

Théorème Soient $\alpha_1, \dots, \alpha_p \in \mathbb{N}^*$ des nombres premiers entre eux dans leur ensemble.

Pour $n \in \mathbb{N}^*$, on note S_n le nombre de solutions $(n_1, \dots, n_p) \in \mathbb{N}^p$ de l'équation

$$\alpha_1 n_1 + \dots + \alpha_p n_p = n.$$

$$\text{Alors } S_n \sim \frac{n^{p-1}}{\alpha_1 \dots \alpha_p (p-1)!}$$

Considérons la série entière définie par le produit de Cauchy $(\sum_{n_1} z^{\alpha_1 n_1}) \dots (\sum_{n_p} z^{\alpha_p n_p})$.

On remarque que le coefficient de z^n dans ce produit de Cauchy est le nombre de manières de combiner les puissances de z de chaque terme du produit pour que leur somme fasse n .

Ainsi, on a :

$$F(z) := \sum_{n=0}^{+\infty} S_n z^n = \left(\sum_{n_1=0}^{+\infty} z^{\alpha_1 n_1} \right) \dots \left(\sum_{n_p=0}^{+\infty} z^{\alpha_p n_p} \right) = \prod_{i=1}^p \frac{1}{1 - z^{\alpha_i}} \text{ avec un rayon de convergence } 1$$

La fonction F est une fraction rationnelle dont les pôles sont les racines α_i -ièmes.

De plus,

• 1 est un pôle d'ordre p

• soit $\omega \neq 1$ un pôle de F supposé d'ordre p , alors $\omega^{\alpha_1} = \dots = \omega^{\alpha_p} = 1$. Or, on peut écrire ω sous la forme $\omega = e^{2i\pi a/b}$ avec $a \wedge b = 1$. On obtient donc $b \mid \alpha_i$ pour tout i , d'où par le lemme de Gauss $b \mid \alpha_i$ pour tout i . Les α_i étant premiers entre eux dans leur ensemble $b = 1$ donc $\omega = 1$. Absurde ! Donc ω est un pôle d'ordre $< p$.

On peut donc écrire la décomposition en éléments simples de F sous la forme :

$$F(z) = \frac{A}{(1-z)^p} + G(z) \quad \text{avec } G(z) = \sum_{\omega \text{ pôle}} \frac{a_{1,\omega}}{\omega - z} + \dots + \frac{a_{p-1,\omega}}{(\omega - z)^{p-1}}$$

Or :

$$\frac{1}{(\omega - z)^k} = \frac{1}{\omega^k} \cdot \frac{1}{(1 - z/\omega)^k} = \frac{1}{\omega^k} \cdot \frac{1}{(k-1)!} \sum_{n=0}^{+\infty} \frac{(n+k-1)!}{n!} \left(\frac{z}{\omega}\right)^n = \sum_{n=0}^{+\infty} \binom{n+k-1}{k-1} \omega^{-n-k} z^n$$

Alors si $|\omega| = 1$, le coefficient devant z^n est un $O(n^{k-1})$ car en n , $\binom{n+k-1}{k-1}$ est un polynôme de degré $k-1$.

Donc le coefficient devant z^n dans G est un $O(n^{p-2})$.

Et :

$$S_n = A \binom{n+p-1}{p-1} + O(n^{p-2}) = \frac{A}{(p-1)!} (n+p-1) \dots (n+1) + O(n^{p-2})$$

$$\text{De plus : } (1-z)^p F(z) = \prod_{i=1}^p \frac{1-z}{1-z^{\alpha_i}} = \prod_{i=1}^p \frac{1}{1 + \dots + z^{\alpha_i-1}}$$

Donc en évaluant en 1,

$$A = \frac{1}{\alpha_1 \dots \alpha_p}$$

$$\text{Finalement, } S_n \sim \frac{1}{\alpha_1 \dots \alpha_p} \frac{n^{p-1}}{(p-1)!}$$

Remarque En calculant toute la décomposition en éléments simples de F , on peut obtenir une formule exacte mais compliquée de S_n .

Application Soit $n \in \mathbb{N}^*$.

Dans un système monétaire $\{1, 2, 5, 10\}$, le nombre q_n de façons de faire n euros, a un comportement asymptotique $q_n \sim \frac{n^3}{600}$