102, 123, 141
120,121

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 $\phi(n)$ est unitaire, $\phi(n)\in\mathbb{Z}[X]$, et est irréductible dans $\mathbb{Z}[X]$.

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

démo :

$\phi(n)$ est unitaire.

– Montrons par récurrence forte sur n que $\phi(n)\in\mathbb{Z}[X]$.

On a $X^n-1=\prod_{d|n}\left(\prod_{\substack{k=1\\ k\wedge d=1}}^{d}(X-e^{\frac{2ik\pi}{n}\frac{n}{d}})\right)$ car $\forall 1\leq l\leq n$, $l=\mathrm{pgcd}(l,n)\times\frac{l}{\mathrm{pgcd}(l,n)}$ et $e^{\frac{2i\pi k}{n}\times\frac{n}{d}}=e^{\frac{2ik\pi}{d}}$

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

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

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

– Montrons que $\phi(n)$ est irred dans $\mathbb{Z}[X]$

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

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

Soit $Q=\mathrm{Irr}(\xi^p,\mathbb{Z})$. Supposons que $Q\neq P$. On a $Q|\phi(n)$, $P|\phi(n)$ $\Rightarrow QP|\phi(n)$ par factorialité.

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

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

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

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

Soit $\hat{P}$ facteur irred de $\overline{P}$ dans $\mathbb{F}_p[X]$. On a $\hat{P}|\overline{Q}^p\Rightarrow\hat{P}|\overline{Q}$

comme P est unitaire, $\overline{P}$ unitaire, donc $\deg(\hat{P})\geq 1$.

$\Rightarrow\hat{P}^2|\overline{Q}\,\overline{P}|\overline{\phi(n)}|\overline{X}^n-1$

$\Rightarrow\hat{P}|\mathrm{pgcd}(\overline{X}^n-1,\bar{n}\overline{X}^{n-1})$

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

Donc ξ^p est une racine de P.

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

Donc $\underbrace{\prod_{\substack{k=1\\ k\wedge n=1}}^{n}(X-\xi^k)}_{\phi(n)}\,|\,P$ dans $\mathbb{C}[X]$, donc $P=\phi(n)$ car P unitaire, $\phi(n)$ unitaire. □

De plus, $\deg(\phi(n))=\#\{1\leq k\leq n \text{ tq } k\wedge n=1\}=\#((\mathbb{Z}/n\mathbb{Z})^\times)=\varphi(n)$.

Prop : Soit p premier, $p \wedge n$, 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 irred. 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~~

<u>Rem :</u> λ est encore une racine n-ième primitive de l'unité dans $\mathbb{F}_{q^{k_0}}$.
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 $Q(X) = \prod_{k=0}^{\hat{k}-1} (X - \lambda_1^{q^k}) = (X - \lambda_1)(X - \lambda_1^q) \cdots (X - \lambda_1^{q^{\hat{k}-1}}) = X^{\hat{k}} + a_{\hat{k}-1} X^{\hat{k}-1} + \dots + a_0$, avec $a_k = \bar{P}_k(\lambda_1, \lambda_1^q, \dots, \lambda_1^{q^{\hat{k}-1}})$~~

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

~~P_k symétrique à coeff. entiers $\Rightarrow \bar{P}_k \in \mathbb{F}_q[X_1, \dots, X_{\hat{k}}]^{S_n}$~~

~~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 $\deg(P) = \hat{k} = \mathrm{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times}(q)$. □~~