# Probabilité pour que deux entiers soient premiers entre eux.

Référence : Oraux X-ENS, Algèbre 1.
Serge Francinou, Hervé Gianella, Serge Nicolas

2011-2012

Prérequis :
– fonction de Möbius
– formule du crible

On rappelle la définition de la fonction de Möbius :

**Définition 1**
*La fonction de Möbius est la fonction* $\mu : \mathbb{N}^* \to \mathbb{Z}$ *définie par :*
– $\mu(1) = 1$
– $\mu(p_1 \cdots p_r) = (-1)^r$ *si les* $p_i$ *sont des nombres premiers distincts*
– $\mu(n) = 0$ *sinon (si* $n$ *est divisible par le carré d'un nombre premier).*

On rappelle de plus la formule du crible :

**Proposition 2 : Formule du crible**
*Soient* $E_1, \ldots, E_k$ *des ensembles finis. Alors :*

$$\operatorname{Card}\left(\bigcup_{i=1}^{k} E_i\right) = \sum_{\emptyset \neq I \subseteq [\![1,k]\!]} (-1)^{1+\operatorname{Card} I} \operatorname{Card}\left(\bigcap_{i \in I} E_i\right).$$

On note aussi $r_n$ la probabilité que deux entiers choisis au hasard dans $[\![1,n]\!]$ soient premiers entre eux.

On a alors :

**Théorème 3**
*On a* $\displaystyle\lim_{n\to\infty} r_n = \frac{6}{\pi^2}$.

*Démonstration.* Appellons, pour tout $n \geqslant 1$,

$$A_n = \{(a,b) \in [\![1,n]\!]^2 \mid a \wedge b = 1\}.$$

On a donc $r_n = \frac{\operatorname{Card} A_n}{n^2}$.

On note $p_1, \ldots, p_k$ la liste des nombres premiers inférieurs à $n$, et $U_i = \{(a,b) \in [\![1,n]\!]^2 \mid p_i | a \text{ et } p_i | b\}$.

On a alors l'identité :

$$A_n = \left(\bigcup_{i=1}^{k} U_i\right)^c .$$

**Lemme 4**
*On a*

$$\operatorname{Card} A_n = \sum_{d=1}^{n} \mu(d) E\left(\frac{n}{d}\right)^2 .$$

*Démonstration.* Soit $I \subseteq [\![1, k]\!]$ non vide. Alors le cardinal de l'intersection $\bigcap_{i\in I} U_i$ est exactement égal au nombre de couples de multiples strictement positifs de $\prod_{i\in I} p_i$ inférieurs à $n$ :

$$\operatorname{Card}\left(\bigcap_{i\in I} U_i\right) = E\left(\frac{n}{\prod_{i\in I} p_i}\right)^2 .$$

On peut donc utiliser la formule du crible :

$$\begin{aligned}\operatorname{Card}\left(\bigcup_{i=1}^{k} U_i\right) &= \sum_{\emptyset\neq I\subseteq[\![1,k]\!]} (-1)^{1+\operatorname{Card} I} \operatorname{Card}\left(\bigcap_{i\in I} U_i\right) \\ &= \sum_{\emptyset\neq I\subseteq[\![1,k]\!]} (-1)^{1+\operatorname{Card} I} E\left(\frac{n}{\prod_{i\in I} p_i}\right)^2\end{aligned}$$

Donc on a :

$$\begin{aligned}\operatorname{Card} A_n &= n^2 - \sum_{\emptyset\neq I\subseteq[\![1,k]\!]} (-1)^{1+\operatorname{Card} I} E\left(\frac{n}{\prod_{i\in I} p_i}\right)^2 \\ &= \sum_{d=1}^{n} \mu(d) E\left(\frac{n}{d}\right)^2\end{aligned}$$

En effet : on veut ne garder dans la somme que les produits de nombres premiers distincts, d'où le $\mu(d)$ pour "enlever" les autres, et $n^2$ correspond à $d = 1$.

D'où le résultat. ◊

On peut en déduire immédiatement que

$$r_n = \frac{1}{n^2} \sum_{d=1}^{n} \mu(d) E\left(\frac{n}{d}\right)^2 .$$

L'intuition nous indique ici de remplacer le terme $\frac{1}{n^2} E\left(\frac{n}{d}\right)^2$ par son équivalent $\frac{1}{d^2}$ (on commence à voir apparaître $\zeta(2)\ldots$).

On estime la différence entre les deux sommes :

$$\left| r_n - \sum_{d=1}^{n} \frac{\mu(d)}{d^2} \right| = \left| \sum_{d=1}^{n} \mu(d) \left( \frac{1}{n^2} E\left(\frac{n}{d}\right)^2 - \frac{1}{d^2} \right) \right| .$$

On remarque que $E(n/d) > n/d - 1$, et donc on a :

$$\frac{1}{n^2} - \frac{2}{dn} < \frac{1}{n^2} E\left(\frac{n}{d}\right)^2 - \frac{1}{d^2} \leqslant 0.$$

Donc, par inégalité triangulaire :

$$\begin{aligned}
\left| r_n - \sum_{d=1}^{n} \frac{\mu(d)}{d^2} \right| &\leqslant \sum_{d=1}^{n} \left( \frac{2}{dn} + \frac{1}{n^2} \right) \\
&\leqslant \frac{2}{n} \sum_{d=1}^{n} \frac{1}{d} + \frac{1}{n} \\
&= \mathcal{O}\left( \frac{\log n}{n} \right)
\end{aligned}$$

Ainsi, on a l'identité :

$$\lim_{n \to \infty} r_n = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}.$$

Calculons cette somme. Pour cela, calculons à tout hasard

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \times \sum_{n=1}^{\infty} \frac{1}{n^2}.$$

Les deux séries convergent absolument, et donc, par théorème de Fubini :

$$\begin{aligned}
\left( \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \right) \left( \sum_{n=1}^{\infty} \frac{1}{n^2} \right) &= \sum_{d,n \geqslant 1} \frac{\mu(d)}{(dn)^2} \\
&= \sum_{d \geqslant 1,\ d|k} \frac{\mu(d)}{k^2} \\
&= \sum_{k \geqslant 1} \sum_{d|k} \frac{\mu(d)}{p^2} \\
&= \sum_{k \geqslant 1} \frac{1}{k^2} \left( \sum_{d|k} \mu(d) \right)
\end{aligned}$$

Il ne nous manque ici plus qu'un petit lemme sur la fonction de Möbius :

**Lemme 5**
*On a*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \geqslant 2. \end{cases}$$

*Démonstration.* Notons $S(n)$ la somme considérée. Il est clair que $S(1) = 1$. Soit donc $n \geqslant 2$, et considérons sa décomposition en facteurs premiers :

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

où les $p_i$ sont des nombres premiers distincts, et $\alpha_i$ des entiers strictements positifs.

Les seuls termes non nuls dans $S(n)$ sont des produits de $p_i$, sans multiplicités. Pour chaque $j$, $n$ a exactement $C_k^j$ diviseurs de cette forme, produits de $i$ $p_j$. D'où

$$
\begin{aligned}
S(n) &= \sum_{j=0}^{k} C_k^j (-1)^j \\
&= (1-1)^k \\
&= 0
\end{aligned}
$$

$\Diamond$

On conclut avec le lemme, et la bien connue valeur de $\zeta(2)$. $\square$