Polynômes irréductibles sur $\mathbb{F}_p$

[TAUVEL, p 119-120]

ÉNONCÉ : Pour $n \in \mathbb{N}^*$, on note $\mathcal{P}_p(n)$ l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_p$ et $I(p,n)$ le cardinal de l'ensemble $\mathcal{P}_p(n)$.
Soit $\mu : \mathbb{N}^* \to \{-1,0,1\}$ est la fonction de MÖBIUS définie par :

$$\begin{array}{rccc} \mu & : & \mathbb{N}^* & \longrightarrow & \{-1, 0+1\} \\ & & n & \longmapsto & \begin{cases} 0 \text{ si } \exists a \in \mathbb{N} \setminus \{1\} \ t.q. \ a \mid n \text{ et } \sqrt{a} \in \mathbb{N} \\ (-1)^k \text{ où } k := \#(\{p \text{ premier} \mid p \mid n\}) \text{ sinon} \end{cases} \end{array}$$

Théorème : Pour $n \in \mathbb{N}^*$, on a :

$$X^{p^n} - X = \prod_{d|n} \prod_{p \in \mathcal{P}_p(d)} P(X)$$

Alors on a :

$$I(q,n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

En particulier, $I(p,n) \geq 1$ et :

$$I(p,n) \underset{n \to +\infty}{\sim} \frac{p^n}{n}$$

DÉVELOPPEMENT :

LEMMES (**Inversion de MÖBIUS**) : Soient $g : \mathbb{N}^* \longrightarrow \mathbb{C}$ une application et $G(n) := \sum_{d|n} g(d)$, alors on a :

$$\forall n \in \mathbb{N}^*, \quad g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$$

Démonstration. Remarquons d'abord que, pour $n \geq 2$, $\sum_{d|n} \mu(d) = 0$. En effet, considérons la décomposition en facteurs premiers de $n := \prod_{i=1}^r p_i^{\alpha_i}$, alors :

$$\sum_{d|n} \mu(d) = \sum_{d|p_1 \dots p_r} \mu(d) = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = 0$$

Maintenant, pour $n \in \mathbb{N}^*$ et $d \mid n$, alors $d' \mid \frac{n}{d} \iff dd' \mid n$. Ainsi, on a :

$$\begin{aligned} \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d' \mid \frac{n}{d}} g(d') \\ &= \sum_{dd'|n} \mu(d) g(d') \\ &= \sum_{d'|n} g(d') \sum_{d \mid \frac{n}{d'}} \mu(d) \\ &= g(n) \end{aligned}$$

□

Démonstration. (*théorème*) : Pour $P \in \mathcal{P}_p(d)$, alors $K = \mathbb{F}_p[X]/(P)$ est un corps de cardinal p^d, donc isomorphe à $\mathbb{F}_{p^d}$. Ainsi, pour tout $x \in K$, on a $x^{p^d} = x$. Mais si $n = dk$ pour un $k \in \mathbb{N}^*$, on a :

$$x^{p^n} = x^{p^{dk}} = \underbrace{(((x^{p^d})^{p^d}) \dots)^{p^d}}_{k \text{ fois}} = x$$

Ainsi, $x^{p^n} - x = 0$ pour toute racine x de P, donc $P \mid X^p - X$ dans $\mathbb{F}_p[X]$. Mais comme les éléments de $\mathcal{P}_p(d)$ sont irréductibles, le produit $\Pi_{d|n} \Pi_{p \in \mathcal{P}_p(d)} P(X)$ divise lui aussi $X^{p^n} - X$.
Réciproquement, soit P un facteur irréductible de degré d de $X^{p^n} - X$ dans $\mathbb{F}_p[X]$. Comme $\mathbb{F}_{p^n}$ est un corps de décomposition de $X^{p^n} - X$, P est scindé sur $\mathbb{F}_{p^n}$. Si x est une racine de P ; on a : $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n = [\mathbb{F}_{p^n} : \mathbb{F}_p(x)][\mathbb{F}_p(x) : \mathbb{F}_p]$. Mais comme P est irréductible, $F_p(x)$ est un corps de rupture de P de degré d sur $\mathbb{F}_p$, donc d divise n.
De plus, $pgcd(P, P') = 1$, donc $X^{p^n} - X$ n'a pas de racine double dans un corps de décomposition, donc n'admet pas de facteur irréductible double. Ainsi, on a bien $X^{p^n} - X = \Pi_{d|n} \Pi_{p \in \mathcal{P}_q(d)} P(X)$.
En passant aux degrés, on a $p^n = \deg(X^{p^n} - X) = \Sigma_{d|n} I(p, d)d$.
En appliquant le lemme à l'application $g : \mathbb{N}^* \to \mathbb{C}^*$ définie par $g(n) = I(p, n)n$ et $G(n) = \Sigma_{d|n} g(d) = p^n$, il vient :

$$\begin{aligned} g(n) &= \sum_{d|n} \mu(d) p^{\frac{n}{d}} \\ &= \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d \end{aligned}$$

D'où :

$$I(p, n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

En posant, pour $n \in \mathbb{N}^*$,

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

On a :

$$|r_n| = \left| \sum_{\substack{d|n \\ d<n}} \mu\left(\frac{n}{d}\right) p^d \right| \leq \sum_{d=1}^{E\left(\frac{n}{2}\right)} p^d = p \frac{p^{E\left(\frac{n}{2}\right)} - 1}{p - 1} \leq \frac{p^{E\left(\frac{n}{2}\right)+1}}{p - 1}$$

d'où $r_n = \underset{n \to +\infty}{o}(p^n)$. Mais comme $I(p, n) = \frac{p^n + r_n}{n}$, on en déduit le résultat : $I(p, n) \underset{n \to +\infty}{\sim} \frac{p^n}{n}$. □

Remarques :

- Il faut savoir appliquer ce théorème à certains polynôme ($X^{16} - X$ sur $\mathbb{F}_2$, par exemple).
- La fonction de MÖBIUS est souvent utilisée dans les problèmes de dénombrement.