Historical introduction to transcendence

Michel Waldschmidt

http://www.math.jussieu.fr/∼miw/

Abstract

The transcendence proofs for constants of analysis are essentially all based on the seminal work by Ch. Hermite : his proof of the transcendence of the number e in 1873 is the prototype of the methods which have been subsequently developed. The founding paper by Hermite was influenced by earlier authors (Lambert, Euler, Fourier, Liouville). We explain how his arguments have been expanded in several directions : Padé approximants, interpolation series, auxiliary functions.

Simultaneous approximation and transcendence

Irrationality proofs involve rational approximation to a single real number θ.

We wish to prove transcendence results.

A complex number θ *is transcendental if and only if the numbers*

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

are $\mathbf{Q}$*–linearly independent.*

Hence our goal is to prove linear independence, over the rational number field, of complex numbers.

$L = a_0 + a_1x_1 + \cdots + a_mx_m$

Let $x_1, \ldots, x_m$ be real numbers and a_0, $a_1, \ldots,$ a_m rational integers, not all of which are zero. We wish to prove that the number

$$L = a_0 + a_1x_1 + \cdots + a_mx_m$$

is not zero. Approximate simultaneously $x_1, \ldots, x_m$ by rational numbers $b_1/b_0, \ldots, b_m/b_0$.
Let $b_0, b_1, \ldots, b_m$ be rational integers. For $1 \le k \le m$ set

$$\epsilon_k = b_0x_k - b_k.$$

Then $b_0L = A + R$ with

$$A = a_0b_0 + \cdots + a_mb_m \in \mathbf{Z} \quad \text{and} \quad R = a_1\epsilon_1 + \cdots + a_m\epsilon_m \in \mathbf{R}.$$

If $0 < |R| < 1$, *then* $L \neq 0$.

How to prove $R \neq 0$?

Zero lemma : $R = a_1\epsilon_1 + \cdots + a_m\epsilon_m \neq 0.$

Suffices $A = a_0b_0 + \cdots + a_mb_m \neq 0.$

We started with a_0, $a_1, \dots,$ a_m rational integers, not all of which are zero.

We considered simultaneous approximations $b_1/b_0, \dots, b_m/b_0$ to $x_1, \dots, x_m$.

$b_0, b_1, \dots, b_m$ is a $m+1$–tuple of rational integers.

If we produce $m+1$ linearly independent such tuples, one at least of them will give a non–zero value for A.

Criterion of linear independence

Let $\underline{\vartheta} = (\vartheta_1, \dots, \vartheta_m) \in \mathbf{R}^m$. *Then the following conditions are equivalent.*

(i) The numbers $1, \vartheta_1, \dots, \vartheta_m$ *are linearly independent over* $\mathbf{Q}$.

(ii) For any $\epsilon > 0$ *there exist* $m + 1$ *linearly independent elements* $\underline{b}_0, \underline{b}_1, \dots, \underline{b}_m$ *in* $\mathbf{Z}^{m+1}$, *say*

$$\underline{b}_i = (q_i, p_{1i}, \dots, p_{mi}), \quad (0 \le i \le m)$$

with $q_i > 0$, *such that*

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

A non–vanishing determinant

The condition on linear independence of the elements $\underline{b}_0, \underline{b}_1, \ldots, \underline{b}_m$ means that the determinant

$$\begin{vmatrix} q_0 & p_{10} & \cdots & p_{m0} \\ \vdots & \vdots & \ddots & \vdots \\ q_m & p_{1m} & \cdots & p_{mm} \end{vmatrix}$$

is not 0.

Simultaneous approximation to the exponential function

Irrationality results follow from rational approximations $A/B \in \mathbf{Q}(x)$ to the exponential function e^x.

One of Hermite's ideas is to consider *simultaneous rational approximations to the exponential function*, in analogy with Diophantine approximation.

Let $B_0, B_1, \dots, B_m$ be polynomials in $\mathbf{Z}[x]$. For $1 \le k \le m$ define

$$R_k(x) = B_0(x)e^{kx} - B_k(x).$$

Set $b_j = B_j(1)$, $0 \le j \le m$ and

$$R = a_0 + a_1 R_1(1) + \cdots + a_m R_m(1).$$

If $0 < |R| < 1$, then $a_0 + a_1 e + \cdots + a_m e^m \neq 0$.

Hermite : approximation to the functions $1, e^{\alpha_1 x}, \ldots, e^{\alpha_m x}$

Let $\alpha_1, \ldots, \alpha_m$ be pairwise distinct complex numbers and $n_0, \ldots, n_m$ be rational integers, all ≥ 0. Set $N = n_0 + \cdots + n_m$.

Hermite constructs explicitly polynomials B_0, $B_1, \ldots,$ B_m with B_j of degree $N - n_j$ such that each of the functions

$$B_0(z)e^{\alpha_k z} - B_k(z), \quad (1 \leq k \leq m)$$

has a zero at the origin of multiplicity at least N.

Solution of Padé problem for exponential functions

Hermite, 1872.

Let $f_1, \ldots, f_m$ *be analytic functions of one complex variable near the origin. Let* $n_0, n_1, \ldots, n_m$ *be non-negative integers. Set*

$$N = n_0 + n_1 + \cdots + n_m.$$

Then there exists a tuple $(Q, P_1, \ldots, P_m)$ *of polynomials in* $\mathbf{C}[X]$ *satisfying the following properties :*

(i) The polynomial Q *is not zero, it has degree* $\leq N - n_0$.

(ii) For $1 \leq \mu \leq m$, *the polynomial* P_μ *has degree* $\leq N - n_\mu$.

(iii) For $1 \leq \mu \leq m$, *the function* $x \mapsto Q(x)f_\mu(x) - P_\mu(x)$ *has a zero at the origin of multiplicity* $\geq N + 1$.

Padé approximants

Henri Eugène Padé (1863 - 1953)
Approximation of complex analytic functions by rational functions.

Theory of divergent series (*L. Euler, E.N. Laguerre,* 1886 : *T.J. Stieltjes semi-convergent series* and *H. Poincaré asymptotic series*).
S. Ramanujan

Hermite–Padé polynomials

Let m be a positive integer, $n_0, \ldots, n_m$ be non-negative integers. Set $N = n_0 + \cdots + n_m$. Define the polynomial $f \in \mathbf{Z}[t]$ of degree N by

$$f(t) = t^{n_0}(t-1)^{n_1} \cdots (t-m)^{n_m}.$$

Further set, for $1 \leq \mu \leq m$,

$$Q(x) = \sum_{k=n_0}^{N} x^{N-k} D^k f(0), \quad P_\mu(x) = \sum_{k=n_\mu}^{N} x^{N-k} D^k f(\mu)$$

and

$$R_\mu(x) = x^{N+1} e^{x\mu} \int_0^\mu e^{-xt} f(t) dt.$$

Hermite–Padé polynomials

Then the polynomial Q has exact degree $N - n_0$, while P_μ has exact degree $N - n_\mu$, and R_μ is an analytic function having at the origin a multiplicity $\geq N + 1$. Further, for $1 \leq \mu \leq m$,

$$Q(x)e^{\mu x} - P_\mu(x) = R_\mu(x).$$

Hence $(Q, P_1, \ldots, P_m)$ is a Padé system of the second type for the m-tuple of functions $(e^x, e^{2x}, \ldots, e^{mx})$, attached to the parameters $n_0, n_1, \ldots, n_m$. Furthermore, the polynomials $(1/n_0!)Q$ and $(1/n_\mu!)P_\mu$ for $1 \leq \mu \leq m$ have integral coefficients.

Independent forms

Fix integers $n_0, \ldots, n_1$, all ≥ 1. For $j = 0, 1, \ldots, m$ denote by $Q_j, P_{j1}, \ldots, P_{jm}$ the Hermite-Padé polynomials attached to the parameters

$$n_0 - \delta_{j0}, n_1 - \delta_{j1}, \ldots, n_m - \delta_{jm},$$

where δ_{ji} is Kronecker's symbol.

These parameters are the rows of the matrix

$$\begin{pmatrix} n_0 - 1 & n_1 & n_2 & \cdots & n_m \\ n_0 & n_1 - 1 & n_2 & \cdots & n_m \\ \vdots & \vdots & \ddots & \vdots & \\ n_0 & n_1 & n_2 & \cdots & n_m - 1 \end{pmatrix}.$$

Independent forms

There exists a non-zero constant c such that the determinant

$$\Delta(x) = \begin{vmatrix} Q_0(x) & P_{10}(x) & \cdots & P_{m0}(x) \\ \vdots & \vdots & \ddots & \vdots \\ Q_m(x) & P_{1m}(x) & \cdots & P_{mm}(x) \end{vmatrix}$$

is the monomial cx^{mN}.

Fix a sufficiently large integer n and use the previous results for $n_0 = n_1 = \cdots = n_m = n$ with $N = (m+1)n$.

Consequence

Define, for $0 \leq j \leq m$, $q_j, p_{1j}, \ldots, p_{nj}$ in $\mathbf{Z}$ by

$$(n-1)!q_j = Q_j(1),\ (n-1)!p_{\mu j} = P_{\mu j}(1), \quad (1 \leq \mu \leq m).$$

There exists a constant $\kappa > 0$ independent on n such that for $1 \leq \mu \leq m$ and $0 \leq j \leq m$,

$$|q_i e^{\mu} - p_{\mu j}| \leq \frac{\kappa^n}{n!}.$$

Further, the determinant

$$\begin{vmatrix} q_0 & p_{10} & \cdots & p_{m0} \\ \vdots & \vdots & \ddots & \vdots \\ q_m & p_{1m} & \cdots & p_{mm} \end{vmatrix}$$

is not zero.

XIX-th Century :
1844 : Liouville : existence of transcendental numbers, examples (continued fractions, fast converging series)

1874, 1891 : G. Cantor : existence of transcendental numbers.

1873 : Ch. Hermite : transcendence of e.

1882 : F. Lindemann : transcendence of π.

Hermite–Lindemann Theorem

For any non-zero complex number z*, one at least of the two numbers* z *and* e^z *is transcendental.*

Hermite (1873) : transcendence of e.

Lindemann (1882) : transcendence of π.

Corollaries : transcendence of $\log \alpha$ and of e^β for α and β non-zero algebraic complex numbers, with $\log \alpha \neq 0$.

First result of algebraic independence

Lindemann–Weierstraß (1885) :

Let $\alpha_1, \dots, \alpha_m$ *be algebraic numbers which are pairwise distinct :* $\alpha_i \neq \alpha_j$ *for* $i \neq j$*. Then the numbers* $e^{\alpha_1}, \dots, e^{\alpha_m}$ *are linearly independent over* $\mathbf{Q}$*.*

Let $\beta_1, \dots, \beta_n$ *be algebraic numbers which are linearly independent over* $\mathbf{Q}$*. Then the numbers* $e^{\beta_1}, \dots, e^{\beta_n}$ *are algebraically independent over* $\mathbf{Q}$ *hence over* $\overline{\mathbf{Q}}$*.*

Let $\alpha_1, \dots, \alpha_m$ *be algebraic numbers which are pairwise distinct. Then the numbers* $e^{\alpha_1}, \dots, e^{\alpha_m}$ *are linearly independent over* $\overline{\mathbf{Q}}$*.*

Hilbert's seventh problem

A.O. Gel'fond and Th. Schneider (1934).
Solution of Hilbert's seventh problem :
transcendence of α^β
and of $(\log \alpha_1)/(\log \alpha_2)$
for algebraic α, β, α_2 *and* α_2.

A. Baker, 1968. *Let* $\log \alpha_1, \ldots, \log \alpha_n$ *be* $\mathbf{Q}$*–linearly independent logarithms of algebraic numbers. Then the numbers* $1, \log \alpha_1, \ldots, \log \alpha_n$ *are linearly independent over the field* $\overline{\mathbf{Q}}$.

Four exponentials Conjecture

S. Ramanujan : highly composite numbers. *Let t be a real number such that 2^t and 3^t are integers. Does it follow that t is a positive integer ?*

Alaoglu and Erdös.

C.L. Siegel, A. Selberg, S. Lang, K. Ramachandra :

Theorem : *If the three numbers 2^t, 3^t and 5^t are integers, then t is a rational number (hence a positive integer).*

Four exponentials Conjecture

Set $2^t = a$ and $3^t = b$. Then the determinant

$$\begin{vmatrix} \log 2 & \log 3 \\ \log a & \log b \end{vmatrix}$$

vanishes.

Four exponentials Conjecture. *Let*

$$\begin{pmatrix} \log \alpha_1 & \log \alpha_2 \\ \\ \log \beta_1 & \log \beta_2 \end{pmatrix}$$

be a 2×2 *matrix whose entries are logarithms of algebraic numbers. Assume the two columns are* $\mathbf{Q}$ *-linearly independent and the two rows are also* $\mathbf{Q}$ *-linearly independent. Then the matrix is regular.*

Four exponentials Conjecture and Six exponentials Theorem

Conjecture. *Let x_1, x_2 be $\mathbf{Q}$–linearly independent complex numbers and y_1, y_2 be also $\mathbf{Q}$–linearly independent complex numbers. Then one at least of the four numbers*

$$e^{x_1 y_1},\ e^{x_1 y_2},\ e^{x_2 y_1},\ e^{x_2 y_2}$$

is transcendental.

Theorem. *Let d and ℓ be positive integers with $d\ell > d + \ell$. Let $x_1, \dots, x_d$ be $\mathbf{Q}$–linearly independent complex numbers and $y_1, \dots, y_\ell$ be also $\mathbf{Q}$–linearly independent complex numbers. Then one at least of the $d\ell$ numbers*

$$e^{x_i y_j}, \quad (1 \le i \le d,\ 1 \le j \le \ell)$$

is transcendental.

Six exponentials Theorem

Theorem (Siegel, Lang, Ramachandra). *Let*

$$\begin{pmatrix} \log \alpha_1 & \log \alpha_2 & \log \alpha_3 \\ \log \beta_1 & \log \beta_2 & \log \beta_3 \end{pmatrix}$$

be a 2 *by* 3 *matrix whose entries are logarithms of algebraic numbers. Assume the three columns are linearly independent over* $\mathbf{Q}$ *and the two rows are also linearly independent over* $\mathbf{Q}$*. Then the matrix has rank* 2*.*

The Strong Six Exponentials Theorem

Denote by $\widetilde{\mathcal{L}}$ the $\overline{\mathbf{Q}}$-vector space spanned by 1 and $\mathcal{L}$: hence $\widetilde{\mathcal{L}}$ is the set of linear combinations with algebraic coefficients of logarithms of algebraic numbers :

$$\widetilde{\mathcal{L}} = \{\beta_0 + \beta_1\lambda_1 + \cdots + \beta_n\lambda_n \ ; \ n \geq 0, \beta_i \in \overline{\mathbf{Q}}, \ \lambda_i \in \mathcal{L}\}.$$

Theorem (D.Roy). *If* x_1, x_2 *are* $\overline{\mathbf{Q}}$*–linearly independent complex numbers and* y_1, y_2, y_3 *are* $\overline{\mathbf{Q}}$*–linearly independent complex numbers, then one at least of the six numbers*

$$x_1y_1, \ x_1y_2, \ x_1y_3, \ \ x_2y_1, \ x_2y_2, \ x_2y_3$$

is not in $\widetilde{\mathcal{L}}$.

The Strong Four Exponentials Conjecture

Conjecture. *If* x_1, x_2 *are* $\overline{\mathbf{Q}}$*–linearly independent complex numbers and* y_1, y_2 *are* $\overline{\mathbf{Q}}$*–linearly independent complex numbers, then one at least of the four numbers*

$$x_1y_1,\ x_1y_2,\ \ x_2y_1,\ x_2y_2$$

is not in $\widetilde{\mathcal{L}}$.

Lower bound for the rank of matrices

- Rank of matrices. An alternate form of the strong Six Exponentials Theorem (resp. the strong Four Exponentials Conjecture) is the fact that *a* 2×3 *(resp.* 2×2*) matrix with entries in* $\widetilde{\mathcal{L}}$

$$\begin{pmatrix}\Lambda_{11} & \Lambda_{12} & \Lambda_{13}\\ \Lambda_{21} & \Lambda_{22} & \Lambda_{23}\end{pmatrix} \qquad \textit{(resp.} \begin{pmatrix}\Lambda_{11} & \Lambda_{12}\\ \Lambda_{21} & \Lambda_{22}\end{pmatrix} \qquad \textit{),}$$

  the rows of which are linearly independent over $\overline{\mathbf{Q}}$ *and the columns of which are also linearly independent over* $\overline{\mathbf{Q}}$*, has maximal rank* 2.

The strong Six Exponentials Theorem

References :

- D. Roy – « Matrices whose coefficients are linear forms in logarithms », *J. Number Theory* **41** (1992), no. 1, p. 22–47.

- M. Waldschmidt – *Diophantine approximation on linear algebraic groups*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. **326**, Springer-Verlag, Berlin, 2000.

Diophantine Approximation

- Liouville's Theorem : *for any real algebraic number* α *there exists a constant* $c > 0$ *such that the set of* $p/q \in \mathbf{Q}$ *with* $|\alpha - p/q| < q^{-c}$ *is finite.*

- Liouville's Theorem yields the transcendence of the value of a series like $\sum_{n\geq 0} 2^{-u_n}$, provided that the sequence $(u_n)_{n\geq 0}$ is increasing and satisfies

$$\limsup_{n\to\infty} \frac{u_{n+1}}{u_n} = +\infty.$$

- For instance $u_n = n!$ satisfies this condition : hence the number $\sum_{n\geq 0} 2^{-n!}$ is transcendental.

Roth's Theorem

- Roth's Theorem : *for any real algebraic number* α, *for any* $\epsilon > 0$, *the set of* $p/q \in \mathbf{Q}$ *with* $|\alpha - p/q| < q^{-2-\epsilon}$ *is finite.*
- Roth's Theorem yields the transcendence of $\sum_{n\geq 0} 2^{-u_n}$ under the weaker hypothesis

$$\limsup_{n\to\infty} \frac{u_{n+1}}{u_n} > 2.$$

- The sequence $u_n = [2^{\theta n}]$ satisfies this condition as soon as $\theta > 1$. For example the number

$$\sum_{n\geq 0} 2^{-3^n}$$

is transcendental.

Transcendence of $\sum_{n\geq 0} 2^{-2^n}$

- A stronger result follows from Ridout's Theorem, using the fact that the denominators 2^{u_n} are powers of 2 : the condition
$$\limsup_{n\to\infty} \frac{u_{n+1}}{u_n} > 1$$
suffices to imply the transcendence of the sum of the series $\sum_{n\geq 0} 2^{-u_n}$
- Since $u_n = 2^n$ satisfies this condition, the transcendence of $\sum_{n\geq 0} 2^{-2^n}$ follows (Kempner 1916).
- Ridout's Theorem : *for any real algebraic number* α*, for any* $\epsilon > 0$*, the set of* $p/q \in \mathbf{Q}$ *with* $q = 2^k$ *and* $|\alpha - p/q| < q^{-1-\epsilon}$ *is finite.*

Schmidt's subspace Theorem

For $\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbf{Z}^m$, set
$|\mathbf{x}| = \max\{|x_0|, \ldots, |x_{m-1}|\}$.
W.M. Schmidt (1970). *Let* $m \geq 2$ *and* $L_0, \ldots, L_{m-1}$ *a set of* m *linearly independent forms in* m *variables with algebraic coefficients. Let* $\epsilon > 0$. *Then the set*

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

is contained in the union of finitely many proper subspaces of $\mathbf{Q}^m$.

A consequence of Schmidt's subspace Theorem

Thue-Siegel-Roth. *Let* α *be an algebraic number. For any* $\epsilon > 0$, *the set of* $p/q \in \mathbf{Q}$ *satisfying* $|\alpha - p/q| \le q^{-2-\epsilon}$ *is finite.*

Proof : In Schmidt's subspace Theorem, take $m = 2$, $L_0(x_0, x_1) = x_0$, $L_1(x_0, x_1) = \alpha x_0 - x_1$.

The condition

$$|L_0(\mathbf{x})L_1(\mathbf{x})| \le |\mathbf{x}|^{-\epsilon}$$

corresponds to

$$q|q\alpha - p| \le q^{-\epsilon}.$$

Schmidt's subspace Theorem

W.M. Schmidt (1970). *Let* $m \geq 2$ *be a positive integer,* S *a finite set of places of* $\mathbf{Q}$ *containing the infinite one. For each* $v \in S$*, let* $L_{0,v}, \ldots, L_{m-1,v}$ *be a system of* m *linearly independent linear forms in* m *variables, with algebraic coefficients in the completion of* $\mathbf{Q}$ *at* v*. Let* $\epsilon > 0$*. Then the set of* $\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbf{Z}^m$ *for which*

$$\prod_{v \in S} |L_{0,v}(\mathbf{x}) \cdots L_{m-1,v}(\mathbf{x})|_v \leq |\mathbf{x}|^{-\epsilon}$$

is contained in the union of finitely many proper subspaces of $\mathbf{Q}^m$.

Ridout's Theorem

Ridout. *For any algebraic number* α, *for any* $\epsilon > 0$, *the set of* $p/q \in \mathbf{Q}$ *with* $q = 2^k$ *and* $|\alpha - p/q| < q^{-1-\epsilon}$ *is finite.*

Proof : In Schmidt's subspace Theorem, take $m = 2$, $S = \{\infty,\ 2\}$,

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

For $(x_0, x_1) = (q, p)$ with $q = 2^k$, we have

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

Mahler's method

Transcendence of $\sum_{n\geq 0} 2^{-2^n}$:

Mahler (1930, 1969) : the function $f(z) = \sum_{n\geq 0} z^{-2^n}$ satisfies $f(z^2) + z = f(z)$ for $|z| < 1$.

K. Kubota
J.H. Loxton and A.J. van der Poorten (1982–1988).

Mahler's method vs Schmidt's Subspace Theorem

P.G. Becker (1994) : *for any given non–eventually periodic automatic sequence* $\mathbf{u} = (u_1, u_2, \dots)$, *the real number*

$$\sum_{k\geq 1} u_k g^{-k}$$

is transcendental, provided that the integer g *is sufficiently large (in terms of* $\mathbf{u}$*).*

• **Theorem** *(*B. Adamczewski, Y. Bugeaud, F. Luca, *2004* –conjecture of A. Cobham, 1968) : *The sequence of digits in a basis* $g \geq 2$ *of an irrational algebraic number is not automatic.*

More on Mahler's method

- K. Nishioka (1991) : algebraic independence measures for the values of Mahler's functions.
- For any integer $d \geq 2$,

$$\sum_{n\geq 0} 2^{-d^n}$$

is a S–number in the classification of transcendental numbers due to... Mahler.

- Reference : K. Nishioka, *Mahler functions and transcendence*, Lecture Notes in Math. **1631**, Springer Verlag, 1996.

Further developments

Transcendence and algebraic independence of values of modular functions (*méthode stéphanoise* and work of Yu.V. Nesterenko).

Measures : transcendence, linear independence, algebraic independence...

Finite characteristic :

Federico Pellarin - *Aspects de l'indépendance algébrique en caractéristique non nulle [d'après Anderson, Brownawell, Denis, Papanikolas, Thakur, Yu,...]*
Séminaire Nicolas Bourbaki, Dimanche 18 mars 2007.
http://www.bourbaki.ens.fr/seminaires/2007/Prog_mars.07.html

Historical introduction to transcendence

Michel Waldschmidt

http://www.math.jussieu.fr/~miw/