Un équivalent du nombre de polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$

Achille Méthivier

Théorème 1. *On note $\mathcal{A}(n,q) = \{P \in \mathbb{F}_q[X] \ : \ P$ irréductible unitaire, $\deg(P) = n\}$ et $I(n,q) = \#\mathcal{A}(n,q)$. Alors,*

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

Lemme 2. *Soit $\mu : \mathbb{N} \to \mathbb{N}$ la fonction multiplicative définie par $\mu(1) = 1$, $\mu(p) = -1$ et $\mu(p^\alpha) = 0$ pour p premier et $\alpha \geq 2$. Soit $g : \mathbb{N} \to \mathbb{N}$ une fonction et s la fonction définie par*

$$s(n) = \sum_{d|n} g(d).$$

Alors,

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

Démonstration. Décomposons n en produit de facteurs premiers

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Soit $d|n$, on a

$$\begin{aligned} \mu(d) \neq 0 &\iff \forall 1 \leq i \leq k \quad p_i^2 \not| d \\ &\iff \exists r \geq 0 \exists i_1, \ldots, i_r \in \{1, \ldots, k\} \text{ distincts } d = p_{i_1} \cdots p_{i_r}. \end{aligned}$$

On a donc $\#\{d : \mu(d) \neq 0\} = \#\{i_1, \ldots, i_r \in \{1, \ldots, k\} \text{ distincts}\} = \binom{k}{r}$.
Donc, pour $n > 1$,

$$\sum_{d|n} \mu(d) = \sum_{r=0}^{k} \binom{k}{r} (-1)^r = 0,$$

et cette somme vaut 1 pour $n = 1$. Maintenant,

$$\begin{aligned} \sum_{d|n} \mu\left(\frac{n}{d}\right) s(d) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{d'|d} g(d') \\ &= \sum_{d'|n} g(d') \sum_{d'|d \ d|n} \mu\left(\frac{n}{d}\right) \\ &= \sum_{d'|n} g(d') \sum_{k|\frac{n}{d'}} \mu(k) = ng(n). \end{aligned}$$

□

Démonstration du théorème. Soit d un diviseur de n et $P \in \mathcal{A}(d,n)$. Pour x une racine de P dans un corps de rupture K. Comme P irréductible et $\deg(P) = d$, on a $[K : \mathbb{F}_q] = d$ donc pour tout $y \in K$ on a $y^{q^d} = y$. Et comme $d|n$, on peut écrire

$$x^{q^n} = \left(\ldots (x^{q^d})^{q^d} \ldots\right)^{q^d} = x.$$

Donc x est racine de $X^{q^n} - X$. Comme P est irréductible, il est scindé à racines simples dans $\mathbb{F}_q$ et toutes ses racines sont racines de $X^{q^n} - X$, donc $P | X^{q^n} - X$. Réciproquement, si P est un facteur irréductible, de degré d, de $X^{q^n} - X$ sur $\mathbb{F}_q[X]$. Comme $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$, pour x racine de P, on a $x \in \mathbb{F}_{q^n}$. Donc $K = \mathbb{F}_q(x)$ est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$. Donc

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

Finalement $d|n$. De plus, la dérivée de $X^{q^n} - X$ est $q^n X^{q^n - 1} - 1 = -1$, donc $X^{q^n} - X$ est à racines simples, donc tous ces facteurs irréductibles sur $\mathbb{F}_q$ sont simples. Finalement,

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

Et donc,

$$q^n = \sum_{d|n} dI(d,q).$$

En appliquant le lemme 2, on obtient

$$nI(n,q) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Posons $I(n,q) = \frac{q^n + r_n}{n}$ avec

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

Or,

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

d'où le résultat.

□

I Références

1. Exercices de mathématiques pour l'agrégation, Francinou, Gianella (page 189)