Développement. Dénombrement des polynômes irréductibles sur un corps fini

Soient p un nombre premier et $n \geqslant 1$ un entier non nul. Avec $q \coloneqq p^n$, on considère le polynôme $P_n \coloneqq X^q - X \in \mathbf{F}_p[X]$.

Lemme 1. Soit $d \geqslant 1$ un entier vérifiant $p^d - 1 \mid p^n - 1$. Alors $d \mid n$.

Preuve On écrit $n = qd + r$ la division euclidienne de n par d. D'une part, on écrit

$$p^n - 1 = p^{qd}p^r - 1 = (p^{qd} - 1)p^r + p^r - 1.$$

D'autre part, on a

$$p^d - 1 \mid (p^d - 1)(p^{q(d-1)} + p^{q(d-2)} + \cdots + 1) = p^{qd} - 1.$$

Comme $p^d - 1 \mid p^n - 1$, les deux dernières divisibilités donnent $p^d - 1 \mid p^r - 1$. Dès lors, si $r \neq 0$, alors $p^r - 1 \neq 0$ et on peut écrire $p^d - 1 \leqslant p^r - 1$ ce qui implique $p^d \leqslant p^r$ puis $d \leqslant r$: c'est impossible car la division euclidienne impose d'avoir $r < d$. Ainsi on obtient $r = 0$ si bien que $n = qd$. ◁

Lemme 2. Tout facteur irréductible sur $\mathbf{F}_p$ du polynôme P_n est de degré divisant n. Réciproquement, pour tout diviseur d de l'entier n, tout polynôme irréductible sur $\mathbf{F}_p$ de degré d divise le polynôme P_n.

Preuve Soit $P \in \mathbf{F}_p[X]$ un facteur irréductible de degré $d \geqslant 1$ du polynôme P_n. On veut montrer que $d \mid n$. Par hypothèse, on a $P_n \equiv 0 \mod P$, c'est-à-dire

$$X^q \equiv X \mod P. \tag{1}$$

Soit $Q \coloneqq \sum_{k=0}^{r} a_k X^k \in \mathbf{F}_p[X]$ un polynôme premier avec le polynôme P. Montrons que

$$Q^{q-1} \equiv 1 \mod P. \tag{2}$$

Alors l'action du morphisme de Frobenius et l'hypothèse (1) donnent

$$\begin{aligned} Q^q &\equiv \Big(\sum_{k=0}^{r} a_k X^k\Big)^q \mod P \\ &\equiv \sum_{k=0}^{r} a_k^q (X^q)^k \mod P \\ &\equiv Q \mod P \end{aligned}$$

si bien qu'on conclut la congruence (2) puisque le polynôme P est premier avec le polynôme Q. De cette congruence (2) et comme $\mathbf{F}_{p^d} \simeq \mathbf{F}_p[X]/\langle P\rangle$, on en déduit que

$$\forall x \in \mathbf{F}_{p^d}^{\times}, \qquad x^{q-1} = 1.$$

Maintenant, le groupe

$$\mathbf{F}_{p^d}^{\times} \simeq \mathbf{Z}/(p^d - 1)\mathbf{Z}$$

étant d'ordre $p^d - 1$, on obtient $p^d - 1 \mid q - 1$, c'est-à-dire $d \mid n$.

Réciproquement, soit $P \in \mathbf{F}_p[X]$ un polynôme irréductible de degré $d \mid n$. Montrons que $P \mid P_n$. Alors le corps $\mathbf{F}_p[X]/\langle P\rangle$ est de cardinal p^d, donc son groupe multiplicatif $\mathbf{Z}/(p^d - 1)\mathbf{Z}$ est de cardinal $p^d - 1$. Par conséquent, le théorème de Lagrange assure que

$$X^{p^d - 1} \equiv 1 \mod P,$$

c'est-à-dire

$$X^{p^d} \equiv X \mod P.$$

Une récurrence immédiate montre que

$$\forall k \in \mathbf{N}, \qquad X^{p^{kd}} \equiv X \mod P.$$

Comme $d \mid n$, on en déduit que $X^{p^n} \equiv X \mod P$, c'est-à-dire $P \mid P_n$. ◁

Théorème 3. Pour un entier $d \in \mathbf{N}$, on considère l'ensemble $I_d(p) \subset \mathbf{F}_p[X]$ des polynômes unitaires de degré d sur $\mathbf{F}_p$. Alors

$$X^{p^n} - X = \prod_{d \mid n} \prod_{P \in I_d(p)} P.$$

Preuve La seconde partie du lemme permet d'écrire

$$R \coloneqq \prod_{d \mid n} \prod_{P \in I_d(p)} P \mid P_n.$$

Réciproquement, soit $Q \in \mathbf{F}_p[X]$ un facteur irréductible du polynôme P_n. Alors son degré d divise n d'après la première partie du lemme, donc $Q \mid R$. Comme $P_n' = -1$, le polynôme P_n est premier avec son dérivé P_n', donc il ne possède pas de facteur carré. De ces deux derniers faits découle ainsi la divisibilité $P_n \mid R$. ◁

Corollaire 4. Notons $\mu \colon \mathbf{N}^* \longrightarrow \{-1, 0, 1\}$ la fonction de Möbius. Alors

$$\sharp I_n(p) = \frac{1}{n} \sum_{d \mid n} \mu\Big(\frac{n}{d}\Big)\, p^d.$$

Preuve Le théorème permet d'écrire

$$p^n = \sum_{d \mid n} d \times \sharp I_d(p)$$

et la formule d'inversion de Möbius conclut. ◁

[1] Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation. Algèbre et géométrie.* 2e édition. De Boeck Supérieur, 2021.