Updated: *May 16, 2010*

Diophantine approximation, irrationality and transcendence

Michel Waldschmidt

Course N°1, *April 14, 2010*

These are informal notes([1]) of my course given in April – June 2010 at IMPA (*Instituto Nacional de Matematica Pura e Aplicada*), Rio de Janeiro, Brazil.

1 Introduction

1.1 Irrationality of $\sqrt{2}$

We first give a geometrical proof of the irrationality of the number

$$\sqrt{2} = 1,414\,213\,562\,373\,095\,048\,801\,688\,724\,209\ \ldots$$

Starting with a rectangle having sides 1 and $1+\sqrt{2}$, we split it into two unit squares and a smaller rectangle. The length of this second rectangle is 1, its width is $\sqrt{2}-1$, hence its proportion is

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

Therefore the first and second rectangles have the same proportion. Now, if we repeat the process and split the small rectangle into two squares (of sides $\sqrt{2}-1$) and a third tiny rectangle, the proportions of this third rectangle will again be $1+\sqrt{2}$. This means that the process will not end, each time we shall get two squares and a remaining smaller rectangle having the same proportion.

[1]This text is available on the internet at the address
`http://www.math.jussieu.fr/~miw/enseignement.html`

On the other hand, if we start with a rectangle having integer side–lengths, if we split it into several squares and if a small rectangle remains, then clearly the small rectangle while have integer side–lengths([2]). Therefore the process will not continue forever, it will stop when there is no remaining small rectangle. This proves the irrationality of $\sqrt{2}$.

In algebraic terms, the number $x = 1 + \sqrt{2}$ satisfies

$$x = 2 + \frac{1}{x},$$

hence also

$$x = 2 + \cfrac{1}{2 + \cfrac{1}{x}} = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{x}}} = \cdots ,$$

which yields the *continued fraction expansion* of $1 + \sqrt{2}$.

1.2 Continued fractions

Here is the definition of the continued fraction expansion of a real number.

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

$$x = \lfloor x \rfloor + \{x\}.$$

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

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

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

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

[2] Starting with a rectangle of side–lengths a and b, the process stops when a square of side–length d is reached, where d is the gcd of a and b: also d is the largest positive integer such that the initial rectangle can be covered with square tiles of side length d.

with two integers a_0 and a_1, with $a_1 \geq 2$ (recall $x_1 > 1$). Otherwise we can define $x_2 = 1/\{x_1\}$, $a_2 = \lfloor x_2 \rfloor$ 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 $0 \leq \{x_n\} < 1$. The connexion with the geometric proof of irrationality of $\sqrt{2}$ by means of rectangles and squares is now obvious: start with a positive real number x and consider a rectangle of sides 1 and x. Divide this rectangle into unit squares and a second rectangle. Then a_0 is the number of unit squares which occur, while the sides of the second rectangle are 1 and $\{x\}$. If x is not an integer, meaning $\{x\} > 0$, then we split the second rectangle into squares of sides $\{x\}$ plus a third rectangle. The number of squares is now a_1 and the third rectangle has sides $\{x\}$ and $1 - a_1\{x\}$. Going one in the same way, one checks that the number of squares we get at the n-th step is a_n.

This geometric point of view shows that the process stops after finitely many steps (meaning that some $\{x_n\}$ is zero, or equivalently that x_n is in $\mathbf{Z}$) if and only if x is rational.

For simplicity of notation, when $x_0, x_1, \ldots, x_n$ are real numbers with $x_1, \ldots, x_n$ positive, we write

$$x = [x_0,\ x_1, \ldots, x_n] \quad \text{for} \quad x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{\ddots \; x_{n-1} + \cfrac{1}{x_n}}}}\cdot$$

When $a_0, a_1, \ldots, a_n$ are integers with $a_1, \ldots, a_n$ positive, then $[a_0,\ a_1, \ldots, a_n]$ is a rational number. Conversely, given a rational number x, the previous algorithm produces a finite continued fraction $[a_0,\ a_1, \ldots, a_n]$ where $a_0 = \lfloor x \rfloor$ and $a_i > 0$ $(1 \leq i \leq n)$ are integers. If x is a rational integer, then $n = 0$,

$a_0 = x$ and the continued fraction which is produced by this algorithm is $x = [a_0]$. If x is not an integer, then $n \geq 1$ and $a_n \geq 2$. For any rational number, there are exactly two finite continued fractions equal to x: one, say $[a_0,\ a_1, \dots, a_{n-1}, a_n]$, is given by the previous algorithm, the other one is $[a_0,\ a_1, \dots, a_{n-1}, a_n - 1, 1]$. For instance if x is an integer the continued fraction produced by the algorithm is $[x]$, as we just saw, while the other continued fraction equal to x is $[x-1, 1]$. The two continued fractions equal to 1 are $[1]$ and $[0, 1]$, while any positive rational number distinct from 1 has one continued fraction expansion with the last term $a_n \geq 2$ and one with the last term 1.

When x is irrational, we write the continued fraction as $[a_0,\ a_1, \dots, a_n, \dots]$. We shall check later that when $a_0, a_1, \dots, a_n, \dots$ are integers with $a_1, \dots, a_n, \dots$ positive, the limit of $[a_0,\ a_1, \dots, a_n]$ exists and is equal to x.

We need a further notation for ultimately periodic continued fraction. Assume that x is irrational and that for some integers n_0 and $r > 0$ its continued fraction expansion $[a_0,\ a_1, \dots, a_n, \dots]$ satisfies

$$a_{n+r} = a_n \quad \text{for any } n \geq n_0.$$

Then we write

$$x = [a_0,\ a_1, \dots, a_{n_0-1}, \overline{a_{n_0},\ a_{n_0+1}, \dots, a_{n_0+r-1}}].$$

For instance

$$\sqrt{2} = [1,\ 2,\ 2,\ 2, \dots] = [1,\ \overline{2}]$$

and

$$\sqrt{3} = [1,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2, \dots] = [1,\ \overline{1, 2}].$$

References on continued fractions are [11, 32, 19, 23, 4]. An interesting remark [30] on the continued fraction expansion of $\sqrt{2}$ is to relate the A4 paper format 21×29.7 to the fraction expansion

$$\frac{297}{210} = \frac{99}{70} = [1,\ 2,\ 2,\ 2,\ 2,\ 2].$$

There is nothing special with the square root of 2: most of the previous argument extend to the proof of irrationality of $\sqrt{n}$ when n is a positive integer which is not the square of an integer. For instance, a proof of the irrationality of $\sqrt{n}$ when n is not the square of an integer runs as follows. Write $\sqrt{n} = a/b$ where b is the smallest positive integer such that $b\sqrt{n}$ is an integer. Further, denote by m the integral part of $\sqrt{n}$: this means that m is the positive integer such that $m < \sqrt{n} < m + 1$. The strict inequality

$m < \sqrt{n}$ is the assumption that n is not a square. From $0 < \sqrt{n} - m < 1$ one deduces

$$0 < (\sqrt{n} - m)b < b.$$

Now the number

$$b' := (\sqrt{n} - m)b = a - mb$$

is a positive rational integer, the product

$$b'\sqrt{n} = bn - am$$

is an integer and $b' < b$, which contradicts the choice of b minimal.

The irrationality of $\sqrt{5}$ is equivalent to the irrationality of the *Golden ratio* $\Phi = (1 + \sqrt{5})/2$, root of the polynomial $X^2 - X - 1$, whose continued fraction expansion is

$$\Phi = [1,\ 1,\ 1,\ 1 \ldots] = [\overline{1}].$$

This continued fraction expansion follows from the relation

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

The geometric irrationality proof using rectangles that we described above for $1 + \sqrt{2}$ works in a similar way for the Golden ratio: a rectangle of sides Φ and 1 splits into a square and a small rectangle of sides 1 and $\Phi - 1$, hence the first and the second rectangles have the same proportion, namely

$$\Phi = \frac{1}{\Phi - 1}\cdot \tag{1}$$

Therefore the process continues forever with one square and one smaller rectangle with the same proportion. Hence Φ and $\sqrt{5}$ are irrational numbers.

Exercise 1. *Check that, in the geometric construction of splitting a rectangle of sides* 1 *and* x *into squares and rectangles, the number of successive squares is the sequence of integers* $(a_n)_{n\geq 0}$ *in the continued fraction expansion of* x*.*
b) Start with a unit square. Put on top of it another unit square: you get a rectangle with sides 1 *and* 2*. Next put on the right a square of sides* 2*, which produces a rectangle with sides* 2 *and* 3*. Continue the process as follows: when you reach a rectangle of small side* a *and large side* b*, complete it with a square of sides* b*, so that you get a rectangle with sides* b *and* $a + b$*. Which is the sequence of sides of the rectangles you obtain with this process?*

Generalizing this idea, given positive integers $a_0,\ a_1,\ldots,a_k$, devise a geometrical construction of the positive rational number having the continued fraction expansion

$$[a_0,\ a_1,\ldots,a_k].$$

Another proof of the irrationality of Φ is to deduce from the equation (1) that a relation $\Phi = a/b$ with $0 < b < a$ yields

$$\Phi = \frac{b}{a-b},$$

hence a/b is not a rational fraction with minimal denominator.

1.3 Irrational numbers

If k is a positive integer and n a positive integer which is not the k-th power of a rational integer, then the number $n^{1/k}$ is irrational. This follows, for instance, from the fact that the roots of $X^k - n$ are algebraic integers, and algebraic integers which are rational numbers are rational integers.

Other numbers for which it is easy to prove the irrationality are quotients of logarithms: if m and n are positive integers such that $(\log m)/(\log n)$ is rational, say a/b, then $m^b = n^a$, which means that *m and n are multiplicatively dependent*. Recall that elements $x_1,\ldots,x_r$ in an additive group are *linearly independent* if a relation $a_1x_1+\cdots+a_rx_r = 0$ with rational integers $a_1,\ldots,a_r$ implies $a_1 = \cdots = a_r = 0$. Similarly, elements $x_1,\ldots,x_r$ in a multiplicative group are *multiplicatively independent* if a relation $x_1^{a_1}\cdots x_r^{a_r} = 1$ with rational integers $a_1,\ldots,a_r$ implies $a_1 = \cdots = a_r = 0$. Therefore a quotient like $(\log 2)/\log 3$, and more generally $(\log m)/\log n$ where m and n are multiplicatively independent positive rational numbers, is irrational.

We have seen that *a real number is rational if and only if its continued fraction expansion is finite*. There is another criterion of irrationality using the b-adic expansion when b is an integer ≥ 2 (for $b = 10$ this is the decimal expansion, for $b = 2$ it is the diadic expansion). Indeed any real number x can be written

$$x = \lfloor x \rfloor + d_1b^{-1} + d_2b^{-2} + \cdots + d_nb^{-n} + \cdots$$

where the integers d_n (the digits of x) are in the range $0 \leq d_n < b$. There is unicity of such an expansion, unless x is an integral multiple of some b^{-n} with $n \geq 0$, in which case x has two expansions: one where all sufficiently large digits vanish, and one for which all sufficiently large digits are $b - 1$.

This is due to the equation

$$b^{-n} = \sum_{k=0}^{n} (b-1) b^{-n-k-1}.$$

Here is the irrationality criterion using such expansions: fix an integer $b \geq 2$. Then *the real number x is rational if and only if the sequence of digits $(d_n)_{n\geq 1}$ of x in basis b is ultimately periodic.*

Exercise 2. *Let $b \geq 2$ be an integer.*
a) Show that a real number x is rational if and only if the sequence $(d_n)_{n\geq 1}$ of digits of x in the expansion in basis b

$$x = \lfloor x \rfloor + d_1 b^{-1} + d_2 b^{-2} + \cdots + d_n b^{-n} + \cdots \qquad (0 \leq d_n < b)$$

is ultimately periodic.
b) Let $(u_n)_{n\geq 0}$ be an increasing sequence of positive integers. Assume there exists $c > 0$ such that, for all sufficiently large n,

$$u_n - u_{n-1} \geq cn.$$

Deduce from a) that the number

$$\vartheta = \sum_{n\geq 0} b^{-u_n}$$

is irrational.

One might be tempted to conclude that it should be easy to decide whether a given real number is rational or not. However this is not the case with many constants from analysis, because most often one does not know any expansion, either in continued fraction or in any basis $b \geq 2$. And the fact is that for many such constants the answer is not known. For instance, one does not know whether the *Euler–Mascheroni constant*

$$\begin{aligned}\gamma &= \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right) \\ &= 0,577\,215\,664\,901\,532\,860\,606\,512\,090\,082\ldots\end{aligned}$$

is rational or not: one expects that it is an irrational number (and even a transcendental number - see later). Other formulas for the same number are

$$\begin{aligned}\gamma &= \sum_{k=1}^{\infty}\left(\frac{1}{k} - \log\left(1+\frac{1}{k}\right)\right)\\ &= \int_1^{\infty}\left(\frac{1}{\lfloor x\rfloor} - \frac{1}{x}\right)dx\\ &= -\int_0^1\int_0^1 \frac{(1-x)dxdy}{(1-xy)\log(xy)}.\end{aligned}$$

J. Sondow uses (a generalization of) the last double integral in [36], he was inspired by F. Beukers' work on Apéry's proof of the irrationality of

$$\zeta(3) = \sum_{n\geq 1}\frac{1}{n^3} = 1,202\,056\,903\,159\,594\,285\,399\,738\,161\,511\ \ldots$$

in 1978. Recall that the values of the *Riemann zeta function*

$$\zeta(s) = \sum_{n\geq 1} n^{-s}$$

was considered by Euler for real s and by Riemann for complex s, the series being convergent for the real part of s greater than 1. Euler proved that the values $\zeta(2k)$ of this function at the even positive integers ($k \in \mathbf{Z}$, $k \geq 1$) are rational multiples of π^{2k}. For instance, $\zeta(2) = \pi^2/6$. It is interesting to notice that Euler's proof relates the values $\zeta(2k)$ at the positive even integers with the values of the same function at the odd negative integers, namely $\zeta(1-2k)$. For Euler this involved divergent series, while Riemann defined $\zeta(s)$ for $s \in \mathbf{C}$, $s \neq 1$, by analytic continuation.

One might be tempted to guess that $\zeta(2k+1)/\pi^{2k+1}$ is a rational number when $k \geq 1$ is a positive integer. However the folklore conjecture is that this is not the case. In fact there are good reasons to conjecture that for any $k \geq 1$ and any non-zero polynomial $P \in \mathbf{Z}[X_0, X_1, \ldots, X_k]$, the number $P(\pi, \zeta(3), \zeta(5), \ldots, \zeta(2k+1))$ is not 0. But one does not know whether

$$\zeta(5) = \sum_{n\geq 1}\frac{1}{n^5} = 1,036\,927\,755\,143\,369\,926\,331\,365\,486\,457\ldots$$

is irrational or not. And there is no proof so far that $\zeta(3)/\pi^3$ is irrational. According to T. Rivoal, among the numbers $\zeta(2n+1)$ with $n \geq 2$, infinitely many are irrational. And W. Zudilin proved that one at least of the four numbers

$$\zeta(5), \zeta(7), \zeta(9), \zeta(11)$$

is irrational. References with more information on this topic are given in the Bourbaki talk [14] by S. Fischler.

A related open question is the arithmetic nature of *Catalan's constant*

$$G = \sum_{n\geq 1} \frac{(-1)^n}{(2n+1)^2} = 0,915\,965\,594\,177\,219\,015\,0\dots$$

Other open questions can be asked on the values of *Euler's Gamma fonction*

$$\Gamma(z) = e^{-\gamma z} z^{-1} \prod_{n=1}^{\infty} \left(1 + \frac{z}{n}\right)^{-1} e^{z/n} = \int_0^{\infty} e^{-t} t^z \cdot \frac{dt}{t} \cdot$$

As an example we do not know how to prove that the number

$$\Gamma(1/5) = 4,590\,843\,711\,998\,803\,053\,204\,758\,275\,929\,152\,0\dots$$

is irrational.

The only rational values of z for which the answer is known (and in fact one knows the transcendence of the Gamma value in these cases) are

$$r \in \left\{ \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6} \right\} \qquad \pmod 1.$$

The number $\Gamma(1/n)$ appears when one computes *periods* of the Fermat curve $X^n + Y^n = Z^n$, and this curve is *simpler* (in technical terms it has genus ≤ 1) for $n = 2, 3, 4$ and 6. For $n = 5$ the genus is 2 and this is related with the fact that one is not able so far to give the answer for $\Gamma(1/5)$.

The list of similar open problems is endless. For instance, is the number

$$e + \pi = 5,859\,874\,482\,048\,838\,473\,822\,930\,854\,632\dots$$

rational or not? The answer is not yet known. And the same is true for any number in the following list

$$\log \pi,\ 2^{\pi},\ 2^{e},\ \pi^{e},\ e^{e}.$$

1.4 History of irrationality

The history of irrationality is closely connected with the history of continued fractions (see[2, 3]). (Even the first examples of transcendental numbers produced by Liouville in 1844 involved continued fractions, before he considered series).

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([3]):

> *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 [20] proved 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 [12].

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

$$e = [2;\ \overline{1, 2j,\ 1}]_{j\ge 1} = [2;\ 1,\ 2,\ 1,\ 1,\ 4,\ 1,\ 1,\ 6,\ 1, \dots],$$
$$e^2 = [7;\ \overline{3j-1,\ 1,\ 1,\ 3j,\ 12j+6}]_{j\ge 1} = [7;\ 2,\ 1,\ 1,\ 3,\ 18,\ 5,\ 1,\ 1,\ 6,\ 30,\ 8, \dots],$$

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 $(e+1)/3$:

$$\frac{e+1}{e-1} = [\overline{2(2j+1)}]_{j\ge 0} = [2;\ 6,\ 10,\ 14, \dots],$$
$$\frac{e^2+1}{e^2-1} = [\overline{2j+1}]_{j\ge 0} = [1;\ 3,\ 5,\ 7, \dots],$$
$$e^{1/n} = [\overline{1,\ (2j+1)n-1,\ 1}]_{j\ge 0} \quad \text{for} \quad n \ge 2,$$
$$e^{2/n} = [\overline{1,\ (n-1)/2+3jn,\ 6n+12jn,\ (5n-1)/2+3jn,\ 1}]_{j\ge 0} \quad \text{for odd} \quad n \ge 3,$$
$$2e = [5,\ 2,\ \overline{3,\ 2j,\ 3,\ 1,\ 2j,\ 1}]_{j\ge 1},$$
$$\frac{e+1}{3} =$$
$$[1,\ 4, \overline{5,\ 4j-3,\ 1,\ 1,\ 36j-16,\ 1,\ 1,\ 4j-2,\ 1,\ 1,\ 36j-4,\ 1,\ 1,\ 4j-1,\ 1,\ 5,\ 4j,\ 1}]_{j\ge 1}.$$

[3] 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

Hermite proved the irrationality of π and π^2 (see [3] p. 207 and p. 247). Furthermore, A.M. Legendre proved, in 1794, by a modification of Lambert's proof, that π^2 is also an irrational number (see [3] p. 14).

There are not so many numbers for which one knows the irrationality but we don't know whether they are algebraic or transcendental ([4]). A notable exception is $\zeta(3)$, known to be irrational (Apéry, 1978) and expected to be transcendental.

1.5 Variation on a proof by Fourier (1815)

That e is not quadratic follows from the fact that the continued fraction expansion of e, which was known by L. Euler in 1737 [11, 7, 33, 37]), is not periodic:

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

Since this expansion is infinite we deduce that e is irrational. The fact that it is not ultimately periodic implies also that e is not a quadratic irrationality, as shown by Lagrange in 1770 – Euler knew already in 1737 that a number with an ultimately periodic continued fraction expansion is quadratic (see [11, 4, 32]).

The following easier and well known proof of the irrationality of e 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: *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.

1.5.1 Irrationality of e

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

$$N!\ e - \sum_{n=0}^{N} \frac{N!}{n!} = \sum_{k\geq 1} \frac{N!}{(N+k)!}. \tag{2}$$

[4]Unless one considers complex numbers of the form ix where x is a real number expected to be transcendental, but for which no proof of irrationality is known: there are plenty of them!

The right hand side of (2) 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 (2) tends to 0 when N tends to infinity. In the left hand side, $\sum_{n=0}^{N} N!/n!$ is an integer. It follows that for any integer $N \geq 1$ the number $N!e$ is not an integer, hence e is an irrational number.

1.5.2 Irrationality of e^{-1}, following C.L. Siegel

In 1949, in his book on transcendental numbers [35], C.L. Siegel simplified the proof by Fourier: considering e^{-1} instead of e yields alternating series, hence it is no more necessary to estimate the remainder term.

The sequence $(1/n!)_{n\geq 0}$ is decreasing and tends to 0, hence for odd N,

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

Multiply by $N!$; the left hand side becomes

$$a_N := N! - \frac{N!}{1!} + \frac{N!}{2!} - \cdots + \frac{N!}{(N-1)!} - \frac{N!}{N!} \in \mathbf{Z},$$

while the right hand side becomes

$$a_N + \frac{1}{N+1} < a_N + 1.$$

Hence $0 < N!e^{-1} - a_N < 1$, and therefore $N!e^{-1}$ is not an integer.

1.5.3 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, for instance, 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 [25] which is quoted by Ch. Hermite [17] ("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 same argument we get

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

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.

Instead of this approach, Liouville writes the quadratic relation as $ae+b+ce^{-1}=0$. This time it works:

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

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 we need a little more work 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

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

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

$$A_N, \quad (N+1)B_N, \quad (N+1)(N+2)C_N$$

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

Exercise 3. *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* $n \geq N_0$*.*

1.5.4 The number e^2 is not quadratic

The proof below is the one given by J. Liouville in 1840 [24] . See also [8].

We saw in § 1.5.3 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 $ae^2 + b + ce^{-2} = 0$. Hence

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

Like in § 1.5.3, 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, [16])

$$v_p(N!) = \sum_{j\geq 1} \left\lfloor \frac{N}{p^j} \right\rfloor. \tag{3}$$

Using the trivial upper bound $\lfloor m/p^j \rfloor \leq m/p^j$ 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 (3) yields

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

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 4. *(Continuation of exercise 3). Let $(a_n)_{n\geq 0}$ be a bounded sequence of rational integers. Prove that these properties are also equivalent to*
(iii) *The number*

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

is rational.

Exercise 5. *Prove that $e^{\sqrt{2}}$ is an irrational number.*
`Hint.` Prove the stronger result that $e^{\sqrt{2}} + e^{-\sqrt{2}}$ is irrational.
Prove also the irrationality of $e^{\sqrt{3}}$.

Michel WALDSCHMIDT
Université P. et M. Curie (Paris VI)
Institut Mathématique de Jussieu
Problèmes Diophantiens, Case 247
4, Place Jussieu
75252 Paris CEDEX 05, France
miw@math.jussieu.fr
http://www.math.jussieu.fr/∼miw/

This text is available on the internet at the address
http://www.math.jussieu.fr/∼miw/enseignement.html