Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$

Référence : Francinou-Gianella : Exercices de mathématiques pour l'agrégation, p. 189

Théorème

Soit $n \in \mathbb{N}^*$.
Notons $A(n,q)$ l'ensemble des polynômes irréductibles unitaires de degré n de $\mathbb{F}_q[X]$ et $I(n,q) = \text{Card}A(n,q)$.
Alors :

1. $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P$
2. Si μ est la fonction de Möbius, $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$
3. $I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$

Preuve :

1. Soient d un diviseur de n (on note $dr = n$) et $P \in A(d,q)$. Soit x une racine de P dans une clôture algébrique. $\mathbb{F}_q(x)$ est un corps de rupture de P et $[\mathbb{F}_q(x) : \mathbb{F}_q] = \deg(P) = d$. On a donc $\mathbb{F}_q(x) \cong \mathbb{F}_{q^d}$ (unicité des corps finis). Or, par construction, $\mathbb{F}_{q^d}$ est le corps de décomposition de $X^{q^d} - X$ ie l'ensemble des racines de $X^{q^d} - X$. En particulier [1], $x^{q^d} = x$. Ainsi,

$$x^{q^n} = \left(\underbrace{\left(\left(x^{q^d} \right)^{q^d} \right)^{q^d} \dots}_{r \text{ fois}} \right)^{q^d} = \left(\underbrace{\left(\left(x^{q^d} \right)^{q^d} \right)^{q^d} \dots}_{r-1 \text{ fois}} \right)^{q^d} = \dots = x^{q^d} = x.$$

Donc x est une racine de $X^{q^n} - X$. D'où $P \mid X^{q^n} - X$ [2] Donc $\prod_{d|n} \prod_{P \in A(d,q)} P \mid X^{q^n} - X$ par irréductibilité.

Réciproquement, soit $P \in \mathbb{F}_q[X]$ un polynôme irréductible divisant $X^{q^n} - X$. $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$. Soit x une racine de P dans $\mathbb{F}_{q^n}$ donc $L := \mathbb{F}_q(x)$ est un corps de rupture de P ie L est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ donc. On a

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : L][L : \mathbb{F}_q] = \deg(P)[\mathbb{F}_{q^n} : L]$$

Donc $\deg(P) \mid n$.

Les racines de $X^{q^n} - X$ dans $\mathbb{F}_{q^n}$ sont simples. Donc tous les facteurs irréductibles de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$ interviennent avec une multiplicité égale à 1. Il vient donc finalement :

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

1. on peut également dire que x non nul. $\mathbb{F}_q(x)*$ de cardinal $q-1$ et on utilise Lagrange.

2. Il s'agit ici de voir que P n'a que des racines simples. En effet, supposons par l'absurde que x soit une racine double de P dans une extension L de K. Alors x est une racine de P'. Si on fait l'algorithme d'Euclide dans L et dans K par unicité de la division euclidienne c'est le même truc à chaque étape donc $\text{pgcd}_L(P,P') = \text{pgcd}_K(P,P')$. Comme P est irréductible dans $K = \mathbb{F}_q$, $\text{pgcd}_K(P,P') = P$ ou 1 donc $\text{pgcd}_K(P,P') = P$ car ils ont une racine commune donc ce n'est pas 1. Donc $\text{pgcd}_K(P,P') = P$ pbm de degré sauf si $P' = 0$ ie $P = Q(X^p) = \sum_{i=1}^{n} q_i X^{ip} = \sum_{i=1}^{n} \tilde{q}_i^p X^{ip} = \left(\sum_{i=1}^{n} \tilde{q}_i X^i \right)^p$. (on a utilisé la surjectivité du Frobenius au 3ième =) absurde car P irréductible.

2. En prenant les degrés dans l'égalité 1., on obtient $q^n = \sum_{d|n} dI(d,q)$.

   En appliquant le formule d'inversion de Möbius (**Lemme**) à $n \mapsto nI(n,q)$ et en disisant par n, on obtient

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

3. On a de plus $I(n,q) = \frac{1}{n}\left(q^n + \underbrace{\sum_{\substack{d|n \\ d<n}} q^d \mu\left(\frac{n}{d}\right)}_{:=r_n}\right)$.

   On a

$$|r_n| \leqslant \sum_{d=1}^{[\frac{n}{2}]} q^d = q\frac{q^{[\frac{n}{2}]}-1}{q-1} \leqslant \underbrace{\frac{q^{[\frac{n}{2}]+1}}{q-1}}_{\text{négligeable devant } q^n}$$

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

4. Bonus : Pour tout $n \geqslant 1$, $|r_n| \leqslant \frac{q^{[\frac{n}{2}]+1}}{q/2} \leqslant 2q^{[\frac{n}{2}]} < q^n$ donc [3] $I(n,q) > 0$ pour tout $n \in \mathbb{N}^*$.

■

Définition

La fonction μ de Möbius est définie par

$$\begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \{-1,0,1\} \\ n & \longmapsto & \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ a un facteur carré} \\ (-1)^r & \text{si } n = p_1 \dots p_r \text{ (premiers distincts)} \end{cases} \end{array} .$$

Lemme

La fonction de Möbius vérifie :

1. μ est multiplicative : $\forall n, m \in \mathbb{N}^*, \text{pgcd}(n,m) = 1,\ \mu(nm) = \mu(n)\mu(m)$;
2. $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases}$;
3. la formule d'inversion : si $g(n) = \sum_{d|n} f(d)$ alors $f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} g\left(\frac{n}{d}\right)\mu(d)$.

Preuve : [FG p.93]

1. Si $n = 1$ ou $m = 1$, le résultat est évident car $\mu(1) = 1$ par définition.
   Si n ou m a un facteur carré, nm a un facteur carré.
   Enfin, comme pgcd(n,m)=1, le dernier cas possible est $n = p_1 \dots p_r$ et $m = q_1 \dots q_s$ avec les p_i et les q_i des nombres premiers tous distincts. On a alors $\mu(nm) = \mu(p_1 \dots p_r q_1 \dots q_s) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(p_1 \dots p_r)\mu(q_1 \dots q_s) = \mu(n)\mu(m)$.
2. Le cas $n = 1$ est évident.

3. car au pire $r_n = -q^n + 1$ donc $I(n,q) = \frac{1}{n} > 0$ (heuristiquement mais c'est impossible car $I(n,q)$ est entier)

Notons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ sa décomposition en facteurs premiers.

$$\begin{aligned}\sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{r} \mu(p_i) + \sum_{i<j} \mu(p_i p_j) + \sum_{i<j<k} \mu(p_i p_j p_k) + \dots + \mu(p_1 \dots p_r) + 0 \\ &= \sum_{k=0}^{r} \binom{r}{k} (-1)^k \\ &= (1-1)^r \\ &= 0\end{aligned}$$

.

3.

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

(on a utilisé le point 2 pour la dernière égalité). Par changement de variable, on a

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

■

Notes :

✓ **A l'oral**, 10' sans Mobius. 14' avec 2 et 3 de Mobius. Allure normale.
✓ Rappel : Corps de rupture = 1 racine.
✓ Quand on cherche Card$\{(i_1, \dots, i_k) \in [\![1, r]\!] \ / \ i_1 < \dots < i_k\}$, on a r possibilités pour i_k, $r-1$ possibilités pour i_{k-1}, etc $r-k$ possibilités pour i_1, ceci étant à permutations près on divise par $k!$ ie $\dfrac{r(r-1)\dots(r-k)}{k!} = \binom{k}{r}$.
✓ Dès 1748, la fonction μ apparaît de manière explicite dans les travaux d'Euler. Mais c'est Möbius qui en 1832 en étudia les propriétés de manière systématique.