Théorème 1. Soit $P \in \mathbb{Z}[X]$ unitaire. On suppose que les racines de P sont de modules plus petit que 1. Alors les racines non nulles de P sont des racines de l'unité.

Preuve.

Remarquons déjà que $A_n := \{P \in \mathbb{Z}[X] \mid \deg(P) = n,\ P \text{ unitaire et } Z(P) \subset D(0,1)\}$ est fini. En effet, soit P dans A_n, alors en notant $(a_0, ..., a_{n-1})$ les coefficients de P et $\lambda_1, ..., \lambda_n$ ses racines on a alors par les relations coeffs/racines :

$$|a_k| \leq \left| \sum_{1 \leq i_1 < ... < i_{n-k} \leq n} \lambda_{i_1} ... \lambda_{i_{n-k}} \right| \leq \sum_{1 \leq i_1 < ... < i_{n-k} \leq n} |\lambda_{i_1} ... \lambda_{i_{n-k}}| \leq \binom{n}{n-k} \leq 2^n$$

Comme les coefficients de P sont entiers, il n'y a qu'un nombre fini de coefficients possibles et donc un nombre fini de tels polynômes d'ou la finitude de A_n.

Soit $P \in A_n$ et $M = C_P$ la matrice compagnon associée à P, M est une matrice à coefficients dans $\mathbb{Z} \subset \mathbb{C}$ donc est trigonalisable dans $\mathbb{C}$. Donc en notant $P = \prod_{i=1}^{n}(X - \lambda_i)$, il existe Q inversible tels que :

$$M = Q \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} Q^{-1}$$

On a donc pour $k \geq 1$ un entier,

$$M^k = Q \begin{pmatrix} \lambda_1^k & & \\ & \ddots & \\ & & \lambda_n^k \end{pmatrix} Q^{-1}$$

Donc $\prod_{i=1}^{n}(X - \lambda_i^k) = \chi_{M^k} \in \mathbb{Z}[X]$ car $M \in \mathcal{M}_n(\mathbb{Z})$ donc $M^k \in \mathcal{M}_n(\mathbb{Z})$.
Donc en notant $D_n = \bigcup_{P \in A_n} Z(P)$, D_n est fini car A_n l'est et par ce qui précède, pour tout $i \in [\![1;n]\!]$, et tout $k \in \mathbb{N}^\star$, $\lambda_i^k \in D_n$ donc nécessairement il existe deux entier $k < j$ tels que $\lambda_i^k = \lambda_i^j$ donc $\lambda_i^{j-k} = 1$ si λ_i est non nul. □

Proposition 1. Si $P \in A_n$ alors P est produit d'une puissance de X et de polynômes cyclotomiques.

Preuve.

Soit $P \in A_n$ et Q un facteur irréductible de P, supposons $Q(0) \neq 0$, alors par le théorème de Kronecker les racines de Q sont des racines de l'unité, comme elles sont en nombres finis et simples (car Q est premier avec sa dérivée car il est irréductible) il existe $N \in \mathbb{N}^\star$ tel que $Q | X^N - 1$. Or $X^N - 1 = \prod_{d|N} \Phi_d$ donc comme Q est irréductible, Q divise un Φ_d mais comme Φ_d irréductible sur $\mathbb{Z}$, $Q = \Phi_d$ et cela conclut. □

Proposition 2. Soit $B_n = A_n \cap \{P(0) \neq 0\}$ et $b_n = |B_n|$, alors pour $|z| < 1$ la série $\sum_{n \geq 0} b_n z^n$ converge et :

$$\sum_{n=0}^{\infty} b_n z^n = \prod_{n=1}^{\infty} \frac{1}{1 - z^{\varphi(n)}}$$

où φ est l'indicatrice d'Euler.

Lemme 1. $\forall n \geq 1$, $\varphi(n) \geq \sqrt{\frac{n}{2}}$. En particulier $\lim_{n \to +\infty} \varphi(n) = +\infty$

Preuve.

L'inégalité est claire pour $n=1$, on suppose maintenant $n \geq 2$ et on écrit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ la décomposition en facteurs premiers de n. On a alors :

$$\frac{\varphi(n)}{\sqrt{n}} = \prod_{i=1}^{k} p_i^{\frac{\alpha_i}{2}-1}(p_i - 1)$$

Si $\alpha_i \geq 2$ alors $p_i^{\frac{\alpha_i}{2}-1}(p_i-1) \geq 1$

Il reste alors à étudier $\dfrac{p_i - 1}{\sqrt{pi}}$ pour p_i premier, or pour $p_i \geq 3$, $\dfrac{p_i-1}{\sqrt{pi}} \geq 1$ par étude de fonction. Il reste alors uniquement le cas $p_i = 2$ à traiter on à la minoration voulue. □

Lemme 2. Pour $|z|< 1$, $\sum_{n\geq 0} b_n z^n$ et $\prod_{n \geq 1} \frac{1}{1 - z^{\varphi(n)}}$ convergent.

Preuve de la proposition :

Preuve.

Soit $P \in B_n$, alors par la proposition précédente, il existe des entiers $k_1, .., k_r$ tels que $P = \prod_{i=1}^{k} \Phi_{k_i}$, de plus on a $n = \sum_{i=1}^{k} \deg(\Phi_{k_i}) = \sum_{i=1}^{k} \varphi(k_i)$. Inversement, si P est de cette forme alors $P \in B_n$. On a donc une bijection entre B_n et :

$$C_n = \left\{ (y_k)_k \in \mathbb{N}^{\mathbb{N}} \ \mid \ \sum_{k=1}^{\infty} y_k \varphi(k) = n \right\}$$

Soit $|z|< 1$, $n \in \mathbb{N}^\star$ et $f_n(z) = \prod_{k=1}^{n} \frac{1}{1-z^{\varphi(k)}}$. On a alors par sommabilité :

$$\begin{aligned} f_n(z) = \prod_{k=1}^{n} \frac{1}{1-z^{\varphi(k)}} &= \prod_{k=1}^{n} \sum_{i=0}^{\infty} z^{i\varphi(k)} \\ &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} z^{i_1\varphi(1)+\dots+i_n\varphi(n)} \\ &= \sum_{p=0}^{\infty} c_p(n) z^p \end{aligned}$$

où $c_p(n) = \left| \left\{ (y_1, ..., y_n) \in \mathbb{N}^n \mid \sum_{i=1}^{n} y_i \varphi(i) = p \right\} \right|$

Remarquons que pour $\varphi(n) \geq p$, $c_p(n) = b_p$. On a alors :

$$\begin{aligned} \left| \sum_{p=0}^{\infty} b_p z^p - f_n(z) \right| &\leq \sum_{p=0}^{\infty} |b_p - c_p(n)||z|^p \\ &\leq \sum_{\{p \leq \varphi(n)\}} |b_p - c_p(n)||z|^p + \sum_{\{p \geq \varphi(n)\}} b_p |z|^p \\ &\leq \sum_{\{p \leq \varphi(n)\}} b_p |z|^p \underset{n\to+\infty}{\longrightarrow} 0 \end{aligned}$$

La dernière inégalité ayant lieu car $b_p \geq c_p(n) \geq 0$ et la limite vaut 0 par le lemme 1.

D'où le résultat car $f_n(z) \underset{n \longrightarrow +\infty}{\longrightarrow} \prod_{k=1}^{\infty} \frac{1}{1 - z^{\varphi(k)}}$ □

Voici maintenant la preuve du Lemme 2 :

Preuve.

Comme $\varphi(n) \geq \sqrt{\frac{n}{2}}$, on a $z^{\varphi(n)} = o\left(\frac{1}{n^2}\right)$ et donc la série $\sum_{n \geq 1} z^{\varphi(n)}$ est absolument convergente et donc $\prod_{n \geq 1} \frac{1}{1 - z^{\varphi(n)}}$ aussi.

On a en utilisant les notations précédentes, $f_n(z) = \sum_{p=0}^{\infty} c_p(n) z^p$. De plus, $c_p(n) \underset{n \to +\infty}{\longrightarrow} b_p$. On a pour $x \in]0, 1[$,

$$\begin{aligned}
\sum_{p=0}^{\infty} (c_p(n+1) - c_p(n)) x^p &= \sum_{p=0}^{\infty} c_p(n+1) x^p - \sum_{p=0}^{\infty} c_p(n) x^p \\
&= f_{n+1}(x) - f_n(x) \\
&= x^{\varphi(n+1)} f_{n+1}(x) \\
&\leq f_{n+1}(x)
\end{aligned}$$

Donc $\sum_{n \geq 0} \left(\sum_{p=0}^{\infty} (c_p(n+1) - c_p(n)) x^p \right)$ converge donc $(c_p(n+1) - c_p(n)) x^p)_{n,p \geq 0}$ est sommable et finalement :

$$\sum_{p=0}^{\infty} \sum_{n=0}^{\infty} |c_p(n+1) - c_p(n)| |x|^p < \infty.$$

Or on a,

$$\sum_{p=0}^{\infty} \sum_{n=0}^{\infty} (c_p(n+1) - c_p(n)) x^p = \sum_{p=0}^{\infty} b_p x^p$$

Donc $\sum_{p \geq 0} a_p x^p$ converge et cela conclut. □

Remarque 1. Cette identité est la première étape d'une (longue) démonstration permettant d'obtenir l'équivalent

$$\log(b_n) \underset{n \to +\infty}{\sim} \frac{\sqrt{105 \zeta(3) n}}{\pi}$$

Remarque 2. On ne fait pas la preuve des deux lemmes dans le développement.

Remarque 3. Pour les références, la proposition 1 est dans Oraux X-ENS Algèbre 1, la proposition 2 est prouvée de manière très similaire dans Oraux X-ENS Analyse 2 avec le nombre $p(n)$ de partitions d'un entier : il suffit de changer les notations.