1 Formule de Mobius et dénombrements des polynômes irréductibles

Définition 1. *Soit $n \in \mathbb{N}$, on définit la fonction de Möbius $\mu : \mathbb{N} \to \mathbb{Z}$ par*

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ n'est pas produit de carrés,} \\ (-1)^k & \text{si } n \text{ est produit de } k \text{ nombres premiers distincts.} \end{cases} \tag{1}$$

Proposition 1. *Soit $n \geq 2$, alors*

$$\sum_{d|n} \mu(d) = 0. \tag{2}$$

Proof. On décompose n en produit de facteurs premiers

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}. \tag{3}$$

On peut ensuite décomposer la somme, en tenant compte que $\mu(d) = 0$ si deux diviseurs premiers divisent d,

$$\sum_{d|n} = \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{i \neq j} \mu(p_i p_j) + \ldots + \mu(p_1 \ldots p_n) \tag{4}$$

$$= \sum_{k=0}^{n} (-1)^k \binom{n}{k} \tag{5}$$

$$= 0. \tag{6}$$

□

Théorème 1 (Formule d'inversion de Möbius)**.** *Soit f une fonction arithmétique, on pose $g(n) = \sum_{d|n} f(d)$. Alors, on a*

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right). \tag{7}$$

Proof. On a

$$\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{e|\frac{n}{d}} f(e) \tag{8}$$

$$= \sum_{de|n} f(e)\mu(d) \tag{9}$$

$$= \sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d) \tag{10}$$

$$= f(n). \tag{11}$$

car $\sum_{d|\frac{n}{e}} \mu(d)$ vaut 0 si $e \neq n$ et 1 sinon. □

Application aux dénombrements de polynômes irréductibles sur $\mathbb{F}_q$

Définition 2. *Soit $\mathbb{K}$ un corps, un polynôme f de $\mathbb{K}[x]$ est dit irréductible si il n'est pas le produit de deux polynômes non inversibles de $\mathbb{K}[x]$, i.e.*

$$f = gh \implies g \in \mathbb{K}[x]^\times \text{ ou } h \in \mathbb{K}[x]^\times. \tag{12}$$

Proposition 2. *Soit q une puissance d'un nombre premier. On note $I(n,q)$ l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$. Alors, on a*

$$x^{q^n} - x = \prod_{d|n} \left(\prod_{f \in I(d,q)} f \right) \tag{13}$$

Proof. Soit $d|n$, on considère $g \in I(d,q)$. On considère ensuite K le corps de rupture de g sur $\mathbb{F}_q$. K est une extension de degré d qui sera isomorphe à $\mathbb{F}_{q^d}$, en considérant K comme $\mathbb{F}_q-$ev de dimension d (en prenant α comme élément primitif). On sait que $\alpha^{q^d} = \alpha$ donc α est une racine de $x^{q^n} - x$. On en déduit donc que f divise $x^{q^n} - x$.

Réciproquement, supposons que f est un facteur irréductible de $x^{q^n} - x$. On note d le degré de f. Par ailleurs, f est scindé dans $\mathbb{F}_{q^n}$ donc les racines de f sont dans $\mathbb{F}_{q^n}$. En particulier, si on considère le corps de rupture K de f sur F_q, on sait que K est une extension de $\mathbb{F}_q$ de degré d.

$$\mathbb{F}_q \subset K \cong \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}. \tag{14}$$

On peut aussi construire $\mathbb{F}_{q^n}$ comme un corps de rupture pour un polynôme irréductible de degré k, d'où

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_{q^d}][\mathbb{F}_{q^d} : \mathbb{F}_q]. \tag{15}$$

D'où $d|n$. □

Théorème 2.

$$|I(n,q)| = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d. \tag{16}$$

Proof. Utilisons la Proposition 2 et comparons les degrés de chaque côté :

$$q^n = \sum_{d|n} |I(d,q)| d. \tag{17}$$

Appliquons ensuite la formule d'inversion avec $n \mapsto |I(n,q)|$. On en déduit que

$$n|I(n,q)| = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d. \tag{18}$$

Il suffit ensuite de diviser par n des deux côtés pour obtenir le résultat attendu

$$|I(n,q)| = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d. \tag{19}$$

□

Remarque 1. *On récupère aussi un équivalent de* $|I(n,q)|$.

$$|I(n,q)| \sim \frac{q^n}{n}. \tag{20}$$

Pour cela, il suffit de remarquer les inégalités suivantes

$$\begin{aligned}
|\frac{1}{n}\sum_{d|n,d<n}\mu\left(\frac{n}{d}\right)q^d| &\leq \frac{1}{n}\sum_{d|n,d<n}|\mu\left(\frac{n}{d}\right)q^d| && (21)\\
&\leq \frac{1}{n}\sum_{d|n,d<n}q^d && (22)\\
&\leq \frac{1}{n}\sum_{d=1}q^{\lfloor\frac{n}{2}q^d\rfloor} && (23)\\
&= \frac{1}{n}\frac{q^{\lfloor\frac{n}{2}q^d\rfloor+1}-1}{q-1} && (24)
\end{aligned}$$

qui est un $o(q^n)$. *Ainsi,* $|I(n,q)| = \frac{q^n}{n} + o(q^n)$, *d'où* $|I(n,q)| \sim \frac{q^n}{n}$.