

123, 141, 130

Lemme:

1. Soit P un diviseur irréductible de $P_m := X^{p^m} - X$ dans $\mathbb{F}_p[X]$. Alors $\deg(P)$ divise m .
2. Soit $d \mid m$. Pour tout $P \in U_d(p)$ (où $U_d(p)$ est l'ensemble des pol. unitaire irréductible de deg. d sur $\mathbb{F}_p$) on a $P \mid P_m$.

Théorème:

$$X^{p^m} - X = \prod_{d \mid m} \prod_{P \in U_d(p)} P \quad \text{et } X^{p^m} - X \text{ est sans facteur carré.}$$

Corollaire

$$\frac{|U_m(p)|}{=I_m(p)} = \frac{1}{m} \sum_{d \mid m} \mu\left(\frac{m}{d}\right) p^d$$

V2

Références:

CROMS: Rombaldi, alg. et géo. par l'agreg.

Pour le lemme, CROMS p. 423

Pour le 1., prenons P irréductible divisant P_m (on peut le supposer unitaire) et notons $d = \deg(P)$.

On a donc $\bar{P}_m = 0$ dans $\frac{\mathbb{F}_p[X]}{(P)} \cong \mathbb{F}_{p^d}$ et donc $\bar{X}^{p^m} = \bar{X}$

Et la famille $(\bar{x}^k)_{0 \leq k \leq d-1}$ est une base de $\mathbb{F}_{p^d}$ en tant que $\mathbb{F}_p$ -ev.

• Hq pour $\bar{Q} \in \frac{\mathbb{F}_p[X]}{(P)} \quad \bar{Q}^{p^m-1} = \bar{1}$

On peut écrire $\bar{Q} = \sum_{k=0}^{d-1} a_k \bar{x}^k$ où $a_0, \dots, a_{d-1} \in \mathbb{F}_p$.

$$\bar{Q}^{p^m} = \left(\sum_{k=0}^{d-1} a_k \bar{x}^k \right)^{p^m}$$

$$= \sum_{k=0}^{d-1} a_k^{p^m} (\bar{x}^k)^{p^m}$$

$$= \sum_{k=0}^{d-1} a_k \bar{x}^k = \bar{Q}$$

morph. Frobenius.

$$(\bar{x}^k)^{p^m} = (\bar{x}^{p^m})^k = \bar{x}^k$$

et $a_k^{p^m} = a_k$ car

$$\begin{aligned} a^{p^m} &= a^{p^{m-1} \cdot p} \\ &= a^{p^{m-1}} \dots a^p \in \mathbb{F}_p \\ &= a \in \mathbb{F}_p \end{aligned}$$

$\downarrow$ (dans $\mathbb{F}_p$)

• Hq $d \mid m$

$$\Leftrightarrow \text{Hq } p^d - 1 \mid p^m - 1$$

on a $\bar{Q}^{p^m-1} = \bar{1}$ dans $\mathbb{F}_{p^d}$

Or $(\mathbb{F}_{p^d})^\times$ est cyclique d'ordre $p^d - 1$. Donc $p^d - 1 \mid p^m - 1$.

Notons $m = qd + r$ la division euclidienne de m par d .
 $\rightarrow$ Hy $r = 0$

$$\begin{aligned} p^m - 1 &= p^{qd+r} - 1 \\ &= p^{qd} p^r - 1 = p^r + p^r \\ &= (p^{qd} - 1) p^r + p^r - 1 \\ &= (p^d - 1) \left(\sum_{k=0}^{q-1} (p^d)^k \right) p^r + p^r - 1 \end{aligned}$$

$\sum_{k=0}^{q-1} (p^d)^k = \frac{(p^d)^q - 1}{p^d - 1}$

On a que $0 \leq p^r - 1 < p^d - 1$ car $r < d$
 Donc la relation obtenue est la division euclidienne de $p^m - 1$
 par $p^d - 1$, or $p^d - 1 \mid p^m - 1$, donc $p^r - 1 = 0$
 D'où $r = 0$, et donc dlm: (ici min)

Prop 2. soit dlm et $P \in \mathcal{U}(p)$.

• Hy $\bar{X}^{p^d} = \bar{X}$ dans $\frac{\mathbb{F}_p[X]}{(P)} \simeq \mathbb{F}_{p^d}$
 $(\mathbb{F}_{p^d})^\times$ est d'ordre $p^d - 1$.

Donc par thm de Lagrange,

$$\bar{X}^{p^d - 1} = 1$$

Donc $\bar{X}^{p^d} = \bar{X}$

dit
 Par Lagrange on a:
 $\bar{X}^{p^d} = \bar{X}$

• Hy $\bar{X}^{p^m} = \bar{X}$ dans $\mathbb{F}_{p^d}$

d divise m on peut donc écrire $m = qd$

$$\begin{aligned} \bar{X}^{p^m} &= \bar{X}^{p^{qd}} \\ &= (\bar{X}^{p^d})^{p^{d(q-1)}} \\ &= (\bar{X})^{p^{d(q-1)}} \\ &= \dots \\ &= \bar{X} \end{aligned}$$

Donc $\bar{X}^m - \bar{X} = 0$ dans $\frac{\mathbb{F}_p[X]}{(P)}$ donc $P \mid X^m - X$ (ici min) $\square$

Pour le théorème, [RouS] p. 424

• M_q P_m est sans facteur carré

$$P'_m = P^m \times P^{m-1} - 1$$

$$= -1$$

dans $\mathbb{F}_p[X]$

Donc P_m est premier à sa dérivée, donc sans facteur carré

• Concluons avec le lemme

Puisque P_m est sans facteur carré,

$$P_m = \prod_{d|m} \prod_{P \in \mathcal{U}(P)} P \quad (*)$$

□

Pour le corollaire, [RouS] p. 424

• Passons au degré dans (*)

$$P^m = \sum_{d|m} \sum_{P \in \mathcal{U}(P)} \stackrel{=d}{\deg(P)}$$

$$= \sum_{d|m} d \cdot \text{Id}(P)$$

• Appliquons la formule de Möbius (Möbius: $u(m) = \sum_{d|m} v(d) \Leftrightarrow v(m) = \sum_{d|m} \mu(d) u(\frac{m}{d})$)

On a:

$$m I_m(P) = \sum_{d|m} \mu(d) P^{\frac{m}{d}}$$

$$= \sum_{d|m} \mu\left(\frac{m}{d}\right) P^d$$

□