Diophantine approximation, irrationality and transcendence

Michel Waldschmidt

Course N°14, *June 2, 2010*

These are informal notes of my course given in April – June 2010 at IMPA (*Instituto Nacional de Matematica Pura e Aplicada*), Rio de Janeiro, Brazil.

From (134) with $c = 1$ and Lemma 137 we deduce that the remainder $R(z)$ in Hermite's fomula with parameters n_0 and n_1 and B monic is given by

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

Replacing t by tz yields:

Lemma 139. *The remainder $R(z)$ in Hermite's fomula with parameters n_0 and n_1 (and B monic) is given by*

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

An easy consequence of Lemma 139 is the estimate for the remainder term given in Lemma 128.

We now recover the explicit formulae for A and B which we derived in Proposition 127 in the context of Theorem 132.

When $S \in \mathbf{C}[[t]]$ is a power series, say

$$S(t) = \sum_{i\ge 0} s_i t^i,$$

and f an analytic complex valued function, we define

$$S(D)f = \sum_{i\ge 0} s_i D^i f,$$

and we shall use this notation only when the sum is finite: either S is a polynomial in $\mathbf{C}[t]$ or f is a polynomial in $\mathbf{C}[z]$.

We reproduce [5], Chap.I § 1: for two power series S_1 and S_2 and an analytic function f we have

$$(S_1+S_2)(D)f = S_1(D)f + S_2(D)f$$

and

$$(S_1S_2)(D)f = S_1(D)\bigl(S_2(D)f\bigr).$$

Also if $s_0 \neq 0$ then the series S has an inverse in the ring $\mathbf{C}[[t]]$, say

$$S^{-1}(t) = \sum_{i\geq 0} \sigma_i t^i, \quad (t_0 = 1/s_0)$$

and

$$S^{-1}(D)\bigl(S(D)f\bigr) = S(D)\bigl(S^{-1}(D)f\bigr) = f.$$

For instance with $S(t) = 1-t$ and $S^{-1}(t) = 1+t+t^2+\cdots$,

$$(1-D)\sum_{n\geq 0} D^n f = \sum_{n\geq 0} D^n(1-D)f = f.$$

If the power series S and the polynomial f have integer coefficients, then $S(D)f$ is also a polynomial with integer coefficients. The same holds also for $S^{-1}(D)f$ if, further, $s_0 = \pm 1$.

For $\lambda \in \mathbf{C}$ and $P \in \mathbf{C}[z]$, we have

$$D(e^{\lambda z}P) = e^{\lambda z}(\lambda + D)P.$$

Hence for $n \geq 1$,

$$D^n(e^{\lambda z}P) = e^{\lambda z}(\lambda + D)^n P$$

and $(\lambda + D)^n P$ is again a polynomial; further, it has the same degree as P when $\lambda \neq 0$. Conversely, assuming $\lambda \neq 0$, given a polynomial $Q \in \mathbf{C}[z]$, the unique solution $P \in \mathbf{C}[z]$ to the differential equation

$$(\lambda + D)^n P = Q$$

is

$$P = (\lambda + D)^{-n} Q$$

and this solution P is a polynomial of the same degree as Q. In the case $\lambda = \pm 1$, when Q has integer coefficients, then so does P.

We come back now to the solution (A, B, R) to the Padé problem (133) in Theorem 132, where $B \in \mathbf{C}[z]$ is monic of degree n_1 and $A \in \mathbf{C}[z]$ has degree n_0, while $R \in \mathbf{C}[[z]]$ has a zero of multiplicity $N+1$ at 0.

From

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

we deduce

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

From this formula it follows that B has integer coefficients. It is easy to explicit the polynomial B. From

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

we deduce

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

which can be written also as

$$B(z) = (-1)^{n_1}\frac{n_1!}{n_0!}\sum_{k=0}^{n_1}(-1)^k \frac{(N-k)!}{(n_1-k)!k!} z^k. \tag{140}$$

One checks that B is monic of degree n_1. This formula matches with Proposition 127 and the duality (136) between (n_0, n_1) and (n_1, n_0).

We can also check the formula for A starting from

$$D^{n_1+1}\bigl(A(z)e^{-z}\bigr) = -D^{n_1+1}\bigl(R(z)e^{-z}\bigr),$$

where the left hand side is the product of e^{-z} with a polynomial of degree $\le n_0$, while the right hand side has a multiplicity $\ge n_0$ at the origin. We deduce

$$D^{n_1+1}\bigl(A(z)e^{-z}\bigr) = az^{n_0}e^{-z}$$

where a is the leading coefficient of A. From

$$D^{n_1+1}\bigl(A(z)e^{-z}\bigr) = e^{-z}(-1+D)^{n_1+1}A(z)$$

we deduce

$$(-1+D)^{n_1+1}A(z) = -az^{n_0}$$

and

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

Hence the same computation as was done before for B will give the formula for A.

Thanks to these explicit formulae, we can express A and B in terms of hypergeometric series:

Lemma 141. *The numerator A_{n_0,n_1} and the denominator B_{n_0,n_1} of the Padé approximant of index (n_0, n_1) for the exponential function are given by hypergeometric polynomials*

$$A_{n_0,n_1}(z) = (-1)^{n_1} \frac{N!}{n_0!} \; {}_1F_1(-n_0; -N; z)$$

and

$$B_{n_0,n_1}(z) = (-1)^{n_1} \frac{N!}{n_0!} \; {}_1F_1(-n_1; -N; -z).$$

Proof. The proofs for both formulae are similar – in fact (136) shows that they are equivalent. Consider

$$A_{n_0,n_1}(z) = (-1)^{n_1} \sum_{k=0}^{n_0} \frac{(N-k)!}{(n_0-k)!k!} \cdot z^k$$

and write

$$(-n_0)_k = (-1)^k \frac{n_0!}{(n_0-k)!} \quad \text{and} \quad (-N)_k = (-1)^k \frac{N!}{(N-k)!}.$$

Then

$$A_{n_0,n_1}(z) = (-1)^{n_1} \frac{N!}{n_0!} \sum_{k=0}^{n_0} \frac{(-n_0)_k}{(-N)_k k!} \cdot z^k = (-1)^{n_1} \frac{N!}{n_0!} \; {}_1F_1(-n_0; -N; z).$$

□

One can find the explicit values of these polynomials on the internet by looking for *Padé table for the exponential function*. Here is the table for B_{n_0,n_1} – the table for A_{n_0,n_1} is easy to deduce from (136).

n_0 \ n_1	0	1	2	3
0	1	$z-1$	z^2-2z+2	z^3-3z^2+6z-6
1	1	$z-2$	z^2-4z+6	$z^3-6z^2+18z-24$
2	1	$z-3$	$z^2-6z+12$	$z^3-9z^2+36z-60$
3	1	$z-4$	$z^2-8z+20$	$z^3-12z^2+60z-120$

These polynomials are also useful for giving continued fractions expressions for the exponential function.

8.3 Hermite's transcendence proof

In 1873 C. Hermite [3] proved that the number e is transcendental. In his paper he explains in a very clear way how he found his proof. He starts with an analogy between simultaneous diophantine approximation of real numbers on the one hand and analytic complex functions of one variable on the other. He first solves the analytic problem by constructing explicitly what is now called Padé approximants for the exponential function. In fact there are two types of such approximants, they are now called type I and type II, and what Hermite did in 1873 was to compute Padé approximants of type II. He also found those of type I in 1873 and studied them later in 1893. K. Mahler was the first in the mid's 1930 to relate the properties of the two types of Padé's approximants and to use those of type I in order to get a new proof of Hermite's transcendence Theorem (and also of the generalisation by Lindemann and Weierstraß as well as quantitative refinements). See [2] Chap. 2 § 3.

In the analogy with number theory, Padé approximants of type II are related with the simultaneous approximation of real numbers $\vartheta_1, \ldots, \vartheta_m$ by rational numbers p_i/q with the same denominator q (one does not require that the fractions are irreducible), which means that we wish to estimate

$$\max_{1\le i\le m}\left|\vartheta_i - \frac{p_i}{q}\right|$$

in terms of q, while type I is related with the study of estimates for linear combinations

$$|a_0 + a_1\vartheta_1 + \cdots + a_m\vartheta_m|$$

when $a_0, \ldots, a_m$ are rational integers, not all of which are 0, in terms of the number $\max_{0\le i\le m}|a_i|$.

We explained Hermite's strategy in § 3.1: in order to apply the criterion for linear independence Proposition 14 and obtain the linear independence over $\mathbf{Q}$ of $1, e, e^2, \ldots$ (and therefore the transcendence of e), Hermite first "approximates" simultaneously the functions $e^z, e^{2z}, \ldots$ by rational fractions P_1/Q, P_m/Q, and then substitutes $z = 1$.

8.3.1 Padé approximants

Henri Eugène Padé (1863–1953), who was a student of Charles Hermite (1822–1901), gave his name to the following objects which he studied thoroughly in his thesis in 1892 (for a complete historical survey of the theory, see [1]).

Lemma 142. *Let $f_1, \dots, f_m$ be analytic functions of one complex variable near the origin. Let $n_0, n_1, \dots, n_m$ be non-negative integers. Set*

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

Then there exists a tuple $(Q, P_1, \dots, P_m)$ 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 $\geq N + 1$.

Definition. *A tuple $(Q, P_1, \dots, P_m)$ of polynomials in $\mathbf{C}[X]$ satisfying the condition of Lemma 142 is called a* Padé system of the second type for $(f_1, \dots, f_m)$ attached to the parameters $n_0, n_1, \dots, n_m$.

Proof. The polynomial Q of Lemma 142 should have degree $\leq N - n_0$, so we have to find (or rather to prove the existence of) its $N - n_0 + 1$ coefficients, not all being zero. We consider these coefficients as unknowns. The property we require is that for $1 \leq \mu \leq m$, the Taylor expansion at the origin of $Q(x)f_\mu(x)$ has zero coefficients for $x^{N-n_\mu+1}, x^{N-n_\mu+1}, \dots, x^N$. If this property holds for $1 \leq \mu \leq m$, we shall define P_μ by truncating the Taylor series at the origin of $Q(x)f_\mu(x)$ at the rank x^{N-n_μ}, hence P_μ will have degree $\leq N - n_\mu$, while the remainder $Q(x)f_\mu(x) - P_\mu(x)$ will have a mutiplicity $\geq N + 1$ at the origin.

Now for each given μ the condition we stated amounts to require that our unknowns (the coefficients of Q) satisfy n_μ homogeneous linear relations, namely

$$\left(\frac{d}{dx}\right)^k \left[Q(x)f_\mu(x)\right]_{x=0} = 0 \quad \text{for} \quad N - n_\mu < k \leq N.$$

Therefore altogether we get $n_1 + \cdots + n_m = N - n_0$ homogeneous linear equations, and since the number $N - n_0 + 1$ of unknowns (the coefficients of Q) is larger, linear algebra tells us that a non-trivial solution exists.

□

There is no unicity, because of the homogeneity of the problem: the set of solutions (together with the trivial solution 0) is a vector space over $\mathbf{C}$, and Lemma 142 tells us that it has positive dimension. In the case where this dimension is 1 (which means that there is unicity up to a multiplicative factor), the system of approximants is called *perfect*. An example is with $m = 1$ and $f(x) = e^x$, as shown by Hermite's work.

Here is the definition of the *Padé approximants of type I*:

Lemma 143. *Let $f_1, \ldots, f_m$ be analytic functions of one complex variable near the origin. Let $d_0, d_1, \ldots, d_m$ be non-negative integers. Set*

$$M = d_0 + d_1 + \cdots + d_m + m.$$

Then there exists a tuple $(A_0, \ldots, A_m)$ of polynomials in $\mathbf{C}[X]$, not all of which are zero, where A_i has degree $\leq d_i$, such that the function

$$A_0 + A_1 f_1 + \cdots + A_m f_m$$

has a zero at the origin of multiplicity $\geq M$.

Definition. *A tuple $(A_0, A_1, \ldots, A_m)$ of polynomials in $\mathbf{C}[X]$ satisfying the condition of Lemma 143 is called a* Padé system of the first type for $(f_1, \ldots, f_m)$ attached to the parameters $n_0, n_1, \ldots, n_m$.

Proof. The map from the product of linear spaces $\mathbf{C}[z]_{\leq n_0} \times \cdots \mathbf{C}[z]_{\leq n_m}$ to $\mathbf{C}^M$ which sends a tuple $(A_0, \ldots, A_m)$ to

$$\big(D^j (A_0 + A_1 f_1 + \cdots + A_m f_m)(0)\big)_{0 \leq j < M}$$

is not injective, and any non–zero element in the kernel satisfies the required property. □

In the case $m = 1$, the notions of Padé approximants of type I and II coincide – and an explicit solution has been given in the previous courses when $f_1(x) = e^x$.

Most often it is not easy to find explicit solutions: we only know their existence. As we are going to show, Hermite succeeded to produce explicit solutions for the systems of Padé approximants of type II for the functions $(e^x, e^{2x}, \ldots, e^{mx})$.

8.3.2 Hermite's identity

FromLemma 139 we deduce the value of the integral

$$\int_0^1 (1-t)^{n_0} t^{n_1} e^{tz} dt.$$

One can compute similar more general integrals, where $f(t) = (1-t)^{n_0} t^{n_1}$ is replaced by any polynomial. We start with a simple example.

Lemma 144. *Let f be a polynomial of degree $\leq N$. Define*

$$F = f + Df + D^2 + \cdots + D^N f.$$

Then for $z \in \mathbf{C}$

$$\int_0^z e^{-t} f(t)dt = F(0) - e^{-z}F(z).$$

We can also write the definition of F as

$$F = (1-D)^{-1} f \quad \text{where} \quad (1-D)^{-1} = \sum_{k\geq 0} D^k.$$

The series in the right hand side is infinite, but when we apply the operator to a polynomial only finitely many $D^k f$ are not 0: when f is a polynomial of degree $\leq N$ then $D^k f = 0$ for $k > N$.

Proof. More generally, if f is a complex function which is analytic at the origin and N is a positive integer, if we set

$$F = f + Df + D^2 + \cdots + D^N f,$$

then the derivative of $e^{-t}F(t)$ is $-e^{-t}f(t) + e^{-t}D^{N+1}f(t)$. □

A change of variables in Lemma 144 leads to a formula for

$$\int_0^u e^{-xt} f(t)dt$$

when x and u are complex numbers. Here, in place of using Lemma 144, we repeat the proof. Integrate by part $e^{-xt}f(t)$ between 0 and u:

$$\int_0^u e^{-xt} f(t)dt = -\left[\frac{1}{x} e^{-xt} f(t)\right]_0^u + \frac{1}{x}\int_0^u e^{-xt} f'(t)dt.$$

By induction we deduce

$$\int_0^u e^{-xt} f(t)dt = -\sum_{k=0}^m \left[\frac{1}{x^{k+1}} e^{-xt} D^k f(t)\right]_0^u + \frac{1}{x^{m+1}}\int_0^u e^{-xt} D^{m+1} f(t)dt.$$

Let N be an upper bound for the degree of f. For $m = N$ the last integral vanishes and

$$\begin{aligned}\int_0^u e^{-xt} f(t)dt &= -\sum_{k=0}^N \left[\frac{1}{x^{k+1}} e^{-xt} D^k f(t)\right]_0^u \\ &= \sum_{k=0}^N \frac{1}{x^{k+1}} D^k f(0) - e^{-xu} \sum_{k=0}^N \frac{1}{x^{k+1}} D^k f(u).\end{aligned}$$

Multipling by $x^{N+1}e^{ux}$ yields:

Lemma 145. *Let f be a polynomial of degree $\leq N$ and let x, u be complex numbers. Then*

$$e^{xu}\sum_{k=0}^{N} x^{N-k}D^k f(0) = \sum_{k=0}^{N} x^{N-k}D^k f(u) + x^{N+1}e^{xu}\int_0^u e^{-xt}f(t)dt.$$

With the notation of Lemma 145, the function

$$x \mapsto \int_0^u e^{-xt}f(t)dt$$

is analytic at $x = 0$, hence its product with x^{N+1} has a mutiplicity $\geq N+1$ at the origin. Moreover

$$Q(x) = \sum_{k=0}^{N} x^{N-k}D^k f(0) \quad \text{and} \quad P(x) = \sum_{k=0}^{N} x^{N-k}D^k f(u)$$

are polynomials in x.

If the polynomial f has a zero of multiplicity $\geq n_0$ at the origin, then Q has degree $\leq N - n_0$. If the polynomial f has a zero of multiplicity $\geq n_1$ at u, then P has degree $\leq N - n_1$.

For instance, in the case $u = 1$, $N = n_0 + n_1$, $f(t) = t^{n_0}(t-1)^{n_1}$, the two polynomials

$$Q(x) = \sum_{k=n_0}^{N} x^{N-k}D^k f(0) \quad \text{and} \quad P(x) = \sum_{k=n_1}^{N} x^{N-k}D^k f(1)$$

satisfy the properties which were required in section §8.1.1 (see Proposition 127), namely $R(z) = Q(z)e^z - P(z)$ has a zero of multiplicity $> n_0 + n_1$ at the origin, P has degree $\leq n_0$ and Q has degree $\leq n_1$.

Lemma 145 is a powerful tool to go much further.

Proposition 146. *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

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

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.

These polynomials $Q, P_1, \ldots, P_m$ are called the *Hermite-Padé polynomials attached to the parameters $n_0, n_1, \ldots, n_m$.*

Remark. If one wants to compare the formulae of § 8.1 with the special case $m = 1$ of Proposition 146, one should be aware that we shifted somewhat the notations: in § 8.1 we worked with $f(t) = t^{n_1}(1-t)^{n_0}$, while in Proposition 146 with $m = 1$ the polynomial which occurs is $f(t) = t^{n_0}(t-1)^{n_1}$.

Proof. The coefficient of x^{N-n_0} in the polynomial Q is $D^{n_0} f(0)$, so it is not zero since f has mutiplicity exactly n_0 at the origin. Similarly for $1 \leq \mu \leq m$ the coefficient of x^{N-n_μ} in P_μ is $D^{n_0} f(\mu) \neq 0$.

The assertion on the integrality of the coefficients follows from the next lemma.

Lemma 147. *Let f be a polynomial with integer coefficients and let k be a non-negative integer. Then the polynomial $(1/k!)D^k f$ has integer coefficients.*

Proof. If $f(X) = \sum_{n \geq 0} a_n X^n$ then

$$\frac{1}{k!} D^k f = \sum_{n \geq 0} a_n \binom{n}{k} X^n \quad \text{with} \quad \binom{n}{k} = \frac{n!}{k!(n-k)!},$$

and the binomial coefficients are rational integers. □

From Lemma 147 it follows that for any polynomial $f \in \mathbf{Z}[X]$ and for any integers k and n with $n \geq k$, the polynomial $(1/k!)D^n f$ also belongs to $\mathbf{Z}[X]$. This completes the proof of Proposition 146.

□