Une estimation du nombre de polynômes irréductibles unitaires dans $\mathbf{F}_q$.

Théorème (Formule d'inversion de Möbius)**.** *Soient* $f : \mathbf{N}^* \to \mathbf{R}$ *et* $g : n \in \mathbf{N}^* \mapsto \sum_{d|n} f(d)$*. Alors pour tout* $n \geq 1$ *:*

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

Preuve. On commence par voir que si $n = 1$, $\sum_{d|n} \mu(d) = 1$ et si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, alors :

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{1 \leq i \leq r} \mu(p_i) + \dots + \mu(p_1 \dots p + r) \\ &= 1 - \binom{r}{1} + \binom{r}{2} - \dots + (-1)^r = (1-1)^r = 0 \end{aligned}$$

de sorte que l'on peut calculer :

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

Et on passe d'une somme à l'autre en posant $d' = n/d$. □

Fort de ce résultat, on va montrer l'estimation suivante.

Théorème. *Pour* $n \in \mathbf{N}^*$*,* $A(n, q)$ *désigne le nombre de polynômes irréductibles unitaires sur* $\mathbf{F}_q$*. On note* $I(n, q) = \operatorname{Card} A(n, q)$*. Il existe des polynômes irréductibles de tout degré sur* $\mathbf{F}_q$ *et*

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

Preuve. La première partie consiste à étudier les diviseurs des polynômes $X^{q^n} - X$.

(1) Si P est un facteur irréductible unitaire de $X^{q^n} - X$ dans $\mathbf{F}_q$, alors notons d son degré. Comme $X^{q^n} - X$ est scindé sur $\mathbf{F}_{q^n}$, P est aussi scindé dans $\mathbf{F}_{q^n}$ et si $x \in \mathbf{F}_{q^n}$ est une racine de P, $\mathbf{F}_q(x)$ est un corps intermédiaire entre $\mathbf{F}_q$ et $\mathbf{F}_{q^n}$ de degré d. Alors, la théorème de la base télescopique donne :

$$[\mathbf{F}_{q^n} : \mathbf{F}_q(x)][\mathbf{F}_q(x) : \mathbf{F}_q] = [\mathbf{F}_{q^n} : \mathbf{F}_q] = n$$

et on peut déjà affirmer que $d|n$. De plus, comme $X^{q_n} - X$ est à racines simples dans $\mathbf{F}^{q^n}$ (c'est la définition), ses facteurs irréductibles dans $\mathbf{F}_q$ sont de multiplicité 1 et on a :

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

(2) Maintenant, si $d|n$ et $P \in A(d, q)$, alors soit $\overline{\mathbf{F}}_q$ une clôture algébrique de $\mathbf{F}_q$.

- Si $x \in \overline{F}_q$ est une racine de P alors par unicité des corps finis, $\mathbf{F}_q(x) \simeq \mathbf{F}_{q^d}$ donc x est aussi une racine de $X^{q^d} - X$.
- Comme $d|n$ un savant bidouillage avec les puissances montre que $X^{q^d} - X \Big| X^{q^n} - X$.
- Comme P Est irréductible, il est à racines simples dans $\overline{F}_q$, en effet sinon il existerait $\alpha \in \overline{F}_q$ tel que $X - \alpha | P$ et $X - \alpha | P'$. Alors $X - \alpha$ divise $P \wedge P'$ qui est donc de degré supérieur ou égal à 1. Mais comme $P \wedge P' | P$ et que ce dernier est irréductible, $P \wedge P' = P$, c'est à dire $P' = 0$. Le morphisme de Frobenius dit alors que P est de la forme $P(X) = R(X^p) = R(X)^p$, c'est absurde.

En conclusion, on vient de montrer en mettant tout ensemble que :

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

Finalement on peut écrire :

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

et la suite n'est que dénombrement : en regardant les degrés, on trouve

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

La formule d'inversion de Möbius donne :

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

où

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

Cela montre déjà que $I(q,n) \neq 0$ pour tout n et en majorant :

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

et on en déduit l'équivalent annoncé. □

Référence. S. Francinou, H. Gianella, *Exercices de Mathématiques pour l'Agrégation, Algèbre 1*

123 Corps finis. Applications.
125 Extensions de corps. Exemples et applications.
141 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
190 Méthodes combinatoires, problèmes de dénombrement.