Etudes

La Loi de Réciprocité Diophantienne

Eugène EHRHART
Strasbourg

Le nombre de solutions d'un *système diophantien linéaire homothétique* est une fonction $f(n)$ du rapport d'homothétie. On précise la nature de $f(n)$ et on indique le moyen de la calculer. Pour deux systèmes «complémentaires» les fonctions $f_1(n)$ et $f_2(n)$ sont liées par une *«loi de réciprocité»* d'une grande simplicité et d'une étonnante généralité.

Cette étude fait partie de *«la géométrie des nombres»* créée par MINSKOWSKI vers 1900. De nos jours, le jumelage fécond de l'arithmétique et de la géométrie s'est considérablement développé et s'appelle maintenant *l'arithmo-géométrie*. Elle a récemment donné naissance à de nombreux travaux.

Problème type ([4], page 105) :

De combien de manières peut-on payer n francs en pièces de 10, 20, 50 et 100 centimes ?

$$X + 2Y + 5Z + 10T = 10n$$
$$X, Y, Z, T \geq 0.$$

Ce système définit un tétraèdre entier fermé P_n *homothétique de* P_1 dont les sommets sont situés sur les axes de l'espace à quatre dimensions.

Ayant calculé le nombre j_n de solutions du système large (≥ 0), on a instantanément le i_n du système strict (>0) par réciprocité :

$$j_n = \frac{1}{6}(n+1)(2n+1)(5n+6)$$

$$i_n = \frac{1}{6}(n-1)(2n-1)(5n-6)$$

On se limitera à l'exposé des principaux résultats. Pour les démonstrations - elles exigeraient toute une brochure - nous renvoyons à nos publications [1], [2], [3], [4].

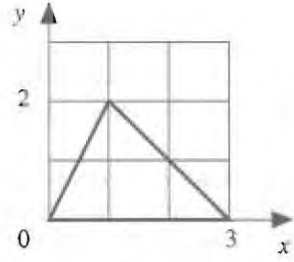
Soient n un entier positif ou nul et a_i, $\alpha \in \mathbf{Z}$. Une inéquation

$$a_1X_1 + a_2X_2 + \ldots + a_KX_K > \alpha n$$

définit un demi-espace dans R^K. Plusieurs inéquations de ce type réunies forment un système diophantien linéaire homothétique (H_n). On ne s'intéresse qu'au cas où le *système primitif* (H_1) définit dans R^K une région bornée, c'est-à-dire un polytope convexe à k dimensions. Alors (H_n) a un nombre fini i_n de solutions entières, qu'on se propose de calculer.

Partons d'un exemple banal. Le nombre de solutions entières est i_n pour le système strict (triangle associé ouvert), j_n pour le système large (triangle associé fermé).

$Y > 0$
$2X - Y > 0$
$X + Y < 3n$
$i_n = 3n^2 - 3n + 1$



$Y \geq 0$
$2X - Y \geq 0$
$X + Y \leq 3n$
$j_n = 3n^2 + 3n + 1$

Si dans cette figure l'unité est le centimètre, le nombre de points entiers du triangle est $i_1 = 1$ ou $j_1 = 7$.

Si l'unité est le millimètre, pour ce même triangle, ces nombres sont $i_{10} = 271$ et $j_{10} = 331$.

1- Polygones entiers.

Un polygone P (et plus généralement un polyèdre ou un polytope de dimension quelconque) est dit *«entier»* si les coordonnées des sommets sont toutes entières. Alors, *le nombre de points entiers du polygone ouvert homothétique nP est*

(1) $$i_n = Sn^2 - \frac{I}{2}n + 1 \quad (*)$$

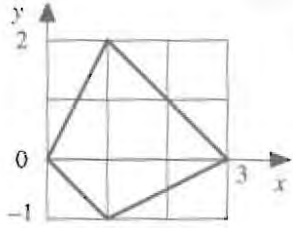
(*) Cette relation se déduit de la formule classique de Pick : $S = i + p/2 - 1$ où i et p sont les points entiers intérieurs ou périphériques d'un polygone entier et S son aire.

où S est l'aire de P et l la *«longueur réticulaire»* de son bord, obtenue en comptant pour 1 la distance de deux points entiers consécutifs. Fait remarquable, *le nombre de points entiers de nP fermé est :*

(2) $$j_n = Sn^2 + \frac{l}{2}n + 1$$

Exemple :

$2X - Y > 0$
$X + Y < 3n$
$X - Y < 3n$
$X + 2Y > 0$



$$i_n = \frac{9}{2}n^2 - \frac{5}{2}n + 1$$

$$j_n = \frac{9}{2}n^2 + \frac{5}{2}n + 1$$

Remarque :
Pour un système diophantien linéaire homothétique, le polygone associé P_n est convexe. Mais *les formules* (1) *et* (2) *s'appliquent même si* P_n *est concave* (pourvu que son contour soit une courbe de Jordan).

2- Polytopes entiers.

Les nombres i_n *et* j_n *des points entiers du polytope ouvert ou fermé nP sont encore des polynômes de degré d* (dimension du polytope). Ils comptent aussi le nombre de solutions entières des systèmes diophantiens stricts ou larges associés.

Le polynôme j_n a pour terme constant 1 et débute par $Vn^d + \frac{S}{2}n^{d-1}$ où V est le volume d-dimensionnel du polytope P et S la «mesure réticulaire» de son bord (dans chaque face, l'unité est la base du réseau de points entiers de son hyperplan support).

Les dénombrants i_n *et* j_n *sont liés par la très remarquable relation*

$$\boxed{j_n = (-1)^d i(-n)} \quad (1)$$

Nous l'appelons **loi de réciprocité**, car on a aussi $i_n = (-1)^d j(-n)$.

On peut calculer les coefficients du polynôme i_n *par quelques dénombre-*

(1) La notation $i(-n)$ désigne le polynôme obtenu en remplaçant n par $-n$ dans le polynôme i_n, alors que la notation i_{-n} désignerait le nombre de points intérieurs à P_{-n}

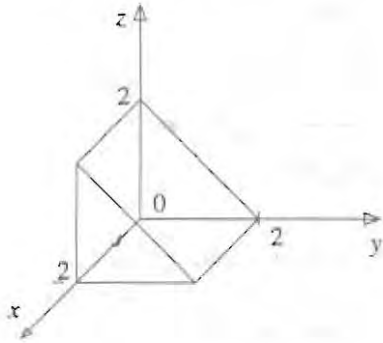
ments initiaux. Ainsi pour un polyèdre de volume V

$$i_n = Vn^3 - an^2 + bn - 1.$$

Connaissant i_1, i_2 par dénombrement direct, on calcule a et b en résolvant

$$V - a + b - 1 = i_1$$
$$8V - 4a + 2b - 1 = i_2.$$

Exemple (prisme droit triangulaire) :



$X < 2n$
$X, Y, Z > 0$
$Y + Z < 2n$

$i_n = (n-1)(2n-1)^2$
$j_n = (n+1)(2n+1)^2$

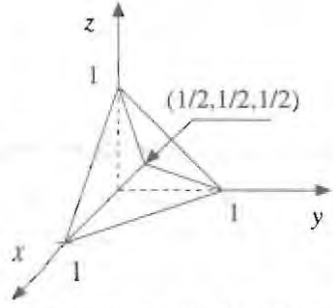
3- Polytopes rationnels (les coordonnées des sommets sont des nombres rationnels).

Les dénombrants i_n ou j_n du polytope ouvert ou fermé à d dimensions sont des «polynômes arithmétiques» (ou polars) de degré d ; leurs coefficients ne sont pas tous constants, mais peuvent présenter des *«entiers périodiques»*. Par exemple, un nombre de période **3** s'écrit

$$[a, b, c] = \begin{cases} a & \text{si } n = 1 \text{ mod.3} \\ b & \text{si } n = 2 \text{ mod.3} \\ c & \text{si } n = 0 \text{ mod.3} \end{cases}$$

On détermine les coefficients d'un *«polar»* à l'aide de la théorie subtile du *«produit sommital»* d'un polytope rationnel, théorie qu'il serait trop long à exposer ici [3], [4]. Bornons-nous à donner i_n et j_n pour un exemple :

$$X + Y \le n$$
$$X + Z \le n$$
$$Y + Z \le n \qquad X, Y, Z \ge 0$$



Le domaine primitif ($n = 1$) est un hexaèdre P_1 dont quatre sommets sont entiers et un seulement rationnel $\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$.

$$i_n = \frac{2n^3 + 9n^2 + 14n + [7,8]}{8} = \left\| \frac{(n+1)(2n^2+7n+7)}{8} \right\|$$

où le nombre périodique [7,8] est égal à 7 ou à 8, suivant que n est impair ou pair, et où $\|A\|$ désigne l'entier le plus proche de A. Remarquons que 1/4, premier coefficient de i_n, est encore le volume de P_1.

La loi de réciprocité s'applique encore : Pour le système strict

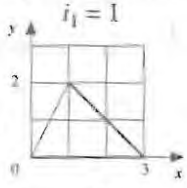
$$i_n = \frac{2n^3 - 9n^2 + 14n - [7,8]}{8} = \left\| \frac{(n-1)(2n^2-7n+7)}{8} \right\|.$$

4- Polytopes semi-ouverts.

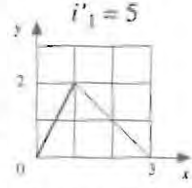
Si dans un système diophantien linéaire homothétique figurent à la fois des inéquations strictes et larges, le polytope associé P_n est *«semi-ouvert»* (certains points entiers du bord appartiennent à P_n, d'autres pas). En échangeant les signes > et ≥, on obtient le *«système complémentaire»*. Son polytope associé P'_n est dit *«polytope complémentaire»* de P_n. *Les dénombrants i_n de P_n, i'_n de P'_n, sont encore des polynômes ou des polynômes arithmétiques de degré d (dimension de P_n), suivant que P_1 est entier ou rationnel. Ils vérifient la loi de réciprocité* $i'_n = (-1)^d i(-n)$.

Exemple (les points entiers des gros traits sont exclus ; les gros traits réunis des deux figures forment le bord complet du triangle) :

$Y > 0$
$2X - Y \geq 0$
$X + Y < 3n$
$i_n = n(3n-2)$



$Y \geq 0$
$2X - Y > 0$
$X + Y \leq 3n$
$i'_n = n(3n+2)$



On détermine les coefficients a, b de $i_n = Sn^2 + an + b$ ($S = 3$ est l'aire du triangle) par deux décomptes initiaux $i_1 = 1$, $i_2 = 8$:

$$3 + a + b = 1$$
$$12 + 2a + b = 8$$

donnent $a = -2$, $b = 0$.

Remarques : Tous nos exemples sont traités en détail dans [3]. Depuis ma thèse [1] et le livre [3] qui la prolonge «la méthode des polytopes» a trouvé de nombreuses applications. En particulier, nous avons montré que *le volume-dimensionnel d'un polytope entier P_1 de dimension d est*

$$V = \frac{(i-1)^{(d)}}{d!} = \frac{(j-1)^{(d)}}{d!} \qquad (*)$$

la puissance symbolique signifiant que, dans le développement, i_r remplace i^r. Ainsi, la surface d'un polygone entier est

$$S = \frac{i_2 - 2i_1 + 1}{2} = \frac{j_2 - 2j_1 + 1}{2}.$$

Bibliographie

[1] Thèse, *«Sur un problème de géométrie diophantienne linéaire»*, Journal de Crelle, Volumes 226 et 227 (1967).

[2] Comptes rendus, Ac.sc., *«Démonstration de la loi de réciprocité pour un polyèdre entier»*, t.265, p.5-7 (3 juillet 1967), *«Démonstration de la loi de réciprocité du polyèdre rationnel»*, t.265, p.91-94 (17 juillet 1967).

[3] *«Polynômes arithmétiques et Méthode des Polyèdres en Combinatoire»*, International Series of Numerical Mathematics», Vol. 35, Birkhaüser Verlag (1977).

[4] *«Histoire et leçons d'une recherche»*, Articles de Mathématiques, Cédic/Nathan (1985).

(*) Le dernier terme de $(j-1)^{(d)}$ est $(-1)^{(d)}$ mais le dernier terme de $(i-1)^{(d)}$ est $(+1)$ quel que soit d. Ainsi, le volume d'un polyèdre entier est : $V = \frac{i_3 - 3i_2 + 3i_1 + 1}{6} = \frac{j_3 - 3j_2 + 3j_1 - 1}{6}$. On le contrôle aisément sur le cube construit sur le tétraèdre (0, 0, 0) (1, 0, 0) (0, 1, 0) (0, 0, 1).