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

↳ Refs : Rombaldi, p 331-333 et 422-424 + cours de Théo C.

Rappel : On note S le $\mathbb{C}$-ev défini par $S := \{f : \mathbb{N}^* \to \mathbb{C}\}$, sur lequel on définit un produit (LCI) appelé produit de convolution (ou de Dirichlet) défini par : pour $u, v \in S$, et $n \in \mathbb{N}^*$, $(u * v)(n) = \sum_{d|n} u\left(\frac{n}{d}\right) v(d) = \sum_{d|n} u(d)\, v\left(\frac{d}{n}\right)$.
Alors $(S, +, \cdot, *)$ est une $\mathbb{C}$-algèbre commutative.
Les éléments inversibles sont les $u \in S$ tq $u(1) \in \mathbb{R}^*$ (où le neutre est la suite $e = (\delta_{1,k})_{k \in \mathbb{N}^*}$ et $v = u^{-1}$ défini par $v(1) = \frac{1}{u(1)}$, $v(n) = \frac{-1}{u(1)} \sum_{\substack{d|n \\ d \neq n}} u\left(\frac{n}{d}\right) v(d)$ pour $n \geq 2$.
On définit la fonction de Möbius μ par : pour $n \in \mathbb{N}^*$,

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n = \prod_{i=1}^{r} p_i \text{ où les } p_i \text{ sont des nbs premiers distincts} \\ 0 & \text{sinon} \end{cases}$$

Proposition : La fonction de Möbius est l'inverse de la suite constante égale à 1 pour $*$.

Théorème 1 : (Formule d'inversion de Möbius) Soient $f, g \in S$ telles que $\forall n \in \mathbb{N}^*$, $f(n) = \sum_{d|n} g(d)$. Alors $\forall n \in \mathbb{N}^*$, $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$.

Soit $q = p^\alpha$ et $\mathbb{F}_q$ un corps de cardinal q. On note $\mathcal{P}_q(d)$ l'ensemble des polynômes irréductibles unitaires de degré d dans $\mathbb{F}_q[X]$.

Lemme : Pour $n \in \mathbb{N}^*$, $X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$.

Théorème 2 : Si l'on note $I(q,n)$ le cardinal de $\mathcal{P}_q(n)$, on a pour $n \in \mathbb{N}^*$,

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

On obtient également que pour tout $n \in \mathbb{N}^*$, il existe dans $\mathbb{F}_q[X]$ au moins un polynôme irréductible de degré n et $I(q,n) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$.

Preuve de la proposition : On a premièrement $(\mu * \mathbb{1})(1) = \mu(1) \times \mathbb{1}(1) = 1$.
Reste à montrer que pour $n \geq 2$, $(\mu * \mathbb{1})(n) = 0$.
Or $(\mu * \mathbb{1})(n) = \sum_{d|n} \mu(d)$. Si l'on écrit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ où les p_i sont premiers deux à deux distincts, on sait que les diviseurs de n sont les $d = \prod_{i=1}^{r} p_i^{\beta_i}$ pour $0 \leq \beta_i \leq \alpha_i$ où $\mu(d) = 0$ si l'un des β_i est supérieur ou égal à 2. Ainsi $(\mu * \mathbb{1})(n) = \sum_{(\beta_1, \dots, \beta_r) \in \{0,1\}^r} \mu\left(\prod_{i=1}^{r} p_i^{\beta_i}\right)$. Pour $i \in [\![1, r]\!]$, il y a $\binom{r}{i}$ façons de choisir un r-uplet $(\beta_1, \dots, \beta_r)$ formé de i termes égaux à 1 et $r-i$ termes égaux à 0, et pour chaque choix, $\mu\left(\prod_{i=1}^{r} p_i^{\beta_i}\right) = (-1)^i$.
Donc $(\mu * \mathbb{1})(n) = \mu(1) + \sum_{i=1}^{r} \binom{r}{i} (-1)^i = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = (1-1)^r = 0$.

Preuve du théorème 1 : On a les équivalences suivantes, d'après la propriété qui précède :

$$\left(\forall n\geq 1, f(n)=\sum_{d\mid n} g(d)\mathbb{1}\left(\tfrac{n}{d}\right)\right) \Leftrightarrow f=g*\mathbb{1} \Leftrightarrow f*\mu = g*\overbrace{\mathbb{1}*\mu}^{e} \Leftrightarrow g=f*\mu$$

$$\Leftrightarrow \left(\forall n\geq 1, g(n)=\sum_{d\mid n}\mu(d)f\left(\tfrac{n}{d}\right)\right).$$

Preuve du lemme : Etape 1 : Montrons que $\prod_{d\mid n}\prod_{P\in\mathcal{P}_q(d)} P \mid X^{q^n}-X$.

Soit $d\mid n$ et $P\in\mathcal{P}_q(d)$. Soit $K=\frac{\mathbb{F}_q[X]}{\langle P\rangle}$, qui est un corps (car $\mathbb{F}_q[X]$ est principal) de cardinal q^d (en fait corps de rupture de P, $K=\mathbb{F}_q(\alpha)$ et $P=\mathrm{Min}(\alpha,\mathbb{F}_q)$). Donc K^* est un groupe multiplicatif d'ordre q^d-1, donc $\overline{X}^{q^d-1}=\overline{1}$ (d'après le thm de Lagrange), ainsi $\overline{X}^{q^d}=\overline{X}$.

Par récurrence immédiate, on en déduit $\overline{X}^{q^{dk}}=(((\overline{X}^{q^d})^{q^d})^{\cdots})^{q^d}=\overline{X}$ pour $k\in\mathbb{N}$.

Or comme d divise n, $\exists k\in\mathbb{N}$, $n=kd$, donc $\overline{X}^{q^n}=\overline{X}$ ie $\overline{X^{q^n}-X}=0$ dans $K=\frac{\mathbb{F}_q[X]}{\langle P\rangle}$ donc P divise $X^{q^n}-X$.

Or les éléments des $\mathcal{P}_q(d)$ pour $d\mid n$ sont des polynômes irréductibles non associés (car unitaires) donc premiers entre eux. Ainsi, d'après le lemme d'Euclide, $\prod_{d\mid n}\prod_{P\in\mathcal{P}_q(d)} P \mid X^{q^n}-X$.

Etape 2 : Montrons l'égalité.

Réciproquement, soit P est un facteur irréductible de degré d de $X^{q^n}-X$ dans $\mathbb{F}_q[X]$. Or $\mathbb{F}_{q^n}$ est un corps de décomposition de $X^{q^n}-X$, donc P est scindé sur $\mathbb{F}_{q^n}$. Donc pour α est une racine de P dans $\mathbb{F}_{q^n}$, alors $\mathbb{F}_q\subseteq\mathbb{F}_q(\alpha)\subseteq\mathbb{F}_{q^n}=D_{\mathbb{F}_q}(X^{q^n}-X)$. Ainsi par thm de la base télescopique,

$$[\mathbb{F}_{q^n}:\mathbb{F}_q(\alpha)]\underbrace{[\mathbb{F}_q(\alpha):\mathbb{F}_q]}_{\substack{\text{corps de rupture de } P\\ \text{(irréd) de deg } d}}=\underbrace{[\mathbb{F}_{q^n}:\mathbb{F}_q]}_{=n}$$ donc $d\mid n$.

Ainsi $P\in\mathcal{P}_q(d)$ pour un $d\mid n$.

Or $X^{q^n}-X$ n'admet pas de facteur carré : en effet, si c'était le cas alors le polynôme aurait une racine double dans un corps de décomposition sur $\mathbb{F}_q$, mais $(X^{q^n}-X)'=q^nX^{q^n-1}-1=-1$ (car $\mathrm{car}(K)=p$) donc cela contredit l'existence d'une éventuelle racine double (car $P'\wedge P=1$). Ainsi $\prod_{d\mid n}\prod_{P\in\mathcal{P}_q(d)} P = X^{q^n}-X$.

Preuve du théorème : En passant aux degrés dans l'égalité précédente, on obtient $q^n=\sum_{d\mid n}\sum_{P\in\mathcal{P}_q(d)}\deg(P)=\sum_{d\mid n} d\,I(q,d)$ (*)

Donc par inversion de Möbius, avec $f(n)=q^n$ et $g(n)=nI(q,n)$, on obtient $\boxed{nI(q,n)=\sum_{d\mid n}\mu\left(\tfrac{n}{d}\right)q^d}$

Montrons maintenant que pour tout $n \in \mathbb{N}^*$, $I(q,n) \geq 1$.

Pour $n=1$, $I(q,1) = q \geq 2$ et pour $n=2$, $I(q,2) = \frac{q^2-q}{2} \geq 1$.

Pour $n \geq 3$, on a $nI(q,n) = q^n + \underbrace{\sum_{\substack{d|n \\ d\neq n}} \mu\left(\frac{n}{d}\right) q^d}_{x_n}$ où

$$|x_n| \leq \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} q^d = \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - q}{q-1} < q^{\lfloor \frac{n}{2} \rfloor + 1} \leq q^{\frac{n}{2}+1}$$

Donc $nI(q,n) > q^n - q^{\frac{n}{2}+1} \geq 0$ donc $I(q,n) > 0$.

Ainsi pour tout $n \in \mathbb{N}^*$, il existe des polynômes irréductibles de degré n dans $\mathbb{F}_q[X]$. De plus,

$$\left| \frac{nI(q,n)}{q^n} - 1 \right| = \left| \frac{1}{q^n} x_n \right| \leq \frac{q^{\frac{n}{2}+1}}{q^n} = \frac{1}{q^{\frac{n}{2}-1}} \xrightarrow[n\to+\infty]{} 0, \text{ d'où } I(q,n) \underset{n\to+\infty}{\sim} \frac{q^n}{n}$$

<u>Remarques</u> : * La fct° de Möbius est souvent utilisée pour la combinatoire, voici un autre exemple classique : $\forall n \geq 1$, $n = \sum_{d|n} \varphi(d)$ (indicatrice d'Euler) et donc $\forall n \geq 1$, $\varphi(n) = \sum_{d|n} d\,\mu\left(\frac{n}{d}\right)$. (intérêt aussi pour les produits de séries de Dirichlet $\mathcal{D}f(s) = \sum_{n=1}^{+\infty} \frac{f(n)}{n^s}$, afin de les appliquer à la fct° ζ, ou encore (c'est lié) à la proport° d'entiers premiers entre eux, cf cours de Théo)

* Si $P \in \mathcal{P}_p(n)$, alors $\mathbb{F}_p[X]/\langle P \rangle$ est un corps à p^n éléments, et ça déjà c'est chouette en pratique pour construire des corps, et ensuite c'est le seul corps à p^n élts à iso près, et c'est aussi sympa pour la théorie par exemple pour étudier les automorphismes de $\mathbb{F}_{p^n}$ (groupe cyclique d'ordre n engendré par le Frobenius) (cf Rombaldi).

* Dans $\mathbb{F}_q[X]$, il y a q^{n-1} polynômes unitaires de degré n, il y a donc une proportion de l'ordre de $\frac{q}{n}$ polynômes irréductibles parmi ces derniers.

* Quelques polynômes irréductibles :

- sur $\mathbb{F}_2$: $\mathcal{P}_2(1) = \{X, X+1\} \Rightarrow I(2,1) = 2$

  $\mathcal{P}_2(2) = \{X^2+X+1\} \Rightarrow I(2,2) = 1$

  $\mathcal{P}_2(3) = \{X^3+X+1, X^3+X^2+1\} \Rightarrow I(2,3) = 2$

  $\mathcal{P}_2(4) = \{X^4+X^3+X^2+X+1, X^4+X^3+1, X^4+X+1\} \Rightarrow I(2,4) = 3$

tout ça peut se vérifier à l'aide de la formule.

et donc par ex, sur $\mathbb{F}_2$,

$$X^{2^4} - X = \underbrace{X(X+1)}_{\mathcal{P}_2(1)} \underbrace{(X^2+X+1)}_{\mathcal{P}_2(2)} \underbrace{(X^4+X^3+X^2+X+1)(X^4+X^3+1)(X^4+X+1)}_{\mathcal{P}_2(4)}.$$

- sur $\mathbb{F}_3$: $\mathcal{P}_3(1) = \{X, X+1, X+2\} \Rightarrow I(3,1) = 3$

  $\mathcal{P}_3(2) = \{X^2+1, X^2+X+2, X^2+2X+2\} \Rightarrow I(3,2) = 3$

* On peut déduire du lemme un critère d'irréductibilité : si P est un polynôme de degré n de $\mathbb{F}_q[X]$, alors
P est irréductible sur $\mathbb{F}_q[X] \iff \begin{cases} P \mid X^{q^n} - X \\ \forall d \mid n,\ d \text{ premier},\ P \wedge (X^{q^{n/d}} - 1) = 1. \end{cases}$