Soit n un entier non nul. On appelle groupe des racines n-ièmes de l'unité le groupe multiplicatif

$$\mu_n(\mathbb{C}) = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}.$$

Ses éléments s'appellent les racines n-ièmes de l'unité. Soit $\zeta \in \mu_n(\mathbb{C})$ si pour tout $d \in [\![1, n-1]\!]$, $\zeta^d \neq 1$, on dit que ζ est une racine n-ième de l'unité primitive. On notera $P_n(\mathbb{C})$ l'ensemble des racines n-ièmes de l'unité primitives.
On pose $\Phi_n = \prod_{\zeta \in P_n(\mathbb{C})} (X - \zeta)$.
Le polynôme Φ_n est donc le polynôme unitaire qui s'annule sur les racines primitives de l'unité.

1) Montrer que $\mu_n(\mathbb{C})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. En déduire alors que $|P_n(\mathbb{C})| = \varphi(n)$.
2) Soit p un nombre premier, on pose $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
   a) Montrer que pour tout $k \in [\![1, p-1]\!]$, $\binom{p}{k}$ est divisible par p.
   b) Montrer que pour tout $P \in \mathbb{F}_p[X]$, $P^p = P(X^p)$.
3) Calculer Φ_1, Φ_2, Φ_3 et Φ_4. Quel est le degré de Φ_n ?
4) Justifier que : $X^n - 1 = \prod_{d|n} \Phi_d$.
5) En déduire que : $n = \sum_{d|n} \varphi(d)$.
6) Soit $P \in \mathbb{Z}[X]$, on appelle contenu de P et on note $c(P)$ le PGCD des coefficients de P.
   a) Montrer que si P et Q sont dans $\mathbb{Z}[X]$ avec $c(P) = c(Q) = 1$ alors $c(PQ) = 1$. *On pourra utiliser une réduction modulo p où p est un nombre premier.*
   b) En déduire que $c(PQ) = c(P)c(Q)$.
   c) Montrer que si P et Q sont deux polynômes unitaires à coefficients dans $\mathbb{Q}$ tels que PQ soit à coefficients entiers alors P et Q sont à coefficients entiers.
7) En déduire que pour tout n, Φ_n est à coefficients entiers.

On veut montrer que Φ_n est irréductible dans $\mathbb{Z}[X]$ (et donc dans $\mathbb{Q}[X]$). Par l'absurde, on suppose que ce n'est pas le cas. Soit $P \in \mathbb{Z}[X]$ un facteur irréductible unitaire, Q le polynôme tel que $\Phi_n = PQ$ et ω une racine de P. On considère aussi p un nombre premier qui ne divise pas n. On notera $\overline{\Phi_n}$, $\overline{P}$ et $\overline{Q}$ les polynômes de $\mathbb{F}_p[X]$ obtenus par réduction modulo p.

8) On suppose que ω^p n'est pas une racine de P.
   a) Justifier que ω est racine de $Q(X^p)$ puis que $P|Q(X^p)$.
   b) Montrer l'existence d'un polynôme irréductible $S \in \mathbb{F}_p[X]$ tel que $S^2|X^n - \overline{1}$.
   On pourra utiliser 2.(b).
   c) Arriver à une contradiction. *On pourra dériver $X^n - \overline{1}$.*
9) En déduire que Φ_n est irréductible.