Explique-moi... l'approximation diophantienne

Notes

Elio Joseph

20 février 2019

Références :

- Introduction à la théorie des nombres, Hardy & Wright,
- Escapades arithmétiques, Frédéric Laroche,
- On height of algebraic subspaces and diophantine approximation, W. M. Schmidt.

Nous allons ici parler d'approximation diophantienne, domaine qui cherche à obtenir des résultats *qualitatifs* sur l'approximation de réels par des rationnels.
Que signifie *qualitatif* ? Assez naturellement, on peut dire que $22/7$ est une "meilleure" approximation de π que $157/50$, alors que ces deux approximations donnent le même nombre de décimales correctes (3).
L'exposé qui suit est peu formel et se veut plus comme une promenade parmi les grands résultats de cette théorie, l'idée étant d'avoir un aperçu de ce qu'est l'approximation diophantienne. L'exposé se compose de trois grandes parties :

1. L'exposant
2. La constante
3. Généralisation à des sous-espaces vectoriels de $\mathbb{R}^n$

En approximation diophantienne, on veut approcher un réel ξ par un rationnel p/q. Autrement dit, on veut

$$\left|\xi - \frac{p}{q}\right| \quad \text{petit.}$$

Mais comme $\mathbb{Q}$ est dense dans $\mathbb{R}$, le problème n'est pas intéressant en l'état. On lie donc la *complexité* du rationnel à la *qualité* de l'approximation. Ainsi, plus on

s'autorisera des fractions *compliquées* (*i.e.* avec un grand dénominateur), plus on imposera à l'approximation d'être *précise*.
Plus précisément, on cherche p/q, α et K tels que

$$\left|\xi - \frac{p}{q}\right| < \frac{K}{q^\alpha}. \tag{1}$$

$\rightarrow$ on voit bien ici que plus le dénominateur est grand, plus l'approximation se doit d'être précise.

1 L'exposant

Dans cette section, on s'intéresse plus précisément au cas de l'exposant α dans (1). On a un premier résultat :

Théorème 1 (Dirichlet)

$$\exists K, \quad \forall \xi \in \mathbb{R}, \quad \exists p/q \in \mathbb{Q}, \quad \left|\xi - \frac{p}{q}\right| < \frac{K}{q^2}.$$

Preuve.
Principe de Dirichlet. □

Remarque 2 Si $\xi \notin \mathbb{Q}$, il existe une infinité de $p/q \in \mathbb{Q}$ vérifiant l'inégalité du théorème 1.

On formalise l'étude de cet exposant, en introduisant une notion fondamentale en approximation diophantienne :

Définition 3 On définit la *mesure d'irrationalité* $\mu(\xi)$ de ξ comme la borne supérieure des $\mu > 0$ tels que

$$\exists\ \infty\text{té } p/q \in \mathbb{Q}, \quad \left|\xi - \frac{p}{q}\right| < \frac{1}{q^\mu}.$$

$\rightarrow$ on a vu que si $\xi \notin \mathbb{Q}$, $\mu(\xi) \geqslant 2$.
On connaît des résultats sur la mesure d'irrationalité, donnons en quelques-uns.

Théorème 4 (Liouville, 1844) Si ξ est algébrique de degré n, alors $\mu(\xi) \leqslant n$.

Preuve.
Formule de Taylor. □

Ce théorème est très intéressant, car de celui-ci découle le corollaire suivant :

$$\mu(\xi) = \infty \implies \xi \text{ est transcendant.}$$

Ce résultat est très puissant. En effet, il est facile de montrer l'*existence* des nombres transcendants (un simple argument de cardinalité fait l'affaire), mais il est déjà plus difficile d'en *exhiber* un. C'est ainsi que le premier nombre prouvé transcendant ne fut donné qu'en 1844, par Liouville :

Proposition 5 Le nombre

$$\xi = \sum_{n \geqslant 1} 10^{-n!}$$

est transcendant.

Le premier nombre a avoir été prouvé transcendant sans avoir été explicitement *construit* pour, est $e \approx 2.718\cdots$, preuve donnée par Hermite en 1873.
La constante π fut quant à elle prouvée transcendante en 1882 par Lindemann.
Ces résultats qui peuvent sembler anecdotiques ne sont pas anodins. Par exemple, la transcendance de π a permis de résoudre le problème de la quadrature du cercle (construire un carré de la même aire qu'un disque à la règle et au compas), problème qui était ouvert depuis trois millénaires !

Remarque 6 Ce que nous venons de voir est philosophiquement intéressant : ce sont les nombres les plus "simples" (les nombres algébriques) qui vont être le moins bien approchés.

Donnons maintenant quelques résultats supplémentaires sur la mesure d'irrationalité.

Théorème 7 Pour presque tout $\xi \in \mathbb{R}$, $\mu(\xi) = 2$.

Enfin un théorème qui a valu la médaille Fields à Roth en 1958 :

Théorème 8 (Roth, 1955) Si x est algébrique, alors $\mu(x) = 2$.

$\rightarrow$ bien évidemment la réciproque est fausse, ce qui se déduit du théorème 7 ; plus explicitement, on a par exemple $\mu(e) = 2$.
Pour finir sur la mesure d'irrationalité, mentionnons celle de π, qui est encore inconnue. On sait que $\mu(\pi) \leqslant 8.0160$ (Hata, 1992), et même mieux : $\mu(\pi) \leqslant 7.6063$ (Salikhov, 2008). La conjecture la plus partagée est que $\mu(\pi) = 2$, mais ce résultat semble encore loin.

2 La constante

Nous allons ici discuter de la constante K dans l'inégalité (1).
On a le célèbre

Théorème 9 (Hurwitz, 1891)

$$\forall \xi \in \mathbb{R} \setminus \mathbb{Q}, \quad \exists \infty \text{té } p/q \in \mathbb{Q}, \quad \left|\xi - \frac{p}{q}\right| < \frac{1}{q^2\sqrt{5}}.$$

De plus, la constante $\sqrt{5}$ est optimale. Elle est notamment réalisée par $\varphi = \frac{1+\sqrt{5}}{2}$ le nombre d'or.

$\rightarrow$ autrement dit : φ est le réel le moins bien approché par des rationnels.

But : améliorer cette constante.

Et si on retirait φ, est-ce qu'il y aurait du progrès ?

Définition 10 On dit que $x, y \in \mathbb{R}$ sont *équivalents* s'il existe $a, b, c, d \in \mathbb{Z}$ tels que

$$\begin{cases} ad - bc = 1 \\ y = \dfrac{ax + b}{cx + d}. \end{cases}$$

$\rightarrow$ peut-être plus concrètement, x est équivalent à y si, et seulement si, les développements en fractions continues de x et y sont égaux à partir d'un certain rang.
Un nombre équivalent au nombre d'or est dit *noble*.
On peut alors répondre à la question que nous nous étions posée. Si dans le théorème d'Hurwitz on interdit à ξ d'être un nombre noble, alors la constante $\sqrt{5}$ peut être améliorée et remplacée par $\sqrt{8}$.
Peut-on continuer ? Oui !
Si on interdit de plus à ξ d'être équivalent à $\sqrt{2}$, alors $\sqrt{8}$ peut être améliorée...
On obtient ainsi une suite :

$$\sqrt{5},\ \sqrt{8},\ \frac{\sqrt{221}}{5},\ \frac{\sqrt{1517}}{13},\ \frac{\sqrt{7565}}{29},\ \frac{\sqrt{2600}}{17},\ \frac{\sqrt{71\,285}}{89}, \dots$$

de nombres L_n, appelés *nombres de Lagrange*.
Etudions un peu cette suite de nombres.

Proposition 11

$$L_n \xrightarrow[n\to\infty]{} 3.$$

Ces nombres sont liés de façon assez surprenante à une équation diophantienne.
On note m_n et on appelle *nombres de Markov* les entiers strictement positifs appartenant à une solution de l'équation diophantienne

$$x^2 + y^2 + z^2 = 3xyz.$$

Les premiers étant

$$1,\ 2,\ 5,\ 13,\ 29,\ 34,\ 89, \dots.$$

On a alors le surprenant

Théorème 12

$$L_n = \sqrt{9 - \frac{4}{m_n^2}}.$$

Donnons un peu plus de résultats sur les constantes dans le théorème d'Hurwitz.
On note $L(\xi)$ la meilleure constante pour $\xi \in \mathbb{R}$ dans le théorème d'Hurwitz ($L(\varphi) = \sqrt{5}$, $L(\sqrt{2}) = \sqrt{8}$,...).

Définition 13 On appelle *spectre de Lagrange* l'ensemble

$$\{L(\xi),\ \xi \in \mathbb{R}\}.$$

On peut alors assez bien décrire le spectre de Lagrange :

Théorème 14 (Freiman,1975) Le spectre de Lagrange est continu à partir de sa dernière discontinuité, la constante de Freiman :

$$\frac{2\,221\,564\,096 + 283\,748\sqrt{462}}{491\,993\,569} \approx 4.5278.$$

De plus, il est discret entre $\sqrt{5}$ et 3, et la transition entre la partie discrète et la partie continue a une structure fractale.

3 Généralisation à des sous-espaces vectoriels de $\mathbb{R}^n$

L'idée est de W. M. Schmidt (1967).

But : Par analogie, on peut "approcher" un sous-espace A^d (de dimension d) de $\mathbb{R}^n$, par un sous-espace B^e (de dimension e) *rationnel* et "pas trop compliqué".

Par analogie, on suppose

$$\forall B^e \text{ rationnel}, \quad A^d \cap B^e = \{0\}.$$

On cherche comme avant les $\mu > 0$ tels que

$$\exists \infty \text{té } B^e \text{ rationnels}, \quad \psi_j(A^d, B^e) \leqslant \frac{K}{H(B^e)^\mu}. \tag{2}$$

Où :

⋆ ψ_j mesure la *proximité* entre A^d et B^e,

⋆ $H(\cdot)$ mesure la *complexité* de B^e.

On définit par analogie à la mesure d'irrationalité une quantité :

$$\mu_n(e, j, d) = \sup\{\mu \text{ vérifiant (2)} \quad \forall A^d\}.$$

Ce que l'on sait sur $\mu_n(e, j, d)$:

Théorème 15 (Schmidt, 1967) On a

$$\frac{d(n-j)}{j(n-d)(n-e)} \leqslant \mu_n(e, j, d) \leqslant \frac{1}{j}\left\lceil \frac{e(n-e)+1}{n+1-d-e} \right\rceil.$$

De plus, le problème est totalement résolu si $\min(d, e) = 1$.

La détermination de $\mu_n(e, j, d)$ est donc encore un problème largement ouvert. Sa valeur exacte n'est connue que quand on cherche à approcher des droites, ou à approcher par des droites (c'est le cas $\min(d, e) = 1$).

L'objectif de la détermination de cette quantité serait de généraliser le critère d'indépendance linéaire de Nesterenko, qui permet sous certaines hypothèses de minorer la dimension du $\mathbb{Q}$-espace vectoriel engendré par une famille de réels. Ce critère permet d'obtenir des résultats du style :

Théorème 16 (Zudilin, 2001) Parmi $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$, l'un au moins est irrationnel.

$\rightarrow$ pour l'instant, seul $\zeta(3)$ est prouvé irrationnel (Apéry, 1978) parmi les $\zeta(2k+1)$.