Références :
Exercice de mathématiques pour l'agrégation, Serge Francinou

Déf. On définit la **fonction de Mobius** μ par

$$\begin{cases} \mu(1) = 1 \\ \mu(n) = 0 \text{ si } n \text{ est divisible par le carré d'un nombre premier} \\ \mu(p_1...p_r) = (-1)^r \text{ si les } p_i \text{ sont premiers et deux à deux distincts.} \end{cases}$$

Prop. *On a*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \ si \ n = 1 \\ 0 \ si \ n > 1 \end{cases}$$

Démonstration. Posons $S(n) = \sum_{d|n} \mu(d)$.
Calculons maintenant $S(n)$ pour $n \in \mathbb{N}^*$. On a, tout d'abord, que $S(1) = 1$. Soit $n \geq 2$ et soit sa décomposition en facteurs premiers $n = \prod_{i=1}^k p_i^{\alpha_i}$ où $p_1, ..., p_k$ sont des nombres premiers distincts et $\alpha_1, ..., \alpha_k$ des entiers strictement positifs.
Les seuls diviseurs d de n pour lesquels $\mu(d)$ est non nul sont les produits de nombres premiers distincts pris parmi $p_1, ..., p_k$. Pour un tel diviseur, on a $\mu(d) = (-1)^i$ où i est le nombre de diviseurs premiers de d. Or n possède $\binom{k}{i}$ diviseurs d à un i fixés. On a donc

$$S(n) = \sum_{i=0}^{k} \binom{k}{i} (-1)^i = (1-1)^k = 0.$$

□

Prop. *Soit $f : \mathbb{N}^* \to \mathbb{R}$. Si on pose*

$$\begin{array}{rcl} g : \mathbb{N}^* & \longrightarrow & \mathbb{R} \\ n & \longmapsto & \displaystyle\sum_{d|n} f(d) \end{array}$$

alors, pour tout $n \geq 1$,

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Démonstration. Soit $n \geq 1$. On a

$$\begin{aligned} \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{n|d} \mu(d) \left(\sum_{d'|\frac{n}{d}} f(d') \right) \\ &= \sum_{d'|n} f(d') \left(\sum_{d|\frac{n}{d'}} \mu(d) \right) \\ &= f(n) \text{ par la proposition précédente} \end{aligned}$$

□

Prop. *Soit $\mathbb{F}_q$ un corps fini de cardinal q (puissance d'un nombre premier). Pour tout $n \in \mathbb{N}^*$, il existe un polynôme irréductible sur $\mathbb{F}_q$ de degré n. Le nombre de tels polynômes est équivalent à $\frac{q^n}{n}$ lorsque $n \to \infty$.*

Démonstration. Soit $n \in \mathbb{N}^*$, on note $A(n, q)$ l'ensemble des polynômes de $\mathbb{F}_q[X]$ irréductibles unitaires et de degré n et $I(n, q) = \text{Card}(A(n, q))$.

- Montrons que

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P = \prod_{\substack{\{P \in \mathbb{F}_q[X], \deg(P)|n \\ \text{et } P \in A(\deg(P),q)\}}} P.$$

Comme $\mathbb{F}_q[X]$ est factoriel, on peut écrire la décomposition en facteurs premiers de $X^{q^n} - X$ et comme les racines dans $\mathbb{F}_{q^n}$ de $X^{q^n} - X$ sont simples, tous les polynômes irréductibles sont différents et vont apparaître une fois dans la décomposition de $X^{q^n} - X$.

$$X^{q^n} - X = \prod_{\substack{\{Q \text{ facteur} \\ \text{irréductible} \\ \text{de } X^{q^n} - X\}}} Q.$$

On veut donc montrer que

$$\underbrace{\{Q \text{ facteur irréductible de } X^{q^n} - X\}}_{A} = \underbrace{\{P \in \mathbb{F}_q[X], \deg(P)|n \text{ et } P \in A(\deg(P), q)\}}_{B}$$

- ▶ Soit $P \in B$. Montrons que P divise $X^{q^n} - X$.
  Soit $K = \mathbb{F}_q[X]/(P) = \mathbb{F}_q(x)$ un corps de rupture de P où x est une racine de P (comme P est irréductible, il est unique à isomorphisme de $\mathbb{F}_q$ algèbre près) Comme P est irréductible, à coefficients dans $\mathbb{F}_q$, unitaire et annulateur pour x, alors P est le polynôme minimal de x. On a $[K : \mathbb{F}_q] = \deg(P) = d$. Par unicité des corps finis, on a donc que K est isomorphe à $\mathbb{F}_{q^d}$. On sait que $\mathbb{F}_{q^d} = \{\text{racines de } X^{q^d} - X\}$.

  > En effet, soit $a \in \mathbb{F}_{q^d}^*$ alors $a^{q^d-1} = 1$ et donc $a^{q^d} = a$. Ainsi, $\mathbb{F}_{q^d}^* \subset \{\text{racines de } X^{q^d} - X\}$. De plus, $O \in \{\text{racines de } X^{q^d} - X\}$, donc $\mathbb{F}_{q^d}^* \subset \{\text{racines de } X^{q^d} - X\}$ et comme $\mathrm{Card}(\{\text{racines de } X^{q^d} - X\}) \leq q^d$, on a bien l'égalité.

  On a donc, en particulier, $x^{q^d} = x$. Comme $d|n$, on a

  $$x^{q^n} = \underbrace{\left(...(x^{q^d})^{q^d}...\right)^{q^d}}_{\frac{n}{d} \text{ fois}} = \underbrace{\left(...(x^{q^d})^{q^d}...\right)^{q^d}}_{\frac{n}{d}-1 \text{ fois}} = ... = x^{q^d} = x$$

  On a donc que x est racine de $X^{q^n} - X$. Ce raisonnement peut être fait pour toute racine de P. On obtient donc que P divise $X^{q^n} - X$. De plus, comme P est irréductible par hypothèse, on obtient $P \in A$.
- ▶ Soit $P \in A$. Montrons que $\deg(P)$ divise n.
  Notons d le degré de P. Le polynôme $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$. Soit x une racine de P dans $\mathbb{F}_{q^n}$. On note $K = \mathbb{F}_q(x)$. On a donc

  $$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K][K : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K]d$$

  Ainsi, d divise n. De plus, comme P est irréductible, on a aussi $P \in A(d, q)$ et donc $P \in B$.

- Montrons que $\sum_{d|n} dI(d, q) = q^n$. On sait par ce qui précède que

  $$X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P.$$

  En regardant les degrés, on obtient $\sum_{d|n} dI(d, q) = q^n$.
- Montrons que $I(n, q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$. On utilise la formule d'inversion de Möbius appliquée à la fonction $n \mapsto nI(n, q)$. On obtient donc

  $$\begin{aligned} nI(n,q) &= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} d' I(n, d') \\ &= \sum_{d|n} \mu(d) q^{\frac{n}{d}} \text{ par le point précédent} \\ &= \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \end{aligned}$$

- Montrons que

  $$I(n, q) \sim \frac{q^n}{n}.$$

  On a

  $$I(n, q) = \frac{q^n + r_n}{n} \text{ avec } r_n = \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) q^d.$$

  On peut majorer r_n :

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

  On obtient donc

  $$r_n \leq \frac{q^{E\left(\frac{n}{2}\right)+1}}{q - 1}$$

  Ainsi, en divisant cette inégalité par q^n, on a que r_n est négligeable devant q^n quand n tend vers l'infini.
  On obtient donc l'équivalent

  $$I(n, q) \sim \frac{q^n}{n}.$$

□

Leçons possibles : 123 - 125 - 141 - 144