise entre la courbe f_1, l'axe des abscisses et les droites d'équation $x = 0$ et $x = 1$
I_2 est l'aire comprise entre la courbe f_2, l'axe des abscisses et les droites d'équation $x = 0$ et $x = 1$
I_3 est l'aire comprise entre la courbe f_3, l'axe des abscisses et les droites d'équation $x = 0$ et $x = 1$
2tant donné la position relative des courbes, $\mathrm{I}_0 > \mathrm{I}_1 > \mathrm{I}_2 > \mathrm{I}_3$. La suite semble être décroissante.

b. $f_{n+1}(x) - f_n(x) = \dfrac{\mathrm{e}^{-(n+1)x}}{1+x} - \dfrac{\mathrm{e}^{-nx}}{1+x} = \dfrac{\mathrm{e}^{-nx}(\mathrm{e}^{-x}-1)}{1+x}$

$x \in [0\,;1]$ donc $-x \leq 0$ donc $\mathrm{e}^{-x} \leq 1$ donc $\mathrm{e}^{-x} - 1 \leq 0$, de plus la fonction exponentielle est strictement positive sur $\mathbb{R}$, et $1 + x \geq 0$ sur $[0\,;1]$ donc $\dfrac{\mathrm{e}^{-nx}(\mathrm{e}^{-x}-1)}{1+x} \leq 0$ donc sur $[0\,;1]$, $f_{n+1}(x) - f_n(x) \leq 0$.

Les fonctions f_n, f_{n+1} sont continues sur $[0\,;1]$ et $0 \leq 1$ donc $\displaystyle\int_0^1 \frac{\mathrm{e}^{-(n+1)x}}{1+x}\,\mathrm{d}x \leq \int_0^1 \frac{\mathrm{e}^{-nx}}{1+x}\,\mathrm{d}x$ soit $\mathrm{I}_{n+1} \leq \mathrm{I}_n$ donc la suite (I_n) est décroissante.

2. *a*. $0 \leq x \leq 1$ donc $1 \leq 1 + x$ donc $1 \leq 1 + x \leq (1 + x)^2$ donc $0 \leq \dfrac{1}{(1+x)^2} \leq \dfrac{1}{1+x} \leq 1$

la fonction exponentielle est strictement positive sur $\mathbb{R}$, donc en multipliant les termes de l'inégalité précédente par e^{-nx}, on a pour tout entier $n > 0$ et pour tout nombre réel x de l'intervalle $[0\,;1]$: $0 \leq \dfrac{\mathrm{e}^{-nx}}{(1+x)^2} \leq \dfrac{\mathrm{e}^{-nx}}{1+x} \leq \mathrm{e}^{-nx}$

b. Les fonctions f_n et $x \to \dfrac{\mathrm{e}^{-nx}}{(1+x)^2}$ et $x \to \mathrm{e}^{-nx}$ sont continues sur $[0\,;1]$ et $0 \leq 1$ donc

$0 \leq \displaystyle\int_0^1 \frac{\mathrm{e}^{-nx}}{(1+x)^2}\,\mathrm{d}x \leq \int_0^1 \frac{\mathrm{e}^{-nx}}{1+x}\,\mathrm{d}x \leq \int_0^1 \mathrm{e}^{-nx}\,\mathrm{d}x$ soit $0 \leq \mathrm{J}_n \leq \mathrm{I}_n \leq \left[-\dfrac{1}{n}\mathrm{e}^{-nx}\right]_0^1$ soit $0 \leq \mathrm{J}_n \leq \mathrm{I}_n \leq \dfrac{1}{n}(1 - \mathrm{e}^{-1})$

$\displaystyle\lim_{n\to+\infty} \frac{1}{n}(1 - \mathrm{e}^{-1}) = 0$ donc d'après le théorème des gendarmes : $\displaystyle\lim_{n\to+\infty} \mathrm{J}_n = \lim_{n\to+\infty} \mathrm{I}_n = 0$

3. *a*. Soit $\begin{cases} u'(x) = \mathrm{e}^{-nx} & u(x) = -\dfrac{1}{n}\mathrm{e}^{-nx} \\ v(x) = \dfrac{1}{1+x} & v'(x) = -\dfrac{1}{(1+x)^2} \end{cases}$ donc $I_n = \left[-\dfrac{1}{n}\mathrm{e}^{-nx} \times \dfrac{1}{1+x}\right]_0^1 - \displaystyle\int_0^1 \frac{1}{n}\mathrm{e}^{-nx} \times \frac{1}{(1+x)^2}\,\mathrm{d}x$

$I_n = \left[-\dfrac{1}{n}\mathrm{e}^{-n} \times \dfrac{1}{2} + \dfrac{1}{n}\right] - \dfrac{1}{n}\displaystyle\int_0^1 \frac{\mathrm{e}^{-nx}}{(1+x)^2}\,\mathrm{d}x$

$I_n = \dfrac{1}{n}\left(-\dfrac{\mathrm{e}^{-n}}{2} + 1\right) - \dfrac{1}{n}J_n$ donc pour tout entier $n \geq 1$: $I_n = \dfrac{1}{n}\left(1 - \dfrac{\mathrm{e}^{-n}}{2} - J_n\right)$

b. $n\,I_n = 1 - \dfrac{\mathrm{e}^{-n}}{2} - J_n$ or $\displaystyle\lim_{n\to+\infty} \mathrm{J}_n = 0$ et $\displaystyle\lim_{n\to+\infty} \frac{\mathrm{e}^{-n}}{2} = 0$ donc $\displaystyle\lim_{n\to+\infty} n\,I_n = 1$

EXERCICE 4 Candidats ayant suivi l'enseignement de spécialité

Partie A Restitution organisée de connaissance

si $a \equiv b \pmod n$, n divise $a - b$ donc il existe un entier relatif q tel que $a - b = n\,q$ donc $a = b + n\,q$
si $c \equiv d \pmod n$, n divise $c - d$ donc il existe un entier relatif q' tel que $c - d = n\,q'$ donc $c = d + n\,q'$
$a\,c = (b + n\,p)\,(d + n\,q') = b\,d + n\,(b\,q' + d\,p + n\,p\,p')$
$a\,c - b\,d = n\,(b\,q' + d\,p + n\,p\,p')$
$(b\,q' + d\,p + n\,p\,p')$ est un entier relatif donc n divise $a\,c - b\,d$ donc $a\,c \equiv b\,d \pmod n$.

Partie B Inverse de 23 modulo 26

1. $23 \times (-9) = 207$ et $26 \times (-8) = 208$ donc $23 \times (-9) - 26 \times (-8) = 1$
Le couple $(-9\,;\,-8)$ est solution de l'équation (E).

2. $\begin{cases} 23\,x - 26\,y = 1 \\ 23 \times (-9) - 26 \times (-8) = 1 \end{cases}$ donc par différence membre à membre : $23\,(x + 9) - 26\,(y + 8) = 0$

$23\,(x + 9) = 26\,(y + 8)$, donc 23 divise $26\,(y + 8)$ or 23 et 26 sont premiers entre eux donc 23 divise $y + 8$
Il existe un entier relatif k tel que $y + 8 = 23\,k$ donc $y = 23\,k - 8$
En remplaçant dans $23\,(x + 9) = 26\,(y + 8)$, alors $x + 9 = 26\,k$ donc $x = 26\,k - 9$
Vérification si $x = 26\,k - 9$ et $y = 23\,k - 8$ alors $23\,x - 26\,y = 23\,(26\,k - 9) - 26\,(23\,k - 8) = 23 \times (-9) - 26 \times (-8) = 1$
Les solutions l'équation (E) sont les couples $(26\,k - 9\,;\,23\,k - 8)$ avec $k \in \mathbb{Z}$.

3. si $23\,a \equiv 1 \pmod{26}$ il existe un entier relatif b tel que $23\,a - 26\,b = 1$ donc $a = 26\,k - 9$
$0 \le a \le 25$ donc $k = 1$ et $a = 26 - 9 = 17$

Partie C Chiffrement de Hill

1. $\underset{\text{mot en clair}}{ST} \xrightarrow{\text{étape 1}} (18, 19)$.

$\begin{cases} y_1 \equiv 11 \times 18 + 3 \times 19 \mod 26 \\ y_2 \equiv 7 \times 18 + 4 \times 19 \mod 26 \end{cases} \Leftrightarrow \begin{cases} y_1 \equiv 255 \mod 26 \\ y_2 \equiv 202 \mod 26 \end{cases}$ or $255 = 26 \times 9 + 21$ et $202 = 26 \times 7 + 20$

donc $y_1 = 21$ et $y_2 = 20$

$$\underset{\text{mot en clair}}{ST} \xrightarrow{\text{étape 1}} (18, 19) \xrightarrow{\text{étape 2}} (21, 20) \xrightarrow{\text{étape 3}} \underset{\text{mot codé}}{VU}$$

Le mot ST est codé par VU

2. *a*. $(S_1)\ \begin{cases} y_1 \equiv 11\,x_1 + 3\,x_2 \mod 26 \\ y_2 \equiv 7\,x_1 + 4\,x_2 \mod 26 \end{cases}$ donc $\begin{cases} 4\,y_1 \equiv 44\,x_1 + 12\,x_2 \mod 26 \\ 23\,y_2 \equiv 141\,x_1 + 112\,x_2 \mod 26 \end{cases}$ et $\begin{cases} 19\,y_1 \equiv 209\,x_1 + 57\,x_2 \mod 26 \\ 11\,y_2 \equiv 77\,x_1 + 44\,x_2 \mod 26 \end{cases}$.

or $209 = 26 \times + 18$; $57 = 26 \times 2 + 5$; $77 = 26 \times 2 + 25$ et $44 = 26 + 18$

donc $\begin{cases} 4\,y_1 \equiv 18\,x_1 + 12\,x_2 \mod 26 \\ 23\,y_2 \equiv 5\,x_1 + 14\,x_2 \mod 26 \end{cases}$ et $\begin{cases} 19\,y_1 \equiv x_1 + 5\,x_2 \mod 26 \\ 11\,y_2 \equiv 25\,x_1 + 18\,x_2 \mod 26 \end{cases}$.

En additionnant terme à terme $\begin{cases} 4\,y_1 \equiv 18\,x_1 + 12\,x_2 \mod 26 \\ 23\,y_2 \equiv 5\,x_1 + 14\,x_2 \mod 26 \end{cases}$ donc $4\,y_1 + 23\,y_2 = 23\,x_1 + 26\,x_2 \pmod{26}$

et $\begin{cases} 19\,y_1 \equiv x_1 + 5\,x_2 \mod 26 \\ 11\,y_2 \equiv 25\,x_1 + 18\,x_2 \mod 26 \end{cases}$ donc $19\,y_1 + 11\,y_2 = 26\,x_1 + 23\,x_2 \pmod{26}$

donc tout couple (x_1, x_2) vérifiant les équations du système (S1), vérifie les équations du système $\begin{cases} 23\,x_1 \equiv 4\,y_1 + 23\,y_2 \mod 26 \\ 23\,x_2 \equiv 19\,y_1 + 11\,y_2 \mod 26 \end{cases}$

.

b. $\begin{cases} 23\,x_1 \equiv 4\,y_1 + 23\,y_2 \mod 26 \\ 23\,x_2 \equiv 19\,y_1 + 11\,y_2 \mod 26 \end{cases}$ donc en multipliant par 17 puisque $23 \times 17 \equiv 1 \pmod{26}$

$\begin{cases} 23\,x_1 \equiv 4\,y_1 + 23\,y_2 \mod 26 \\ 23\,x_2 \equiv 19\,y_1 + 11\,y_2 \mod 26 \end{cases}$ donc $\begin{cases} 23 \times 17\,x_1 \equiv 4 \times 17\,y_1 + 23 \times 17\,y_2 \mod 26 \\ 23 \times 17\,x_2 \equiv 19 \times 17\,y_1 + 11 \times 17\,y_2 \mod 26 \end{cases}$

n	4×17	23×17	19×17	11×17
reste de la division de n par 26	16	1	11	5
quotient de la division de n par 26	2	15	12	7

donc tout couple (x_1, x_2) vérifiant les équations du système (S_2), vérifie les équations du système (S_3) $\begin{cases} x_1 \equiv 16\,y_1 + y_2 \mod 26 \\ x_2 \equiv 11\,y_1 + 5\,y_2 \mod 26 \end{cases}$

c. $\begin{cases} 11\,x_1 \equiv 16\times 11\,y_1 + 11\,y_2 \mod 26 \\ 3\,x_2 \equiv 11\times 3\,y_1 + 5\times 3\,y_2 \mod 26 \end{cases}$ et $\begin{cases} 7\,x_1 \equiv 16\times 7\,y_1 + \times 7\,y_2 \mod 26 \\ 4\,x_2 \equiv 11\times 4\,y_1 + 5\times 4\,y_2 \mod 26 \end{cases}$.

n	$16\times 11 = 176$	$11\times 3 = 33$	$16\times 7 = 112$	$11\times 4 = 44$	$5\times 4 = 20$
reste de la division de n par 26	20	7	8	18	9
quotient de la division de n par 26	6	1	4	1	1

$\begin{cases} 11\,x_1 \equiv 20\,y_1 + 11\,y_2 \mod 26 \\ 3\,x_2 \equiv 7\,y_1 + 15\,y_2 \mod 26 \end{cases}$ et $\begin{cases} 7\,x_1 \equiv 8\,y_1 + \times 7\,y_2 \mod 26 \\ 4\,x_2 \equiv 18\,y_1 + 20\,y_2 \mod 26 \end{cases}$.

Par addition terme à terme :

$\begin{cases} 11\,x_1 \equiv 20\,y_1 + 11\,y_2 \mod 26 \\ 3\,x_2 \equiv 7\,y_1 + 15\,y_2 \mod 26 \end{cases}$ donc $11\,x_1 + 3\,x_2 \equiv 27\,y_1 + 26\,y_2$ (mod 26) soit $11\,x_1 + 3\,x_2 \equiv y_1$ (mod 26)

$\begin{cases} 7\,x_1 \equiv 8\,y_1 + \times 7\,y_2 \mod 26 \\ 4\,x_2 \equiv 18\,y_1 + 20\,y_2 \mod 26 \end{cases}$ donc $7\,x_1 + 4\,x_2 \equiv 26\,y_1 + 27\,y_2$ (mod 26) soit $7\,x_1 + 4\,x_2 \equiv y_2$ (mod 26)

Tout couple (x_1, x_2) vérifiant les équations du système (S_3) $\begin{cases} x_1 \equiv 16\,y_1 + y_2 \mod 26 \\ x_2 \equiv 11\,y_1 + 5\,y_2 \mod 26 \end{cases}$, vérifie les équations du système (S_1).

d. $\underset{\text{mot en clair}}{\text{Y J}} \xrightarrow{\text{étape 1}} (24, 9)$

$(y_1\,;\,y_2)$ donc $\begin{cases} x_1 \equiv 16\times 24 + 9 \mod 26 \\ x_2 \equiv 11\times 24 + 5\times 9 \mod 26 \end{cases}$ or $16 \times 4 + 9 = 26 \times 15 + 3$ et $11 \times 24 + 5 \times 9 = 11 \times 26 + 23$ donc $\begin{cases} x_1 \equiv 3 \mod 26 \\ x_2 \equiv 23 \mod 26 \end{cases}$

$$\underset{\text{mot codé}}{\text{Y J}} \xrightarrow{\text{étape 1}} (24, 9) \xrightarrow{\text{étape 2}} (3, 23) \xrightarrow{\text{étape 3}} \underset{\text{mot en clair}}{\text{D X}}$$

Le mot en clair est DX

EXERCICE 4 (5 points) Candidats n'ayant pas suivi l'enseignement de spécialité

Partie A Restitution organisée de connaissances

$|z_1 \; z_2|^2 = z_1 z_2 \overline{z_1 z_2} = z_1 z_2 \overline{z_1} \times \overline{z_2} = z_1 \overline{z_1} \times z_2 \overline{z_2} = |z_1|^2 |z_2|^2$

Le module d'un complexe est un réel positif donc $|z_1 \; z_2| = |z_1| \, |z_2|$.

Partie B Étude d'une transformation particulière

1. Soit C le point d'affixe $z_C = -2 + i$.

a. L'affixe $z_{C'} = \dfrac{1 - z_C}{\overline{z_C} - 1} = \dfrac{1-(-2+i)}{-2-i-1} = \dfrac{3-i}{-3-i} = \dfrac{-3+i}{3+i} = \dfrac{(-3+i)(3-i)}{(3+i)(3+i)} = \dfrac{-9+6i+1}{10}$

L'affixe du point C' image de C par la transformation f est $-0{,}8 + 0{,}6\,i$

b. $|-0{,}8 + 0{,}6\,i| = \sqrt{0{,}8^2 + 0{,}6^2} = 1$ donc OC' = 1 donc le point C' appartient au cercle $\mathscr{C}$ de centre O et de rayon 1.

c. $\overrightarrow{AC}$ a pour affixe $z_C - z_A = -3 + i$; $\overrightarrow{AC'}$ a pour affixe $z_{C'} - z_A = -1{,}8 + 0{,}6\,i = 0{,}6 \times (-3 + i)$ donc $\overrightarrow{AC'} = 0{,}6\,\overrightarrow{AC}$.

Les points A, C et C' sont alignés.

2. $f(M) = A \Leftrightarrow \dfrac{1-z}{\overline{z}-1} = 1$ et $z \neq 1 \Leftrightarrow 1 - z = \overline{z} - 1$ et $z \neq 1 \Leftrightarrow z + \overline{z} = 2$ et $z \neq 1$

Il existe deux réels x et y tels que $z = x + i\,y$ alors $f(M) = A \Leftrightarrow z + \overline{z} = 2$ et $z \neq 1 \Leftrightarrow 2x = 2$ et $x + i\,y \neq 1 \Leftrightarrow x = 1$ et M ≠ A

L'ensemble Δ des points du plan qui ont le point A pour image par la transformation f est la droite d'équation $x = 1$ privée du point A.

3. $|z'| = \left|\dfrac{1-z}{\overline{z}-1}\right| = \dfrac{|1-z|}{|\overline{z}-1|}$ or $|\overline{z}-1| = |\overline{z-1}| = |z-1| = |1-z|$ donc $|z'| = 1$ soit OM' = 1

Pour tout point M distinct de A ; le point M' appartient au cercle $\mathscr{C}$.

4. $z' - 1 = \dfrac{1-z}{\overline{z}-1} - 1 = \dfrac{1-z-(\overline{z}-1)}{\overline{z}-1} = \dfrac{2-z-\overline{z}}{\overline{z}-1}$

Il existe deux réels x et y tels que $z = x + i\,y$ donc $\dfrac{z'-1}{z-1} = \dfrac{2-z-\overline{z}}{(\overline{z}-1)(z-1)} = \dfrac{2-2x}{|z-1|^2}$,

Pour tout nombre complexe $z \neq 1$; $\dfrac{z'-1}{z-1}$ est réel donc il existe un réel k te l que $z' - 1 = k(z-1)$ soit $\overrightarrow{AM'} = k\,\overrightarrow{AM}$.

Les points A, M et M' sont alignés.

5. D n'appartient pas à la droite d'équation $x = 1$ donc $f(D) \neq A$.

Les points A, D, D' sont alignés et D' appartient au cercle $\mathscr{C}$ donc D' est le deuxième point d'intersection autre que A de la droite (AD) et du cercle $\mathscr{C}$.