PSI* 2025/26 DL 5

"Probabilité" d'être premiers entre eux

- On note $p_1 = 2 < p_2 = 3 < \cdots < p_n < \ldots$ la suite des nombres premiers.
- Rappel : deux nombres entiers sont dits premiers entre eux quand ils n'ont aucun facteur premier en commun.

On trouve sur internet la « démonstration »suivante

Ne pas prendre ce qui suit pour argent comptant....

« La probabilité qu'un entier soit multiple de 2 est $\frac{1}{2}$, la probabilité qu'il soit multiple de 3 est $\frac{1}{3}$, ..., la probabilité qu'il soit multiple de m est $\frac{1}{m}$.

On tire deux nombres X, Y au hasard dans $\mathbb{N}^*$ de façon indépendante et on s'intéresse à l'événement M_k : "X et Y ne pas tous les deux multiples de k". Sa probabilité est donc $\left(1 - \frac{1}{k^2}\right)$.

Lorsqu'on considère les M_{p_i} associés aux nombres premiers p_i successifs, ce sont des événements indépendants. Donc la probabilité que deux entiers pris au hasard dans $\mathbb{N}^*$ soient premiers entre eux vaut

$$\rho = \prod_{p \text{ premier}} \left(1 - \frac{1}{p^2}\right) = \left(\sum_{n=1}^{+\infty} \frac{1}{n^2}\right)^{-1} = \frac{6}{\pi^2}. \qquad \text{»}$$

Qu'est-ce qui est vrai ?

Les deux dernières égalités sont correctes :

- on a vu en exercice la formule d'Euler reliant $\zeta(k)$ à un produit infini.
- par ailleurs il existe plusieurs démonstrations classiques de $\zeta(2) = \frac{\pi^2}{6}$. On pourra l'admettre ici, sauf ceux qui veulent faire la preuve en annexe.

On va s'interroger sur la pertinence des autres affirmations.

Et par ailleurs on se servira du fait suivant, aussi vu en exercice : la série $\sum \frac{1}{p_k}$ est divergente. On le considère ici comme admis.

1. Une probabilité équitable sur $\mathbb{N}$?

On note $A_n = \{kn, k \in \mathbb{N}^*\}$. On suppose qu'il existe une structure d'espace probabilisé $(\mathbb{N}^*, \mathcal{A}, \mathbb{P})$ sur $\mathbb{N}^*$ vérifiant pour tout $n \in \mathbb{N}^*$, $A_n \in \mathcal{A}$ et $\mathbb{P}(A_n) = \frac{1}{n}$.

On note

$$A = \bigcap_{s \in \mathbb{N}^*} \bigcup_{\ell \geq s} A_{p_\ell}$$

a. Montrer que A est un événement. Identifier clairement cet ensemble, en déduire sa probabilité.

b. Montrer que les événements $(A_{p_i})_{i\in\mathbb{N}^*}$ sont indépendants.

c. Montrer que pour touts entiers m et s tels que $1 \leq s \leq m$, on a

$$\mathbb{P}\left(\bigcup_{i=s}^{m} A_{p_i}\right) \geq 1 - \exp\left(-\sum_{i=s}^{m} \mathbb{P}(A_{p_i})\right)$$

d. En déduire $\mathbb{P}(A) = 1$. Que conclure concernant la démonstration proposée ?

2. Le problème en version probabilité finie

On aura besoin d'une notation issue de l'arithmétique. On rappelle le théorème fondamental de décomposition : tout entier naturel $n \geq 2$ s'écrit de façon unique sous la forme

$$n = q_1^{m_1} q_2^{m_2} \dots q_s^{m_s}$$

avec $q_1 < q_2 < \dots < q_s$ des nombres premiers et des exposants m_i dans $\mathbb{N}^*$.

• On définit alors la notation suivante (fonction de Möbius) :

$$\mu(1) = 1, \qquad \text{et si } n \geq 2, \qquad \mu(n) = \begin{cases} 0 & \text{si un des exposants } m_i \geq 2 \\ (-1)^s & \text{si tous les } m_i \text{ valent 1} \end{cases}$$

A titre d'exemple, voici le calcul des valeurs $\mu(k)$ pour $10 \leq k \leq 20$

k	10	11	12	13	14	15	16	17	18	19	20
Décomposition de k	2.5	11	$2^2.3$	13	2.7	3.5	2^4	17			
$\mu(k)$	1	-1	0	-1	1	1	0	-1			

Soit un entier $n \geq 2$ fixé. On modélise un tirage au hasard de deux entiers inférieurs à n. On considère pour cela deux variables aléatoires X et Y, indépendantes, suivant la loi uniforme $\mathcal{U}(n)$.
Soit un entier $v \leq n$. On note A_v l'événement "X est un multiple de v".

a. Compléter les cases manquantes dans le tableau et donner un exemple d'entier $n \geq 2$, non premier,pour lequel $\mu(n) = -1$.

b. Exprimer le cardinal de A_v à l'aide de n et v.

c. Quelle est la probabilité que v divise X et Y ?

d. Montrer que si $q_1, \dots, q_s$ sont des diviseurs premiers de n alors les événements $A_{q_1}, \dots, A_{q_s}$ sont indépendants.

e. Montrer qu'on peut trouver un contre exemple si on ne suppose pas qu'il s'agit de diviseurs de n : on donnera un entier $n \geq 2$ et deux nombres premiers $q_1 \leq n$ et $q_2 \leq n$ tels que A_{q_1} et A_{q_2} ne sont pas indépendants.

• Pour des événements $B_1, \dots, B_p$ d'un espace probabilisé, on rappelle la formule du « crible »

$$\mathbb{P}\left(\bigcup_{i=1}^{p} B_i\right) = \sum_{J\subset[\![1,p]\!], J\neq\emptyset} (-1)^{\mathrm{Card}(J)+1} \mathbb{P}\left(\bigcap_{i\in J} B_i\right)$$

f. On note π_n la probabilité de l'événement "X et Y sont premiers entre eux". Montrer que

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

3. Résolution en cardinal infini

a. Montrer que si $d \leq n$,

$$0 \leq \frac{1}{d^2} - \frac{1}{n^2}\left\lfloor \frac{n}{d} \right\rfloor^2 \leq \frac{2}{dn} - \frac{1}{n^2}$$

b. En déduire que la limite de π_n est $p = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^2}$

c. Montrer que si $n \geq 2$, $\sum_{d \text{ diviseur de } n} \mu(d) = 0$.

d. Justifier la formule suivante : si les séries $\sum a_n$ et $\sum b_n$ convergent absolument,

$$\left(\sum_{n=1}^{+\infty} a_n\right)\left(\sum_{n=1}^{+\infty} b_n\right) = \sum_{n=1}^{+\infty}\left(\sum_{(k,\ell)\in\mathbb{N}^2, k\times\ell=n} a_k b_\ell\right)$$

e. Montrer que

$$p = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}$$

A défaut de probabilité sur $\mathbb{N}$, on a donc fait un calcul de "densité". C'est-à-dire qu'on regarde le problème sur $[\![1,n]\!]$ muni de la probabilité uniforme, suivi d'un calcul de limite. Cette densité est une limite de probabilités et pas une véritable probabilité. Et le calcul, on le voit, peut être difficile.

Annexe : comment trouver la somme des $\frac{1}{n^2}$ ("problème de Bâle") ?

Il y a plusieurs démarches. Lorsque les séries de Fourier étaient au programme, elles fournissaient un des arguments les plus rapides.

Voici les éléments pour une démonstration en termes élémentaires. On utilise la fonction $\operatorname{cotan} x = \frac{1}{\tan x}$.

1. Montrer que pour $0 < x < \frac{\pi}{2}$, on a $0 < \sin x \leq x \leq \tan x$ puis

$$(\operatorname{cotan} x)^2 \leq \frac{1}{x^2} \leq 1 + (\operatorname{cotan} x)^2$$

2. On va calculer $S_n = \sum_{k=1}^{n} \left(\operatorname{cotan} \frac{k\pi}{2n+1}\right)^2$ en utilisant le polynôme $P(X) = \sum_{k=0}^{n} (-1)^k \binom{2n+1}{2k+1} X^{n-k}$.

a. Prouver que $x_k = \left(\operatorname{cotan} \frac{k\pi}{2n+1}\right)^2$ est une racine de P.

Pour cela , on peut utiliser le développement de $\sin((2n+1)t) = \mathfrak{Im}\left((\cos t + i \sin t)^{2n+1}\right)$

b. En déduire S_n.

3. Conclure par encadrement et passage à la limite.