Nom : .... **Prénom** : ....

RENDRE TOUT LE SUJET AVEC VOTRE COPIE

BACCALAURÉAT GÉNÉRAL « BLANC »

MATHÉMATIQUES

Série S

ÉPREUVE DU MERCREDI 16 JANVIER 2019

Durée de l'épreuve : 4 heures Coefficient : 9

ENSEIGNEMENT DE SPÉCIALITÉ

L'usage de tout modèle de calculatrice, avec ou sans mode examen, est autorisé.

Le sujet est composé de 4 exercices indépendants. Le candidat doit traiter tous les exercices.

Dans chaque exercice, le candidat peut admettre un résultat précédemment donné dans le texte pour aborder les questions suivantes, à condition de l'indiquer clairement sur la copie.

Le candidat est invité à faire figurer sur la copie toute trace de recherche, même incomplète ou non fructueuse, qu'il aura développée.

Il est rappelé que la qualité de la rédaction, la clarté et la précision des raisonnements seront prises en compte dans l'appréciation des copies.

Avant de composer, le candidat s'assurera que le sujet comporte bien 4 pages numérotées.

EXERCICE 1 [7 points] *Commun à tous les candidats*

Les parties A et B sont indépendantes.

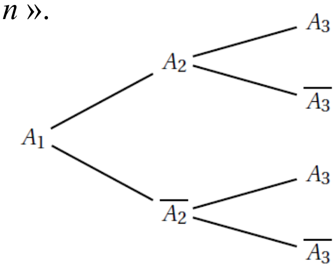
Un détaillant en fruits et légumes étudie l'évolution de ses ventes de melons afin de pouvoir anticiper ses commandes.

Partie A

Le détaillant réalise une étude sur ses clients. Il constate que :

- parmi les clients qui achètent un melon une semaine donnée, 90 % d'entre eux achètent un melon la semaine suivante ;
- parmi les clients qui n'achètent pas de melon une semaine donnée, 60 % d'entre eux n'achètent pas de melon la semaine suivante.

On choisit au hasard un client ayant acheté un melon au cours de la semaine 1 et, pour $n \geqslant 1$, on note A_n l'évènement : « le client achète un melon au cours de la semaine *n* ».
On a ainsi $\mathrm{p}(\mathrm{A}_1)=1$.



1. a) Reproduire et compléter l'arbre de probabilités ci-contre, relatif aux trois premières semaines.

b) Démontrer que $\mathrm{p}(\mathrm{A}_3)=0{,}85$.

c) Sachant que le client achète un melon au cours de la semaine 3, quelle est la probabilité qu'il en ait acheté un au cours de la semaine 2 ? Arrondir au centième.

Dans la suite, on pose pour tout entier $n \geqslant 1$: $p_n=\mathrm{p}(\mathrm{A}_n)$. On a ainsi $p_1=1$.

2. Démontrer que, pour tout entier $n \geqslant 1$: $p_{n+1}=0{,}5\,p_n+0{,}4$.

3. a) Démontrer par récurrence que, pour tout entier $n \geqslant 1$: $p_n>0{,}8$.

b) Démontrer que la suite (p_n) est décroissante.

c) La suite (p_n) est-elle convergente ?

4. On pose pour tout entier $n \geqslant 1$: $v_n=p_n-0{,}8$.

a) Démontrer que (v_n) est une suite géométrique dont on donnera le premier terme v_1 et la raison.

b) Exprimer v_n en fonction de *n*.
En déduire que, pour tout $n \geqslant 1$, $p_n=0{,}8+0{,}2\times 0{,}5^{n-1}$.

c) Déterminer la limite de la suite (p_n).

Partie B

Le détaillant veut faire un sondage auprès de ses clients.
Il interroge au hasard *n* clients, en admettant que ce choix se ramène à *n* tirages successifs indépendants et avec remise. On suppose que la probabilité qu'un client choisi au hasard ait acheté un de ses melons est égale à 0,8. On note X la variable aléatoire égale au nombre de clients ayant acheté un de ses melons parmi les *n* interrogés.

1. Déterminer la loi de probabilité suivie par la variable aléatoire X.

2. Dans cette question, on suppose que $n=40$.
a) Déterminer la probabilité qu'exactement 15 des 40 clients interrogés aient acheté un de ses melons.

b) Déterminer la probabilité qu'au moins la moitié des clients interrogés aient acheté un de ses melons.

EXERCICE 2 [5 points] *Commun à tous les candidats*

Soient f et g les fonctions définies sur $\mathbb{R}$ par $f(x) = \mathrm{e}^x$ et $g(x) = 2\mathrm{e}^{\frac{x}{2}} - 1$.

On note $\mathscr{C}_f$ et $\mathscr{C}_g$ les courbes représentatives des fonctions f et g dans un repère orthogonal.

1. Démontrer que les courbes $\mathscr{C}_f$ et $\mathscr{C}_g$ ont un point commun d'abscisse 0 et qu'en ce point, elles ont la même tangente Δ dont on déterminera une équation.
2. Étude de la position relative de la courbe $\mathscr{C}_g$ et de la droite Δ

   Soit h la fonction définie sur $\mathbb{R}$ par $h(x) = 2\mathrm{e}^{\frac{x}{2}} - x - 2$.

   a. Déterminer la limite de la fonction h en $-\infty$.

   b. Justifier que, pour tout réel $x \neq 0$, $h(x) = x\left(\dfrac{\mathrm{e}^{\frac{x}{2}}}{\frac{x}{2}} - 1 - \dfrac{2}{x}\right)$.

   En déduire la limite de la fonction h en $+\infty$.

   c. On note h' la fonction dérivée de la fonction h sur $\mathbb{R}$.

   Pour tout réel x, calculer $h'(x)$ et étudier le signe de $h'(x)$ suivant les valeurs de x.

   d. Dresser le tableau de variations de la fonction h sur $\mathbb{R}$.

   e. En déduire que, pour tout réel x, $2\mathrm{e}^{\frac{x}{2}} - 1 \geqslant x + 1$.

   f. Que peut-on en déduire quant à la position relative de la courbe $\mathscr{C}_g$ et de la droite Δ ?
3. Étude de la position relative des courbes $\mathscr{C}_f$ et $\mathscr{C}_g$

   a. Pour tout réel x, développer l'expression $\left(\mathrm{e}^{\frac{x}{2}} - 1\right)^2$.

   b. Déterminer la position relative des courbes $\mathscr{C}_f$ et $\mathscr{C}_g$.

EXERCICE 3 [3 points] *Commun à tous les candidats*

On munit le plan complexe d'un repère orthonormé direct.

On considère l'équation : (E) $z^4 + 2z^3 - z - 2 = 0$ ayant pour inconnue le nombre complexe z.

1. Donner une solution entière de (E).
2. Démontrer que, pour tout nombre complexe z,

$$z^4 + 2z^3 - z - 2 = \left(z^2 + z - 2\right)\left(z^2 + z + 1\right).$$

3. Résoudre l'équation (E) dans l'ensemble des nombres complexes.
4. Les solutions de l'équation (E) sont les affixes de quatre points A, B, C, D du plan complexe tels que ABCD est un quadrilatère non croisé.

   Le quadrilatère ABCD est-il un losange ? Justifier.

EXERCICE 4 [5 points] *Candidats ayant choisi l'enseignement de spécialité*

Le but de cet exercice est d'envisager une méthode de cryptage à clé publique d'une information numérique, appelée système RSA, en l'honneur des mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman, qui ont inventé cette méthode de cryptage en 1977 et l'ont publiée en 1978.

Les questions 1 et 2 sont des questions préparatoires, la question 3 aborde le cryptage, la question 4 le décryptage.

1. Cette question envisage de calculer le reste dans la division euclidienne par 55 de certaines puissances de 8.
a) Vérifier que $8^7 \equiv 2$ [55]. En déduire le reste dans la division euclidienne par 55 du nombre 8^{21}.

b) Vérifier que $8^2 \equiv 9$ [55], puis déduire de la question a) le reste dans la division euclidienne par 55 de 8^{23}.

2. Dans cette question, on considère l'équation (E) $23x-40y=1$, dont les solutions sont des couples $(x\,;y)$ d'entiers relatifs.

a) Justifier le fait que l'équation (E) admet au moins un couple solution.

b) Donner un couple, solution particulière de l'équation (E). *Aucune justification n'est demandée.*

c) Déterminer tous les couples d'entiers relatifs solutions de l'équation (E).

d) En déduire qu'il existe un unique entier d vérifiant les conditions $0 \leqslant d < 40$ et $23\,d \equiv 1$ [40].

3. Cryptage dans le système RSA
Une personne A choisit deux nombres premiers p et q, puis calcule les produits $\mathrm{N}=pq$ et $n=(p-1)(q-1)$. Elle choisit également un entier naturel c premier avec n.
La personne A publie le couple $(\mathrm{N}\,;c)$, qui est une clé publique permettant à quiconque de lui envoyer un nombre crypté. Les messages sont numérisés et transformés en une suite d'entiers compris entre 0 et $\mathrm{N}-1$.
Pour crypter un entier a de cette suite, on procède ainsi : on calcule le reste b dans la division euclidienne par N du nombre a^c, et le nombre crypté est l'entier b.
Dans la pratique, cette méthode est sûre si la personne A choisit des nombres premiers p et q très grands, s'écrivant avec plusieurs dizaines de chiffres.
On va l'envisager ici avec des nombres plus simples : $p = 5$ et $q = 11$.
La personne A choisit également $c = 23$.

a) Calculer les nombres N et n, puis justifier que la valeur de c vérifie la condition voulue.

b) Un émetteur souhaite envoyer à la personne A le nombre $a = 8$.
Déterminer la valeur du nombre crypté b.

4. Décryptage dans le système RSA
La personne A calcule dans un premier temps l'unique entier naturel d vérifiant les conditions $0 \leqslant d < n$ et $c\,d \equiv 1$ [n]. Elle garde secret ce nombre d qui lui permet, et à elle seule, de décrypter les nombres qui lui ont été envoyés cryptés avec sa clé publique.
Pour décrypter un nombre crypté b, la personne A calcule le reste a dans la division euclidienne par N du nombre b^d, et le nombre en clair – c'est-à-dire le nombre avant cryptage – est le nombre a.
On admet l'existence et l'unicité de l'entier d, et le fait que le décryptage fonctionne.
Les nombres choisis par A sont encore $p = 5$, $q = 11$ et $c = 23$.

a) Quelle est la valeur de d ?

b) En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est $b = 17$.