4 Dénombrement des solutions d'une équation diophatienne

Théorème. *Soient $\alpha_1, \cdots, \alpha_m \in \mathbb{N}^*$ premiers entre eux globalement. Pour tout $n \in \mathbb{N}$, notons S_n le nombre de m-uplets $(n_1, \cdots, n_m) \in \mathbb{N}^m$ tels que*

$$\alpha_1 n_1 + \cdots + \alpha_m n_m = n.$$

Alors,

$$S_n \sim_{n\to+\infty} \frac{1}{\alpha_1 \cdots \alpha_n} \frac{n^{m-1}}{(m-1)!}$$

Tout d'abord, rappelons que l'anneau des fractions rationnelles de $\mathbb{C}(T)$ sans pôle en 0 est un sous-anneau de $\mathbb{C}[[T]]$, ce qu'on utilisera plusieurs fois dans la suite.

Notons $F(T) = \sum_{n\geq 0} S_n T^n \in \mathbb{C}[[T]]$. Alors, dans $\mathbb{C}[[T]]$, par définition du produit de séries formelles

$$\prod_{i=1}^{m} \frac{1}{1-T^{\alpha_i}} = \prod_{i=1}^{m} \sum_{n_i \geq 0} T^{\alpha_i n_i} = \sum_{(n_1,\cdots,n_m)\in\mathbb{N}^n} T^{(\sum_{i=1}^m \alpha_i n_i)} = \sum_{n\in\mathbb{N}} S_n T^n.$$

Ainsi, F a pour seuls pôles les racines α_i-ièmes de l'unité où i parcourt $1, \cdots, m$. De plus, pour tout α, $T^\alpha - 1$ est scindé à racines simples dans $\mathbb{C}$ et si $\zeta^{\alpha_i} = 1$ pour tout i, comme $\alpha_1, \cdots, \alpha_m$ sont premiers entre eux globalement, il existe une combinaison linéaire entière de ceux-ci valant 1, donc $\zeta = 1$. Ceci prouve que F a un pôle d'ordre exactement m en 1, et que tous les autres pôles de F sont situés en des racines de l'unité et d'ordre au plus $m-1$. Par décomposition en éléments simple, on peut donc écrire

$$F(T) = \frac{A}{(1-T)^m} + \sum_{\zeta\in U} \sum_{k=1}^{m-1} \frac{A_{\zeta,k}}{(\zeta - T)^k} + P(T)$$

avec A et les $A_{\zeta,k}$ des constantes complexes, U l'ensemble des racines α_i-ièmes de l'unité pour un certain α_i et $P = \sum_{n=0}^{N} P_n T^n \in \mathbb{C}[T]$. Par récurrence et dérivation sur les séries formelles, pour tout $\zeta \in U$ et tout $k \in \mathbb{N}^*$, on a

$$\frac{1}{(\zeta - T)^k} = \left(\frac{1}{\zeta - T}\right)^{(k-1)} = \frac{1}{\zeta^k (k-1)!} \sum_{n\geq 0} (n+1)\cdots(n+k-1) \left(\frac{T}{\zeta}\right)^n.$$

Ainsi, pour tout $n \in \mathbb{N}$, par identification des coefficients,

$$\begin{aligned} S_n &= A\frac{(n+1)\cdots(n+m-1)}{(m-1)!} + \sum_{\zeta\in U}\sum_{k=1}^{m-1} \frac{A_{\zeta,k}(n+1)\cdots(n+k-1)}{(k-1)!\zeta^{n+k}} + P_n \\ &= \frac{An^{m-1}}{(m-1)!} + o(n^{m-1}) + \sum_{\zeta\in U}\sum_{k=1}^{m-1} o(n^{k-1}) \\ &= \frac{An^{m-1}}{(m-1)!} + o(n^{m-1}). \end{aligned}$$

Il reste donc à calculer A. En se plaçant dans $\mathbb{C}(T)$, comme A est le coefficient attaché au pôle d'ordre le plus élevé en 1, on a

$$\begin{aligned} A &= ((1-T)^m F(T))_{T=1} \\ &= \prod_{i=1}^{m} \left(\frac{1}{1+T+\cdots+T^{\alpha_i-1}}\right)_{T=1} \\ &= \frac{1}{\alpha_1 \cdots \alpha_m}. \end{aligned}$$

ce qui conclut la preuve.

Référence : [Goblot], Exercice 9.2.

Leçons compatibles :

124 Anneau des séries formelles. Applications

126 Exemples d'équations diophantiennes

140 Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications

190 Méthodes combinatoires, problèmes de dénombrement (le présenter comme un problème de nombre de partitions)