Fields Institute University of Ottawa, Ontario Canada June 30 – July 4, 2008
http://www.fields.utoronto.ca/programs/scientific/07-08/analytic/
`updated:` August 4, 2008

Summer School in Analytic Number Theory and Diophantine Approximation

An Introduction to Irrationality and Transcendence Methods.

Michel Waldschmidt

1 Irrationality of some constants arising from analysis

1.1 Irrationality and continued fractions

The history of irrationality is closely connected with the history of continued fractions (see [3, 4]). Even the first examples of transcendental numbers produced by Liouville in 1844 [17] involved continued fractions, before he considered series.

Recall that the definition of the continued fraction expansion of a real number.

Given a real number x, the Euclidean division in $\mathbb{R}$ of x by 1 yields a quotient $[x] \in \mathbb{Z}$ (the *integral part of* x) and a remainder $\{x\}$ in the interval $[0, 1)$ (the *fractional part of* x) satisfying

$$x = [x] + \{x\}.$$

Set $a_0 = [x]$. Hence $a_0 \in \mathbb{Z}$. If x is an integer then $x = [x] = a_0$ and $\{x\} = 0$. In this case we just write $x = a_0$ with $a_0 \in \mathbb{Z}$. Otherwise we have $\{x\} > 0$ and we set $x_1 = 1/\{x\}$ and $a_1 = [x_1]$. Since $\{x\} < 1$ we have $x_1 > 1$ and $a_1 \geq 1$. Also

$$x = a_0 + \frac{1}{a_1 + \{x_1\}}\cdot$$

Again, we consider two cases: if $x_1 \in \mathbb{Z}$ then $\{x_1\} = 0$, $x_1 = a_1$ and

$$x = a_0 + \frac{1}{a_1}$$

with two integers a_0 and a_1, with $a_1 \geq 2$ (recall $x_1 > 1$). Otherwise we can define $x_2 = 1/\{x_1\}$, $a_2 = [x_2]$ and go one step further:

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \{x_2\}}}\cdot$$

Inductively one obtains a relation

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; a_{n-1} + \cfrac{1}{a_n + \{x_n\}}}}}$$

with $0 \le \{x_n\} < 1$. For ease of notation we write either

$$x = [a_0, a_1, a_2, \dots, a_{n-1}, a_n + \{x_n\}]$$

or

$$x = a_0 + \frac{1\,|}{|a_1} + \frac{1\,|}{|a_2} + \;\cdots\; + \frac{1\;\;|}{|a_{n-1}} + \frac{1\qquad|}{|a_n + \{x_n\}}\cdot$$

This last notation is mainly used for *irregular* continued fractions[1].

It is easy to check that a real number is rational if and only if its continued fraction expansion is finite. This criterion is most often more convenient to use than to check whether the expansion in a basis $b \ge 2$ is periodic or not.

The question of the irrationality of π was raised in India by Nīlakaṇṭha Somayājī, who was born around 1444 AD. In his comments on the work of Āryabhaṭa, (b. 476 AD) who stated that an approximation for π is $\pi \sim 3.1416$, Somayājī asks [19]:

> *Why then has an approximate value been mentioned here leaving behind the actual value? Because it (exact value) cannot be expressed.*

In 1767, H. Lambert [14] found the following continued fraction expansion for the tangent function:

$$\tan x = \frac{x|}{|1} - \frac{x^2|}{|\,3} - \frac{x^2|}{|\,5} - \frac{x^2|}{|\,7} - \cdots - \frac{x^2\quad|}{|2n+1} - \cdots \qquad (1.1)$$

Here is how this irregular continued fraction occurs. Given two functions $A_0(x)$ and $A_1(x)$, define inductively

$$A_{n+1}(x) = (2n+1)A_n(x) - x^2 A_{n-1}(x) \quad (n \ge 1)$$

and set $u_n(x) = A_n(x)/A_{n-1}(x)$ $(n \ge 1)$. Hence

$$u_n(x) = \frac{A_n(x)}{A_{n-1}(x)} = -\frac{x^2 A_n(x)}{(2n+1)A_n(x) - A_{n+1}} = -\frac{x^2}{(2n+1) - u_{n+1}(x)}\cdot$$

---

[1] A continued fraction expansion of the form

$$x = a_0 + \frac{b_1|}{|a_1} + \frac{b_2|}{|a_2} + \;\cdots\; \frac{b_{n-1}|}{|a_{n-1}} + \frac{b_n|}{|a_n} + \cdots$$

is called "*regular*" if $b_1 = b_2 = \cdots = b_n = 1$.

Therefore, for $k \geq 1$,

$$u_n(x) = -\frac{x^2 \mid}{\mid 2n+1} - \frac{x^2 \mid}{\mid 2n+3} - \frac{x^2 \mid}{\mid 2n+5} - \cdots - \frac{x^2 \mid}{\mid 2n+2k+1} - u_{n+k+1}(x).$$

The main point is to see that the right hand side has a limit as $n \to \infty$ for a suitable choice of A_0 and A_1, namely

$$A_0(x) = \sin x, \quad A_1(x) = \sin x - x\cos x.$$

For this particular choice the sequence $(A_n)_{n\geq 0}$ is given by the integral formula

$$A_n(x) = \int_0^x tA_{n-1}(t)dt \quad (n \geq 1)$$

and there are sequences of polynomials f_n and g_n in $\mathbb{Z}[x]$ such that

$$A_n(x) = f_n(x)\sin x + g_n(x)\cos x.$$

Using these properties, one checks (see for instance [9]) that the continued fraction expansion is convergent; since

$$u_1(x) = 1 - \frac{x}{\tan x},$$

one deduces

$$\tan x = \frac{x}{1-u_1(x)} \quad \text{with} \quad u_1(x) = -\frac{x^2 \mid}{\mid 3} - \frac{x^2 \mid}{\mid 5} - \frac{x^2 \mid}{\mid 7} - \cdots$$

This proves the formula (1.1).

Replacing x by ix yields the continued fraction expansion

$$\frac{e^x - e^{-x}}{e^x + e^{-x}} = \frac{x \mid}{\mid 1} + \frac{x^2 \mid}{\mid 3} + \frac{x^2 \mid}{\mid 5} + \frac{x^2 \mid}{\mid 7} + \cdots + \frac{x^2 \mid}{\mid 2n+1} + \cdots$$

involving the inductive relation

$$A_{n+1}(x) = (2n+1)A_n(x) + x^2 A_{n-1}(x) \quad (n \geq 1)$$

and the quotients $-A_n(x)/A_{n-1}(x)$. With the initial values

$$A_0(x) = e^x - 1, \quad A_1(x) = e^x(2-x) - 2 - x$$

the solution is

$$A_n(x) = \frac{x^{2n+1}}{n!} \int_0^1 e^{-tx} t^n (1-t)^{\cdot} dt.$$

Compare with Hermite's formulae in § 1.4. See also for instance [4] as well as [9, 21, 23].

Lambert proved in his paper [14] that for x rational and non–zero, the number $\tan x$ cannot be rational. Since $\tan \pi/4 = 1$, it follows that π is irrational. Then he produced a continued fraction expansion for e^x and deduced that e^r is irrational when r is a non–zero rational number. This is equivalent to the fact that non–zero positive rational numbers have an irrational logarithm. A detailed description of Lambert's proof is given in [9].

Euler gave continued fractions expansions not only for e and e^2:

$$
\begin{aligned}
e &= [2,\ \overline{1, 2j,\ 1}]_{j\geq 1} = [2,\ 1,\ 2,\ 1,\ 1,\ 4,\ 1,\ 1,\ 6,\ 1\ldots], \qquad (1.2)\\
e^2 &= [7,\ \overline{3j-1,\ 1,\ 3j,\ 12j+6}]_{j\geq 1} = [7\ 2,\ 1,\ 3,\ 18,\ 5,\ 1,\ 6,\ 30,\ 18\ldots],
\end{aligned}
$$

but also for $(e+1)/(e-1)$, for $(e^2+1)/(e^2-1)$, for $e^{1/n}$ with $n > 1$, for $e^{2/n}$with odd $n > 1$ and Hurwitz (1896) for $2e$ and $(e+1)/3$:

$$
\begin{aligned}
\frac{e+1}{e-1} &= [\overline{2(2j+1)}]_{j\geq 0} = [2,\ 6,\ 10,\ 14\ldots],\\
\frac{e^2+1}{e^2-1} &= [\overline{2j+1}]_{j\geq 0} = [1,\ 3,\ 5,\ 7\ldots],\\
e^{1/n} &= [\overline{1,\ (2j+1)n-1,\ 1}]_{j\geq 0},\\
e^{2/n} &= [\overline{1,\ (n-1)/2+3jn,\ 6n+12jn,\ (5n-1)/2+3jn,\ 1}]_{j\geq 0},\\
2e &= [5,\ 2,\ \overline{3,\ 2j,\ 3,\ 1,\ 2j,\ 1}]_{j\geq 1},\\
\frac{e+1}{3} &=\\
&[1,\ 4, \overline{5,\ 4j-3,\ 1,\ 1,\ 36j-16,\ 1,\ 1,\ 4j-2,\ 1,\ 1,\ 36j-4,\ 1,\ 1,\ 4j-1,\ 1,\ 5,\ 4j,\ 1}]_{j\geq 1}.
\end{aligned}
$$

Hermite proved the irrationality of π and π^2 (see [4] p. 207 and p. 247). Also A.M. Legendre proved, in 1794, by a modification of Lambert's proof, that π^2 is an irrational number (see [4] p. 14).

There are not so many numbers for which one knows the irrationality but we don't know whether there are algebraic or transcendental. A notable exception is $\zeta(3)$, known to be irrational (Apéry, 1978) and expected to be transcendental - see [11].

1.2 Variation on a proof by Fourier (1815)

Since the continued fraction expansion (1.2) of e, which was known by L. Euler in 1737 [8, 6, 21, 23, 3], is infinite, the number e is irrational. Since it is not ultimately periodic, e is not a quadratic irrationality, as was shown by Lagrange in 1770 – Euler knew already in 1737 that a number with an ultimately periodic continued fraction expansion is quadratic (see [8, 5, 20]).

Exercise 1.3. *a) Let b be a positive integer. Give the continued fraction expansion of the number*

$$\frac{-b+\sqrt{b^2+4}}{2}.$$

b) Let a and b be two positive integers. Write a degree 2 polynomial with integer coefficients having a root at the real number whose continued fraction expansion is

$$[0, \overline{a, b}].$$

c) Let a, b and c be positive integers. Write a degree 2 polynomial with integer coefficients having a root at the real number whose continued fraction expansion is

$$[0, \overline{a, b, c}].$$

The following easier and well known proof of the irrationality of e (§ 1.2.1) was given by J. Fourier in his course at the École Polytechnique in 1815. Later, in 1872, C. Hermite proved that e is transcendental, while the work of F. Lindemann a dozen of years later led to a proof of the so-called Hermite–Lindemann Theorem 2.1: *for any nonzero algebraic number α the number e^α is transcendental.* However for this first section we study only weaker statements which are very easy to prove. We also show that Fourier's argument can be pushed a little bit further than what is usually done, as pointed out by J. Liouville in 1840 [15, 16].

1.2.1 Irrationality of e

We truncate the exponential series giving the value of e at some point N:

$$N!\, e - \sum_{n=0}^{N} \frac{N!}{n!} = \sum_{k\geq 1} \frac{N!}{(N+k)!}\cdot \qquad (1.4)$$

The right hand side of (1.4) is a sum of positive numbers, hence is positive (not zero). From the lower bound (for the binomial coefficient)

$$\frac{(N+k)!}{N!k!} \geq N+1 \quad \text{for } k\geq 1,$$

one deduces

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

Therefore the right hand side of (1.4) tends to 0 when N tends to infinity. Since $\sum_{n=0}^{N} N!/n!$ is an integer, it follows that for any positive integer N the number $N!e$ is not an integer. Hence e is an irrational number.

As pointed out by F. Beukers, a simpler proof is obtained by considering the expansion of the Taylor series at $z = -1$ rather than at $z = 1$: with the expansion of e^{-1} no computation is required for estimating the error term, since it is alternate.

1.2.2 The number e is not quadratic

.

The fact that e is not a rational number implies that for each $m \geq 1$ the number $e^{1/m}$ is not rational. To prove that e^2 is also irrational is not so easy (see the comment on this point in [1]).

The proof below is essentially the one given by J. Liouville in 1840 [15] which is quoted by Ch. Hermite in [13] ("*ces travaux de l'illustre géomètre*").

To prove that e does not satisfy a quadratic relation $ae^2 + be + c$ with a, b and c rational integers, not all zero, requires some new trick. Indeed if we just mimic the argument of § 1.1, we get

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

The left hand side is a rational integer, but the right hand side tends to infinity (and not 0) with N, so we draw no conclusion.

Liouville writes the quadratic relation as $ae + b + ce^{-1} = 0$. He deduces

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

Again the left hand side is a rational integer, but now the right hand side tends to 0 when N tends to infinity, which is what we expected. However a further argument is necessary to conclude: we do not yet get the desired conclusion, we only deduce that both sides vanish. Now let us look more closely to the series in the right hand side. Write the two first terms A_N for $k = 0$ and B_N for $k = 1$:

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

with

$$A_N = \left(a - (-1)^N c\right) \frac{1}{N+1}, \qquad B_N = \left(a + (-1)^N c\right) \frac{1}{(N+1)(N+2)}$$

and

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

The above proof that the sum $A_N + B_N + C_N$ tends to zero as N tends to infinity shows more: each of the three sequences

$$\big(A_N\big)_{N \geq 1}, \quad \big((N+1)B_N\big)_{N \geq 1}, \quad \big((N+1)(N+2)C_N\big)_{N \geq 1}$$

tends to 0 as N tends to infinity. From the fact that the sum $A_N + B_N + C_N$ vanishes for all sufficiently large N, it easily follows that for all sufficiently large N, each of the three terms A_N, B_N and C_N also vanishes, hence $a - (-1)^N c$ and $a + (-1)^N c$ vanish, therefore $a = c = 0$, and finally $b = 0$.

Exercise 1.5. *Let $(a_n)_{n\geq 0}$ be a bounded sequence of rational integers. Prove that the following conditions are equivalent:*
(i) The number

$$\vartheta_1 = \sum_{n\geq 0} \frac{a_n}{n!}$$

is rational.
(ii) There exists $N_0 > 0$ such that $a_n = 0$ for all $n \geq N_0$.

1.2.3 Irrationality of $e^{\sqrt{2}}$

We follow here a suggestion of D.M. Masser and use Fourier's argument to prove the irrationality of $e^{\sqrt{2}}$.

The trick here is to prove the stronger statement that $\vartheta = e^{\sqrt{2}} + e^{-\sqrt{2}}$ is an irrational number.

Summing the two series

$$e^{\sqrt{2}} = \sum_{n\geq 0} \frac{2^{n/2}}{n!} \quad \text{and} \quad e^{-\sqrt{2}} = \sum_{n\geq 0} (-1)^n \frac{2^{n/2}}{n!},$$

we deduce

$$\vartheta = 2\sum_{m\geq 0} \frac{2^m}{(2m)!}\cdot$$

Let N be a sufficiently large integer. Then

$$\frac{(2N)!}{2^N}\vartheta - 2\sum_{m=0}^{N} \frac{(2N)!}{2^{N-m}(2m)!} = 4\sum_{k\geq 0} \frac{2^k(2N)!}{(2N+2k+2)!}\cdot \tag{1.6}$$

The right hand side of (1.6) is a sum of positive numbers, in particular it is not 0. Moreover the upper bound

$$\frac{(2N)!}{(2N+2k+2)!} \leq \frac{1}{(2N+2)(2k+1)!}$$

shows that the right hand side of (1.6) is bounded by

$$\frac{2}{N+1}\sum_{k\geq 0} \frac{2^k}{(2k+1)!} < \frac{\sqrt{2}e^{\sqrt{2}}}{N+1},$$

hence tends to 0 as N tends to infinity.

It remains to check that the coefficients $(2N)!/2^N$ and $(2N)!/2^{N-m}(2m)!$ $(0 \leq m \leq N)$ which occur in the left hand side of (1.6) are integers. The first one is nothing else than the special case $m = 0$ of the second one. Now for $0 \leq m \leq N$ the quotient

$$\frac{(2N)!}{(2m)!} = (2N)(2N-1)(2N-2)\cdots(2m+2)(2m+1)$$

is the product of $2N-2m$ consecutive integers, $N-m$ of which are even; hence it is an integral multiple of 2^{N-m}.

The same proof shows that the number $\sqrt{2}(e^{\sqrt{2}}-e^{-\sqrt{2}})$ is also irrational, but the argument does not seem to lead to the conclusion that $e^{\sqrt{2}}$ is not a quadratic number.

1.2.4 The number e^2 is not quadratic

The proof below is the one given by J. Liouville in 1840 [16]. See also [7].

We saw in § 1.2.2 that there was a difficulty to prove that e is not a quadratic number if we were to follow too closely Fourier's initial idea. Considering e^{-1} provided the clue. Now we prove that e^2 is not a quadratic number by truncating the series at carefully selected places. Consider a relation $ae^4+be^2+c=0$ with rational integer coefficients a, b and c. Write it $ae^2+b+ce^{-2}=0$. Hence

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

Like in § 1.2.2, the right hand side tends to 0 as N tends to infinity, and if the two first terms of the series vanish for some value of N, then we conclude $a=c=0$. What remains to be proved is that the numbers

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

are integers. For $n=0$ this is the coefficient of b, namely $2^{-N+1}N!$. The fact that these numbers are integers is not true for all values of N, it is not true even for all sufficiently large N; but we do not need so much, it suffices that they are integers for infinitely many N, and that much is true.

The exponent $v_p(N!)$ of p in the prime decomposition of $N!$ is given by the (finite) sum (see for instance [12])

$$v_p(N!)=\sum_{j\geq 1}\left[\frac{N}{p^j}\right]. \tag{1.7}$$

Using the trivial upper bound $[m/p^j]\leq m/p^j$, we deduce the upper bound

$$v_p(n!)\leq\frac{n}{p-1}$$

for all $n\geq 0$. In particular $v_2(n!)\leq n$. On the other hand, when N is a power of p, say $N=p^t$, then (1.7) yields

$$v_p(N!)=p^{t-1}+p^{t-2}+\cdots+p+1=\frac{p^t-1}{p-1}=\frac{N-1}{p-1}\cdot$$

Therefore, when N is a power of 2, the number $N!$ is divisible by 2^{N-1} and we have, for $0\leq m\leq N$,

$$v_2(N!/n!)\geq N-n-1,$$

which means that the numbers $N!/2^{N-n-1}n!$ are integers.

Exercise 1.8. *Let $(a_n)_{n\geq 0}$ be a bounded sequence of rational integers. Prove that the following conditions are equivalent:*
(i) The number

$$\vartheta_2 = \sum_{n\geq 0} \frac{a_n 2^n}{n!}$$

is rational.
(ii) There exists $N_0 > 0$ such that $a_n = 0$ for all $n \geq N_0$.
(Compare with Exercise 1.5).

The irrationality of e^2 follows from Exercise 1.8 with $a_n = 1$ for all n and the irrationality of $e^{\sqrt{2}}$ with

$$a_n = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ 1 & \text{if } n \text{ is even.} \end{cases}$$

1.2.5 The number $e^{\sqrt{3}}$ is irrational

Set $\vartheta = e^{\sqrt{3}} + e^{-\sqrt{3}}$. From the series expansion of the exponential function we derive

$$\frac{(2N)!}{3^{N-1}}\vartheta - 2\sum_{m=0}^{N} \frac{(2N)!}{(2m)!3^{N-m-1}} = 2\sum_{k\geq 0} \frac{3^k(2N)!}{(2N+2k+2)!}.$$

Take N of the form $(3^t+1)/2$ for some sufficiently large integer t. We deduce from (1.7) with $p = 3$

$$v_3((2N)!) = \frac{3^t-1}{2} = N-1, \quad v_3((2m)!) \leq m, \quad (0 \leq m \leq N)$$

hence $v_3((2N)!/(2m)!) \geq N - m - 1$.

1.2.6 Is-it possible to go further?

The same argument does not seem to yield the irrationality of e^3 (a proof using some particular continued fractions was given by Hurwitz in 1896 - see [3] p. 14–15). The range of applications of this method is limited. The main ideas allowing to go further have been introduced by Charles Hermite. They are basic for the development of transcendental number theory which we shall discuss in § 2.

1.3 Irrationality Criteria

The main tool in Diophantine approximation is the basic property that *any non-zero integer has absolute value at least* 1. There are many corollaries of this fact. We consider here is the following:
If ϑ is a rational number, there is a positive constant $c = c(\vartheta)$ such that, for any rational number p/q with $p/q \neq \vartheta$,

$$\left|\vartheta - \frac{p}{q}\right| \geq \frac{c}{q}. \tag{1.9}$$

This result is obvious: if $\vartheta = a/b$, then an admissible value for c is $1/b$, because the non-zero integer $aq - bp$ has absolute value at least 1.

This property is characteristic of rational numbers: a rational number cannot be well approximated by other rational numbers, while an irrational number can be well approximated by rational numbers.

1.3.1 First criterion

Lemma 1.10. *Let ϑ be a real number. The following conditions are equivalent*
(i) *ϑ is irrational.*
(ii) *For any $\epsilon > 0$ there exists $p/q \in \mathbb{Q}$ such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}\cdot$$

(iii) *For any real number $Q > 1$ there exists an integer q in the range $1 \le q < Q$ and a rational integer p such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{qQ}\cdot$$

(iv) *There exist infinitely many $p/q \in \mathbb{Q}$ such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{q^2}\cdot$$

So far we needed only (ii)⇒(i), which is the easiest part, as we just checked in (1.9).

According to this implication, in order to prove that some number is irrational, it is sufficient (and in fact also necessary) to produce good rational approximations. Lemma 1.10 tells us that an irrational real number ϑ has very good *friends* among the rational numbers, the sharp inequality (iv) shows indeed that ϑ is well approximated by rational numbers (and a sharper version of (iv), due to Hurwitz, will be proved in Lemma 1.12 below). Conversely, the proof we just gave shows that a rational number has *no good friend*, apart from himself. Hence in this world of rational approximation it suffices to have one good friend (not counting oneself) to guarantee that one has many very good friends.

The implication (i)⇒(iii) is a Theorem due to Dirichlet. We shall prove it in a more general form below (Lemma 1.17).

The next exercise extends the irrationality criterion Lemma 1.10 by replacing $\mathbb{Q}$ by $\mathbb{Q}(i)$. The elements in $\mathbb{Q}(i)$ are called the *Gaussian numbers*, the elements in $\mathbb{Z}(i)$ are called the *Gaussian integers*. The elements of $\mathbb{Q}(i)$ will be written p/q with $p \in \mathbb{Z}[i]$ and $q \in \mathbb{Z}$, $q > 0$.

Exercise 1.11. *Let ϑ be a complex number. Check that the following conditions are equivalent.*

(i) $\vartheta \notin \mathbb{Q}(i)$.
(ii) *For any* $\epsilon > 0$ *there exists* $p/q \in \mathbb{Q}(i)$ *such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}\cdot$$

(iii) *For any rational integer* $N \geq 1$ *there exists a rational integer* q *in the range* $1 \leq q \leq N^2$ *and a Gaussian integer* p *such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\sqrt{2}}{qN}\cdot$$

(iv) *There exist infinitely many Gaussian numbers* $p/q \in \mathbb{Q}(i)$ *such that*

$$\left|\vartheta - \frac{p}{q}\right| < \frac{\sqrt{2}}{q^{3/2}}\cdot$$

1.3.2 Hurwitz Theorem

The following result improves the implication (i)⇒(iv) of Lemma 1.10.

Lemma 1.12. *Let* ϑ *be a real number. The following conditions are equivalent*
(i) ϑ *is irrational.*
(ii) *There exist infinitely many* $p/q \in \mathbb{Q}$ *such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}\cdot$$

Of course the implication (ii)⇒(i) in Lemma 1.12 is weaker than the implication (iv)⇒(i) in Lemma 1.10. What is new is the converse.

Classical proofs of the equivalence between (i) and (ii) in Lemma 1.12 involve either continued fractions (see for instance [12], § 11.8, th. 193) or Farey series (see [20], Chap. I, §. 2). We give here a proof which does not involve continued fractions, but they occur implicitly.

Lemma 1.13. *Let* ϑ *be a real irrational number. Then there exists infinitely many pairs* $(p/q, r/s)$ *of irreducible fractions such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \textit{and} \quad qr - ps = 1.$$

In this statement and the next ones it is sufficient to prove inequalities $\leq$ in place of $<$: the strict inequalities are plain from the irrationality of ϑ.

Proof. Let H be a positive integer. Among the irreducible rational fractions a/b with $1 \leq b \leq H$, select one for which $|\vartheta - a/b|$ is minimal. If $a/b < \vartheta$ rename a/b as p/q, while if $a/b > \vartheta$, then rename a/b as r/s.

First consider the case where $a/b < \vartheta$, hence $a/b = p/q$. Since $\gcd(p, q) = 1$, using Euclidean's algorithm, one deduces (Bézout's Theorem) that there exist

$(r,s) \in \mathbb{Z}^2$ such that $qr - sp = 1$ with $1 \le s < q$ and $|r| < |p|$. Since $1 \le s < q \le H$, from the choice of a/b it follows that

$$\left|\vartheta - \frac{p}{q}\right| \le \left|\vartheta - \frac{r}{s}\right|,$$

hence r/s does not belong to the interval $[p/q, \vartheta]$. Since $qr - sp > 0$ we also have $p/q < r/s$, hence $\vartheta < r/s$.

In the second case where $a/b > \vartheta$ and $r/s = a/b$ we solve $qr - sp = 1$ by Euclidean algorithm with $1 \le q < s$ and $|p| < r$, and the argument is similar.

We now complete the proof of infinitely many such pairs. Once we have a finite set of such pairs $(p/q, r/s)$, we use the fact that there is a rational number m/n closer to ϑ than any of these rational fractions. We use the previous argument with $H \ge n$. This way we produce a new pair $(p/q, r/s)$ of rational numbers which is none of the previous ones (because one at least of the two rational numbers p/q, r/s is a better approximation than the previous ones). Hence this construction yields infinitely many pairs, as claimed.

□

Lemma 1.14. *Let ϑ be a real irrational number. Assume $(p/q, r/s)$ are irreducible fractions such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \textit{and} \quad qr - ps = 1.$$

Then

$$\min\left\{q^2\left(\vartheta - \frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s} - \vartheta\right)\right\} < \frac{1}{2}\cdot$$

Proof. Define

$$\delta = \min\left\{q^2\left(\vartheta - \frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s} - \vartheta\right)\right\}.$$

From

$$\frac{\delta}{q^2} \le \vartheta - \frac{p}{q} \quad \text{and} \quad \frac{\delta}{s^2} \le \frac{r}{s} - \vartheta$$

with $qr - ps = 1$ one deduces that the number $t = s/q$ satisfies

$$t + \frac{1}{t} \le \frac{1}{\delta}\cdot$$

Since the minimum of the function $t \mapsto t + 1/t$ is 2 and since $t \ne 1$, we deduce $\delta < 1/2$.

□

Remark. *The inequality $t + (1/t) \ge 2$ for all $t > 0$ with equality if and only if $t = 1$ is equivalent to the arithmetico-geometric inequality*

$$\sqrt{xy} \le \frac{x+y}{2},$$

when x and y are positive real numbers, with equality if and only if $x = y$. The correspondance between both estimates is $t = \sqrt{x/y}$.

From Lemmas 1.13 and 1.14 it follows that for $\vartheta \in \mathbb{R}\setminus\mathbb{Q}$, there exist infinitely many $p/q \in \mathbb{Q}$ such that
$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{2q^2}\cdot$$
A further step is required in order to complete the proof of Lemma 1.12.

Lemma 1.15. *Let ϑ be a real irrational number. Assume $(p/q, r/s)$ are irreducible fractions such that*
$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \textit{and} \quad qr - ps = 1.$$
Define $u = p + r$ and $v = q + s$. Then
$$\min\left\{q^2\left(\vartheta - \frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s} - \vartheta\right)\ ,\ v^2\left|\vartheta - \frac{u}{v}\right|\right\} < \frac{1}{\sqrt{5}}\cdot$$

Proof. First notice that $qu - pv = 1$ and $rv - su = 1$. Hence
$$\frac{p}{q} < \frac{u}{v} < \frac{r}{s}\cdot$$

We repeat the proof of Lemma 1.14 ; we distinguish two cases according to whether u/v is larger or smaller than ϑ. Since both cases are quite similar, let us assume $\vartheta < u/v$. The proof of Lemma 1.14 shows that
$$\frac{s}{q} + \frac{q}{s} \le \frac{1}{\delta} \quad \text{and} \quad \frac{v}{q} + \frac{q}{v} \le \frac{1}{\delta}\cdot$$

Hence each of the four numbers s/q, q/s, v/q, q/v satisfies $t + 1/t \le 1/\delta$. Now the function $t \mapsto t + 1/t$ is decreasing on the interval $(0, 1)$ and increasing on the interval $(1, +\infty)$. It follows that our four numbers all lie in the interval $(1/x, x)$, where x is the root > 1 of the equation $x + 1/x = 1/\delta$. The two roots x and $1/x$ of the quadratic polynomial $X^2 - (1/\delta)X + 1$ are at a mutual distance equal to the square root of the discriminant $\Delta = (1/\delta)^2 - 4$ of this polynomial. Now
$$\frac{v}{q} - \frac{s}{q} = 1,$$

hence the length $\sqrt{\Delta}$ of the interval $(1/x, x)$ is ≥ 1 and therefore $\delta \le 1/\sqrt{5}$. This completes the proof of Lemma 1.15. □

Denote by $\Phi = (1 + \sqrt{5})/2 = 1.6180339887499\ldots$ the *Golden ratio*, root of the polynomial $X^2 - X - 1$, whose continued fraction expansion is
$$\Phi = [1, 1, 1, 1, \ldots] = [\overline{1}].$$

Recall also the definition of the Fibonacci sequence $(F_n)_{n\ge 0}$:
$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \quad (n \ge 2).$$

Exercise 1.16. *a) Show that, for any $q \ge 1$ and any $p \in \mathbb{Z}$,*

$$\left|\Phi - \frac{p}{q}\right| > \frac{1}{\sqrt{5}q^2 + (q/2)}\cdot$$

b) Show also

$$\lim_{n\to\infty} F_{n-1}^2 \left|\Phi - \frac{F_n}{F_{n-1}}\right| = \frac{1}{\sqrt{5}}\cdot$$

Deduce that Hurwitz's estimate in Lemma 1.12 is optimal.

1.3.3 Irrationality of at least one number

Lemma 1.10 is a criterion for the irrationality of one number, we extend it to a criterion for the irrationality of at least one number in a given set. There are far reaching generalizations (especially due to Yu. V. Ñesterenko) of such results to quantitative statements, yielding irrationality measures or even measures of linear independence.

Lemma 1.17. *Let $\vartheta_1, \ldots, \vartheta_m$ be real numbers. The following conditions are equivalent*
(i) *One at least of $\vartheta_1, \ldots, \vartheta_m$ is irrational.*
(ii) *For any $\epsilon > 0$ there exist $p_1, \ldots, p_m, q$ in $\mathbb{Z}$ with $q > 0$ such that*

$$0 < \max_{1\le i\le m} \left|\vartheta_i - \frac{p_i}{q}\right| < \frac{\epsilon}{q}\cdot$$

(iii) *For any integer $Q > 1$ there exists $p_1, \ldots, p_m, q$ in $\mathbb{Z}$ such that $1 \le q \le Q^m$ and*

$$0 < \max_{1\le i\le m} \left|\vartheta_i - \frac{p_i}{q}\right| \le \frac{1}{qQ}\cdot$$

(iv) *There is an infinite set of $q \in \mathbb{Z}$, $q > 0$, for which there there exist $p_1, \ldots, p_m$ in $\mathbb{Z}$ satisfying*

$$0 < \max_{1\le i\le m} \left|\vartheta_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+1/m}}\cdot$$

Proof. The proofs of (iii)⇒(iv)⇒(ii)⇒(i) are easy.

For (i)⇒(iii) we use Dirichlet's box principle like in the proof of Lemma 1.10. Consider the $Q^m + 1$ elements

$$\xi_q = \bigl(\{q\vartheta_1\}, \ldots, \{q\vartheta_m\}\bigr) \quad (q = 0, 1, \ldots, Q^m)$$

in the unit cube $[0,1)^m$ of $\mathbb{R}^m$. Split this unit cube into Q^m cubes having sides of lengths $1/Q$. One at least of these small cubes contains at least two ξ_q, say ξ_{q_1} and ξ_{q_2}, with $0 \le q_2 < q_1 \le Q^m$. Set $q = q_1 - q_2$ and take for p_i the nearest integer to ϑ_i, $1 \le i \le m$. This completes the proof of Lemma 1.17.

□

An alternative arguments relies on geometry of numbers - see [20] Chap. II, § 1 - it follows that it is not necessary to assume Q to be an integer, and the strict inequality $q < Q^m$ can be achieved.

1.3.4 Another irrationality criterion

We give a further irrationality criterion which will be extended in § 2.1 to a criterion of linear independence.

Lemma 1.18. *Let ϑ be a real number. The following conditions are equivalent*
(i) *ϑ is irrational.*
(ii) *For any $\epsilon > 0$ there exists p/q and r/s in $\mathbb{Q}$ such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s}, \quad qr - ps = 1$$

and

$$\max\{q\vartheta - p\ ;\ r - s\vartheta\} < \epsilon.$$

(iii) *There exist infinitely many pairs $(p/q, r/s)$ of rational numbers such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s}, \quad qr - ps = 1$$

and

$$\max\{q(q\vartheta - p)\ ;\ s(r - s\vartheta)\} < 1.$$

Proof. The implications (iii)⇒(ii)⇒(i) are easy. For (i)⇒(iii) we use the arguments in the proof of Lemma 1.13, but we use also an auxiliary result from the theory of continued fractions.

Since ϑ is irrational, Hurwitz Lemma 1.12 shows that there are infinitely many p/q such that

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

We shall use the fact that such a p/q is a so-called *best approximation to ϑ*: this means that for any $a/b \in \mathbb{Q}$ with $1 \le b \le q$ and $a/b \ne p/q$, we have

$$\left|\vartheta - \frac{a}{b}\right| > \left|\vartheta - \frac{p}{q}\right|.$$

Assume first $p/q < \vartheta$. Let r/s be defined by $qr - ps = 1$ and $1 \le s < q$, $|r| < |p|$. We have

$$0 < \frac{r}{s} - \vartheta < \frac{r}{s} - \frac{p}{q} = \frac{1}{qs} \le \frac{1}{s^2}.$$

Next assume $p/q > \vartheta$. In this case rename it r/s and define p/q by $qr - ps = 1$ and $1 \le q < s$, $|p| < |r|$.

Finally repeat the argument in the proof of Lemma 1.13 to get an infinite set of approximations. Lemma 1.18 follows. □

1.4 Introduction to Hermite's work

The proofs given in subsection 1.2 of the irrationality of e^r for several rational values of r (namely $r \in \{1/a, 2/a, \sqrt{2}/a, \sqrt{3}/a \ ; \ a \in \mathbb{Z}, \ a \neq 0\}$) are similar: the idea is to start from the expansion of the exponential function, to truncate it and to deduce rational approximations to e^r. In terms of the exponential function this amounts to approximate e^z by a polynomial. Such polynomial approximations to the exponential function e^z yields, by substituting $z = a$, rational approximations to e^a with denominator $n!$. However there are better approximation to e^a if one allows other denominators.

The main idea, due to C. Hermite [13], is to approximate e^z by rational functions $A(z)/B(z)$. The word "*approximate*" has the following meaning (Hermite-Padé): an analytic function f is *well approximated* by a rational function $A(z)/B(z)$ (where A and B are polynomial) if the first coefficients of the Taylor expansions of both functions match:

$$f(z) = \frac{A(z)}{B(z)} + z^N g(z),$$

where g is analytic at the origin. It amounts to the same to say that the difference $B(z)f(z) - A(z)$ has a zero at the origin of high multiplicity:

$$B(z)f(z) - A(z) = z^N B(z)g(z).$$

When we just truncate the series expansion of the exponential function, we approximate e^z by a polynomial in z with rational coefficients; when we substitute $z = a$ where a is a positive integer, this polynomial produces a rational number, but the denominator of this number is quite large (unless $a = \pm 1$). A trick gave the result also for $a = \pm 2$, but definitely for a a larger prime number for instance there is a problem: if we multiply by the denominator then the "*remainder*" is by no means small. As shown by Hermite, to produce a sufficiently large gap in the power expansion of $B(z)e^z$ will solve this problem.

Our first goal in this section is to prove Lambert's result on the irrationality of e^r when r is a non-zero rational number. Next we show how a slight modification implies the irrationality of π.

This proof serves as an introduction to Hermite's method. There are slightly different ways to present it: one is Hermite's original paper [13], another one is Siegel more algebraic point of view [22], and another was derived by Yu. V.Ñesterenko [2, 10, 18].

1.4.1 Irrationality of e^r for $r \in \mathbb{Q}$: sketch of proof

If $r = a/b$ is a rational number such that e^r is also rational, then $e^{|a|}$ is also rational, and therefore the irrationality of e^r for any non-zero rational number r follows from the irrationality of e^a for any positive integer a. We shall approximate the exponential function e^z by a rational function $A(z)/B(z)$ and show that $A(a)/B(a)$ is a good rational approximation to e^a, sufficiently good in fact so that one may use Lemma 1.10.

Write

$$e^z = \sum_{k\geq 0} \frac{z^k}{k!}\cdot$$

We wish to multiply this series by a polynomial so that the Taylor expansion at the origin of the product $B(z)e^z$ has a large gap: the polynomial preceding the gap will be $A(z)$, the remainder $R(z) = B(z)e^z - A(z)$ will have a zero of high multiplicity at the origin.

In order to create such a gap, we shall use the differential equation of the exponential function - hence we introduce derivatives.

In Fourier's proof, we use for B a constant polynomial, of degree 0. For N sufficiently large set

$$B_N = N!, \quad A_N(z) = \sum_{n=0}^{N} \frac{N!}{n!} z^n, \quad R_N(z) = \sum_{n\geq N+1} \frac{N!}{n!} z^n.$$

Notice that the first term in the Taylor expansion of R_N is

$$\frac{1}{N+1} z^{N+1}.$$

This is sufficient for proving the irrationality of e, since for $z = 1$ we have

$$\lim_{N\to\infty} R_N(1) = 0.$$

But for $a > 1$ the sequence $(R_N(a))_{N\geq 1}$ tends to infinity.

Now take for B_N a degree 1 polynomial in $\mathbb{Z}[z]$ that we select so that the coefficient of z^N vanishes. It is easy to check that the solution is to take a multiple of $z - N$, and we take the product by $(N-1)!$ in order to have integral coefficients for A. So set

$$B_N(z) = (N-1)!z - N!, \quad A_N(z) = -N! - \sum_{n=1}^{N-1} \frac{(N-1)!}{n!}(N-n)z^n, \quad (1.19)$$

$$R_N(z) = \sum_{n\geq N+1} \frac{(N-1)!}{n!}(n-N)z^n$$

so that again $B_N(z)e^z = A_N(z) + R_N(z)$. Here the first term in the Taylor expansion of R_N is

$$\frac{1}{N(N+1)} z^{N+1}.$$

This is a tiny progress, since in the denominator we get a degree 2 polynomial in place of a degree 1 polynomial in N. But this is not sufficient to ensure that for fixed $a > 1$ the sequence $(R_N(a))_{N\geq 1}$ tends to zero. So we shall take for B_N a polynomial of larger degree, depending on N.

1.4.2 First introduction to Hermite's proof

We first explain how to produce, from an analytic function whose Taylor development at the origin is

$$f(z) = \sum_{k\geq 0} a_k z^k, \tag{1.20}$$

another analytic function with one given Taylor coefficient, say the coefficient of z^m, is zero. The coefficient of z^m for f is $a_m = m! f^{(m)}(0)$. The same number a_m occurs when one computes the Taylor coefficient of z^{m-1} for the derivative f' of f. Writing

$$ma_m = m!(zf')^{(m)}(0),$$

we deduce that the coefficient of z^m in the Taylor development of $zf'(z) - mf(z)$ is 0, which is what we wanted.

It is the same thing to write

$$zf'(z) = \sum_{k\geq 0} ka_k z^k$$

so that

$$zf'(z) - mf(z) = \sum_{k\geq 0} (k-m)a_k z^k.$$

Now we want that several consecutive Taylor coefficients cancel. It will be convenient to introduce derivative operators.

We introduce the derivative operator $D = d/dz$. As usual, D^2 denotes $D \circ D$ and $D^m = D^{m-1} \circ D$ for $m \geq 2$. The Taylor expansion at the origin of an analytic function f is

$$f(z) = \sum_{\ell\geq 0} \frac{1}{\ell!} D^\ell f(0) z^\ell.$$

The derivation D and the multiplication by z do not commute:

$$D(zf) = f + zD(f),$$

relation which we write $Dz = 1 + zD$. From this relation it follows that the non-commutative ring generated by z and D over $\mathbb{C}$ is also the ring of polynomials in D with coefficients in $\mathbb{C}[z]$. In this ring $\mathbb{C}[z][D]$ there is an element which will be very useful for us, namely $\delta = zd/dz$. It satisfies $\delta(z^k) = kz^k$. To any polynomial $T \in \mathbb{C}[t]$ one associates the derivative operator $T(\delta)$.

By induction on m, one checks $\delta^m z^k = k^m z^k$ for all $m \geq 0$. By linearity, one deduces that if T is a polynomial with complex coefficients, then

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

For our function f with the Taylor development (1.20) we have

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

Hence if we want a function with a Taylor expansion having 0 as coefficient of z^k, it suffices to consider $T(\delta)f(z)$ where T is a polynomial satisfying $T(k)=0$. For instance if n_0 and n_1 are two non-negative integers and if we take

$$T(t)=(t-n_0-1)(t-n_0-2)\cdots(t-n_0-n_1),$$

then the series $T(\delta)f(z)$ can be written $A(z)+R(z)$ with

$$A(z)=\sum_{k=0}^{n_0} T(k)a_k z^k$$

and

$$R(z)=\sum_{k\ge n_0+n_1+1} T(k)a_k z^k.$$

This means that in the Taylor expansion at the origin of $T(\delta)f(z)$, all coefficients of $z^{n_0+1}, z^{n_0+2},\ldots,z^{n_0+n_1}$ are 0.

Let $n_0\ge 0$, $n_1\ge 0$ be two integers. Define $N=n_0+n_1$ and

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

Since T is monic of degree n_1 with integer coefficients, it follows from the differential equation of the exponential function

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

that there is a polynomial $B\in\mathbb{Z}[z]$, which is monic of degree n_1, such that $T(\delta)e^z=B(z)e^z$.

Set

$$A(z)=\sum_{k=0}^{n_0} T(k)\frac{z^k}{k!} \quad\text{and}\quad R(z)=\sum_{k\ge N+1} T(k)\frac{z^k}{k!}\cdot$$

Then

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

where A is a polynomial with rational coefficients of degree n_0 and leading coefficient

$$\frac{T(n_0)}{n_0!}=(-1)^{n_1}\frac{n_1!}{n_0!}\cdot$$

Also the analytic function R has a zero of multiplicity $\ge N+1$ at the origin.

We can explicit these formulae for A and R. For $0\le k\le n_0$ we have

$$\begin{aligned}T(k)&=(k-n_0-1)(k-n_0-2)\cdots(k-N)\\&=(-1)^{n_1}(N-k)\cdots(n_0+2-k)(n_0+1-k)\\&=(-1)^{n_1}\frac{(N-k)!}{(n_0-k)!}\cdot\end{aligned}$$

For $k\ge N+1$ we write in a similar way

$$T(k)=(k-n_0-1)(k-n_0-2)\cdots(k-N)=\frac{(k-n_0-1)!}{(k-N-1)!}\cdot$$

Hence we have proved:

Proposition 1.21 (Hermite's formulae for the exponential function)**.** *Let $n_0 \geq 0$, $n_1 \geq 0$ be two integers. Define $N = n_0 + n_1$. Set*

$$A(z) = (-1)^{n_1} \sum_{k=0}^{n_0} \frac{(N-k)!}{(n_0-k)!k!} \cdot z^k \quad \text{and} \quad R(z) = \sum_{k \geq N+1} \frac{(k-n_0-1)!}{(k-N-1)!k!} \cdot z^k.$$

Finally, define $B \in \mathbb{Z}[z]$ by the condition

$$(\delta - n_0 + 1)(\delta - n_0 + 2) \cdots (\delta - N)e^z = B(z)e^z.$$

Then

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

Further, B is a monic polynomial with integer coefficients of degree n_1, A is a polynomial with rational coefficients of degree n_0 and leading coefficient $(-1)^{n_1} n_1!/n_0!$, and the analytic function R has a zero of multiplicity $N+1$ at the origin.
Furthermore, the polynomial $(n_0!/n_1!)A$ has integer coefficients. In particular, if $n_1 \geq n_0$, then the coefficients of A itself are integers.

Remark. *For $n_1 < n_0$ the leading coefficient $(-1)^{n_1} n_1!/n_0!$ of A is not an integer.*

Lemma 1.22. *Let $z \in \mathbb{C}$. Then*

$$|R(z)| \leq \frac{|z|^{N+1}}{n_0!} e^{|z|}.$$

Proof. We have

$$R(z) = \sum_{k \geq N+1} \frac{(k-n_0-1)!}{(k-N-1)!k!} \cdot z^k = \sum_{\ell \geq 0} \frac{(\ell+n_1)!}{(\ell+N+1)!} \cdot \frac{z^{\ell+N+1}}{\ell!}.$$

The trivial estimates

$$\frac{(\ell+N+1)!}{(\ell+n_1)!} = (\ell+N+1)(\ell+N)(\ell+N-1)\cdots(\ell+n_1+1) \geq (n_0+1)! \geq n_0!$$

yield

$$|R(z)| \leq \frac{|z|^{N+1}}{n_0!} \sum_{\ell \geq 0} \frac{|z|^\ell}{\ell!}.$$

Lemma 1.22 follows. □

1.4.3 Second introduction to Hermite's proof

In [22], C.L. Siegel introduces an algebraic point of view which yields the following:

Theorem 1.23. *Given two integers $n_0 \geq 0$, $n_1 \geq 0$, there exist two polynomials A and B in $\mathbb{C}[z]$ with A of degree $\leq n_0$ and $B \neq 0$ of degree $\leq n_1$ such that the function $R(z) = B(z)e^z - A(z)$ has a zero at the origin of multiplicity $\geq N+1$ with $N = n_0+n_1$. This solution (A, B, R) is unique if we require B to be monic. Moreover A has degree n_0, B has degree n_1 and R has multiplicity $N+1$ at the origin.*

Proof. We first prove the existence of a non-trivial solution (A, B, R). For $n \geq 0$, denote by $\mathbb{C}[z]_{\leq n}$ the $\mathbb{C}$–vector space of polynomials of degree $\leq n$. Its dimension is $n+1$. Consider the linear mapping

$$\begin{array}{cccc} \mathcal{L}: & \mathbb{C}[z]_{\leq n_1} & \longrightarrow & \mathbb{C}^{n_1} \\ & B(z) & \longmapsto & \Big(D^\ell\big(B(z)e^z\big)_{z=0}\Big)_{n_0<\ell\leq N} \end{array}$$

This map is not injective, its kernel has dimension ≥ 1. Let $B \in \ker \mathcal{L}$. Define

$$A(z) = \sum_{\ell=0}^{n_0} D^\ell\big(B(z)e^z\big)_{z=0} \frac{z^\ell}{\ell!}$$

and

$$R(z) = \sum_{\ell \geq N+1} D^\ell\big(B(z)e^z\big)_{z=0} \frac{z^\ell}{\ell!}.$$

Then (A, B, R) is a solution to the problem:

$$B(z)e^z = A(z) + R(z). \tag{1.24}$$

There is an alternative proof of the existence as follows [22]. Consider the linear mapping

$$\begin{array}{ccc} \mathbb{C}[z]_{\leq n_0} \times \mathbb{C}[z]_{\leq n_1} & \longrightarrow & \mathbb{C}^{N+1} \\ \big(A(z), B(z)\big) & \longmapsto & \Big(D^\ell\big(B(z)e^z - A(z)\big)_{z=0}\Big)_{0\leq\ell\leq N} \end{array}$$

This map is not injective, its kernel has dimension ≥ 1. If (A, B) is a non-zero element in the kernel, then $B \neq 0$.

We now check that the kernel of $\mathcal{L}$ has dimension 1. Let $B \in \ker \mathcal{L}$, $B \neq 0$ and let (A, B, R) be the corresponding solution to (1.24).

Since A has degree $\leq n_0$, the (n_0+1)-th derivative of R is

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

hence it is the product of e^z with a polynomial of the same degree as the degree of B and same leading coefficient. Now R has a zero at the origin of multiplicity $\geq n_0+n_1+1$, hence $D^{n_0+1}R(z)$ has a zero of multiplicity $\geq n_1$ at the origin. Therefore

$$D^{n_0+1}R = cz^{n_1}e^z \tag{1.25}$$

where c is the leading coefficient of B; it follows also that B has degree n_1. This proves that $\ker \mathcal{L}$ has dimension 1.

Since $D^{n_0+1}R$ has a zero of multiplicity exactly n_1, it follows that R has a zero at the origin of multiplicity exactly $N+1$, so that R is the unique function satisfying $D^{n_0+1}R = cz^{n_1}e^z$ with a zero of multiplicity $\geq n_0$ at 0.

It remains to check that A has degree n_0. Multiplying (1.24) by e^{-z}, we deduce

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

We replace z by $-z$:

$$A(-z)e^{z} = B(-z) - R(-z)e^{z}. \tag{1.26}$$

It follows that $\big(B(-z), A(-z), -R(-z)e^z\big)$ is a solution to the Padé problem (1.24) for the parameters (n_1, n_0), hence A has degree n_0.

□

Following [22], we give formulae for A, B and R.

Consider the operator J defined (on the set of analytic functions near the origin) by

$$J(\varphi) = \int_0^z \varphi(t)dt.$$

It satisfies

$$DJ\varphi = \varphi \quad \text{and} \quad JDf = f(z) - f(0).$$

Hence the restriction of the operator of D to the functions vanishing at the origin is a one-to-one map with inverse J.

The next lemma extends the fact that $z\log z - z$ is a primitive of $\log z$.

Lemma 1.27. *For $n \geq 0$,*

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

Proof. The formula is valid for $n = 0$. We first check it for $n = 1$. The derivative of the function

$$\int_0^z (z-t)\varphi(t)dt = z\int_0^z \varphi(t)dt - \int_0^z t\varphi(t)dt$$

is

$$\int_0^z \varphi(t)dt + z\varphi(z) - z\varphi(z) = \int_0^z \varphi(t)dt.$$

We now proceed by induction. For $n \geq 1$ the derivative of the function of z

$$\frac{1}{n!}\int_0^z (z-t)^n\varphi(t)dt = \sum_{k=0}^{n} \frac{(-1)^{n-k}}{k!(n-k)!} \cdot z^k \int_0^z t^{n-k}\varphi(t)dt$$

is

$$\sum_{k=0}^{n} \frac{(-1)^{n-k}}{k!(n-k)!}\left(kz^{k-1}\int_0^z t^{n-k}\varphi(t)dt + z^n\varphi(z)\right). \qquad (1.28)$$

Since $n \geq 1$, we have

$$\sum_{k=0}^{n} \frac{(-1)^{n-k}}{k!(n-k)!} = 0$$

and (1.28) is nothing else than

$$\sum_{k=1}^{n} \frac{(-1)^{n-k}}{(k-1)!(n-k)!}\cdot z^{k-1}\int_0^z t^{n-k}\varphi(t)dt = \frac{1}{(n-1)!}\int_0^z (z-t)^{n-1}\varphi(t)dt.$$

□

Using (1.25) with $c = 1$ together with Lemma 1.27, we deduce:

Lemma 1.29. *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

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

This gives another proof of Lemma 1.22.

Remark. *This is the estimate for B monic. When $n_1 < n_0$ the coefficients of the associated polynomial A are not integers. For instance in case $n_1 = 0$ (hence $n_0 = N$) the polynomial B is 1 and A (which is the head of the Taylor expansion of the exponential function) has denominator $N!$. In case $n_1 = 1$ we need to multiply by $(N-1)!$, as explained in (1.19) above, to get integer coefficients. More generally in case $n_1 < n_0$ we need to multiply by $n_0!/n_1!$ in order to get integer coefficients, so the remainder in this case is bounded by*

$$\frac{n_0!}{n_1!}|R(z)| \leq \frac{|z|^{N+1}}{n_1!} e^{|z|}.$$

If we want to have a small remainder we need to take n_1 at least a constant times $N/\log N$. The choice $n_1 = n_0 = N/2$ is the most natural one.

We now give formulae for A and B in Theorem 1.23, following C.L. Siegel [22].

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

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

and f an analytic complex valued function, we define

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

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

We reproduce [22], Chap.I § 1: for two powers series S_1 and S_2 and an analytic function f we have

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

and

$$\big(S_1(D)S_2(D)\big)f = S_1(D)\big(S_2(D)\big)f.$$

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

$$S^{-1}(t) = \sum_{i\geq 0} \sigma_i t^i, \quad (\sigma_0 = 1/s_0)$$

and

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

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 $\lambda \in \mathbb{C}$ and $P \in \mathbb{C}[z]$, 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, let $\lambda \neq 0$ be a complex number and let $Q \in \mathbb{C}[z]$ be a polynomial. We wish to solve the equation

$$D^n\big(e^{\lambda z}P\big) = e^{\lambda z}Q,$$

where the unknown is the polynomial P. This amounts to solving the differential equation

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

and the unique solution $P \in \mathbb{C}[z]$ is

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

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 (1.24) in Theorem 1.23, where $B \in \mathbb{C}[z]$ is monic of degree n_1 and $A \in \mathbb{C}[z]$ has degree n_0, while $R \in \mathbb{C}[[z]]$ has a zero of multiplicity $N + 1$ at 0.

From

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

we deduce

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

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

$$\boxed{B(z) = (-1)^{n_1} \frac{n_1!}{n_0!} \sum_{k=0}^{n_1} (-1)^k \frac{(N-k)!}{(n_1-k)!k!} z^k.} \tag{1.30}$$

One readily checks that B is monic of degree n_1.

If we request B to be monic, then $c = 1$ in (1.25) and it follows that the coefficient of z^{N+1} in R is

$$\frac{n_1!}{(N+1)!}.$$

In the proof of Theorem 1.23, we found a link (1.26) between the Padé solution with parameters (n_0, n_1) and the solution with parameters (n_1, n_0). We explicit this link. We denote by $(A_{n_0,n_1}, B_{n_0,n_1}, R_{n_0,n_1})$ the solution of (1.24) for the parameters (n_0, n_1). From (1.26) we infer

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

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

$$R_{n_0,n_1}(z) = (-1)^N \frac{n_1!}{n_0!} R_{n_1,n_0}(-z) e^{-z}.$$

Hence

$$\boxed{A(z) = (-1)^{n_1} \sum_{k=0}^{n_0} \frac{(N-k)!}{(n_0-k)!k!} \cdot z^k.} \tag{1.31}$$

The leading coefficient of A is $(-1)^{n_1} n_1!/n_0!$. It follows also from (1.31) that $(n_0!/n_1!)A$ has integer coefficients. In particular if $n_1 \ge n_0$, then A is in $\mathbb{Z}[z]$.

We can also check this formula (1.31) starting from

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

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

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

where a is the leading coefficient of a. From

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

we deduce

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

and

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

1.4.4 Irrationality of e^r: end of the proof

We are now able to complete the proof of the irrationality of e^r for $\in \mathbb{Q}$, $r \neq 0$.

Let $r = a/b$ be a non-zero rational number. Assume (wlog) r is positive. Set $s = e^r$, let n be a sufficiently large integer, choose $n_0 = n_1 = n$ and replace z by $a = br$ in (1.24); we deduce

$$B_n(a)s^b - A_n(a) = R_n(a),$$

where A_n, B_n and R_n stand for A, B, R with our choice $n_0 = n_1 = n$. All coefficients in R_n are positive, hence $R_n(a) > 0$. Therefore $B_n(a)s^b - A_n(a) \neq 0$. By Lemma 1.22, $R_n(a)$ tends to 0 when n tends to infinity. Since $B_n(a)$ and $A_n(a)$ are rational integers, we may use the implication (ii)$\Rightarrow$(i) in Lemma 1.10: we deduce that the number s^b is irrational. Hence $s = e^r$ is also irrational.

1.4.5 Irrationality of π

This proof of the irrationality of $\log s$ for s a positive rational number given in § 1.4.4 can be extended to the case $s = -1$ in such a way that one deduces Lambert's result (see § 1.1) on the irrationality of the number π.

Assume π is a rational number, $\pi = a/b$. Again let n be a sufficiently large integer, take $n_0 = n_1 = n$ and denote by A_n, B_n and R_n the solution of the Padé problem (1.24). Substitute $z = ia = i\pi b$. Notice that $e^z = (-1)^b$:

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

and that the two complex numbers $A_n(ia)$ and $B_n(ia)$ are in $\mathbb{Z}[i]$. The left hand side is in $\mathbb{Z}[i]$, the right hand side tends to 0 as n tends to infinity, hence both sides are 0.

In the proof of § 1.4.1, we used the positivity of the coefficients of R_n and we deduced that $R_n(a)$ was not 0 (this is the so-called ““*zero estimate*” in transcendental number theory). Here we need another argument.

The last step of the proof of the irrationality of π is achieved by using two consecutive indices n and $n+1$. We eliminate e^z among the two relations

$$B_n(z)e^z - A_n(z) = R_n(z) \quad \text{and} \quad B_{n+1}(z)e^z - A_{n+1}(z) = R_{n+1}(z).$$

We deduce that the polynomial

$$\Delta_n = B_n A_{n+1} - B_{n+1} A_n \tag{1.32}$$

can also be written

$$\Delta_n = -B_n R_{n+1} + B_{n+1} R_n. \tag{1.33}$$

As we have seen, the polynomial B_n is monic of degree n; the polynomial A_n also has degree n, its highest degree term is $(-1)^n z^n$. It follows from (1.32) that Δ_n is a polynomial of degree $2n+1$ and highest degree term $(-1)^n 2z^{2n+1}$. On the other hand, since R_n has a zero of multiplicity at least $2n+1$, the relation (1.33) shows that it is the same for Δ_n. Consequently

$$\Delta_n(z) = (-1)^n 2z^{2n+1}.$$

It follows that Δ_n does not vanish outside 0. From (1.33) we deduce that R_n and R_{n+1} have no common zero apart from 0. This completes the proof of the irrationality of π.

References

[1] M. Aigner & G.M. Ziegler – *Proofs from THE BOOK*, Springer (2001).

[2] R. Breusch– *A Proof of the Irrationality of* π, The American Mathematical Monthly, Vol. **61**, No. 9 (Nov., 1954), pp. 631-632.

[3] C. Brezinski – *The long history of continued fractions and Padé approximants.* Padé approximation and its applications, Amsterdam 1980, pp. 1–27, Lecture Notes in Math., **888**, Springer, Berlin-New York, 1981.

[4] C. Brezinski – *History of continued fractions and Padé approximants.* Springer Series in Computational Mathematics, **12**. Springer-Verlag, Berlin, 1991.

[5] Y. Bugeaud – *Approximation by algebraic numbers*, Cambridge Tracts in Mathematics, vol. 160, Cambridge University Press, Cambridge, 2004.

[6] H. Cohn – *A short proof of the simple continued fraction expansion of* e, Math Monthly **113** January 2006, 57–62.
http://fr.arXiv.org/abs/math.NT/061660

[7] J. Cosgrave – *New Proofs of the Irrationality of* e^2 *and* e^4, unpublished.
http://services.spd.dcu.ie/johnbcos/esquared.htm

[8] L. Euler – *De fractionibus continuis dissertatio*, Commentarii Acad. Sci. Petropolitanae, 9 (1737), 1744, p. 98–137; Opera Omnia Ser. I vol. 14, Commentationes Analyticae, p. 187–215.

[9] P. Eymard & J-P. Lafon – *Autour du nombre* π, Hermann, 2000. *The number* π, Amer. Math. Soc., 2004.

[10] N. I. Fel'dman & Yu. V. Ñesterenko – *Transcendental numbers*, in *Number Theory, IV*, Encyclopaedia Math. Sci., vol. **44**, Springer, Berlin, 1998, p. 1–345.

[11] S. Fischler – *Irrationalité de valeurs de zêta, (d'après Apéry, Rivoal,...)*, Sém. Bourbaki 2002-2003, N° 910 (Novembre 2002). Astérisque **294** (2004), 27-62.
http://www.math.u-psud.fr/~fischler/publi.html

[12] G. H. Hardy & A. M. Wright, – *An Introduction to the Theory of Numbers*, Oxford Sci. Publ., 1938.

[13] C. Hermite – *Sur la fonction exponentielle*, C. R. Acad. Sci. Paris, **77** (1873), 18–24; 74–79; 226–233; 285–293; *Oeuvres*, Gauthier Villars (1905), III, 150–181. See also *Oeuvres* III, 127–130, 146–149, and *Correspondance Hermite-Stieltjes*, II, lettre 363, 291–295.

[14] H. Lambert – *Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques*, Mémoires de l'Académie des Sciences de Berlin, **17** (1761), 1768, p. 265–322; lu en 1767; Math. Werke, t. II.

[15] J. Liouville – *Sur l'irrationalité du nombre* $e = 2,718\ldots$, J. Math. Pures Appl. (1) **5** (1840), p. 192.

[16] J. Liouville – *Addition à la note sur l'irrationalité du nombre* e, J. Math. Pures Appl. (1) **5** (1840), p. 193–194.

[17] J. Liouville – *Sur des classes très étendues de quantités dont la valeur n"est ni algébrique, ni même réductible à des irrationnelles algébriques*, C.R. Acad. Sci. Paris, **18** (1844), 883–885 and 910–911. J. Math. Pures et Appl. (1) **16** (1851), 133–142.

[18] Yu. V. Ñesterenko – *A simple proof of the irrationality of* π, Russ. J. Math. Phys. **13** (2006), no. 4, 473).

[19] K. Ramasubramanian – *The Notion of Proof in Indian Science*, 13th World Sanskrit Conference, 2006.
http://www.iitb.ac.in/campus/diary/2006/august/tday2.htm

[20] W. M. Schmidt – *Diophantine approximation*, Lecture Notes in Mathematics, vol. **785**, Springer-Verlag, Berlin, 1980.

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

[22] C. L. Siegel – *Transcendental Numbers*, Annals of Mathematics Studies, **16**. Princeton University Press, Princeton, N. J., 1949.

[23] B. Sury – *Bessels contain continued fractions of progressions*, Resonance, vol. **10** N°3, March 2005, 80–87.
http://www.ias.ac.in/resonance/