27 Dénombrement des solutions d'une équation diophantienne

Soient α_1, ..., α_r des entiers non nuls premiers entre eux (dans leur ensemble). Pour chaque $n \in \mathbb{N}$, on considère l'équation diophantienne $(E_n) : \alpha_1 n_1 + ... + \alpha_r n_r = n$ (où l'inconnue est $(n_1, ..., n_r) \in \mathbb{N}^r$).

THÉORÈME. *L'équation diophantienne (E_n) a un nombre fini de solutions s_n que l'on peut calculer de manière explicite. De plus, $s_n \sim \dfrac{1}{\alpha_1 ... \alpha_r} \dfrac{n^r}{(r-1)!}$ quand $n \to +\infty$.*

Preuve.
Dans l'énoncé, le terme « explicite » signifie que nous allons donner une méthode pour calculer (en temps fini) une expression de s_n qui sera valable $\forall n$.

Soit $F(X) = \prod_{i=1}^{r} \dfrac{1}{1 - X^{\alpha_i}}$. D'une part, on a (dans $\mathbb{C}[[X]]$)

$$F(X) = \prod_{i=1}^{r} \sum_{n \geqslant 0} X^{n\alpha_i}$$

puis

$$F(X) = \sum_{n \geqslant 0} \sum_{n_1\alpha_1 + ... + n_r\alpha_r = n} X^n$$

d'où $F(X) = \sum s_n X^n$.

D'autre part, $F(X)$ admet une décomposition en éléments simples de la forme

$$F(X) = \sum_{\omega \in \bigcup \mu_{\alpha_i}(\mathbb{C})} \frac{a_{\omega,1}}{\omega - X} + ... + \frac{a_{\omega,m_\omega}}{(\omega - X)^{m_\omega}}$$

où on a noté $\mu_{\alpha_i}(\mathbb{C})$ le groupe des racines α_i-èmes de l'unité dans $\mathbb{C}$. Cette décomposition a lieu dans $\mathbb{C}(X)$ mais elle est valable dans $\mathbb{C}[[X]]$ car 0 n'est pas un pôle de F. On sait que les $a_{\omega i}$ peuvent être calculés de manière explicite.

Ensuite, on écrit que

$$\frac{1}{(\omega - X)^k} = \frac{1}{(k-1)!} \frac{\mathrm{d}^{k-1}}{\mathrm{d}X^{k-1}} \left(\frac{1}{\omega - X} \right)$$

d'où

$$\frac{1}{(\omega - X)^k} = \frac{1}{(k-1)!} \sum_{n \geqslant 0} (n+1)...(n+k-1)\omega^{-n-k} X^n$$

En reportant dans l'expression précédente de $F(X)$ et en identifiant les coefficients, on en déduit une expression de s_n.

Comme $F(X) = \prod_{i=1}^{r} \frac{1}{1-X^{\alpha_i}}$, 1 est un pôle de F d'ordre r. Tous les autres pôles ω sont d'ordre $m_\omega < r$. En effet, chaque polynôme $1 - X_i^{\alpha}$ est à racines simples, donc ω est un pôle d'ordre $\leqslant r$ de F et s'il était d'ordre r, il serait racine de chaque $1 - X^{\alpha_i}$. D'après l'identité de Bezout, il existe des entiers u_1, ..., u_r tels que $u_1\alpha_1 + ... + u_r\alpha_r = 1$ (car les α_i sont premiers entre eux). On obtiendrait alors $\omega = \omega^{u_1\alpha_1+...+u_r\alpha_r} = 1$.

Le terme général de la série $\frac{1}{(\omega - X)^k}$ est un $O(n^{k-1})$ (cf. ci-dessus, en se rappelant que $|\omega| = 1$), donc un $o(n^{r-1})$ sauf si $\omega = 1$ et $k = r$. On en déduit que dans l'expression de s_n, les contributions des $\frac{1}{(\omega - X)^k}$ sont négligeables devant celle de $\frac{1}{(1-X)^r}$. Ainsi, $s_n \sim a_{1,r}\frac{n^{r-1}}{(r-1)!}$ quand $n \to +\infty$.

Enfin, calculons $a_{1,r}$. Pour cela, on écrit que $a_{1,r} = (1-z)^r F(z)_{|z=1}$. Or $(1-X)^r F(X) = \prod_{i=1}^{r} \frac{1-X}{1-X^{\alpha_i}}$ soit encore $(1-X)^r F(X) = \prod_{i=1}^{r} \frac{1}{1+X+...+X^{\alpha_i-1}}$. Finalement, on a $a_{1,r} = \frac{1}{\alpha_1...\alpha_r}$, d'où le résultat attendu. □

Leçons possibles
114 Équations diophantiennes du premier degré $ax + by = c$. Autres exemples d'équations diophantiennes.
115 Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.
145 Méthodes combinatoires, problèmes de dénombrement.
224 Comportement asymptotique des suites numériques. Rapidité de convergence. Exemples.

Références
Gourdon, chambi ?