Probabilité que eux entiers soient premiers entre eux

Léo Gayral

2017-2018

ref : FGN – Oraux X-ENS, Algèbre 1 – p.156

Définition 1 (Fonction de Möbius)**.** Pour un nombre premier p, on définit la valuation p-adique par $\nu_p(n) = \max\{k \in \mathbb{N}, n \in p^k\mathbb{N}\} < \infty$.

Soit $\mu(n) := \begin{cases} (-1)^r & \text{si} \quad \forall p, \nu_p(n) \leq 1 \quad \text{et} \quad n = p_1 \times \cdots \times p_r \\ 0 & \text{si} \quad \exists p, \nu_p(n) \geq 2 \end{cases}$ la fonction de Möbius, définie sur $\mathbb{N}^*$. C'est une fonction multiplicative, au sens où si $m \wedge n = 1$, alors $\mu(mn) = \mu(m)\mu(n)$.

Lemme 1. Pour $n \geq 2$, on a $\sum\limits_{d/n} \mu(d) = 0$. En réalité, μ est même entièrement définie par cette relation.

Démonstration.
Soit $n = \prod\limits_{i=1}^{r} p_i^{\alpha_i}$. Tout diviseur d correspond à une unique famille $(\beta_i) \in \mathbb{N}^r$ telle que $\beta_i \leq \alpha_i$. On peut d'office éliminer les familles avec un $\beta_i \geq 2$, pour lesquelles $\mu(d) = 0$. En décomposant la somme selon le nombre de diviseurs premiers distincts de d on a alors :

$$\sum_{d/n} \mu(d) = \sum_{i=0}^{r} \sum_{d = p_{j_1} \cdots p_{j_i} / n} \mu(d) = \sum_{i=0}^{r} \binom{r}{i} \times (-1)^i = (1-1)^r = 0 \ .$$

□

Lemme 2 (Formule du crible)**.** Soient $(U_i)_{1 \leq i \leq k}$ des ensembles finis. On a l'égalité :

$$\#\left(\bigcup_{i=1}^{k} U_i\right) = \sum_{\substack{J \subset [\![1,k]\!] \\ J \neq \emptyset}} (-1)^{|J|+1} \times \#\left(\bigcap_{j \in J} U_j\right) \ .$$

Théorème 1. Soient $A_n := \{(x,y) \in [\![1,n]\!]^2, x \wedge y = 1\}$, et $r_n = \frac{\# A_n}{n^2}$ la probabilité que deux entiers uniformément choisis entre 1 et n soient premiers entre eux. On a alors :

$$r_n = \frac{1}{n^2} \sum_{d=1}^{n} \mu(d) \times \left\lfloor \frac{n}{d} \right\rfloor^2 \underset{n \to \infty}{\longrightarrow} \frac{6}{\pi^2} \ .$$

Démonstration.
On considère $p_1 < \cdots < p_k$ la suite des premiers de $[\![1,n]\!]$. On pose $U_i = [\![1,n]\!]^2 \cap (p_i \mathbb{N})^2$ l'ensemble des couples (a,b) tels que $p_i/(a \wedge b)$, de sorte que $\bigcup\limits_{i=1}^{k} U_i$ et A_n sont complémentaires dans $[\![1,n]\!]^2$.

Pour calculer le cardinal de $\bigcup U_i$, on va utiliser la formule du crible. $\bigcap\limits_{j \in J} U_j$ est l'ensemble des couples (a,b) tels que $d := \left(\prod\limits_{j \in J} p_j\right)$ divise $a \wedge b$, donc $\#\left(\bigcap\limits_{j \in J} U_j\right) = \left\lfloor \frac{n}{d} \right\rfloor^2$. En réinjectant ce résultat dans la formule du crible, on a alors :

$$|A_n| = n^2 - \#\left(\bigcup_{i=1}^{k} U_i\right) = n^2 + \sum_{I \subset [\![1,k]\!], I \neq \emptyset} (-1)^{|I|} \times \left\lfloor \frac{n}{\prod\limits_{i \in I} p_i} \right\rfloor^2 = \sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2 \ .$$

On a donc montré l'égalité sur r_n, reste encore à étudier son comportement asymptotique.

A d fixé, on a $\frac{1}{n^2} \times \left\lfloor \frac{n}{d} \right\rfloor^2 \in \left[\left(\frac{1}{d} - \frac{1}{n}\right)^2, \frac{1}{d^2}\right]$ d'où $\left|\frac{1}{n^2} \times \left\lfloor \frac{n}{d} \right\rfloor - \frac{1}{d^2}\right| \leq \frac{1}{n}\left(\frac{2}{d} + \frac{1}{n}\right)$. Il en découle $\left| r_n - \sum\limits_{d=1}^{n} \frac{\mu(d)}{d^2} \right| \leq \sum\limits_{d=1}^{n} \frac{2}{dn} + \frac{1}{n^2} = O\left(\frac{\ln(n)}{n}\right)$.

On sait que $\sum\limits_{n \in \mathbb{N}} \frac{1}{n^2} = \frac{\pi^2}{6}$. On va donc montrer que $\sum\limits_{n \in \mathbb{N}} \frac{1}{n^2} \times \sum\limits_{d \in \mathbb{N}} \frac{\mu(d)}{d^2} = 1$, ce qui nous permettra de conclure.

La série à deux paramètres $\left(\frac{\mu(d)}{d^2 n^2}\right)_{n,d \in \mathbb{N}}$ est sommable, donc on peut sommer par paquets sur la partition $(\mathbb{N}^*)^2 = \bigsqcup_{i \in \mathbb{N}^*} \{(n,d), nd = i\}$:

$$\sum_{n,d \in \mathbb{N}} \frac{\mu(d)}{d^2 n^2} = \sum_{i \in \mathbb{N}^*} \frac{1}{i^2} \sum_{d/i} \mu(d) = 1$$

$\square$