Second course: september 14, 2007. [2]

1.2.3 Irrationality of $e^{\sqrt{2}}$ (Following a suggestion of D.M. Masser)

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

$$\frac{(2N)!}{2^N}\vartheta - 2\sum_{m=0}^{N} \frac{(2N)!}{2^{N-m}(2m)!} = 4\sum_{k\geq 0} \frac{2^k(2N)!}{(2N+2k+2)!}\cdot \tag{1.3}$$

The right hand side of (1.3) 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 (1.3) 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 (1.3) 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 a 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.

[2] Updated: October 12, 2007

1.2.4 The number e^2 is not quadratic

The proof below is the one given by J. Liouville in 1840 [3] . See also [1].

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 $ae^2 + b + ce^{-2} = 0$. 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 [2])

$$v_p(N!) = \sum_{j \geq 1} \left[\frac{N}{p^j} \right]. \tag{1.4}$$

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 (1.4) 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.

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 (1.4) 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. The range of applications of this method is limited. The main ideas allowing to go further have been introduced by Charles Hermite. These new ideas are basic for the development of transcendental number theory which we shall discuss later.

1.2.7 A geometrical proof of the irrationality of e

The following proof of the irrationality of e is due to Jonathan Sondow [4]. Start with an interval I_1 of length 1. We are going to construct inductively a sequence of intervals $(I_n)_{n\geq 1}$, where for each n the interval I_n is obtained by splitting I_{n-1} into n intervals of the same length and keeping only one such piece. Hence the length of I_n will be $1/n!$.

In order to have the origin of I_n as

$$1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}$$

we start with $I_1 = [2,3]$. For $n \geq 2$, split I_{n-1} into n intervals and keep the second one: this is I_n. Hence

$$\begin{aligned}
I_1 &= \left[1 + \frac{1}{1!}\,,\, 1 + \frac{2}{1!}\right] = [2,3],\\
I_2 &= \left[1 + \frac{1}{1!} + \frac{1}{2!}\,,\, 1 + \frac{1}{1!} + \frac{2}{2!}\right] = \left[\frac{5}{2!}\,,\, \frac{6}{2!}\right],\\
I_3 &= \left[1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!}\,,\, 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{2}{3!}\right] = \left[\frac{16}{3!}\,,\, \frac{17}{3!}\right].
\end{aligned}$$

The origin of I_n is

$$1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} = \frac{a_n}{n!},$$

the length is $1/n!$, hence the endpoint of I_n is $(a_n+1)/n!$. Also for $n \geq 1$ we have $a_{n+1} = (n+1)a_n + 1$.

The number e is the intersection of all these intervals, hence it lies in the interior of each I_n, and therefore it cannot be written as $a/n!$ with $a \in \mathbb{Z}$.

Since

$$\frac{p}{q} = \frac{(q-1)!\, p}{q!},$$

the irrationality of e follows.

As pointed out by Sondow in [4], the proof shows that for any integer $n > 1$,

$$\frac{1}{(n+1)!} < \min_{m \in \mathbb{Z}} \left| e - \frac{m}{n!} \right| < \frac{1}{n!}\cdot$$

The *Smarandache function* is defined as follows: $S(q)$ is the least positive integer such that $S(q)!$ is a multiple of q:

$$S(1) = 1,\ S(2) = 2,\ S(3) = 3,\ S(4) = 4,\ S(5) = 5,\ S(6) = 3 \ldots$$

Hence $S(n) \leq n$ or all $n \geq 1$, $S(p) = p$ for p prime and $S(n!) = n$. From his proof Sondow [4] deduces an irrationality measure for e: *for any* $p/q \in \mathbb{Q}$,

$$\left| e - \frac{p}{q} \right| > \frac{1}{(S(q)+1)!}\cdot$$

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 consequences of this fact. The first one 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 $p/q \neq \vartheta$,

$$\left| \vartheta - \frac{p}{q} \right| \geq \frac{c}{q}\cdot \tag{1.5}$$

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.

We now give several such criteria. The first one was used implicitly in § 1.2.

1.3.1 Statement of the first criterion

Lemma 1.6. *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 (1.5).

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 1.6 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) will be proved in Lemma 1.8 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.

1.3.2 Proof of Dirichlet's Theorem (i)⇒(iii) in the criterion 1.6

The implications (iii)⇒(iv)⇒(ii)⇒(i) in Lemma 1.6 are easy. It only remains to prove (i)⇒(iii), which is a Theorem due to Dirichlet. For this we shall use the *box* or *pigeon hole* principle.

Proof of (i)⇒(iii). Let $Q > 1$ be given. Define $N = \lceil Q \rceil$: this means that N is the integer such that $N - 1 < Q \le N$. Since $Q > 1$, we have $N \ge 2$.

For $x \in \mathbb{R}$ write $x = [x] + \{x\}$ with $[x] \in \mathbb{Z}$ (integral part of x) and $0 \le \{x\} < 1$ (fractional part of x). Let $\vartheta \in \mathbb{R} \setminus \mathbb{Q}$. Consider the subset E of the unit interval $[0, 1]$ which consists of the $N + 1$ elements

$$0,\ \{\vartheta\},\ \{2\vartheta\},\ \{3\vartheta\},\ \ldots, \{(N-1)\vartheta\},\ 1.$$

Since ϑ is irrational, these $N+1$ elements are pairwise distinct. Split the interval $[0, 1]$ into N intervals

$$I_j = \left[\frac{j}{N}\,,\ \frac{j+1}{N}\right] \quad (0 \le j \le N-1).$$

One at least of these N intervals, say I_{j_0}, contains at least two elements of E. Apart from 0 and 1, all elements $\{q\vartheta\}$ in E with $1 \le q \le N-1$ are irrational, hence belong to the union of the *open* intervals $(j/N,\ (j+1)/N)$ with $0 \le j \le N-1$.

If $j_0 = N-1$, then the interval

$$I_{j_0} = I_{N-1} = \left[1 - \frac{1}{N}\ ;\ 1\right]$$

contains 1 as well as another element of E of the form $\{q\vartheta\}$ with $1 \le q \le N-1$. Set $p = [q\vartheta]+1$. Then we have $1 \le q \le N-1 < Q$ and

$$p - q\vartheta = [q\vartheta] + 1 - [q\vartheta] - \{q\vartheta\} = 1 - \{q\vartheta\}, \quad \text{hence} \quad 0 < p - q\vartheta < \frac{1}{N} \le \frac{1}{Q}\cdot$$

Otherwise we have $0 \le j_0 \le N-2$ and I_{j_0} contains two elements $\{q_1\vartheta\}$ and $\{q_2\vartheta\}$ with $0 \le q_1 < q_2 \le N-1$. Set

$$q = q_2 - q_1, \quad p = [q_2\vartheta] - [q_1\vartheta].$$

Then we have $0 < q = q_2 - q_1 \le N-1 < Q$ and

$$|q\vartheta - p| = |\{q_2\vartheta\} - \{q_1\vartheta\}| < 1/N \le 1/Q.$$

□

There are other proofs of (i)⇒(iii) – for instance one can use Minkowski's Theorem in the geometry of numbers, which is more powerful than Dirichlet's box principle. We shall come back to this point in section § 2.2.7.

1.3.3 Irrationality of at least one number

We shall use the following variant of Lemma 1.6 later.

Lemma 1.7. *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 [3] like in the proof of Lemma 1.6. Consider the Q^m+1 elements

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

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 1.7.

□

1.3.4 Hurwitz Theorem

The following result improves the implication (i)⇒(iv) of Lemma 1.6.

Lemma 1.8. *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 1.8 is weaker than the implication (iv)⇒(i) in Lemma 1.6. What is new is the converse.

Classical proofs of the equivalence between (i) and (iv) involve either continued fractions or Farey series. We give here a proof which does not involve continued fractions, but they occur implicitly.

Lemma 1.9. *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 $\le$ in place of $<$: the strict inequalities are plain from the irrationality of ϑ.

Proof. First let H be a positive integer. Among the irreducible rational fractions a/b with $1\le b\le H$, 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

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

[3] An alternative arguments relies on geometry of numbers - see section § 2.2.7 and W.M. Schmidt's lecture notes - as a consequence it is not necessary to assume that Q is an integer, and the strict inequality $q<Q^m$ can be achieved.

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 $1 \leq q < s$ 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 closer to ϑ than any of these rational fractions. We use the previous argument with $H = \max\{|a|, b\}$. 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.

$\square$

Lemma 1.10. *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

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

one deduces that the number $t = s/q$ satisfies

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

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

$\square$

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

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

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 1.9 and 1.10 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 1.8.

Lemma 1.11. *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 1.10 ; 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 1.10 shows that

$$\frac{s}{q} + \frac{q}{s} \leq \frac{1}{\delta} \quad \text{and} \quad \frac{v}{q} + \frac{q}{v} \leq \frac{1}{\delta} \cdot$$

Hence each of the four numbers s/q, q/s, v/q, q/v satisfies $t + 1/t \leq 1/\delta$. 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 $\delta \geq 1/\sqrt{5}$. This completes the proof of Lemma 1.11. □

References

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

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

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

[4] J. Sondow – *A geometric proof that e is irrational and a new measure of its irrationality*, Amer. Math. Monthly **113** (2006) 637-641.