TRANSCENDENCE OF e

KEITH CONRAD

1. Introduction

A complex number z is called *algebraic* if $f(z) = 0$ for a nonzero polynomial f with rational coefficients. Algebraic numbers include $\sqrt{2}$ and $\sqrt{2}+\sqrt{3}$: they are roots of x^2-2 and x^4-10x^2+1. Complex numbers that are not algebraic are called *transcendental*. A transcendental number is a "strong" type of irrational number: the irrational numbers are not roots of linear polynomials with rational coefficients, while transcendental numbers are not roots of polynomials of arbitrary positive degree with rational coefficients.

The concept of a transcendental number is due to Euler. He did not give a precise definition, but he thought of such numbers as "transcending" the methods of algebra. In 1775 he suggested that π is transcendental when he wrote [3, §12]

> "It appears quite certain that the perimeter of a circle constitutes such a peculiar kind of transcendental quantity that it can in no way be compared with any other quantities."

At that time π was already known to be irrational by work of Lambert [7], but its transcendence would take over 100 more years to be established.[1] The first proofs that transcendental numbers really exist appeared in the 19th century.

- In 1844, Liouville [9, p. 885] introduced a technique that proves $\sum_{n\geq 0} 1/b^{n!}$ is transcendental for each integer $b \geq 2$, with full details appearing in 1851 [10]. Such sums are not as mathematically interesting as π or e.
- In 1873, Hermite [4] proved e is transcendental.
- In 1874, Cantor [1] published his first paper on set theory, where he showed that the set of algebraic real numbers is countable while an interval $[a,b]$ with $a<b$ is not. Therefore $[a,b]$ contains transcendental real numbers (otherwise it is a subset of the algebraic real numbers, and hence countable), so transcendental numbers exist.[2]
- In 1882, Lindemann [8] proved π is transcendental by modifying the proof for e.

We'll prove below that e is transcendental. The main tools are (i) the identity $(e^t)' = e^t$ (a characterizing property of e), (ii) integration by parts, and (iii) Taylor's formula for coefficients in terms of higher derivatives.

2. A transcendence criterion

Ultimately all proofs of transcendence of specific numbers are based on the fact that there are no integers between 0 and 1, or equivalently $|n| \geq 1$ for all nonzero integers n. To understand how this can help, let's first see how it implies that rational numbers don't have "good approximations" by other rational numbers. That might sound strange, since

[1] In 1744 Euler [2, §105] said that for positive rational a and b, with $b \neq 1$, if $\log_b a$ is irrational then it is transcendental. This was proved by Gelfond and Schneider, independently, in 1934.

[2] For an account of [1], see `https://en.wikipedia.org/wiki/Cantor's_first_set_theory_article`.

rational numbers are dense in the real line: every real number α can be approximated arbitrarily closed by a rational number, such as by a truncation of its decimal expansion. So how can we say a number can't be approximated well by rational numbers? It's a matter of defining what the term "good approximation" means!

Rather than measuring the approximation of α by a fraction p/q using $|\alpha - p/q|$, we will use $|q\alpha - p|$. Here and below, p and q are integers, with $q > 0$ (denominators are always positive). That is, we consider p/q to be a good approximation to α if $|q\alpha - p|$ is small.[3] That equals $q|\alpha - p/q|$, so we are increasing the usual notion of closeness by a factor coming from the denominator q: the size of the denominator is now just as important for us as the distance between α and p/q in order to consider p/q to be a good approximation to α.

Example 2.1. For $\alpha = \sqrt{3} = 1.732\ldots$, if we use $p/q = 173/100$ (a reduced form fraction), then $|q\alpha - p| = |100\sqrt{3} - 173| \approx .205$, which might seem good, but for the fraction $p/q = 26/15$ we have $|q\alpha - p| = |15\sqrt{3} - 26| \approx .019$, which is ten times less and uses a much smaller denominator (15 vs. 100). So for our purposes, we consider 26/15 to be a much better approximation to $\sqrt{3}$ than 173/100 is.

Let's put this viewpoint to work for the approximation of fractions by other fractions. If $\alpha = a/b$ is rational with $b > 0$ and p/q is another rational number, then $|\alpha - p/q| = |a/b - p/q| = |qa - pb|/bq$, so $|q\alpha - p| = q|\alpha - p/q| = |qa - pb|/b$. Since $p/q \neq \alpha$, $q\alpha - p$ is not 0, so the integer $qa - pb$ is not 0. Thus $|qa - pb| \geq 1$, so $|q\alpha - p| \geq 1/b$: we can't approximate a fraction a/b by other fractions, in the $|q\alpha - p|$ sense, to less than $1/b$. Therefore if α is a real number for which we can find a sequence of *different* fractions p_r/q_r such that $|q_r\alpha - p_r| \to 0$, then α must be irrational: a number that can be approximated too well by rational numbers can't be a rational number. And the converse is true too: for every irrational number α there is a sequence of reduced form fractions p_r/q_r with $q_r \to \infty$ as $r \to \infty$ such that $|q_r\alpha - p_r| < 1/q_r$, so $|q_r\alpha - p_r| \to 0$ as $r \to \infty$.

To improve this criterion for irrationality of α to a criterion for transcendence of α, we'll put a condition on approximations not just of α, but of its powers: if $\alpha, \alpha^2, \ldots, \alpha^m$, for each $m \in \mathbf{Z}^+$, can be simultaneously approximated well by fractions with a suitable *common* denominator, then α is transcendental.

Theorem 2.2. *For nonzero α in $\mathbf{R}$, assume for each $m \in \mathbf{Z}^+$ that there are m sequences of rational numbers $p_{r1}/q_r, \ldots, p_{rm}/q_r$ for $r = 1, 2, \ldots$ such that*

(i) $\max_{1 \leq k \leq m} |q_r\alpha^k - p_{rk}| \to 0$ *as* $r \to \infty$,
(ii) $p_{r1}, \ldots, p_{rm}$ *have a common factor d_r that is relatively prime to q_r and $d_r \to \infty$ as $r \to \infty$.*

Then α is transcendental.

When we refer to the sequences $p_{r1}/q_r, \ldots, p_{rm}/q_r$ for $r \geq 1$, what we mean is the sequences of $(m+1)$-tuples $(p_{r1}, \ldots, p_{rm}, q_r)$, since we use the numerators and denominators in (i) and (ii). And for a given m, we allow $p_{r1}, \ldots, p_{rm}$, and q_r to depend on m.

Proof. Assume α is algebraic, so $a_0 + a_1\alpha + \cdots + a_m\alpha^m = 0$ for some $m \geq 1$ where the rational coefficients $a_0, \ldots, a_m$ are not all 0. Take m as small as possible, which forces $a_m \neq 0$ and

[3]If p/q is not in reduced form, say $p/q = dp'/dq'$ with $d = (p, q)$, then $|q\alpha - p| = d|q'\alpha - p'| \geq |q'\alpha - p'|$, so when $|q\alpha - p|$ is small for a fraction p/q that may not be reduced, replacing p/q with its reduced form will make this new method of measuring a rational approximation smaller, not larger.

$a_0 \neq 0$ (since $\alpha \neq 0$). Multiply through the equation by a common denominator of the coefficients, so we can assume $a_0, \ldots, a_m$ are all integers.

Since p_{rk}/q_r should be a good approximation of α^k, in the relation $a_0 + a_1\alpha + \cdots + a_m\alpha^m = 0$ let's replace α^k with p_{rk}/q_r and see how close to 0 it is:

$$
\begin{aligned}
a_0 + a_1\frac{p_{r1}}{q_r} + \cdots + a_m\frac{p_{rm}}{q_r} &= a_0 + a_1\frac{p_{r1}}{q_r} + \cdots + a_m\frac{p_{rm}}{q_r} - \sum_{k=0}^{m} a_k\alpha^k \quad (2.1)\\
&= a_0 - a_0 + a_1\left(\frac{p_{r1}}{q_r} - \alpha\right) + \cdots + a_m\left(\frac{p_{rm}}{q_r} - \alpha^m\right)\\
&= \sum_{k=1}^{m} a_k\left(\frac{p_{rk}}{q_r} - \alpha^k\right)\\
\Longrightarrow a_0q_r + \sum_{k=1}^{m} a_kp_{rk} &= \sum_{k=1}^{m} a_k(p_{rk} - \alpha^kq_r) \quad (2.2)
\end{aligned}
$$

by clearing the denominator q_r to get the last equation.

The left side of (2.2) is an integer and the right side of (2.2) tends to 0 as $r \to \infty$:

$$\left|\sum_{k=1}^{m} a_k(p_{rk} - \alpha^kq_r)\right| \leq \sum_{k=1}^{m} |a_k||p_{rk} - \alpha^kq_r| \leq \left(\sum_{k=1}^{m} |a_k|\right) \max_{1\leq k\leq m} |p_{rk} - \alpha^kq_r|,$$

where $\sum_{k=1}^{m} |a_k|$ is independent of r and $\max_{1\leq k\leq m} |p_{rk} - \alpha^kq_r| \to 0$ as $r \to \infty$ by condition (i). Since the only integer with absolute value less than 1 is 0, for large enough r

$$a_0q_r + \sum_{k=1}^{m} a_kp_{rk} = 0.$$

By condition (ii), $\sum_{k=1}^{m} a_kp_{rk}$ is divisible by d_r, so $d_r \mid a_0q_r$. Since $(d_r, q_r) = 1$, $d_r \mid a_0$ for large r. Since $d_r \to \infty$ as $r \to \infty$ and $a_0 \neq 0$, we get a contradiction once $|d_r| > |a_0|$. □

3. Transcendence of e

To prove e is transcendental, we follow the basic idea of Hermite's proof with simplifications introduced later by Hilbert [6]. We begin with a calculation based on integration by parts. For a polynomial $f(t)$ with real coefficients and $x \in \mathbf{R}$,

$$\int_0^x e^{-t}f(t)\,dt = f(0) - e^{-x}f(x) + \int_0^x e^{-t}f'(t)\,dt.$$

The integral on the right is the same as that on the left side except f has been replaced by f'. Repeating the integration by parts once more,

$$
\begin{aligned}
\int_0^x e^{-t}f(t)\,dt &= f(0) - e^{-x}f(x) + (f'(0) - e^{-x}f'(x)) + \int_0^x e^{-t}f''(t)\,dt\\
&= (f(0) + f'(0)) - e^{-x}(f(x) + f'(x)) + \int_0^x e^{-t}f''(t)\,dt.
\end{aligned}
$$

Do this repeatedly, and since $f^{(j)} = 0$ for large enough j, the integral term on the right eventually disappears and we're left with

$$\int_0^x e^{-t}f(t)\,dt = \sum_{j\geq 0} f^{(j)}(0) - e^{-x}\sum_{j\geq 0} f^{(j)}(x), \quad (3.1)$$

where the two sums on the right each have finitely many terms since $f^{(j)} = 0$ for large j.

Remark 3.1. On the right side of (3.1), the first sum is $\int_0^\infty e^{-t} f(t)\,dt$ and the second sum is $\int_x^\infty e^{-t} f(t)\,dt$.

Set $I_f(t) := \sum_{j\geq 0} f^{(j)}(t)$. It is a polynomial of degree $\deg f$.[4] Using $I_f(t)$ on the right side of (3.1) and multiplying both sides by e^x, we obtain what is called *Hermite's identity*:

$$e^x \int_0^x e^{-t} f(t)\,dt = I_f(0)e^x - I_f(x) \tag{3.2}$$

for a polynomial $f(t)$.

Theorem 3.2. *The number e is transcendental.*

Proof. We will apply Hermite's identity to a carefully chosen sequence of polynomials $f_r(t)$.

Fix $m \in \mathbf{Z}^+$. For $r \geq 1$, set

$$f_r(t) = t^{r-1}(t-1)^r(t-2)^r \cdots (t-m)^r. \tag{3.3}$$

(Although this polynomial depends on m, we keep m out of the notation to avoid clutter.) What is important about $f_r(t)$ is that it has integral coefficients, high-order zeros at $0, 1, 2, \ldots, m$ when r is large, and the order of its zero at $t = 0$ is one less than the order of its zeros at $1, \ldots, m$. For perspective, in many proofs of transcendence of specific types of numbers, there is a key step involving the construction of polynomials or analytic or meromorphic functions satisfying some type of behavior at specific points, such as high-order zeros at certain points or growth conditions at ∞. While we can define the functions $f_r(t)$ in an explicit way, in more difficult transcendence proofs the existence of suitable functions with growth conditions may only be known by an indirect method, such as from the pigeonhole principle.

In Hermite's identity (3.2), set $x = k$ to be a nonnegative integer:

$$e^k \int_0^k e^{-t} f_r(t)\,dt = I_{f_r}(0)e^k - I_{f_r}(k). \tag{3.4}$$

Since $f_r(t)$ has coefficients in $\mathbf{Z}$, so do its derivatives $f_r^{(j)}(t)$. Therefore $I_{f_r}(0)$ and $I_{f_r}(k)$ are integers. The right side of (3.4) is going to play the role of $q_r\alpha^k - p_{rk}$ in Theorem 2.2 after we remove a common factor in $I_{f_r}(0)$ and $I_{f_r}(k)$ for $1 \leq k \leq m$: we're going to show $I_{f_r}(0)$ is divisible by $(r-1)!$ and $I_{f_r}(k)$ is divisible by $r!$ for $1 \leq k \leq m$.

From Taylor's formula for coefficients in terms of derivatives,

$$f_r(t) = \sum_{j\geq r-1} \frac{f_r^{(j)}(0)}{j!} t^j = \sum_{j\geq r} \frac{f_r^{(j)}(k)}{j!}(t-k)^j,$$

where we can start the sums at $j = r-1$ and $j = r$ because $f_r(t)$ is divisible by t^{r-1} and $(t-k)^r$. Because $f_r(t)$ has integral coefficients, each $f_r^{(j)}(0)/j!$ for $j \geq r-1$ is an integer, which makes $f_r^{(j)}(0)$ a multiple of $j!$. Thus $f_r^{(r-1)}(0)$ is a multiple of $(r-1)!$ and $f_r^{(j)}(0)$ is a multiple of $r!$ when $j \geq r$. The coefficients of $f_r(t)$ as a polynomial in $t-k$ are also integral

[4] The motivation to consider this sum of higher derivatives in $I_f(t)$ comes from the successive use of integration by parts. Integration by parts can be replaced by the Mean Value Theorem, as in the proof of transcendence of e in [5, §5.2] but that leaves the role of $I_f(t)$ completely mysterious.

(since $\mathbf{Z}[t]=\mathbf{Z}[t-k]$), so when $j \geq r$, $f_r^{(j)}(k)/j!$ is an integer and thus $f_r^{(j)}(k)$ is a multiple of $r!$.

In (3.4),

$$I_{f_r}(0)=\sum_{j\geq 0} f_r^{(j)}(0)=f_r^{(r-1)}(0)+\sum_{j\geq r} f_r^{(j)}(0) \tag{3.5}$$

and all terms in the sum over $j \geq r$ are multiples of $r!$. Similarly, $I_{f_r}(k)=\sum_{j\geq r} f_r^{(j)}(k)$ is a multiple of $r!$. Since $I_{f_r}(0)$ and $I_{f_r}(k)$ are multiples of $(r-1)!$, divide (3.4) by $(r-1)!$:

$$\frac{e^k}{(r-1)!}\int_0^k e^{-t} f_r(t)\,dt=\frac{I_{f_r}(0)}{(r-1)!}e^k-\frac{I_{f_r}(k)}{(r-1)!}=q_r e^k-p_{rk}, \tag{3.6}$$

where $q_r=I_{f_r}(0)/(r-1)!$ and $p_{rk}=I_{f_r}(k)/(r-1)!$. The numbers q_r and $p_{r1},\ldots,p_{rm}$ are integers with $\boxed{p_{rk}\equiv 0 \bmod r}$. We can compute $f_r^{(r-1)}(0)$ explicitly: the coefficient of t^{r-1} in $f_r(t)$ is $f_r^{(r-1)}(0)/(r-1)!$, and also by the definition of $f_r(t)$ that coefficient is $(-1)^r(-2)^r\cdots(-m)^r=\pm m!^r$, so $f_r^{(r-1)}(0)=\pm m!^r(r-1)!$. All terms in (3.5) after $f_r^{(r-1)}(0)$ are divisible by $r!$, so $I_{f_r}(0)\equiv \pm m!^r(r-1)! \bmod r!$. Therefore $\boxed{q_r\equiv \pm m!^r \bmod r}$.

We're now going to check that $q_re^k-p_{rk}$ in (3.6) fits conditions (i) and (ii) in Theorem 2.2 when $\alpha=e$.

Condition (i): for $1\leq k\leq m$,

$$\begin{aligned}|q_re^k-p_{rk}| &= \left|\frac{e^k}{(r-1)!}\int_0^k e^{-t}f_r(t)\,dt\right| \\ &\leq \frac{e^k}{(r-1)!}\int_0^k e^{-t}|f_r(t)|\,dt \\ &\leq \frac{e^m}{(r-1)!}\int_0^m e^{-t}|t|^{r-1}|t-1|^r\cdots|t-m|^r\,dt.\end{aligned}$$

When $0\leq t\leq m$, $|t|\leq m$ and $|t-j|\leq m$ for $j=1,\ldots,m$, so

$$|q_re^k-p_{rk}|\leq \frac{e^m}{(r-1)!}\int_0^m e^{-t}m^{r-1}\underbrace{m^r\cdots m^r}_{m\text{ copies}}\,dt=\frac{e^m m^{r-1+mr}}{(r-1)!}\int_0^m e^{-t}\,dt.$$

Since $\int_0^m e^{-t}\,dt=1-e^{-m}<1$,

$$|q_re^k-p_{rk}|<\frac{e^m m^{r-1+mr}}{(r-1)!}=\frac{e^m m^{(m+1)(r-1)+m}}{(r-1)!}=e^m m^m\frac{(m^{m+1})^{r-1}}{(r-1)!}.$$

This upper bound tends to 0 as $r\to\infty$ since $A^{r-1}/(r-1)!\to 0$ for every number A; we use $A=m^{m+1}$ (note m is fixed when verifying condition (i)).

Condition (ii): for $1\leq k\leq m$, we already noted that each p_{rk} is a multiple of r, so $d_r:=r$ is a common factor of $p_{r1},\ldots p_{rm}$. We also saw that $q_r\equiv \pm m!^r \bmod r$, so if $(r,m!)=1$ then $(r,q_r)=1$. To make $(r,m!)=1$, focus on integers r such that $r\equiv 1 \bmod m!$ or use prime r that are greater than m. There are infinitely many such r either way.[5]

[5]Most accounts of a proof of transcendence of e use prime $r>m$ right from the start of the proof, so they only use polynomials $f_p(t)$ where p is prime. This gives an impression that the proof of the transcendence of e actually needs the infinitude of the primes, which is incorrect: just use $r=1+m!M$ for big M since all we need about r is that $(r,m!)=1$ and that we can let $r\to\infty$.

In Theorem 2.2 we work with $r \to \infty$ through the positive integers, but the proof works with r running over any sequence of integers tending to ∞, so by letting $r \to \infty$ through the integers relatively prime to $m!$, we have shown the two conditions in Theorem 2.2 are satisfied when $\alpha = e$, so e is trancendental. □

Remark 3.3. The choice of $f_r(t)$ in (3.3) is due to Hilbert [6] and appears in all modern proofs of transcendence of e. Hermite used other polynomials. A survey of the polynomials used by different authors in proofs of transcendence of e is in [11, pp. 85–88].

The proof of Theorem 2.2 gives, for each m, good rational approximations to $e, e^2, \ldots, e^m$: for $1 \leq k \leq m$, e^k is well approximated by p_{rk}/q_r where $p_{rk} = \sum_{j\geq 0} f_r^{(j)}(k)/(r-1)!$ and $q_r = \sum_{j\geq 0} f_r^{(j)}(0)/(r-1)!$. Both numerators are finite sums since $f_r(t)$ is a polynomial.

Example 3.4. Taking $m = 2$, here is a table of approximations to $e = 2.718281828459\ldots$ and $e^2 = 7.389056098930\ldots$ for $1 \leq r \leq 4$, using $f_r(t) = t^{r-1}(t-1)^r(t-2)^r$.

r	p_{r1}	p_{r2}	q_r	p_{r1}/q_r	p_{r2}/q_r
1	1	3	1	1.000000000	3.0000000000
2	92	250	34	2.705882352	7.3529411764
3	17049	46344	6272	2.718271683	7.3890306122
4	5888864	16007592	2166392	2.718281825	7.3890560895

References

[1] G. Cantor, Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen, *Journal Reine Angew. Mathematik* **77** (1874), 258–262. URL https://eudml.org/doc/148238.

[2] L. Euler, "Introduction to Analysis of the Infinite, Volume 1," M.-M. Bousquet, Lausanne, 1748. URL http://www.17centurymaths.com/contents/introductiontoanalysisvol1.htm.

[3] L. Euler, De relatione inter ternas pluresve quantitates instituenda, *Opuscula Analytica* **2** (1755), 91–101. URL https://scholarlycommons.pacific.edu/euler-works/591/. English translation: http://eulerarchive.maa.org/docs/translations/E591trans.pdf.

[4] C. Hermite, Sur la fonction exponentielle, *Comptes Rendus Acad. Sci. Paris* **77** (1873), 18–24, 74–79, 226–233, 285–293. URL https://gallica.bnf.fr/ark:/12148/bpt6k3034n/f18.item.

[5] I. N. Herstein, "Topics in Algebra," 2nd ed., Wiley, New York, 1975.

[6] D. Hilbert, Ueber die Transcendenz der Zahlen e und π, *Math. Annalen* **43** (1893), 216–219. URL https://eudml.org/doc/157679.

[7] J. H. Lambert, Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques, *Histoire de l'Académie Royale des Sciences et Belles-Lettres de Berlin, Année* 1761 **17** 1768, 265–322. URL http://www.bibnum.education.fr/mathematiques/theorie-des-nombres/lambert-et-l-irrationalite-de-p-1761. English translation at https://hal.archives-ouvertes.fr/hal-02984214/document.

[8] F. Lindemann, Über die Zahl π, *Math. Annalen* **20** (1882), 213–225. URL https://eudml.org/doc/157031.

[9] J. Liouville, Sur les classes très-étendues de quantités dont la valeur n'est ni rationelle ni même réductible à des irrationelles algébriques, *Comptes Rendus Acad. Sci. Paris* **18** (1844), 883–885, 910–911. URL http://www.bibnum.education.fr/mathematiques/theorie-des-nombres/propos-de-l-existence-des-nombres-transcendants.

[10] J. Liouville, Sur les classes très-étendues de quantités dont la valeur n'est ni algébrique, *Journal Math. Pures et Appl.* **16** (1851), 133–142. URL https://gallica.bnf.fr/ark:/12148/bpt6k16395z/f141n10.capture.

[11] N. I. Feldman and Y. V. Nesterneko, "Number Theory IV: Transcendental Numbers," Springer-Verlag, Berlin, 1998.

[12] A. Shidlovskii, "Transcendental Numbers," de Gruyter, Berlin 1989.