Nancy, colloquium de l'Institut Élie Cartan
25 mars 2008

La méthode de Charles Hermite en théorie des nombres transcendants

Michel Waldschmidt

http://www.math.jussieu.fr/∼miw/

Résumé

Les méthodes de transcendance ont toutes leur fondement dans les travaux précurseurs de Charles Hermite en 1873, quand il a démontré la transcendance du nombre e. On connaissait alors depuis une trentaine d'années des exemples de nombres transcendants, grâce aux travaux de Joseph Liouville, mais ceux qu'il avait exhibés étaient artificiels, spécialement construits pour satisfaire des contraintes d'approximation diophantienne très strictes. La démonstration par Georg Cantor de l'existence de *beaucoup* de nombres transcendants était nettement moins explicite. Hermite est le premier à démontrer la transcendance d'une constante fondamentale de l'analyse. Sa démonstration allait être exploitée en 1881 par Ferdinand Lindemann, qui donnait ainsi la réponse définitive au problème de la quadrature du cercle.

Résumé (suite et fin)

Nous présentons quelques unes des idées du mémoire d'Hermite et nous montrons comment elles ont évolué depuis, permettant de résoudre un certain nombre de problèmes de transcendance – mais les questions ouvertes sont encore les plus nombreuses.

Crédit photos :
http ://www-history.mcs.st-andrews.ac.uk/history/

Introduction aux Nombres Transcendants

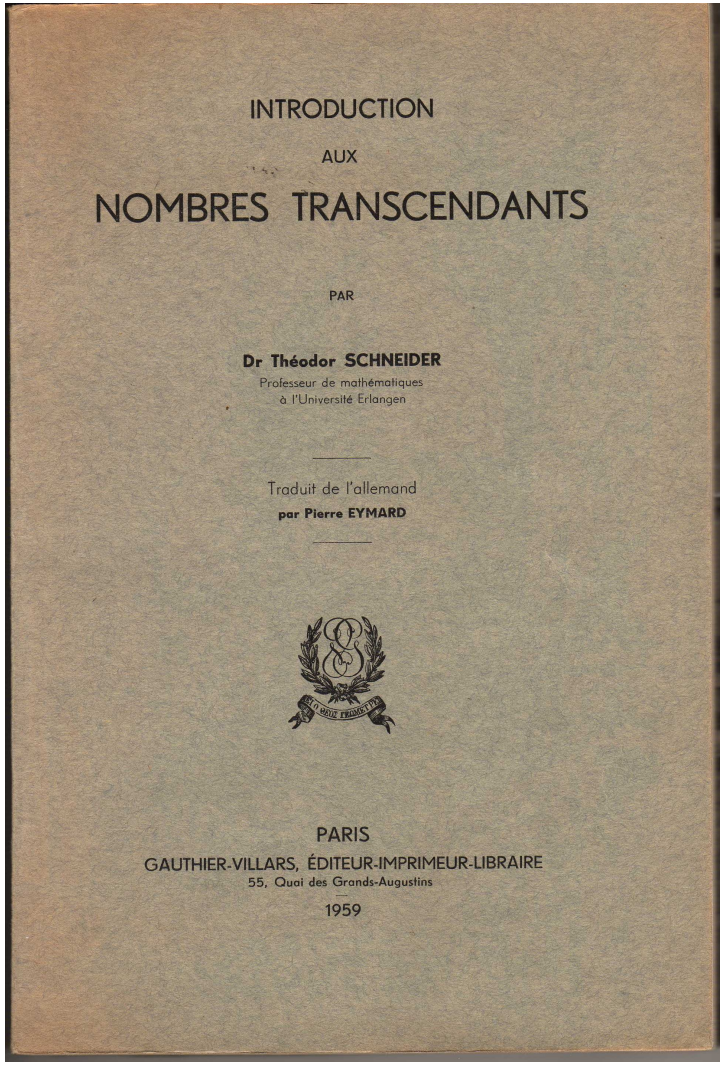
Theodor Schneider

Einführung in die Transzendenten Zahlen

Springer, 1957.

Traduction française par Pierre Eymard

Gauthier-Villars, 1959


INTRODUCTION

AUX

NOMBRES TRANSCENDANTS

PAR

Dr Théodor SCHNEIDER

Professeur de mathématiques
à l'Université Erlangen

Traduit de l'allemand
par Pierre EYMARD

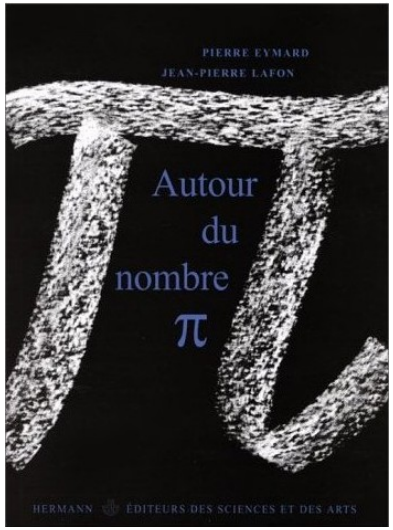
PARIS

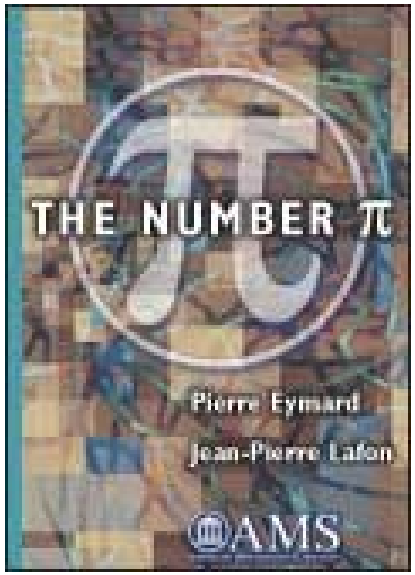
GAUTHIER-VILLARS, ÉDITEUR-IMPRIMEUR-LIBRAIRE

55, Quai des Grands-Augustins

1959

Autour du nombre pi





Pierre Eymard, Jean-Pierre Lafon

Autour du nombre π
(Hermann 2000)

The Number π
(AMS 2004)

Transcendance du nombre e (1873)

Charles Hermite
Sur la fonction exponentielle,
C. R. Acad. Sci. Paris,
77 (1873), 18–24 ; 74–79 ;
226–233 ; 285–293 ;
Œuvres, Gauthier Villars
(1905), III, 150–181.

Hermite, Ch.

Sur la fonction exponentielle. (French)

[J] C. R. LXXVII. 18-24, 74-79, 226-233, 285-293. (1873)

Eine Aufgabe, welche als eine Verallgemeinerung des Problems der Annäherung durch algebraische Kettenbrüche angesehen werden kann, ist folgende : ,,Die n rationalen Brüche

$$\frac{\Phi_1(x)}{\Phi(x)}, \frac{\Phi_2(x)}{\Phi(x)}, \cdots \frac{\Phi_n(x)}{\Phi(x)}$$

als Näherungswerthe der n Functionen $\varphi_1(x), \varphi_2(x), \cdots \varphi_n(x)$ so zu bestimmen, dass die Reihenentwickelungen nach steigenden Potenzen von x bis zur Potenz x^M übereinstimmen“. Es werde vorausgesetzt, dass sich die Functionen $\varphi(x)$ in Reihen von der Form $\alpha + \beta x + \gamma x^2 + \cdots$ entwickeln lassen, und man mache

$$\Phi(x) = Ax^m + Bx^{m-1} + \cdots + Kx + L.$$

Dann kann man im Allgemeinen über die Coefficienten $A, B, \cdots L$ so verfügen, dass in den Producten $\varphi_i(x)\Phi(x)$ die Glieder mit

$$x^M, x^{M-1}, \cdots x^{M-\mu_i+1},$$

wo μ_i irgend eine ganze Zahl ist, verschwinden. So bildet man μ_i homogene Gleichungen ersten Grades und hat

$$\varphi_i(x)\Phi(x) = \Phi_i(x) + \varepsilon_1 x^{M+1} + \varepsilon_2 x^{M+2} + \cdots ,$$

wo $\varepsilon_1, \varepsilon_2, \cdots$ Constanten, $\Phi_i(x)$ ein ganzes Polynom vom Grade $M - \mu_i$. Da aber hieraus folgt, dass

$$\varphi_i(x) = \frac{\Phi_i(x)}{\Phi(x)} + \frac{\varepsilon_1 x^{M+1} + \varepsilon_2 x^{M+2} + \cdots}{\Phi(x)},$$

so sieht man, dass die Reihenentwickelungen des rationalen Bruches und der Function in der That dieselben sein werden bis zu x^M , und da die Gesammtzahl der gemachten Bedingungen gleich $\mu_1 + \mu_2 + \cdots + \mu_n$ ist, so genügt es, die einzige Bedingung

$$\mu_1 + \mu_2 + \cdots + \mu_n = m$$

hinzuzufügen, wo die ganzzahligen μ_i bis dahin ganz willkürlich geblieben sind. Diese Betrachtung ist der Ausgangspunkt, den der Herr Verfasser für die in seiner Arbeit entwickelte Theorie der Exponentialfunction genommen hat, indem er nämlich das Obige anwendet auf die Grössen

$$\varphi_1(x) = e^{ax}, \varphi_2(x) = e^{bx}, \cdots \varphi_n(x) = e^{hx}.$$

État de la question en 1873

- Irrationalité de e : L. Euler (1737), J.H. Lambert (1761)
- Irrationalité de e^r pour r rationnel non nul, de $\log s$ pour s rationnel > 0, de π : J.H.Lambert (1767)
- Démonstration de l'irrationalité de e par J. Fourier (1815), de e^2 par J. Liouville (1840) : e^2 *n'est pas quadratique*
- Existence de nombres transcendants par J. Liouville (1844, 1852) et G. Cantor (1874 et 1891)
- Problème de la quadrature du cercle

Hermite et π

Lettre de Ch. Hermite à C.A. Borchardt

Je ne hasarderai point à la recherche d'une démonstration de la transcendance du nombre π. Que d'autres tentent l'entreprise ; mais croyez m'en, mon cher ami, il ne laissera pas que de leur en coûter quelques efforts.

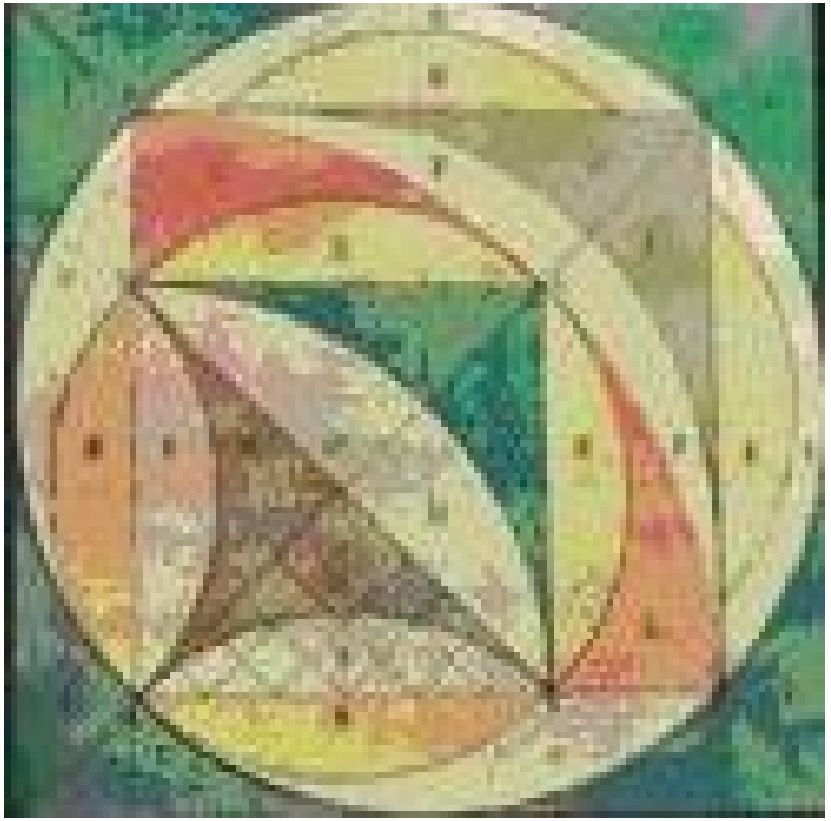
Hermite, 1849

Tout ce que je puis, c'est de refaire ce qu'a déjà fait Lambert, seulement d'une autre manière.

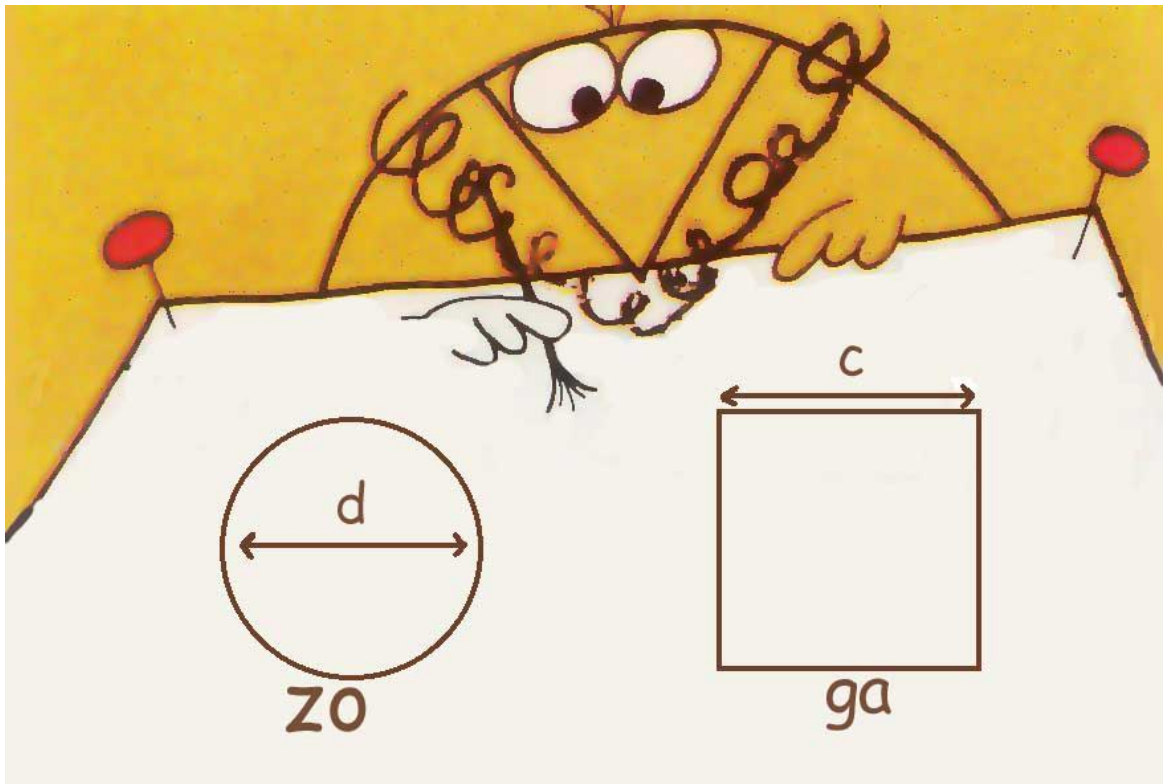
La quadrature du cercle

Marie Jacob

La quadrature du cercle
Un problème
à la mesure des Lumières
Fayard (2006).



Quadrature du cercle par les Shadocks



http ://www.chez.com/mathproject/

Irrationalité de π

Johann Heinrich Lambert (1728 - 1777)
Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques,
Mémoires de l'Académie des Sciences de Berlin, **17** (1761), p. 265-322 ;
read in 1767 ; Math. Werke, t. II.

Histoire de Pi

Frédéric II, Roi de Prusse
et H. Lambert
— Que savez vous, Lambert ?
— Tout, Sire.
— Et de qui le tenez–vous ?
— De moi-même !

Lambert (1767)

Le nombre $\tan(v)$ est irrationnel pour toute valeur rationnelle de $v \neq 0$ et $\tan(\pi/4) = 1$.

$$\tan(x) = \frac{1}{i}\tanh(ix), \qquad \tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}.$$

Développement en fraction continue de $\tan(x)$

$$\tan(x) = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{5 - \cfrac{x^2}{7 - \cfrac{x^2}{9 - \ddots}}}}}.$$

Développement en fraction continue de $\tan(x)$

P. Eymard et Lafon – *Autour du nombre pi*, Herman, 2000 et AMS, 2004.

S.A. Shirali – *Continued fraction for e*, Resonance, vol. **5** N°1, Jan. 2000, 14–28. http ://www.ias.ac.in/resonance/

Introductio in analysin infinitorum

Anticipe le 7ème
problème de D. Hilbert
sur la transcendance de a^b

Leonhard Euler (1737)

(1707 – 1783)

Introductio in analysin infinitorum

Fraction continue de e

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{\ddots}}}}}}$$

Joseph Fourier

Cours d'analyse à l'école polytechnique, 1815.

Irrationalité de e, d'après J. Fourier

$$e = \sum_{n=0}^{N} \frac{1}{n!} + \sum_{k\geq 0} \frac{1}{(N+1+k)!}\cdot$$

$$N!\, e - \sum_{n=0}^{N} \frac{N!}{n!} = \sum_{k\geq 0} \frac{N!}{(N+1+k)!} > 0\cdot$$

$$\frac{N!}{(N+1+k)!} \leq \frac{1}{N+1}\cdot\frac{N!}{(N+k)!} \leq \frac{1}{N+1}\cdot\frac{1}{k!}\cdot$$

$$\sum_{k\geq 0} \frac{N!}{(N+1+k)!} < \frac{1}{N+1}\sum_{k\geq 0}\frac{1}{k!} = \frac{e}{N+1}\cdot$$

Irrationalité de e, d'après J. Fourier

Dans la relation

$$N!\, e - \sum_{n=0}^{N} \frac{N!}{n!} = \sum_{k\geq 0} \frac{N!}{(N+1+k)!}$$

les nombres

$$N! \quad \text{et} \quad \sum_{n=0}^{N} \frac{N!}{n!}$$

sont entiers, tandis que le membre de droite est > 0 et tend vers 0 quand N tend vers l'infini.
Donc e est irrationnel.

Comme e est irrationnel, il en est de même de $e^{1/b}$ pour b entier positif.

Variante de l'argument de Fourier

F. Beukers : la série de e^{-1} est alternée.

Pour N impair,

$$1-\frac{1}{1!}+\frac{1}{2!}-\cdots-\frac{1}{N!}<e^{-1}<1-\frac{1}{1!}+\frac{1}{2!}-\cdots+\frac{1}{(N+1)!}$$

$$\frac{a_N}{N!}<e^{-1}<\frac{a_N}{N!}+\frac{1}{(N+1)!}$$

$$a_N<N!e^{-1}<a_N+1.$$

Donc $N!e^{-1}$ n'est pas entier.

Le nombre e n'est pas quadratique

Rappel (Euler, 1737) : $e = [2;\, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$ et ce développement n'est pas périodique. Donc e n'est pas rationnel (J-H. Lambert, 1766) ni même quadratique irrationnel (J-L. Lagrange, 1770).

Si $ae^2 + be + c = 0$ on peut écrire

$$cN! + \sum_{n=0}^{N} (2^n a + b) \frac{N!}{n!}$$

$$= -\sum_{k \geq 0} \left(2^{N+1+k} a + b\right) \frac{N!}{(N+1+k)!}.$$

Le membre de gauche est un entier, celui de droite tend vers l'infini !

e n'est pas quadratique (Liouville, 1840)

On écrit la relation quadratique sous la forme $ae + b + ce^{-1} = 0$.

$$bN! + \sum_{n=0}^{N} \left(a + (-1)^n c\right) \frac{N!}{n!}$$

$$= -\sum_{k \geq 0} \left(a + (-1)^{N+1+k} c\right) \frac{N!}{(N+1+k)!}.$$

Même argument : les deux membres s'annulent pour N suffisamment grand.

Le nombre e^2 n'est pas quadratique

J. Liouville (1809 - 1882) a démontré que e^2 n'est pas quadratique en 1840.

Sur l'irrationalité du nombre $e = 2,718\ldots$,
J. Math. Pures Appl.
(1) **5** (1840), p. 192 et p. 193-194.

Par exemple on en déduit l'irrationalité de e^4, donc de $e^{4/b}$ pour b entier positif.

e^2 n'est pas quadratique, d'après Liouville

On écrit $ae^2 + b + ce^{-2} = 0$ et

$$\frac{N!b}{2^{N-1}} + \sum_{n=0}^{N} (a + (-1)^n c) \frac{N!}{2^{N-n-1} n!}$$

$$= -\sum_{k \geq 0} \left(a + (-1)^{N+1+k} c\right) \frac{2^k N!}{(N+1+k)!}.$$

On vérifie que les nombres

$$\frac{N!}{2^{N-n-1} n!}, \quad (0 \leq n \leq N)$$

sont entiers pour une infinité de N.

Limite de la méthode

Le même argument ne semble pas suffire pour démontrer l'irrationalité du nombre e^3, encore moins pour montrer que le nombre e ne vérifie pas de relation cubique.

D.W. Masser a remarqué que cette démonstration donnait l'irrationalité de $e^{\sqrt{2}}$.

On obtient aussi l'irrationalité du nombre $e^{\sqrt{3}}$.

Le champ d'application de cette méthode est limité. On doit à Hermite l'idée fondamentale permettant d'aller plus loin, qui est à la base de la quasi-totalité des démonstrations de transcendance.

Irrationalité et approximation rationnelle

Si un nombre réel x est rationnel, alors il est mal approché par des nombres rationnels autres que lui même :
il existe $c > 0$ *tel que, pour tout* $p/q \in \mathbf{Q}$ *avec* $p/q \neq x$,

$$\left| x - \frac{p}{q} \right| \geq \frac{c}{q}.$$

Il suffit de prendre $c = 1/b$ quand $x = a/b$:

$$|aq - bp| \geq 1.$$

Un nombre $x \in \mathbf{R}$ *tel que, pour tout* $\epsilon > 0$, *il existe* $p/q \in \mathbf{Q}$ *avec*

$$0 < \left| x - \frac{p}{q} \right| \leq \frac{\epsilon}{q}$$

est donc irrationnel.

Réciproque : Adolf Hurwitz (1859 - 1919)

Inversement, Hurwitz a montré que si $x \in \mathbf{R}$ est irrationnel, alors il existe une infinité de $p/q \in \mathbf{Q}$ avec

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

Donc tout nombre irrationnel possède de très bonnes approximations rationnelles.
Or il suffit d'en trouver d'assez bonnes (ϵ/q) pour montrer qu'un nombre est irrationnel.

Idée d'Hermite (1873)

On veut démontrer l'irrationalité de e^a quand a est un entier positif. On en déduira l'irrationalité de e^r quand r est un nombre rationnel non nul :

$$e^{-a} = \frac{1}{e^a}, \qquad \left(e^{a/b}\right)^b = e^a.$$

Tronquer le développement de Taylor de l'exponentielle produit des approximations rationnelles de dénominateur $n!$, il en existe de meilleures avec d'autres dénominateurs.

L'idée d'Hermite est d'approcher la *fonction* e^z par une fraction rationnelle $A(z)/B(z)$, puis de substituer $z = a$.

Irrationalité de e^r et π, méthode d'Hermite

But : écrire $B_n(z)e^z = A_n(z) + R_n(z)$ avec A_n et B_n dans $\mathbf{Z}[z]$ et $R_n(a) \neq 0$, $\lim_{n\to\infty} R_n(a) = 0$.

On spécialise $z = a$, on pose $q = B_n(a)$, $p = A_n(a)$ et on obtient

$$0 < |qe^a - p| < \epsilon.$$

L'irrationalité de e^a en résulte.

Pour $a = 1$, $B_n = 1$ suffit : on tronque la série exponentielle (Ch. Fourier, 1815)

Pour $a = 2$ aussi : J. Liouville, 1840.

Approximation rationnelle d'une fonction

Une fraction rationnelle A/B *est une approximation d'une fonction analytique* f (au sens d'Hermite, puis de Padé) *si les développements de Taylor à l'origine ont les mêmes premiers termes.*

Quand $B(0) \neq 0$ cela signifie que $B(z)f(z)$ et $A(z)$ ont le même début de développement de Taylor à l'originedonc que $B(z)f(z)$ a un grand trou dans son développement de Taylor à l'origine : on prend pour $A(z)$ le début de ce développement.

Approximations rationnelles de la fonction exp

Étant donnés $n_0 \geq 0$ *et* $n_1 \geq 0$, *trouver* A *et* B *dans* $\mathbf{R}[z]$ *de degrés* $\leq n_0$ *et* $\leq n_1$ *tels que* $R(z) = B(z)e^z - A(z)$ *ait un zéro à l'origine de multiplicité* $\geq N + 1$ *avec* $N = n_0 + n_1$.
On utilisera cette construction avec $n_0 = n_1 = n$.

Théorème *Il existe une solution, elle est unique avec* B *unitaire. De plus,* B *est dans* $\mathbf{Z}[z]$ *et* $(n_0!/n_1!)A$ *est dans* $\mathbf{Z}[z]$, *le polynôme* A *est de degré exactement* n_0 *et* B *de degré* n_1, *tandis que* R *a un zéro de multiplicité exactement* $N + 1$ *à l'origine.*

$B(z)e^z = A(z) + R(z)$

Démonstration. Unicité de R, donc de A et B.
Soit $D = d/dz$. Comme A est de degré $\leq n_0$,

$$D^{n_0+1}R = D^{n_0+1}(B(z)e^z).$$

Le membre de droite est le produit de e^z par un polynôme de degré égal à celui de B et de même coefficient directeur. Comme $D^{n_0+1}R(z)$ a un zéro de multiplicité $\geq n_1$ à l'origine, $D^{n_0+1}R = z^{n_1}e^z$. Donc R est l'unique solution de l'équation différentielle $D^{n_0+1}R = z^{n_1}e^z$ avec un zéro de multiplicité $\geq n_0$ en 0. De plus B est de degré n_1 et la multiplicité de R en 0 est $N + 1 = n_0 + n_1 + 1$.

$A(z)$ est de degré n_0

On multiplie

$$B(z)e^z = A(z) + R(z).$$

par e^{-z} et on remplace z par $-z$:

$$A(-z)e^z = B(-z) - R(-z)e^z.$$

Donc $\left(B(-z), A(-z), -R(-z)e^z\right)$ est la solution du problème avec les paramètres (n_1, n_0), donc A est de degré n_0.
Si on a une formule explicite pour A, on en déduit une pour B et inversement.

Présentation de la méthode de Hermite par Siegel

C.L. Siegel, 1949.

On veut résoudre
$D^{n_0+1}R(z) = z^{n_1}e^z$.
Conditions initiales :
premières dérivées nulles à l'origine.

On itère l'opérateur $J\varphi = \int_0^z \varphi(t)dt$, inverse de D :

$$J^{n+1}\varphi = \int_0^z \frac{1}{n!}(z-t)^n\varphi(t)dt.$$

Donc

$$R(z) = \frac{1}{n_0!}\int_0^z (z-t)^{n_0}t^{n_1}e^t dt.$$

Formules de Hermite–Siegel pour $A(z)$ et $B(z)$

Soit $B \in \mathbf{C}[z]$ unitaire de degré n_1 et $A \in \mathbf{C}[z]$ de degré n_0, tels que $R(z) = B(z)e^z - A(z)$ ait un zéro de multiplicité $N+1$ en 0.

De

$$D^{n_0+1}\big(B(z)e^z\big) = z^{n_1}e^z$$

Siegel déduit

$$B(z) = (1+D)^{-n_0-1}z^{n_1}.$$

Il en résulte que B a ses coefficients entiers.

Formule pour B

Formule explicite pour B :

$$(1+D)^{-n_0-1} = \sum_{\ell \geq 0} (-1)^\ell \binom{n_0+\ell}{\ell} D^\ell.$$

D'où

$$B(z) = \sum_{\ell=0}^{n_1} (-1)^\ell \binom{n_0+\ell}{\ell} \frac{n_1!}{(n_1-\ell)!} z^{n_1-\ell},$$

que l'on peut écrire

$$B(z) = (-1)^{n_1} \frac{n_1!}{n_0!} \sum_{k=0}^{n_1} (-1)^k \frac{(N-k)!}{(n_1-k)!k!} z^k.$$

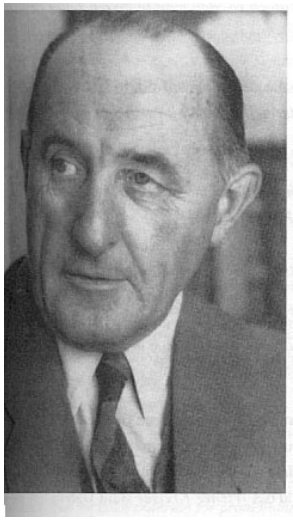
On vérifie que B est unitaire de degré n_1.

Autre présentation, selon Yu.V. Nesterenko

Charles Hermite (1873)

Carl Ludwig Siegel (1929, 1949)

Yuri Nesterenko (2005)



L'opérateur $\delta = zd/dz$

On pose $\delta = zd/dz$, qui vérifie $\delta(z^k) = kz^k$. Alors $\delta^m z^k = k^m z^k$ pour $m \geq 0$. Par linéarité, si $T \in \mathbf{C}[z]$, on a

$$T(\delta)z^k = T(k)z^k.$$

Donc, pour

$$f(z) = \sum_{k \geq 0} a_k z^k,$$

on a

$$T(\delta)f(z) = \sum_{k \geq 0} a_k T(k) z^k$$

On annule le coefficient de Taylor de z^k en considérant $T(\delta)f(z)$ où T satisfait $T(k) = 0$.

Annuler plusieurs coefficients du développement

Soient $N \geq n_0$ des entiers et

$$T(z) = (z - n_0 - 1)(z - n_0 - 2) \cdots (z - N).$$

Alors $T(\delta)f(z) = A(z) + R(z)$ avec

$$A(z) = \sum_{k=0}^{n_0} T(k)a_k z^k \quad \text{et} \quad R(z) = \sum_{k \geq N+1} T(k)a_k z^k.$$

Dans le développement de $T(\delta)f(z)$ les coefficients de $z^{n_0+1}, z^{n_0+2}, \ldots, z^N$ sont nuls.

Approximations rationnelles de e^z

On prend $f(z) = e^z$ avec $a_k = 1/k!$ et $n_0 = n$, $N = 2n$. Soit

$$T_n(z) = (z - n - 1)(z - n - 2) \cdots (z - 2n).$$

On a

$$\delta(e^z) = ze^z.$$

Il existe $B_n \in \mathbf{Z}[z]$, unitaire de degré n, tel que $T_n(\delta)e^z = B_n(z)e^z$. Donc

$$\boxed{B_n(z)e^z = A_n(z) + R_n(z)}$$

avec

$$A_n(z) = \sum_{k=0}^{n} T_n(k)\frac{z^k}{k!} \quad \text{et} \quad R_n(z) = \sum_{k \geq 2n+1} T_n(k)\frac{z^k}{k!}.$$

Les coefficients de A_n sont entiers

Chaque coefficient de A_n est multiple d'un coefficient du binôme

$$\frac{T_n(k)}{k!} = (-1)^n(2n-k)(2n-k-1)\cdots(n+1) \cdot \frac{n(n-1)\cdots(n-k+1)}{k!}$$

pour $0 \leq k \leq n$. Donc $A_n \in \mathbf{Z}[z]$.

Irrationalité de e^r

Soit a un entier positif. On pose $s = e^a$. Si on remplace z par a on trouve

$$B_n(a)s - A_n(a) = R_n(a).$$

Les coefficients de R_n sont tous positifs, donc $R_n(a) > 0$ et $B_n(a)s - A_n(a) \neq 0$. Comme $R_n(a)$ tend vers 0 quand n tend vers l'infini et comme $B_n(a)$ et $A_n(a)$ sont des entiers, il en résulte que s est irrationnel.

Irrationalité de logarithmes, y compris π

L'irrationalité de e^r pour $r \in \mathbf{Q}^\times$, équivaut à l'irrationalité de $\log s$ pour $s \in \mathbf{Q}_{>0}$.

Le même argument donne l'irrationalité de $\log(-1)$, au sens où $\log(-1) = i\pi \notin \mathbf{Q}(i)$.

Donc $\pi \notin \mathbf{Q}$.

Irrationalité de π

On suppose que π est un nombre rationnel, $\pi = a/b$. On remplace z par $ia = i\pi b$ dans les formules précédentes. Comme $e^z = (-1)^b$ on a

$$B_n(ia)(-1)^b - A_n(ia) = R_n(ia),$$

et les deux nombres complexes $A_n(ia)$ et $B_n(ia)$ sont dans $\mathbf{Z}[i]$. Le membre de gauche est dans $\mathbf{Z}[i]$, celui de droite tend vers 0 quand n tend vers l'infini. Donc tous les deux sont nuls.

En prenant un résultant, on montre enfin que R_n et R_{n+1} n'ont pas de zéro commun en dehors de 0. D'où la contradiction.

Irrationalité de e^r et de π^2

Une démonstration courte (J. Niven 1946)
Soit $a \in \mathbf{Z}$, $a \neq 0$.
Supposons $e^a = p/q$. Le nombre

$$R_n := qa^{2n+1} \int_0^1 e^{ax} x^n (1-x)^n dx$$

est entier et pour n suffisamment grand, $0 < R_n < 1$.
Contradiction.
De même pour l'irrationalité de π^2 (A.M. Legendre 1794).
Supposons $\pi^2 = p/q$. Pour n entier suffisamment grand, l'entier rationnel

$$R_n := \pi \cdot \frac{p^n}{n!} \int_0^1 \sin(\pi x) x^n (1-x)^n dx$$

vérifie $0 < R_n < 1$. Contradiction.
1979, F. Beukers : $\zeta(2) \notin \mathbf{Q}$ (R. Apéry, 1978, $\zeta(3) \notin \mathbf{Q}$).

Approximation simultanée et transcendance

Les démonstrations d'irrationalité font intervenir des approximations rationnelles du nombre considéré.

On veut obtenir des énoncés de transcendance.

Un nombre complexe θ est transcendant si et seulement si

$$1, \theta, \theta^2, \ldots, \theta^m, \ldots$$

sont $\mathbf{Q}$–linéairement indépendants.

Donc le but est de démontrer des résultats d'indépendance linéaire, sur le corps des nombres rationnels, de nombres complexes.

$L = a_0 + a_1 x_1 + \cdots + a_m x_m$

Soient $x_1, \ldots, x_m$ des nombres réels et a_0, $a_1, \ldots,$ a_m des entiers rationnels qui ne sont pas tous nuls. On veut démontrer que le nombre

$$L = a_0 + a_1 x_1 + \cdots + a_m x_m$$

n'est pas nul. L'idée est d'approcher simultanément les nombres $x_1, \ldots, x_m$ par des nombres rationnels $b_1/b_0, \ldots, b_m/b_0$.
Soient $b_0, b_1, \ldots, b_m$ des entiers rationnels. Pour $1 \leq k \leq m$ posons

$$\epsilon_k = b_0 x_k - b_k.$$

Alors $b_0 L = A + R$ avec

$$A = a_0 b_0 + \cdots + a_m b_m \in \mathbf{Z} \quad \text{et} \quad R = a_1 \epsilon_1 + \cdots + a_m \epsilon_m \in \mathbf{R}.$$

Si $0 < |R| < 1$, *alors* $L \neq 0$.

Approximation simultanée de la fonction exponentielle

L'énoncé d'irrationalité de e^r reposait sur la construction explicite d'approximations rationnelles $A/B \in \mathbf{Q}(x)$ de la fonction exponentielle e^x.

Une des idées d'Hermite est d'introduire des *approximations rationnelles simultanées de la fonction exponentielle*, en analogie avec les résultats récents (à l'époque) sur l'approximation diophantienne de nombres. (Dirichlet notamment).

ANALYSE. — *Sur la fonction exponentielle;* par M. HERMITE.

« I. Étant donné un nombre quelconque de quantités numériques $\alpha_1, \alpha_2, \ldots, \alpha_n$, on sait qu'on peut en approcher simultanément par des fractions de même dénominateur, de telle sorte qu'on ait

$$\alpha_1 = \frac{A_1}{A} + \frac{\delta_1}{A\sqrt[n]{A}},$$

$$\alpha_2 = \frac{A_2}{A} + \frac{\delta_2}{A\sqrt[n]{A}},$$

$$\ldots\ldots\ldots\ldots\ldots,$$

$$\alpha_n = \frac{A_n}{A} + \frac{\delta_n}{A\sqrt[n]{A}},$$

$\delta_1, \delta_2, \ldots, \delta_n$ ne pouvant dépasser une limite qui dépend seulement de n. C'est, comme on voit, une extension du mode d'approximation résultant de la théorie des fractions continues, qui correspondrait au cas le plus simple de $n = 1$. Or on peut se proposer une généralisation semblable de la théorie des fractions continues algébriques, en cherchant les expressions approchées de n fonctions, $\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x)$ par des fractions rationnelles $\frac{\Phi_1(x)}{\Phi(x)}, \frac{\Phi_2(x)}{\Phi(x)}, \ldots, \frac{\Phi_n(x)}{\Phi(x)}$, de manière que les développements en série suivant les puissances croissantes de la variable coïncident jusqu'à une puissance déterminée x^M. Voici d'abord à cet égard un premier résultat qui s'offre immédiatement. Supposons que les fonctions $\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x)$ soient toutes développables en séries de la forme $\alpha + \beta x + \gamma x^2 + \ldots$ et faisons

$$\Phi(x) = A x^m + B x^{m-1} + \ldots + K x + L.$$

Approximants de Padé

Il y a deux points de vue, duaux l'un de l'autre. Ils donnent lieu aux deux types d'*approximants de Padé*.

Henri Eugène Padé (1863 - 1953)
Approximation de
fonctions analytiques
par des fractions rationnelles.

Théorie des séries divergentes
(*L. Euler, E.N. Laguerre,*
1886 : *T.J. Stieltjes Séries semi-convergentes* et
H. Poincaré séries asymptotiques).
S. Ramanujan

Hermite 1873

Si $\alpha_1, \ldots, \alpha_m$ sont des nombres complexes deux à deux distincts, $n_0, \ldots, n_m$ des entiers ≥ 0, Hermite construit explicitement des polynômes $Q_0, Q_1, \ldots, Q_m$ avec Q_k de degré $M - n_k$ tels que chacune des fonctions

$$Q_0(z)e^{\alpha_k z} - Q_k(z), \quad (1 \leq k \leq m)$$

ait à l'origine un zéro de multiplicité supérieur à $M = n_0 + \cdots + n_m$.

Pour $\alpha_k = k$ et $z = 1$ il en déduit des approximations rationnelles simultanées des nombres e, e^2, $\ldots e^m$, qui permettent de déduire que ces nombres sont linéairement indépendants sur $\mathbf{Q}$, donc que e est transcendant.

» Il en résulte qu'on ne peut, en général, admettre que le déterminant proposé Δ s'annule, car les quantités $P = f(p)$, $Q = f(q), \ldots$, fonctions entières semblables des racines p, $q, \ldots$, de l'équation dérivée $f'(x) = 0$ seront comme ces racines différentes entre elles. C'est ce qu'il fallait établir pour démontrer l'impossibilité de toute relation de la forme

$$N + e^a N_1 + e^b N_2 + \ldots + e^h N_n = 0,$$

et arriver ainsi à prouver *que le nombre e ne peut être racine d'une équation algébrique de degré quelconque à coefficients entiers.*

» Mais une autre voie conduira à une seconde démonstration plus rigoureuse; on peut en effet, comme on va le voir, étendre aux fractions rationnelles

$$\frac{\Phi_1(x)}{\Phi(x)}, \quad \frac{\Phi_2(x)}{\Phi(x)}, \ldots, \quad \frac{\Phi_n(x)}{\Phi(x)}$$

le mode de formation des réduites donné par la théorie des fractions continues, et par là mettre plus complétement en évidence le caractère arithmétique d'une irrationnelle non algébrique. Dans cet ordre d'idées, M. Liouville a déjà obtenu un théorème remarquable qui est l'objet de son travail intitulé : *Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques* (*), et je rappellerai aussi que l'illustre géomètre a démontré le premier la proposition qui est le sujet de ces recherches pour les cas de l'équation du second degré et de

(*) *Comptes rendus*, t. XVIII, p. 883 et 910.

l'équation bicarrée [*Journal de Mathématiques* (*Note sur l'irrationnalité du nombre e*, t. V, p. 192)]. Sous le point de vue auquel je me suis placé, voici la première proposition à établir.

Comment démontrer le lemme de zéros ?

On part de a_0, $a_1, \ldots, a_m$ entiers rationnels non tous nuls.

On veut démontrer $L = a_0 + a_1 x_1 + \cdots + a_m x_m \neq 0$.

On considère des approximations simultanées $b_1/b_0, \ldots, b_m/b_0$ de $x_1, \ldots, x_m$.

On a $L = A + R$ avec $A = a_0 b_0 + \cdots + a_m b_m \in \mathbf{Z}$ et $R = a_1 \epsilon_1 + \cdots + a_m \epsilon_m$, $|R| < 1$.

Il reste à vérifier $R \neq 0$ ou $A \neq 0$ (lemme de zéro).

$b_0, b_1, \ldots, b_m$ est un $m+1$–uplet d'entiers rationnels.

Si on produit $m+1$ uplets indépendants, un au moins donnera une valeur non nulle pour A.

Critère d'indépendance linéaire

Soit $(x_1, \ldots, x_m) \in \mathbf{R}^m$. *Les conditions suivantes sont équivalentes*
(i) Les nombres $1, x_1, \ldots, x_m$ *sont linéairement indépendants sur* $\mathbf{Q}$.
(ii) Pour tout $\epsilon > 0$ *il existe* $m+1$ *éléments linéairement indépendants* $\mathbf{Z}^{m+1}$, *disons*

$$(q_i, p_{1i}, \ldots, p_{mi}), \quad (0 \leq i \leq m)$$

avec $q_i > 0$, *tels que*

$$\max_{1 \leq k \leq m} \left| x_k - \frac{p_{ki}}{q_i} \right| \leq \frac{\epsilon}{q_i}, \quad (0 \leq i \leq m).$$

Théorèmes de Hermite et Lindemann

Hermite (1873) :
transcendance de e.

Lindemann (1882) :
transcendance de π.

Théorème de Hermite–Lindemann
Pour tout nombre complexe non nul z, un au moins des deux nombres z, e^z est transcendant.

Corollaires : transcendance de $\log \alpha$ et de e^β pour α and β nombres algébriques non nuls avec $\log \alpha \neq 0$.

Approximants de Padé de type II

Approximants de Padé de deuxième espèce : polynômes $A_1, \ldots, A_m$ avec A_j de degré $\leq M - n_j$ tels que chacune des fonctions

$$A_i(z)f_j(z) - A_j(z)f_i(z) \quad (1 \leq i < j \leq m)$$

ait à l'origine un zéro de multiplicité $> M$.

Référence : N.I. Feldman and Yu.V. Nesterenko, *Number Theory IV*, Transcendental Numbers, Encyclopaedia of Mathematical Sciences, **44** (1998) Chap. 2.

Approximants de Padé de type I

Soient $f_1, \ldots, f_m$ des fonctions analytiques au voisinage de l'origine. Soient $n_1, \ldots, n_m$ des entiers ≥ 0,
$M = n_0 + \cdots + n_m$.

Approximants de Padé de première espèce : polynômes $P_1, \ldots, P_m$ avec P_j de degré $\leq n_j$ tels que la fonction

$$P_1(z)f_1(z) + \cdots + P_m(z)f_m(z)$$

ait à l'origine un zéro de multiplicité au moins $M + m - 1$.

Hermite 1893

Si $\alpha_1, \ldots, \alpha_m$ sont des nombres complexes deux à deux distincts, $n_0, \ldots, n_m$ des entiers ≥ 0, Hermite construit explicitement des polynômes $P_1, \ldots, P_m$ avec P_j de degré n_j tels que la fonction

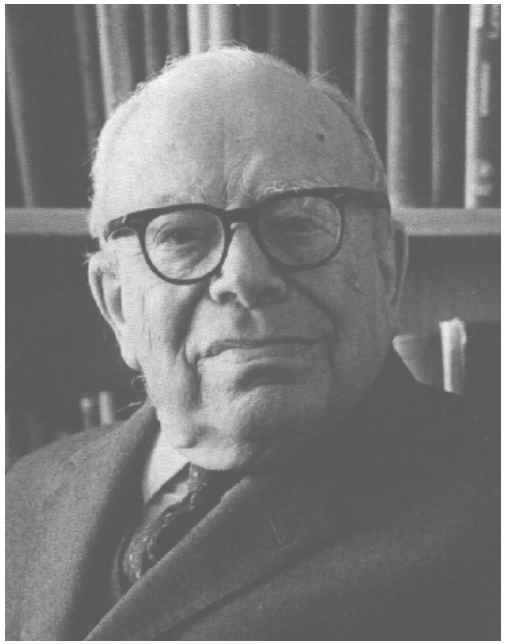
$$P_1(z)e^{\alpha_1 z} + \cdots + P_m(z)e^{\alpha_m z}$$

ait à l'origine un zéro de multiplicité au moins $n_1 + \cdots + n_m + m - 1$.

C. Hermite (1917) : autre expression intégrale pour le reste.

Application à la transcendance : *K. Mahler (1930).*

Approximants de Padé de type I



1930 : K. Mahler, utilisation des formules de Hermite pour les approximants de Padé de type I
Version quantitative du théorème de Hermite–Lindemann et Lindemann–Weierstrass
1953 : $e^b - a$

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)

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

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

avec une constante absolue c ?

Equivalent :

$$|b - \log a| > a^{-c}, \quad |e^b - a| > e^{-cb}, \quad |e^b - a| > a^{-c}.$$

Heuristique : on peut même espérer mieux :

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

Equivalent :

$$|b - \log a| > a(\log a)^{-c}, \quad |e^b - a| > b^{-c}, \quad |e^b - a| > a(\log a)^{-c}.$$

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.

Énoncés diophantiens

Théorème (S. Khemira – P. Voutier)

Pour a et b dans $\mathbf{Q}$ avec $b \neq 0$, on a

$$|b - \log a| \geq \exp\{-C(\log A)(\log B)\}$$

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

- La hauteur d'un nombre rationnel p/q est définie par $H(p/q) = \max\{|p|,\ q)$.
- La constante absolue C est explicitée.

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.