Approximation diophantienne et réseaux

Benoît Mselati

Introduction La théorie de l'approximation diophantienne est l'étude de diverses propriétés d'approximation de nombres par les rationnels. Dans le cas d'un seul réel, le problème est assez simple, comme nous le verrons dans la première partie. En revanche, les choses se complique dès que l'on veut approximer simultanément plusieurs réels par des rationnels.Ce problème revient à approximer un vecteur de $\mathbb{R}^n$ par un vecteur à coordonnées rationnelles, de même dénominateur, c'est-à-dire par un point du réseau des vecteurs de $\mathbb{R}^n$ à coordonnées rationnelles de même dénominateur. Nous verrons qu'alors on perd en précision, ce qui est naturel puisque l'on doit prendre en compte plus de contraintes.

L'approximation diophatienne intervient dans de nombreux domaines des mathématiques, on peut notamment établir des "correspondances" entre ces résultats et des théorèmes de systèmes dynamiques ou de théorie ergodique.

1 Approximation diophantienne dans $\mathbb{R}$

Le cas le plus simple est celui d'un seul nombre réel. Bien sûr, on peut approcher tout réel par des rationnels aussi proche que l'on veut, au sens où, si x est un réel :

$$\forall \epsilon > 0, \exists p, q \in \mathbb{Z}, \quad |x + \frac{p}{q}| \leq \epsilon$$

Mais lorsque l'on fait tendre ϵ vers 0, les entiers p et q qui conviennent tendent vers l'infini, et nous n'avons en fait aucun contrôle de l'interdépendance entre la taille de q et l'écart ϵ. Notre but est en fait de construire des rationnels $\frac{p}{q}$ approchant x au sens où l'écart $|x - \frac{p}{q}|$ sera majoré par une puissance de q.

Bien sûr, on peut aisément obtenir une majoration par la quantité $\frac{1}{q}$. Plus précisément :

Propriété 1.1 *Soit x un réel, q un entier strictement positif. Alors il existe un entier relatif p tel que*

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{2q}$$

Démonstration On considère la partie entière n du produit qx. Deux cas sont alors possibles :

- Soit $qx - n \leq \frac{1}{2}$, auquel cas on pose $p = n$.
- Soit $\frac{1}{2} \leq qx - n \leq 1$, auquel cas $(n+1) - qx \leq \frac{1}{2}$, et l'on pose $p = n + 1$.

Dans tous les cas, on a trouvé un entier p tel que $|qx - p| \leq \frac{1}{2}$, et donc

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{2q} \qquad \square$$

Mais on voudrait une plus grande précision. On peut en fait obtenir une majoration par $\frac{1}{q^2}$, selon le résultat suivant :

Théorème 1.2 (Dirichlet) .
Soit $x \in \mathbb{R}$. Il existe une infinité de $q \in \mathbb{Z}$ tels que

$$|qx + p|.|q| < 1. \tag{1}$$

pour un certain $p \in \mathbb{Z}$.

C'est-à-dire que les approximations de x, de la forme $-\frac{p}{q}$, vérifieront :

$$|x + \frac{p}{q}| < \frac{1}{|q|^2}$$

Démonstration Nous reprenons la démonstration originelle de Dirichlet. Soit n un entier non nul. Considérons les $n+1$ nombres de $[0,1)$:

$$x_k = kx - \mathrm{E}(kx), 0 \leqslant k \leqslant n$$

où $\mathrm{E}(x)$ désigne la partie entière de x. Appliquons le principe des tiroirs aux n intervalles de $[0,1)$:

$$\mathrm{I}_k = [k/n, (k+1)/n)$$

à la réunion desquels appartiennent les $n+1$ nombres précédents. Il existe ainsi deux entiers $i_n < j_n$ et un entier k_n tels que x_{i_n} et x_{j_n} appartiennent à I_{k_n}. Posons $q_n = j_n - i_n$ et $p_n = \mathrm{E}(i_n x) - \mathrm{E}(j_n x)$. On vérifie que

$$|x_{j_n} - x_{i_n}| = |q_n x + p_n| < 1/n \leqslant 1/q_n$$

Le cas où x est rationnel est évident (il suffit de prendre pour q_n des multiples du dénominateur). Si x n'est pas rationnel, on a construit deux suites d'entiers $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ telles que $|q_n x + p_n| < 1/n \leqslant 1/q_n$. Pour terminer la preuve du théorème de Dirichlet, il suffit de montrer que la suite $(q_n)_{n\in\mathbb{N}}$ prend une infinité de valeurs distinctes. Pour cela, il suffit encore de montrer qu'elle tend vers l'infini, ce qui est assuré par le lemme suivant (et le théorème est ainsi démontré.

$\square$

Lemme 1.3 *Soit x un irrationnel positif. Soient $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ deux suites d'entiers naturels telles que*

$$\frac{p_n}{q_n} \overset{n\to\infty}{\longrightarrow} x$$

alors

$$q_n \overset{n\to\infty}{\longrightarrow} \infty$$

Démonstration Soit donc x un irrationnel positif. Soient $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ deux suites d'entiers naturels telles que

$$\lim_{n\to\infty} \frac{p_n}{q_n} = x$$

Or x est irrationnel, donc pour tout entier naturel n, $d\left(x, \frac{1}{n}\mathbb{Z}\right) > 0$, c'est-à-dire qu'il exite un intervalle de longueur $l_n > 0$, centré en x et ne contenant aucun rationnel de la forme $\frac{p}{n}$.

Soit N un entier naturel. L'intervalle centré en x et de longueur $\min_{n\leq \mathrm{N}} l_n$ ne contient alors aucun rationnel de dénominateur inférieur ou égal à N.

Mais comme la suite $\frac{p_n}{q_n}$ tend vers x, tous ses termes sont dans cet intervalle à partir d'un certain rang. Autrement dit, à partir d'un certain rang, tous les dénominateurs q_n sont plus grands que N.

Formellement, on a montré :

$$\forall \mathrm{N}, \exists n_0, \quad n \geq n_0 \Longrightarrow q_n \geq \mathrm{N}$$

C'est-à-dire

$$\lim_{n\to\infty} q_n = +\infty$$

□

D'autres méthodes permettent de prouver ce théorème, la plus constructive faisant intervenir les fractions continues (cf[HW]). Un rationnel p/q vérifiant (1) est appelé "approximation rationnelle" de x.

2 Approximation simultanée de réels par des rationnels

Cependant, on s'intéresse souvent en théorie des nombres à des propriétés d'approximation simultanée de nombres par des rationnels, ou, ce qui revient au même, à des propriétés d'approximation de vecteurs de $\mathbb{R}^n$ par des vecteurs à coordonnées rationnelles. Pour obtenir en particulier une généralisation du théorème 1 du paragraphe précédent, nous aurons besoin de résultats de ce qu'on appelle la "géométrie des nombres", parmi lesquels le célèbre théorème suivant dont existent différentes versions, et de nombreuses applications(cf[C]) :

Théorème 2.1 (Théorème de Minkowski) .

Soit $\mathrm{A} \in \mathrm{GL}(n, \mathbb{R})$. *Supposons donnés des réels positifs* $\lambda_1, ..., \lambda_n$ *vérifiant* $\prod_{j=1}^n \lambda_j \geqslant \det \mathrm{A}$ *et un entier* $i \in [\![1\,; n]\!]$. *Alors il existe* $x \in \mathbb{Z}^n - \{0\}$ *tel que*

$$|(\mathrm{A}x)_i| \leqslant \lambda_i \text{ et } |(\mathrm{A}x)_j| < \lambda_j \text{ pour } j \neq i.$$

Démonstration La démonstration repose sur le lemme suivant. Nous noterons $|\mathrm{X}|$ la mesure de Lebesgue d'un ensemble mesurable X de $\mathbb{R}^n$.

Lemme 2.2 (Blichfeldt) .

Soit X un ensemble mesurable de $\mathbb{R}^n$ *tel que*

$$|\mathrm{X}| > 1$$

Alors il existe x *et* y *distincts dans* X *tels que* $x - y \in \mathbb{Z}^n$.

Démonstration Supposons le résultat du lemme faux. Dans ce cas, si z et z' sont distincts dans $\mathbb{Z}^n$, les ensembles $\mathrm{X}+z$ et $\mathrm{X}+z'$ sont disjoints. Or, si l'on pose

$$\mathrm{P} = \{(x_1, ..., x_n) \mid 0 \leqslant x_i < 1\}$$

on peut écrire

$$\mathrm{X} = \bigsqcup_{z \in \mathbb{Z}^n} (\mathrm{X} \cap (\mathrm{P}+z))$$

et par conséquent

$$\begin{aligned} |\mathrm{X}| &= \sum_{z \in \mathbb{Z}^n} |(\mathrm{X} \cap (\mathrm{P}+z)| \\ &= \sum_{z \in \mathbb{Z}^n} |(\mathrm{X}-z) \cap \mathrm{P}| \\ &= |\bigsqcup_{z \in \mathbb{Z}^n} (\mathrm{X}-z) \cap \mathrm{P}| \end{aligned}$$

d'où

$$|\mathrm{X}| \leqslant |\mathrm{P}| = 1$$

ce qui est absurde.

$\square$

Revenons-en au théorème. Soit un entier $\mathrm{N} \geqslant 1$. Considérons l'ensemble

$$\mathrm{C_N} = \{x \in \mathbb{R}^n \mid |x_i| < \lambda_i + \frac{1}{\mathrm{N}} \text{ et } |x_j| < \lambda_j \text{ pour } j \neq i\}$$

Alors $\mathrm{C_N}$ est un pavé, de mesure de Lebesgue $2\left(\lambda_i + \frac{1}{\mathrm{N}}\right)\prod_{k \neq i}^n 2\lambda_k$. On en déduit la minoration :

$$|\frac{1}{2}\mathrm{A}^{-1}\mathrm{C_N}| = 2^{-n}.(\det \mathrm{A})^{-1}|\mathrm{C_N}| = (\det \mathrm{A})^{-1}\left(\prod_{k=1}^n \lambda_k\right).\frac{\lambda_i + \frac{1}{\mathrm{N}}}{\lambda_i}$$

Comme $\prod_{k=1}^n \lambda_k \geqslant \det \mathrm{A}$, il vient

$$|\frac{1}{2}\mathrm{A}^{-1}\mathrm{C_N}| \geq \frac{\lambda_i + \frac{1}{\mathrm{N}}}{\lambda_i} > 1$$

En appliquant le lemme de Blichfeldt, on obtient l'existence de $x^{(\mathrm{N})}$ et $y^{(\mathrm{N})}$ dans $\mathrm{A}^{-1}\mathrm{C_N}$ distincts tels que

$$\frac{1}{2}(x^{(\mathrm{N})} - y^{(\mathrm{N})}) \in \mathbb{Z}^n.$$

La suite $\frac{1}{2}(x^{(\mathrm{N})} - y^{(\mathrm{N})})$ étant à valeurs dans l'ensemble

$$\mathrm{A}^{-1}\mathrm{C}_1 \cap (\mathbb{Z}^n - \{0\})$$

qui est discret et borné, donc fini, on peut supposer qu'elle est stationnaire quitte à en considérer une sous-suite.

Soit z sa limite. Alors $z \in \mathbb{Z}^n - \{0\}$, et $\mathrm{A}z$ est dans l'intersection $\bigcap_{\mathrm{N} \in \mathbb{N}} \mathrm{C_N}$, c'est-à-dire que z vérifie :

$$\left\{\begin{array}{l} z \in \mathbb{Z}^n - \{0\} \\ |(\mathrm{A}z)_i| \leqslant \lambda_i \\ |(\mathrm{A}z)_j| < \lambda_j \text{ pour } j \neq i. \end{array}\right.$$

Le théorème de Minkowski est ainsi démontré.

□

Pour x et y dans $\mathbb{R}^n$, nous poserons

$$x.y = \sum_{i=1}^{n} x_i y_i \text{ et } \|x\| = \max_{1 \leqslant i \leqslant n} |x_i|.$$

La première conséquence simple du théorème de Minkowski est la suivante, qui généralise le théorème 1 :

Théorème 2.3 .

Pour tout $y \in \mathbb{R}^n$, il existe une infinité de $q \in \mathbb{Z} - \{0\}$ tels que

$$\|qy + p\|^n.|q| < 1$$

pour un certain $p \in \mathbb{Z}^n$.

On a alors, pour un entier q qui vérifie la propriété précédente, une famille d'approximations des coordonnées de y par des rationnels de dénominateur q. En revanche, on perd un peu sur la précision de ces approximation par rapport à la situation dans $\mathbb{R}$. En effet, si y_i désigne la i^{eme} composante de y et p_i celle de p, on a ici :

$$|qy_i + p_i| \leq \|qy + p\|$$

donc
$$|qy_i + p_i|^n.|q| < 1$$

soit
$$|y_i + \frac{p_i}{q}| < \frac{1}{|q|^{1+\frac{1}{n}}}$$

Démonstration Fixons un entier $\mathrm{N} \geqslant 2$, et notons

$${}^t y = (y_1, ..., y_n)$$

Soit la matrice :

$$\mathrm{A} = \begin{pmatrix} 1 & 0 \\ y & \mathcal{I}_n \end{pmatrix}$$

A est de déterminant 1. On pose $\lambda_1 = \mathrm{N}^n$ et pour $2 \leq i \leq n+1$, $\lambda_i = \dfrac{1}{\mathrm{N}}$.

Alors par construction $\prod_{i=1}^{n+1} \lambda_i = 1 \geq \det \mathrm{A}$, et nous sommes donc dans les conditions d'applications du théorème de Minkovski, qui nous donne un vecteur x de $\mathbb{Z}^{n+1}$ tel que $|(\mathrm{A}x)_1| \leq \mathrm{N}^n$ et pour tout $2 \leq i \leq n+1$, $|(\mathrm{A}x)_i| < \dfrac{1}{\mathrm{N}}$.

Si l'on appelle $q^{(\mathrm{N})}$ la première composante de x et $p^{(\mathrm{N})}$ le vecteur colonne de longueur n composé des coordonnées suivantes, on a :

$$(\mathrm{A}x)_1 = q^{(\mathrm{N})} \text{ et pour tout } i, (\mathrm{A}x)_{i+1} = qy_i + p_i^{(\mathrm{N})}$$

On a donc construit $q^{(\mathrm{N})} \in \mathbb{Z} - \{0\}$ et $p^{(\mathrm{N})} \in \mathbb{Z}^n$ tels que $\|q^{(\mathrm{N})}y + p^{(\mathrm{N})}\| < \frac{1}{\mathrm{N}}$ et $|q^{(\mathrm{N})}| \leqslant \mathrm{N}^n$.

Le résultat suit en remarquant que, soit y est à coordonnées rationnelles et le résultat du théorème 3 est évident, soit nécessairement :

$$|q^{(\mathrm{N})}| \overset{\mathrm{N}\to\infty}{\longrightarrow} \infty$$

□

3 Des approximations plus ou moins bonnes

3.1 Définitions

Ces résultats connus, il semble assez naturel de se demander s'il existe des vecteurs ayant des "bonnes" ou des "mauvaises" propriétés d'approximation. Précisons cette idée avec les notions de vecteur très bien approchable (TBA) et de vecteur très mal approchable (TMA) introduites en partie par Schmidt ([S]).

Définition - Un vecteur $y \in \mathbb{R}^n$ est dit TMA si et seulement s'il existe $c > 0$ tel que

$$\|qy + p\|^n.|q| \geqslant c$$

pour tout $p \in \mathbb{Z}^n$ et tout $q \in \mathbb{Z} - \{0\}$.

- Un vecteur $y \in \mathbb{R}^n$ est dit TBA si et seulement s'il existe $\epsilon > 0$ pour lequel il y a une infinité de $q \in \mathbb{Z}$ tels que

$$\|qy + p\|^n.|q| \leqslant |q|^{-\epsilon} \tag{2}$$

pour un certain $p \in \mathbb{Z}^n$.

Lorsqu'on cherche à étudier les ensembles de vecteurs TBA ou TMA, ces définitions exprimées sous cette forme-là, s'avèrent parfois étrangement moins maniables que des définitions équivalentes données par le "transference principle" de Khintchine. Ce principe, qui est d'ailleurs une conséquence du théorème de Minkowski, nous dit qu'étant donné $\mathrm{A} \in \mathrm{M}(m, n, \mathbb{R})$, si l'on sait qu'existent des solutions entières $x \in \mathbb{Z}^n$ non nulles "petites"(par rapport à la majoration obtenue par le théorème de Minkowski) au problème

$$\|\mathrm{A}x\| \leqslant \mathrm{C}$$

alors il existe une quantité D dépendant de C et $\|x\|$, et il existe $y \in \mathbb{Z}^n$ non nul, avec $\|y\| \leqslant \mathrm{D}$, tels que ${}^t\mathrm{A}\, y$ soit "petit" au sens précédent (${}^t\mathrm{A}$ désigne la transposée de A). Il est possible d'en déduire des définitions équivalentes pour les vecteurs TBA et TMA.

Définitions équivalentes

- Un vecteur y est TMA si et seulement s'il existe $c > 0$ tel que

$$|q.y + p|.\|q\|^n \geqslant c$$

pour tout $p \in \mathbb{Z}$ et tout $q \in \mathbb{Z}^n - \{0\}$.

- Un vecteur y est TBA si et seulement s'il existe $\epsilon > 0$ tel que pour une infinité de $q \in \mathbb{Z}^n$

$$|q.y + p|.\|q\|^n \leqslant \|q\|^{-n\epsilon} \tag{3}$$

pour un certain $p \in \mathbb{Z}$.

3.2 Une propriété d'approximation en moyenne

Munis des définitions du précédent paragraphe, nous pouvons nous demander quelle est la "taille" de l'ensemble des vecteurs TBA ou TMA. Nous présentons ici un premier résultat. (L'espace $\mathbb{R}^n$ est muni de la mesure de Lebesgue.)

Proposition 3.1 *Presque tout vecteur de $\mathbb{R}^n$ n'est pas TBA.*

Démonstration Il suffit bien entendu de montrer que l'ensemble des vecteurs TBA de $[0,1]^n$ est de mesure nulle et même de montrer pour tout $\epsilon > 0$ que l'ensemble E_ϵ des vecteurs de $[0,1]^n$ tels qu'existe une infinité de $q \in \mathbb{Z} - \{0\}$ avec

$$\|qy + p\|^n.|q| \leqslant |q|^{-\epsilon}$$

pour un certain $p \in \mathbb{Z}^n$ est de mesure nulle. Fixons donc $\epsilon > 0$ et pour $q \in \mathbb{N} - \{0\}$ posons

$$\mathrm{E}_{q,\epsilon} = \{y \in [0,1]^n | \exists p \in \mathbb{Z}^n, \|qy + p\|^n.|q| \leqslant |q|^{-\epsilon}\}$$

de sorte qu'un vecteur est dans E_ϵ si et seulement s'il appartient à une infinité de $\mathrm{E}_{q,\epsilon}$. Or l'ensemble $\mathrm{E}_{q,\epsilon}$ est inclus dans la réunion des boules de centre $(\frac{p_1}{q}, ..., \frac{p_n}{q})$ et de rayon $|q|^{-(1+\frac{1+\epsilon}{n})}$ avec $[0,1]^n$ où $(p_1, ..., p_n)$ parcourt l'ensemble des n-uplets d'entiers à coordonnées comprises entre 0 et q. Ainsi, nous obtenons l'inégalité

$$|\mathrm{E}_{q,\epsilon}| \leqslant (q+1)^n.q^{-n-1-\epsilon} \leqslant 2^n q^{-(1+\epsilon)}$$

de sorte que, grâce au critère de Riemann,

$$\sum_{q>0} |\mathrm{E}_{q,\epsilon}| < \infty.$$

Rappelons le lemme de Borel-Cantelli.

Lemme 3.2 (Borel-Cantelli) *Soit $(\Omega, \mathcal{F}, \mu)$ un espace mesuré et $\{\mathrm{A}_n\}_{n\in\mathbb{N}}$ des ensembles mesurables de Ω. Supposons*

$$\sum_{n\in\mathbb{N}} \mu(\mathrm{A}_n) < \infty.$$

Alors, $\mu(dx)$-presque sûrement, x n'appartient qu'à un nombre fini de A_n.

Le lemme de Borel-Cantelli et la remarque précédente nous permettent alors d'affirmer que l'on a $|\mathrm{E}_\epsilon| = 0$.

$\square$

Références

[C] Cassels, J.W.S. (1957). An introduction to diophantine approximation, Cambridge University Press.

[HW] Hardy, G.H., Wright, E.M.. An introduction to the theory of numbers, Oxford.

[S] Schmidt, W.M. (1966). On badly approximable numbers and certain games, Trans. Amer. Math. Soc. (123), 178-199.