

Corrigé du devoir en temps libre n°17

Problème I

1. Soit $E = \mathbb{R}^n$ que l'on s'autorise à confondre avec $\mathcal{M}_{n,1}(\mathbb{R})$ et qu'on munit de sa structure euclidienne canonique. La matrice M_0 est symétrique réelle donc diagonalisable d'après le théorème spectral. Notant U la colonne de $\mathcal{M}_{n,1}(\mathbb{R})$ constituée de 1, on a $M_1 U = nU$. La matrice M_1 est de rang égal à 1 avec pour $X \in \mathcal{M}_{n,1}(\mathbb{R})$ et

$$M_1 X = 0 \iff \sum_{i=1}^n x_i = 0 \iff X \in \text{Vect}(U)^\perp$$

et par conséquent $\text{Ker } M_1 = E_0(M_1)$ est un hyperplan de E . Ainsi, on a

$$\{0, n\} \subset \text{Sp}(M_1) \quad E_0(M_1) = \text{Vect}(U)^\perp \quad \text{Vect}(U) \subset E_n(M_1)$$

et pour raison de dimension, les inclusions qui précèdent sont des égalités. On dispose de $P \in \mathcal{O}_n(\mathbb{R})$ telle que $P^\top M_1 P = \text{diag}(n, 0, \dots, 0)$. Par suite

$$M_0 = M_1 - I_n = P \text{diag}(n-1, -1, \dots, -1) P^\top$$

pour cette même matrice de passage P d'où

$$\boxed{\text{Sp}(M_0) = \{-1, n-1\} \quad E_{-1}(M_0) = \text{Vect}(U)^\perp \quad E_{n-1}(M_0) = \text{Vect}(U)}$$

2. Soit x réel. On a

$$M_x = xI_n + M_0 = xI_n + P \text{diag}(n-1, -1, \dots, -1) P^\top = P \text{diag}(x+n-1, x-1, \dots, x-1) P^\top$$

d'où

$$\det(M_x) = (x+n-1)(x-1)^{n-1}$$

Par ailleurs, on a

$$\det(M_x) = \begin{vmatrix} x & 1 & \dots & 1 \\ 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & x \end{vmatrix} = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n (M_x)_{i, \sigma(i)}$$

avec $\forall \sigma \in S_n \quad \forall i \in \llbracket 1; n \rrbracket \quad (M_x)_{i, \sigma(i)} = \begin{cases} 1 & \text{si } \sigma(i) \neq i \\ x & \text{si } \sigma(i) = i \end{cases}$

d'où $\forall \sigma \in S_n \quad \prod_{i=1}^n (M_x)_{i, \sigma(i)} = x^{\nu(\sigma)}$

Ainsi

$$\boxed{\forall x \in \mathbb{R} \quad \sum_{\sigma \in S_n} \varepsilon(\sigma) x^{\nu(\sigma)} = (x-1)^{n-1}(x+n-1)}$$

3. En particulier, pour $x = 1$, on trouve

$$\boxed{\sum_{\sigma \in S_n} \varepsilon(\sigma) = 0}$$

Par dérivation d'applications polynomiales, en considérant $0 \times \dots = 0$ par évaluation « paresseuse », il vient

$$\forall x \in \mathbb{R} \quad \sum_{\sigma \in S_n} \varepsilon(\sigma) \nu(\sigma) x^{\nu(\sigma)-1} = (n-1)(x-1)^{n-2}(x+n-1) + (x-1)^{n-1}$$

D'où pour $x = 1$

$$\boxed{\sum_{\sigma \in S_n} \varepsilon(\sigma) \mu(\sigma) = 2\delta_{n,2}}$$

Pour x réel, on a $\sum_{\sigma \in S_n} \varepsilon(\sigma) x^{\nu(\sigma)} = (x-1)^n + n(x-1)^{n-1}$

et par intégration en utilisant la linéarité de l'intégrale

$$\begin{aligned} \sum_{\sigma \in S_n} \frac{\varepsilon(\sigma)}{1 + \nu(\sigma)} x^{\nu(\sigma)+1} &= \int_0^x \sum_{\sigma \in S_n} \varepsilon(\sigma) t^{\nu(\sigma)} dt \\ &= \int_0^x [(t-1)^n + n(t-1)^{n-1}] dt = \frac{(x-1)^{n+1}}{n+1} + (x-1)^n - (-1)^n \frac{n}{n+1} \end{aligned}$$

Ainsi, pour $x = 1$

$$\boxed{\sum_{\sigma \in S_n} \frac{\varepsilon(\sigma)}{1 + \nu(\sigma)} = (-1)^{n-1} \frac{n}{n+1}}$$

Problème II

1. On a $I_n \in GL_n(\mathbb{Z})$. Pour $M \in GL_n(\mathbb{Z})$, on a $M^{-1} \in GL_n(\mathbb{Z})$ puisque $M^{-1} \in GL_n(\mathbb{R})$ et M^{-1} ainsi que $(M^{-1})^{-1} = M$ sont à coefficients dans $\mathbb{Z}$. Enfin, pour $(M, N) \in GL_n(\mathbb{Z})^2$, on a M et N dans $GL_n(\mathbb{R})$ d'où $MN \in GL_n(\mathbb{R})$ puis MN et $(MN)^{-1} = N^{-1}M^{-1}$ à coefficients dans $\mathbb{Z}$ par définition du produit matriciel et la structure d'anneau de $(\mathbb{Z}, +, \times)$. On conclut

$\boxed{\text{L'ensemble } GL_n(\mathbb{Z}) \text{ est un sous-groupe de } (GL_n(\mathbb{R}), \times) \text{ d'où une structure de groupe induite.}}$

2. Le polynôme scindé à racines simples $X^d - 1 = \prod_{k=0}^{d-1} (X - e^{\frac{2ik\pi}{d}})$ est annulateur de M . On en déduit qu'il existe $P \in GL_n(\mathbb{C})$ telle que $M = PDP^{-1}$ avec $P = \text{diag}(\omega^0, \dots, \omega^{d-1})$ où $\omega = e^{\frac{2i\pi}{d}}$. Par suite, on a

$$\forall k \in \mathbb{N} \quad P^{-1}AP = \text{diag}\left(\frac{\omega^k - 1}{3}\right)_{0 \leq k \leq d-1}$$

Or $\forall k \in \mathbb{N} \quad \left| \frac{\omega^k - 1}{3} \right| \leq \frac{|\omega^k| + |1|}{3} = \frac{2}{3}$

d'où $\text{diag}\left(\frac{\omega^k - 1}{3}\right)_{0 \leq k \leq d-1} \xrightarrow{k \rightarrow \infty} 0$

et par continuité du produit matriciel, on conclut

$$\boxed{A^k \xrightarrow{k \rightarrow \infty} 0}$$

3.(a) Par définition du produit matriciel dans $\mathcal{M}_n(\mathbb{Z})$ et par compatibilité de l'addition et de la multiplication avec la relation de congruence

$\boxed{\text{L'application } \varphi \text{ est un morphisme d'anneaux.}}$

3.(b) Il en résulte que l'application φ induit un morphisme φ^* de groupes multiplicatifs entre les inversibles des anneaux de départ et d'arrivée, à savoir de $(\text{GL}_n(\mathbb{Z}), \times)$ sur $(\text{GL}_n(\mathbb{F}_3), \times)$ et qui induit lui-même un morphisme de groupes multiplicatifs de $(G, \times)$ sur $(\varphi(G), \times)$. Soit $M \in G \cap \text{Ker } \varphi^*$. On a $\varphi(M) = \varphi(I_n)$ d'où $\varphi(M - I_n) = 0$ puis $M - I_n \in 3\mathcal{M}_n(\mathbb{Z})$ et on peut donc poser

$$A = \frac{M - I_n}{3} \in \mathcal{M}_n(\mathbb{Z})$$

Notant d l'ordre du groupe G , on a $M^d = I_n$ et d'après le résultat de la question précédente, il vient $A^k \xrightarrow[k \rightarrow \infty]{} 0$. Or, la suite de matrices $(A^k)_k$ est à valeurs dans $\mathcal{M}_n(\mathbb{Z})$ et convergente donc stationnaire. On en déduit que $A^k = 0$ à partir d'un certain rang. Il en résulte que la matrice A est à la fois nilpotente et diagonalisable donc nulle et par conséquent

$$G \cap \text{Ker } \varphi^* = \{I_n\}$$

Ainsi

Le morphisme d'anneaux φ induit un isomorphisme de groupes de $(G, \times)$ sur son image.

3.(c) On en déduit $\text{Card } G = \text{Card } \varphi(G) \leq \text{Card } \mathcal{M}_n(\mathbb{F}_3)$

Et on conclut

$$\text{Card } G \leq 3^{n^2}$$

Problème III

1. Soit n entier non nul. Pour $(a, b) \in \llbracket 1; n \rrbracket^2$, le pgcd $a \wedge b$ est un diviseur de a et b donc un nombre dans $\llbracket 1; n \rrbracket$ et celui-ci est unique. Par conséquent, on a bien l'union disjointe

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

Pour $k \in \llbracket 1; n \rrbracket$ et $(a, b) \in \llbracket 1; n \rrbracket^2$, on dispose d'un unique couple (a', b') d'entiers non nuls tels que $a = a'k$, $b = b'k$ et $a' \wedge b' = 1$. On observe en particulier

$$1 \leq a' = \frac{a}{k} \leq \left\lfloor \frac{n}{k} \right\rfloor \quad \text{et} \quad 1 \leq b' = \frac{b}{k} \leq \left\lfloor \frac{n}{k} \right\rfloor$$

Ainsi, il vient pour $k \in \llbracket 1; n \rrbracket$

$$\text{Card } \{(a, b) \in \llbracket 1; n \rrbracket^2 \mid a \wedge b = k\} = \text{Card } \left\{ (a', b') \in \llbracket 1; \left\lfloor \frac{n}{k} \right\rfloor \rrbracket^2 \mid a' \wedge b' = 1 \right\}$$

Et par union disjointe, on conclut

$$\forall n \in \mathbb{N}^* \quad n^2 = \sum_{k=1}^n \text{Card } \Lambda \left(\left\lfloor \frac{n}{k} \right\rfloor \right) = \sum_{k=1}^n P \left(\left\lfloor \frac{n}{k} \right\rfloor \right)$$

2. On a $\left\lfloor \frac{x}{a} \right\rfloor \leq \frac{x}{a}$ puis $\frac{\lfloor x/a \rfloor}{b} \leq \frac{x}{ab}$

et par croissance de la partie entière $\left\lfloor \frac{\lfloor x/a \rfloor}{b} \right\rfloor \leq \left\lfloor \frac{x}{ab} \right\rfloor$

Ensuite, on a $\left\lfloor \frac{x}{ab} \right\rfloor \leq \frac{x}{ab}$ puis $\left\lfloor \frac{x}{ab} \right\rfloor b \leq \frac{x}{a}$

Par croissance de la partie entière, il vient

$$\left\lfloor \frac{x}{ab} \right\rfloor b \leq \left\lfloor \frac{x}{a} \right\rfloor \quad \text{d'où} \quad \left\lfloor \frac{x}{ab} \right\rfloor \leq \frac{\lfloor x/a \rfloor}{b}$$

et de nouveau par croissance de la partie entière

$$\left\lfloor \frac{x}{ab} \right\rfloor \leq \left\lfloor \frac{\lfloor x/a \rfloor}{b} \right\rfloor$$

On conclut

$$\boxed{\forall (x, a, b) \in \mathbb{R} \times (\mathbb{N}^*)^2 \quad \left\lfloor \frac{x}{ab} \right\rfloor = \left\lfloor \frac{\lfloor x/a \rfloor}{b} \right\rfloor}$$

3. Le cas $n = 1$ est immédiat. Soit n entier ≥ 2 . On note $p_1, \dots, p_r$ ses facteurs premiers. Comme la fonction μ s'annule en présence d'un facteur premier au carré, il vient

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

On conclut

$$\boxed{\forall n \in \mathbb{N}^* \quad \sum_{d|n} \mu(d) = \delta_{n,1}}$$

4. Soit n entier non nul. On a

$$\sum_{k=1}^n P\left(\left\lfloor \frac{n}{k} \right\rfloor\right) \left(\sum_{d|k} \mu(d) \right) = \sum_{k=1}^n P\left(\left\lfloor \frac{n}{k} \right\rfloor\right) \delta_{k,1} = P(n)$$

Puis, on obtient

$$P(n) = \sum_{(k,d) \in \llbracket 1; n \rrbracket^2, d|k} P\left(\left\lfloor \frac{n}{k} \right\rfloor\right) \mu(d)$$

On somme alors par paquets en posant $k = \ell d$ avec $\ell d \leq n$. Il vient

$$P(n) = \sum_{(d,\ell) \in \llbracket 1; n \rrbracket^2, \ell d \leq n} P\left(\left\lfloor \frac{n}{\ell d} \right\rfloor\right) \mu(d) = \sum_{d=1}^n \mu(d) \left(\sum_{\ell=1}^{\lfloor \frac{n}{d} \rfloor} P\left(\left\lfloor \frac{n}{\ell d} \right\rfloor\right) \right)$$

Avec les égalités établies aux questions 2 et 1, il vient

$$P(n) = \sum_{d=1}^n \mu(d) \left(\sum_{\ell=1}^{\lfloor \frac{n}{d} \rfloor} P\left(\left\lfloor \frac{\lfloor n/\ell \rfloor}{d} \right\rfloor\right) \right) = \sum_{d=1}^n \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2$$

Ainsi

$$\boxed{M = P}$$

5. On considère le recouvrement disjoint $(I_p)_{p \geq 1}$ de $(\mathbb{N}^*)^2$ défini par

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

D'après le théorème de Fubini et le théorème de sommation par paquets pour des familles sommables, il vient

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

Ainsi

$$\boxed{\left(\sum_{n=1}^{+\infty} \frac{1}{n^2} \right) \left(\sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2} \right) = 1}$$

6. Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé avec n entier non nul et $X^{(n)}, Y^{(n)}$ des variables aléatoires indépendantes de loi uniforme $\mathcal{U}_{\llbracket 1; n \rrbracket}$. On a

$$r_n = \mathbb{P}(X^{(n)} \wedge Y^{(n)} = 1) = \sum_{(a,b) \in \Lambda(n)} \mathbb{P}(X^{(n)} = a, Y^{(n)} = b) = \frac{P(n)}{n^2} = \sum_{d=1}^n \mu(d) \frac{1}{n^2} \left\lfloor \frac{n}{d} \right\rfloor^2$$

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

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

On conclut

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

Expérimentation numérique

On saisit :

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

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 $\mathcal{U}_{[1;n]}$. On implémente une méthode de *Monte-Carlo* avec l'estimation

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

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()
```

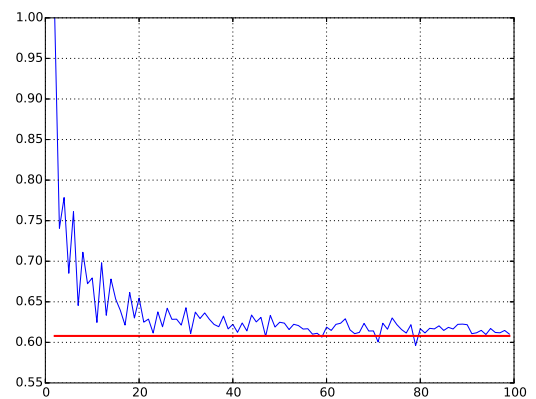


FIGURE 1 – Approximation stochastique de $(r_n)_n$