CONCOURS BLANC JUIN 2022

# MATHÉMATIQUES 2

## Corrigé

**EXERCICE 1 — (ANALYSE - ENS LYON 2019).**

**1.** Rappeler sans démonstration le développement limité à l'ordre 3 en 0 de $x \longmapsto \dfrac{1}{1-x}$.

Au voisinage de 0 : $\dfrac{1}{1-x} = 1 + x + x^2 + x^3 + o(x^3)$

**2.** Déterminer le développement limité à l'ordre 7 en 0 de $x \longmapsto \dfrac{1}{1+x^2}$.

Par changement de variable à partir de la question précédente, et par parité de $x \longmapsto \dfrac{1}{1+x^2}$, on a au voisinage de 0 : $\dfrac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + o(x^7)$

**3.** En déduire le développement limité à l'ordre 7 en 0 de $x \longmapsto \arctan(x)$.

Par intégration à partir de la question précédente, et en utilisant $\arctan(0) = 0$, on a au voisinage de 0 : $\arctan(x) = x - \dfrac{x^3}{3} + \dfrac{x^5}{5} - \dfrac{x^7}{7} + o(x^7)$

Soient $f, g : ]-1,1[ \longrightarrow \mathbb{R}$ deux fonctions de classe $\mathscr{C}^\infty$ telles que $f(0) = g(0) = 0$.
On pose : $h = f \circ g$ et $H = f \circ g - g \circ f$.

**4.** Montrer que les fonctions $h$ et $H$ sont bien définies sur un voisinage de l'origine.

Puisque par hypothèse $f(0) = 0$ et $f$ est continue en 0 :

$$\exists\, \alpha > 0,\ f\left(]-\alpha, \alpha[\right) \subset ]-1,1[$$

Pour les mêmes raisons :

$$\exists\, \beta > 0,\ g\left(]-\beta, \beta[\right) \subset ]-1,1[$$

En posant $\gamma = \min(\alpha, \beta)$, les fonctions $f \circ g$ et $g \circ f$ sont définies sur $]-\gamma, \gamma[$.

Il s'ensuit que $h$ et $H$ le sont également.

**Conclusion**. Les fonctions $h$ et $H$ sont définies au voisinage de 0.

**5.** Exprimer les dérivées $h'$, $h''$ et $h'''$ en fonction de celles de $f$ et de $g$.

Au voisinage de 0, on a : $h(x) = f(g(x))$.

D'après l'énoncé et les TG, $h$ est de classe $\mathscr{C}^\infty$ sur un voisinage de 0 et :

- $h'(x) = f'(g(x))g'(x)$
- $h''(x) = f''(g(x))(g'(x))^2 + f'(g(x))g''(x)$
- $h^{(3)}(x) = f^{(3)}(g(x))(g'(x))^3 + 2f''(g(x))g'(x)g''(x) + f''(g(x))g'(x)g''(x) + f'(g(x))g^{(3)}(x)$

$$\iff h^{(3)}(x) = f^{(3)}(g(x))(g'(x))^3 + 3f''(g(x))g'(x)g''(x) + f'(g(x))g^{(3)}(x)$$

**6.** On suppose dorénavant que $f$ et $g$ sont impaires, avec : $f'(0) = g'(0) = 1$.

Montrer que $H\left(x\right) = O\left(x^5\right)$ au voisinage de 0.

En notant $\varphi = f$ ou $g$, on a déjà selon l'énoncé :

$$\varphi(0) = \varphi''(0) = \varphi^{(4)}(0) = 0 \text{ (car } \varphi \text{ est impaire)} \qquad \text{et} \qquad \varphi'(0) = 1 \qquad (\spadesuit)$$

Par ailleurs, la fonction $H$ admet un DL à l'ordre 5 en 0 ($H$ étant de classe $\mathscr{C}^\infty$ au voisinage de 0, d'après l'énoncé et les TG), donné par la formule de Taylor-Young :

$$H(x) = H(0) + H'(0)x + H''(0)\frac{x^2}{2!} + H^{(3)}(0)\frac{x^3}{3!} + H^{(4)}(0)\frac{x^4}{4!} + H^{(5)}(0)\frac{x^5}{5!} + o\left(x^5\right) \qquad (\clubsuit)$$

Or, les fonctions $f$ et $g$ étant impaires, $f \circ g$ et $g \circ f$ le sont aussi ; donc $H$ est impaire.

Il s'ensuit que :

$$H(0) = H''(0) = H^{(4)}(0) = 0 \qquad (\heartsuit)$$

En outre :

- $H'(0) = f'(g(0))g'(0) - g'(g(0))f'(0) = 0$ (selon 5 et $(\spadesuit)$)
- $H^{(3)}(0) = f^{(3)}(g(0))(g'(0))^3 + 3f''(g(0))g'(0)g''(0) + f'(g(0))g^{(3)}(0)$
  $-g^{(3)}(f(0))(f'(0))^3 + 3g''(f(0))f'(0)f''(0) + g'(f(0))f^{(3)}(0) = 0$ (selon 5 et $(\spadesuit)$)

De ces 2 denières valeurs, ainsi que de $(\spadesuit)$, $(\clubsuit)$ et $(\heartsuit)$, on déduit que sur un voisinage de 0 :

$$H(x) = H^{(5)}(0)\frac{x^5}{5!} + o\left(x^5\right)$$

**Conclusion.** $H\left(x\right) = O\left(x^5\right)$ au voisinage de 0.

**7.** En continuant le développement de $H$, montrer que : $H(x) = O\left(x^7\right)$.

Grâce à la question précédente, et toujours selon la formule de Taylor-Young, on a au voisinage de 0 :

$$H(x) = H^{(5)}(0)\frac{x^5}{5!} + H^{(6)}(0)\frac{x^6}{6!} + H^{(7)}(0)\frac{x^7}{7!} + o\left(x^7\right)$$

Or $H$ étant impaire (cf question précédente), on a : $H^{(6)}(0) = 0$. Par suite :

$$H(x) = H^{(5)}(0)\frac{x^5}{5!} + H^{(7)}(0)\frac{x^7}{7!} + o\left(x^7\right)$$

Il ne reste donc plus qu'à calculer la dérivée 5-ème de $H$.

Commencer par noter que : $H^{(5)} = (f \circ g)^{(5)} - (g \circ f)^{(5)}$.

Au voisinage de 0, on a (en dérivant l'expression de $h^{(3)}$ obtenue à la question 5) :

$$\begin{aligned}(f \circ g)^{(4)}(x) = {} & f^{(4)}(g(x))g'(x)^4 + 6f^{(3)}(g(x))g''(x)g'(x)^2 + 3f''(g(x))g''(x)^2 \\ & +4f''(g(x))g'(x)g^{(3)}(x) + f'(g(x))g^{(4)}(x)\end{aligned}$$

Encouragés par ce résultat prometteur, continuons les calculs en dérivant une nouvelle fois cette expression :

$$(f \circ g)^{(5)}(x) = \begin{array}{l} f^{(5)}(g(x))g'(x)^5 + 4f^{(4)}(g(x))g''(x)g'(x)^3 + 6f^{(4)}(g(x))g''(x)g'(x)^2 \\ +6f^{(3)}(g(x))g^{(3)}(x)g'(x)^2 + 12f^{(3)}(g(x))g''(x)^2g'(x) + 3f^{(3)}(g(x))g'(x)g''(x)^2 \\ +6f''(g(x))g''(x)g^{(3)}(x) + 4f^{(3)}(g(x))g^{(3)}(x)g'(x)^2 + 4f''(g(x))g''(x)g^{(3)}(x) \\ +4f''(g(x))g'(x)g^{(4)}(x) + f''(g(x))g'(x)g^{(4)}(x) + f'(g(x))g^{(5)}(x) \end{array}$$

Expression qui se simplifie spectaculairement en :

$$(f \circ g)^{(5)}(x) = \begin{array}{l} f^{(5)}(g(x))g'(x)^5 + 4f^{(4)}(g(x))g''(x)g'(x)^3 + 6f^{(4)}(g(x))g''(x)g'(x)^2 \\ +10f^{(3)}(g(x))g^{(3)}(x)g'(x)^2 + 15f^{(3)}(g(x))g''(x)^2g'(x) + 10f''(g(x))g''(x)g^{(3)}(x) \\ +5f''(g(x))g'(x)g^{(4)}(x) + f'(g(x))g^{(5)}(x) \end{array}$$

On en déduit facilement l'expression de $(g \circ f)^{(5)}(x)$, donc l'expression de

$$H^{(5)}(0) = (f \circ g)^{(5)}(0) - (g \circ f)^{(5)}(0)$$

Explicitement, on obtient grâce au calcul ci-dessus et aux conditions notées (♠) dans la question précédente :

$$H^{(5)}(0) = \underbrace{f^{(5)}(0) + 10f^{(3)}(0)g^{(3)}(0) + g^{(5)}(0)}_{=(f\circ g)^{(5)}(0)} - \underbrace{g^{(5)}(0) + 10g^{(3)}(0)f^{(3)}(0) + f^{(5)}(0)}_{=(g\circ f)^{(5)}(0)}$$

D'où $H^{(5)}(0) = 0$, ce qui est une agréable surprise...

**Conclusion**. Au voisinage de 0, on a : $H(x) = H^{(7)}(0)\dfrac{x^7}{7!} + o\left(x^7\right)$. D'où : $H(x) = O(x^7)$

**8.** On admet la formule suivante (qui tient compte des hypothèses faites plus haut) pour la dérivée 7ème de $h$ :

$$h^{(7)}(0) = g^{(7)}(0) + 21g^{(5)}(0)f^{(3)}(0) + 70g^{(3)}(0)^2\, f^{(3)}(0) + 35g^{(3)}(0)f^{(5)}(0) + f^{(7)}(0)$$

Trouver le développement limité à l'ordre 7 en 0 de $H$ en 0.

La fonction $H$ étant impaire, on a déjà : $H^{(6)}(0) = 0$.

De plus, grâce à l'indication de l'énoncé, on a :

$$\begin{aligned} H^{(7)}(0) &= g^{(7)}(0) + 21g^{(5)}(0)f^{(3)}(0) + 70g^{(3)}(0)^2\, f^{(3)}(0) + 35g^{(3)}(0)f^{(5)}(0) + f^{(7)}(0) \\ &\quad - \left[f^{(7)}(0) + 21f^{(5)}(0)g^{(3)}(0) + 70f^{(3)}(0)^2\, g^{(3)}(0) + 35f^{(3)}(0)g^{(5)}(0) + g^{(7)}(0)\right] \end{aligned}$$

$$\begin{aligned} \Longleftrightarrow H^{(7)}(0) &= 21\left(g^{(5)}(0)f^{(3)}(0) - f^{(5)}(0)g^{(3)}(0)\right) + 70\left(g^{(3)}(0)^2\, f^{(3)}(0) - f^{(3)}(0)^2\, g^{(3)}(0)\right) \\ &\quad +35\left(g^{(3)}(0)f^{(5)}(0) - f^{(3)}(0)g^{(5)}(0)\right) \end{aligned}$$

$$\Longleftrightarrow H^{(7)}(0) = 14\left(g^{(3)}(0)f^{(5)}(0) - f^{(3)}(0)g^{(5)}(0)\right) + 70\left(g^{(3)}(0)^2\, f^{(3)}(0) - f^{(3)}(0)^2\, g^{(3)}(0)\right)$$

Par suite, au voisinage de 0, on a :

$$H(x) = \frac{\alpha}{7!}x^7 + o(x^7)$$

$$\text{avec } \alpha = 14\left(g^{(3)}(0)f^{(5)}(0) - f^{(3)}(0)g^{(5)}(0)\right) + 70\left(g^{(3)}(0)^2\, f^{(3)}(0) - f^{(3)}(0)^2\, g^{(3)}(0)\right)$$

Autrement écrit :

$$H(x) = \frac{\beta}{6!}x^7 + o(x^7)$$

$$\text{avec } \beta = 2\left(g^{(3)}(0)f^{(5)}(0) - f^{(3)}(0)g^{(5)}(0)\right) + 10\left(g^{(3)}(0)^2\, f^{(3)}(0) - f^{(3)}(0)^2\, g^{(3)}(0)\right)$$

**9.** En déduire que :

$$\lim_{x\longrightarrow 0} \frac{\arctan\left(\sin(x)\right) - \sin\left(\arctan(x)\right)}{x^7} = -\frac{1}{30}$$

Posons $f = \arctan$ et $g = \sin$. Avec les notations précédemment utilisées dans l'exercice, on a :

$$\text{au voisinage de 0,} \qquad H(x) = \arctan\left(\sin(x)\right) - \sin\left(\arctan(x)\right)$$

En outre, les fonctions $f = \arctan$ et $g = \sin$ vérifient les hypothèses faites dans les questions précédentes, et le DL à l'ordre 7 en 0 de la fonction H est donc donné par la question 8.

Pour obtenir explicitement ce DL, il suffit de calculer les différentes valeurs des dérivées intervenant dans la formule de la question 8.

Puisque : $f(x) = \arctan(x) = x - \dfrac{x^3}{3} + \dfrac{x^5}{5} + o(x^5)$ on a : $f^{(3)}(0) = -2$ et $f^{(5)}(0) = 24$.

Puisque : $g(x) = \sin(x) = x - \dfrac{x^3}{6} + \dfrac{x^5}{120} + o(x^5)$ on a : $g^{(3)}(0) = -1$ et $g^{(5)}(0) = 1$.

On en déduit, avec la question 8 que :

$$\beta = 2\left(-24+2\right) + 10\left(-2+4\right) = -24$$

Ainsi : $H(x) = \dfrac{-24}{6!}\,x^7 + o(x^7)$. D'où : $H(x) = -\dfrac{1}{30}\,x^7 + o(x^7)$.

Ce qui prouve le joli résultat :

$$\left[\arctan\left(\sin(x)\right) - \sin\left(\arctan(x)\right)\right] \sim_0 \; -\frac{1}{30}\,x^7$$

**Conclusion**. $\displaystyle\lim_{x\longrightarrow 0} \frac{\arctan\left(\sin(x)\right) - \sin\left(\arctan(x)\right)}{x^7} = -\frac{1}{30}$

## Exercice 2 — (Arithmétique et probabilités).

**Notations et rappels de terminologie**. On appelle espace probabilisé $(\Omega, P)$ la donnée d'un ensemble $\Omega$ (appelé univers) et d'une probabilité $P$ sur $\mathscr{P}(\Omega)$. Les éléments de $\Omega$ sont appelés issues, et les parties de $\Omega$ évènements.

Un évènement $A$ étant donné, on note $\Omega \backslash A$ (plutôt que $\overline{A}$) l'évènement contraire de $A$.

Deux évènements $A$ et $B$ sont dits indépendants lorsque : $P(A \cap B) = P(A) \times P(B)$. Cette définition admet la généralisation suivante.

Définition. Soit $n$ un entier $\geqslant 2$, et soit $A_1, \ldots, A_n$ une famille de $n$ évènements.
Les évènements $A_1, \ldots, A_n$ sont **mutuellement indépendants** si pour tout entier $j$ compris entre 2 et $n$, et pour toute famille d'indices deux à deux distincts $i_1, \ldots, i_j$ dans $[\![ 1, n ]\!]$ on a :

$$P\left(\bigcap_{k=1}^{j} A_{i_k}\right) = \prod_{k=1}^{j} P\left(A_{i_k}\right)$$

## Partie I — Indicatrice d'Euler

Pour tout entier $n \geqslant 2$, on note $\phi(n)$ le nombre d'entiers naturels inférieurs à $n$ qui sont premiers avec $n$. On définit ainsi une application $\phi : \mathbb{N} \backslash \{0, 1\} \longrightarrow \mathbb{N}^*$, appelée **indicatrice d'Euler**.

Par exemple : $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$.

On notera $\mathscr{P}$ l'ensemble des nombres premiers.

**1.** En justifiant brièvement vos réponses, donner les valeurs de $\phi(5)$, $\phi(9)$ et $\phi(12)$. [*]

On a $\boxed{\phi(5) = 4}$ car les entiers 1, 2, 3, et 4 sont premiers avec 5 ; $\boxed{\phi(9) = 6}$ car les entiers 1, 2, 4, 5, 7 et 8 sont premiers avec 9 ; et $\boxed{\phi(15) = 8}$ car les entiers 1, 2, 4, 7, 8, 11, 13 et 14 sont premiers avec 15.

**2.** Soit $p \in \mathscr{P}$.

**a.** Etablir que $\phi(p) = p - 1$.

Puisque $p$ est premier, $p$ est premier avec tout entier qu'il ne divise pas. Puisque par ailleurs $p$ ne divise aucun entier compris entre 1 et $p - 1$ (mais qu'il divise 0 et $p$), on en déduit que : $\boxed{\phi(p) = p - 1}$.

**b.** Soit $\alpha \in \mathbb{N}^*$. Soit $n$ un entier naturel. Montrer que : $[n \wedge p = 1] \Longleftrightarrow [n \wedge p^\alpha = 1]$.

Si $n \wedge p^\alpha = 1$, il existe d'après le théorème de Bezout deux entiers $m$ et $q$ tels que : $nm + qp^\alpha = 1$. On a donc : $nm + \underbrace{\left(qp^{\alpha-1}\right)}_{\in \mathbb{Z}} p = 1$, ce qui implique : $n \wedge p = 1$.

[*]. Après calculs et justifications, vous pourrez vérifier la justesse de vos résultats en constatant que $\phi(12) = \phi(3) \times \phi(4)$, et que $\phi(9) \neq \phi(3) \times \phi(3)$.

Réciproquement, supposons que $n \wedge p = 1$. On peut observer que les diviseurs dans $\mathbb{N}$ de $p^\alpha$ sont exactement les entiers $p^\beta$, avec $\beta \in [\![ 0, \alpha ]\!]$. Si $n$ n'était pas premier avec $p^\alpha$, il existerait un entier non nul $\beta$ tel que $p^\beta$ divise $n$. En particulier, $\beta$ étant non nul, $p$ diviserait $n$, ce qui est en contradiction avec $n \wedge p = 1$. D'où : $n \wedge p^\alpha = 1$, ce qui prouve l'implication réciproque.

Finalement : $\boxed{[n \wedge p = 1] \iff [n \wedge p^\alpha = 1]}$.

**c.** En déduire que pour tout $\alpha \in \mathbb{N}^*$, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Soit $n$ un entier naturel inférieur (ou égal) à $p^\alpha$. D'après ce qui précède, il est équivalent de dire que $n$ et $p^\alpha$ ne sont pas premiers entre eux, ou que $n$ et $p$ ne sont pas premiers entre eux ; ce qui revient à dire que $p$ divise $n$. Les entiers compris entre 0 et $p^\alpha$ non premiers avec $p^\alpha$ (et $\leqslant p^\alpha$) sont donc les multiples de $p^\alpha$ : il en existe exactement $p^{\alpha-1}+1$ entre 0 et $p^\alpha$. Comme par ailleurs il existe exactement $p^\alpha + 1$ entiers entre 0 et $p^\alpha$, on en déduit que le nombre d'entiers naturels inférieurs à $p^\alpha$ premiers avec $p^\alpha$ sont au nombre de $p^\alpha + 1 - (p^{\alpha-1}+1)$, càd : $p^\alpha - p^{\alpha-1}$.

$\boxed{\textbf{Conclusion} : \forall p \in \mathscr{P},\ \phi(p^\alpha) = p^\alpha - p^{\alpha-1}}$.

## Partie II — Probabilités

Soit $(\Omega, P)$ un espace probabilisé.

**3.** Soient $A$ et $B$ deux évènements (deux parties de $\Omega$).

**a.** Etablir que : $A \cap (\Omega \backslash B) = A \backslash (A \cap B)$.

Soit $x \in A \cap (\Omega \backslash B)$. Alors $x \in A$ et $x \notin B$. Donc : $x \in A$ et $x \notin A \cap B$. D'où : $x \in A \backslash (A \cap B)$. Ce qui prouve l'inclusion : $\boxed{A \cap (\Omega \backslash B) \subset A \backslash (A \cap B)\ \ (\spadesuit)}$.

Réciproquement, soit $x \in A \backslash (A \cap B)$. Alors $x \in A$ et $x \notin B$. Donc $x \in A$ et $x \in \Omega \backslash B$. Donc : $x \in A \cap (\Omega \backslash B)$. D'où : $\boxed{A \backslash (A \cap B) \subset A \cap (\Omega \backslash B)\ \ (\clubsuit)}$.

D'après $(\spadesuit)$, $(\clubsuit)$ et la règle de double inclusion : $\boxed{A \backslash (A \cap B) = A \cap (\Omega \backslash B)}$

**b.** Etablir que $A$ et $B$ sont indépendants si et seulement si $A$ et $\Omega \backslash B$ sont indépendants.

Supposons $A$ et $B$ indépendants. Alors :

$$P(A \cap (\Omega \backslash B)) = P(A \backslash (A \cap B)) = P(A) - P(A \cap B) = P(A) - P(A)P(B) = P(A)(1 - P(B)).$$

D'autre part : $P(A)P(\Omega \backslash B) = P(A)(1 - P(B))$.

Donc : $P(A \cap (\Omega \backslash B)) = P(A)P(\Omega \backslash B)$. Ce qui signifie que les évènements $A$ et $\Omega \backslash B$ sont indépendants.

Ainsi : $\boxed{[A \text{ et } B \text{ indépendants}] \Longrightarrow [A \text{ et } \Omega \backslash B \text{ indépendants}]\ (\spadesuit)}$.

Réciproquement, supposons $A$ et $\Omega \backslash B$ indépendants. Alors d'après l'implication précédente, les évènements $A$ et $\Omega \backslash (\Omega \backslash B)$ sont indépendants. Puisque $\Omega \backslash (\Omega \backslash B) = B$, on en déduit que $A$ et $B$ sont indépendants. Ce qui prouve : $\boxed{[A \text{ et } \Omega \backslash B \text{ indépendants}] \Longrightarrow [A \text{ et } B \text{ indépendants}]\ (\clubsuit)}$.

$\boxed{\textbf{Conclusion}.\ [A \text{ et } B \text{ indépendants}] \iff [A \text{ et } \Omega \backslash B \text{ indépendants}]}$.

**c.** En déduire que $A$ et $B$ sont indépendants si et seulement si $\Omega\backslash A$ et $\Omega\backslash B$ sont indépendants.

D'après la question précédente, les évènements $A$ et $B$ sont indépendants SSI les évènements $A$ et $\Omega\backslash B$ sont indépendants.

D'après cette même question, les évènements $A$ et $\Omega\backslash B$ sont indépendants SSI les évènements $\Omega\backslash A$ et $\Omega\backslash B$ sont indépendants. †

On en déduit que : $\boxed{[A \text{ et } B \text{ indépendants}] \Longleftrightarrow [\Omega\backslash A \text{ et } \Omega\backslash B \text{ indépendants}]}$.

**4.** Soit $(A_i)_{i\in[\![1,n]\!]}$ une famille de $n$ évènements (avec $n \in \mathbb{N}$, $n \geqslant 2$) mutuellement indépendants.

**a.** Etablir que les évènements $\Omega\backslash A_1,\ A_2,\dots,\ A_n$ sont mutuellement indépendants.

Notons $A'_1 = \Omega\backslash A_1$, et pour tout entier $i \in [\![\, 2, n \,]\!]$, $A'_i = A_i$.

Soit $J$ une partie non vide de $[\![\, 1, n \,]\!]$ ($J$ est une famille d'indices).

Si $1 \notin J$, alors : $P\left(\bigcap\limits_{j\in J} A'_j\right) = P\left(\bigcap\limits_{j\in J} A_j\right) = \prod\limits_{j\in J} P(A_j)$ ; la première égalité provenant de la définition des $A'_j$, la seconde de l'hypothèse suivant laquelle la famille $(A_i)_{i\in[\![1,n]\!]}$ est constituée d'évènements mutuellement indépendants.

Si $1 \in J$ (et si card$(J) \geqslant 2\dots$), on a :

$$\bigcap_{j\in J} A'_j = A'_1 \cap \left(\bigcap_{j\in J\backslash\{1\}} A'_j\right) = (\Omega\backslash A_1) \cap \left(\bigcap_{j\in J\backslash\{1\}} A_j\right) = \left(\bigcap_{j\in J\backslash\{1\}} A_j\right) \backslash \left(\left(\bigcap_{j\in J\backslash\{1\}} A_j\right) \cap A_1\right)$$

D'où : $\bigcap\limits_{j\in J} A'_j = \left(\bigcap\limits_{j\in J\backslash\{1\}} A_j\right) \backslash \left(\bigcap\limits_{j\in J} A_j\right)$.

On en déduit que :

$$P\left(\bigcap_{j\in J} A'_j\right) = P\left(\bigcap_{j\in J\backslash\{1\}} A_j\right) - P\left(\bigcap_{j\in J} A_j\right) = \prod_{j\in J\backslash\{1\}} P(A_j) - \prod_{j\in J} P(A_j)$$

$$= \prod_{j\in J\backslash\{1\}} P(A_j) - P(A_1) \prod_{j\in J\backslash\{1\}} P(A_j) = (1 - P(A_1)) \prod_{j\in J\backslash\{1\}} P(A_j) = \prod_{j\in J} P(A'_j)$$

Dans les deux cas, on a établi que : $P\left(\bigcap\limits_{j\in J} A'_j\right) = \prod\limits_{j\in J} P(A_j)$. Puisque cette égalité tient pour tout famille $J$ de $[\![\, 1, n \,]\!]$, on peut conclure que :

$\boxed{\text{les évènements } \Omega\backslash A_1,\ A_2,\dots,\ A_n \text{ sont mutuellement indépendants.}}$

†. Pour s'en convaincre, faire jouer dans la propriété précédente le rôle de $A$ à $\Omega\backslash B$ et le rôle de $B$ à $A$.

**b.** En déduire que les évènements $\Omega \backslash A_1, \Omega \backslash A_2, \ldots, \Omega \backslash A_n$ sont mutuellement indépendants.

Supposons les évènements $A_1$, $A_2, \ldots$, $A_n$ mutuellement indépendants.

D'après la question précédente, les évènements $\Omega \backslash A_1$, $A_2, \ldots$, $A_n$ sont mutuellement indépendants.

Donc les évènements $A_2, \ldots$, $A_n$, $\Omega \backslash A_1$ sont mutuellement indépendants.

D'après la question précédente, les évènements $\Omega \backslash A_2$, $A_3, \ldots$, $A_n$, $\Omega \backslash A_1$ sont mutuellement indépendants.

Donc les évènements $A_3, \ldots$, $A_n$, $\Omega \backslash A_1$, $\Omega \backslash A_2$ sont mutuellement indépendants.

Etc... Au final, les évènements $\boxed{\Omega \backslash A_1, \ldots, \Omega \backslash A_n \text{ sont mutuellement indépendants.}}$

## Partie III — Indicatrice d'Euler et probabilités

Soit $n \geqslant 2$ un entier naturel. On choisit de manière équiprobable un entier compris entre 1 et $n$.
Soient $p$ un diviseur positif de $n$, et $A_p$ l'évènement : "l'entier choisi est divisible par $p$".

**5.** Calculer $P(A_p)$.

Soit $p$ un diviseur de $n$. Il existe un entier $q$ tel que $n = pq$. Les multiples de $p$ compris entre 1 et $n$ sont : $p$, $2p, \ldots$, $qp$. Il existe donc exactement $q$ entiers compris entre 1 et $n$ qui sont divisibles par $p$. On en déduit que la probabilité qu'un entier choisi au hasard entre 1 et $n$ soit multiple de $p$ est : $q/n = 1/p$.

$\boxed{\textbf{Conclusion}.\ P(A_p) = \dfrac{1}{p}}$.

**6.** On note $p_1, \ldots$, $p_r$ les diviseurs premiers de $n$.

**a.** Soit $m$ un entier naturel. Etablir que $[\forall i \in [\![ 1, r ]\!],\ p_i | m\ ] \Longleftrightarrow \left[ \left( \prod_{i=1}^{r} p_i \right) | m \ \right]$

Soit $m$ un entier naturel (non nul, sinon il n'y a pas grand chose à prouver).

Supposons que $\forall i \in [\![ 1, r ]\!],\ p_i | m$. Alors : $\forall i \in [\![ 1, r ]\!],\ v_{p_i}(m) > 0$. La décomposition en facteurs premiers de $m$ peut donc s'écrire :

$$m = \prod_{i=1}^{r} p_i^{v_{p_i}(m)} \times \prod_{p \in \mathscr{P} \backslash \{p_1, \ldots, p_r\}} p^{v_p(m)} = \prod_{i=1}^{r} p_i \times \underbrace{\left( \prod_{i=1}^{r} p_i^{v_{p_i}(m)-1} \times \prod_{p \in \mathscr{P} \backslash \{p_1, \ldots, p_r\}} p^{v_p(m)} \right)}_{\in \mathbb{N}}$$

On déduit de cette écriture que : $\prod_{i=1}^{r} p_i \, | m$. Par suite : $[\forall i \in [\![ 1, r ]\!],\ p_i | m] \Longrightarrow \left[ \prod_{i=1}^{r} p_i \, | m \right]$.

La réciproque est triviale, et on peut conclure : $\boxed{[\forall i \in [\![ 1, r ]\!],\ p_i | m] \Longleftrightarrow \left[ \prod_{i=1}^{r} p_i \, | m \right]}$.

**b.** Etablir que les évènements $A_{p_1}, \ldots, A_{p_r}$ sont mutuellement indépendants.

Supposons $r \geqslant 2$ (sinon il n'y a pas grand chose à faire), et soit $J$ une partie de $[\![ 1, r ]\!]$ de cardinal $c$ supérieur ou égal à 2 (sinon…).

Quitte à renuméroter les $p_i$, on peut supposer que $J = \{1, 2, \ldots, c\}$. D'après la question précédente on a : $\bigcap_{i=1}^{c} A_{p_i} = A_{\prod_{i=1}^{c} p_i}$. D'où : $P\left(\bigcap_{i=1}^{c} A_{p_i}\right) = P\left(A_{\prod_{i=1}^{c} p_i}\right) = \dfrac{1}{\prod_{i=1}^{c} p_i} = \prod_{i=1}^{c} \dfrac{1}{p_i} = \prod_{i=1}^{c} P\left(A_{p_i}\right)$

$\boxed{\textbf{Conclusion}\text{. Les évènements } A_{p_1}, \ldots, A_{p_r} \text{ sont mutuellement indépendants.}}$

**7.** On note désormais $A$ l'évènement "l'entier choisi est premier avec $n$".

Calculer $P(A)$, et en déduire que : $\varphi(n) = n \prod_{i=1}^{r} \left(1 - \dfrac{1}{p_i}\right)$

Soit $m$ un entier compris entre 1 et $n$. L'entier $m$ est premier avec $n$ si et seulement si il est premier avec tout diviseur premier $p_i$ de $n$. Puisque les $p_i$ sont premiers(!), il revient au même de dire qu'aucun des $p_i$ ne divise $n$. De ce raisonnement on déduit que : $A = \bigcap_{i=1}^{r} (\Omega \backslash A_{p_i})$.

Or, puisque les évènements $A_{p_i}$ sont mutuellement indépendants (d'après 4-b), les évènements $\Omega \backslash A_{p_i}$ le sont également (d'après 2-b). Il s'ensuit que :

$$P(A) = P\left(\bigcap_{i=1}^{r} (\Omega \backslash A_{p_i})\right) = \prod_{i=1}^{r} P\left(\Omega \backslash A_{p_i}\right) = \prod_{i=1}^{r} \left(1 - P\left(A_{p_i}\right)\right)$$

D'où finalement : $\boxed{P(A) = \prod_{i=1}^{r} \left(1 - \dfrac{1}{p_i}\right) \quad (\spadesuit)}$

Par ailleurs, et par définition de l'indicateur d'Euler : $\boxed{P(A) = \dfrac{\varphi(n)}{n} \quad (\clubsuit)}$

On déduit alors de ($\spadesuit$) et de ($\clubsuit$) que : $\boxed{\varphi(n) = n \prod_{i=1}^{r} \left(1 - \dfrac{1}{p_i}\right)}$.

**8.** Dans cette ultime question, $n$ et $m$ désignent deux entiers $\geqslant 2$.

Etablir que : $[n \wedge m = 1] \Longrightarrow [\varphi(nm) = \varphi(n)\varphi(m)]$

Soient $n$ et $m$ deux entiers strictement plus grands que 1. Supposons que $n$ et $m$ sont premiers entre eux. Alors aucun facteur premier intervenant dans la décomposition de $n$ n'intervient dans celle de $m$, et réciproquement. En d'autres termes il existe $(r + s)$ nombres premiers $p_1, \ldots, p_r$, $q_1, \ldots, q_s$ et (r+s) entiers naturels non nuls $\alpha_1, \ldots, \alpha_r$, $\beta_1, \ldots, \beta_s$ tels que :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} \quad \text{et} \quad m = \prod_{j=1}^{s} q_j^{\beta_j}$$

Puisque les $p_i$ et les $q_j$ sont des nombres premiers deux à deux distincts, la décomposition en facteurs premiers de $nm$ est : $nm = \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} q_j^{\beta_j}$.

On déduit alors de la question précédente que :

$$\varphi(nm) = nm \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right) = \left(n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)\right) \left(m \prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right)\right) = \varphi(n)\varphi(m)$$

$\boxed{\textbf{Conclusion}.\ \forall\ (n,m) \in\ (\mathbb{N}\backslash\{0,1\})^2,\ [n \wedge m = 1] \Longrightarrow [\varphi(nm) = \varphi(n)\varphi(m)]}$.