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

Référence : *Francinou-Gianella, Exercices de mathématiques pour l'agrégation, p189*

Théorème. *Notons $A(n,q)$ l'ensemble des polynômes irréductibles de $\mathbb{F}_q[X]$ et $I(n,q) = A(n,q)$. Montrons que pour tout $n \in \mathbb{N}^*$ et tout q, $I(n,q) \geq 1$ et que $I(n,q) \underset{n\to+\infty}{\sim} \dfrac{q^n}{n}$.*

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

Soient $d \mid n$ et $P \in A(d,q)$. Soit x une racine de P dans une clôture algébrique. $\mathbb{F}_q[x]$ est un corps de rupture de P et $[\mathbb{F}_q[x] : \mathbb{F}_q] = \deg(P) = d$. On a donc $\mathbb{F}_q[x] \cong \mathbb{F}_{q^d}$. Or, par construction, $\mathbb{F}_{q^d}$ est le corps de décomposition de $X^{q^d} - X$. En particulier, $x^{q^d} = x$. Ainsi, en notant $dr = n$,

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

Donc x est une racine de $X^{q^n} - X$. D'où $P \mid X^{q^n} - X$.

Réciproquement, soit P un polynôme irréductible divisant $X^{q^n} - X$. Soit L un corps de rupture de P. On a $[L : \mathbb{F}_q] = \deg(P)$. Or L est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ donc, par multiplicativité des degrés, $\deg(P) \mid n$. On a donc le résultat escompté.

En prenant les degrés dans l'égalité otenue, on obtient $q^n = \sum_{d|n} dI(d,q)$. En appliquant le formule d'inversion de Möbius (démontrée ci-après), on obtient

$$I(n,q) = \frac{1}{n}\sum_{d|n} q^d \mu\left(\frac{n}{d}\right) = \frac{1}{n}\left(q^n + \sum_{\substack{d|n \\ d<n}} q^d \mu\left(\frac{n}{d}\right)\right) = \frac{1}{n}\left(q^n + r_n\right).$$

On a

$$|r_n| \leq \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q^d = q\frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q-1} \leq q^{\lfloor \frac{n}{2} \rfloor + 1}$$

qui est négligeable devant q^n. Ainsi $I(n,q) \underset{n\to+\infty}{\sim} \dfrac{q^n}{n}$.

De plus, $|r_n| < q^n$ donc $I(n,q) > 0$ pour tout $n \in \mathbb{N}^*$.

□

Définition. La fonction μ de Möbius est définie par

$$\begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \{-1,0,1\} \\ n & \longmapsto & \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ a un facteur carré} \\ (-1)^r & \text{si } n = p_1 \dots p_r \text{ (premiers distincts)} \end{cases} \end{array}.$$

Lemme. *La fonction de Möbius vérifie :*

1. *μ est multiplicative : $\forall n, m \in \mathbb{N}^*, pgcd(n,m) = 1,\ \mu(nm) = \mu(n)\mu(m)$;*
2. $\displaystyle\sum_{d|n} \mu(d) = \begin{cases} 1 & si\ n = 1 \\ 0 & sinon \end{cases}$;
3. *la formule d'inversion : si $g(n) = \displaystyle\sum_{d|n} f(d)$ alors $f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} g\left(\frac{n}{d}\right)\mu(d)$.*

Démonstration.

1. Si $n = 1$ ou $m = 1$, le résultat est évident car $\mu(1) = 1$ par définition.
   Si n ou m a un facteur carré, nm a un facteur carré.
   Enfin, comme pgcd(n,m)=1, le dernier cas possible est $n = p_1 \dots p_r$ et $m = q_1 \dots q_s$ avec les p_i et les q_i des nombres premiers tous distincts. On a alors $\mu(nm) = \mu(p_1 \dots p_r q_1 \dots q_s) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(p_1 \dots p_r)\mu(q_1 \dots q_s) = \mu(n)\mu(m)$.
2. Le cas $n = 1$ est évident.
   Notons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$.

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{r} \mu(p_i) + \sum_{i<j} \mu(p_i p_j) + \sum_{i<j<k} \mu(p_i p_j p_k) + \dots + \mu(p_1 \dots p_r) + 0 \\ &= 1 + \sum_{i=1}^{r} (-1) + \sum_{i<j} (-1)^2 + \sum_{i<j<k} (-1)^3 + \dots + (-1)^r \\ &= 1 - \binom{1}{r} + \binom{2}{r} - \binom{3}{r} + \dots + (-1)^r \\ &= (1-1)^r \\ &= 0 \end{aligned}$$

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

   (on a utilisé le point 2 pour la dernière égalité). Par changement de variable, on a

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

□