# Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$

Léo Gayral

2017-2018

ref : Francinou – Exercices de mathématiques pour l'agrégation – p.189

**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, $\mu$ 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 :

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

□

**Lemme 2.** Soit $f \in \mathbb{R}^{\mathbb{N}^*}$. On définit $g \in \mathbb{R}^{\mathbb{N}^*}$ par $g(n) = \sum\limits_{d/n} f(d)$. Alors $f(n) = \sum\limits_{d/n} \mu(d) g\left(\frac{n}{d}\right)$.

*Démonstration.*
On a $\sum_{d/n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d/n} \mu(d) \sum_{e/\frac{n}{d}} f(e) = \sum_{e/n} f(e) \sum_{d/\frac{n}{e}} \mu(d) = f(n)$. □

**Théorème 1.** On pose $\mathcal{P}(d) \subset \mathbb{F}_q[X]$ l'ensemble des polynômes irréductibles unitaires de degré $d$. Pour $n > 0$ on a la factorisation $X^{q^n} - X = \prod_{d/n} \prod_{P \in \mathcal{P}(d)} P$.

*Démonstration.*
Soit $P \in \mathcal{P}(d)$. On considère le corps de rupture $\mathbb{F}_q[X]/(P) \cong \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$. Pour $x \in \mathbb{F}_{q^d}$, on a donc $x^{q^d} = x$ (si $x \neq 0$, $x \in \mathbb{F}_{q^d}^*$ donc $x^{q^d-1} = 1$ par le théorème de Lagrange) puis par récurrence $x^{q^{(k+1)d}} = \left(x^{q^{kd}}\right)^{q^d} = x^{q^d} = x$. En particulier, si $d/n$ alors $x^{q^n} = x$. Toute racine de $P$ est racine de $X^{q^n} - X$ dans $\mathbb{F}_{q^n}$ donc $P$ est un facteur irréductible de ce polynôme.

En outre, $\left(X^{q^n} - X\right)' = -1$ donc $X^{q^n} - X$ est à racines simples dans $\mathbb{F}_{q^n}$ : c'est un produit de polynômes irréductibles deux à deux distincts. De plus, si on considère $P \in \mathbb{F}_q[X]$ un facteur irréductible de $X^{q^n} - X$, polynôme minimal de $x \in \mathbb{F}_{q^n}$, alors $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)] \times \deg(P)$, donc $\deg(P)/n$. □

**Corollaire 1.** On a $|\mathcal{P}(n)| = \frac{1}{n} \sum_{d|n} q^d \mu\left(\frac{n}{d}\right) \underset{n\to\infty}{\sim} \frac{q^n}{n}$.

*Démonstration.*
En regardant les degrés dans la formule qui précède on a $q^n = \sum_{d/n} d \times |\mathcal{P}(d)|$. Si on pose $f(d) = d \times |\mathcal{P}(d)|$ et $g(d) = q^d$, le second lemme donne :

$$n \times |\mathcal{P}(n)| = \sum_{d/n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d/n} \mu\left(\frac{n}{d}\right) q^d \ .$$

Pour évaluer le comportement asymptotique, on a la majoration :

$$\left| \sum_{d/n} \mu\left(\frac{n}{d}\right) q^d - q^n \right| \leq \sum_{d=0}^{\lfloor \frac{n}{2} \rfloor} q^d = \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{q - 1} = O\left(\sqrt{q}^n\right) = o\left(q^n\right) \ .$$

d'où le résultat voulu, $n\,|\mathcal{P}(n)| \sim q^n$. □

**Remarque 1.** Il y a, au total $q^{n-1}$ polynômes unitaires de degré $n$ dans $\mathbb{F}_q[X]$. En conséquence, la proportion de polynômes irréductibles de degré $n$ est de l'ordre de $\frac{q}{n}$.