Polynômes irréductibles sur $\mathbb{F}_q$: 123, 128, 141, 144, 190

Dans toute la suite, on prend q une puissance d'un nombre premier et $n \in \mathbb{N}^*$

Théorème : On note $K(n,q) = \{P \in \mathbb{F}_q[X],\ P \text{ irréductible},\ d^\circ P = n\}$

Alors $\# K(n,q) \underset{n \to +\infty}{\sim} q^n/n$

On procède en 3 étapes :

- On montre une factorisation de $X^{q^n} - X$
- On démontre la formule d'inversion de Moebius
- On déduit l'expression exacte de $K(n,q)$ qui donne l'équivalent.

Notons dans la suite $P(d) = \{P \in \mathbb{F}_q[X],\ \text{irréductible, unitaire},\ d^\circ P = d\}$

Lemme 1 : On a $X^{q^n} - X = \prod_{d|n} \prod_{P \in P(d)} P$

preuve : Soit $P \in P(d)$, $\mathbb{F}_q[X]/(P)$ est un corps de rupture de P, isomorphe à $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$

Pour $x = \bar{X} \in \mathbb{F}_{q^d}$, on a $x^{q^d} = x$ (Lagrange) et par récurrence, $x^{q^{(k+1)d}} = (x^{q^{kd}})^{q^d} = x^{q^d} = x$

En particulier, si $d | n$, $x^{q^n} = x$, donc toute racine de P est racine de $X^{q^n} - X$

donc $P | X^{q^n} - X$ et P est irréductible donc par le lemme de Gauss :

$$\prod_{d|n} \prod_{P \in P(d)} P \mid X^{q^n} - X$$

De plus, si P est un facteur irréductible de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$, comme $\mathbb{F}_{q^n}$ est le corps de décomposition de $X^{q^n} - X$, P est scindé sur $\mathbb{F}_{q^n}$.

Si x est racine de P dans $\mathbb{F}_{q^n}$, on a $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q]$

et P étant irréductible de degré d sur $\mathbb{F}_q$, P est le polynôme minimal de x sur $\mathbb{F}_q$ donc $n = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)] \times d \ \rightarrow\ \underline{d | n}$.

De plus, comme $(X^{q^n} - X)' = -1$ dans toute extension de $\mathbb{F}_q$, $X^{q^n} - X$ est à racines simples dans son corps de décomposition $\mathbb{F}_{q^n}$: $X^{q^n} - X$ est produit de polynômes irréductibles distincts.

D'où la formule $X^{q^n} - X = \prod_{d|n} \prod_{P \in P(d)} P$.

Définition : (fonction de Moebius) Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_1, \dots, p_r$ premiers distincts.

$$\mu(n) = \begin{cases} (-1)^r & \text{si } \forall i \in [\![1,r]\!],\ \alpha_i \leq 1 \\ 0 & \text{sinon} \end{cases}$$

Notons que si $n \wedge m = 1$, alors $\mu(nm) = \mu(n)\mu(m)$

Proposition : pour $n \geq 2$, $\sum_{d|n} \mu(d) = 0$

démo : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$,

$$\sum_{d|n} \mu(d) \underset{(1)}{=} \sum_{i=0}^{r} \sum_{\substack{d = p_{j_1} \cdots p_{j_i} \\ d|n}} \mu(d) \underset{(2)}{=} \sum_{i=0}^{r} \binom{r}{i} (-1)^i = 0.$$

(1) : on peut éliminer tous les éléments d contenant un p_i^2 dans leur décomposition

(2) : le choix de $d = p_1 \cdots p_r$ le revient au choix de $\beta \in \{0,1\}^r$, indexé par $i = |\beta|$, on a $\binom{r}{i}$ choix

Lemme 7 : Soit $f : \mathbb{N} \to \mathbb{N}$, $F : n \in \mathbb{N} \mapsto \sum_{d|n} f(d)$, on a

$$\forall n \in \mathbb{N},\ f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

- preuve :
$$\sum_{d|n} \mu\left(\frac{d}{n}\right) F(d) = \sum_{d|n} \mu(d) F\left(\frac{d}{n}\right) = \sum_{d|n} \mu(d) \left(\sum_{d' | \frac{n}{d}} f(d')\right)$$

notons que $d' | \frac{n}{d}$ ssi $dd' | n$

$$= \sum_{dd'|n} \mu(d) f(d') = \sum_{d'|n} f(d') \underbrace{\left(\sum_{d | \frac{n}{d'}} \mu(d)\right)}_{\substack{= 0 \text{ si } \frac{n}{d'} \geq 2 \\ = 1 \text{ si } n = d'}}$$

$$= f(n)$$

Corollaire : $\# K(q,n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$ et $\# K(q,n) \underset{n \to +\infty}{\sim} q^n/n$

démo : Posons $f : n \mapsto n \# K(q,n)$, appliquant la formule d'inversion de Moebius à f, on a :

$$f(n) = \sum_{d|n} \mu(d) \sum_{d' | \frac{n}{d}} d' \# K(q,d')$$

En passant au degré dans le lemme 1, on obtient $q^n = \sum_{d|n} d \# K(q,d)$

et donc $f(n) = \sum_{d|n} \mu(d) q^{n/d} = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$

$$\to \# K(q,n) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d.$$

On a $f(n) = q^n + r_n$ avec $r_n = \sum_{\substack{d|n \\ d<n}} \mu(n/d) q^d$

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

et $|r_n|/q^n = \frac{1}{q-1} q^{1 + \lfloor n/2 \rfloor - n} \xrightarrow[n \to +\infty]{} 0$: $r_n = o(q^n)$

$\to f(n) = q^n + o(q^n)$: $\# K(q,n) \underset{n \to +\infty}{\sim} q^n/n$.

Remarque : on a au total q^{n-1} polynômes unitaires de degré n dans $\mathbb{F}_q[X]$.
La proportion d'irréductibles parmi ces polynômes est donc de l'ordre de q/n.