★ Exercices d'algèbre pour agreg., Francinou
Mathématiques pour agreg., Rombaldi

Dénombrement des polynômes irréductibles unitaires de $\mathbb{F}_q$

Définition [Fonction de Möbius] On considère $\mu : \mathbb{N}^* \longrightarrow \{-1, 0, 1\}$ la fonction multiplicative de Möbius. Elle est définie par $\mu(n) = 0$ si n est divisible par un carré parfait, $\mu(n) = -1$ si n est le produit d'un nombre impair de premiers distincts, 1 sinon.

multiplicative : $n \wedge n' \Rightarrow \mu(nn') = \mu(n)\mu(n')$

Formule d'inversion de Möbius Soient $f : \mathbb{N}^* \longrightarrow \mathbb{R}$ multiplicative et $g : n \in \mathbb{N}^* \longmapsto \sum_{d|n} f(d)$.
On a alors pour tout $n \in \mathbb{N}^*$, $f(n) = \sum_{d|n} \left(\frac{n}{d}\right) g(d)$

Soit $n \in \mathbb{N}^*$. On a :

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

$$= \sum_{dd'|n} \mu(d) f(d')$$

$$= \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d)$$

$$= f(n)$$

$\sum_{k|j} \mu(k) = \begin{cases} 1 \text{ si } j = 1 \\ 0 \text{ si } j > 1 \end{cases}$

Lemme On considère $U(n, q)$ l'ensemble des polynômes irréductibles unitaires de degré n de $\mathbb{F}_q[X]$.
Alors pour $d|n$ et $P \in U(d, q)$, $P \mid X^{q^n} - X$ et, si P irréductible divise $X^{q^n} - X$, $\deg P \mid n$.

- Soient $d|n$ et $P \in U(d, q)$.

On considère $K = \mathbb{F}_q(x)$ un corps de rupture de P, x racine de P.
On a :
$[K : \mathbb{F}_q] = \deg P = d$ donc par unicité des corps finis $K \simeq \mathbb{F}_{q^d}$.
En particulier, $x^{q^d} = x$ et :

$$x^{q^n} = \underbrace{((x^{q^d})\cdots)^{q^d}}_{\frac{n}{d} \text{ fois}} = \underbrace{(x^{q^d})^{q^d}\cdots}_{\frac{n}{d}-1 \text{ fois}}{}^{q^d} = x^{q^d} = x$$ alors x est racine de $X^{p^n} - X$.

Donc :
P divise $X^{q^n} - X$.

- Soit P un facteur irréductible de $X^{q^n} - X$ et notons d son degré.

Le polynôme $X^{q^n} - X$ est scindé dans $\mathbb{F}_{q^n}$. → ses racines sont les éléments de $\mathbb{F}_{q^n}$, s'agissant d'un corps le polynôme admet au plus q^n racines et donc exactement q^n
Notons alors x une racine de P et considérons $K = \mathbb{F}_q(x)$.
On obtient alors :

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

Ainsi : $d = [K : \mathbb{F}_q]$ est un diviseur de n.

Proposition Considérons $I(n, q) = \#U(n, q)$.
Alors : $I(n, q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$.

Les racines de $X^{q^n} - X$ dans $\mathbb{F}_{q^n}$ sont simples, donc les facteurs irréductibles apparaissent avec multiplicité 1.
Donc d'après le lemme,

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in U(d,q)} P \quad \text{et en regardant les degrés} \quad q^n = \sum_{d|n} d\, I(d, q).$$

En appliquant la formule de Möbius à $n \longmapsto n I(n, q)$, on obtient : → car $g(n) = \sum_{d|n} f(d)$ $= \sum_{d|n} d\, I(d, q) = q^n$

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

Proposition Soit $n \in \mathbb{N}^*$.

Alors : $I(n,q) \underset{+\infty}{\sim} \frac{q^n}{n}$ et $I(n,q) \geqslant 1$.

D'après ce qui précède,

$$I(n,q) = \frac{q^n + R_n}{n}$$

Avec :

$$|r_n| = \left| \sum_{\substack{d \mid n \\ d \neq n}} \mu\left(\frac{n}{d}\right) q^d \right| \leqslant \sum_{d=1}^{\lfloor n/2 \rfloor} q^d = q \frac{q^{\lfloor n/2 \rfloor} - 1}{q-1}$$

Donc :

$$|r_n| \leqslant \frac{q^{\lfloor n/2 \rfloor + 1}}{q-1} = o(q^n) \quad \text{donc} \quad I(n,q) \sim \frac{q^n}{n}$$

$$|r_n| \leqslant \frac{q^{\lfloor n/2 \rfloor + 1}}{q/2} \leqslant 2q^{\lfloor n/2 \rfloor} < q^n \quad \text{donc} \quad I(n,q) > 0 \text{ i.e. } I(n,q) \geqslant 1$$

→ car $q \geqslant 2$ donc $q - 1 \geqslant q/2$

9. ajouté au mon selon le temps du développement