Développement : Dénombrements des polynômes irréductibles unitaires sur un corps fini.

RM

2022-2022

Référence :

1. Corps commutatif Tauvel

Énoncé :

Soit p un nombre premier. Pour $n \in \mathbb{N}^*$, on note $\mathcal{P}_p(n)$ l'ensemble des polynômes unitaires irréductibles de degré n de $\mathbb{F}_p[X]$ et $I_p(n)$ le cardinal de $\mathcal{P}_p(n)$. Alors on a

$$I_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}.$$

Résolution :

On va démontrer un théorème et une proposition pour conclure.

Théorème 1 : Soient p un entier premier et $n \in \mathbb{N}^*$, et soit $q = p^n$. Alors,

$$X^q - X = \prod_{d|n} \prod_{P \in \mathcal{P}_p(d)} P(X).$$

Démonstration : Notons $Q(X)$ le second membre de l'égalité ci-dessus. Le polynôme X divise $X^q - X$.
Soient d un diviseur de n, $r = p^d$, et $P \in \mathcal{P}_p(d)$ distinct de X. Comme P est irréductible, on a que $\mathbb{F}_r = \mathbb{F}_p[X]/(P)$ et donc il y a un élément dans $\mathbb{F}_r$ qu'on appelle α tel que son polynôme minimal soit P. Or pour tout élément x de $\mathbb{F}_r^*$, on a $x^{r-1} = 1$ et donc $x^r - x = 0$. Donc $\alpha^r - \alpha = 0$ et on a que le polynôme minimal de α divise $X^r - X$. On a donc que P divise $X^r - X$, et donc $X^{r-1} - 1$ par lemme d'Euclide car P irréductible. Par ailleurs, $\mathbb{F}_r$ est un sous corps de $\mathbb{F}_q$, donc $\mathbb{F}_r^*$ est un sous-groupe de $\mathbb{F}_q^*$. Il en résulte que $r - 1$ divise $q - 1$. On note $q - 1 = k(r - 1)$.
Comme $X^{q-1} = X^{k(r-1)} = (X^{r-1})^k$, et que $X^{r-1} \equiv 1[X^{r-1} - 1]$, alors $X^{q-1} \equiv 1^k \equiv 1[X^{r-1} - 1]$ et donc $X^{r-1} - 1 | X^{q-1} - 1$. On en déduit donc que P divisant $X^{r-1} - 1$, on a $P | X^{q-1} - 1$.
Donc si d divine n et si $P \in \mathcal{P}_p(d)$, alors P divise $X^q - X$. Pour d divisant n, les polynômes $P \in \mathcal{P}_p(d)$ sont premiers entre eux deux à deux. On en déduit alors que Q divise $X^q - X$.
Écrivons $X^q - X = R(X)Q(X)$, avec $R \in \mathbb{F}_p[X]$ unitaire. Supposons $R \neq 1$, et soit S un facteur irréductible de R. Donc S divise $X^q - X$ et on a alors que $deg(S)|n$. Cela signifie que S est aussi un facteur de S, et donc que $X^q - X$ est divisible par S^2. Comme $X^q - X$ est scindé sur $\mathbb{F}_q$, il en résulte que $X^q - X$ a une racine double dans $\mathbb{F}_q$. C'est absurde car $(X^q - X)' = qX^{q-1} - 1 = -1$ (caractéristique q) et donc finalement on a le résultat voulus. □

Proposition 2 : Soient $g : \mathbb{N}^* \mapsto \mathbb{C}$. Alors pour $n \in \mathbb{N}^*$, on a pour $G(n) = \sum_{d|n} g(n/d)$

$$g(n) = \sum_{d|n} \mu(d) G(n/d).$$

où μ est la fonction de Möbius.

Démonstration : Pour cela on remarque que pour $n \geq 2$,$\sum_{d|n} \mu(d) = 0$.
On pose $S(n) = \sum_{d|n} \mu(d)$. On a donc que $S(1) = 1$ et on va montrer que $S(n) = 0$ pour $n \geq 2$.
Tout d'abords, si n est premiers, alors $S(n) = \mu(1) + \mu(n) = 1 + (-1)^1 = 0$ et c'est donc vrai.
Si n n'est pas premier, on considère sa décomposition en produit de facteur premiers : $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ avec donc $p_1, ..., p_k$ des nombres premiers distincts et $\alpha_1, ..., \alpha_k$ des entiers strictement positifs. Or $\mu(d)$ est non nul si d est sans facteur carré, c'est-à-dire si $d = \prod_{i \in I} p_i$ ou $I \subset [\![1\,;k]\!]$.
On a donc $\mu(d) = (-1)^{Card(I)}$. Cela correspond donc à choisir i nombre entre $p_1, ..., p_k$. Il y a donc $\binom{k}{i}$ choix possible. On en déduit que

$$\sum_{d|n} \mu(d) = \sum_{i=0}^{k} \binom{k}{i} (-1)^i = (1-1)^k = 0$$

On a donc que $\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \geq 2 \end{cases}$

Alors

$$\begin{aligned}
\sum_{d|n} \mu(d) G(n/d) &= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} g(n/dd') \\
&= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} g(d') \text{ En parcourant la somme dans l'autre sens} \\
&= \sum_{dd'|n} \mu(d) g(d') \text{ car } d'|\frac{n}{d} \Leftrightarrow dd'|n \\
&= \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu(d) = g(n) \text{ car } \sum_{d|\frac{n}{d'}} \mu(d) \neq 0 \text{ si } \frac{n}{d'} = 1
\end{aligned}$$

□

Maintenant, on utilise le théorème 1 en utilisant une égalité sur les degré. Le terme de gauche est de degré p^n et le terme de droite est de degré $\sum_{d|n} \sum_{P \in \mathcal{P}_p(d)} d = \sum_{d|n} d I_p(d)$.
On en déduit que $p^n = \sum_{d|n} d I_p(d)$.
Pour finir, on va appliquer la formule d'inversion de Möbius sur la fonction $g(n) = n I_p(n)$. Donc

$$n I_p(n) = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} d' I_p(d') = \sum_{d|n} \mu(d) p^{n/d}.$$

(car de même on peut remplacer n/dd' par d' en parcourant dans l'autre sens). Finalement on trouve bien

$$I_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}.$$