Congrès International sur l'Algèbre,
la Théorie des Nombres et leurs applications
Oujda, 11-14 Mai 2006

http ://www.iro.umontreal.ca/∼azizi/CIATNA2006/

Approximation diophantienne et applications

Michel Waldschmidt

Institut de Mathématiques de Jussieu + CIMPA
http ://www.math.jussieu.fr/∼miw/

12 Mai 2006

Approximation diophantienne et applications
Michel Waldschmidt

Congrès International sur l'Algèbre,
la Théorie des Nombres et leurs applications
Oujda, 11-14 Mai 2006
http ://www.iro.umontreal.ca/∼azizi/CIATNA2006/

1. Approximation Diophantienne dans la vie courante
2. Nombres de Liouville et systèmes dynamiques
3. Problème de Mahler et informatique théorique
4. Conjecture de Schanuel et problème des trois corps

Résumé

De nombreux phénomènes de la vie courante font intervenir des approximations diophantiennes. Dès qu'un phénomène est périodique, il conduit à des questions arithmétiques sur le tore. Les fractions continues constituent l'outil le mieux adapté à l'étude de l'approximation d'un nombre réel par des nombres rationnels.

Il faut d'autres arguments pour étudier l'approximation par des nombres algébriques. Les premiers sont apparus dans le mémoire fondateur de Liouville en 1844, où il établit une propriété d'approximation rationnelle des nombres algébriques qui lui permet de construire les premiers exemples de nombres transcendants.

La théorie connaît actuellement d'intéressants développements, il reste cependant beaucoup de questions ouvertes. Nous ferons un tour du sujet sans prétendre être exhaustif. Nous mettrons l'accent sur les applications.

Approximation Diophantienne dans la vie courante

- Mécanique céleste :
  Périodes des orbites de Saturne (Divisions de Cassini)
  Stabilité du système solaire
  Systèmes planétaires ; questions de résonance en astronomie.
- Petits diviseurs et systèmes dynamiques (H. Poincaré)
- Engrenages
- Calendriers : années bissextiles
- Phénomènes presque périodiques. Quasi-cristaux
- Acoustique des salles de concert
- Transmission de données. Radars

Number Theory in Science and communication

M.R. Schroeder.
Number theory in science and communication :
with applications in cryptography, physics, digital information, computing and self similarity
Springer series in information sciences **7** 1986.
4th ed. (2006) 367 p.

Number Theory in Science and communication par M.R. Schroeder

Number Theory in Science and Communication is a well-known introduction for non-mathematicians to this fascinating and useful branch of applied mathematics . It stresses intuitive understanding rather than abstract theory and highlights important concepts such as continued fractions, the golden ratio, quadratic residues and Chinese remainders, trapdoor functions, pseudoprimes and primitive elements. **Their applications to problems in the real world are one of the main themes of the book.** This revised fourth edition is augmented by recent advances in primes in progressions, twin primes, prime triplets, prime quadruplets and quintruplets, factoring with elliptic curves, quantum factoring, Golomb rulers and "baroque" integers.

Acoustique des salles de concert, d'après M.R. Schroeder

Eigenfrequenzstatistik und Angerungsstatistik in Räumen,
Acustica **4** (1954), 45–68.

- Entiers qui sont sommes de trois cubes.
- Transformée de Fourier discrète.
- Résidus quadratiques, racines primitives.
- Mesure des réponses acoustiques dans des salles de concert pleines.

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 $x_2 = 1/\{x_1\}$:

$$x = [x] + \frac{1}{[x_1] + \dfrac{1}{x_2}} \quad \text{avec } x_2 > 1.$$

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

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

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

Fractions continues (exemples)

- Les développements

$$[1],\quad [2],\quad [1;2],\quad [1;1,2],\quad [1;1,1,2],\quad [1;1,1,1,2]\dots$$

  sont ceux des quotients

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

  des nombres de Fibonacci consécutifs

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

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

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

  qui vérifie

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

Fractions continues (autres exemples)

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

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

car

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

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

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

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

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

Approximation rationnelle de $\log_2 3$

- Le logarithme en base 2 de 3 :

$$\log_2 3 = (\log 3)/\log 2 = 1,58496250072\ldots$$

est la solution x de l'équation $2^x = 3$

- Les approximations rationnelles a/b de $\log_2 3$ correspondent à des puissances de 2 proches de puissances de 3 :

$$\log_2 3 \simeq a/b, \qquad 2^a \simeq 3^b.$$

- Le développement en fraction continue

$$\log_2 3 = [1; 1, 1, 2, 2, 3, 1, 5, \ldots]$$

fournit des valeurs numériques qui jouent un rôle important dans les gammes musicales.

Approximations de $\log_2 3 = 1,58496250072\ldots$

- $$[1;1,1] = [1;2] = \frac{3}{2} = 1,5$$
  $$3^2 = 9, \quad 2^3 = 8, \quad (3/2)^2 = 2,25 \simeq 2$$
  deux quintes font un peu plus qu'un octave.
- $$[1;1,1,2] = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}} = \frac{8}{5} = 1,6$$
  $$3^5 = 243, \quad 2^8 = 256, \quad (3/2)^5 = 7,59375 \simeq 2^3 = 8$$
  cinq quintes font presque trois octaves.

Approximation de $\log_2 3 = [1;1,1,2,2,3,1,5,\ldots]$

- $$[1;1,1,2,2] = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2}}}} = \frac{19}{12}$$
  $$3^{12} = 531\,441, \quad 2^{19} = 524\,288,$$
  $$(3/2)^{12} = 129,463\cdots \simeq 2^7 = 128.$$
  Douze quintes font à peine plus que sept octaves.
- Comma de Pythagore :
  $$\frac{3^{12}}{2^{19}} = 1,01364\ldots$$

Mathématiques et musique

G. Assayag, H.G. Feichtinger, J.F. Rodrigues (Ed.),
Mathematics and musics,
A Diderot Mathematical Forum.
Springer 2002.

Approximation de $\log_2 5 = 2,32192809488\ldots$

$$\log_2 5 = (\log 5)/\log 2 = [2; 3, 9, 2, 2, 4, 6\ldots]$$
$$[2; 3] = 7/3 = 2,333\ldots, \quad 5^3 = 125, \quad 2^7 = 128$$

- Trois tierces majeures couvrent presque une octave :
$$(5/4)^3 = 1,953125 \simeq 2.$$
- Autre conséquence : $2^{10} = 1024 \simeq 10^3$
- *Informatique :* kilo octets
- *Acoustique :* multiplier l'intensité par 10, c'est ajouter 10 décibels.
  - Multiplier l'intensité par k, c'est ajouter d décibels avec
  $$10^d = k^{10}$$
  - Comme $10^3 \simeq 2^{10}$, doubler l'intensité, c'est (à peu près) ajouter 3 décibels.

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) 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.

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)

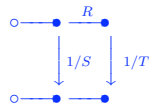
- Narayana cows (Tom Johnson)
- $x^2 - 103y^2 = 1$
  $x = 227\,528$, $y = 22\,419$.
  $227\,528^2 - 103 \cdot 22\,419^2 = 51\,768\,990\,784 - 51\,768\,990\,783 = 1$.
- $\sqrt{103} = [10; \overline{6,\ 1,\ 2,\ 1,\ 1,\ 9,\ 1,\ 1,\ 2,\ 1,\ 6,\ 20}]$
- $[10; 6,\ 1,\ 2,\ 1,\ 1,\ 9,\ 1,\ 1,\ 2,\ 1,\ 6] = \dfrac{227\,528}{22\,419}$

Référence sur l'histoire de la théorie des nombres

André Weil
Number theory. :
An approach through history. From Hammurapi to Legendre.
Birkhäuser Boston, Inc., Boston, Mass., (1984) 375 pp.
MR 85c :01004

Réseaux électriques et fractions continues

La résistance U du circuit



est donnée par

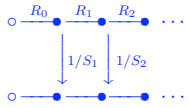
$$\frac{1}{U} = \frac{1}{S + \dfrac{1}{R + \dfrac{1}{T}}}$$

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 :

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

pour le circuit

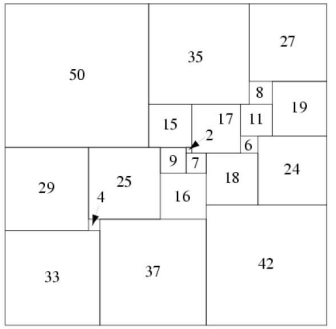


R_i : résistances en séries

$1/S_j$: résistances en parallèle

- Par exemple les réseaux avec $R_i = S_j = 1$ auront pour résistance les nombres de Fibonacci.
- 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.

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

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

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

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

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

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

- 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

$$\left| \xi - \frac{p}{q} \right| \geq \frac{C}{q^\kappa}.$$

- J.C. Yoccoz : *Conjugaison différentiable des difféomorphismes du cercle dont le nombre de rotation vérifie une condition diophantienne.* Ann. scient. Éc. Norm. Sup. 4$^{\text{e}}$ 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

$$\varrho(f) = \lim_{n \to \infty} \frac{1}{n} \big(f^n(x) - x \big)$$

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

Théorème (W.M. Schmidt – 1970).

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

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

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 $m = 2$, $S = \{\infty, 2\}$,

$L_{0,\infty}(x_0, x_1) = L_{0,2}(x_0, x_1) = x_0$,
$L_{1,\infty}(x_0, x_1) = \alpha x_0 - x_1$, $\quad L_{1,2}(x_0, x_1) = x_1$.

Pour $(x_0, x_1) = (q, p)$ avec $q = 2^k$, on a

$|L_{0,\infty}(x_0, x_1)|_\infty = q$, $\quad |L_{1,\infty}(x_0, x_1)|_\infty = |q\alpha - p|$,
$|L_{0,2}(x_0, x_1)|_2 = q^{-1}$, $\quad |L_{1,2}(x_0, x_1)|_2 = |p|_2 \leq 1$.

□

Transcendance de $\log \alpha$ et e^β

Théorème (Hermite–Lindemann).

- *Si α est un nombre algébrique non nul et $\log \alpha$ une détermination non nulle de son logarithme, alors $\log \alpha$ est transcendant.*
- *Si β est un nombre algébrique non nul, alors e^β est transcendant.*
- *Conséquence : Si a et b sont des entiers positifs, alors $\log a \neq b$.*

Problème de Mahler (1967)

Problème.
Si a et b sont des entiers positifs, a-t-on

$$|b - \log a| > e^{-cb}$$

avec une constante absolue c ?

- **Heuristique :** on peut même espérer mieux :

$$|b - \log a| > b^{-c}.$$

Réponses partielles au problème de Mahler (1967)

- K. Mahler (1953, 1967), M. Mignotte (1974), F. Wielonsky (1997) :

$$|b - \log a| > b^{-20b}$$

- Méthode : les démonstrations reprennent les arguments de Hermite (1873) reposant sur les approximants de Padé, avec des raffinements et des développements ultérieurs.

Extension du problème de Mahler aux nombres rationnels

- Travail en commun avec Yu.V. Nesterenko (1996) : minoration de $|b - \log a|$ pour a et b nombres rationnels.
- Démonstration : utilise les arguments de la méthode de Gel'fond–Schneider–Baker avec les déterminants d'interpolation de M. Laurent.
- Raffinement par S. Khemira (2005)

Énoncés Diophantiens

Théorème (S. Khemira – 2005).
Pour a et b dans $\mathbf{Q}$ avec $b \neq 0$, on a

$$|b - \log a| \geq \exp\{-1,3 \cdot 10^5 (\log A)(\log B)\}$$

où $A = \max\{H(a),\ A_0\}$, $B = \max\{H(b),\ 2\}$.

- La hauteur d'un nombre rationnel p/q est définie par $H(p/q) = \max\{|p|,\ q)$.
- Le nombre A_0 peut être explicité.

Travail en commun avec Nesterenko, 1995

Théorème.
Soient α et β deux nombres algébriques non nuls et $\log \alpha$ une détermination non nulle du logarithme de α. On pose $\mathbf{K} = \mathbf{Q}(\alpha, \beta)$ et $D = [\mathbf{K} : \mathbf{Q}]$. Soient A et E deux nombres réels positifs satisfaisant $E \geq e$ et

$$\log A \geq \max\big(h(\alpha)\,,\ D^{-1} \log E\,,\ D^{-1}|\beta|E\big).$$

Alors

$$|\beta - \log \alpha| \geq \exp\Big(-105500 \cdot D^2 \log A$$
$$\big(h(\beta) + \log_+ \log A + \log D + \log E\big)\big(D \log D + \log E\big) \cdot (\log E)^{-2}\Big)$$

Erreurs d'arrondis en calculs numériques

M.R. Schroeder : l'inverse de la matrice

$$\begin{bmatrix} 1 & 1 \\ 1 & 1+\epsilon \end{bmatrix}$$

est

$$\begin{bmatrix} 1+\frac{1}{\epsilon} & -\frac{1}{\epsilon} \\ -\frac{1}{\epsilon} & \frac{1}{\epsilon} \end{bmatrix}$$

Calculer sans erreurs d'arrondis avec les opérations élémentaires

Stratégie pour ne pas introduire d'erreurs d'arrondis dans la division : utilisation des fractions de Farey.

Un ordinateur ne connaît qu'un ensemble fini de nombres, tous rationnels, disons a/b avec $(a,b)=1$ et $-N \leq a \leq N$, $1 \leq b \leq N$. On choisit un entier $m \geq N^2+1$. On remplace chaque fraction a/b avec $(b,m)=1$ par l'entier modulo m qui est congru à ab^{-1} modulo m, où b^{-1} est l'inverse de b modulo m. On abolit ainsi la division !

Problèmes d'arrondis en informatique pour les fonctions élémentaires

Applications en informatique théorique :
Muller, J-M. ; Tisserand, A.
Towards exact rounding of the elementary functions. Alefeld, Goetz (ed.) et al.,
Scientific computing and validated numerics.
Proceedings of the international symposium on scientific computing, computer arithmetic and validated numerics SCAN-95, Wuppertal, Germany, September 26-29, 1995.
Berlin : Akademie Verlag. Math. Res. 90, 59-71 (1996).

Applications en informatique théorique

Computer Arithmetic
—
Projet Arénaire
http ://www.ens-lyon.fr/LIP/Arenaire/

Validated scientific computing
Arithmetic, reliability, accuracy, and speed
Improvement of the available arithmetic on computers, processors, dedicated or embedded chips
Getting more accurate results or getting them more quickly
Power consumption, reliability of numerical software.

La conjecture de Schanuel

Conjecture (Schanuel).

Soient $x_1, \dots, x_n$ des nombres complexes linéairement indépendants sur $\mathbf{Q}$. Alors parmi les $2n$ nombres

$$x_1, \dots, x_n, e^{x_1}, \dots, e^{x_n},$$

il y en a au moins n qui sont algébriquement indépendants.

- **Hypothèse :** si $a_1 x_1 + \cdots + a_n x_n = 0$ avec des a_i rationnels, alors $a_1 = \cdots = a_n = 0$.
- **Conclusion :** il existe $y_1, \dots, y_n$ dans l'ensemble $\{x_1, \dots, x_n, e^{x_1}, \dots, e^{x_n}\}$ tels que, pour tout polynôme non nul P en n variables à coefficients rationnels, on ait $P(y_1, \dots, y_n) \neq 0$.

La conjecture de Schanuel (suite)

- **Autre forme de la conclusion :** *le degré de transcendance sur $\mathbf{Q}$ du corps*

$$\mathbf{Q}(x_1, \dots, x_n, e^{x_1}, \dots, e^{x_n})$$

est $\geq n$.

- *Cas particuliers connus* :
  - **Théorème de Lindemann-Weierstrass** sur l'indépendance algébrique de $e^{\beta_1}, \dots, e^{\beta_n}$
  - Indépendance linéaire de logarithmes sur le corps des nombres algébriques (A. Baker).
- *Conséquences de la conjecture de Schanuel* : indépendance algébrique de logarithmes de nombres algébriques, non annulation de régulateurs.

Conséquence de la conjecture de Schanuel

Conjecture (sur l'indépendance algébrique de logarithmes de nombres algébriques).

Soient $\lambda_1, \dots, \lambda_n$ des nombres complexes linéairement indépendants sur $\mathbf{Q}$. On suppose $e^{\lambda_i} \in \overline{\mathbf{Q}}$ pour $1 \le i \le n$. Alors les nombres $\lambda_1, \dots, \lambda_n$ sont algébriquement indépendants.

- Posons $\alpha_i = e^{\lambda_i} \quad (1 \le i \le n)$. Si on écrit (abusivement) $\lambda_i = \log \alpha_i$, l'énoncé dit que des logarithmes $\log \alpha_1, \dots, \log \alpha_n$ sont algébriquement indépendants dès qu'ils sont linéairement indépendants.
- La conjecture de Schanuel contient bien d'autres conséquences, comme l'indépendance algébrique de familles de nombres telles que

$$e,\ \pi,\ \log 2,\ \log \pi,\ e^{\pi},\ 2^{\sqrt{2}},\ e^{e},\ \pi^{e},\ \pi^{\pi},\ \log\log \pi,\ \pi^{\pi^{\pi}} \dots$$

Conjecture sur l'indépendance algébrique de logarithmes de nombres algébriques, d'après D. Roy

Conjecture.

Soit

$$\mathcal{L} = \left\{ \log \alpha\ ;\ \alpha \in \overline{\mathbf{Q}}^{\times} \right\} = \exp^{-1}(\overline{\mathbf{Q}}^{\times}) \subset \mathbf{C}$$

le $\mathbf{Q}$-espace vectoriel des logarithmes de nombres algébriques et soit V une sous-variété algébrique de $\mathbf{C}^n$ définie sur le corps des nombres algébriques. Alors

$$V \cap \mathcal{L}^n = \bigcup_{W \subset V} W \cap \mathcal{L}^n,$$

où W décrit l'ensemble des sous-espaces vectoriels de $\mathbf{C}^n$ définis sur $\mathbf{Q}$ et contenus dans V.

Le problème des trois corps et la conjecture de Schanuel

Lien avec le problème des trois corps :
Ax, James
Transcendence and differential algebraic geometry.
Actes Congr. internat. Math. 1970, **1**, 483-485 (1971).
Zbl 0232.14008

Conjecture de Schanuel, d'après J. Ax

Soit $\mathbf{G}$ le groupe algébrique $\mathbf{G}_a^n \times \mathbf{G}_m^n$ produit de n copies du groupe additif $\mathbf{G}_a$ par n copies du groupe multiplicatif $\mathbf{G}_m$.
On désigne par A le graphe de l'exponentielle

$$\exp_{\mathbf{G}} : \mathbf{C}^n \to (\mathbf{C}^\times)^n$$

c'est un sous-groupe analytique de $\mathbf{G}(\mathbf{C}) = \mathbf{C}^n \times (\mathbf{C}^\times)^n$.
Soit V un sous-ensemble algébrique de $\mathbf{G}$ défini sur $\mathbf{Q}$ de dimension inférieure à n. Soit $p \in V \cap A$.

Conjecture (de Schanuel vue par Ax).
Il existe un sous-groupe algébrique propre L de $\mathbf{C}^n$ tel que $L \times \exp(L)$ soit un sous-groupe algébrique de G contenant p.

Équations différentielles algébriques

- Le graphe A de l'exponentielle $\exp_{\mathbf{G}} : \mathbf{C}^n \to (\mathbf{C}^\times)^n$ peut être décrit comme la variété intégrale passant par l'origine du système complètement intégrable de 1-formes $dy_i - dz_i/z_i$, $(1 \leq i \leq n)$.
- La conjecture de Schanuel porte sur les propriétés algébriques de l'intersection de variétés analytiques définies par des équations différentielles algébriques.
- D'autres questions peuvent s'énoncer de façon similaire. Plusieurs conjectures de S. Lang en géométrie diophantienne concernent l'intersection de variétés analytiques définies par des équations différentielles algébriques.
  Les réponses (quelquefois seulement partielles) utilisent des arguments d'approximation diophantienne, principalement le théorème du sous-espace de W.M. Schmidt.

Conjecture de Mordell-Manin-Mumford-Lang en géométrie diophantienne

L'énoncé suivant conjecturé par S. Lang est maintenant un théorème grâce aux travaux de Faltings complétés par Hindry, Vojta et McQuillan (*références :* texte de Marc Hindry dans la Gazette des Mathématiciens de la SMF en mémoire de Lang).

Théorème.
Soient A une variété semi-abélienne définie sur $\mathbf{C}$, Γ un sous-groupe de $A(\mathbf{C})$ de rang fini et V une sous-variété fermée de A. Alors il existe un ensemble fini de $\gamma_i \in \Gamma$ et de sous-groupes algébriques B_i tels que $\gamma_i + B_i \subset V$ et

$$V(\mathbf{C}) \cap \Gamma = \bigcup_{i=1}^{s} \gamma_i + (B_i(\mathbf{C}) \cap \Gamma).$$

Conjecture de Mordell-Manin-Mumford-Lang : développements

La conjecture de Mordell-Manin-Mumford-Lang continue à être la source de travaux intéressants comme par exemple la théorie différentielle algébrique des jets (Buium) elle-même inspirée des travaux pionniers de Manin, l'apparition surprenante de la théorie des modèles dans ces questions (Hrushovski) ou des simplications (dans le cas où Γ est le groupe de torsion (Pink-Roessler), voir aussi les travaux de Raynaud et Rémond.

À propos du théorème de Siegel sur l'indépendance algébrique de fonctions de Bessel

J. Ax : *ce serait bien d'avoir un critère satisfaisant qui détermine la dimension du corps engendré par les solutions d'un système linéaire d'équations différentielles sur le corps des fractions rationnelles.*

Théorème de Brun sur les intégrales algébriques dans le problème des trois corps

- S sous-variété algébrique réelle (*espace des états*) de dimension 19
  W champ de vecteurs algébrique sur S dont la valeur en une fonction est son crochet de Poisson avec le Hamiltonien.
- Une *intégrale algébrique* est une fonction F sur S qui est constante sur les orbites de W. Un exemple est l'énergie.
- On connaît 9 autres intégrales algébriques indépendantes, provenant de la linéarité du mouvement du centre de gravité et de la constance des moments linéaires et angulaires.
- Brun (1887) : *toutes les intégrales algébriques sont fonctions de ces dix intégrales classiques.*

Problème des trois corps, d'après J. Ax

- Soit T un revêtement fini du complexifié de S tel qu'il existe un champ de vecteurs uniforme Y sur T correspondant à W.
- Théorème de Brun : *il existe un morphisme universel $\varphi : T \to T_0$ de variétés algébriques qui est constant sur les orbites de Y, avec T_0 de dimension 10.*
- Si $\psi : T \to T'$ est un morphisme, alors ou bien il existe $\tau : T_0 \to T'$ tel que $\psi = \tau \circ \varphi$ (auquel cas $\dim \tau(T_0) \leq 10$), ou bien il existe une fibre V de ψ et une orbite A de Y tels que $\emptyset \neq V \cap A \neq A$.
- Cet énoncé révèle qu'un aspect du problème considéré est l'analogue algébrique de la théorie des systèmes dynamiques.

Autres applications de la théorie des nombres

- Hua Loo Keng, Wang Yuan
  Application of number theory to numerical analysis
  Springer Verlag 1981
  Répartition modulo 1, discrépance, intégration numérique, interpolation, solutions approchées d'équations intégrales et différentielles.

- Cryptographie : messages secrets, transmissions sécurisées, certification de signatures...

- Codes correcteurs d'erreurs

Approximation diophantienne et applications

Michel Waldschmidt

Congrès International sur l'Algèbre,
la Théorie des Nombres et leurs applications
Oujda, 11-14 Mai 2006

http ://www.iro.umontreal.ca/∼azizi/CIATNA2006/

1. Approximation Diophantienne dans la vie courante
2. Nombres de Liouville et systèmes dynamiques
3. Problème de Mahler et informatique théorique
4. Conjecture de Schanuel et problème des trois corps