

Exercice 1 (Centrale 2023)

1. Rappeler la définition de la fonction indicatrice d'Euler puis, pour n entier non nul, exprimer $\varphi(n)$ en fonction de sa décomposition en facteurs premiers.
2. Pour n entier non nul, calculer $\sum_{d|n} \varphi(d)$.
3. En déduire le déterminant de $C = (i \wedge j)_{1 \leq i, j \leq n}$ avec n entier non nul.

Corrigé : 1. On définit

$$\forall n \in \mathbb{N}^* \quad \varphi(n) = \text{Card} \{k \in \llbracket 1; n \rrbracket \mid k \wedge n = 1\}$$

Pour $n \geq 2$, on note $n = \prod_{i=1}^r p_i^{\alpha_i}$ sa décomposition en facteurs premiers avec les p_i premiers deux à deux distincts et les α_i entiers non nuls. D'après le théorème chinois et le comptage des diviseurs d'une puissance d'un nombre premier, il vient

$$\varphi \left(\prod_{i=1}^r p_i^{\alpha_i} \right) = \prod_{i=1}^r \varphi(p_i^{\alpha_i}) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1})$$

D'où

$$\boxed{\varphi \left(\prod_{i=1}^r p_i^{\alpha_i} \right) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i} \right)}$$

2. On a

$$\llbracket 1; n \rrbracket = \bigsqcup_{d|n} \{k \in \llbracket 1; n \rrbracket \mid k \wedge n = d\}$$

Par ailleurs, pour $d|n$, on a

$$k \wedge n = d \iff \exists!(k', n') \in \mathbb{Z}^2 \mid k = k'd \quad n = n'd \quad \text{et} \quad k' \wedge n' = 1$$

Comme n est entier non nul, alors $n' = \frac{n}{d}$ l'est également. Ainsi, on peut mettre en bijection $k \in \llbracket 1; n \rrbracket$ vérifiant $k \wedge n = d$ avec $k' \in \llbracket 1; n' \rrbracket$ vérifiant $k' \wedge n' = 1$. Il s'ensuit

$$\text{Card} \{k \in \llbracket 1; n \rrbracket \mid k \wedge n = d\} = \text{Card} \{k' \in \llbracket 1; n' \rrbracket \mid k' \wedge n' = 1\} = \varphi(n')$$

Comme il s'agit d'union disjointe, on obtient

$$\text{Card} \llbracket 1; n \rrbracket = \sum_{d|n} \varphi \left(\frac{n}{d} \right)$$

et comme l'application $d \mapsto \frac{n}{d}$ réalise une permutation de l'ensemble des diviseurs de n (involutive), on conclut

$$\boxed{\forall n \in \mathbb{N}^* \quad \sum_{d|n} \varphi(d) = n}$$

3. Soit $(i, j) \in \llbracket 1; n \rrbracket$. On rappelle que pour d entier, on a

$$d|i \wedge j \iff d|i \quad \text{et} \quad d|j$$

D'après la relation précédemment établie, il vient

$$i \wedge j = \sum_{d|i \wedge j} \varphi(d) = \sum_{d|i, d|j} \varphi(d) = \sum_{k=1}^n \varphi(k) \mathbf{1}_{\mathcal{D}_i}(k) \mathbf{1}_{\mathcal{D}_j}(k) = \sum_{k=1}^n a_{i,k} b_{k,j}$$

avec

$$a_{i,k} = \varphi(k) \mathbf{1}_{\mathcal{D}_i}(k) \quad \text{et} \quad b_{k,j} = \mathbf{1}_{\mathcal{D}_j}(k)$$

d'où

$$C = AB \quad \text{avec} \quad A = (a_{i,j})_{1 \leq i, j \leq n} \quad \text{et} \quad B = (b_{i,j})_{1 \leq i, j \leq n}$$

La matrice A est triangulaire inférieure et la matrice B est triangulaire supérieure. Ainsi, on obtient

$$\det C = (\det A)(\det B) = \left(\prod_{i=1}^n a_{i,i} \right) \left(\prod_{i=1}^n b_{i,i} \right)$$

Et on conclut

$$\boxed{\det C = \prod_{k=1}^n \varphi(k)}$$

Exercice 2 (Centrale 2022)

Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé et X une variable aléatoire réelle. Si A est un événement non négligeable, on définit sous réserve d'existence

$$\mathbb{E}(X|A) = \sum_{x \in X(\Omega)} x \mathbb{P}(X = x|A)$$

1. Montrer que si X est d'espérance finie, alors $\mathbb{E}(X|A)$ est bien définie.
2. Si X suit la loi géométrique de paramètre $p \in]0; 1[$, calculer $\mathbb{E}(X|X > m)$ pour m entier.
3. Montrer que si $(A_k)_k$ est un système complet d'événements et si X est d'espérance finie, alors

$$\mathbb{E}(X) = \sum_{k=0}^{+\infty} \mathbb{E}(X|A_k) \mathbb{P}(A_k)$$

Corrigé : 1. On a

$$\forall x \in X(\Omega) \quad |x| \mathbb{P}(X = x|A) = \frac{|x| \mathbb{P}(\{X = x\} \cap A)}{\mathbb{P}(A)} \leq \frac{|x| \mathbb{P}(X = x)}{\mathbb{P}(A)}$$

La famille $(x \mathbb{P}(X = x))_{x \in X(\Omega)}$ est sommable et par comparaison, la famille $(x \mathbb{P}(X = x|A))_{x \in X(\Omega)}$ l'est aussi et on conclut

Si X est d'espérance finie, alors $\mathbb{E}(X|A)$ est bien définie.

2. Soit $X \sim \mathcal{G}(p)$ et m entier. On a

$$\mathbb{P}(X > m) = \sum_{k=m+1}^{+\infty} p(1-p)^{k-1} = (1-p)^m$$

puis

$$\begin{aligned} \mathbb{E}(X|X > m) &= \sum_{k=1}^{+\infty} k \mathbb{P}(X = k|X > m) \\ &= \sum_{k=m+1}^{+\infty} k \frac{\mathbb{P}(\{X = k\} \cap \{X > m\})}{\mathbb{P}(X > m)} = \frac{1}{\mathbb{P}(X > m)} \sum_{k=m+1}^{+\infty} k \mathbb{P}(X = k) \end{aligned}$$

d'où

$$\mathbb{E}(X|X > m) = \frac{1}{(1-p)^m} \sum_{k=m+1}^{+\infty} kp(1-p)^{k-1}$$

Pour $x \in]-1; 1[$, on a par dérivation de séries entières

$$\sum_{k=1}^{+\infty} kx^{k-1} = \frac{d}{dx} \left[\frac{1}{1-x} \right] = \frac{1}{(1-x)^2}$$

puis

$$\begin{aligned} \sum_{k=1}^n kx^{k-1} &= \frac{d}{dx} \left[\sum_{k=0}^n x^k \right] \\ &= \frac{d}{dx} \left[\frac{1-x^{n+1}}{1-x} \right] = \frac{1}{(1-x)^2} [-(n+1)x^n(1-x) + 1-x^{n+1}] \end{aligned}$$

d'où

$$\sum_{k=m+1}^{+\infty} kx^{k-1} = \sum_{k=1}^{+\infty} kx^{k-1} - \sum_{k=1}^m kx^{k-1} = \frac{x^m}{(1-x)^2} [(m+1)(1-x) + x]$$

Ainsi

$$\mathbb{E}(X|X > m) = \frac{1}{(1-p)^m} \frac{p(1-p)^m}{p^2} (mp+1)$$

On conclut

$$\forall m \in \mathbb{N} \quad \mathbb{E}(X|X > m) = \frac{mp+1}{p}$$

3. On considère l'utilisation étendue de la notation *probabilité conditionnelle* qui assure un sens, pour $(A, B) \in \mathcal{A}^2$ à $\mathbb{P}(B|A)\mathbb{P}(A) = \mathbb{P}(A \cap B)$ même si l'événement A est négligeable. Considérons la famille $(x\mathbb{P}(\{X = x\} \cap A_k))_{(x,k) \in X(\Omega) \times \mathbb{N}}$. Pour $x \in X(\Omega)$, on a par σ -additivité

$$\sum_{k=0}^{+\infty} x\mathbb{P}(\{X = x\} \cap A_k) = x \sum_{k=0}^{+\infty} \mathbb{P}(\{X = x\} \cap A_k) = x\mathbb{P}(X = x)$$

et $(x\mathbb{P}(X = x))_{x \in X(\Omega)}$ est sommable puisque la variable X est d'espérance finie. Par interversion de l'ordre de sommation, il vient

$$\begin{aligned} \mathbb{E}(X) &= \sum_{x \in X(\Omega)} x\mathbb{P}(X = x) = \sum_{x \in X(\Omega)} \sum_{k=0}^{+\infty} x\mathbb{P}(\{X = x\} \cap A_k) \\ &= \sum_{k=0}^{+\infty} \sum_{x \in X(\Omega)} x\mathbb{P}(\{X = x\} \cap A_k) = \sum_{k=0}^{+\infty} \sum_{x \in X(\Omega)} x\mathbb{P}(X = x|A_k)\mathbb{P}(A_k) \end{aligned}$$

Ainsi

$$\boxed{\mathbb{E}(X) = \sum_{k=0}^{+\infty} \mathbb{E}(X|A_k)\mathbb{P}(A_k)}$$

Remarque : Il s'agit de la *formule de l'espérance totale*.

Exercice 3 (Centrale 2023)

Soit E euclidien et $f \in \mathcal{L}(E)$.

1. Rappeler les identités de polarisation et l'identité du parallélogramme.
2. Montrer que les conditions suivantes sont équivalentes :
 - (a) $\exists c \in \mathbb{R} \mid \forall (x, y) \in E^2 \quad \langle f(x), f(y) \rangle = c \langle x, y \rangle$;
 - (b) $\forall (x, y) \in E^2 \quad \langle x, y \rangle = 0 \implies \langle f(x), f(y) \rangle = 0$.
3. Trouver les $u \in \mathcal{L}(E)$ tels que $u(F^\perp) \subset u(F)^\perp$ pour tout F sev de E .

Corrigé : 1. On a pour les identité de polarisation

$$\begin{aligned} \forall (x, y) \in E^2 \quad \langle x, y \rangle &= \frac{1}{2} (\|x + y\|^2 - \|x\|^2 - \|y\|^2) \\ &= \frac{1}{2} (\|x\|^2 + \|y\|^2 - \|x - y\|^2) = \frac{1}{4} (\|x + y\|^2 - \|x - y\|^2) \end{aligned}$$

et pour l'identité du parallélogramme

$$\forall (x, y) \in E^2 \quad \|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2)$$

2. L'implication (a) \implies (b) est évidente. On suppose l'assertion (b) vraie. Soient u, v vecteurs unitaires de E . On a

$$\langle u + v, u - v \rangle = \|u\|^2 - \|v\|^2 = 0$$

Soit v vecteur unitaire de E . Pour $x \in E \setminus \{0_E\}$, posant $u = \frac{x}{\|x\|}$, on a d'après le résultat de la question précédente

$$\langle u + v, u - v \rangle = 0$$

Par hypothèse sur f , il s'ensuit $\langle f(u + v), f(u - v) \rangle = 0$

et on a $\langle f(u + v), f(u - v) \rangle = \langle f(u) + f(v), f(u) - f(v) \rangle = \|f(u)\|^2 - \|f(v)\|^2$

d'où $\forall x \in E \setminus \{0_E\} \quad \|f\left(\frac{x}{\|x\|}\right)\| = \|f(v)\|$

Ainsi $\forall x \in E \quad \|f(x)\| = \|f(v)\| \|x\|$

l'égalité étant trivialement vérifiée pour $x = 0_E$. Notant $c = \|f(v)\|^2$, on obtient

$$\forall x \in E \quad \|f(x)\| = \sqrt{c} \|x\|$$

et par polarisation, on en déduit l'assertion (a). On conclut

Les assertions (a) et (b) sont équivalentes.

3. Soit $u \in \mathcal{L}(E)$ tel que $u(F^\perp) \subset F^\perp$ pour tout F sev de E . Ainsi, pour tout $a \in E$, on a $u(\text{Vect}(a)^\perp) \subset u(\text{Vect}(a))^\perp$ ce qui signifie, en observant $u(\text{Vect}(a)) = \text{Vect}(u(a))$

$$\forall x \in E \quad \langle x, a \rangle = 0 \implies \langle u(x), u(a) \rangle = 0$$

et ceci vaut pour tout $a \in E$. On en déduit que l'endomorphisme u conserve l'orthogonalité. Réciproquement, on suppose que l'endomorphisme u conserve l'orthogonalité ou, de manière équivalente, qu'il existe c réel tel que

$$\forall (x, y) \in E^2 \quad \langle u(x), u(y) \rangle = c \langle x, y \rangle$$

Soit F sev de E et $x \in F^\perp$. Alors, il vient

$$\forall y \in F \quad \langle u(x), u(y) \rangle = c \langle x, y \rangle = 0$$

ce qui prouve $u(x) \in u(F)^\perp$ d'où $u(F^\perp) \subset F^\perp$. On conclut

Les endomorphismes solutions sont ceux conservant l'orthogonalité.
--

Exercice 4 (Mines 2022)

Pour n entier non nul, on note $\tau(n)$ le nombre de diviseurs de n , φ la fonction indicatrice d'Euler et ζ le fonction de Riemann.

1. Montrer $\forall \alpha > 1 \quad \sum_{n=1}^{+\infty} \frac{\tau(n)}{n^\alpha} = \zeta(\alpha)^2$

Que dire pour $\alpha \leq 1$?

2. Montrer $\forall \alpha > 2 \quad \sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^\alpha} = \frac{\zeta(\alpha-1)}{\zeta(\alpha)}$

Que dire pour $\alpha \leq 2$?

Corrigé : 1. Soit α réel. On opte pour le point de vue des familles sommables. Pour n entier non nul, on note D_n l'ensemble des diviseurs de n . On a dans $[0; +\infty]$

$$\sum_{n=1}^{+\infty} \frac{\tau(n)}{n^\alpha} = \sum_{n=1}^{+\infty} \left(\sum_{d \in D_n} \frac{1}{n^\alpha} \right)$$

On pose

$$\Lambda = \{(n, d) \in (\mathbb{N}^*)^2 : d|n\}$$

La famille $(\{n\} \times D_n)_{n \geq 1}$ est un recouvrement disjoint de Λ . Ainsi, d'après le théorème de sommation par paquets pour une famille à termes positifs, on trouve

$$\sum_{n=1}^{+\infty} \left(\sum_{d \in D_n} \frac{1}{n^\alpha} \right) = \sum_{(n,d) \in \Lambda} \frac{1}{n^\alpha}$$

On pose

$$\forall k \in \mathbb{N}^* \quad I_k = \{(n, d) \in (\mathbb{N}^*)^2 \mid n = dk\}$$

La famille $(I_k)_{k \geq 1}$ est un recouvrement disjoint de Λ et par sommation par paquets de familles à termes positifs, il vient

$$\sum_{(n,d) \in \Lambda} \frac{1}{n^\alpha} = \sum_{k=1}^{+\infty} \left(\sum_{(n,d) \in I_k} \frac{1}{n^\alpha} \right)$$

On remarque

$$\forall k \in \mathbb{N}^* \quad I_k = \{(dk, d), d \in \mathbb{N}^*\}$$

On obtient

$$\sum_{(n,d) \in \Lambda} \frac{1}{n^\alpha} = \sum_{k=1}^{+\infty} \left(\sum_{d=1}^{+\infty} \frac{1}{(dk)^\alpha} \right) = \left(\sum_{k=1}^{+\infty} \frac{1}{k^\alpha} \right) \left(\sum_{d=1}^{+\infty} \frac{1}{d^\alpha} \right) = \left(\sum_{k=1}^{+\infty} \frac{1}{k^\alpha} \right)^2$$

autrement dit

$$\sum_{n=1}^{+\infty} \frac{\tau(n)}{n^\alpha} = \left(\sum_{n=1}^{+\infty} \frac{1}{n^\alpha} \right)^2$$

l'égalité ayant lieu dans $[0; +\infty]$ pour tout α réel. Enfin, on a par critère de Riemann

$$\sum_{k=1}^{+\infty} \frac{1}{k^\alpha} = +\infty \iff \alpha \leq 1$$

Et on conclut

$$\forall \alpha \in \mathbb{R} \quad \sum_{n=1}^{+\infty} \frac{\tau(n)}{n^\alpha} = \begin{cases} \zeta(\alpha)^2 & \text{si } \alpha > 1 \\ +\infty & \text{sinon} \end{cases}$$

2. Soit α réel. Dans $[0; +\infty]$, d'après le théorème de Fubini pour des familles à termes positifs, il vient

$$\left(\sum_{k=1}^{+\infty} \frac{1}{k^\alpha} \right) \left(\sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^\alpha} \right) = \sum_{(k,n) \in (\mathbb{N}^*)^2} \frac{\varphi(n)}{(kn)^\alpha}$$

On pose $\forall \ell \in \mathbb{N}^* \quad J_\ell = \{(k, n) \in (\mathbb{N}^*)^2 \mid kn = \ell\}$

La famille $(J_\ell)_{\ell \geq 1}$ est un recouvrement disjoint de $(\mathbb{N}^*)^2$ et par sommation par paquets de famille à termes positifs, il vient

$$\sum_{(k,n) \in (\mathbb{N}^*)^2} \frac{\varphi(n)}{(kn)^\alpha} = \sum_{\ell=1}^{+\infty} \left(\sum_{(k,n) \in J_\ell} \frac{\varphi(n)}{\ell^\alpha} \right) = \sum_{\ell=1}^{+\infty} \frac{1}{\ell^\alpha} \sum_{n|\ell} \varphi(n)$$

Puis, on observe pour ℓ entier non nul

$$\llbracket 1; \ell \rrbracket = \bigsqcup_{n|\ell} \{k \in \llbracket 1; \ell \rrbracket \mid k \wedge \ell = n\}$$

et pour n diviseur de ℓ et $k \in \llbracket 1; \ell \rrbracket$ tel que $k \wedge \ell = n$, il existe un unique $d \in \llbracket 1; \ell/n \rrbracket$ tel que $k = nd$ et $d \wedge \ell/n = 1$. Ainsi

$$\begin{aligned} \ell &= \sum_{n|\ell} \text{Card} \{k \in \llbracket 1; \ell \rrbracket \mid k \wedge \ell = n\} \\ &= \sum_{n|\ell} \text{Card} \{d \in \llbracket 1; \ell/n \rrbracket \mid d \wedge \ell/n = 1\} = \sum_{n|\ell} \varphi\left(\frac{\ell}{n}\right) = \sum_{n|\ell} \varphi(n) \end{aligned}$$

la dernière égalité résultant du fait que l'application $n \mapsto \frac{\ell}{n}$ réalise une permutation de l'ensemble des diviseurs de ℓ . Par conséquent

$$\left(\sum_{k=1}^{+\infty} \frac{1}{k^\alpha} \right) \left(\sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^\alpha} \right) = \sum_{\ell=1}^{+\infty} \frac{1}{\ell^{\alpha-1}}$$

Par critère de Riemann, il vient pour $\alpha > 2$

$$\zeta(\alpha) \sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^\alpha} = \zeta(\alpha - 1)$$

et pour $\alpha \in]1; 2]$

$$\zeta(\alpha) \sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^\alpha} = +\infty$$

Enfin, la minoration $\varphi(n) \geq 1$ pour n entier non nul prouve que $\sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^\alpha} = +\infty$ pour $\alpha \leq 1$ et on conclut

$$\forall \alpha \in \mathbb{R} \quad \sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^\alpha} = \begin{cases} \frac{\zeta(\alpha - 1)}{\zeta(\alpha)} & \text{si } \alpha > 2 \\ +\infty & \text{sinon} \end{cases}$$

Exercice 5 (Mines 2022)

Soit X une variable aléatoire réelle positive dans L^2 .

1. Rappeler pourquoi X est d'espérance finie.
2. Établir
$$\forall \lambda \geq 0 \quad X \leq \lambda \mathbb{E}(X) + X \mathbf{1}_{\{X \geq \lambda \mathbb{E}(X)\}}$$
3. On suppose $\mathbb{E}(X^2) > 0$. Montrer

$$\forall \lambda \in [0; 1] \quad \mathbb{P}(X \geq \lambda \mathbb{E}(X)) \geq (1 - \lambda)^2 \frac{\mathbb{E}(X)^2}{\mathbb{E}(X^2)}$$

Corrigé : 1. On a $|X| \leq \frac{1 + X^2}{2}$ et le résultat suit.

2. Soit $\lambda \geq 0$. On a

$$X = X \mathbf{1}_{\{X < \lambda \mathbb{E}(X)\}} + X \mathbf{1}_{\{X \geq \lambda \mathbb{E}(X)\}} \leq \lambda \mathbb{E}(X) \mathbf{1}_{\{X < \lambda \mathbb{E}(X)\}} + X \mathbf{1}_{\{X \geq \lambda \mathbb{E}(X)\}}$$

Par positivité de λ et X , il vient $\lambda \mathbb{E}(X) \mathbf{1}_{\{X < \lambda \mathbb{E}(X)\}} \leq \lambda \mathbb{E}(X)$

Et on conclut

$$\boxed{\forall \lambda \geq 0 \quad X \leq \lambda \mathbb{E}(X) + X \mathbf{1}_{\{X \geq \lambda \mathbb{E}(X)\}}}$$

3. Soit $\lambda \in [0; 1]$. Passant à l'espérance, il vient

$$(1 - \lambda) \mathbb{E}(X) \leq \mathbb{E}(X \mathbf{1}_{\{X \geq \lambda \mathbb{E}(X)\}})$$

D'après l'inégalité de Cauchy-Schwarz, on obtient

$$\mathbb{E}(X \mathbf{1}_{\{X \geq \lambda \mathbb{E}(X)\}})^2 \leq \mathbb{E}(X^2) \mathbb{E}(\mathbf{1}_{\{X \geq \lambda \mathbb{E}(X)\}}^2)$$

et

$$\mathbb{E}(\mathbf{1}_{\{X \geq \lambda \mathbb{E}(X)\}}^2) = \mathbb{E}(\mathbf{1}_{\{X \geq \lambda \mathbb{E}(X)\}}) = \mathbb{P}(X \geq \lambda \mathbb{E}(X))$$

On conclut

$$\boxed{\forall \lambda \in [0; 1] \quad \mathbb{P}(X \geq \lambda \mathbb{E}(X)) \geq (1 - \lambda)^2 \frac{\mathbb{E}(X)^2}{\mathbb{E}(X^2)}}$$

Remarque : Il s'agit de l'inégalité de *Paley-Zygmund*.

Exercice 6 (Navale 2019)

Soit la série entière $\sum \binom{2n}{n} x^{2n}$.

1. Déterminer son rayon de convergence. On notera $f(x)$ sa somme.
2. Montrer que f est solution d'une équation différentielle linéaire d'ordre 1.
3. En déduire une expression de $f(x)$.

Corrigé : 1. Notons $u_n = \binom{2n}{n} r^{2n}$ pour $r > 0$, on a

$$\left| \frac{u_{n+1}}{u_n} \right| = \frac{(2n+2)!}{(2n)!} \frac{(n!)^2}{(n+1)!^2} r^2 = \frac{2(2n+1)}{n+1} r^2 \xrightarrow{n \rightarrow +\infty} 4r^2$$

- Si $4r^2 > 1$ ce qui équivaut à $r > 1/2$, la série diverge grossièrement d'où $R \leq 1/2$.
- Si $4r^2 < 1$ ce qui équivaut à $r < 1/2$, la série converge absolument donc son terme général est borné et par suite $R \geq 1/2$.

Ainsi

$$\boxed{R = \frac{1}{2}}$$

2. Notons $I = \left] -\frac{1}{2}; \frac{1}{2} \right[$. Par dérivation d'une série entière, il vient

$$\begin{aligned} \forall x \in I \quad f'(x) &= \sum_{n=1}^{+\infty} 2n \binom{2n}{n} x^{2n-1} = \sum_{n=0}^{+\infty} 2(n+1) \binom{2(n+1)}{n+1} x^{2n+1} \\ &= \sum_{n=0}^{+\infty} 2(n+1) \frac{2(n+1)(2n+1)}{(n+1)^2} \binom{2n}{n} x^{2n+1} = 4 \sum_{n=0}^{+\infty} (2n+1) \binom{2n}{n} x^{2n+1} \end{aligned}$$

Supposant la linéarité *a priori*, il vient

$$\forall x \in I \quad f'(x) = 4x^2 \sum_{n=1}^{+\infty} 2n \binom{2n}{n} x^{2n-1} + 4xf(x) = 4x^2 f'(x) - 4xf(x)$$

Les séries définissant $f(x)$ et $f'(x)$ étant convergentes, ceci justifie la linéarité et on obtient

$$\boxed{\forall x \in I \quad (1 - 4x^2)f'(x) - 4xf(x) = 0}$$

3. La fonction f est solution du problème de Cauchy

$$\begin{cases} (1 - 4x^2)y' - 4xy = 0 \\ y(0) = 1 \end{cases}$$

L'ensemble des solutions de l'équation homogène est

$$S_H = \text{Vect}(\varphi) \quad \text{avec} \quad \forall x \in I \quad \varphi(x) = e^{A(x)} \quad \text{où} \quad A(x) = \int \frac{4x}{1-4x^2} dx = -\frac{1}{2} \ln |1-4x^2|$$

D'après l'unicité fournie par le théorème de Cauchy linéaire, on conclut

$$\boxed{\forall x \in I \quad f(x) = \frac{1}{\sqrt{1-4x^2}}}$$

Exercice 7 (Navale 2017)

Soit n entier avec $n \geq 2$ et φ l'indicatrice d'Euler.

1. Montrer qu'il y a $\varphi(d)$ éléments de $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre d un diviseur de n .

2. Établir
$$n = \sum_{d|n} \varphi(d)$$

3. En déduire un programme python permettant le calcul de $\varphi(n)$.

Corrigé : 1. Soit d diviseur de n . On a $n = cd$ avec c entier non nul puis

$$\langle \bar{c} \rangle = \{\bar{0}, \bar{c}, \dots, (d-1)\bar{c}\}$$

donc $\langle \bar{c} \rangle$ est de cardinal d . Montrons l'unicité de ce sous-groupe. Soit H sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d . Pour $\bar{x} \in H$ et $x \in \bar{x}$, on a $d\bar{x} = \bar{0}$ d'où $dx \equiv 0 [n]$, i.e. $dx = kn$ avec $k \in \mathbb{Z}$ puis $dx = kdc$ autrement dit $x = kc$ d'où $\bar{x} \in \langle \bar{c} \rangle$. Il s'ensuit que $H \subset \langle \bar{c} \rangle$ et par égalité des cardinaux, on conclut que $H = \langle \bar{c} \rangle$. Ainsi

Pour d diviseur de n , il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d .

Un élément d'ordre d engendre un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ à d éléments donc engendre $\langle \overline{n/d} \rangle$. Réciproquement, tout générateur de $\langle \overline{n/d} \rangle$ est d'ordre d . Comme $\langle \overline{n/d} \rangle$ est cyclique, il est isomorphe à $\mathbb{Z}/d\mathbb{Z}$ et possède donc $\varphi(d)$ générateurs. Ainsi

Il y a $\varphi(d)$ éléments de $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre d .

2. On a l'union disjointe $\llbracket 1; n \rrbracket = \bigsqcup_{d|n} \{k \in \llbracket 1; n \rrbracket, o(k) = d\}$. Passant au cardinal, on conclut

$$n = \sum_{d|n} \varphi(d)$$

3. On observe que $\varphi(n) = n - \sum_{d|n, d < n} \varphi(d)$. On implémente cette approche avec :

```
def phi(n):
    if n==1:
        return 1
    else:
        div=[ k for k in range(1,n) if n%k==0]
        return n-sum([phi(d) for d in div])
```

On peut économiser le cas de base car la liste `div` est vide si `n==1`. C'est plus court mais pas forcément plus lisible ...

```
def phi(n):
    div=[ k for k in range(1,n) if n%k==0]
    return n-sum([phi(d) for d in div])
```

Exercice 8 (Centrale 2021)

Pour x réel, on pose sous réserve de convergence

$$F(x) = \int_0^{+\infty} \frac{e^{-xt}}{1+t^2} dt \quad \text{et} \quad G(x) = \int_0^{+\infty} \frac{\sin(t)}{x+t} dt$$

et on considère l'équation différentielle sur $]0; +\infty[$

$$y'' + y = \frac{1}{x} \tag{E}$$

1. Déterminer les ensembles de définition de F et G .
2. Tracer la courbe de F .
3. Tracer la courbe de G en expliquant pourquoi la méthode naïve ne convient pas. Faire une conjecture concernant F et G .
4. Soit ϕ de classe \mathcal{C}^2 sur un intervalle I ouvert et $x_0 \in I$. À l'aide du développement limité de ϕ , exprimer $\phi''(x_0)$ comme limite d'une expression faisant intervenir $\phi(x_0+h)$ et $\phi(x_0-h)$.
5. En admettant que F soit de classe \mathcal{C}^2 , vérifier numériquement qu'elle satisfait l'équation (E).
6. Montrer que F et G sont continues sur $]0; +\infty[$.
7. Montrer que F et G sont de classe \mathcal{C}^2 sur $]0; +\infty[$.
8. Montrer que F et G sont solutions de (E) puis que $F = G$.
9. En déduire la valeur de l'intégrale $\int_0^{+\infty} \frac{\sin(t)}{t} dt$.

Corrigé : 1. On pose

$$\forall (x, t) \in \mathbb{R} \times [0; +\infty[\quad f(x, t) = \frac{e^{-xt}}{1+t^2} \quad g(x, t) = \frac{\sin(t)}{x+t}$$

Pour x réel, la fonction $t \mapsto f(x, t)$ est continue par morceaux sur $[0; +\infty[$. Pour $x < 0$, on a $1 \underset{t \rightarrow +\infty}{=} O(f(x, t))$ avec $t \mapsto 1$ d'intégrale divergente d'où $\int_0^{+\infty} f(x, t) dt$ également par comparaison de fonctions positives. Pour $x \geq 0$, on a

$$\forall t \geq 0 \quad 0 \leq f(x, t) \leq \frac{1}{1+t^2}$$

ce qui prouve l'intégrabilité de $t \mapsto f(x, t)$ sur \mathbb{R}_+ . Pour $x < 0$, la fonction $t \mapsto g(x, t)$ n'est pas continue par morceaux sur \mathbb{R}_+ . Pour $x \geq 0$, la fonction $t \mapsto g(x, t)$ est continue par morceaux sur \mathbb{R}_+ et une étude de convergence a donc du sens. On a $t \mapsto \frac{1}{x+t}$ et $t \mapsto 1 - \cos(t)$ de classe \mathcal{C}^1 avec

$$-\frac{1 - \cos(t)}{x+t} \xrightarrow{t \rightarrow 0} 0 \quad \text{et} \quad -\frac{1 - \cos(t)}{x+t} \xrightarrow{t \rightarrow +\infty} 0$$

Ainsi, les intégrales $\int_0^{+\infty} \frac{\sin(t)}{x+t} dt$ et $\int_0^{+\infty} \frac{1 - \cos(t)}{(x+t)^2} dt$

sont de même nature. La seconde converge puisque

$$\frac{1 - \cos(t)}{(x+t)^2} \underset{t \rightarrow 0}{=} O(1) \quad \text{et} \quad \frac{1 - \cos(t)}{(x+t)^2} \underset{t \rightarrow +\infty}{=} O\left(\frac{1}{t^2}\right)$$

On conclut

Les fonctions F et G sont définies sur \mathbb{R}_+ .

2. On saisit :

```
F=lambda x:integr.quad(lambda t:np.exp(-x*t)/(1+t**2),0,np.inf)[0]

tx=np.linspace(0,10,100)
tF=[F(x) for x in tx]
plt.plot(tx,tF)
plt.show()
```

On observe :

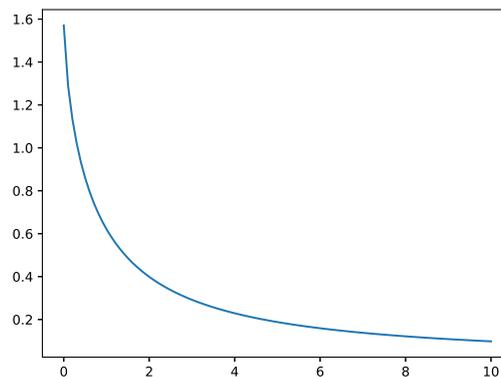


FIGURE 1 – Graphe de F

3. On saisit :

```
G=lambda x:integr.quad(lambda t:np.sin(t)/(x+t),0,np.inf)[0]

tG=[G(x) for x in tx]
plt.plot(tx,tG)
plt.show()
```

On obtient l'avertissement :

```
Warning (from warnings module):
  File "D:/DRIVE CPGE/ORAU/CENTRALE2/EX023.py", line 18
    G=lambda x:integr.quad(lambda t:np.sin(t)/(x+t),0,np.inf)[0]
IntegrationWarning: The integral is probably divergent, or slowly convergent.
```

On peut raisonnablement imaginer que l'avertissement vient du fait que l'intégrande définissant G n'est pas intégrable. Il s'agit d'un cas d'intégrale semi-convergente. On code plutôt :

```
G=lambda x:integr.quad(lambda t:np.sin(t)/(x+t),0,100)[0]
```

et en superposant les graphes de F et G, on observe :

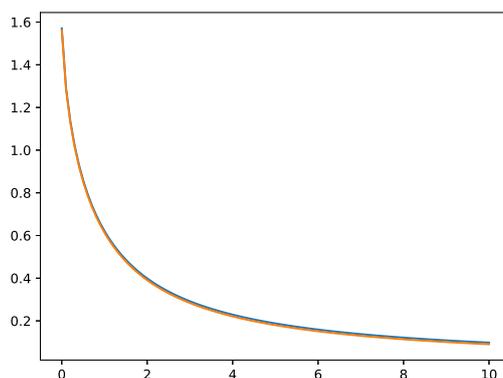


FIGURE 2 – Graphe de G

On conjecture

$$\boxed{F = G}$$

4. D'après le théorème de Taylor-Young, on a

$$\begin{aligned} \phi(x_0 + h) &\underset{h \rightarrow 0}{=} \phi(x_0) + \phi'(x_0)h + \phi''(x_0)\frac{h^2}{2} + o(h^2) \\ \phi(x_0 - h) &\underset{h \rightarrow 0}{=} \phi(x_0 - h) - \phi'(x_0)h + \phi''(x_0)\frac{h^2}{2} + o(h^2) \end{aligned}$$

d'où

$$\phi(x_0 + h) - 2\phi(x_0) + \phi(x_0 - h) = h^2\phi''(x_0) + o(h^2)$$

Ainsi

$$\boxed{\frac{\phi(x_0 + h) - 2\phi(x_0) + \phi(x_0 - h)}{h^2} \xrightarrow{h \rightarrow 0} \phi''(x_0)}$$

5. On saisit :

```
h=1e-4
tx=np.linspace(.1,10,100)
tdiff=[F(x)+(F(x+h)-2*F(x)+F(x-h)))/h**2-1/x for x in tx]
plt.plot(tx,tdiff)
plt.show()
```

On observe :

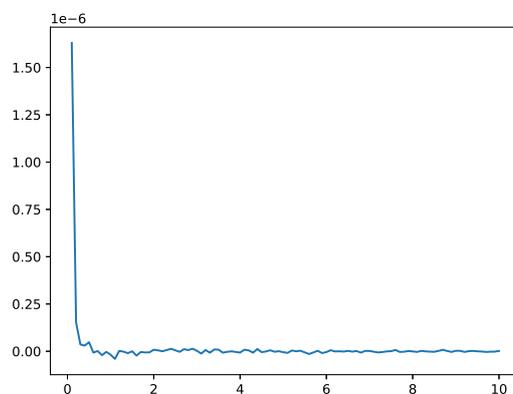


FIGURE 3 – Graphe d'une approximation de $x \mapsto F''(x) + F(x) - \frac{1}{x}$

La simulation numérique conforte l'idée que la fonction F satisfait l'équation (E).

6. Vérifions les hypothèses du théorème de continuité sous l'intégrale.

- Pour $x \geq 0$, on a $t \mapsto f(x, t) \in \mathcal{C}_{pm}(\mathbb{R}_+, \mathbb{R})$ par théorèmes généraux.
- Pour $t \geq 0$, on a $x \mapsto f(x, t) \in \mathcal{C}^0(\mathbb{R}_+, \mathbb{R})$ par théorèmes généraux.
- Domination : On a

$$\forall (x, t) \in \mathbb{R}_+^2 \quad 0 \leq f(x, t) \leq \varphi(t) \quad \text{avec} \quad \varphi(t) = \frac{1}{1+t^2}$$

La fonction φ est continue (par morceaux) et intégrable sur \mathbb{R}_+ puisque $\int_0^{+\infty} \varphi(t) dt = [\text{Arctan } t]_0^{+\infty} = \frac{\pi}{2}$. D'après l'intégration par parties réalisée à la première question, il vient pour $x \geq 0$

$$\int_0^{+\infty} \frac{\sin(t)}{x+t} dt = \underbrace{\left[\frac{1 - \cos(t)}{x+t} \right]_0^{+\infty}}_{=0} + \int_0^{+\infty} \frac{1 - \cos(t)}{(x+t)^2} dt$$

Avec la domination

$$\forall (x, t) \in \mathbb{R}_+ \times]0; +\infty[\quad 0 \leq \frac{1 - \cos(t)}{(x+t)^2} \leq \frac{1 - \cos(t)}{t^2}$$

on établit sans difficulté la continuité de la nouvelle écriture de G et on conclut

$$\boxed{\text{Les fonctions F et G sont définies, continues sur } \mathbb{R}_+ .}$$

7. Une domination locale permet d'établir sans difficulté que $F \in \mathcal{C}^2(]0; +\infty[, \mathbb{R})$. Pour $x > 0$, on obtient par changement de variable

$$\int_0^{+\infty} \frac{\sin(t)}{x+t} dt \quad \text{et} \quad \int_x^{+\infty} \frac{\sin(u-x)}{u} du = \int_x^{+\infty} \frac{\cos(x) \sin(u) - \sin(x) \cos(u)}{u} du$$

Les intégrales $A(x) = \int_x^{+\infty} \frac{\sin(u)}{u} du$ et $B(x) = \int_x^{+\infty} \frac{\cos(u)}{u} du$ convergent (intégration par parties). Ainsi, par linéarité

$$\forall x > 0 \quad G(x) = \cos(x)A(x) - \sin(x)B(x)$$

Les intégrandes des fonctions A et B sont continues et même de classe \mathcal{C}^1 donc A et B sont de classe \mathcal{C}^1 avec A' et B' de classe \mathcal{C}^1 d'où A, B de classe \mathcal{C}^2 et par conséquent

$$\boxed{\text{Les fonctions F et G sont de classe } \mathcal{C}^2 \text{ sur }]0; +\infty[.}$$

8. Par dérivation sous l'intégrale, il vient

$$\forall x > 0 \quad F''(x) + F(x) = \int_0^{+\infty} \frac{t^2 e^{-xt}}{1+t^2} dt + \int_0^{+\infty} \frac{e^{-xt}}{1+t^2} dt = \int_0^{+\infty} e^{-xt} dt$$

et avec
$$\forall x > 0 \quad A'(x) = -\frac{\sin(x)}{x} \quad \text{et} \quad B'(x) = -\frac{\cos(x)}{x}$$

on trouve finalement

$$\boxed{\text{Les fonctions F et G vérifient } y'' + y = \frac{1}{x} \text{ sur }]0; +\infty[.}$$

La fonction $F - G$ est donc solution de l'équation homogène $y'' + y = 0$ et par conséquent, il existe a, b réels tels que $F - G = a \cos + b \sin$. Or, on a (convergence assurée)

$$\forall x > 0 \quad 0 \leq F(x) \leq \int_0^{+\infty} e^{-xt} dt = \frac{1}{x}$$

et $G(x) = \cos(x)A(x) \sin(x)B(x)$ avec $A(x) \underset{x \rightarrow +\infty}{=} o(1)$ et $B(x) \underset{x \rightarrow +\infty}{=} o(1)$

Par suite $F(x) \underset{x \rightarrow +\infty}{\longrightarrow} 0$ et $G(x) \underset{x \rightarrow +\infty}{\longrightarrow} 0$

donc la fonction $a \cos + b \sin$ admet une limite en $+\infty$ ce qui prouve $a = b = 0$. Ainsi, on a

$$\forall x > 0 \quad F(x) = G(x)$$

Enfin, par continuité sur \mathbb{R}_+ , il vient

$$F(0) = \lim_{x \rightarrow 0^+} F(x) = \lim_{x \rightarrow 0^+} G(x) = G(0)$$

Ainsi

$$\boxed{F = G}$$

9. On a $\int_0^{+\infty} \frac{\sin(t)}{t} dt = G(0) = F(0) = \int_0^{+\infty} \frac{dt}{1+t^2}$

Et on conclut

$$\boxed{\int_0^{+\infty} \frac{\sin(t)}{t} dt = \frac{\pi}{2}}$$

Exercice 9 (Mines-Telecom 2015)

On pose $\forall n \in \mathbb{N}^* \quad I_n = \int_0^{+\infty} \frac{dt}{\operatorname{ch}(t)^n}$

1. Justifier que l'intégrale définissant I_n est convergente pour n entier non nul.
2. Montrer la convergence de la suite $(I_n)_{n \geq 1}$ et préciser sa limite.
3. Préciser la nature et éventuellement la somme de la série $\sum_{n \geq 1} I_n$.
4. Préciser la nature et éventuellement la somme de la série $\sum_{n \geq 1} (-1)^n I_n$.

Corrigé : 1. On pose $\forall (n, t) \in \mathbb{N}^* \times]0; +\infty[\quad f_n(t) = \frac{1}{\operatorname{ch}(t)^n}$

Pour n entier non nul, on a $f_n \in \mathcal{C}_{pm}([0; +\infty[, \mathbb{R})$ et

$$f_n(t) \underset{n \rightarrow +\infty}{\sim} 2^n e^{-nt}$$

d'où l'intégrabilité de f_n en $+\infty$ et on conclut

L'intégrale définissant I_n pour n entier non nul converge.

2. Pour n entier non nul, on considère I_n comme intégrale sur $]0; +\infty[$, faussement impropre en zéro. On a

$$\forall (n, t) \in \mathbb{N}^* \times]0; +\infty[\quad 0 \leq f_n(t) \leq f_1(t) \quad \text{et} \quad \forall t > 0 \quad f_n(t) \xrightarrow{n \rightarrow \infty} 0$$

On a $f_1 \in L^1(]0; +\infty[, \mathbb{R})$ et par convergence dominée, on conclut

$$I_n \xrightarrow{n \rightarrow \infty} 0$$

3. On a $\operatorname{ch}(t) \leq e^t$ pour $t \geq 0$ et après intégration, on obtient

$$\forall n \in \mathbb{N}^* \quad \frac{1}{n} = \int_0^{+\infty} e^{-nt} dt \leq I_n$$

La série $\sum_{n \geq 1} \frac{1}{n}$ diverge d'où par comparaison

La série $\sum_{n \geq 1} I_n$ diverge.

Variante : Supposons la série $\sum_{n \geq 1} I_n$ convergente. Pour $t > 0$, la série $\sum_{n \geq 1} \frac{1}{\operatorname{ch}(t)^n}$ converge en tant que série géométrique convergente et on a

$$\forall t > 0 \quad \sum_{n=1}^{+\infty} \frac{1}{\operatorname{ch}(t)^n} = \frac{1}{\operatorname{ch}(t)} \frac{1}{1 - 1/\operatorname{ch}(t)} = \frac{1}{\operatorname{ch}(t) - 1}$$

La somme $\sum_{n=1}^{+\infty} f_n$ est continue par morceaux sur $]0; +\infty[$ et par intégration terme à terme, on a

l'intégrabilité de $\sum_{n=1}^{+\infty} f_n$ sur $]0; +\infty[$ et la permutation des symboles Σ/\int . Or, on trouve

$$\int_0^{+\infty} \sum_{n=1}^{+\infty} f_n(t) dt = \int_0^{+\infty} \frac{dt}{\operatorname{ch}(t) - 1} \quad \text{avec} \quad \frac{1}{\operatorname{ch}(t) - 1} \underset{t \rightarrow 0}{\sim} \frac{2}{t^2} > 0$$

ce qui contredit la convergence d'après le critère des équivalents (licite, signe constant) et critère de Riemann. On conclut comme précédemment.

4. La série $\sum_{n \geq 1} (-1)^n I_n$ est alternée avec $(I_n)_{n \geq 1}$ clairement décroissante et de limite nulle d'où la convergence de la série. Soit N entier non nul. Il vient par linéarité du symbole somme

$$\begin{aligned} \sum_{n=1}^N (-1)^n I_n &= \int_0^{+\infty} \sum_{n=1}^N \frac{(-1)^n}{\operatorname{ch}(t)^n} dt \\ &= \int_0^{+\infty} -\frac{1}{\operatorname{ch}(t)} \frac{1 - (-1)^N / \operatorname{ch}(t)^N}{1 + 1/\operatorname{ch}(t)} dt = -\int_0^{+\infty} \frac{1 - (-1)^N / \operatorname{ch}(t)^N}{\operatorname{ch}(t) + 1} dt \end{aligned}$$

Sans difficulté, l'intégrale $\int_0^{+\infty} \frac{dt}{\operatorname{ch}(t) + 1}$ converge et par linéarité de l'intégrale (car convergence), il vient

$$\Delta_N = \sum_{n=1}^N (-1)^n I_n + \int_0^{+\infty} \frac{dt}{\operatorname{ch}(t) + 1} = (-1)^N \int_0^{+\infty} \frac{dt}{(1 + \operatorname{ch}(t)) \operatorname{ch}(t)^N}$$

On observe $|\Delta_N| \leq I_N$ et passant à la limite

$$\sum_{n=1}^{+\infty} (-1)^n I_n = \int_0^{+\infty} \frac{dt}{\operatorname{ch}(t) + 1} = \int_0^{+\infty} \frac{2e^t dt}{(e^t + 1)^2} \underbrace{=}_{u=e^t+1} -2 \int_2^{+\infty} \frac{du}{u^2}$$

On conclut

La série $\sum_{n \geq 1} (-1)^n I_n$ converge et sa somme vaut -1 .

Exercice 10 (Mines-Telecom 2021)

1. Résoudre $x^2 = x$ d'inconnue $x \in \mathbb{Z}/p\mathbb{Z}$ avec p nombre premier.
2. Résoudre $x^2 = x$ d'inconnue $x \in \mathbb{Z}/34\mathbb{Z}$.

Corrigé : 1. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps puisque p est premier. Par intégrité, il vient

$$x^2 = x \iff x(x - \bar{1}) = \bar{0} \iff x \in \{\bar{0}, \bar{1}\}$$

2. On a $34 = 2 \times 17$ avec $2 \wedge 17 = 1$. D'après le théorème chinois, on dispose de l'isomorphisme $\pi : \mathbb{Z}/34\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$, $\bar{x} \mapsto (\widehat{x}, \dot{x})$. Ainsi, pour $x \in \mathbb{Z}$, on a

$$\bar{x}^2 = \bar{x} \iff \begin{cases} \widehat{x}^2 = \widehat{x} \\ \dot{x}^2 = \dot{x} \end{cases} \iff (\widehat{x}, \dot{x}) \in \{(\widehat{0}, \dot{0}), (\widehat{1}, \dot{0}), (\widehat{0}, \dot{1}), (\widehat{1}, \dot{1})\}$$

On a l'égalité $17 - 2 \times 8 = 1$ d'où

$$\widehat{17} = \widehat{1}, \quad \dot{17} = \dot{0}, \quad \widehat{-16} = \widehat{0}, \quad \dot{-16} = \dot{1}$$

et on conclut

$$\text{Pour } x \in \mathbb{Z}, \text{ on a } x^2 \equiv x [34] \iff \bar{x} \in \{\bar{0}, \bar{17}, \bar{-16}, \bar{17-16}\}$$

Remarque : En réalité, l'équation $\widehat{x}^2 = \widehat{x}$ est toujours vraie. On a simplement

$$\bar{x}^2 = \bar{x} \iff \dot{x}^2 = \dot{x} \iff x \equiv 0 [17] \quad \text{ou} \quad x \equiv 1 [17] \iff \bar{x} \in \{\bar{0}, \bar{17}, \bar{1}, \bar{18}\}$$

La démarche générale présentée ci-avant aurait plus d'intérêt sur une configuration moins triviale, par exemple avec $3 \times 17 \dots$

Exercice 11 (Centrale 2022)

Un nombre de Carmichael est un entier $n \geq 2$ non premier tel que

$$\forall a \in \mathbb{Z} \quad a^n \equiv a \pmod{n}$$

1. Soit $n \geq 2$ non premier tel que

$$\forall a \in \llbracket 0; n-1 \rrbracket \quad a^n \equiv a \pmod{n}$$

Montrer que n est un nombre de Carmichael.

2. Écrire une fonction `carmichael(n)` d'argument n entier qui renvoie `True` si n est un nombre de Carmichael et `False` sinon.

3. Déterminer à l'aide de l'outil informatique le plus petit nombre de Carmichael.

4. Soit $n = \prod_{i=1}^r p_i$ avec $r \geq 2$ et les p_i des nombres premiers deux à deux distincts vérifiant $p_i - 1 \mid n - 1$ pour tout $i \in \llbracket 1; r \rrbracket$.

(a) Montrer $\forall i \in \llbracket 1; r \rrbracket \quad \forall a \in \mathbb{Z} \quad a^n \equiv a \pmod{p_i}$

(b) Montrer que n est un nombre de Carmichael.

5. Soit n un nombre de Carmichael. Montrer que n est un produit de nombres premiers deux à deux distincts.

6. Soit (G, \times) un groupe abélien fini.

(a) Soient x, y dans G avec $o(x) \wedge o(y) = 1$. Montrer que $o(xy) = o(x)o(y)$.

(b) Soit $x \in G$. Pour d diviseur de $o(x)$, montrer qu'il existe un élément de G d'ordre d .

(c) Soit m l'ordre maximal des éléments de G . Montrer que l'ordre de tout élément de G divise m .

(d) En déduire $\forall p \in \mathcal{P} \quad \mathrm{U}(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

7. Soit n un nombre de Carmichael et p un diviseur premier de n . Montrer que $p-1 \mid n-1$.

Corrigé : 1. Soit n entier ≥ 2 vérifiant la condition annoncée et soit $a \in \mathbb{Z}$. D'après le théorème de la division euclidienne, on dispose d'un unique couple $(q, r) \in \mathbb{Z} \times \llbracket 0; n-1 \rrbracket$ tel que $a = qn + r$. Dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, on a

$$\bar{a}^n = \bar{r}^n = \bar{r} = \bar{a}$$

Ainsi

L'entier n est un nombre de Carmichael.

2. Pour tester si un entier $n \geq 2$ est un nombre de Carmichael, on commence par tester sa non primalité. S'il existe d un diviseur strict de n , alors on a $d \leq \sqrt{n}$ ou $\frac{n}{d} \leq n$. Sinon, on aurait $d > \sqrt{n}$ et $\frac{n}{d} > \sqrt{n}$ d'où $n > n$ ce qui est absurde. On saisit :

```
def carmichael(n):
    d=2
    diviseur_trouve=False
    while d**2<=n and not diviseur_trouve:
        if n%d==0:
            diviseur_trouve=True
        d+=1
```

```
if not diviseur_trouve:
    return False
for k in range(n):
    if (k**n)%n!=k:
        return False
return True
```

3. On saisit :

```
n=2
while not carmichael(n):
    n+=1
print("Premier nombre de Carmichael=",n)
```

On obtient :

```
Premier nombre de Carmichael= 561
```

On peut améliorer la performance de cette fonction en procédant différemment et en gardant la mémoire des nombres premiers rencontrés au cours des itérations :

```
P=[2]

def carmichael(n):
    global P
    est_premier=True
    for p in P:
        if n%p==0:
            est_premier=False
    if est_premier:
        P.append(n)
        return False
    for k in range(n):
        if (k**n)%n!=k:
            return False
    return True
```

Puis, on saisit en démarrant à $n = 3$ (on sait que 2 n'est pas de Carmichael puisqu'il n'est pas premier) :

```
n=3
while not carmichael(n):
    n+=1
print("Premier nombre de Carmichael=",n)
```

La liste P est enrichie à chaque appel de la fonction `carmichael` des nouveaux nombres premiers rencontrés ce qui permet d'accélérer le test de non primalité.

4.(a) Soit $i \in \llbracket 1; r \rrbracket$ et $a \in \mathbb{Z}$. Si p_i divise a , alors p_i divise a^n et l'égalité a lieu. Supposons que p_i ne divise pas a ce qui équivaut à $a \wedge p_i = 1$. D'après le petit théorème de Fermat, on a donc

$$a^{p_i-1} \equiv 1 [p_i]$$

Comme $p_i - 1 | n - 1$, on dispose de q_i entier non nul tel que $n - 1 = q_i(p_i - 1)$. Par suite, il vient

$$a^n \equiv (a^{p_i-1})^{q_i} a \equiv a [p_i]$$

On conclut

$$\boxed{\forall i \in \llbracket 1; r \rrbracket \quad \forall a \in \mathbb{Z} \quad a^n \equiv a [p_i]}$$

4.(b) Les p_i sont des nombres premiers deux à deux distincts et sont donc deux à deux premiers entre eux. D'après le théorème chinois, l'application

$$\pi: \begin{cases} \mathbb{Z}/n\mathbb{Z} \longrightarrow \prod_{i=1}^r \mathbb{Z}/p_i\mathbb{Z} \\ \bar{a}^{[n]} \longmapsto (\bar{a}^{[p_i]})_{1 \leq i \leq r} \end{cases}$$

est un isomorphisme d'anneaux. Ainsi, pour $a \in \mathbb{Z}$, on a

$$\bar{a}^{[n]} = \bar{a}^{[n]} \iff \pi(\bar{a}^{[n]}) = \pi(\bar{a}^{[n]}) \iff \forall i \in \llbracket 1; r \rrbracket \quad \bar{a}^{[p_i]} = \bar{a}^{[p_i]}$$

et comme la dernière assertion est vraie d'après le résultat de la question précédente, on conclut

$$\boxed{\text{L'entier } n \text{ est un nombre de Carmichael.}}$$

5. Supposons qu'il existe p premier et α entier ≥ 2 tel que $p^\alpha | n$. Comme le nombre n est de Carmichael, on a $p^n \equiv p [n]$ d'où $p^n \equiv p [p^2]$ ce qui signifie qu'on dispose de $q \in \mathbb{Z}$ tel que $p^n = p + qp^2$ d'où

$$p(p^{n-2} - q) = 1$$

ce qui est absurde. Ainsi, les valuations des facteurs premiers dans la décomposition de n sont égales à 1 et il n'y a pas qu'un facteur premier sans quoi l'entier n serait premier. On conclut

$$\boxed{\text{Un nombre de Carmichael est produit de nombres premiers deux à deux distincts.}}$$

6.(a) On a

$$(xy)^{o(x)o(y)} = (x^{o(x)})^{o(y)}(y^{o(y)})^{o(x)} = 1$$

d'où $o(xy) | o(x)o(y)$. Puis, on a $(xy)^{o(xy)} = 1$ d'où

$$(xy)^{o(xy)o(x)} = (x^{o(x)})^{o(xy)}y^{o(xy)o(x)} = y^{o(xy)o(y)} = 1$$

d'où $o(y) | o(xy)o(x)$ et comme $o(x) \wedge o(y) = 1$, il s'ensuit $o(y) | o(xy)$ d'après le lemme de Gauss. Par symétrie des rôles, on a également $o(x) | o(xy)$ d'où $o(x) \vee o(y) | o(xy)$. Or, on a

$$o(xy) = (o(x) \wedge o(y))(o(x) \vee o(y)) = o(x) \vee o(y)$$

Ceci prouve que $o(x)o(y) | o(x)o(y)$ et les entiers $o(xy)$ et $o(x)o(y)$ sont donc des entiers associés. On conclut

$$\boxed{o(xy) = o(x)o(y)}$$

Variante : On peut aussi observer

$$(xy)^{o(xy)} = 1 \iff \underbrace{x^{o(xy)}}_{\in \langle x \rangle} = \underbrace{y^{-o(xy)}}_{\in \langle y \rangle}$$

Or, l'intersection $\langle x \rangle \cap \langle y \rangle$ est sous-groupe de $\langle x \rangle$ et de $\langle y \rangle$ donc d'ordre divisant $o(x)$ et $o(y)$ d'où $\langle x \rangle \cap \langle y \rangle = 1$. On en déduit

$$x^{o(xy)} = 1 \quad \text{et} \quad y^{o(xy)} = 1$$

d'où $o(x)|o(xy)$ et $o(y)|o(xy)$ et on conclut comme précédemment.

6.(b) Soit $x \in G$ et d diviseur de $o(x)$. On dispose de c entier non nul tel que $o(x) = dc$. On a $(x^c)^d = x^{dc} = 1$ d'où $d|o(x^c)$. Puis, on a $(x^c)^{o(x^c)} = 1 = x^{co(x^c)}$ d'où $o(x)|co(x^c)$, c'est-à-dire $dc|co(x^c)$ d'où $d|o(x^c)$. Les entiers d et $o(x^c)$ sont associés donc égaux et par conséquent

Il existe un élément de G d'ordre d .

6.(c) La quantité $\max\{o(x), x \in G\}$ est bien définie comme maximum d'une partie finie non vide. On note $m = \max\{o(x), x \in G\}$ et $x \in G$ tel que $o(x) = m$. Supposons qu'il existe $y \in G$ tel que $o(y)$ ne divise pas $o(x)$. Ainsi, on dispose de $q \in \mathcal{P}$ tel que $v_q(o(y)) > v_q(o(x))$. D'après le résultat de la question précédente, on dispose de $x' \in G$ d'ordre $\prod_{p \in \mathcal{P} \setminus \{q\}} p^{v_p(o(x))}$ et de $y' \in G$ d'ordre $p^{v_p(o(y))}$. Or, on a

$$q^{v_q(o(y))} \wedge \prod_{p \in \mathcal{P} \setminus \{q\}} p^{v_p(o(x))} = 1$$

et d'après le résultat de la question 6.(a), on obtient

$$o(x'y') = o(x')o(y') = q^{v_q(o(y))} \prod_{p \in \mathcal{P} \setminus \{q\}} p^{v_p(o(x))} > o(x)$$

ce qui est absurde par maximalité de $o(x)$. On conclut

L'ordre de tout élément de G divise m .

6.(d) Soit $p \in \mathcal{P}$. Le groupe $(U(\mathbb{Z}/p\mathbb{Z}), \times)$ est d'ordre $p - 1$. Notons m l'ordre maximal des éléments de G . On a $\bar{x}^m = \bar{1}$ pour tout $\bar{x} \in U(\mathbb{Z}/p\mathbb{Z})$ d'après le résultat de la question précédente. Comme l'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps, le polynôme $X^m - \bar{1}$ de $\mathbb{Z}/p\mathbb{Z}[X]$ admet au plus m racines distinctes (résultat qui n'est pas officiellement au programme, à savoir redémontrer par récurrence sur le degré avec une factorisation de Bernoulli). Ainsi, on a $p - 1 \leq m$ et comme l'ordre d'un élément d'un groupe divise l'ordre du groupe, on a aussi $m|p - 1$ d'où $m \leq p - 1$ et par conséquent $m = p - 1$ ce qui prouve que le groupe $(U(\mathbb{Z}/p\mathbb{Z}), \times)$ admet un générateur. On conclut

$$\forall p \in \mathcal{P} \quad U(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/(p - 1)\mathbb{Z}$$

7. Pour $a \in \mathbb{Z}$, on a $a^n \equiv a [n]$ d'où $a^n \equiv a [p]$. Pour $a \in \llbracket 1; p - 1 \rrbracket$, on a $\bar{a} \in U(\mathbb{Z}/p\mathbb{Z})$ et il vient

$$\bar{a}^{n-1} = \bar{a}^{-1}\bar{a}^n = \bar{a}^{-1}\bar{a} = \bar{1}$$

Comme le groupe $(U(\mathbb{Z}/p\mathbb{Z}), \times)$ est cyclique, on choisit $a \in \llbracket 1; p - 1 \rrbracket$ d'ordre égal à $p - 1$. Ainsi, on trouve

$$o(\bar{a}) = p - 1 | n - 1$$

Commentaire : On a donc établi l'équivalence suivante :

Le nombre $n \geq 2$ est de Carmichael si et seulement si $n = \prod_{i=1}^r p_i$ avec $r \geq 2$ et les p_i des nombres premiers distincts vérifiant $p_i - 1 | n - 1$ pour tout $i \in \llbracket 1; r \rrbracket$.

Exercice 12 (CCINP 2024)

1. Soit $(u_n)_n$ suite décroissante positive de limite nulle.
 - (a) Démontrer que la série $\sum (-1)^n u_n$ converge.
 - (b) Donner une majoration de la valeur absolue du reste de la série $\sum (-1)^n u_n$.

2. On pose $\forall (n, x) \in \mathbb{N}^* \times \mathbb{R} \quad f_n(x) = \frac{(-1)^n e^{-nx}}{n}$
 - (a) Étudier la convergence simple sur \mathbb{R} de la série de fonctions $\sum_{n \geq 1} f_n$.
 - (b) Étudier la convergence uniforme sur $[0; +\infty[$ de la série de fonctions $\sum_{n \geq 1} f_n$.

Corrigé : Exercice 8 CCPINP 2024

Exercice 13 (CCINP 2024)

Soit n entier non nul. On pose

$$\forall (M, N) \in \mathcal{M}_n(\mathbb{R})^2 \quad \langle M, N \rangle = \text{Tr} (M^\top N)$$

1. Montrer que $(M, N) \mapsto \langle M, N \rangle$ est un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$.
2. Pour $(M, N) \in \mathcal{O}_n(\mathbb{R})^2$, établir $\langle M, N \rangle \leq n$.
3. Pour $(A, B) \in \mathcal{S}_n(\mathbb{R})^2$, montrer $\text{Tr} ((AB)^2) \leq \text{Tr} (A^2 B^2)$.
4. Pour $(A, B) \in \mathcal{S}_n(\mathbb{R})^2$, montrer $\text{Tr} ((AB + BA)^2) \leq 4 \text{Tr} (A^2) \text{Tr} (B^2)$.

Corrigé : 1. Pour $A = (a_{i,j})_{1 \leq i,j \leq n}$ et $B = (b_{i,j})_{1 \leq i,j \leq n}$ dans $\mathcal{M}_n(\mathbb{R})$, on a $\langle A, B \rangle = \sum_{j=1}^n \sum_{i=1}^n a'_{j,i} b_{i,j}$ avec $A^\top = (a'_{i,j})$. D'où

$$\langle A, B \rangle = \sum_{1 \leq i,j \leq n} a_{i,j} b_{i,j}$$

expression symétrique en les coefficients d'où la symétrie de l'application. On en déduit sans difficulté qu'il s'agit d'une forme bilinéaire symétrique définie et positive et on conclut

$$\boxed{\text{L'application } (M, N) \mapsto \langle M, N \rangle \text{ est un produit scalaire sur } \mathcal{M}_n(\mathbb{R}).}$$

2. Soit $(M, N) \in \mathcal{O}_n(\mathbb{R})^2$. D'après l'inégalité de Cauchy-Schwarz, il vient

$$\langle M, N \rangle \leq \|M\| \|N\|$$

avec

$$\|M\|^2 = \text{Tr} (M^\top M) = \text{Tr} (I_n) = n$$

et de même pour N . On conclut

$$\boxed{\forall (M, N) \in \mathcal{O}_n(\mathbb{R})^2 \quad \langle M, N \rangle \leq n}$$

3. Soit $(A, B) \in \mathcal{S}_n(\mathbb{R})^2$. On pose $C = AB - BA$. On observe $C \in \mathcal{A}_n(\mathbb{R})$. Soit $\lambda \in \mathbb{C}$ et $X \in \mathcal{M}_{n,1}(\mathbb{C}) \setminus \{0\}$ tel que $CX = \lambda X$. On multiplie par \bar{X}^\top à gauche et on trouve $\bar{X}^\top CX = \lambda \bar{X}^\top X$. Puis, on conjugue et transpose l'égalité $CX = \lambda X$ et on multiplie à droite par X pour obtenir $-\bar{X}^\top CX = \bar{\lambda} \bar{X}^\top X$. En additionnant les deux égalités obtenues, il vient

$$(\lambda + \bar{\lambda}) \bar{X}^\top X = (\lambda + \bar{\lambda}) \underbrace{\sum_{i=1}^n |x_i|^2}_{>0} = 0$$

notant x_i les coordonnées de X dont l'une au moins n'est pas nulle. On en déduit $\lambda + \bar{\lambda} = 0$ d'où $\lambda \in i\mathbb{R}$. La matrice C^2 est clairement symétrique réelle donc diagonalisable d'après le théorème spectral et $\text{Sp}(C^2) \subset]-\infty; 0]$ d'après ce qui précède. Il s'ensuit $\text{Tr}(C^2) \leq 0$, autrement dit

$$\text{Tr} ((AB)^2 - 2AB^2A + (BA)^2) = \text{Tr} ((AB)^2) - 2 \text{Tr} (AB^2A) + \text{Tr} ((BA)^2) \leq 0$$

D'après la propriété fondamentale de la trace, on a $\text{Tr} (AB^2A) = \text{Tr} (A^2B^2)$ et par invariance de la transposition $\text{Tr} ((BA)^2) = \text{Tr} ((AB)^2)$. On conclut

$$\boxed{\forall (A, B) \in \mathcal{S}_n(\mathbb{R})^2 \quad \text{Tr} ((AB)^2) \leq \text{Tr} (A^2 B^2)}$$

4. Soit $(A, B) \in \mathcal{S}_n(\mathbb{R})$. En utilisant les propriétés de la trace mentionnées ci-avant, il vient

$$\text{Tr} ((AB + BA)^2) = \text{Tr} ((AB)^2 + 2AB^2A + (BA)^2) = 2 \text{Tr} ((AB)^2) + 2 \text{Tr} (A^2 B^2)$$

et avec l'inégalité précédente, il vient

$$\text{Tr} ((AB + BA)^2) \leq 4 \text{Tr} (A^2 B^2)$$

D'après l'inégalité de Cauchy-Schwarz, on a

$$\mathrm{Tr}(A^2 B^2) = \langle A^2, B^2 \rangle \leq \|A^2\| \|B^2\|$$

On dispose de $P \in \mathcal{O}_n(\mathbb{R})$ tel que $P^\top A P = D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ d'où $A^2 = P D^2 P^\top$ et $A^4 = P D^4 P^\top$. Ainsi

$$\|A^2\|^2 = \mathrm{Tr}(A^4) = \sum_{i=1}^n \lambda_i^4 \leq \left(\sum_{i=1}^n \lambda_i^2 \right)^2$$

ce qui prouve

$$\|A^2\| \leq \mathrm{Tr}(A^2)$$

et de même pour B . On conclut

$\forall (A, B) \in \mathcal{S}_n(\mathbb{R})^2 \quad \mathrm{Tr}((AB + BA)^2) \leq 4 \mathrm{Tr}(A^2) \mathrm{Tr}(B^2)$
--

Exercice 14 (Mines-Telecom 2023)

On pose $\forall n \geq 2 \quad u_n = \sum_{k=2}^n \frac{\ln(k)}{k}$

1. Établir $u_n \underset{n \rightarrow +\infty}{\sim} \frac{\ln(n)^2}{2}$

2. Déterminer un équivalent de $u_n - \frac{\ln(n)^2}{2}$ lorsque $n \rightarrow +\infty$.

Corrigé : 1. On a $\forall k \in \mathbb{N}^* \quad \frac{\ln(k)}{k+1} \leq \int_k^{k+1} \frac{\ln(t)}{t} dt \leq \frac{\ln(k+1)}{k}$

d'où $\int_k^{k+1} \frac{\ln(t)}{t} dt \underset{k \rightarrow +\infty}{\sim} \frac{\ln(k)}{k}$

Par sommation des relations de comparaison, il vient

$$\sum_{k=1}^n u_k \underset{n \rightarrow +\infty}{\sim} \int_1^{n+1} \frac{\ln(t)}{t} dt = \frac{(\ln(n+1))^2}{2}$$

Ainsi

$$\boxed{\sum_{k=1}^n u_k \underset{n \rightarrow +\infty}{\sim} \frac{\ln(n)^2}{2}}$$

2. On pose $\forall x \geq 1 \quad F(x) = \int_1^x \frac{\ln(t)}{t} dt$

La fonction F est primitive d'une fonction \mathcal{C}^∞ sur $]0; +\infty[$ et est donc elle-même de classe \mathcal{C}^∞ sur $]0; +\infty[$. Par dérivation, on trouve

$$\forall x > 0 \quad F'(x) = \frac{\ln(x)}{x} \quad F''(x) = \frac{1 - \ln(x)}{x^2}$$

Soit $k \geq 1$. D'après l'inégalité de Taylor-Lagrange, on obtient

$$|F(k+1) - F(k) - F'(k)| \leq \frac{1}{2} \|F^{(2)}\|_{\infty, [k; k+1]}$$

avec $\|F^{(2)}\|_{\infty, [k; k+1]} \leq \frac{\ln(k+1) + 1}{k^2} \underset{k \rightarrow +\infty}{=} O\left(\frac{\ln(k)}{k^2}\right) \underset{k \rightarrow +\infty}{=} O\left(\frac{1}{k^{\frac{3}{2}}}\right)$

Puis, il vient pour n entier non nul

$$\sum_{k=1}^n (F(k+1) - F(k) - F'(k)) = F(n+1) - \sum_{k=1}^n F'(k) = \sum_{k=1}^n O\left(\frac{1}{k^{\frac{3}{2}}}\right)$$

Par critère de Riemann, il existe λ réel tel que

$$\sum_{k=1}^n F'(k) - F(n+1) \xrightarrow[n \rightarrow \infty]{} \lambda$$

c'est-à-dire $\sum_{k=1}^n \frac{\ln(k)}{k} - \int_1^{n+1} \frac{\ln(t)}{t} dt = \lambda + o(1)$

ou encore $\sum_{k=1}^n \frac{\ln(k)}{k} - \left[\frac{\ln(t)^2}{2}\right]_1^{n+1} = \lambda + o(1)$

On a
$$\ln(n+1) = \ln(n) + \ln\left(1 + \frac{1}{n}\right) = \ln(n) + O\left(\frac{1}{n}\right)$$

d'où
$$\ln(n+1)^2 = \ln(n)^2 + o(1)$$

On conclut
$$\boxed{\sum_{k=1}^n \frac{\ln(k)}{k} = \frac{\ln(n)^2}{2} + \lambda + o(1)}$$

Remarque : La constante λ ne semble pas simple à déterminer ... Elle porte un nom : on l'appelle *constante de Stieljes*.

Exercice 15 (Mines-Telecom 2023)

Soit $A \in \mathcal{M}_n(\mathbb{R})$.

1. On suppose $A^2 + A + I_n = 0$. Montrer que l'entier n est pair.
2. On suppose $A^3 + A^2 + A = 0$. Montrer que $\text{rg}(A)$ est pair.

Corrigé : 1. Le polynôme $P = X^2 + X + 1$ est annulateur de A . Si l'entier n est impair, alors on a pour x réel

$$\chi_A(x) = x^n + o(x^n) \xrightarrow{x \rightarrow \pm \infty} \pm \infty$$

et comme l'application polynomiale $x \mapsto \chi_A(x)$ est continue sur \mathbb{R} , on en déduit d'après le théorème des valeurs intermédiaires qu'elle admet une racine. Or, les valeurs propres de A , c'est-à-dire les racines de χ_A sont contenues dans $P^{-1}(\{0\}) \cap \mathbb{R}$ qui est vide. On conclut

L'entier n est pair.

2. On note $u \in \mathcal{L}(\mathbb{R}^n)$ canoniquement associé à A . L'image $\text{Im } u$ est stable par u et on note $v = u|_{\text{Im } u}$ l'induit par u sur $\text{Im } u$. Soit $x \in \text{Im } u$. On dispose de $t \in E$ tel que $x = u(t)$ et il vient

$$(v^2 + v + \text{id})(x) = (u^2 + u + \text{id})(u(t)) = (u^3 + u^2 + u)(t) = 0_E$$

On applique alors le résultat de la première question à l'endomorphisme v et on conclut

L'entier $\text{rg}(u) = \text{rg}(A)$ est pair.

Exercice 16 (Centrale 2017)

On note r_n la probabilité que deux nombres aléatoires dans $\llbracket 1; n \rrbracket$ soient premiers entre eux.

On souhaite montrer
$$r_n \xrightarrow{n \rightarrow \infty} \frac{6}{\pi^2}$$

On admet que $\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ et la *formule du crible* :

$$\text{Card} \left(\bigcup_{i=1}^k U_i \right) = \sum_{I \subset \llbracket 1; k \rrbracket, I \neq \emptyset} (-1)^{1+\text{Card } I} \text{Card} \left(\bigcap_{i \in I} U_i \right)$$

On définit la fonction μ de Möbius de \mathbb{N}^* dans $\{-1, 0, 1\}$ de la manière suivante : $\mu(1) = 1$, $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier et $\mu(n) = (-1)^r$ si n est le produit de r nombres premiers distincts. Pour n entier non nul, on note

$$A_n = \{(a, b) \in \llbracket 1; n \rrbracket^2 \mid a \wedge b = 1\}$$

Notant p_1, \dots, p_k les nombres premiers dans $\llbracket 1; n \rrbracket$, on pose

$$\forall i \in \llbracket 1; k \rrbracket \quad U_i = \{(a, b) \in \llbracket 1; n \rrbracket^2 \mid p_i | a \text{ et } p_i | b\}$$

1. Écrire une fonction $\text{pgcd}(a, b)$ d'arguments des entiers a, b et qui renvoie le $\text{pgcd } a \wedge b$.
2. Vérifier la conjecture sur la limite de $(r_n)_n$.
3. Exprimer A_n en fonction des U_i .
4. Soit ℓ entier non nul. Déterminer le nombre de multiples de ℓ dans $\llbracket 1; n \rrbracket$.
5. En déduire le cardinal de $\bigcap_{i \in I} U_i$ avec I une partie non vide de $\llbracket 1; k \rrbracket$.

6. Montrer
$$\text{Card}(A_n) = \sum_{d=1}^n \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2$$

7. Conclure.

Corrigé : 1. On saisit :

```
def pgcd(a,b):
    u,v=a,b
    while v!=0:
        u,v=v,u%v
    return u
```

2. Pour n entier non nul, soient $X_1^{(n)}, \dots, X_N^{(n)}, Y_1^{(n)}, \dots, Y_N^{(n)}$ des variables aléatoires indépendantes de loi uniforme $\mathcal{U}_{\llbracket 1; n \rrbracket}$. On implémente une méthode de *Monte-Carlo* avec l'estimation

$$\frac{1}{N} \sum_{i=1}^N \mathbf{1}_{X_i^{(n)} \wedge Y_i^{(n)} = 1} \simeq \mathbb{E} \left(\mathbf{1}_{X_1^{(n)} \wedge Y_1^{(n)} = 1} \right) = \mathbb{P} \left(X_1^{(n)} \wedge Y_1^{(n)} = 1 \right) = r_n$$

On saisit :

```
tr=[]
tn=range(2,100)
for n in tn:
    X=rd.randint(1,n,N)
    Y=rd.randint(1,n,N)
    res=0
    for k in range(N):
        res+=pgcd(X[k],Y[k])==1
    res/=N
    tr.append(res)
plt.plot(tn,tr)
plt.grid();plt.show()
```

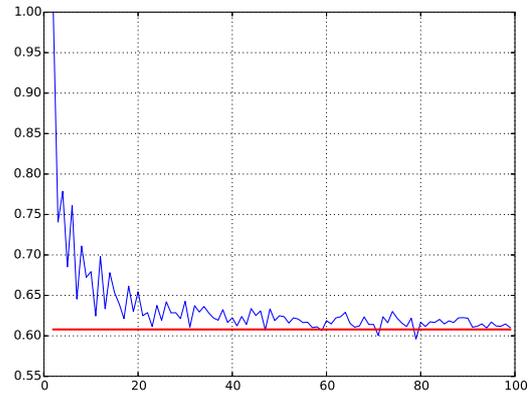


FIGURE 4 – Approximation stochastique de $(r_n)_n$

3. Un couple d'entiers de $\llbracket 1; n \rrbracket^2$ n'est pas dans A_n si et seulement s'il existe un facteur premier commun à ces deux entiers, autrement dit

$$\llbracket 1; n \rrbracket^2 \setminus A_n = \bigcup_{i=1}^k U_i$$

Et on conclut

$$A_n = \llbracket 1; n \rrbracket^2 \setminus \bigcup_{i=1}^k U_i$$

4. Les multiples de ℓ dans $\llbracket 1; n \rrbracket$ sont $\ell, 2\ell, \dots, \lfloor \frac{n}{\ell} \rfloor \ell$ et par suite

$$\text{Il y a } \lfloor \frac{n}{\ell} \rfloor \text{ multiples de } \ell \text{ dans } \llbracket 1; n \rrbracket.$$

5. Les éléments de $\bigcap_{i \in I} U_i$ sont les couples de multiples dans $\llbracket 1; n \rrbracket^2$ de $\prod_{i \in I} p_i$ d'où

$$\text{Card} \left(\bigcap_{i \in I} U_i \right) = \left\lfloor \frac{n}{\prod_{i \in I} p_i} \right\rfloor^2$$

6. Avec la formule du crible, il vient :

$$\begin{aligned} \text{Card } A_n &= n^2 - \text{Card} \left(\bigcup_{i=1}^k U_i \right) \\ &= n^2 - \sum_{I \subset \llbracket 1; k \rrbracket, I \neq \emptyset} (-1)^{\text{Card } I+1} \text{Card} \left(\bigcap_{i \in I} U_i \right) \\ \text{Card } A_n &= n^2 - \sum_{I \subset \llbracket 1; k \rrbracket, I \neq \emptyset} (-1)^{\text{Card } I+1} \left\lfloor \frac{n}{\prod_{i \in I} p_i} \right\rfloor^2 \end{aligned}$$

Choisir $I \neq \emptyset$ dans la somme précédente équivaut, par unicité de la décomposition en facteurs premiers, à choisir $d \in \llbracket 2; n \rrbracket$ produit de facteurs premiers distincts. Un tel d est donc ≥ 2 .

L'utilisation de la fonction μ permet d'écrire une somme pour $d \in \llbracket 2; n \rrbracket$, celle-ci étant complétée par des zéros dans le cas où d possède un facteur premier au carré. Ainsi, on trouve

$$\text{Card } A_n = n^2 + \sum_{d=2}^n \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2$$

Et finalement

$$\boxed{\text{Card } A_n = \sum_{d=1}^n \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2}$$

7. On a $\forall n \geq 1 \quad r_n = \frac{\text{Card } A_n}{\text{Card } \llbracket 1; n \rrbracket^2} = \frac{\text{Card } A_n}{n^2}$

Avec l'encadrement $x - 1 \leq \lfloor x \rfloor \leq x$ pour x réel, il vient

$$\left(\frac{n}{d} - 1\right)^2 \leq \left\lfloor \frac{n}{d} \right\rfloor^2 \leq \left(\frac{n}{d}\right)^2$$

puis
$$\sum_{d=1}^n \frac{\mu(d)}{d^2} - \frac{2}{n} \sum_{d=1}^n \frac{\mu(d)}{d} + \frac{1}{n} \leq r_n \leq \sum_{d=1}^n \frac{\mu(d)}{d^2}$$

On a $|\mu(d)| \leq 1$ pour tout d entier et par comparaison série/intégrale, on obtient $\sum_{d=1}^n \frac{\mu(d)}{d} = O(\ln n)$ et par suite

$$r_n = \sum_{d=1}^n \frac{\mu(d)}{d^2} + o(1)$$

Les familles $\left(\frac{\mu(d)}{d^2}\right)_{d \geq 1}$ et $\left(\frac{1}{n^2}\right)_{n \geq 1}$ sont sommables et d'après le théorème de Fubini, la famille $\left(\frac{\mu(d)}{(dn)^2}\right)_{(d,n) \in (\mathbb{N}^*)^2}$ est sommable. En considérant la partition $(I_p)_{p \geq 1}$ avec

$$\forall p \geq 1 \quad I_p = \{(d, n) \in (\mathbb{N}^*)^2 \mid dn = p\}$$

il vient après sommation par paquets

$$\sum_{(d,n) \in (\mathbb{N}^*)^2} \frac{\mu(d)}{(dn)^2} = \sum_{p=1}^{+\infty} \sum_{dn=p} \frac{\mu(d)}{(dn)^2} = \sum_{p=1}^{+\infty} \frac{1}{p^2} \left(\sum_{d|p} \mu(d) \right)$$

Évaluons enfin $\sum_{d|n} \mu(d)$ pour n entier non nul. Les facteurs premiers de n sont p_1, \dots, p_k . Comme la fonction μ s'annule en présence d'un facteur premier au carré, il vient

$$\sum_{d|n} \mu(d) = \sum_{I \subset \llbracket 1; k \rrbracket} \mu\left(\prod_{i \in I} p_i\right) = \sum_{j=0}^k \sum_{I \subset \llbracket 1; k \rrbracket, \text{Card } I=j} \mu\left(\prod_{i \in I} p_i\right) = \sum_{j=0}^k \binom{k}{j} (-1)^j = (1-1)^k$$

et par conséquent

$$\sum_{d|n} \mu(d) = \delta_{n,1}$$

d'où
$$\frac{\pi^2}{6} \left(\lim_{n \rightarrow +\infty} r_n \right) = \left(\sum_{n=1}^{+\infty} \frac{1}{n^2} \right) \left(\sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2} \right) = \sum_{(d,n) \in (\mathbb{N}^*)^2} \frac{\mu(d)}{(dn)^2} = \sum_{p=1}^{+\infty} \frac{\delta_{p,1}}{p^2} = 1$$

On conclut

$$\boxed{r_n \xrightarrow{n \rightarrow \infty} \frac{6}{\pi^2}}$$

Exercice 17 (Mines 2019)

1. Soit $n \geq 2$. Trouver les $P \in \mathbb{R}[X]$ tels que, pour toute matrice $A \in \mathcal{A}_n(\mathbb{R})$, la matrice $P(A)$ soit aussi antisymétrique.
2. Soit $n \geq 2$. Trouver les $P \in \mathbb{R}[X]$ tels que, pour toute matrice $A \in \mathcal{O}_n(\mathbb{R})$, la matrice $P(A)$ soit aussi orthogonale.

Corrigé : 1. Soit $A \in \mathcal{A}_n(\mathbb{R})$, $\lambda \in \mathbb{C}$ et $X \in \mathcal{M}_{n,1}(\mathbb{C}) \setminus \{0\}$ telle que $AX = \lambda X$. En conjuguant puis multipliant par X^\top à gauche, on obtient

$$X^\top A \bar{X} = \bar{\lambda} X^\top \bar{X}$$

Puis, si on transpose l'égalité $AX = \lambda X$ et qu'on multiplie à droite par \bar{X} , il vient

$$-X^\top A \bar{X} = \lambda X^\top \bar{X}$$

Et en sommant ces deux égalités il vient

$$(\lambda + \bar{\lambda})X^\top \bar{X} = 0 \quad \text{avec} \quad X^\top \bar{X} = \sum_{i=1}^n |x_i|^2 > 0$$

On en déduit $\text{Sp}_{\mathbb{C}}(A) \subset i\mathbb{R}$. En considérant la matrice $\text{diag}(\alpha \mathbb{R}(\pi/2), 0, \dots, 0)$ avec α réel, on en déduit que $i\alpha$ peut être valeur propre d'une matrice antisymétrique et donc tout imaginaire pur est valeur propre d'une matrice antisymétrique. Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ tel que $P(M) \in \mathcal{A}_n(\mathbb{R})$ pour toute matrice M antisymétrique. Avec α réel et $A \in \mathcal{A}_n(\mathbb{R})$ tel que $i\alpha \in \text{Sp}_{\mathbb{C}}(A)$, il vient

$$P(i\alpha) = \sum_{k=0}^{+\infty} a_{2k} (-1)^k \alpha^{2k} + i \sum_{k=0}^{+\infty} a_{2k+1} (-1)^k \alpha^{2k+1}$$

Comme $P(i\alpha) \in \text{Sp}_{\mathbb{C}}(P(A))$, il s'ensuit que $P(i\alpha) \in i\mathbb{R}$ ce qui prouve que le polynôme $\sum_{k=0}^{+\infty} a_{2k} (-1)^k X^{2k}$ admet α comme racine et ceci pour tout α réel ce qui signifie donc une infinité de racines et par conséquent la nullité de $\sum_{k=0}^{+\infty} a_{2k} (-1)^k X^{2k}$. On en déduit que le polynôme P est impair et la réciproque est immédiate par transposition. On conclut

Les polynômes impairs sont les polynômes $P \in \mathbb{R}[X]$ vérifiant $P(\mathcal{A}_n(\mathbb{R})) \subset \mathcal{A}_n(\mathbb{R})$.

2. Soit $A \in \mathcal{O}_n(\mathbb{R})$. Soit $\lambda \in \text{Sp}_{\mathbb{C}}(A)$ et $X \in \mathcal{M}_{n,1}(\mathbb{C}) \setminus \{0\}$ tel que $AX = \lambda X$. En conjuguant puis transposant, on a $\bar{X}^\top A^\top = \bar{\lambda} \bar{X}^\top$ puis

$$\bar{X}^\top A^\top A X = \bar{\lambda} \lambda \bar{X}^\top X \quad \text{et} \quad \bar{X}^\top A^\top A X = \bar{X}^\top X \quad \text{avec} \quad \bar{X}^\top X = \sum_{i=1}^n |x_i|^2 > 0$$

d'où $|\lambda|^2 = 1$. Autrement dit, on a $\text{Sp}_{\mathbb{C}}(A) \subset \mathbb{U}$. En considérant la matrice $\text{diag}(\mathbb{R}(\theta), I_{n-2})$ avec θ réel, on en déduit que $e^{i\theta}$ est valeur propre d'une matrice orthogonale et donc tout élément de \mathbb{U} est valeur propre d'une matrice orthogonale. Soit $P \in \mathbb{R}[X]$ tel que $P(M)$ soit orthogonale pour toute matrice M orthogonale. Pour $z \in \mathbb{U}$ et $A \in \mathcal{O}_n(\mathbb{R})$ tel que $z \in \text{Sp}_{\mathbb{C}}(A)$, il vient $P(z) \in \text{Sp}_{\mathbb{C}}(P(A))$ d'où $P(z) \in \mathbb{U}$ et par conséquent $P(\mathbb{U}) \subset \mathbb{U}$. Soit $d = \deg P$. On a

$$\forall \theta \in \mathbb{R} \quad P(e^{i\theta})P(e^{-i\theta}) = 1$$

d'où $\forall \theta \in \mathbb{R} \quad P(e^{-i\theta})e^{id\theta}P(e^{-i\theta}) = e^{id\theta}$

ce qui prouve que le polynôme $P - X^d P(1/X) - X^d$ admet une infinité de racines et est donc le polynôme nul. On en déduit que P divise X^d et comme $d = \deg P$, il vient $P = \pm X^d$. La réciproque est immédiate et on conclut

Les polynômes $\pm X^d$ sont les polynômes $P \in \mathbb{R}[X]$ vérifiant $P(\mathcal{O}_n(\mathbb{R})) \subset \mathcal{O}_n(\mathbb{R})$.

Exercice 18 (Mines 2016)

Soit $(u_n)_{n \geq 1}$ une suite de réels définis par $u_1 > 0$ et

$$\forall n \geq 1 \quad u_{n+1} = u_n + \frac{1}{n^\alpha u_n}$$

avec $\alpha > 0$.

1. Discuter de la convergence de $(u_n)_{n \geq 1}$ en fonction de α .
2. Si $(u_n)_{n \geq 1}$ est convergente de limite ℓ , déterminer un équivalent simple de $u_n - \ell$ pour $n \rightarrow +\infty$.
3. Préciser un équivalent simple de u_n pour $n \rightarrow +\infty$ si $(u_n)_{n \geq 1}$ diverge.

Corrigé : 1. La suite $(u_n)_{n \geq 1}$ est clairement à termes positifs et clairement croissante. On a

$$\forall n \geq 1 \quad u_{n+1}^2 = u_n^2 + \frac{2}{n^\alpha} + \frac{1}{n^{2\alpha} u_n^2}$$

d'où
$$u_{n+1}^2 - u_n^2 \underset{n \rightarrow +\infty}{\sim} \frac{2}{n^\alpha}$$

La suite $(u_n)_{n \geq 1}$ est de même nature que la suite $(u_n^2)_{n \geq 1}$ qui est de même nature que la série télescopique $\sum [u_{n+1}^2 - u_n^2]$ d'où, par critère de Riemann

La suite $(u_n)_{n \geq 1}$ converge si et seulement si $\alpha > 1$.

2. Supposons $\alpha > 1$. Par sommation des relations de comparaison, on a

$$\sum_{k=n}^{+\infty} [u_{k+1}^2 - u_k^2] = \ell^2 - u_n^2 \underset{n \rightarrow +\infty}{\sim} \sum_{k=n}^{+\infty} \frac{2}{k^\alpha}$$

Par comparaison série/intégrale, on a

$$\sum_{k=n}^{+\infty} \frac{2}{k^\alpha} \underset{n \rightarrow +\infty}{\sim} \int_n^{+\infty} \frac{2dt}{t^\alpha} = \frac{2}{(\alpha - 1)n^{\alpha-1}}$$

et
$$\ell^2 - u_n^2 = (\ell - u_n)(\ell + u_n) \underset{n \rightarrow +\infty}{\sim} 2\ell(\ell - u_n)$$

D'où

$$u_n - \ell \underset{n \rightarrow +\infty}{\sim} \frac{1}{(1 - \alpha)\ell n^{\alpha-1}}$$

3. Pour $\alpha \in]0; 1[$, on a par sommation des relations de comparaison et comparaison série/intégrale

$$\sum_{k=1}^{n-1} [u_{k+1}^2 - u_k^2] = u_n^2 - u_1^2 \underset{n \rightarrow +\infty}{\sim} \sum_{k=1}^{n-1} \frac{2}{k^\alpha} \underset{n \rightarrow +\infty}{\sim} \int_1^n \frac{2dt}{t^\alpha}$$

On conclut

$$u_n \underset{n \rightarrow +\infty}{\sim} \sqrt{\frac{2}{1 - \alpha}} n^{\frac{1-\alpha}{2}} \quad \text{si } \alpha \in]0; 1[\quad \text{et } \sqrt{2 \ln n} \quad \text{si } \alpha = 1$$