X

DENOMBREMENT DES POLYNÔMES IRRÉDUCTIBLES SUR $\mathbb{F}_q$.

chap 2 sujet d'étude
1 Gozard alg
+ FG p 189

Prérequis : corps de rupture, de décomposition, polynôme minimal
unicité corps fini, multiplicativité des degrés.

13'20 en faisant rapide sur Möbius. 12'15

15 sans Möbius.

Soit $q = p^m$ avec $p \in \mathbb{N}$ un nombre premier et $m \in \mathbb{N}^*$.

Pour tout $n \in \mathbb{N}$, on note $\mathcal{P}_q(n)$ l'ensemble des polynômes unitaires irréductibles de degré n dans l'anneau $\mathbb{F}_q[X]$. On note $I_q(n) = \mathrm{Card}\, \mathcal{P}_q(n)$.

Thm : On a . $X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P$, $q^n = \sum_{d|n} q^d I_q(d)$, $I_q(n) > 0$ et $I_q(n) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$

. Si μ est la fonction de Möbius, $I_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$.

Etape 1 : Dans $\mathbb{F}_q[X]$, on a $X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P$

- Soit $d|n$. Soit $P \in \mathcal{P}_q(d)$. Un corps de rupture de P est $K = \frac{\mathbb{F}_q[X]}{(P)}$, c'est un corps de cardinal q^d car $\deg P = d$. D'après l'unicité des corps finis, on a $K \simeq \mathbb{F}_{q^d}$.
On note $x \in K$ la classe de X dans K, c'est une racine de P.
Or $\mathbb{F}_{q^d}$ est par construction ~~le corps de décomposition~~ l'ens des racines de $X^{q^d} - X$, et comme $x \in K \simeq \mathbb{F}_{q^d}$, on a $x^{q^d} = x$.

  Ainsi, en écrivant $n = kd$ (car $d|n$) où $k \in \mathbb{N}^*$, on a

  $$x^{q^n} = x^{q^{kd}} = (x^{q^d})^{q^{(k-1)d}} = x^{q^{(k-1)d}} \overset{\text{réc}}{=} \dots = x^{q^d} = x$$

  Donc x est une racine de $X^{q^n} - X$, or P est le polynôme minimal de x sur $\mathbb{F}_q$ (il annule x et il est irréductible) donc $P | X^{q^n} - X$.

  Donc par irréductibilité, $\prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P \,\Big|\, X^{q^n} - X$.

- Réciproquement, soit $P \in \mathbb{F}_q[X]$ un facteur irréductible de $X^{q^n} - X$. Comme $X^{q^n} - X$ est scindé sur ~~$K \simeq$~~ $\mathbb{F}_{q^n}$ (car $\mathbb{F}_{q^n}$ est son corps de décomposition), il existe une racine x ~~$\in K$~~ de P dans $\mathbb{F}_{q^n}$.
Comme $\mathbb{F}_q(x)$ est un corps de rupture de P, c'est un corps intermédiaire entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ car $\mathbb{F}_{q^n}$ est le corps de décomposition.
On a donc

  $$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)] \underbrace{[\mathbb{F}_q(x) : \mathbb{F}_q]}_{= \deg P}.$$

  car P est le polynôme minimal de x car irréductible

  donc $\deg P | n$. Ainsi tout facteur irréductible de $X^{q^n} - X$ est de degré divisant n

- $X^{q^n} - X$ est sans facteur carré non constant sur $\mathbb{F}_q$:
(Supposons par l'absurde que $X^{q^n} - X = Q^2 P$ avec $Q, P \in \mathbb{F}_q[X]$ alors en dérivant,
$q^n X^{q^n - 1} - 1 = 2QQ'P + Q^2 P'$ donc $Q | q^n X^{q^n - 1} - 1 = -1$ donc Q est constant.

ou car premier avec son polynôme dérivé.

Ainsi, sa décomposition en produit de polynômes irréductibles dans $\mathbb{F}_q[X]$ ne contient que des facteurs simples. $\mathbb{F}_q$ corps donc $\mathbb{F}_q[X]$ factoriel ~~donc $\mathbb{F}_q$ factoriel~~

On écrit $X^{q^n}-X=\prod_{i=1}^{k} Q_i^{\alpha_i}$ donc $\alpha_i=1$, avec les Q_i deux à deux distincts.

et on a montré que $Q_i \in \mathcal{P}_q(d)$ avec $d \mid n$ donc $X^{q^n}-X \mid \prod_{d \mid n} \prod_{Q \in \mathcal{P}_q(d)} Q$

Or on a vu que $\prod_{d \mid n} \prod_{Q \in \mathcal{P}_q(d)} Q \mid X^{q^n}-X$ et ces deux polynômes sont unitaires donc ils sont égaux.

Etape 2 : $I_q(n)=\frac{1}{n}\sum_{d \mid n}\mu\left(\frac{n}{d}\right)q^d$ et $I_q(n)>0$. c'est $(q-1)I_q(n)$ pour pas avoir que les unitaires.

- On applique le degré à la formule obtenue à l'étape précédente : $q^n=\sum_{d \mid n} d\, I_q(d)$

(*) (On applique la formule d'inversion de Möbius à $n \mapsto n I_q(n)$ et on divise par n des deux côtés donc $I_q(n)=\frac{1}{n}\sum_{d \mid n} q^d \mu\left(\frac{n}{d}\right)$.)

- On a alors pour tout $k \in \mathbb{N}$ $k I_q(k) \leq q^k$ car $q^k = k I_q(k) + \underbrace{\sum_{\substack{d \mid k \\ d \neq k}} d\, I_q(d)}_{\geq 0}$

d'où

$$n I_q(n) = q^n - \sum_{\substack{d \mid n \\ d \neq n}} d\, I_q(d) \geq q^n - \sum_{\substack{d \mid n \\ d \neq n}} q^d$$

$$\geq q^n - \sum_{d=0}^{n-1} q^d \overset{q \neq 1}{=} q^n - \frac{q^n-1}{q-1} = \frac{q^n(q-2)+1}{q-1} > 0.$$

Etape 3 : On a $I_q(n) \underset{n\to+\infty}{\sim} \frac{q^n}{n}$

On va minorer plus finement. On sait déjà que $n I_q(n) \leq q^n$

De plus, $n I_q(n) = q^n - \sum_{\substack{d \mid n \\ d \neq n \\ d \neq 0}} d\, I_q(d) \geq q^n - \sum_{d=1}^{\lfloor n/2 \rfloor} q^d = q^n - \underbrace{q\,\frac{q^{\lfloor n/2 \rfloor}-1}{q-1}}_{\text{négligeable devant } q^n}$ $\quad q \neq 1$

Donc $I_q(n) \underset{n\to+\infty}{\sim} \frac{q^n}{n}$

~~Etape 3~~ : Expression avec la fonction de Möbius

(*)

Définition

La fonction μ de Möbius est définie par

$$\begin{array}{rcl} \mathbb{N}^* & \longrightarrow & \{-1,0,1\} \\ n & \longmapsto & \begin{cases} 1 & \text{si } n=1 \\ 0 & \text{si } n \text{ a un facteur carré} \\ (-1)^r & \text{si } n=p_1\dots p_r \text{ (premiers distincts)} \end{cases} \end{array}$$

Lemme

La fonction de Möbius vérifie :

1. μ est multiplicative : $\forall n,m \in \mathbb{N}^*, \mathrm{pgcd}(n,m)=1,\ \mu(nm)=\mu(n)\mu(m)$;
2. $\sum_{d \mid n}\mu(d) = \begin{cases} 1 & \text{si } n=1 \\ 0 & \text{sinon} \end{cases}$;
3. la formule d'inversion : si $g(n)=\sum_{d \mid n} f(d)$ alors $f(n)=\sum_{d \mid n} g(d)\mu\left(\frac{n}{d}\right)=\sum_{d \mid n} g\left(\frac{n}{d}\right)\mu(d)$.

Preuve : [FG p.93]

1. Si $n=1$ ou $m=1$, le résultat est évident car $\mu(1)=1$ par définition.
   Si n ou m a un facteur carré, nm a un facteur carré.
   Enfin, comme pgcd(n,m)=1, le dernier cas possible est $n=p_1\dots p_r$ et $m=q_1\dots q_s$ avec les p_i et les q_i des nombres premiers tous distincts. On a alors $\mu(nm)=\mu(p_1\dots p_r q_1\dots q_s)=(-1)^{r+s}=(-1)^r(-1)^s=\mu(p_1\dots p_r)\mu(q_1\dots q_s)=\mu(n)\mu(m)$.
2. Le cas $n=1$ est évident.

Notons $n=p_1^{\alpha_1}\dots p_r^{\alpha_r}$ sa décomposition en facteurs premiers.

$$\begin{aligned} \sum_{d \mid n}\mu(d) &= \mu(1)+\sum_{i=1}^{r}\mu(p_i)+\sum_{i<j}\mu(p_ip_j)+\sum_{i<j<k}\mu(p_ip_jp_k)+\dots+\mu(p_1\dots p_r)+0 \\ &= \sum_{k=0}^{r}\binom{r}{k}(-1)^k \\ &= (1-1)^r \\ &= 0 \end{aligned}$$

3.

$$\sum_{d \mid n} g\left(\frac{n}{d}\right)\mu(d) = \sum_{d \mid n}\sum_{d' \mid \frac{n}{d}} f(d')\mu(d) = \sum_{dd' \mid n} f(d')\mu(d) = \sum_{d' \mid n} f(d') \sum_{d \mid \frac{n}{d'}} \mu(d) = f(n)$$

(on a utilisé le point 2 pour la dernière égalité). Par changement de variable, on a

$$\sum_{d \mid n} g\left(\frac{n}{d}\right)\mu(d) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d).$$