dev : dénombrement polynômes irréductibles sur $\mathbb{F}_q$.

leçons : 123, 141, 144, 190.
réf : Rombaldi p422. Ber 654.

cadre : $P_n(X) = X^{p^n} - X \in \mathbb{F}_p[X]$, $p \geq 2$ premier ; $\mathcal{U}_n(p) = \{$pol. irréd. unit. de $\mathbb{F}_p[X]$ de $d^\circ n\}$
$I_n(p) := |\mathcal{U}_n(p)|$

Lemme : 1) Soit $P \in \mathbb{F}_p[X]$ irréd. $P \mid P_n \Rightarrow \deg P \mid n$.
2) Soit $d \mid n$. Tout $P \in \mathcal{U}_d(p)$ divise P_n.

dem :
1) Soit $d \in \mathbb{N}$ et $P \in \mathcal{U}_d(p)$. Supposons $P \mid P_n$. On a alors, dans $\mathbb{F}_{p^d} = \mathbb{F}_p[X]/(P)$ (corps car P irréd.).
$\overline{P_n} = \overline{0} \iff \overline{X}^{p^n} = \overline{X}$
Comme $(\overline{X}^k)_{0 \leq k \leq d-1}$ est une base de $\mathbb{F}_{p^d}$ (comme $\mathbb{F}_p$-ev) on a pour $\overline{Q} \in \mathbb{F}_{p^d}$

$$\overline{Q} = \sum_{k=0}^{d-1} a_k \overline{X}^k \quad \text{où } a_k \in \mathbb{F}_p$$

$$\overline{Q}^{p^n} = \sum_{k=0}^{d-1} a_k^{p^n} (\overline{X}^k)^{p^n} \quad \text{car } car(\mathbb{F}_p) = p$$

$$= \sum_{k=0}^{d-1} a_k (\overline{X}^{p^n})^k \quad \text{par le thm de Fermat } a_k^p = a \text{ dans } \mathbb{F}_p \text{ + réc.}$$

$$= \sum_{k=0}^{d-1} a_k \overline{X}^k \quad \text{car } X^{p^n} - X = 0 \text{ dans } \mathbb{F}_{p^d}.$$

$$= \overline{Q}.$$

Ainsi, $\forall \overline{Q} \in \mathbb{F}_{p^d}^*$ $\overline{Q}^{p^n - 1} = \overline{1}$.
→ car $\mathbb{F}_{p^d}$ corps de card p^d

(?) $\mathbb{F}_{p^d}^*$ est cyclique d'ordre $p^d - 1$ donc il existe $\omega \in \mathbb{F}_{p^d}^*$ d'ordre $p^d - 1$.
On a donc $p^d - 1 \mid p^n - 1$ puis $d \mid n$.

(K corps H ss gpe fini de K^* est cyclique / cf p348 BER)

dem : Par div euclidienne $n = qd + r$ $0 \leq r < d$.
$p^n - 1 = p^{dq} p^r - 1 = (p^{dq} - 1) p^r + p^r - 1 = (p^d - 1)(p^{d(q-1)} + \dots + p + 1) p^r + p^r - 1$.
donc $p^d - 1 \mid p^r - 1$ or $p^r - 1 < p^d - 1$ (car $r < d$ et $p \geq 2$)
donc $r = 0$.

2) Soit $d \mid n$ et $P \in \mathcal{U}_d(p)$. On pose $\mathbb{F}_{p^d} := \mathbb{F}_p[X]/(P)$.

$|\mathbb{F}_{p^d}^*| = p^d - 1$ donc $\overline{X}^{p^d - 1} = \overline{1}$ par le thm de Lagrange.
d'où $\overline{X}^{p^d} = \overline{X}$
Par récurrence, on en déduit $\overline{X}^{p^{dk}} = \overline{X}$ pour tout $k \in \mathbb{N}$.
$X^{p^{d(k+1)}} = (X^{p^{d(k-1)}})^{p^d} = X^{p^{d(k-1)}}$

Comme $d \mid n$, on en déduit $\overline{X}^{p^n} = \overline{X}$ puis $\overline{X}^{p^n} - \overline{X} = \overline{0}$ (bof (par prop^{T}))
$\Rightarrow \overline{P_n} = \overline{0}$
Donc P divise $X^{p^n} - X$.

Thm : $\forall n \in \mathbb{N}^*$ $\quad nI_n(p) = \sum \mu(n/d) p^d$.

dem :
Soit $n \in \mathbb{N}$.
$P_n' = p^n X^{p^n - 1} - 1 = -1$ (car $car(\mathbb{F}_p) = p$)
donc $P_n' \wedge P_n = 1$. On en déduit que P_n est sans facteurs carrés et par le lemme :

$$P_n = \prod_{d \mid n} \prod_{P \in \mathcal{U}_d(p)} P$$

$\forall d \mid n$, $\forall P \in \mathcal{U}_d(p)$ $P \mid P_n$ (cf 2)) d'où $\prod \prod P \mid P_n$ (car irred)
De plus si $P \mid P_n$, alors $\deg P \mid n$ donc il n'y a pas de diviseur de P avec un $d^\circ \neq$ de $d \mid n$
De plus tout ? unit^{é} donc $=$

En regardant les degrés : $p^n = \sum_{d|n} d\, I_n(p)$

d'où, par la formule d'inversion de Möbius : $nI_n(p) = \sum_{d|n} \mu(d)\, p^{n/d}$

car $d \mapsto \frac{n}{d}$ est une permutation de l'ens des diviseurs $= \sum_{d|n} \mu\left(\frac{d}{n}\right) p^d$