102, 123, 141

Réf :

Théorème : Caractérisation des polynômes cyclotomiques.

Soit $n>0$. Soit $X^n-1 = \prod_{k=1}^{n} (X - e^{\frac{2ik\pi}{n}})$ dans $\mathbb{C}[X]$.

On définit $\Phi_n(X) = \prod_{k\wedge n=1} (X - e^{\frac{2ik\pi}{n}}) \in \mathbb{C}[X]$.

Alors Φ_n est unitaire, $\Phi_n \in \mathbb{Z}[X]$, et est irréductible dans $\mathbb{Z}[X]$.

Et $\deg(\Phi_n) = \varphi(n)$.

démo :

Φ_n est unitaire.

- Montrons par récurrence forte sur n que $\Phi_n \in \mathbb{Z}[X]$.

On a $X^n-1 = \prod_{d\mid n} \Phi_d(X)$ dans $\mathbb{C}[X]$.

car $\forall 1\le k\le n$, $k = \gcd(k,n) \times \frac{k}{\gcd(k,n)}$ et $e^{\frac{2ik\pi}{n}} = e^{\frac{2i\frac{k}{d}\pi}{\frac{n}{d}}} = e^{\frac{2ik\pi}{d}}$

$= \prod_{d\mid n} \Phi_d(X)$ dans $\mathbb{C}[X]$.

Car $n=1$, on a $X-1 = \Phi_1(X) \in \mathbb{Z}[X]$.

Supposons l'hypothèse vraie $\forall k<n$. On a $X^n-1 = \Phi_n(X) \times \left(\prod_{\substack{d\mid n \\ d\neq n}} \Phi_d(X)\right)$. ($\Phi_n$ unitaire $\in \mathbb{Z}[X]$, $\prod \in \mathbb{Z}[X]$) $\Rightarrow \Phi_n(X) \in \mathbb{Z}[X]$ en divisant X^n-1 par $\prod_{\substack{d\mid n \\ d\neq n}} \Phi_d$ dans $\mathbb{Z}[X]$.

- Montrons que Φ_n est irred dans $\mathbb{Z}[X]$

Soit ζ racine de $\Phi_n(X)$ dans $\mathbb{C}$. Soit $P(X) = \mathrm{Irr}(\zeta, \mathbb{Z})(X)$. Il existe car $\mathbb{Z}[X]$ factoriel et car $\Phi_n(\zeta) = 0$.

Soit p premier, $p\wedge n = 1$. Montrons que ζ^p est racine de P.

Soit $Q = \mathrm{Irr}(\zeta^p, \mathbb{Z})$. Supposons que $Q \neq P$. On a $Q \mid \Phi_n$, $P \mid \Phi_n$ $\Rightarrow QP \mid \Phi_n$ par factorialité.

On a $Q(\zeta^p) = 0$.

Donc $R(X) = Q(X^p)$, $R(\zeta) = 0$. Donc $P(X) \mid Q(X^p)$ car P irred dans $\mathbb{Z}[X]$.

Donc $Q(X^p) = P(X) \times P_1(X)$ dans $\mathbb{Z}[X]$.

$\hookrightarrow \overline{Q(X^p)} = \bar{Q}(X)^p = \bar{P}(X) \cdot \bar{P_1}(X)$ dans $\mathbb{F}_p[X]$ en passant modulo p.

Soit $\hat{P}$ facteur irred de $\bar{P}$ dans $\mathbb{F}_p[X]$. On a $\hat{P} \mid \bar{Q}^p \Rightarrow \hat{P} \mid \bar{Q}$ (comme P est unitaire, $\bar{P}$ unitaire, donc $\deg(\hat{P}) \geq 1$.)

$\Rightarrow \hat{P}^2 \mid \bar{Q}\bar{P} \mid \bar{\Phi}_n \mid \bar{X}^n - 1$

$\Rightarrow \hat{P} \mid \gcd(\bar{X}^n - 1, n\bar{X}^{n-1})$

Mais comme $n \wedge p = 1$, $\bar{X}^n - 1 \wedge n X^{n-1} = 1$, contradiction.

Donc ζ^p est une racine de P.

Pour $\zeta = e^{\frac{2i\pi}{n}}$, $1\le k\le n$, $k\wedge n = 1$, $k = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, $p_i \wedge n = 1$, on montre ainsi que $\zeta^{p_1^{\alpha_1}\cdots p_r^{\alpha_r}}$ est racine de P.

Donc $\prod_{\substack{k=1 \\ k\wedge n=1}}^{n} (X - \zeta^k) \mid P$ dans $\mathbb{C}[X]$, donc $P = \Phi_n$ car P unitaire. (Φ_n unitaire.) □

De plus, $\deg(\Phi_n) = \#\{1\le k\le n \mid k\wedge n = 1\} = \#\left((\mathbb{Z}/n\mathbb{Z})^\times\right) = \varphi(n)$.

Prop : Soit p premier, $p \nmid n$, et $q = p^a$. Dans $\mathbb{F}_q[X]$, les facteurs irréductibles de $\bar{\Phi}(n)$ sont tous de degré $\mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(q)$.

démo :

Soit P facteur irréd. de $\bar{\Phi}(n)$. Soit $k_0 = \deg(P)$. Soit K un corps de rupture de P sur $\mathbb{F}_q$. On a $K \simeq \mathbb{F}_{q^{k_0}}$.
Soit λ racine de P dans K. On a $X-\lambda \mid P \mid \bar{\Phi}(n) \mid X^n - 1 \Rightarrow \mathrm{ord}(\lambda) \mid n$.
Si $\mathrm{ord}(\lambda) = d \neq n$, alors $X-\lambda \mid X^d - 1 \Rightarrow (X-\lambda)^2 \mid X^d - 1 \times \bar{\Phi}(n) \mid X^n - 1 \Rightarrow X^n - 1$ a une racine double, contradiction.
Donc $\mathrm{ord}(\lambda) = n$.
Or, $\lambda \in K^\times \Rightarrow \lambda^{q^{k_0}-1} = 1 \Rightarrow n \mid q^{k_0}-1 \Leftrightarrow q^{k_0} \equiv 1 [n] \Leftrightarrow \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(q) \mid k_0$.

Regardons maintenant $\mathbb{F}_{q^{\hat{k}}}$ avec $\hat{k} = \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(q)$. Alors $q^{\hat{k}} \equiv 1 [n] \Leftrightarrow n \mid q^{\hat{k}}-1$. Donc $X^n - 1 = \prod_{d \mid n} \bar{\Phi}(d) \mid \prod_{d \mid q^{\hat{k}}-1} \bar{\Phi}(d) = X^{q^{\hat{k}}-1} - 1$
Comme $X^{q^{\hat{k}}-1} - 1$ est scindé sur $\mathbb{F}_{q^{\hat{k}}}$, $X^n - 1$ est scindé sur $\mathbb{F}_{q^{\hat{k}}}$, donc P est scindé sur $\mathbb{F}_{q^{\hat{k}}}$.
Donc pour λ racine de P dans $\mathbb{F}_{q^{\hat{k}}}$, $\mathbb{F}_q(\lambda)$ sous-corps de $\mathbb{F}_{q^{\hat{k}}}$. Comme $\mathbb{F}_q(\lambda) \simeq K \simeq \mathbb{F}_{q^{k_0}}$, on a donc $k_0 \leq \hat{k}$.
Donc $\deg(P) = k_0 = \hat{k} = \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(q)$. □

~~Or, comme $\bar{\Phi}(n) \mid X^n - 1$, on a $\lambda_1^n = 1$. Montrons que $\mathrm{ord}(\lambda_1) = n$. Si $\mathrm{ord}(\lambda_1) = d$, $d \mid n$, $d \neq n$, alors $(X-\lambda_1) \mid X^d - 1$~~
~~$(X-\lambda_1) \mid \bar{\Phi}(n)$~~
~~$\Rightarrow (X-\lambda_1)^2 \mid X^n - 1$~~
~~$\Rightarrow X^n - 1$ a un facteur carré~~
~~impos~~

Rem : λ est encore une racine n-ième primitive de l'unité dans $\mathbb{F}_{q^{\hat{k}}}$
Si $n = p^\alpha n'$, $(X^n - 1) = (X^{n'} - 1)^{p^\alpha}$, donc on se ramène à n', $n' \wedge p = 1$.

~~Donc $\mathrm{ord}(\lambda_1) = n$. Donc $\lambda_1^{q^{\hat{k}}-1} = 1 \Leftrightarrow n \mid q^{\hat{k}}-1 \Leftrightarrow q^{\hat{k}} \equiv 1 [n]$~~

~~Donc $\hat{k} = \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(q)$, par minimalité.~~

~~Soit $Q(X) = \prod_{k=0}^{\hat{k}-1} (X - \lambda_1^{q^k}) = (X-\lambda_1)(X-\lambda_1^q) \cdots (X-\lambda_1^{q^{\hat{k}-1}}) = X^{\hat{k}} + a_{\hat{k}-1} X^{\hat{k}-1} + \cdots + a_0$, avec $a_k = \bar{P}_k(\lambda_1, \lambda_1^q, \ldots, \lambda_1^{q^{\hat{k}-1}})$~~

~~Et $a_k^q = \bar{P}_k(\lambda_1, \ldots, \lambda_1^{q^{\hat{k}-1}})^q = \bar{P}_k(\lambda_1^q, \lambda_1^{q^2}, \ldots, \lambda_1^{q^{\hat{k}-1}}, \lambda_1^{q^{\hat{k}}}) = \bar{P}_k(\lambda_1, \lambda_1^q, \ldots, \lambda_1^{q^{\hat{k}-1}}) = a_k$~~
~~$\lambda_1^{q^{\hat{k}}} = \lambda_1$ car $\bar{P}_k$ sym~~

~~$\bar{P}_k$ symétrique à coeffs entiers~~
~~$\Rightarrow \bar{P}_k \in \mathbb{F}_q[X_1, \ldots, X_{\hat{k}}]^{\mathfrak{S}_{\hat{k}}}$~~

~~Donc $a_k \in \mathbb{F}_q$ car racine de $X^q - X$.~~

~~Donc $Q \in \mathbb{F}_q[X]$ et $Q(X) \mid P(X) \Rightarrow Q(X) = P(X)$, et $\deg(P) = \hat{k} = \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(q)$.~~ □