# Quelques résultats de dénombrement

Soit $q = p^n$ une puissance d'un nombre premier $p$. Soit $\mathbb{F}_q$ le corps à $q$ éléments et $\mathbb{F}_{q^m}$ son extension de degré $m$.

## 1 Nombre de polynômes irréductibles

Le nombre de polynômes à coefficients dans $\mathbb{F}_q$, normalisés, de degré $m$, irréductibles sur $\mathbb{F}_q$ est :

$$I_q(m) = \frac{1}{m} \sum_{d|n} q^d \mu(\frac{m}{d})$$

où la fonction de Möbius $\mu$ est définie par : soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$,

$$\mu(n) = \begin{cases} 0 & \text{si n divisible par un carré} \\ (-1)^k & \text{sinon} \end{cases}$$

## 2 Nombes de polynômes $q$-primitifs

On rappelle q'un polynôme $q$-primitif est le polynôme minimal d'un élément primitif de $\mathbb{F}_{q^m}$ dans l'extension $\mathbb{F}_{q^m}/\mathbb{F}_q$.

Le nombre de polynômes à coefficients dans $\mathbb{F}_q$, normalisés, de degré $m$, $q$-primitifs est :

$$J_q(m) = \frac{\phi(q^m - 1)}{m}$$

où la fonction d'Euler $\phi$ est définie par : soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$,

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

## 3 Nombre de polynômes nomaux

On rappelle que un élément $\alpha$ est normal dans l'extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ si

$$\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}\}$$

constitue une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$.

Le polynôme minimal d'un élément normal est appelé polynôme normal. Un tel polynôme est nécessairement de degré $m$.

Pour donner le nombre de polynômes normaux on doit introduire les notations suivantes. Écrivons le degré $m$ de l'extension sous la forme

$$m = m_1 p^e$$

où $\gcd(m_1, p) = 1$. Posons $t = p^e$. On sait alors que

$$X^m - 1 = X^{m_1 t} - 1 = (X^{m_1} - 1)^t.$$

De plus $X^{m_1} - 1$ n'a pas de facteurs multiples. Donc on peut écrire

$$X^{m_1} - 1 = \phi_1(X)\phi_2(X)\cdots\phi_r(X).$$

Notons $d_i$ le degré de $\phi_i$. Le nombre de polynômes normaux est

$$\boxed{V_q(m) = \frac{1}{m}\prod_{i=1}^{r} q^{d_i(t-1)}(q^{d_i} - 1)}$$