1) On pose $\zeta = \exp(\frac{2i\pi}{n}) \in \mu_n(\mathbb{C})$ et $\Theta : \mathbb{Z} \to \mu_n(\mathbb{C})$ définie par $k \mapsto \zeta^k$ qui existe car $\mu_n(\mathbb{C})$ est un groupe. De plus, Θ est un morphisme de groupes car

$$\forall (k,k') \in \mathbb{Z}^2, \Theta(k+k') = \zeta^{k+k'} = \zeta^k \zeta^{k'} = \Theta(k)\Theta(k').$$

Maintenant, $\mathrm{Ker}(\Theta) = n\mathbb{Z}$. En effet, $n \in \mathrm{Ker}(\Theta)$ puisque, par définition, $\Theta(n) = \zeta^n = 1$.
Pour $x \in \mathbb{Z}/n\mathbb{Z}$ et $m, m' \in \mathbb{Z}$ deux représentants de x qui vérifient que $x = \overline{m} = \overline{m'}$, on a $m - m' \in n\mathbb{Z}$ et donc $\Theta(m) = \Theta(m')$.
On en déduit que l'on peut définir $\theta : \mathbb{Z}/n\mathbb{Z} \to \mu_n(\mathbb{C})$ en posant pour $x \in \mathbb{Z}/n\mathbb{Z}$ et m un représentant de x dans $\mathbb{Z}$, $\theta(x) = \Theta(m)$.
L'application θ est encore un morphisme de groupe.
Montrons qu'il est injectif. Soit $x \in \mathbb{Z}/n\mathbb{Z}$ tel que $\theta(x) = 1$, soit m **le** représentant de x dans $\{0, 1, \ldots, n-1\}$, on a $\Theta(x) = \zeta^m = 1$ ce qui implique que $m \in n\mathbb{Z}$ et donc $x = 0$.
On peut alors conclure que θ est un isomorphisme de groupes car $|\mathbb{Z}/n\mathbb{Z}| = n = |\mu_n(\mathbb{C})|$.
Par définition, $P_n(\mathbb{C})$ est l'ensemble des éléments d'ordre n de $\mu_n(\mathbb{C})$, il y a donc autant d'éléments dans $P_n(\mathbb{C})$ que d'éléments d'ordre n dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire des générateurs de $\mathbb{Z}/n\mathbb{Z}$. Finalement,

$$|P_n(\mathbb{C})| = \varphi(n).$$

2) Soit p un nombre premier, on pose $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
   a) Soit $k \in [\![1, p-1]\!]$, on sait que
   $$k\binom{p}{k} = p\binom{p-1}{k-1}.$$
   Donc p divise $k\binom{p}{k}$ mais comme k est premier avec p (car p est un nombre premier), p divise $\binom{p}{k}$.
   b) Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathbb{F}_p[X]$, montrons par récurrence sur le degré de P que $P^p = P(X^p)$ [1].
   — Si P est de degré 0, on a $P = \alpha$, d'où $P^p = \alpha^p = \alpha$ car, d'après le petit théorème de Fermat, pour $k \in \mathbb{Z}$, $k^p \equiv k[p]$ et donc pour $x \in \mathbb{F}_p$ $x^p = x$
   — On suppose le résultat pour P de degré $n-1$. On écrit alors $P = a_n X^n + Q$ où $\deg Q < n$. en utilisant la formule du binôme, on obtient que

$$\begin{aligned} P^p &= (a_n X^n + Q)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} a_n^k X^{nk} Q^{n-k} \\ &= a_n^p X^{np} + Q^p \text{ d'après la question précédente} \\ &= a_n (X^p)^n + Q(X^p) \text{ par l'hypothèse de récurrence} \\ &= P(X^p) \end{aligned}$$

3) On a $\Phi_1 = X - 1, \Phi_2 = X + 1, \Phi_3 = (X - j)(X - \overline{j}) = X^2 + X + 1$ et $\Phi_4 = (X - i)(X + i) = X^2 + 1$. On a $\deg(\Phi_n) = \varphi(n)$ d'après la question 1.

4) On sait que $X^n - 1 = \prod_{\zeta \in \mu_n(\mathbb{C})} (X - \zeta)$. Maintenant on peut regrouper les racines de l'unité selon leur ordre dans le groupe $\mu_n(\mathbb{C})$ en remarquant que cet ordre divise n qui est le cardinal de $\mu_n(\mathbb{C}) = \{\exp(2ik\pi/n) \mid k \in [\![0, n-1\,;\,]\!]\}$.

1. On peut éviter la récurrence en remplaçant la formule du binôme par celle du multinôme.

On en déduit que

$$X^n - 1 = \prod_{d|n} \prod_{\substack{\zeta \in \mu_n(\mathbb{K}) \\ \zeta \text{ d'ordre } d}} (X - \zeta) = \prod_{d|n} \Phi_d.$$

En effet, les ζ qui sont d'ordre d dans $\mu_n(\mathbb{C})$ sont par définition les racines d-ièmes de l'unité primitives.

5) En prenant les degrés,

$$n = \deg(X^n - 1) = \deg\left(\prod_{d|n} \Phi_d\right) = \sum_{d|n} \varphi(d).$$

6) a) Soit p un nombre premier, le morphisme

$$\psi_p : \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$$

qui associe à tout polynôme P sa réduction modulo p est un morphisme d'anneaux. Soit P et Q dans $\mathbb{Z}[X]$ avec $c(P) = c(Q) = 1$, en particulier $\psi_p(P) \neq 0$ et $\psi_p(Q) \neq 0$ car tous les coefficients ne sont pas divisibles par p. On en déduit que

$$\psi_p(PQ) = \psi_p(P)\psi_p(Q) \neq 0$$

car $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre. De ce fait, il n'existe pas de nombre premier qui divise tous les coefficients de PQ donc $c(PQ) = 1$.

b) D'après les propriétés du PGCD, on a pour $P \in \mathbb{Z}[X]$ et $\lambda \in \mathbb{Z}$, $c(\lambda P) = \lambda c(P)$. De ce fait pour P et Q deux polynômes, on peut factoriser par le PGCD des coefficients. On écrit :

$$P = c(P)P_1 \text{ et } Q = c(Q)Q_1$$

avec $c(P_1) = c(Q_1) = 1$. On en déduit que

$$c(PQ) = c(P)c(Q)c(P_1Q_1) = c(P)c(Q).$$

c) On voit que PQ est unitaire comme produit de deux polynômes unitaires. De ce fait, $c(PQ) = 1$. Maintenant, on considère λ le PPCM des dénominateurs des coefficients de P et μ le PPCM des dénominateurs des coefficients de Q. On a donc $\lambda P \in \mathbb{Z}[X]$ et $\mu Q \in \mathbb{Z}[X]$ avec $c(\lambda P) = c(\mu Q) = 1$. On a donc d'après ii

$$1 = c(\lambda P).c(\mu Q) = c(\lambda.\mu.PQ) = \lambda.\mu c(PQ) = \lambda.\mu.$$

On en déduit que $\lambda = \mu = 1$ c'est-à-dire que P et Q sont à coefficients entiers.

7) On montre que pour tout entier n, Φ_n est à coefficients entiers. On procède par récurrence forte sur n.

— Initialisation : Pour $n = 1$, $\Phi_1 = X - 1$ est à coefficients entiers.

— Hérédité : Soit $n > 1$, on suppose que pour tout $d < n$, Φ_d est à coefficients entiers. On a

$$X^n - 1 = \Phi_n \times \prod_{\substack{d|n \\ d \neq n}} \Phi_d.$$

De plus, par récurrence, $Q = \prod_{\substack{d|n \\ d \neq n}} \Phi_d$ est un polynôme unitaire à coefficients entiers. On en déduit que Φ_n est à coefficients rationnels puis, comme Φ_n est unitaire, en utilisant la question précédente Φ_n est à coefficients entiers.

Par récurrence, pour tout entier n, $\Phi_n \in \mathbb{Z}[X]$.

8) On suppose que ω^p n'est pas une racine de P.

a) On sait que ω est une racine de Φ_n. C'est donc une racine primitive n-ième de l'unité. Comme p est un nombre premier qui ne divise pas n, il est premier avec n et donc ω^p est aussi une racine primitive n-ième de l'unité. De ce fait,

$$\Phi_n(\omega^p) = P(\omega^p)Q(\omega^p) = 0.$$

Comme on a supposé que ω^p n'est pas une racine de P, ω^p est une racine de Q et donc ω est une racine de $Q(X^p)$.

Comme P est un polynôme irréductible unitaire qui annule ω, c'est le polynôme minimal de ω. De ce fait $Q(X^p) \in (P)$ et donc $P|Q(X^p)$.

b) On a vu que $P|Q(X^p)$ dont en réduisant modulo p, dans $\mathbb{F}_p[X]$, $\overline{P}$ divise $\overline{Q(X^p)}$. De plus, $\overline{Q(X^p)} = \overline{Q}(X^p) = \overline{Q}^p$ d'après 2.b.

Soit $S \in \mathbb{F}_p[X]$ un polynôme irréductible divisant $\overline{P}$, il divise $\overline{Q}^p$ et donc $\overline{Q}$. De ce fait, S^2 divise $\overline{PQ} = \overline{\Phi_n}$. Finalement, S^2 divise $X^n - \overline{1}$.

c) Si on dérive $T = X^n - \overline{1}$, on obtient $T' = \overline{n}X^{n-1}$. Il est premier avec T car p ne divise pas n. De ce fait, T ne peut pas avoir de facteur carré. On a donc une absurdité.

9) Avec les notations précédentes, soit ω une racine de P (dans $\mathbb{C}$) qui est donc un élément de $P_n(\mathbb{Q})$. On vient de montrer pour tout nombre premier p qui ne divise pas n, ω^p est aussi une racine de P. En appliquant de nouveau ce résultat à la racine ω^p on trouve que ω^{p^2} est aussi une racine. De ce fait, par une récurrence immédiate, ω^{p^α} est une racine de P. De même en appliquant encore ce résultat, on montre que ω^k est une racine de P où k est un entier premier avec n (en le décomposant sous la forme : $k = p_1^{\alpha_1}.\cdots.p_r^{\alpha_r}$). On en déduit que tous les éléments de $P_n(\mathbb{Q})$ sont des racines de P et donc $\Phi_n|P$ d'où $\Phi_n = P$.

On en déduit que Φ_n est irréductible.