Comptage de polynômes irréductibles unitaires de $\mathbb{F}_q[X]$

Leçons 123,125,141,190

Définition

Soit p un nombre premier et soit $q = p^r$. Soit l'ensemble:

$$\mathcal{A}(n,q) \quad = \quad \{\text{Polynômes de } \mathbb{F}_q[X] \text{ irréductibles, unitaires de degré } n\}$$

On pose également: $I(n,q) = \#\mathcal{A}(n,q)$

Théorème

On a les résultats suivants:

1. On a:
$$X^{q^n} - X \quad = \quad \prod_{d|n} \prod_{P \in \mathcal{A}(d,q)} P \tag{1}$$
2. Si μ est la fonction de Möbius, alors on a:
$$I(n,q) \quad = \quad \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$
3. On a l'équivalent: $I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$

Voici le plan de la démonstration:

1. Montrer le premier point en montrant que chaque polynôme divise l'autre (le plus difficile)
2. Passer aux degrés sur (1) puis utiliser la formule d'inversion de Möbius
3. Montrer le troisième point (c'est de l'analyse !)

Démonstration. *1. $X^{q^n} - X$ est scindé (ses racines sont les éléments de $\mathbb{F}_{q^n}$). Soit $P \in \mathcal{A}(d,q)$ un diviseur de $X^{q^n} - X$. $P | X^{q^n} - X$ et $X^{q^n} - X$ est scindé dans $\mathbb{F}_{q^n}$ donc les racines de P sont aussi dans $\mathbb{F}_{q^n}$. Soit $\alpha \in \mathbb{F}_{q^n}$ une racine de P. $P \in \mathbb{F}_q[X]$ est irréductible et $P(\alpha) = 0$, donc P est le polynôme minimal de α sur $\mathbb{F}_q$. Donc, par le théorème de la base télescopique, on a $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)] \underbrace{[\mathbb{F}_q(\alpha) : \mathbb{F}_q]}_{=d}$*

donc $d|n$ et on a:

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

Réciproquement, soit d un diviseur de n, soit $P \in \mathcal{A}(d,q)$. Soit $\mathbb{F}_q(\alpha)$ un corps de rupture de P, où $\alpha \in \mathbb{F}_{q^n}$. Alors $\mathbb{F}_q(\alpha) \simeq \mathbb{F}_{q^d} \hookrightarrow \mathbb{F}_{q^n}$ car $d|n$, et α est bien une racine de $X^{q^n} - X$. Or, P est irréductible sur $\mathbb{F}_q$, donc est à racines simples dans $\mathbb{F}_{q^n}$ (cf. Lemme 2) donc $P|X^{q^n} - X$. $X^{q^n} - X$ est scindé à racines simples sur $\mathbb{F}_{q^n}$, donc chaque diviseur irréductible est de multiplicité 1, donc on a:

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

Les polynômes considérés étant unitaires, on a bien l'égalité (1)

2. *On montre la formule d'inversion de Möbius:*

Lemme 1

Soit $f : \mathbb{N}^* \longrightarrow \mathbb{R}$, et soit g donnée par:

$$\begin{array}{rccc} g: & \mathbb{N}^* & \longrightarrow & \mathbb{R} \\ & n & \longmapsto & \sum_{d|n} f(d) \end{array}$$

Alors, pour tout $n \in \mathbb{N}^*$, on a:

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

Démonstration. *Posons:*

$$S_n = \sum_{d|n} \mu(d)$$

On a $S_1 = 1$. Si $n \geqslant 2$, soit P_n l'ensemble des diviseurs premiers de n. On a:

$$\begin{aligned} S_n &= \sum_{D \subset P_n} \mu\left(\prod_{p \in D} p\right) \\ &= \sum_{D \subset P_n} (-1)^{|D|} \qquad (2) \\ &= \sum_{j=0}^{|P_n|} \binom{|P_n|}{j} (-1)^j \qquad (3) \\ &= (1-1)^{|P_n|} \\ &= 0 \end{aligned}$$

avec, par convention:

$$\prod_{p \in \emptyset} p = 1$$

Ainsi, on a:

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

■

En regardant les degrés dans l'expression (1)*, on établit que:*

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

Ainsi, en appliquant la formule d'inversion de Möbius, on obtient:

$$I(n,q) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d \tag{4}$$

3. *Il reste à montrer l'équivalent demandé. On sait que:*

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

Or, on a:

$$\begin{aligned}\left|\sum_{d|n,d<n}\mu\left(\frac{n}{d}\right)q^d\right| &\leqslant \sum_{d=1}^{\lfloor\frac{n}{2}\rfloor}q^d\\ &= \frac{q^{\lfloor\frac{n}{2}\rfloor}-1}{q-1}\\ &\underset{n\to+\infty}{=} o\left(q^n\right)\end{aligned}$$

D'où:

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

■

Remarques. *1. Voici le lemme 2:*

> **Lemme 2**
> *Si $P \in \mathbb{F}_q[X]$ est irréductible, alors il est à racines simple dans $\mathbb{F}_{q^n}$.*

Démonstration. *Si P admet une racine double $\alpha \in \mathbb{F}_{q^n}$, alors on a également $P'(\alpha) = 0$. $P(\alpha) = 0$ et P est irréductible sur $\mathbb{F}_q$ donc P est le polynôme minimal de α sur $\mathbb{F}_q$. Or, $\deg(P') < \deg(P)$ donc on a $P' = 0$. Comme on est en caractéristique p, cela veut dire qu'il existe $R \in \mathbb{F}_q[X]$ tel que $P = R^p$, donc P n'est pas irréductible, ce qui est absurde.*

■

2. *Le passage de (2) à (3) s'explique par le fait que si $|D| = j$, alors on a $\begin{pmatrix} |P_n| \\ j \end{pmatrix}$ choix possible pour $D \subset P_n$.*
3. *Afin d'obtenir l'égalité (4), on a pris dans la formule d'inversion de Möbius les fonctions $f(n) = nI(n,q)$ et $g(n) = q^n$ (cf. Lemme 1).*