Math93.com

Baccalauréat 2018 - S
Correction Centres Étrangers

Série S Obli. et Spé.

11 Juin 2018

Like Math93 on Facebook / Follow Math93 on Twitter

Remarque : *dans la correction détaillée ici proposée, les questions des exercices sont presque intégralement réécrites pour faciliter la lecture et la compréhension du lecteur. Il est cependant exclu de faire cela lors de l'examen, le temps est précieux! Il est par contre nécessaire de numéroter avec soin vos questions et de souligner ou encadrer vos résultats. Pour plus de précisions et d'astuces, consultez la page dédiée de math93.com : présenter une copie, trucs et astuces.*

Exercice 1. Fonctions et Suites — 4 points

Commun à tous/toutes les candidat/e/s

Dans une usine, on se propose de tester un prototype de hotte aspirante pour un local industriel. Avant de lancer la fabrication en série, on réalise l'expérience suivante : dans un local clos équipé du prototype de hotte aspirante, on diffuse du dioxyde de carbone (CO2) à débit constant. Dans ce qui suit, t est le temps exprimé en minute. À l'instant $t = 0$, la hotte est mise en marche et on la laisse fonctionner pendant 20 minutes. Les mesures réalisées permettent de modéliser le taux (en pourcentage) de CO_2 contenu dans le local au bout de t minutes de fonctionnement de la hotte par l'expression $f(t)$, où f est la fonction définie pour tout réel t de l'intervalle $[0; 20]$ par : $f(t) = (0,8t + 0,2)\ e^{-0,5t} + 0,03$.

t	0		1.75	α	20
Signe de $f'(t)$		+	0	−	
Variations de f	0.23	↗	$f(1.75) \approx 0.697$	↘ 0.035	↘ $f(20) \approx 0.031$

1. *Dans cette question on arrondira au millième.*

1. a. Calculer $f(20)$.

$$f(20) = 16,2\,e^{-10} + 0,03 \approx \underline{0,031}$$

1. b. Déterminer le taux maximal de CO_2 présent dans le local pendant l'expérience.

La fonction f admet un maximal local sur $[0; 20]$ pour $x = 1,75$ donc le taux maximal de CO_2 présent dans le local pendant l'expérience est environ de 69,7% car : $f(1,75) \approx \underline{0,697}$.

2. On souhaite que le taux de CO2 dans le local retrouve une valeur V inférieure ou égale à 3,5%.

2. a. Justifier qu'il existe un unique instant T satisfaisant cette condition.

- Sur [0 ; 1,75] la fonction est strictement croissante et son minimum est $f(0) = 0,23 > 0,035$ donc l'équation $f(t) = 0,035$ n'y admet pas de solution.

- Application du corollaire sur $[1,75\,;\,20]$:

Théorème 1 (Corollaire du théorème des valeurs intermédiaires)

Si f est une fonction définie, **continue** et strictement **monotone** sur un intervalle $[a\,;\,b]$, alors, pour tout réel k compris entre $f(a)$ et $f(b)$, l'équation $f(x)=k$ admet une unique solution dans $[a\,;\,b]$.

Remarque *: Le première démonstration rigoureuse de ce théorème est due au mathématicien autrichien Bernard Bolzano (1781-1848).*

  - La fonction f est *continue* et *strictement décroissante* sur l'intervalle $[1,75\,;\,20]$;
  - Le réel $k=0,035$ est compris entre $f(1,75)\approx 0,697$ et $f(20)\approx 0,031$
  - Donc, d'après le *corollaire du théorème des valeurs intermédiaires,* l'équation $f(t)=0,035$ admet une solution unique α sur l'intervalle $[1,75\,;\,20]$.

- Valeur approchée (non demandée) .
Pour avoir un encadrement de α, on peut utiliser la fonction TABLE de la calculatrice.
  - Avec un pas de $\Delta=0.01$ on obtient :

$$\left\{\begin{array}{lcl} f(15,68) & \approx & 0,03502>0,035 \\ f(15,69) & \approx & 0,034995<0,035 \end{array}\right., \text{ donc } 15,68<\alpha<15,69.$$

2. b. *On considère l'algorithme suivant :*

```
t ← 1,75
p ← 0,1
V ← 0,7
Tant que V > 0,035
    t ← t + p
    V ← (0,8t + 0,2)e^(−0,5t) + 0,03
Fin Tant que
```

Quelle est la valeur de la variable t à la fin de l'algorithme ? Que représente cette valeur dans le contexte de l'exercice ?

À l'aide de la calculatrice on trouve que la variable t à la fin de l'algorithme vaut 15,75. En effet on a :

$$\left\{\begin{array}{l} f(15,65)>0,035 \\ f(15,75)<0,035 \end{array}\right.$$

Cela signifie qu'il faut attendre 15 minutes et 45 secondes pour obtenir un taux de CO2 inférieur ou égal à 3,5%.

Remarque : $15,75\,\text{min}=15\,\text{min}+0,75\times 60\,\text{s}=15\,\text{min}\,45\,\text{s}$.

©ISSN 2272-5318

3. *On désigne par V_m le taux moyen (en pourcentage) de CO2 présent dans le local pendant les 11 premières minutes de fonctionnement de la hotte aspirante.*

3. a. Soit F la fonction définie sur l'intervalle $[0;11]$ par : $F(t) = (-1,6t - 3,6)\ \mathrm{e}^{-0,5t} + 0,03t$. Montrer que la fonction F est une primitive de la fonction f sur l'intervalle $[0;11]$.

$$F : \left\{ \begin{array}{rcl}]0;20[& \longrightarrow & \mathbb{R} \\ t & \longmapsto & F(t) = (-1,6t - 3,6) \times \mathrm{e}^{-0,5t} + 0,03t \end{array} \right.$$

La fonction F est dérivable sur $]0;20[$.
La fonction F est de la forme $uv + 0,03t$ donc de dérivée $u'v + uv' + 0,03$ avec :

$$\forall\, t \in]0;20[\ ;\ F(t) = u(t) \times v(t) + 0,03t\ :\ \left\{ \begin{array}{lll} u(t) = (-1,6t - 3,6) & ; & u'(t) = -1,6 \\ v(t) = \mathrm{e}^{-0,5t} & ; & v'(t) = \left(-0,5\,\mathrm{e}^{-0,5t}\right) \end{array} \right.$$

On a donc :

$$\begin{aligned} \forall\, t \in]0;20[,\ \ F'(t) &= u'(t) \times v(t) + u(t) \times v'(t) + 0,03 \\ F'(t) &= -1,6 \times \mathrm{e}^{-0,5t} + (-1,6t - 3,6) \times \left(-0,5\,\mathrm{e}^{-0,5t}\right) \end{aligned}$$

Soit

$$\boxed{\forall\, t \in]0;20[\ ;\ F'(t) = (0,8t + 0,2)\ \mathrm{e}^{-0,5t} + 0,03}$$

Donc F est une primitive de f.

3. b. En déduire le taux moyen V_m , valeur moyenne de la fonction f sur l'intervalle $[0;11]$. Arrondir le résultat au millième, soit à 0,1%.

$$\begin{aligned} V_m &= \frac{1}{11-0}\int_0^{11} f(t)\,\mathrm{d}t \\ &= \frac{1}{11}\left[F(11) - F(0)\right] \\ &= \frac{-21,2\,\mathrm{e}^{-5,5} + 0,33 + 3,6}{11} \\ &= \frac{-21,2\,\mathrm{e}^{-5,5} + 3,93}{11} \\ V_m &\approx \underline{0,349} \end{aligned}$$

©ISSN 2272-5318

Exercice 2. Vrai/faux — 4 points

Commun à tous/toutes les candidat/e/s

Affirmation 1 (Vraie)

Un type d'oscilloscope a une durée de vie, exprimée en année, qui peut être modélisée par une variable aléatoire D qui suit une loi exponentielle de paramètre λ. On sait que la durée de vie moyenne de ce type d'oscilloscope est de 8 ans.
Affirmation 1 : pour un oscilloscope de ce type choisi au hasard et ayant déjà fonctionné 3 ans, la probabilité que la durée de vie soit supérieure ou égale à 10 ans, arrondie au centième, est égale à 0,42.

- Déterminons λ.

Propriété 1

Soit λ un réel strictement positif.
Si T suit la loi exponentielle de paramètre λ alors pour tout réel a et b tels que $0 \leq a \leq b$:

$$P(a \leq T \leq b) = \mathrm{e}^{-\lambda a} - \mathrm{e}^{-\lambda b}$$

et donc

$$P(T \leq b) = 1 - \mathrm{e}^{-\lambda b} \quad \text{et} \quad P(T \geq a) = \mathrm{e}^{-\lambda a}$$

En outre la variable T est d'espérance : $E(T) = \dfrac{1}{\lambda}$.

Puisque la durée de vie moyenne est de 8 ans on a :

$$E(D) = 8 = \frac{1}{\lambda} \Longrightarrow \lambda = \frac{1}{8} = 0,125 \text{ année}^{-1}$$

- Calculons $P_{D>3}(D \geq 10)$.
On cherche pour un oscilloscope de ce type choisi au hasard et ayant déjà fonctionné 3 ans, la probabilité que la durée de vie soit supérieure ou égale à 10 ans, soit $P_{D>3}(D \geq 10)$.

Propriété 2 (Durée de vie sans vieillissement)

Si X est une variable aléatoire suivant une loi exponentielle, alors pour tous réels positifs t et h :

$$P_{X \geqslant t}(X \geqslant t + h) = P(X \geqslant h)$$

Cette propriété traduit le fait que la loi exponentielle est « sans mémoire ».

D'après la propriété dite de « *Durée de vie sans vieillissement* » :

$$\begin{aligned} P_{D>3}(D \geq 10) &= P_{D>3}(D \geq 3 + 7) \\ &= P(D \geq 7) \\ &= \mathrm{e}^{-\lambda \times 7} \end{aligned}$$

$$P_{D>3}(D \geq 10) = \mathrm{e}^{-\frac{7}{8}} \approx \underline{0,42}$$

Affirmation 2 (Vraie)

En 2016, en France, les forces de l'ordre ont réalisé 9,8 millions de dépistages d'alcoolémie auprès des automobilistes, et 3,1 % de ces dépistages étaient positifs. Dans une région donnée, le 15 juin 2016, une brigade de gendarmerie a effectué un dépistage sur 200 automobilistes.
Affirmation 2 : en arrondissant au centième, la probabilité que, sur les 200 dépistages, il y ait eu strictement plus de 5 dépistages positifs, est égale à 0,59.

- Remarque importante : On va considérer que l'effectif est suffisamment grand pour pouvoir assimiler le tirage à un tirage avec remise et que chaque tirage est indépendant.
- Modélisation
  Soit X la variable aléatoire qui compte le nombre de dépistages positifs.
  Il y a répétition de $n = 200$ événements indépendants et identiques (on tire un dépistage).
  Chaque tirage a deux issues possibles (épreuve de Bernoulli) :
  - succès de probabilité $p = 0,031$ quand un dépistage est positif;
  - et échec de probabilité $1 - p = 0,969$ sinon.

  Donc la variable aléatoire X qui est égale au nombre de succès au cours de ces $n = 200$ épreuves *indépendantes* de *Bernoulli* de paramètre $p = 0,031$ suit une *loi binomiale* de paramètres $n = 200$ et $p = 0,031$.
  On peut écrire :
  $$X \text{ suit } \mathscr{B}\left(200\ ;\ 0,031\right) \text{ ou } X \sim \mathscr{B}\left(200\ ;\ 0,031\right).$$
- Calculs
  La probabilité que, sur les 200 dépistages, il y ait eu strictement plus de 5 dépistages positifs, est directement donnée par la calculatrice :
  $$P(X > 5) = 1 - P(X \leq 5) \approx \underline{0,59}$$
  L'affirmation est vraie.

  Calculatrices
  - *Sur la TI Voyage 200 :* $1 -$ *TIStat.binomFdR* (200 , 0,031 , 5) $\approx 0,5888$
  - *Sur TI82/83+ : Menu Distrib* $\Rightarrow 1 -$ *binomFrép* (200 , 0,031 , 5) $\approx 0,5888$
  - *Sur Casio 35+ ou 75 : Menu Opt/STAT/DIST/DINM* $\Rightarrow 1 -$ *binomialCD* (5 , 200 , 0,031) $\approx 0,5888$

Affirmation 3 (Fausse)

On considère dans $\mathbb{R}$ l'équation : $\ln(6x-2) + \ln(2x-1) = \ln(x)$.
Affirmation 3 : l'équation admet deux solutions dans l'intervalle $\left]\frac{1}{2}\ ;\ +\infty\right[$.

- Ensemble de définition.
  La fonction ln est définie sur $\mathbb{R}_+^*$ donc il faut que :
  $$\begin{cases} 6x-2>0 \\ 2x-1>0 \\ x>0 \end{cases} \Longrightarrow \begin{cases} x > \frac{1}{3} \\ x > \frac{1}{2} \\ x>0 \end{cases} \Longrightarrow x > \frac{1}{2}$$
  Sur l'intervalle $I = \left]\frac{1}{2}\ ;\ +\infty\right[$, l'expression est donc définie.
- Résolution sur cet intervalle I.
  $$\begin{aligned} \ln(6x-2) + \ln(2x-1) = \ln(x) &\iff \ln(6x-2)(2x-1) = \ln(x) \text{ et } x \in I \\ &\iff (6x-2)(2x-1) = x \text{ et } x \in I \\ &\iff 12x^2 - 6x - 4x + 2 = x \text{ et } x \in I \\ &\iff 12x^2 - 11x + 2 = 0 \text{ et } x \in I \end{aligned}$$

©ISSN 2272-5318

L'équation $12x^2-11x+2=0$ est une équation de second degré de la forme $ax^2+bx+c=0$ avec $\begin{cases} a=12 \\ b=-11 \\ c=2 \end{cases}$.

Le discriminant est $\Delta=(-11)^2-4\times 12\times 2=25>0$. Donc elle admet deux racines réelles qui sont :

$$x_1=\frac{11-\sqrt{25}}{24}=\frac{1}{4}\notin \left]\frac{1}{2}\,;\,+\infty\right[\quad \text{et} \quad x_2=\frac{11+\sqrt{25}}{24}=\frac{2}{3}\in \left]\frac{1}{2}\,;\,+\infty\right[$$

L'équation admet donc une unique solution dans $\left]\frac{1}{2}\,;\,+\infty\right[$ qui est : $\frac{2}{3}$. L'affirmation est donc fausse.

Affirmation 4 (Vraie)

On considère dans $\mathbb{C}$ l'équation : $\left(4z^2-20z+37\right)(2z-7+2\mathrm{i})=0$.
Affirmation 4 : les solutions de l'équation sont les affixes de points appartenant à un même cercle de centre le point P d'affixe 2.

On a :

$$\left(4z^2-20z+37\right)(2z-7+2\mathrm{i})=0 \iff \begin{cases} 4z^2-20z+37=0 \\ 2z-7+2\mathrm{i}=0 \end{cases} \iff \begin{cases} 4z^2-20z+37=0 \\ z_1=\dfrac{7-2\mathrm{i}}{2} \end{cases}$$

L'équation $4z^2-20z+37=0$ est une équation de second degré de la forme $az^2+bz+c=0$ avec $\begin{cases} a=4 \\ b=-20 \\ c=37 \end{cases}$.

Le discriminant est $\Delta=-192<0$. Donc elle admet deux racines complexes conjuguées qui sont :

$$z_2=\frac{20+\sqrt{192}\mathrm{i}}{8}=\frac{5+2\mathrm{i}\sqrt{3}}{2} \quad \text{et} \quad z_3=\overline{z_2}=\frac{5-2\mathrm{i}\sqrt{3}}{2}$$

Les trois solutions complexes de l'équation sont donc :

$$\left(4z^2-20z+37\right)(2z-7+2\mathrm{i})=0 \iff \begin{cases} z_2=\dfrac{5+2\mathrm{i}\sqrt{3}}{2} \\ z_3=\overline{z_2}=\dfrac{5-2\mathrm{i}\sqrt{3}}{2} \\ z_1=\dfrac{7-2\mathrm{i}}{2} \end{cases}$$

Notons alors A, B, C et P les points d'affixe z_1, z_2, z_3 et 2. On a alors :

$$\begin{cases} PA=|z_1-2|=\left|\dfrac{3}{2}-\mathrm{i}\right|=\dfrac{\sqrt{13}}{2} \\ PB=|z_2-2|=\left|\dfrac{5+2\mathrm{i}\sqrt{3}}{2}-2\right|=\left|\dfrac{1}{2}-\sqrt{3}\,\mathrm{i}\right|=\dfrac{\sqrt{13}}{2} \\ PC=|z_3-2|=\left|\overline{z_2}-2\right|=\left|\overline{z_2-2}\right|=PB=\dfrac{\sqrt{13}}{2} \end{cases}$$

Les solutions de l'équation sont les affixes de points appartenant à un même cercle de centre le point P d'affixe 2, l'affirmation est vraie.

Exercice 3. Probabilités — 7 points

Commun à tous/toutes les candidat/e/s

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

Partie A

Le détaillant constate que ses melons se vendent bien lorsque leur masse est comprise entre 900 *g et 1 200 g. Dans la suite, de tels melons sont qualifiés « conformes ». Le détaillant achète ses melons auprès de trois maraîchers, notés respectivement A, B et C. Pour les melons du maraîcher A, on modélise la masse en gramme par une variable aléatoire M_A qui suit une loi uniforme sur l'intervalle* [850 ; x], *où x est un nombre réel supérieur à 1 200. La masse en gramme des melons du maraîcher B est modélisée par une variable aléatoire M_B qui suit une loi normale de moyenne 1 050 et d'écart-type inconnu σ. Le maraîcher C affirme, quant à lui, que 80 % des melons de sa production sont conformes.*

1. Le détaillant constate que 75 % des melons du maraîcher A sont conformes. Déterminer x.

Propriété 3

Soit X la variable aléatoire suivant une loi uniforme sur l'intervalle [a ; b]. Pour tout c et d de l'intervalle [a ; b] avec $c < d$ on a :

$$\boxed{P(c \leq X \leq d) = \frac{d-c}{b-a}} \text{ : (1)} \quad \text{et} \quad \boxed{E(X) = \frac{b+a}{2}} \text{ : (2)}$$

Pour les melons du maraîcher A, on modélise la masse en gramme par une variable aléatoire M_A qui suit une loi uniforme sur l'intervalle [850 ; x], où x est un nombre réel supérieur à 1 200. Donc puisque 75 % des melons du maraîcher A sont conformes on a :

$$P(900 \leq M_A \leq 1200) = 0,75 \iff \frac{1200-900}{x-850} = 0,75 \iff x = \frac{300}{0,75} + 850 = \underline{1\,250}$$

2. Il constate que 85 % des melons fournis par le maraîcher B sont conformes. Déterminer l'écart-type σ de la variable aléatoire M_B. En donner la valeur arrondie à l'unité.

La masse en gramme des melons du maraîcher B est modélisée par une variable aléatoire M_B qui suit une loi normale de moyenne 1 050 et d'écart-type inconnu σ. Or on sait que 85 % des melons fournis par le maraîcher B sont conformes donc $P(900 \leq M_B \leq 1250) = 0,85$.

Propriété 4

Soit μ un réel et σ un réel strictement positif.

La variable aléatoire M_B suit la loi normale $\mathcal{N}(\mu\,;\,\sigma^2)$ si et seulement si, la variable aléatoire $Z = \dfrac{M_B - \mu}{\sigma}$ suit la loi normale centrée réduite $\mathcal{N}(0\,;\,1)$.

Donc ici, puisque M_B suit la loi normale $\mathcal{N}(1050\,;\,\sigma^2)$, la v.a. $Z = \dfrac{M_B - 1050}{\sigma}$ suit la loi normale centrée réduite $\mathcal{N}(0\,;\,1)$.
On cherche ici une valeur approchée à 10^{-0} de σ sachant que $P(900 \leqslant M_B \leqslant 1200) = 0,85$, or :

$$P(900 \leqslant M_B \leqslant 1200) = 0,85 \iff P\left(\frac{900-1050}{\sigma} \leqslant \frac{M_B - 1050}{\sigma} \leqslant \frac{1200-1050}{\sigma}\right) = 0,85$$
$$\iff P\left(\frac{-150}{\sigma} \leqslant Z \leqslant \frac{150}{\sigma}\right) = 0,85$$

Or la v.a. Z suit la loi normale centrée réduite et on rappelle que :

©ISSN 2272-5318

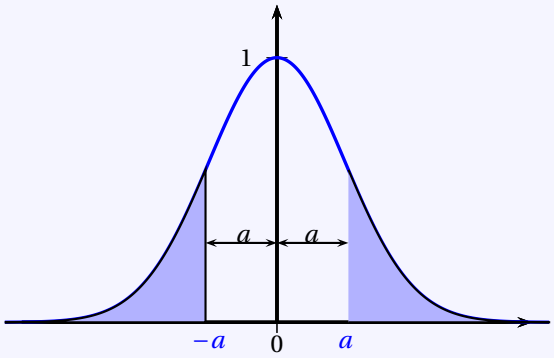
Propriété 5

Soit Z une v.a. qui suit la loi normale centrée réduite $\mathcal{N}(0\,;\,1)$.

2. a. La fonction Φ est définie sur $\mathbb{R}$ par $\Phi(t) = P(Z \leq t)$.

2. b. Pour tout réel a on a :

- (1) : $P(Z \leq -a) = P(Z \geq a)$
- (2) : $\Phi(-a) = 1 - \Phi(a)$
- (3) : $P(-a \leq Z \leq a) = 2\Phi(a) - 1$



De ce fait en appliquant la relation (3) de la propriété 5 :

$$\begin{aligned} P(900 \leqslant M_B \leqslant 1200) = 0,85 &\iff P\left(\frac{-150}{\sigma} \leqslant Z \leqslant \frac{150}{\sigma}\right) = 0,85 \\ &\iff 2\Phi\left(\frac{150}{\sigma}\right) - 1 = 0,85 \\ &\iff \Phi\left(\frac{150}{\sigma}\right) = \frac{0,85+1}{2} = 0,925 \\ &\iff P\left(Z \leq \frac{150}{\sigma}\right) = 0,925 \end{aligned}$$

La calculatrice nous donne alors avec la fonction répartition normale réciproque :

$$Z \sim \mathcal{N}(0\,;\,1) \Longrightarrow \frac{150}{\sigma} \approx 1,439\,531\,471$$

Soit arrondi à 10^{-0} près :

$$\boxed{\sigma \approx 104}$$

Calculatrices

- *Sur la TI Voyage 200 : TIStat.invNorm*(0,925 , 0 , 1) $\approx$ 1,439 531 471
- *Sur TI82/83+ : invNorm*(0,925 , 0 , 1) *ou (fr.) FracNormale*(0,925 , 0 , 1)
- *Sur Casio 35+ ou 75 : Menu STAT/DIST/NORM/InvN* $\Rightarrow$ *InvNormCD*(0,925 , 1 , 0)

3. Le détaillant doute de l'affirmation du maraîcher C. Il constate que sur 400 melons livrés par ce maraîcher au cours d'une semaine, seulement 294 sont conformes. Le détaillant a-t-il raison de douter de l'affirmation du maraîcher C ?

- **Analyse des données** :
  - « Sur un échantillon de $n = 400$ melons. Il est constaté que 294 d'entre eux sont conformes. ». Donc la fréquence observée melons conformes est
    $$f = 294 \div 400 = 0,735 \text{ soit } \underline{f = 0,735}$$
  - Le maraîcher C affirme, quant à lui, que 80 % des melons de sa production sont conformes. On veut tester l'hypothèse : « la proportion de melons conformes est $\underline{p = 80\%}$ ».

- **Intervalle de fluctuation** :

Théorème 2 (Intervalle de fluctuation asymptotique)

Si les conditions suivantes sont remplies : $\begin{cases} \checkmark & n \geq 30 \\ \checkmark & np \geq 5 \\ \checkmark & n(1-p) \geq 5 \end{cases}$

Alors un intervalle de fluctuation asymptotique au seuil 95% de la fréquence F_n d'un caractère dans un échantillon de taille n est si p désigne la proportion de ce caractère dans la population :

$$I_n = \left[p - 1{,}96\,\frac{\sqrt{p(1-p)}}{\sqrt{n}} \,;\; p + 1{,}96\,\frac{\sqrt{p(1-p)}}{\sqrt{n}} \right]$$

On a pour le cas étudié, $n = 400$, $p = 80$ %. Vérifions les conditions d'application du théorème :

$$\begin{cases} \checkmark & n = 400 \geq 30 \\ \checkmark & np = 400 \times 0{,}8 = 320 \geq 5 \\ \checkmark & n(1-p) = 400 \times 0{,}2 = 80 \geq 5 \end{cases}$$

Un intervalle fluctuation asymptotique au seuil 95% est alors :

$$I_n = \left[p - 1{,}96\frac{\sqrt{p(1-p)}}{\sqrt{n}} \,;\; p + 1{,}96\frac{\sqrt{p(1-p)}}{\sqrt{n}} \right] = \left[0{,}8 - 1{,}96\,\frac{\sqrt{0{,}8 \times 0{,}2}}{\sqrt{400}} \,;\, 0{,}8 + 1{,}96\,\frac{\sqrt{0{,}8 \times 0{,}2}}{\sqrt{400}} \right]$$

Soit puisque les borne sont :

- $p - 1{,}96\,\dfrac{\sqrt{p(1-p)}}{\sqrt{n}} \approx 0{,}7608$. On arrondit la borne inférieure par défaut à 10^{-3} près soit $\underline{0{,}76}$.
- $p + 1{,}96\,\dfrac{\sqrt{p(1-p)}}{\sqrt{n}} \approx 0{,}8392$. On arrondit la borne supérieure par excès à 10^{-3} près soit $\underline{0{,}84}$.

$$\boxed{I_{400} \approx [0{,}76 \;;\; 0{,}84]}$$

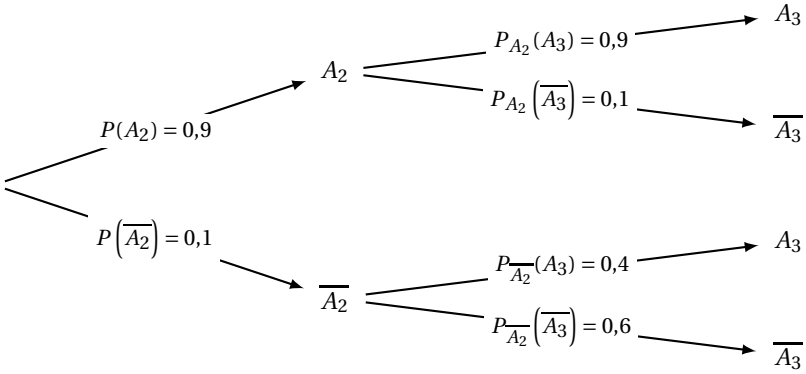
- **Conclusion**
La fréquence observée appartient à l'intervalle, $f = 0{,}735 \notin I$ donc le résultat du contrôle remet en question l'hypothèse, au seuil de 95%.

Partie B

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 $p(A_1) = 1$.

1.

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



©ISSN 2272-5318

1. b. Démontrer que $p(\overline{A_3}) = 0,85$.

Les évènements A_2 et $\overline{A_2}$ formant une partition de l'univers, on a d'après la formule des probabilités totales :

$$\begin{aligned}
P(A_3) &= P(A_3 \cap A_2) + P\left(A_3 \cap \overline{A_2}\right)\\
P(A_3) &= P(A_2) \times P_{A_2}(A_3) + P\left(\overline{A_2}\right) \times P_{\overline{A_2}}(A_3)\\
P(A_3) &= 0,9 \times 0,9 + 0,1 \times 0,4\\
P(A_3) &= 0,81 + 0,04\\
P(A_3) &= \underline{0,85}
\end{aligned}$$

1. 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.

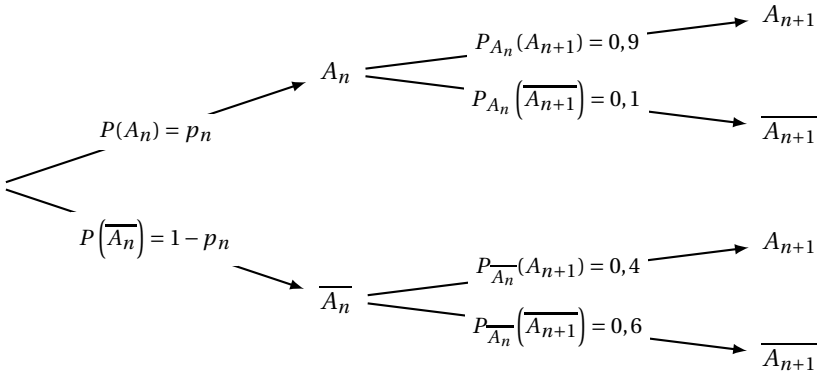
La probabilité cherchée est $P_{A_3}(A_2)$ soit :

$$\begin{aligned}
P_{A_3}(A_2) &= \frac{P(A_2 \cap A_3)}{P(A_3)}\\
&= \frac{0,9 \times 0,9}{0,85}\\
&= \frac{81}{85}\\
P_{A_3}(A_2) &\approx \underline{0,95}
\end{aligned}$$

Dans la suite, on pose pour tout entier $n \geqslant 1$: $p_n = P(A_n)$. On a ainsi $p_1 = 1$.

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

On peut représenter la situation par l'arbre suivant :



D'après la formule des probabilités totales on a pour n entier, $n \geq 1$:

$$\begin{aligned}
p_{n+1} &= P(A_n \cap A_{n+1}) + P\left(\overline{A_n} \cap A_{n+1}\right)\\
&= 0,9p_n + 0,4\left(1 - p_n\right)\\
p_{n+1} &= \underline{0,5p_n + 0,4}
\end{aligned}$$

3.

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

Notons pour tout entier naturel $n \geq 1$ le postulat

$$(P_n) \ : \ p_n > 0,8$$

- **Initialisation**
  Pour $n = 1$, le postulat (P_1) est vrai puisque : $p_1 = 1 > 0,8$.
- **Hérédité**
  Supposons que pour n entier fixé, (P_n) soit vérifié et montrons qu'alors il est aussi vrai au rang $n+1$.
  D'après la question (B.2.) on a :
  $$p_{n+1} = 0,5p_n + 0,4$$

©ISSN 2272-5318

On applique alors l'hypothèse de récurrence qui implique que : (P_n) soit vérifié et donc que $p_n > 0,8$, on a alors :

$$p_{n+1} = 0,5p_n + 0,4 > 0,5 \times 0,8 + 0,4 = 0,8$$

On a alors montré que $p_{n+1} > 0,8$ et donc que (P_{n+1}) est vrai.

- **Conclusion**
On a montré que (P_1) est vrai. De plus, si l'on suppose le postulat (P_n) vérifié, alors il l'est aussi au rang suivant, (P_{n+1}) est vrai. De ce fait la relation est vrai pour tout entier $n \geq 1$.

$$\boxed{p_n > 0,8}$$

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

Pour n entier, $n \geq 1$:

$$\begin{aligned} p_{n+1} - p_n &= 0,5p_n + 0,4 - p_n \\ &= -0,5p_n + 0,4 \\ &= 0,5\left(-p_n + 0,8\right) \end{aligned}$$

Or on vient de montrer dans la question (B.3.a) que $p_n > 0,8$ donc pour n entier, $n \geq 1$

$$\begin{aligned} p_n > 0,8 &\Longrightarrow \left(-p_n + 0,8\right) < -0,8 + 0,8 = 0 \\ &\Longrightarrow 0,5\left(-p_n + 0,8\right) < 0 \\ &\Longrightarrow p_{n+1} - p_n < 0 \end{aligned}$$

La suite (p_n) est décroissante.

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

La suite (p_n) est décroissante et minorée par 0,8, elle est donc convergente vers $L \geq 0,8$.

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

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

Les suites (p_n) et (v_n) sont définies pour tout entier n par :

$$(p_n) : \begin{cases} p_1 &= 1 \\ p_{n+1} &= 0.5 \times p_n + 0,4 \end{cases} \quad \Big| \quad (v_n) : \begin{cases} v_1 & \\ v_n &= p_n - 0,8 \end{cases}$$

Pour tout entier $n \geq 1$ on a :

$$\begin{aligned} v_{n+1} &= p_{n+1} - 0,8 \\ v_{n+1} &= \left(0,5\ p_n + 0,4\right) - 0,8 \\ v_{n+1} &= 0,5 \times p_n - 0,4 \\ v_{n+1} &= 0,5 \times \left(p_n + \frac{-0,4}{0,5}\right) \\ v_{n+1} &= 0,5 \times \left(p_n - 0,8\right) \\ v_{n+1} &= 0,5 \times v_n \end{aligned}$$

La suite (v_n) est donc une suite géométrique de raison $q = 0,5$, et de premier terme $v_1 = 0,2$ puisque :

$$\begin{aligned} v_1 &= p_1 - 0,8 \\ v_1 &= 1 - 0,8 \\ v_1 &= 0,2 \end{aligned}$$

Soit :

$$\boxed{(v_n) : \begin{cases} v_1 &= 0,2 \\ v_{n+1} &= 0,5 \times v_n \end{cases} ;\ \forall n \geq 1}$$

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

La suite (v_n) est géométrique de raison $q = 0,5$, et de premier terme $v_1 = 0,2$ donc son terme général est

$$\forall n \geq 1 \; ; \; v_n = v_1 \times (q)^{n-1}$$

Soit

$$\boxed{\forall n \geq 1 \; ; \; v_n = 0,2 \times (0,5)^{n-1}}$$

De l'égalité définie pour tout entier $n \geq 1$:

$$v_n = p_n - 0,8$$

On peut en déduire l'expression :

$$p_n = v_n + 0,8$$

Soit :

$$\boxed{\forall n \geq 1 \; ; \; p_n = 0,2 \times (0,5)^{n-1} + 0,8}$$

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

Théorème 3

Si le réel q est tel que : $-1 < q < 1$ on a : $\lim\limits_{n \to +\infty} q^n = 0$.

Ici $-1 < q = 0,5 < 1$ et d'après le théorème 3 on a : $\lim\limits_{n \to +\infty} (0,5)^n = 0$. Donc :

$$\lim_{n \to +\infty} 0,2 \times (0,5)^{n-1} = 0 \Longrightarrow \lim_{n \to +\infty} \Big(\underbrace{0,2 \times (0,5)^{n-1} + 0,8}_{p_n} \Big) = 0,8$$

Ce qui nous donne la limite de la suite (p_n) :

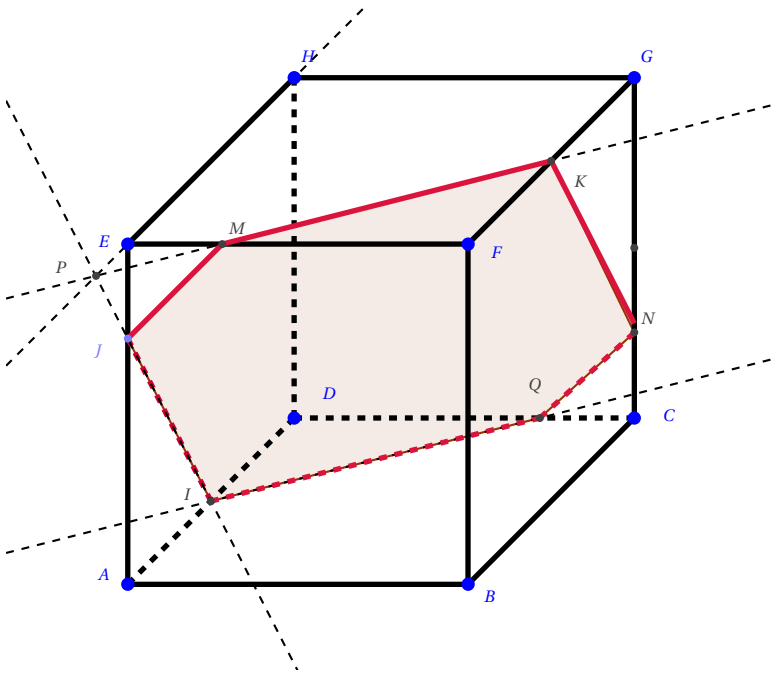
$$\boxed{\lim_{n \to +\infty} p_n = 0,8}$$

©ISSN 2272-5318

Exercice 4. Obligatoire : Espace — 5 points

Candidats n'ayant pas suivi la spécialité mathématique

La figure ci-contre représente un cube ABCDEFGH. Les trois points I, J, K sont définis par les conditions suivantes : I est le milieu du segment [AD] ; J est tel que $\overrightarrow{AJ} = \frac{3}{4}\overrightarrow{AE}$ *; K est le milieu du segment [FG].*



Partie A

1. **Sur la figure donnée en annexe, construire sans justifier le point d'intersection P du plan (IJK) et de la droite (EH). On laissera les traits de construction sur la figure.**

2. **En déduire, en justifiant, l'intersection du plan (IJK) et du plan (EFG).**
L'intersection du plan (IJK) et du plan (EFG) est la droite (PK) puisque :
   - le point P est le point d'intersection du plan (IJK) et de la droite (EH) incluse dans le plan (EFG) ;
   - le point K appartient aussi au deux plans.

Partie B

On se place désormais dans le repère orthonormé $\left(A\,;\,\overrightarrow{AB},\overrightarrow{AD},\overrightarrow{AE}\right)$.

1.

1. a. Donner sans justification les coordonnées des points I, J et K.

$$I\left(0\,;\,\frac{1}{2}\,;\,0\right)\,;\,J\left(0\,;\,0\,;\,\frac{3}{4}\right)\,;\,K\left(1\,;\,\frac{1}{2}\,;\,1\right)$$

1. b. Déterminer les réels a et b tels que le vecteur $\vec{n}$ $(4\,;\,a\,;\,b)$ soit orthogonal aux vecteurs $\overrightarrow{IJ}$ et $\overrightarrow{IK}$.

$$\begin{cases} I\left(0\,;\,\frac{1}{2}\,;\,0\right) \\ J\left(0\,;\,0\,;\,\frac{3}{4}\right) \end{cases} \Longrightarrow \vec{n}\begin{pmatrix}4\\a\\b\end{pmatrix}.\overrightarrow{IJ}\begin{pmatrix}0\\-\frac{1}{2}\\\frac{3}{4}\end{pmatrix} = -\frac{a}{2}+\frac{3b}{4} = 0$$

$$\begin{cases} I\left(0\,;\,\frac{1}{2}\,;\,0\right) \\ K\left(1\,;\,\frac{1}{2}\,;\,1\right) \end{cases} \Longrightarrow \vec{n}\begin{pmatrix}4\\a\\b\end{pmatrix}.\overrightarrow{IK}\begin{pmatrix}1\\0\\1\end{pmatrix} = 4+b = 0$$

©ISSN 2272-5318

On obtient donc :

$$\begin{cases} -\dfrac{a}{2}+\dfrac{3b}{4}=0 \\ b=-4 \end{cases} \Longrightarrow \begin{cases} a=-6 \\ b=-4 \end{cases}$$

De ce fait : $\vec{n}\,(4\,;\,-6\,;\,-4)$.

1. c. En déduire qu'une équation cartésienne du plan (IJK) est : $4x-6y-4z+3=0$.

Propriété 6

Soit vecteur $\vec{u}$ non nul et un point A de l'espace. L'unique plan $\mathscr{P}$ passant par A et de vecteur normal $\vec{u}$ est l'ensemble des points M tels que $\overrightarrow{AM}\,.\,\vec{u}=0$.
Dans un repère de l'espace, son équation est alors de la forme :

$$\overrightarrow{AM}\begin{pmatrix} x-x_A \\ y-y_A \\ z-z_A \end{pmatrix}.\vec{u}\begin{pmatrix} a \\ b \\ c \end{pmatrix}=0 \Longleftrightarrow a(x-x_A)+b\left(y-y_A\right)+c(z-z_A)=0$$

Donc d'après la propriété 6 :

$$M(x\,;\,y\,;\,z)\in(IJK) \Longleftrightarrow \overrightarrow{IM}\begin{pmatrix} x-0 \\ y-\dfrac{1}{2} \\ z-0 \end{pmatrix}.\vec{n}\begin{pmatrix} 4 \\ -6 \\ -4 \end{pmatrix}=0$$

$$M(x\,;\,y\,;\,z)\in(IJK) \Longleftrightarrow 4x-6\left(y-\frac{1}{2}\right)-4z=0$$

$$M(x\,;\,y\,;\,z)\in(IJK) \Longleftrightarrow 4x-6y+3-4z=0$$

$$\boxed{(IJK)\ :\ 4x-6y-4z+3=0}$$

2.

2. a. Donner une représentation paramétrique de la droite (CG).

La droite (CG) passant par le point $C\,(1\,;1\,;0)$ et de vecteur directeur $\overrightarrow{CG}\,(0\,;0\,;1)$ est l'ensemble des points M de l'espace tels que le vecteur $\overrightarrow{CM}$ soit colinéaire à $\overrightarrow{CG}$. On a alors :

$$(CG)=\left\{M(x\,;\,y\,;\,z)\,;\,\overrightarrow{CM}\begin{pmatrix} x-1 \\ y-1 \\ z-0 \end{pmatrix}=t\,\overrightarrow{CG}\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\ ,\ t\in\mathbb{R}\right\}$$

Une représentation paramétrique de la droite (CG) est donc :

$$\boxed{(CG)\ :\ \begin{cases} x=1 \\ y=1 \\ z=t \end{cases},\ t\in\mathbb{R}}$$

2. b. Calculer les coordonnées du point N, intersection du plan (IJK) et de la droite (CG).

On va résoudre le système :

$$\begin{cases} x=1 \\ y=1 \\ z=t \\ 4x-6y-4z+3=0 \end{cases} \Longleftrightarrow \begin{cases} x=1 \\ y=1 \\ z=t \\ 4-6-4t+3=0 \end{cases} \Longleftrightarrow \begin{cases} x=1 \\ y=1 \\ z=t \\ t=\dfrac{1}{4} \end{cases} \Longleftrightarrow \boxed{N\left(1\,;\,1\,;\,\frac{1}{4}\right)}$$

2. c. Placer le point N sur la figure et construire en couleur la section du cube par le plan (IJK).

©ISSN 2272-5318

Partie C

On note R le projeté orthogonal du point F sur le plan (IJK). Le point R est donc l'unique point du plan (IJK) tel que la droite (FR) est orthogonale au plan (IJK). On définit l'intérieur du cube comme l'ensemble des points $M(x\,;\,y\,;\,z)$ tels que
$\begin{cases} \mathbf{0 < x < 1} \\ \mathbf{0 < y < 1} \\ \mathbf{0 < z < 1} \end{cases}$ **Le point R est-il à l'intérieur du cube?**

- La droite (FR).

  La droite (FR) est orthogonale au plan (IJK) donc le vecteur $\vec{n}\begin{pmatrix}4\\-6\\-4\end{pmatrix}$ est un vecteur directeur de cette droite. On peut donc en déterminer une équation paramétrique .

$$(FR) = \left\{ M(x\,;\,y\,;\,z)\,;\, \overrightarrow{FM}\begin{pmatrix}x-1\\y-0\\z-1\end{pmatrix} = t\,\vec{n}\begin{pmatrix}4\\-6\\-4\end{pmatrix}\ ,\ t\in\mathbb{R} \right\}$$

  Une représentation paramétrique de la droite (FR) est donc :

$$\boxed{(FR)\ :\ \begin{cases} x = 4t+1 \\ y = -6t \\ z = -4t+1 \end{cases}\ ,\ t\in\mathbb{R}}$$

- Coordonnées de R.
  Les coordonnées du point R sont solutions du système suivant :

$$\begin{cases} x = 1+4t \\ y = -6t \\ z = 1-4t \\ 4x-6y-4z+3=0 \end{cases} \iff \begin{cases} x = 1+4t \\ y = -6t \\ z = 1-4t \\ 4+16t+36t-4+16t+3=0 \end{cases}$$

$$\iff \begin{cases} x = 1+4t \\ y = -6t \\ z = 1-4t \\ 68t+3=0 \end{cases}$$

$$\iff \begin{cases} x = 1+4t \\ y = -6t \\ z = 1-4t \\ t = -\dfrac{3}{68} \end{cases}$$

$$\iff \begin{cases} x = \dfrac{14}{17} < 1 \\ y = \dfrac{9}{34} < 1 \\ z = \dfrac{20}{17} > 1 \\ t = -\dfrac{3}{68} \end{cases} \iff \boxed{R\left(\frac{14}{17}\,;\,\frac{9}{34}\,;\,\frac{20}{17}\right)}$$

- Conclusion : On a $z_R = \dfrac{20}{17} > 1$ donc le point R n'est pas à l'intérieur du cube.

©ISSN 2272-5318

Exercice 5. Spécialité : Arithmétique — 5 points

Candidats ayant suivi la spécialité mathématique

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 l'entier 8.

1. a. Vérifier que $8^7 \equiv 2 \mod 55$. En déduire le reste dans la division euclidienne par 55 du nombre 8^{21}.

On a :

$$\begin{cases} 8^2 = 64 \equiv 9 \mod 55 \\ 8^6 = \left(8^2\right)^3 \end{cases} \Longrightarrow 8^6 \equiv 9^3 \mod 55$$

$$\Longrightarrow 8^6 \equiv 729 \mod 55$$
$$\Longrightarrow 8^6 \equiv 14 \mod 55$$
$$\Longrightarrow 8^7 \equiv 14 \times 8 \mod 55$$
$$\Longrightarrow 8^7 \equiv 112 \mod 55$$
$$\Longrightarrow \underline{8^7 \equiv 2 \mod 55}$$

De même

$$\begin{cases} 8^7 \equiv 2 \mod 55 \\ 8^{21} = \left(8^7\right)^3 \end{cases} \Longrightarrow 8^{21} \equiv 2^3 \mod 55$$

$$\Longrightarrow \underline{8^{21} \equiv 8 \mod 55}$$

On rappelle que :

Propriété 7 (Compatibilité avec les opérations)

Soit m un entier $m \geq 2$ et a, b, a', b' des entiers.

- (1) : Si $a \equiv b\,[m]$ et $a' \equiv b'\,[m]$, alors $a + a' \equiv b + b'\,[m]$
- (2) : Si $a \equiv b\,[m]$ et $a' \equiv b'\,[m]$, alors $a \times a' \equiv b \times b'\,[m]$
- (3) : Pour $n \in \mathbb{N}^*$, si $a \equiv b\,[m]$, alors $a^n \equiv b^n\,[m]$

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

$$\begin{cases} 8^2 \equiv 9 \mod 55 \\ 8^{21} \equiv 8 \mod 55 \\ 8^{23} = 8^{21} \times 8^2 \end{cases} \Longrightarrow 8^{23} \equiv 8 \times 9 \mod 55$$

$$\Longrightarrow \underline{8^{23} \equiv 17 \mod 55}$$

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

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

Les entiers 23 et 40 sont premiers entre eux donc d'après le théorème de Bezout, l'équation $23x - 40y = 1$ possède un couple de solution (x, y) avec x et y entiers relatifs.

Théorème 4 (Bézout, 1730-1883)

Deux entiers naturels a et b sont premiers entre eux, si et seulement si, il existe deux entiers u et v tels que $au+bv=1$.

Soit :

$$\text{PGCD}(a\,;\,b)=1 \Longleftrightarrow \exists (u\,;\,v)\in\mathbb{Z}^2\,;\,au+bv=1$$

Remarque *: C'est le groupe Bourbaki qui donne vers 1948 le nom de Bézout à ce théorème qui en fait est énoncé et démontré par le mathématicien français Claude-Gaspard Bachet de Méziriac (1581-1638) dans ses « Problèmes plaisans et délectables » publié en 1624. Bézout démontre lui une généralisation de ce théorème aux polynômes en 1764 dans un mémoire présenté à l'académie des sciences.*

2. b. Donner un couple, solution particulière de l'équation (E).

Par divisions euclidiennes successives on obtient avec $a=23$ et $b=40$:

Division euclidienne	**Reste**	**Egalité avec a et b**
$23=40\times 0+23$	$23=23-0\times 40$	
$40=23\times 1+17$	$17=40-1\times 23$	$17=-1\,a+1\,b$
$23=17\times 1+6$	$6=23-1\times 17$	$6=a-1\,b$
$17=6\times 2+5$	$5=17-2\times 6$	$5=(-1\,a+1\,b)-2\times(2\,a-1\,b)$ $5=-5\,a+3\,b$
$6=5\times 1+1$	$1=6-1\times 5$	$1=(2\,a-1\,b)-1\times(-5\,a+3\,b)$ $1=7\,a+(-4)\,b$

Le PGCD des nombres 23 et 40 est le dernier reste non nul du procédé, c'est-à-dire 1.
Les nombres 23 et 40 sont donc premiers entre eux et le théorème 4 dit de Bézout-Bachet assure donc l'existence de couples $(x\,;\,y)$ d'entiers relatifs solutions de l'équation :

$$23\,x+40\,y=1$$

Pour trouver une solution, il suffisait d'exprimer le reste de la division euclidienne en fonction de a et b pour chaque ligne du procédé. Un couple solution de l'équation $23\,x+40\,y=1$ est donc : $(7\,;\,-4)$.
De ce fait, un couple solution de l'équation :

$$23\,x-40\,y=1$$

est donc :

$$\boxed{(x=7\,;\,y=4)}$$

Une solution particulière est : $(7\,;\,4)$

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

- Soit (x, y) un couple solution.

  – **Transformation de l'équation**

  $$(E)\ :\ 23x-40y=1$$

  Puisque le couple $(7\ ;\ 4)$ est une solution particulière de l'équation (E) on a : $23\times 7-40\times 4=1$.
  Donc

  $$\begin{cases} 23\times x - 40\times y = 1 \\ 23\times 7 - 40\times 4 = 1 \end{cases} \underset{\text{par soustraction}}{\Longrightarrow} 23(x-7)-40(y-4)=0$$

  Donc l'équation (E) devient :

  $$(E)\ :\ 23(x-7)=40(y-4)$$

  – **Application du théorème de Gauss**

  $$(E)\ :\ 23(x-7)=40(y-4)$$

  Puisque 23 et 40 sont premiers entre eux, alors en appliquant le théorème de Gauss :

  $$\begin{cases} 23 \text{ divise le produit } 40(y-4) \\ 23 \text{ et } 40 \text{ sont premiers entre eux} \end{cases} \underset{\text{d'après le th. de Gauss}}{\Longrightarrow} 23 \text{ divise } (y-4)$$

  $$\begin{cases} 40 \text{ divise le produit } 23(x-7) \\ 23 \text{ et } 40 \text{ sont premiers entre eux} \end{cases} \underset{\text{d'après le th. de Gauss}}{\Longrightarrow} 40 \text{ divise } (x-7)$$

  Il existe donc des entiers k et k' tels que :

  $$\begin{cases} (y-4) = 23k \\ (x-7) = 40k' \end{cases}$$

  En reportant dans l'équation (E) on obtient

  $$23\times 40k' = 40\times 23k \Longleftrightarrow k=k'$$

  Ainsi, les solutions de l'équation (E) sont les couples de la forme

  $$\boxed{(7+40k\ \ ;\ 4+23k)\ ;\ k\in\mathbb{Z}}$$

- Réciproquement,
  si k est un entier relatif, $(7+40k, 4+23k)$ est solution de l'équation (E) puisque : $23\times(7+40k)-40\times(4+23k)=1$.
- Conclusion : Les solutions de l'équation (E) sont donc les couples $(7+40k, 4+23k)$ pour tout entier relatif k.

Théorème 5 (Carl Friedrich Gauss, 1777-1855)

Soit a, b, c des entiers.

Si $\begin{cases} a \text{ divise le produit } bc \\ \text{et} \\ a \text{ et } b \text{ sont premiers entre eux} \end{cases}$, alors a divise c.

Remarque *: Le mathématicien allemand Carl Friedrich Gauss énonce et prouve ce théorème (sous forme de lemme en fait) en 1801 dans son ouvrage « Disquisitiones arithmeticae ».*

©ISSN 2272-5318

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

- On vient de montrer que les solution de l'équation $23x - 40y = 1$ sont les couples $(7+40k, 4+23k)$ pour tout entier relatif k. De ce fait :

$$23x - 40y = 1 \iff 23x = 1 + 40y \iff 23x \equiv 1 \mod 40 \iff x = 7 + 40k$$

- Si on impose alors que $0 \leqslant x < 40$ alors nécessairement $k = 0$ et donc $x = 7$.
- Conclusion : il existe un unique entier d vérifiant les conditions $0 \leqslant d < 40$ et $23d \equiv 1 \mod 40$.
  Cet entier est : $\underline{d = 7}$.

3. *Cryptage dans le système RSA. Une personne A choisit deux nombres premiers p et q, puis calcule les produits $N = pq$ et $n = (p-1)(q-1)$. Elle choisit également un entier naturel c premier avec n. La personne A publie le couple $(N\ ;\ c)$, 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 $N-1$. 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 $c = 23$.*

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

On a :

$$\begin{cases} p = 5 \\ q = 11 \end{cases} \Longrightarrow \begin{cases} N = pq = 55 \\ n = (p-1)(q-1) = 40 \end{cases}$$

L'entier premier $c = 23$ doit être premier avec $n = 40$ ce qui est bien la cas.

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

Pour crypter l'entier $a = 8$, on calcule le reste b dans la division euclidienne par $N = 55$ du nombre $a^c = 8^{23}$, et le nombre crypté est l'entier b. On a donc d'après la question (1.b) :

$$a^c = 8^{23} \equiv 17 \mod 55 \Longrightarrow \underline{b = 17}$$

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 $cd \equiv 1 \mod n$. 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. Les nombres choisis par A sont encore $p = 5$, $q = 11$ et $c = 23$.*

4. a. Quelle est la valeur de d ?

La personne A calcule dans un premier temps l'unique entier naturel d vérifiant les conditions $0 \leqslant d < n$ et $cd \equiv 1 \mod n$. Or ici on a

$$\begin{cases} n = 40 \text{ et } c = 23 \\ 0 \leqslant d < n \\ cd \equiv 1 \mod n \end{cases} \Longrightarrow \begin{cases} 0 \leqslant d < 40 \\ 23d \equiv 1 \mod n \end{cases}$$

La question (2.d) a montré que $\underline{d = 7}$.

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

Pour décrypter un nombre crypté $b = 17$, la personne A calcule le reste a dans la division euclidienne par $N = 55$ du nombre $b^d = 17^7$, et le nombre en clair – c'est-à-dire le nombre avant cryptage – est le nombre a. On a donc :

$$b^d = 17^7 \equiv 8 \mod 55 \Longrightarrow \underline{a = 8}$$

On a :

$$\begin{cases} 17^2 = 289 \equiv 14 \mod 55 \\ 17^6 = \left(17^2\right)^3 \end{cases} \Longrightarrow 17^6 \equiv 14^3 \mod 55$$

$$\Longrightarrow 17^6 \equiv 2\,744 \mod 55$$

$$\Longrightarrow 17^6 \equiv 49 \mod 55$$

$$\Longrightarrow 17^7 \equiv 49 \times 17 \mod 55$$

$$\Longrightarrow 14^7 \equiv 833 \mod 55$$

$$\Longrightarrow \underline{17^7 \equiv 8 \mod 55}$$

Fin du devoir

©ISSN 2272-5318