Rombaldi p423

POLYNÔMES IRRÉDUCTIBLES SUR UN CORPS FINI

123, 125, 141, 190

Soit p un nombre premier. Pour $n \in \mathbb{N}^*$, notons $U_n(p)$ l'ensemble des polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$, et notons $I_n(p)$ le cardinal de $U_n(p)$. Posons $P_n = X^{p^n} - X$.

Lemme : 1▸ Si $P \in \mathbb{F}_p[X]$ est irréductible et divise P_n, alors $\deg(Q) \mid n$.
2▸ Pour tout $d \mid n$, pour tout $P \in U_d(p)$, P divise P_n.

Thm : $P_n (= X^{p^n} - X) = \prod_{d \mid n} \prod_{P \in U_d(p)} P$ et P_n est sans facteur carré.

Cor : $I_n(p) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$

Fonction de MOEBIUS:

$$\mu : n \longmapsto \begin{cases} 1 \text{ si } n = 1 \\ (-1)^r \text{ si } n \text{ est le produit de } r \text{ facteurs premiers distincts} \\ 0 \text{ sinon} \end{cases}$$

Thm (formule d'inversion) : Soit $(u, v) \in (\mathbb{R}^{\mathbb{N}^*})^2$.
Si $\forall n \in \mathbb{N}^*$, $u_n = \sum_{d \mid n} v_d$, alors $\forall n \in \mathbb{N}^*$, $v_n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) u_d$.

Preuve du Lemme : 1▸ Soit $P \mid P_n$ irréductible - on peut le supposer unitaire. Posons $d = \deg(P)$ (Rq : $P \in U_d(p)$). Comme $P \mid P_n$ et P est irréductible, $\overline{P_n} = \overline{0}$ dans le corps $\frac{\mathbb{F}_p[X]}{\langle P \rangle} = \mathbb{F}_{p^d}$, autrement dit $\overline{X}^{p^n} = \overline{X}$. Or $(\overline{X}^k)_{0 \leq k \leq d-1}$ est une $\mathbb{F}_p$-base de $\mathbb{F}_{p^d}$, donc pour tout $\overline{Q} = \sum_{k=0}^{d-1} a_k \overline{X}^k \in \mathbb{F}_{p^d}$, $\overline{Q}^{p^n} = \sum_{k=0}^{d-1} a_k^{p^n} \left(\overline{X}^k\right)^{p^n} = \sum_{k=0}^{d-1} a_k \overline{X}^k = \overline{Q}$ (morphisme de FROBENIUS, puis théorème de FERMAT : $a_k^p = a_k$ dans $\mathbb{F}_p$). Par conséquent, $\forall \overline{Q} \in \mathbb{F}_{p^d}^\times$, $\overline{Q}^{p^n - 1} = \overline{1}$, mais $\mathbb{F}_{p^d}^\times$ est cyclique donc $p^d - 1 \mid p^n - 1$, donc $d \mid n$ (en effet, si $n = qd + r$ est la division euclidienne de n par d, alors $p^n - 1 = p^{qd+r} - 1 = (p^{qd} - 1)p^r + p^r - 1 = (p^d - 1)\left(1 + p^q + \cdots + p^{q(d-1)}\right)p^r + p^r - 1$, et $0 \leq p^r - 1 < p^d - 1$, donc on a là la division euclidienne de $p^n - 1$ par $p^d - 1$, mais $p^d - 1 \mid p^n - 1$ donc $p^r - 1 = 0$, i.e. $r = 0$, i.e. $d \mid n$).

2▸ Soit $P \in U_d(p)$. Avec les mêmes argument que ci-dessus, couplés au théorème de LAGRANGE, on montre que $\overline{X}^{p^d} = \overline{X}$ dans $\frac{\mathbb{F}_p[X]}{\langle P \rangle} = \mathbb{F}_{p^d}$. Or $\exists q \in \mathbb{N} : n = qd$, et $\overline{X}^{p^n} = \overline{X}^{p^{dq}} = \left(\overline{X}^{p^d}\right)^{p^{d(q-1)}} = (\overline{X})^{p^{d(q-1)}} = \cdots = \overline{X}$, donc $\overline{P_n} = \overline{X}^{p^n} - \overline{X} = \overline{0}$, i.e. $P \mid P_n$. ■

Preuve du Thm : $P_n' = p^n X^{p^n - 1} - 1 = -1$ ($P_n \in \mathbb{F}_p[X]$), donc $P_n \wedge P_n' = 1$, donc P_n est sans facteur carré. D'après le lemme, tout diviseur irréductible de P_n appartient à un $U_d(p)$ pour un $d \mid n$, donc $P \mid \prod_{d \mid n} \prod_{P \in U_d(p)} P$. Toujours d'après le lemme, pour tous $d \mid n$ et $P \in U_d(p)$, $P \mid P_n$, et comme P_n n'a pas de facteur carré, $\prod_{d \mid n} \prod_{P \in U_d(p)} P \mid P_n$. Enfin, ces deux polynômes sont unitaires et associés, donc égaux. ■

Preuve du Cor : En prenant les degrés : $p^n = \deg\left(\prod_{d \mid n} \prod_{P \in U_d(p)} P\right) = \sum_{d \mid n} \sum_{P \in U_d(p)} \underbrace{\deg(P)}_{= d} = \sum_{d \mid n} d\, I_d(p)$. D'après la formule d'inversion de MOËBIUS, $n I_n(p) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$. ■

Preuve de la formule d'inversion de MOEBIUS : Montrons d'abord que $\sum_{d \mid n} \mu(d) = \delta_{n=1}$: pour $n = 1$, c'est évident. Soit $n \geq 2$, écrivons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ sa décomposition en produit de facteurs premiers. On a donc :

$$\sum_{d \mid n} \mu(d) = \sum_{\substack{1 \leq i \leq r \\ 0 \leq k_i \leq \alpha_i}} \mu\left(p_1^{k_1} \cdots p_r^{k_r}\right) = \sum_{\substack{1 \leq i \leq r \\ k_i \in \{0,1\}}} \mu\left(p_1^{k_1} \cdots p_r^{k_r}\right) = \sum_{j=0}^{r} \sum_{\substack{1 \leq i \leq r \\ k_i \in \{0,1\},\ k_1 + \cdots + k_r = j}} (-1)^j = \sum_{j=0}^{r} \binom{r}{j} (-1)^j = (1 + (-1))^r = 0. \text{ De là,}$$

$$\sum_{d \mid n} \mu\left(\frac{n}{d}\right) u_d = \sum_{d \mid n} \mu(d)\, u_{n/d} = \sum_{d \mid n} \mu(d) \sum_{k \mid \frac{n}{d}} v_k = \sum_{d \mid n} \sum_{k \mid \frac{n}{d}} \mu(d) v_k = \sum_{d \cdot k \mid n} \mu(d) v_k = \sum_{k \mid n} \sum_{d \mid \frac{n}{k}} \mu(d) v_k = \sum_{k \mid n} \delta_{\frac{n}{k} = 1}\, v_k = v_n$$ ■