A proof that e is transcendental

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
30 September, 2021 (at *17:54*)

ABSTRACT: Uses calculus and divisibility to show that e is not algebraic. The file has two proofs, a short one due to Hilbert and a long one, probably of Hermite.

Notation. For posint N, let $\equiv_N$ means "mod-N congruent". Let $::_N::$ mean $\equiv_{N!}$ ie., congruence mod N-factorial.

1: Lemma. *For k a natnum, integral $J_k := \int_0^\infty x^k \mathrm{e}^{-x}\,\mathrm{d}x$ equals*

$$J_k \quad = \quad k!\,. \qquad \Diamond$$

Proof. IByParts yields $J_n = n \cdot J_{n-1}$. And $J_0 = 1$. ♦

2: Corollary. *For each natnum M and intpoly f:*

$$\int_0^\infty f(x)\cdot x^M \mathrm{e}^{-x}\,\mathrm{d}x \quad ::_{M+1}:: \quad f(0)\cdot M!\,.$$

$$\textit{Thus} \quad \int_0^\infty f(x)\cdot x^M \mathrm{e}^{-x}\,\mathrm{d}x \quad ::_M:: \quad 0\,. \qquad \Diamond$$

Hilbert's proof that e is transcendental

The Set-up. FTSOC, suppose e is algebraic of degree $\boldsymbol{D} \in \mathbb{Z}_+$. We thus have an intpoly

$$h(x) := B_{\boldsymbol{D}} x^{\boldsymbol{D}} + \cdots + B_1 x + B_0\,, \text{ with } B_{\boldsymbol{D}} \neq 0,$$

such that $h(\mathrm{e}) = 0$. And $B_0 \neq 0$, since $h()$ has minimal degree. □

Proof of transcendentality. For a posint exponent r to be chosen later, define

$$\Phi(x) \;:=\; [x-1][x-2][x-3]\cdots[x-\boldsymbol{D}]\,, \quad \text{and}$$

$$\mathbf{I}_\ell^u \;:=\; \int_\ell^u x^r \big[\Phi(x)\big]^{r+1} \mathrm{e}^{-x}\,\mathrm{d}x\,, \quad \textit{where } \ell{,}u \in [0,\infty].$$

Thus $0 = 0 \cdot \mathbf{I}_0^\infty = h(\mathrm{e}) \cdot \mathbf{I}_0^\infty = U(r) + L(r)$, where we have split each integral into an Upper part and a Lower part:

$$U(r) \;:=\; B_0 \mathbf{I}_0^\infty + \sum_{K=1}^{\boldsymbol{D}} B_K\, \mathrm{e}^K\, \mathbf{I}_K^\infty\,, \quad \text{and}$$

$$L(r) \;:=\; \sum_{K=1}^{\boldsymbol{D}} B_K\, \mathrm{e}^K\, \mathbf{I}_0^K\,.$$

Since $U(r) + L(r) = 0$, we have that

$$\frac{U(r)}{r!} + \frac{L(r)}{r!} \;=\; 0\,.$$

The contradiction will come by showing that $\frac{U(r)}{r!}$ is always a non-zero integer; then showing that r can be chosen large enough that $\left|\frac{L(r)}{r!}\right|$ is less than 1.

Upperbounding $L(r)$. Over all x in the compact interval $[0, \boldsymbol{D}]$, let $\mathbf{A}$ be an upperbnd for the abs-value of $x \cdot \Phi(x)$ and of $\Phi(x)$. So

$$\left|x^r \Phi(x)^{r+1} \mathrm{e}^{-x}\right| \;\leq\; \mathbf{A}^r \mathbf{A} \cdot 1 \;=\; \mathbf{A}^{r+1}\,.$$

For $K \in [1\,..\,\boldsymbol{D}]$, then, $|\mathbf{I}_0^K| \leq K\mathbf{A}^{r+1} \leq \boldsymbol{D}\mathbf{A}^{r+1}$.

Let $\mathbf{B} := \sum_{K=1}^{\boldsymbol{D}} |B_K| \cdot \mathrm{e}^K$. It follows that

$$|L(r)| \;\leq\; \mathbf{B} \cdot \boldsymbol{D}\mathbf{A}^{r+1}\,.$$

Divided by $r!$, this quantity goes to zero as $r \nearrow \infty$.

Value $U(r)$ is a non-zero multiple of $r!$. Fix a $K \in [1\,..\,\boldsymbol{D}]$. Consider Change-of-Var $y := x - K$. Then $\mathrm{d}x = \mathrm{d}y$, and $\mathrm{e}^K \cdot \mathrm{e}^{-x} = \mathrm{e}^{-y}$. So $\mathrm{e}^K \cdot \mathbf{I}_K^\infty$ equals

$$*: \int_0^\infty [y+K]^r \Big[[y+K-1][y+K-2]\cdots[y+K-\boldsymbol{D}]\Big]^{r+1} \mathrm{e}^{-y}\,\mathrm{d}y.$$

For $K \in [1\,..\,\boldsymbol{D}]$, the K^{th}-term is $[y + K - K]$. Consequently

$$\mathrm{e}^K \cdot \mathbf{I}_K^\infty \;=\; \int_0^\infty f_K(y) \cdot y^{r+1} \mathrm{e}^{-y}\,\mathrm{d}y\,,$$

for some intpoly f_K. Hence

$$\dagger: \qquad \mathrm{e}^K \cdot \mathbf{I}_K^\infty \;::_{r+1}::\; 0\,,$$

by setting $M := r+1$ in (2Lower).

For $K = 0$, integral $\mathbf{I}_0^\infty$ has form $\int_0^\infty f(x) \cdot x^r \mathrm{e}^{-x}\,\mathrm{d}x$, where $f(x) := [\Phi(x)]^{r+1}$. By (2Upper), then,

$$\ddagger: \quad \mathbf{I}_0^\infty \;::_{r+1}::\; f(0)\cdot r! \;=\; \big[[-1]^{\boldsymbol{D}} \cdot \boldsymbol{D}!\big]^{r+1} \cdot r!\,.$$

Adding up $B_K \cdot \mathrm{e}^K \mathbf{I}_K^\infty$ over all $K \in [0\,..\,\boldsymbol{D}]$ gives, courtesy (†,‡), that $\frac{U(r)}{r!}$ is an integer. Moreover,

$$\frac{U(r)}{r!} \;\equiv_{[r+1]}\; B_0 \cdot \big[[-1]^{\boldsymbol{D}} \cdot \boldsymbol{D}!\big]^{r+1}\,.$$

The righthand quantity is not zero, so integer $\frac{U(r)}{r!}$ is not zero. ♦

Credit. The following proof may be due to Hermite. I found several versions on the web. □

Preliminaries. For a poly(nomial) $\mathbf{H}$, I use $\text{Dim}(\mathbf{H})$ for $1+\text{Deg}(\mathbf{H})$; this is the dimension of the vector-space obtained by varying the coefficients of $\mathbf{H}$.

Next[♡1] a few lemmata, then to the details. Use $\binom{7}{2,5}$ for the binomial coeff; it equals $\frac{7!}{2!\cdot 5!}$.

3: Lemma. *For ℓ-times diff'able fncs f and g, the ℓ^{th}-derivative of their product is*

$$3': \qquad [f\cdot g]^{(\ell)} = \sum_{j+k=\ell} f^{(j)}\cdot g^{(k)}\cdot \binom{\ell}{j,k},$$

where the sum is taken over natnums j and k. ◊

4: Prop'n. *Fix an integer T and natnum Q. Let*

$$\mathbf{H}(x) := [x-T]^Q\cdot g(x),$$

where $g()$ is an intpoly. Differentiating,

a: $\forall \ell\in[0..Q):\quad \mathbf{H}^{(\ell)}(T) = 0.$

b: $\forall \ell\in\mathbb{N}:\quad \mathbf{H}^{(\ell)}(T) \;|\!\bullet\; Q!.$

c: $\quad \mathbf{H}^{(Q)}(T) = Q!\cdot g(T).$

If $g(x)=\gamma(x)^{Q+1}$, with γ an intpoly, then

d: $\forall \ell\in\mathbb{N}\setminus\{Q\}:\quad \mathbf{H}^{(\ell)}(T) \;|\!\bullet\; [Q+1]!.$ ◊

Proof. Let $f(x):=[x-T]^Q$. For each natnum $j\neq Q$, note, $f^{(j)}(T)$ is zero. So (3′) yields (4a).

Hence expression $[f\cdot g]^{(\ell)}(T)$ can be non-zero only when $\ell\geq Q$. And $f^{(Q)}(T)=Q!$, so by (3′),

$$*: \qquad [f\cdot g]^{(\ell)}(T) = Q!\cdot g^{(\ell-Q)}(T)\cdot\binom{\ell}{Q,\ \ell-Q}.$$

But $g^{(\ell-Q)}$ is an intpoly, so $g^{(\ell-Q)}(T)$ is an integer. Thus (4b). Setting $\ell:=Q$ in $(*)$ gives (4c).

As for (4d), WLOG $\ell\geq Q+1$ (by (4a)). Note that $g'(x)$ equals $[Q+1]$ times some intpoly. (We don't need to know that the intpoly is $\gamma^Q\cdot\gamma'$.) So

$$\forall k\geq 1: \qquad g^{(k)}(T) \;|\!\bullet\; Q+1;$$

this used that T is an integer. Finally, $(*)$ implies

$$\mathbf{H}^{(\ell)}(T) \;|\!\bullet\; Q!\cdot g^{(k)}(T),$$

where $k:=\ell-Q$. Together with the preceding line, this implies (4d). ♦

5: Trick Lemma. *Consider a poly $\mathbf{H}()$ and real number $T\geq 0$. Let*

$$6: \qquad \langle T,\mathbf{H}\rangle := \int_0^T [-\mathsf{e}^{T-x}]\cdot\mathbf{H}(x)\cdot dx.$$

Letting $N:=\text{Dim}(\mathbf{H})$, then,

$$7: \qquad \langle T,\mathbf{H}\rangle = \Big[\sum_{\ell\in[0..N)}\mathbf{H}^{(\ell)}(T)\Big] - \mathsf{e}^T\cdot Z,$$

where $Z:=\sum_{\ell\in[0..N)}\mathbf{H}^{(\ell)}(0)$. If $T\in\mathbb{N}$ and $\mathbf{H}()$ is an intpoly, then $\langle T,\mathbf{H}\rangle$ is an integer. Note that Z does not depend on T. ◊

Proof. Integrating by-parts, our $\langle T,\mathbf{H}\rangle$ equals

$$[\mathsf{e}^{T-x}]\cdot\mathbf{H}(x)\Big|_{x=0}^{x=T} - \int_0^T [\mathsf{e}^{T-x}]\cdot\mathbf{H}'(x)\cdot dx$$
$$= [\mathbf{H}(T)-\mathsf{e}^T\mathbf{H}(0)] + \langle T,\mathbf{H}'\rangle.$$

Using this recurrence N times gives

$$\langle T,\mathbf{H}\rangle = \text{RhS}(7) + \langle T,\mathbf{H}^{(N)}\rangle.$$

But $\mathbf{H}^{(N)}\equiv 0$, so integral $\langle T,\mathbf{H}^{(N)}\rangle$ is zero. ♦

[♡1] Use $\equiv_N$ to mean "congruent mod N". Let $n\perp k$ mean that n and k are co-prime [no prime in common].

Use $k \bullet\!| \; n$ for "k divides n". Its negation $k\nmid n$ means "k does not divide n." Use $n \;|\!\bullet\; k$ and $n \;\not|\!\bullet\; k$ for "n is/is-not a multiple of k." Finally, for p a prime and E a natnum: Use double-verticals, $p^E \bullet\!\| \; n$, to mean that E is the ***highest*** power of p which divides n. Or write $n \;\|\!\bullet\; p^E$ to emphasize that this is an assertion about n. Use ***PoT*** for Power of Two and ***PoP*** for Power of (a) Prime.

Sequence-properties. Below, "sequence" will mean a sequence of integers *indexed by the primes*, e.g $\vec{\mathbf{V}} = (V_2, V_3, V_5, V_7, V_{11}, \ldots, V_p, \ldots)$.

Say that a $\vec{\mathbf{V}}$ is ***slow*** if there exist posreals α and β with

S1: $$|V_p| \leq \alpha \cdot \beta^p$$

for all large primes p. Evidently:

‡: *A finite linear-combination of slow sequences, is slow.*

The argument for transcendence of e will produce a slow sequence $\vec{\mathbf{V}}$. On the other hand, were e algebraic then each V_p would be an integer with

S2: $$V_p \bullet [p{-}1]!\,, \qquad \text{yet}$$

S3: $$V_p \not\bullet\, p\,.$$

Together (S2,S3) imply that $|V_p| \geq [p{-}1]!$. But this contradicts (S1), seen by sending $p \nearrow \infty$.

The Proof

8: Theorem (Hermite). *e is transcendental.* ◊

Proof. FTSOContradiction, suppose e is algebraic of, say, degree 5. Thus

9: $$\sum_{T \in [0\,..\,6)} C_T \cdot \mathrm{e}^T = 0\,,$$

for some integers $C_0, \ldots, C_5$, with $C_0 \neq 0$.

A dim=N intpoly $\mathbf{H}()$ yields an integer

A1: $$V := \sum_{T \in [0\,..\,6)} C_T \cdot \langle T, \mathbf{H} \rangle\,.$$

Courtesy (7) and (9),

A2: $$V = \sum_{T \in [0\,..\,6)} C_T \cdot \sum_{\ell \in [0\,..\,N)} \mathbf{H}^{(\ell)}(T)\,.$$

We now choose a particular poly $\mathbf{H}()$.

Slownessitude (S1). Each prime p determines a polynomial

10: $$\begin{aligned}\mathbf{H}(x) &:= \mathbf{H}_p(x) \\ &:= [x-0]^{p-1} \cdot \big[[x-1][x-2]\cdot \ldots \cdot [x-5]\big]^p\,.\end{aligned}$$

For each real $x \in [0, 5]$, certainly

$$|\mathbf{H}(x)| \leq 5^{p-1} \cdot [5 \cdot \ldots \cdot 5]^p \overset{\text{note}}{\leq} [5^6]^p\,.$$

To upperbound $\boxed{V_p := V_{\mathbf{H}_p}}$, it suffices to upperbound $\langle T, \mathbf{H}_p \rangle$. Each $T \in [0\,..\,5]$ gives

$$\begin{aligned}|\langle T, \mathbf{H}_p \rangle| &\leq \int_0^T |-\mathrm{e}^{T-x}| \cdot |\mathbf{H}(x)| \cdot \mathrm{d}x \\ &\leq \int_0^5 \mathrm{e}^5 \cdot |\mathbf{H}(x)| \cdot \mathrm{d}x\,.\end{aligned}$$

So $|\langle T, \mathbf{H}_p \rangle| \leq 5 \cdot \mathrm{e}^5 \cdot [5^6]^p$. Hence $p \mapsto \langle T, \mathbf{H}_p \rangle$ is slow. The linear combination (A1), then, is slow; i.e $p \mapsto V_p$ is slow. We have (S1).

For the next two arguments, fix a prime

$$p > \mathrm{Max}(5, |C_0|)$$

and prepare to apply Lemma 4 with $\boxed{Q := p{-}1}$.

Divisibility (S2). Each integer $T \in [0\,..\,5]$ is a zero of $\mathbf{H}()$ with multiplicity at least $p{-}1$. For each natnum ℓ, then,

$$\mathbf{H}^{(\ell)}(T) \bullet [p{-}1]!\,,$$

from (4b). So (A2) implies (S2).

Lack of Divisibility (S3). For integers B and B', use $B \bowtie B'$ to mean:

> *Either both B and B' are divisible by p, or neither is.*

For $T = 1, \ldots, 5$, lemma (4b) yields that each $\mathbf{H}^{(\ell)}(T)$ is divisible by $p!$, hence by p. Thus

$$V \bowtie C_0 \cdot \sum_{\ell \in [0\,..\,N)} \mathbf{H}^{(\ell)}(0)\,.$$

By hypothesis, $0 < |C_0| < p$. Since p is prime,

$$V \bowtie \sum_{\ell \in [0\,..\,N)} \mathbf{H}^{(\ell)}(0)\,.$$

Using (10), the definition

$$\gamma(x) \;:=\; [x-1][x-2]\cdot\ldots\cdot[x-5]$$

shows that $\mathbf{H}()$ has the correct form for lemma (4d). Thus $V \bowtie \mathbf{H}^{(p-1)}(0)$. Using (4c) with $Q := p-1$ and $T := 0$ gives

$$V \quad \bowtie \quad g(0) \overset{\text{note}}{=\!=} \gamma(0)^{p}\,.$$

Hence $V \bowtie \gamma(0)$. And $\gamma(0) \bowtie 5!$. But $5! \not\,\vdots\; p$, since prime p was chosen to exceed the degree, 5, of e's purported minimal-polynomial. ♦

Filename: `Problems/NumberTheory/e_transcendental.latex`
As of: *Tuesday 24Feb2004.* Typeset: *30Sep2021 at 17:54.*