Dénombrement des polynômes unitaires irréductibles sur $\mathbb{F}_p[X]$.

Leçons : 123, 125, 141, 144, 190

Référence : Rombaldi pour partie II et Brezis pour partie I.

Lemme Inversion de Möbius par la convolution de Dirichlet.

Dans $(\mathbb{R}^{\mathbb{N}^*}, +, *)$, $\mu * \mathbb{1} = \mathbb{1} * \mu = \delta_1$.

Théorème Soit $n \geq 1$ et p premier. Il y a $\frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$ polynômes unitaires irréductibles sur $\mathbb{F}_p$.

Démonstration du lemme.

1) Convolution de Dirichlet

On se place dans $F = \mathbb{R}^{\mathbb{N}^*}$ $\left(= (\mathbb{R}^{\mathbb{N}^*}, +)\right)$. Pour tout $f, g \in F$, on note :

$$(f*g)(n) := \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) \quad \forall n \geq 1.$$

On montre facilement que $(F, *)$ est un anneau commutatif intègre, dont le neutre pour $*$ est noté $\delta_1 = (1, 0, \dots)$.

Savoir le montrer.

$f, g \in F \setminus \{0\}$. $a = \min\{k \geq 1 \mid f(k) \neq 0\}$

$b = \min\{k \geq 1 \mid g(k) \neq 0\}$

$n = ab$

$f*g(n) = \sum_{ab=n} f(a)g(b) = f(b)g(a) \neq 0$

2) Définition de la fonction de Möbius

$$\mu : \mathbb{N}^* \longrightarrow \{-1, 0, 1\}$$

$$p_1^{\alpha_1} \cdots p_r^{\alpha_r} = n \longmapsto \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } \exists i \in \{1, \dots, r\},\ \alpha_i \geq 2 \\ (-1)^r & \text{sinon.} \end{cases}$$

μ a pour inverse $\mathbb{1} = (1)_{n\geq 1}$ pour $*$: si $n=1$, $\mu(1) = 1$.

$$\forall n \geq 1, \quad (\mu * \mathbb{1})(n) = \sum_{d|n} \mu(d)$$

$$= \sum_{k=1}^{r} \binom{r}{k} (-1)^k$$ où $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, donc seuls les produits $p_{i_1} \cdots p_{i_j}$ contribuent à la somme.

$$\left.\begin{array}{l} = (1-1)^r = 0 \quad \text{si } n > 1 \\ \\ = 1 \quad \text{si } n = 1 \end{array}\right.$$

$$= \delta_1 .$$

D'où $\mu * \mathbb{1} = \mathbb{1} * \mu = \delta_1$. De plus, si $f, g \in F$, on a alors :

$$\forall n \geq 1, \ g(n) = \sum_{d|n} f(d) \iff g = f * \mathbb{1}$$

$$\iff g * \mu = f$$

$$\iff \forall n \geq 1, \ f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

C'est la formule d'inversion de Möbius. □

<u>Démonstration du théorème</u> :

Soit p premier. Notons :

* $U_d(p) := \{ P \in \mathbb{F}_p[X], \ P \text{ unitaire irréductible sur } \mathbb{F}_p \text{ et } d^\circ P = d \}$

* $I(d,p) := \text{card}\,(U_d(p))$.

* $Q_n = X^{p^n} - X \in \mathbb{F}_p[X]$.

On souhaiterait montrer que $Q_n = \prod_{d|n} \prod_{P \in \mathcal{U}_d(p)} P$. Pour cela, on montre que si $P \in \mathcal{U}_d(p)$ alors on a l'équivalence suivante :

$$\boxed{P \mid Q_n \iff d \mid n}$$

Si $P, Q \mid Q_n$ et $P \neq Q$ alors $P \wedge Q = 1$ car P et Q unitaire donc $PQ \mid Q_n$.

$\boxed{\Rightarrow}$ Supposons que $P \mid Q_n$. Dans $\mathbb{F}_{p^n}$, on a $x^{p^n} = x$ pour tout $x \in \mathbb{F}_{p^n}$, donc $Q_n = \prod_{x \in \mathbb{F}_{p^n}} (X - x)$. Donc $\mathrm{Dec}_{\mathbb{F}_p}(P) \subset \mathbb{F}_{p^n}$. Soit $\mathbb{K}$ un corps de rupture, ie $\mathbb{K} \simeq \mathbb{F}_p[X]/(P) \simeq \mathbb{F}_{p^d}$. On a alors :

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{K}] \times [\mathbb{K} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{K}] \times d$$

par la théorème de la base téléscopique. D'où $d \mid n$.

$\boxed{\Leftarrow}$ Supposons que $d \mid n$. Soit $q \in \mathbb{N}$, $n = qd$. Il s'agit de montrer que $\overline{Q_n} = 0$ dans $\mathbb{K}$. Soit α l'image de X dans $\mathbb{K}$. On a alors :

$$\alpha^{p^n} = \alpha^{p^{qd}} = \alpha^{p^d \cdots p^d} = \left(\alpha^{p^d}\right)^{p^d \cdots p^d} = \alpha \quad \text{car } \mathbb{K} \simeq \mathbb{F}_{p^d}.$$

D'où $\overline{Q_n} = 0$ dans $\mathbb{K}$.

On a donc bien $Q_n = \prod_{d|n} \prod_{P \in \mathcal{U}_d(p)} P$. Si l'on compare les degrés de ces polynômes on a :

$$\forall n \geq 1, \quad p^n = \sum_{d|n} d\, I(d,p) \iff \forall n \geq 1, \quad I(n,p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

$\Rightarrow$ un équivalent ?