Université Laval, Québec

Séminaire de Théorie des Nombres

Mercredi 5 juillet 2006, à 10 h 30

Local 2830 Pavillon Alexandre-Vachon

Approximation rationnelle de nombres réels

Michel Waldschmidt

Institut de Mathématiques de Jussieu + CIMPA

http ://www.math.jussieu.fr/∼miw/

Approximation rationnelle de nombres réels

Michel Waldschmidt

http ://www.math.jussieu.fr/∼miw/

Résumé

La théorie des nombres transcendants est née en 1844, quand Liouville a exhibé les premiers exemples : il s'appuie pour cela sur une propriété qu'il découvre concernant l'approximation rationnelle de nombres réels algébriques par des nombres rationnels.

Un siècle et demi plus tard cette propriété se révèle essentielle pour comprendre le comportement de certains systèmes dynamiques.

Le théorème d'approximation de Liouville a connu des raffinements, améliorations et généralisations, qui culminent avec le théorème du sous-espace de W.M. Schmidt.

Un des outils privilégiés pour étudier l'approximation d'un nombre réel par des nombres rationnels est donné par le développement en fraction continue. Nous présentons cette théorie en donnant quelques exemples.

L'approximation par des nombres rationnels du logarithme ou de l'exponentielle d'un nombre rationnel est utile dans des travaux d'informatique théorique visant à établir la validité de calculs faits par ordinateur. Nous donnons un exemple d'énoncé récent qui est utile dans cette direction.

Le théorème d'approximation diophantienne de Liouville

Théorème (Liouville, 1844).
Soit α un nombre réel algébrique. Il existe une constante $\kappa > 0$ telle que, pour tout nombre rationnel p/q distinct de α avec $q \geq 2$, on ait

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{q^\kappa}\cdot$$

Existence et construction de nombres transcendants

Corollaire.
Soit ξ *un nombre réel. Supposons que pour tout* $\kappa > 0$ *il existe un nombre rationnel* p/q *avec* $q \geq 2$ *tel que*

$$0 < \left| \xi - \frac{p}{q} \right| < \frac{1}{q^\kappa} \cdot$$

Alors ξ *est transcendant.*

Nombres de Liouville

- Définition : un *nombre de Liouville* est un nombre réel tel que pour tout $\kappa > 0$ il existe un nombre rationnel p/q avec $q \geq 2$ satisfaisant
$$0 < \left| \xi - \frac{p}{q} \right| < \frac{1}{q^\kappa} \cdot$$
- Un nombre réel irrationnel qui n'est pas de Liouville est appelé *diophantien* (par les spécialistes de systèmes dynamiques). On dit aussi qu'il *vérifie une condition diophantienne* : il existe $\kappa \geq 2$ et $C > 0$ tels que
$$\left| \xi - \frac{p}{q} \right| \geq \frac{C}{q^\kappa} \cdot$$
- J.C. Yoccoz : *Conjugaison différentiable des difféomorphismes du cercle dont le nombre de rotation vérifie une condition diophantienne.* Ann. scient. Éc. Norm. Sup. 4$^{\text{è}}$ série, t. **17** (1984), 333-359.

Difféomorphismes du cercle : nombre de rotation

- Un difféomorphisme du cercle $\mathbf{T}^1 = \mathbf{R}/\mathbf{Z}$ peut être vu comme une application différentiable $f : \mathbf{R} \to \mathbf{R}$ telle que $f - \mathrm{Id}_{\mathbf{R}}$ soit $\mathbf{Z}$–périodique.
- Le nombre de rotation de f est
$$\varrho(f) = \lim_{n\to\infty} \frac{1}{n}(f^n(x) - x)$$
où f^n est le n-ième itéré de f.
- $\varrho(f)$ est rationnel si et seulement si f admet une orbite périodique.
- f est topologiquement conjugué à la rotation d'angle p/q si et seulement si f^q est la rotation d'angle p
- $\varrho(f) = p/q$ si et seulement si $f^q - \mathrm{Id}_{\mathbf{R}} - p$ a un zéro sur $\mathbf{R}$.
- H. Poincaré (1885) : Mécanique céleste, systèmes dynamiques.

Difféomorphismes du cercle : historique

- A. Denjoy (1932) : construction de difféomorphismes de classe C^1 de nombre de rotation α qui ne soient pas conjugués à la rotation R_α.
- V.I. Arnold (1961) : construction de difféomorphismes analytiques de nombre de rotation irrationnel pour lesquels la conjugaison n'est pas absolument continue : la perte de régularité est due aux *petits dénominateurs.*
- M. Hermann (1978) : Proc. ICM Helsinki + 1979 Publ. IHÉS : lien avec la condition diophantienne.
- **J-C. Yoccoz (1983) :** *Si le nombre de rotation d'un difféomorphisme du cercle f de classe C^∞ satisfait une condition diophantienne, f est conjugué à une rotation. Le résultat est optimal pour la conjugaison C^∞.*

Raffinements du théorème de Liouville

- Liouville (1844) : si α est un nombre algébrique de degré d, alors pour tout nombre rationnel $p/q \neq \alpha$, on a
$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^d}.$$
- Thue (1909) : remplace $c(\alpha)/q^d$ par $c(\alpha,\epsilon)/q^\kappa$ où $\kappa = (d/2) + 1 + \epsilon$.
- Siegel (1921) : $\kappa = 2\sqrt{d} + \epsilon$.
- Gel'fond et Dyson (1947) : $\kappa = \sqrt{2d} + \epsilon$.
- Roth (1954) : $\kappa = 2 + \epsilon$.
- Schmidt (1970) : théorème du sous-espace.

Le théorème du sous-espace de W.M. Schmidt (énoncé très simplifié)

Pour $\mathbf{x} = (x_0, \dots, x_{m-1}) \in \mathbf{Z}^m$, on pose $|\mathbf{x}| = \max\{|x_0|, \dots, |x_{m-1}|\}$.

Théorème (W.M. Schmidt – 1970).

Soit $m \geq 2$. Soit $L_0, \dots, L_{m-1}$ un ensemble de m formes linéaires indépendantes en m variables à coefficients complexes algébriques. Soit $\epsilon > 0$. Alors l'ensemble

$$\{\mathbf{x} = (x_0, \dots, x_{m-1}) \in \mathbf{Z}^m \; ; \; |L_0(\mathbf{x}) \cdots L_{m-1}(\mathbf{x})| \leq |\mathbf{x}|^{-\epsilon}\}$$

est contenu dans la réunion d'un nombre fini de sous-espaces vectoriels propres de $\mathbf{Q}^m$.

Une conséquence du théorème du sous-espace de Schmidt

Corollaire (Thue-Siegel-Roth).
Pour tout nombre algébrique α, pour tout $\epsilon > 0$, l'ensemble des $p/q \in \mathbf{Q}$ satisfaisant $|\alpha - p/q| \leq q^{-2-\epsilon}$ est fini.

- Démonstration.
  Prendre dans le théorème du sous-espace de Schmidt $m = 2$, $L_0(x_0, x_1) = x_0$, $L_1(x_0, x_1) = \alpha x_0 - x_1$.
  La condition
  $$|L_0(\mathbf{x})L_1(\mathbf{x})| \leq |\mathbf{x}|^{-\epsilon}$$
  correspond à
  $$q|q\alpha - p| \leq q^{-\epsilon}.$$
  □

Le théorème du sous-espace de W.M. Schmidt (énoncé simplifié)

Théorème (W.M. Schmidt – 1970).
Soient $m \geq 2$ un entier positif, S un ensemble fini de places de $\mathbf{Q}$ contenant la place à l'infini. Pour chaque $v \in S$ soit $L_{0,v}, \ldots, L_{m-1,v}$ un système de m formes linéaires indépendantes en m variables à coefficients algébriques dans le complété de $\mathbf{Q}$ en v. Soit $\epsilon > 0$. Alors l'ensemble des $\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbf{Z}^m$ pour lesquels
$$\prod_{v \in S} |L_{0,v}(\mathbf{x}) \cdots L_{m-1,v}(\mathbf{x})|_v \leq |\mathbf{x}|^{-\epsilon}$$
est contenu dans la réunion d'un nombre fini de sous-espaces vectoriels propres de $\mathbf{Q}^m$.

Théorème de Ridout

Corollaire (Ridout).
Pour tout nombre algébrique α, pour tout $\epsilon > 0$, l'ensemble des $p/q \in \mathbf{Q}$ avec $q = 2^k$ et $|\alpha - p/q| < q^{-1-\epsilon}$ est fini.

- Démonstration.
  Dans le théorème du sous-espace de Schmidt, prendre $m = 2$, $S = \{\infty,\ 2\}$,
  $L_{0,\infty}(x_0, x_1) = L_{0,2}(x_0, x_1) = x_0$,
  $L_{1,\infty}(x_0, x_1) = \alpha x_0 - x_1, \qquad L_{1,2}(x_0, x_1) = x_1.$
  Pour $(x_0, x_1) = (q, p)$ avec $q = 2^k$, on a
  $|L_{0,\infty}(x_0, x_1)|_\infty = q, \qquad |L_{1,\infty}(x_0, x_1)|_\infty = |q\alpha - p|,$
  $|L_{0,2}(x_0, x_1)|_2 = q^{-1}, \qquad |L_{1,2}(x_0, x_1)|_2 = |p|_2 \leq 1.$
  □

Fractions continues

Soit $x \in \mathbf{R}$.

- On écrit
  $$x = [x] + \{x\} \quad \text{avec } [x] \in \mathbf{Z} \text{ et } 0 \leq \{x\} < 1.$$
- Si x n'est pas entier, alors $\{x\} \neq 0$ et on pose $x_1 = 1/\{x\}$, de sorte que
  $$x = [x] + \frac{1}{x_1} \quad \text{avec } [x] \in \mathbf{Z} \text{ et } x_1 > 1.$$
- Si x_1 n'est pas entier, on pose $x_2 = 1/\{x_1\}$:
  $$x = [x] + \cfrac{1}{[x_1] + \cfrac{1}{x_2}} \quad \text{avec } x_2 > 1.$$

Fractions continues (suite)

On pose $a_0 = [x]$ et $a_i = [x_i]$ pour $i \geq 1$.

- En poursuivant on obtient ainsi l'écriture

$$x = [x] + \cfrac{1}{[x_1] + \cfrac{1}{[x_2] + \cfrac{1}{\ddots}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

  avec un développement fini si et seulement si x est rationnel.
- On écrit ce développement

$$x = [a_0\ ;\ a_1,\ a_2,\ a_3 \ldots]$$

- Remarque : si $a_k \geq 2$, alors $[a_0\ ;\ a_1,\ a_2,\ a_3, \ldots, a_k] = [a_0\ ;\ a_1,\ a_2,\ a_3, \ldots, a_k - 1, 1]$.

Fractions continues (exemples)

- Les développements

  $[1], \quad [1; 1], \quad [1; 1, 1], \quad [1; 1, 1, 1], \quad [1; 1, 1, 1, 1], \quad [1; 1, 1, 1, 1, 1] \ldots$

  sont ceux des quotients

$$\begin{array}{cccccccc} F_2/F_1 & F_3/F_2 & F_4/F_3 & F_5/F_4 & F_6/F_5 & F_7/F_6 & \\ \| & \| & \| & \| & \| & \| & \ldots \\ 1 & 2 & 3/2 & 5/3 & 8/5 & 13/8 & \end{array}$$

  des nombres de Fibonacci consécutifs

  $(F_n)_{n \geq 0} = 0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ \ldots$

- Le développement $[1; 1, 1, 1, 1 \ldots]$ est celui du nombre d'or

$$\Phi = \frac{1 + \sqrt{5}}{2} = \lim_{n \to \infty} \frac{F_{n+1}}{F_n} = 1,6180339887499\ldots$$

  qui vérifie

$$\Phi = 1 + \frac{1}{\Phi}.$$

Fractions continues (autres exemples)

- La fraction continue de $\sqrt{2} = 1,4142135623731\dots$ est

$$\sqrt{2} = [1;\ 2,\ 2,\ 2,\ 2,\ 2,\ \dots]$$

car

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2}+1}.$$

- La fraction continue de $e = 2,718281828459\dots$ est

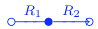
$$e = [2;\ 1,\ 2,\ 1,\ 1,\ 4,\ 1,\ 1,\ 6,\ 1,\ 1,\ 8,\ 1,\ 1,\ 10,\ 1\dots]$$

- Celle de $\pi = 3,1415926535898\dots$ s'écrit

$$\pi = [3;\ 7,\ 15,\ 1,\ 292,\ 1,\ 1,\ 1,\ 2,\ 1,\ 3,\ 1,\ 14,\ 2,\ 1,\ 1\dots]$$

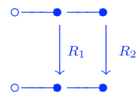
Résistance d'un réseau électrique

- La résistance du réseau en série



est la somme $R_1 + R_2$.

- La résistance R du réseau en parallèle

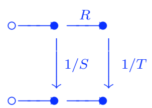


est donnée par

$$\frac{1}{R} = \frac{1}{R_1} + \frac{1}{R_2}.$$

Réseaux électriques et fractions continues

La résistance U du circuit



est donnée par

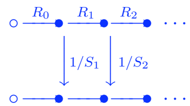
$$\frac{1}{U} = \frac{1}{S + \frac{1}{R + \frac{1}{T}}}$$

Réseaux électriques, fractions continues et décomposition d'un carré en carrés

- La résistance d'un réseau en échelle est donnée par un développement en fractions continues :

$$[R_0; S_1, R_1, S_2, R_2 \ldots]$$

pour le circuit

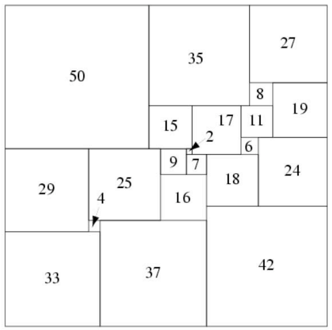


R_i : résistances en séries

$1/S_j$: résistances en parallèle

- Par exemple les réseaux avec $R_i = S_j = 1$ auront pour résistance les quotients des nombres de Fibonacci consécutifs.
- Les réseaux électriques et les fractions continues ont permis de donner la première solution au problème de décomposer un carré entier en carrés entiers distincts.

Solution de la quadrature du carré



21-*square perfect square*

There is a unique simple perfect square of order 21 (the lowest possible order), discovered in 1978 by A. J. W. Duijvestijn (Bouwkamp and Duijvestijn 1992). It is composed of 21 squares with total side length 112, and is illustrated above.

Suites de Farey

- La suite de Farey d'indice n est la suite finie croissante des fractions a/b avec $0 \leq a < b \leq n$ et $(a, b) = 1$.
- Par exemple la suite de Farey d'indice 6 est

$$\frac{0}{1}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}.$$

- Exemple d'application : si on veut approcher π par un nombre rationnel dont le dénominateur est ≤ 6, la fraction continue $\pi = [3;\ 7,\ 15,\ 1,\ 292\ldots]$ ne donne que l'approximation 3, alors que l'élément $1/6$ de la suite de Farey d'indice 6 le plus proche de $\pi - 3$ fournit l'approximation $3 + (1/6) = 19/6 = 3,166\ldots$ qui est meilleure.

Approximation diophantienne

Une des applications les plus classiques de la théorie des fractions continues et des suites de Farey concerne l'approximation diophantienne de nombres réels par des nombres rationnels.
Soit ξ un nombre réel.

- Le principe des tiroirs de Dirichlet permet de montrer que pour tout nombre réel $Q > 1$ existe $p/q \in \mathbf{Q}$ avec $1 \leq q < Q$ vérifiant

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{qQ}.$$

- Il en résulte que si ξ est irrationnel, alors il existe une infinité de $p/q \in \mathbf{Q}$ vérifiant

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Fractions continues, suites de Farey et approximation diophantienne

- La théorie des fractions continues aussi bien que celle des suites de Farey permet de démontrer (théorème de A. Hurwitz, 1891) que si ξ est un nombre réel irrationnel, alors il existe une infinité de $p/q \in \mathbf{Q}$ vérifiant

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

- Le nombre d'or Φ montre que le théorème de Hurwitz est optimal.

Nombres quadratiques

- Le développement en fraction continue d'un nombre réel irrationnel x est ultimement périodique si et seulement si le nombre x est quadratique.
- Un nombre réel de la forme $\sqrt{d}$ avec $d > 0$ sans facteur carré a un développement en fraction continue purement périodique de la forme

$$[a_0;\ a_1,\ a_2,\ \dots,\ a_k,\ a_1,\ a_2,\ \dots,\ a_k,\ a_1,\ a_2,\ \dots,]$$

que l'on écrit pour simplifier

$$[a_0;\ \overline{a_1,\ a_2,\ \dots,\ a_k}].$$

- Ainsi $\sqrt{2} = [2;\ \overline{2}]$. La même notation s'applique au nombre d'or $\Phi = \frac{1+\sqrt{5}}{2} = [1;\ \overline{1}]$.

Développement en fraction continue de $\sqrt{d}$

- Dans le développement en fraction continue

$$\sqrt{d} = [a_0;\ \overline{a_1,\ a_2,\ \dots,\ a_k}]$$

de la racine carrée de l'entier $d > 0$ (sans facteur carré) on a $a_0 = [\sqrt{d}]$ et $a_k = 2a_0$. De plus

$$a_1,\ a_2,\ \dots,\ a_{k-1}$$

est un *palindrome* : $a_i = a_{k-i}$ $(1 \leq i \leq k-1)$.

- La longueur k de ce développement est impaire (resp. paire) si et seulement si l'unité fondamentale du corps $\mathbf{Q}(\sqrt{d})$ a pour norme -1 (resp. $+1$).

Lien avec l'équation de $x^2 - dy^2 = \pm 1$

Soit d un entier positif sans facteur carré. Considérons l'équation diophantienne

$$(1) \qquad x^2 - dy^2 = \pm 1$$

dont les inconnues x, y sont dans $\mathbf{Z}$.

- Si (x, y) est une solution, alors $(x - \sqrt{d}y)(x + \sqrt{d}y) = 1$, donc x/y est une approximation rationnelle de $\sqrt{d}$ d'autant meilleure que x est grand.
- Les *meilleures* approximations rationnelles d'un nombre réel x sont données en tronquant son développement en fraction continue.

Fractions continues et approximation diophantienne

- Pour
$$x = [a_0;\ a_1,\ a_2, \dots, a_k, \dots]$$
la suite de fractions
$$p_k/q_k = [a_0;\ a_1,\ a_2, \dots, a_k] \qquad (k = 1, 2, \dots)$$
fournit des approximations rationnelles de x qui sont optimales quand on compare la qualité de l'approximation et la taille du dénominateur.
- Ceci explique qu'une stratégie pour résoudre l'équation (1) soit fondée sur une utilisation du développement en fraction continue de $\sqrt{d}$.

Résoudre l'équation $x^2 - dy^2 = \pm 1$ grâce aux fractions continues

- Soit d un entier ≥ 2 sans facteur carré. Écrivons

$$\sqrt{d} = [a_0;\ \overline{a_1,\ a_2,\ \ldots,\ a_k}].$$

- Quand k est pair, la plus petite solution de l'équation $x^2 - dy^2 = 1$ est donnée par

$$\frac{x}{y} = [a_0;\ a_1,\ a_2,\ \ldots,\ a_{k-1}]$$

  et il n'y a pas de solution à l'équation $x^2 - dy^2 = -1$.

Résoudre l'équation $x^2 - dy^2 = \pm 1$ grâce aux fractions continues (suite)

- Quand k est impair, la plus petite solution de l'équation $x^2 - dy^2 = -1$ est donnée par

$$\frac{x}{y} = [a_0;\ a_1,\ a_2,\ \ldots,\ a_{k-1}]$$

  et la plus petite solution de l'équation $x^2 - dy^2 = 1$ est donnée par

$$\frac{x}{y} = [a_0;\ a_1,\ a_2,\ \ldots,\ a_{k-1},\ a_k,\ a_1,\ a_2,\ \ldots,\ a_{k-1}].$$

Problème de Brahmagupta (628)

- Brahmasphutasiddhanta : résoudre en entier l'équation

$$x^2 - 92y^2 = 1$$

- Si (x, y) est une solution, alors $(x - \sqrt{92}y)(x + \sqrt{92}y) = 1$, donc x/y est une bonne approximation rationnelle de $\sqrt{92} = 9,591663046625\ldots$.
- Le développement en fractions continues de $\sqrt{92}$ est

$$\sqrt{92} = [9; \overline{1,\ 1,\ 2,\ 4,\ 2,\ 1,\ 1,\ 18}]$$

référence : `http ://wims.unice.fr/wims/`

- La théorie prédit qu'une solution est obtenue à partir du nombre rationnel

$$[9;\ 1,\ 1,\ 2,\ 4,\ 2,\ 1,\ 1] = \frac{1151}{120}.$$

- En effet $1151^2 - 92 \cdot 120^2 = 1\,324\,801 - 1\,324\,800 = 1$.

Bhaskara II (12è siècle)

- *Lilavati*
- (*Bijaganita*, 1150) $x^2 - 61y^2 = 1$
- $x = 1\,766\,319\,049$, $y = 226\,153\,980$.
  Méthode cyclique (Chakravala) de Brahmagupta.
- $\sqrt{61} = [7; \overline{1,\ 4,\ 3,\ 1,\ 2,\ 2,\ 1,\ 3,\ 4,\ 1,\ 14}]$
  $[7; 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, 4, 3, 1, 2, 2, 1, 3, 5] = \dfrac{1\,766\,319\,049}{226\,153\,980}$
- $[7; 1, 4, 3, 1, 2, 2, 1, 3, 5] = \dfrac{29\ 718}{3\ 805}$
- $29\ 718^2 = 883\ 159\ 524, \qquad 61 \cdot 3805^2 = 883\ 159\ 525$
  solution de $x^2 - 61y^2 = -1$.

Narayana (14è siècle)

- Narayana cows (Tom Johnson)
- $x^2 - 103y^2 = 1$
  $x = 227\,528$, $y = 22\,419$.
  $227\,528^2 - 103 \cdot 22\,419^2 = 51\,768\,990\,784 - 51\,768\,990\,783 = 1.$
- $\sqrt{103} = [10; \overline{6,\ 1,\ 2,\ 1,\ 1,\ 9,\ 1,\ 1,\ 2,\ 1,\ 6,\ 20}]$
- $[10; 6,\ 1,\ 2,\ 1,\ 1,\ 9,\ 1,\ 1,\ 2,\ 1,\ 6] = \dfrac{227\,528}{22\,419}$

Variétés riemanniennes de courbure négative

- L'étude d'équations diophantiennes "à la Pell-Fermat" permet de construire des variétés riemanniennes de courbure négative : les variétés arithmétiques.
- Les variétés arithmétiques représentent essentiellement les seules variétés de courbure négative que l'on sache construire en dimension > 3. Il est donc naturel de se demander quels types de variétés topologiques peuvent être ainsi obtenus ?
- Nicolas Bergeron (Paris VI) : "Sur la topologie de certains espaces provenant de constructions arithmétiques"