Théorème de Kronecker

Théorème : Soit $P \in \mathbb{Z}[X]$ unitaire de racines de module ≤ 1.
Si $P(0) \neq 0$, alors les racines de P sont racines de l'unité.

Soit $n = \deg P$. Notons $z_1, \dots, z_n$ racines de P comptées avec multiplicité.
$P = X^n - \sigma_1 X^{n-1} + \dots + (-1)^n \sigma_n$ où les σ_i sont les fonctions symétriques élémentaires

$$|\sigma_k| = \left| \sum_{1 \leq i_1 < \dots < i_k \leq n} z_{i_1} \cdots z_{i_k} \right| = \left| \sum_{I \in \mathcal{P}_k([\![1,n]\!])} \prod_{i \in I} z_i \right| \leq \#\mathcal{P}_k([\![1,n]\!]) = \binom{n}{k}.$$

De plus, $P \in \mathbb{Z}[X]$, donc $\forall i \in \{1, \dots, n\}$, $\sigma_i \in \mathbb{Z}$.
Il y a un nb de choix fini pour les σ_i, donc $\mathcal{R}_n = \{P \in \mathbb{Z}[X], \begin{cases} P \text{ unitaire, } \deg P = n \\ \mathrm{Rac}(P) \subset \overline{D(0,1)} \end{cases}\}$ est fini.

- Pour $k \in \mathbb{N}^*$, posons $P_k = \prod_{i=1}^{n} (X - z_i^k) \in \mathbb{C}[X]$, unitaire de degré n à racines de module ≤ 1.

Si $\Sigma_1, \dots, \Sigma_n$ sont les fonctions symétriques élémentaires des z_i^k, alors
$(-1)^r \Sigma_r$ est le coefficient de X^{n-r} dans P_k
polynôme symétrique en les z_i (car en les z_i^k) à coeff dans $\mathbb{Z}$.
Donc $P_k \in \mathbb{Z}[X]$. Donc $P_k \in \mathcal{R}_n$, $\forall k \in \mathbb{N}^*$.

- Or $\mathcal{R}_n$ est fini donc l'ensemble E des racines des éléments de $\mathcal{R}_n$ est fini
Ainsi, $\forall i \in \{1, \dots, n\}$, $\begin{array}{ccc} \mathbb{N}^* & \to & E \\ k & \mapsto & z_i^k \end{array}$ est non injective : $\exists k \neq l$, $z_i^k = z_i^l$ donc z_i racine de l'unité.

Corollaire : Soit $P \in \mathbb{Z}[X]$ unitaire irréductible à racines de module ≤ 1.
$P = X$ ou P est un cyclotomique.

Supposons $P \neq X$. P étant irréductible, $P(0) \neq 0$ (sinon $X \mid P$).
Par le théorème ci-dessus, les racines de P sont racines de l'unité
Donc $\exists N \in \mathbb{N}^*$, $\forall z \in \mathrm{Rac}(P)$, $z^N - 1 = 0$.
De plus, P est à racines simples, car sinon on aurait $P \wedge P' \mid P$
Donc $P \mid X^N - 1 = \prod_{d \mid N} \Phi_d$ décomposition irréd. de $X^N - 1$ dans $\mathbb{Z}[X]$.
Puisque P est irréductible, P est l'un des Φ_d.

Corollaire : Soit $P \in \mathbb{Z}[X]$ unitaire à racines de module ≤ 1.
P est produit d'une puissance de X et de polynômes cyclotomiques.

Il suffit de regarder la décomposition en irréductibles (unitaires) de P.