21 Equation diophantienne et série génératrice

ref : Chambert-Loir

THÉORÈME 21.1 *Soient $\alpha_1, \dots, \alpha_m \in N^*$ premiers entre eux dans leur ensemble. On pose $p(n) = \text{card}\{(x_1, \dots, x_m) \in (\mathbb{N}^*)^n \quad | \quad \sum_i \alpha_i x_i = n\}$. On a l'équivalent :*

$$p(n) \sim \frac{n^{m-1}}{\alpha_1 \dots \alpha_m (m-1)!}$$

PREUVE. On pose la série formelle génératrice $G(X) = \sum_{n \leq 0} p(n) X^n$. On va reconnaitre un produit de Cauchy :

$$G(X) = \sum_{n \geq 0} (\sum_{\alpha_1 x_1 + \dots + \alpha_m x_m = n} 1) X^n = \sum_{n \geq 0} (\sum_{i_1 + \dots + i_m = n} b_{i_1} \dots b_{i_m}) X^n$$

où on a posé $b_{i_k} = 1$ si $\alpha_k | i_k$ et 0 sinon. D'où :

$$G(X) = \prod_{i=1}^{m} (\sum_{k \geq 0} b_{i_k} X^{i_k}) = \prod_{i=1}^{m} \sum_{k \geq 0} X^{k \alpha_i} = \prod_{i=1}^{m} \frac{1}{1 - X^{\alpha_i}}$$

On est ramené à étudier cette fraction rationnelle. Ses pôles sont des racines de l'unité et 1 est le seule pôle d'ordre maximal puisque les α_i sont premiers entre eux dans leur ensemble. En effet, si $\zeta^{\alpha_i} = 1$ pour tout i, par Bézout ζ vaut 1.

La décomposition de G en éléments simples s'écrit donc :

$$G(X) = \frac{A}{(1-X)^m} + B(X)$$

où $A \in \mathbb{C}$, $B \in \mathbb{C}(X)$ où les pôles de B sont d'ordre strictement inférieur à m.

Par dérivation successive du développement $\frac{1}{1-X} = \sum_{n \geq 0} X^n$ on a :

$$\frac{1}{(a-X)^m} = \frac{1}{a^m (m-1)!} \sum_{n \geq 0} (n+1) \dots (n+m-1) (\frac{X}{a})^n$$

Le terme général de cette série formelle est équivalent à :

$$\frac{n^{m-1}}{(m-1)! a^{m-n}}$$

Le terme du développement correspondant au pôle 1 domine donc asymptotiquement sur les autres car son ordre m est strictement plus grand. On a donc l'équivalent :

$$p(n) \sim \frac{A n^{m-1}}{(m-1)!}$$

Il reste à déterminer le coefficient A.

En multipliant par $(1-X)^m$, on obtient :

$$G(X)(1-X)^m = A + B(X)(1-X)^m$$

Les deux membres sont des fractions rationnelles dont 1 n'est pas un pôle, on peut donc les évaluer en 1. Le terme $B(X)(1-X)^m$ vaut 0 en 1 et le terme de gauche se calcule :

$$G(X)(1-X)^m = \prod_{i=1}^{m} \frac{1-X}{1-X^{\alpha_i}} = \prod_{i=1}^{m} \frac{1}{1 + X + \dots + X^{\alpha_i - 1}}$$

En évaluant en 1, cela donne $A = \frac{1}{\alpha_1 \dots \alpha_m}$ et l'équivalent souhaité :

$$p(n) \sim \frac{n^{m-1}}{\alpha_1 \dots \alpha_m (m-1)!}$$

□