# A Historical Introduction to Transcendental Number Theory

Varun Rao

June 2022

Abstract. Transcendental numbers are an intriguing, yet mysterious, subject in number theory. In this paper, we discuss some fundamental theorems in the study of transcendental numbers from a historical perspective. In proving these theorems we illustrate the techniques used to discover transcendence, such as auxiliary polynomials, rational approximations, and a general strategy to build upon. We attempt to build an intuitive foundation for the reader without requiring many prerequisites.

## 1 Introduction

> "Our knowledge of transcendental numbers is extraordinarily limited, and thus these commonplace numbers remain safely shrouded in a veil of mystery."

This quote from *Making Transcendence Transparent* by Burger and Tubbs (see [BT04]) characterizes the transcendental numbers and their seemingly obscure nature. In this exposition, we will attempt to reach a higher level of understanding of transcendence.

The main results we prove are the existence of transcendental numbers, Liouville's theorem on Diophantine approximation, the transcendence of $e$ and $\pi$, and the Lindemann Weierstrass theorem.

We begin by defining the various types of numbers and then discover the existence of transcendental numbers with an argument of Georg Cantor. Next, we use some ideas from Diophantine approximation to construct the first known transcendental numbers, due to Liouville. We then state a general strategy to prove transcendence and apply it to Hermite's proof that $e$ is transcendental. Hermite's argument can be modified to prove the transcendence of $\pi$, and we extend this further to a generalization known as the Lindemann-Weierstrass theorem.

## 2 Cantor and Classifications of Numbers

### 2.1 The History of Numbers

To define transcendence effectively, we take a chronological excursion through the different classes of numbers. We begin with the set of numbers used for counting: $\{1, 2, 3, 4, 5, \dots\}$. These are the natural numbers, $\mathbb{N}$. If we take a deeper, more analytical look at $\mathbb{N}$, we may

notice that it is closed under addition. In other words, for all $x, y \in \mathbb{N}$, $x+y \in \mathbb{N}$. Moreover, $\mathbb{N}$ is closed under multiplication. (Note that multiplication is simply repeated addition.) What about subtraction? Consider the counterexample $2 - 5$, which has no solution in $\mathbb{N}$. To construct a set which is closed under subtraction, we must add 0 and the negative numbers, to create $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, the integers. However, we have still left out one basic operation: division. We can verify that $\mathbb{Z}$ is not closed under division (take $2 \div 5$, for example). What more do we need to perform all four basic operations freely? Fractions. With this addition, we have the rational numbers $\mathbb{Q}$, in which we can perform a large range of calculations.

For approximately 1100 years after the discovery of the first fractions, ancient civilizations believed that all numbers were rational. Even $\sqrt{2}$, discovered using the Pythagorean Theorem, was conjectured to be rational at first. However, Pythagorean mathematicians later realized that $\sqrt{2}$ was irrational. This discovery was so appalling and controversial that it was kept secret. Legend claims that Hippasus of Metapontum was the first to reveal a proof to the public and was drowned as a result.

Nevertheless, mathematicians began to accept the notion of irrational numbers, and the real numbers $\mathbb{R}$ became the new set believed to contain all numbers. With the development of algebra in Arabia, it was noticed that most real numbers could be represented as solutions to some polynomial. The handful of exceptions included $e$ and $\pi$, but they had not even been proven to be irrational. Thus, it was conjectured that they too were roots to some undiscovered polynomials.

Complex and imaginary numbers were invented in the 1500s to fill in the missing roots to polynomial equations. With so many numbers which could be characterized by polynomials, many wondered if all numbers satisfied this condition.

**Definition 2.1.** A complex number is *algebraic* if it is a root of some nonzero polynomial with integer (or equivalently rational) coefficients.

Were all numbers algebraic, or did there exist some which could transcend the world of algebra? (See Figure 2.1 for a diagram of the numbers conjectured to be algebraic.) We travel to the late 19th century, when Georg Cantor provided a straightforward argument to answer this question using the cardinalities of sets.

## 2.2 Countability

We begin with a definition:

**Definition 2.2.** The *cardinality* of a set $S$ is a measure of the number of elements in $S$, denoted $|S|$. For finite sets, the cardinality is simply the number of elements in the set, but this has been generalized to infinite sets as well. Two sets have the same cardinality if there is a bijection between them.

In his first set theory article (see [Gra94]), Cantor developed the notion of countability.

**Definition 2.3.** An infinite set $S$ is said to be *countable* if $|S| = |\mathbb{N}|$. (All finite sets are also countable, but this is of little significance.)

Equivalently, if an infinite set is countable, then there exists some order in which we can "count" its elements. We now make the following claim, which is intuitively surprising at first:

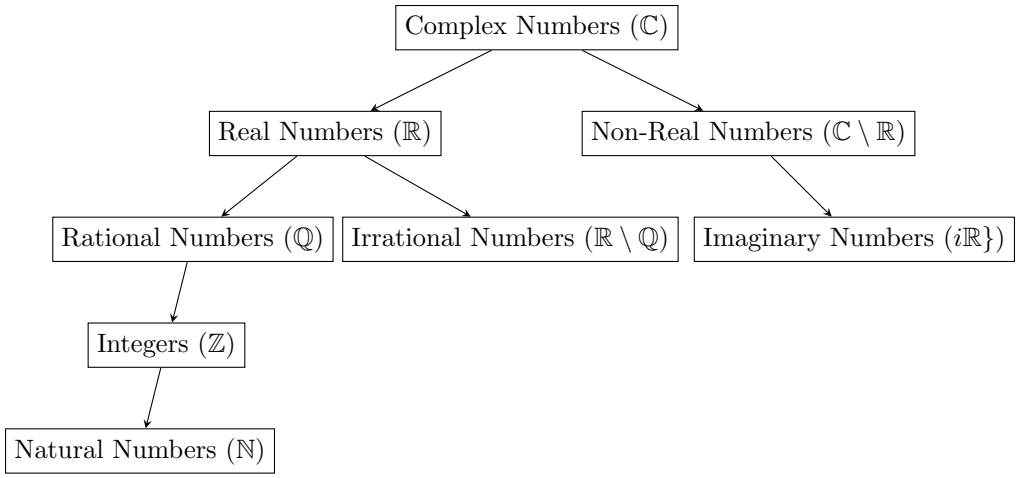


Figure 2.1: Number Classification Tree

**Theorem 2.4.** *The integers $\mathbb{Z}$ are countable. In other words, $|\mathbb{Z}| = |\mathbb{N}|$.*

*Proof.* For every $n \in \mathbb{N}$, both $n$ and $-n$ are elements of $\mathbb{Z}$. Therefore, it is natural to expect that $|\mathbb{Z}|$ is at least 2 times $|\mathbb{N}|$. It turns out, however, that constant factors like 2 are insignificant in the presence of infinite quantities like $|\mathbb{N}|$.

To show that $|\mathbb{N}| = |\mathbb{Z}|$, we provide a one-to-one correspondence from the natural numbers to the integers and vice versa. Consider the following function $f : \mathbb{N} \to \mathbb{Z}$ and its inverse $f^{-1} : \mathbb{Z} \to \mathbb{N}$:

$$f(x) = \begin{cases} 0 & x = 1 \\ \frac{x}{2} & x \equiv 0 \pmod 2 \\ -\frac{x-1}{2} & x \equiv 1 \pmod 2, x \neq 1 \end{cases}.$$

$$f^{-1}(x) = \begin{cases} 1 & x = 0 \\ 2x & x > 0 \\ -2x + 1 & x < 0 \end{cases}.$$

We can verify $f$ is a bijection between $\mathbb{N}$ and $\mathbb{Z}$. Thus, $\mathbb{Z}$ is countable. □

With Theorem 2.4 established, we propose an even more seemingly outlandish statement:

**Theorem 2.5.** *The rational numbers $\mathbb{Q}$ are countable.*

*Proof.* We will present a strategy to "count" the rational numbers rather than a function. Figure 2.2 depicts the strategy visually. Consider the points of $\mathbb{Z}^2$ on a coordinate plane. Starting at $(0, 0)$, follow the blue counterclockwise spiral of points depicted in the figure. We now explain what to do at any point in time.

Suppose that during our counting strategy, we are at point $(i, j)$ and have counted the first $n$ elements of $\mathbb{Q}$ called $a_1, a_2, \ldots, a_n$. Then, if $\frac{i}{j} = a_k$ for some $1 \leq k \leq n$ or if $\frac{i}{j}$ is undefined, call the point $(i, j)$ "bad." (In the figure, we have circled all bad points in red.)

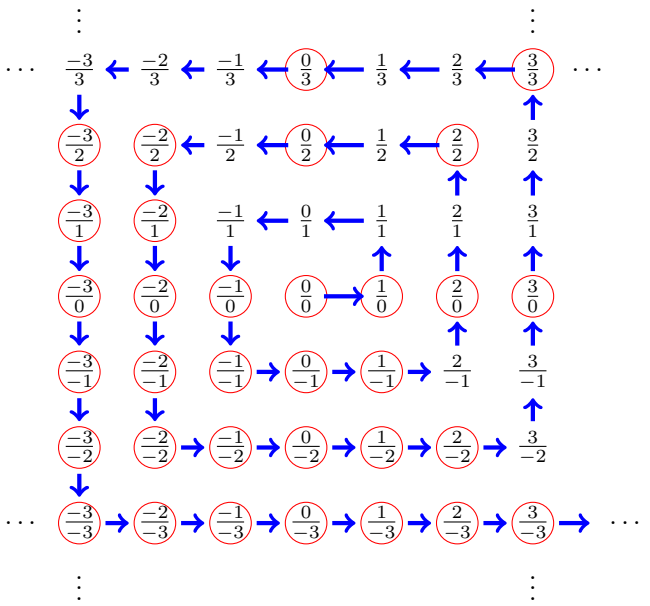

Figure 2.2: Counting the rational numbers.

If $(i, j)$ is bad, then continue to the next point in the spiral. Otherwise, set $a_{n+1} = \frac{i}{j}$ and continue to the next point in the spiral.

This strategy is a valid bijection between $\mathbb{N}$ and $\mathbb{Q}$ because given a natural number, we can move along the spiral to find its corresponding rational number. Similarly, given a rational number, we can follow the spiral and strategy for a finite number of moves until we reach the integer which it corresponds to. □

The instinctive confusion we may initially have with the statements of Theorems 2.4 and 2.5 can be allayed with the following lemma, which can be applied to both results:

**Lemma 2.6.** *The union of countably many countable sets is countable.*

*Proof.* Suppose we have a countable number of sets, each of which is countable. Since we have countably many sets, we can count them in some order, say $A_1, A_2, A_3, A_4, \ldots$. Now, since each set is countable, we can count the elements of $A_i$. We denote the $j$th element of $A_i$ as $a_{i,j}$.

Our next step is to an order by which to count all the $a_{i,j}$'s. We begin by sorting all the $a_{i,j}$'s by their corresponding sum $i + j$. For $i + j = 2$, there is only one such element: $a_{1,1}$. We count this as the first element. For $i + j = 3$, we have $a_{1,2}$ and $a_{2,1}$. We count $a_{1,2}$ as the second element and $a_{2,1}$ as the third element because $a_{1,2}$ has a smaller $i$. Continuing this strategy, we iterate through each possible $i + j$, sorting all of its corresponding $a'_{i,j}s$ by $i$ value. The first few elements we count are

$$a_{1,1},\ a_{2,1},\ a_{1,2},\ a_{1,3},\ a_{2,2},\ a_{3,1},\ a_{1,4},\ a_{2,3},\ a_{3,2},\ a_{4,1},\ \ldots$$

Since we are considering the union, there may be some duplicate elements. We can simply remove those from our count if we encounter them along the way. We have presented an order to count the union of $A_1, A_2, A_3, A_4, \ldots$, so it is countable. □

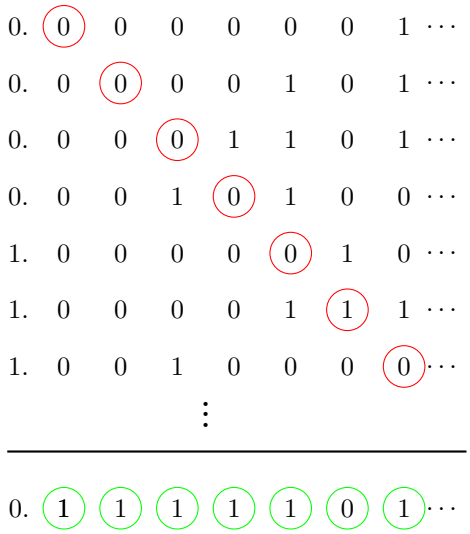


Figure 2.3: Cantor's diagonalization argument.

Now, we are ready to discuss Cantor's article. His two main claims:

**Theorem 2.7.** *The algebraic numbers are countable.*

**Theorem 2.8.** *The real numbers $\mathbb{R}$ are uncountable, or not countable.*

*Proof of Theorem 2.7.* If we can show that the roots of all nonzero polynomials with integer coefficients of degree $d$ form a countable set, then we can apply Lemma 2.6 to prove our desired result. We have already shown this for $d = 1$, since those are the rational numbers. For other integers $d$, we have the following counting strategy:

Consider the set $P_d$ of all such polynomials of degree $d$, in the form

$$a_d x^d + a_{d-1} x^{d-1} + \cdots + a_2 x^2 + a_1 x + a_0.$$

Sort $P_d$ lexicographically by the coefficients $a_d, a_{d-1}, \ldots, a_2, a_1, a_0$. Now, iterating through $P_d$ in this order, sort each polynomial's roots by their complex magnitude and count them. When there are duplicates, do not count them a second time.

Thus, the algebraic numbers are countable. □

For the second claim, we present the famous proof known as Cantor's diagonalization argument. Contrary to popular belief, this was not presented in Cantor's first set theory article but in a later publication.

*Proof of Theorem 2.8.* See Figure 2.3 for a visualization of this proof. Suppose on the contrary that $\mathbb{R}$ is countable. Then, we can count all of the reals in some order, say as $a_1$, $a_2$, $a_3$, .... Write down the list of $a_i$'s in binary, such that the decimal points of each $a_i$ line up. Add trailing zeroes if necessary. The list we have should form a table of digits like that in the figure.

We will now construct a real number $\alpha$ in the interval $[0, 1]$ which cannot possibly be in our list. For every natural number $i$, make the $i$th digit after the decimal point of $\alpha$ the

opposite of the $i$th digit after the decimal point of $a_i$. That is, if the $i$th digit of $a_i$ is 0, let the $i$th digit of $\alpha$ be 1, and vice versa. We claim that the binary number $\alpha$ built by this process cannot be in our list. This is because for any natural number $i$, $\alpha \neq a_i$ since their $i$th digits are different. We have reached a contradiction by showing that there always exists a real number which is not in our list, regardless of its size. This completes the proof. $\square$

Here is an immediate corollary of the uncountability of $\mathbb{R}$:

**Corollary 2.8.1.** *The complex numbers $\mathbb{C}$ are uncountable.*

*Proof.* Since $\mathbb{R} \subset \mathbb{C}$ and $\mathbb{R}$ is uncountable, $|\mathbb{N}| < |\mathbb{R}| \leq |\mathbb{C}|$. $\mathbb{C}$ has cardinality greater than that of the natural numbers, so it is uncountable. $\square$

Since the set of all algebraic numbers is countable while the set of all complex numbers is uncountable, Cantor concluded that there must exist complex numbers which are not algebraic. (In fact, the vast majority of complex numbers are not algebraic.) With this established, we are finally ready to define the transcendental numbers.

**Definition 2.9.** A complex number is *transcendental* if it is not algebraic.

Notice that the transcendental number is defined by what it is not, rather than what it is. This nuance is the root cause of the extreme difficulty it requires to show that a number is transcendental.

# 3 Liouville Discovers Transcendence

Georg Cantor was not the first to disprove the conjecture that all complex numbers are algebraic. In 1844, thirty years before Cantor's work, Joseph Liouville did the same by cleverly constructing the first transcendental numbers from an elegant result. To understand what influenced his thought process, we present some ideas from Diophantine approximation.

## 3.1 Diophantine Approximation

Diophantine approximation is the approximation of irrational numbers with rational numbers, having origins in Ancient Greece. For ancient civilizations, rational approximations of many irrational numbers were of practical use in fields like architecture and engineering. Additionally, early mathematicians were very interested in computing famous irrational numbers to various levels of precision. As a result, by Liouville's time, significant progress had been made in the theory of Diophantine approximation.

To develop some basic intuition on the subject, let's try to approximate $\sqrt{2}$ ourselves. Without much thought, we can come up with $\frac{3}{2}$. This may seem useless, but given the size of its denominator, $\frac{3}{2}$ is indeed quite close to $\sqrt{2}$. With a bit more experimentation, we can find $\frac{7}{5}$, which is within 2 hundredths of $\sqrt{2}$. Much closer, but can we do better? $\frac{17}{12}$ is the next approximation which is noticeably better than $\frac{7}{5}$, getting within 3 thousandths of $\sqrt{2}$. If we continue this trend, we get the following sequence, known as the Pell-Lucas numbers:

$$\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \frac{239}{169}, \frac{577}{408}, \ldots.$$

Evidently, we can find more rational approximations and get closer and closer to $\sqrt{2}$, but the denominators of the approximations are growing rapidly. Is $\frac{577}{408}$ really that much better

than $\frac{17}{12}$, given the level of precision with which twelfths are defined as opposed to 408ths? Similarly, is the rate at which the denominators of the approximations grow proportional to the rate at which the distance to $\sqrt{2}$ shrinks?

We can measure how "good" a rational approximation $\frac{p}{q}$ of some real $\alpha$ is by counting how many orders of magnitude (in terms of $q$) it is away from $\alpha$. Mathematically phrased, the largest integer $u$ such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^u}$$

helps measure how good $\frac{p}{q}$ is at approximating $\alpha$. We now have the background to motivate Liouville's result.

## 3.2 Liouville's Theorem

In his studies of Diophantine approximation, Liouville noticed that irrational algebraic numbers cannot be approximated very well by rational numbers. We provide a preliminary definition before stating the theorem:

**Definition 3.1.** The *minimal polynomial* $p(z)$ associated with an algebraic number $\alpha$ is the unique polynomial satisfying the following criteria:

- $p(\alpha) = 0$,
- $p(z)$ is irreducible,
- the coefficients of $p(z)$ are all relatively prime integers,
- the leading coefficient of $p(z)$ is positive.

**Theorem 3.2** (Liouville)**.** *Suppose $\alpha$ is an irrational algebraic number, and $d$ is the degree of the minimal polynomial associated with $\alpha$. Then, there exists some constant $c$ depending entirely on $\alpha$ such that for all rationals $\frac{p}{q}$, we have*

$$\frac{c}{q^d} \leq \left|\alpha - \frac{p}{q}\right|.$$

That is to say, if $\alpha$ is irrational and algebraic, $\alpha$ cannot be approximated by some rational $\frac{p}{q}$ which gets within $-d$ orders of magnitude ($q^{-d}$) of $\alpha$.

*Proof.* We begin with the case where $\alpha$ is a complex number. Let $\alpha = a + bi$ for some $a, b, \in \mathbb{R}$. Then, since $\frac{p}{q}$ is a real number,

$$\left|\alpha - \frac{p}{q}\right| = \left|a + bi - \frac{p}{q}\right| \geq b \geq \frac{b}{q^d}.$$

Thus, we let $c = b$ since $\frac{b}{q^d} \leq b \leq |\alpha - p/q|$. From now on, we assume that $\alpha \in \mathbb{R}$. We now consider another case: where $\frac{p}{q}$ is a bad approximation of $\alpha$. If

$$1 < \left|\alpha - \frac{p}{q}\right|,$$

then we can simply set $c = 1$ since $\frac{1}{q^d} \leq 1$ for all $q, d$. Now, we can assume $\frac{p}{q}$ is at most 1 away from $\alpha$ for the rest of the proof.

Let $f$ be the minimal polynomial of $\alpha$, and recall that $d$ is the degree of $f$ by definition. Consider $f(p/q)$, which is

$$f\left(\frac{p}{q}\right) = a_d\left(\frac{p}{q}\right)^d + a_{d-1}\left(\frac{p}{q}\right)^{d-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0,$$

where the $a_i$'s are the integer coefficients of $f$. We can rewrite this expression as a fraction with denominator $q^d$ as follows:

$$f\left(\frac{p}{q}\right) = \frac{a_d p^d + a_{d-1}p^{d-1}q + \cdots + a_1 pq^{d-1} + a_0 q^d}{q^d}.$$

For simplicity, let $N$ be the numerator of the RHS. Note that $N$ is an integer. It is also nonzero because $f$ is irreducible, so $f(p/q) \neq 0$. We can use these two facts to construct a simple bound:

$$\frac{1}{q^d} \leq \frac{|N|}{q^d} = \left|f\left(\frac{p}{q}\right)\right|.$$

The LHS of the inequality is starting to look like what we want, and it explains the motivation for considering $f(p/q)$. But we are still missing one piece of the puzzle: $\alpha$. Since $f(\alpha) = 0$ by definition, we can simply add it in as we like. We now have

$$\frac{1}{q^d} \leq \left|f(\alpha) - f\left(\frac{p}{q}\right)\right|.$$

We need to get rid of $f$ in our inequality and somehow end up with $|\alpha - p/q|$ on the RHS. Fortunately, the Mean Value Theorem fixes this issue. It states that for some $\xi$ in between $\alpha$ and $\frac{p}{q}$,

$$f'(\xi)\left(\alpha - \frac{p}{q}\right) = f(\alpha) - f\left(\frac{p}{q}\right).$$

Substituting this into our inequality gives

$$\frac{1/|f'(\xi)|}{q^d} \leq \left|\alpha - \frac{p}{q}\right|.$$

It seems as if we can set $c = 1/|f'(\xi)|$ and complete the proof, but $\xi$ is defined in terms of both $\alpha$ and $\frac{p}{q}$. We need a constant determined entirely by $\alpha$. By our assumption early in the proof that $|\alpha - \frac{p}{q}| \leq 1$, we know that $\alpha - 1 \leq \xi \leq \alpha + 1$. Therefore, we can set

$$m = \max_{\alpha - 1 \leq x \leq \alpha + 1} |f'(x)|.$$

Note that $m$ depends entirely on $\alpha$. Since $m \geq |f'(\xi)|$, we know that

$$\frac{1/m}{q^d} \leq \frac{1/|f'(\xi)|}{q^d} \leq \left|\alpha - \frac{p}{q}\right|.$$

Thus, we set $c = \frac{1}{m}$ for the case when $\alpha$ is real and $|\alpha - p/q| \leq 1$ □

## 3.3 The First Transcendental Numbers

Since we have shown that irrational algebraic numbers cannot be approximated very well by rationals, any such number that can must be transcendental! Our first transcendental number:

**Corollary 3.2.1.** *The number*

$$\mathcal{L}_1 = \sum_{n=1}^{\infty} 10^{-n!} = 0.11000100000000000000000100\ldots$$

*is transcendental.*

*Proof.* We first show that $\mathcal{L}_1$ is irrational so that we can derive a contradiction from Liouville's theorem. To do this, note that the number of zeros between each pair of ones in the decimal expansion grows without bound, so $\mathcal{L}_1$ cannot be a terminating or repeating decimal. Now that we know $\mathcal{L}_1$ is irrational, suppose for the sake of contradiction that there exists some $c$ satisfying

$$\frac{c}{q^d} \leq \left|\mathcal{L}_1 - \frac{p}{q}\right|$$

for all $p, q$. We will use some good rational approximations of $\mathcal{L}_1$ to show that there $p, q$ for which we cannot construct a valid $c$ in terms of $\alpha$. Consider truncations of the the series which defines $\mathcal{L}_1$, or

$$\frac{p_N}{q_N} = \sum_{n=1}^{N} 10^{-n!}.$$

We set

$$p_N = 10^{N!} \sum_{n=1}^{N} 10^{-n!},$$
$$q_N = 10^{N!}.$$

Because of the way $\mathcal{L}_1$ is defined, these are very good approximations of it. We have

$$\left|\mathcal{L}_1 - \frac{p}{q}\right| = \sum_{n=1}^{\infty} 10^{-n!} - \sum_{n=1}^{N} 10^{-n!} = \sum_{n=N+1}^{\infty} 10^{-n!}.$$

To bound $c$, we can form an upper bound on $|\mathcal{L}_1 - \frac{p}{q}|$, which is easy to do with a geometric series. Since $10^{-n!} < 10^{-n}$ for all $n > 2$,

$$\left|\mathcal{L}_1 - \frac{p}{q}\right| = \sum_{n=N+1}^{\infty} 10^{-n!} < \sum_{n=N+1}^{\infty} 10^{-n} = \frac{10}{9} 10^{-(N+1)!}$$

by the formula for geometric series. Connecting this to our proposed inequality with $c$, we have

$$\frac{c}{q^d} = 10^{-dN!} c \leq \left|\mathcal{L}_1 - \frac{p}{q}\right| < \frac{10}{9} 10^{-(N+1)!}.$$

To reach the contradiction, we remove the middle expression to deal with just $c$, $d$, and $N$. Because $0 < 10^{-dN!} c$, we have

$$0 < 10^{-dN!} c < \frac{10}{9} 10^{-(N+1)!},$$

which can be rewritten as

$$0 < 9 < \frac{10}{c} 10^{dN! - (N+1)!}.$$

For any $N \geq d$, the exponent $10^{dN! - (N+1)!}$ gets arbitrarily close to 0 as $N$ increases. Thus, if we choose sufficiently large $N$, the RHS expression will be less than 1 regardless of $c$ ($c$ cannot be defined in terms of $N$). This gives us

$$0 < 9 < \frac{10}{c} 10^{dN! - (N+1)!} < 1$$

for $N$ greater than some $N_1$. Since 9 is not in between 0 and 1, we have a contradiction. The only problem with our argument is the assumption that Liouville's Theorem holds true for $\mathcal{L}_1$, so $\mathcal{L}_1$ is transcendental. □

All numbers which can be approximated very well like $\mathcal{L}_1$ are named after Liouville in his honor.

**Definition 3.3.** A *Liouville number* is a real number with very good rational approximations. Formally, $\mathcal{L}$ is a Liouville number if for all positive integers $n$, there exists a rational number $\frac{p}{q}$ such that

$$\left| \mathcal{L} - \frac{p}{q} \right| < \frac{1}{q^n}.$$

By Liouville's theorem and the definition of Liouville numbers, we know that

**Theorem 3.4.** *All Liouville numbers are transcendental.*

An interesting consequence of the way Liouville numbers are defined is the following:

**Theorem 3.5.** *Every real number can be represented as the sum and product of two Liouville numbers.*

See [Erd32] for the proof. With Theorem 3.5 established, it seems as if the Liouville numbers are abundant and might even be able to help us prove the transcendence of other real numbers. However, this is not the case. It turns out that the set of Liouville numbers has measure 0. In other words, the probability of randomly choosing a Liouville number from $\mathbb{R}$ is 0.

We conclude by realizing that the Liouville numbers were designed specifically to make it easier to prove their transcendence. Because the vast majority of numbers do not have desirable Liouville properties, we must employ other techniques to discover more transcendental numbers.

It is logical to wonder whether the bound $c/q^d$ in Liouville's theorem can be improved to reveal the transcendence of more numbers and provide a better characterization of the algebraic numbers. This was of great interest to many mathematicians, including Axel Thue, Carl Ludwig Siegel, Freeman Dyson, and Klaus Roth. Roth was awarded the Fields Medal in 1958 for his groundbreaking improvement:

**Theorem 3.6.** *Suppose $\alpha$ is an irrational algebraic number and $\epsilon$ is any (very small) positive number. Then, there exists a positive constant $c$ depending on $\alpha$ and $\epsilon$ such that for all rationals $\frac{p}{q}$,*

$$\frac{c}{q^{2+\epsilon}} < \left| \alpha - \frac{p}{q} \right|.$$

Roth's theorem allows us to prove the transcendence of a few more numbers (such as the Champernowne constant), but even now, the vast majority of transcendental numbers remain unproven. Is more work being done to improve Roth's result and perhaps unearth more transcendental numbers? It turns out that Roth optimized Liouville's theorem so well that it cannot be pushed much further. Consider this immediate corollary of Dirichlet's approximation theorem:

**Theorem 3.7.** *For irrational $\alpha$, there exist infinitely many integers $p, q$ such that*

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

This means that if $\epsilon = 0$ in Theorem 3.6, the statement would not hold. Roth's theorem is (almost) the best possible improvement to Liouville's theorem. Therefore, we are forced to abandon Liouville's techniques in pursuit of more results about transcendence.

We noticed that the Liouville numbers have a special property which helps dramatically in proving their transcendence: good rational approximations. Another number with many special properties and more mathematical relevance is $e$. We investigate its transcendence next.

# 4 The Transcendence of $e$

Euler's number $e$ is needs no introduction, appearing in a variety of formulas and natural observations. Among the numbers conjectured to be transcendental after Liouville's results, $e$ was the first to be proven so, by Charles Hermite in 1873. We begin our discovery that $e$ and a number of its cousins are transcendental by providing a general strategy to prove transcendence. Some of the strategy is motivated by our proof of Corollary 3.2.1.

## 4.1 How to Prove a Number is Transcendental

This subsection is adapted primarily from [BT04].

Suppose we wish to prove that $\alpha$ is transcendental. Since a transcendental number is defined by being *not* algebraic, we will employ proof by contradiction. Consequently, our first step is to assume that $\alpha$ is the solution to some nonzero polynomial with integer coefficients, say

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_2 x^2 + a_1 x + a_0.$$

We wish to show that if $p(\alpha) = 0$, we can manipulate this equation to derive a contradiction to some underlying principle of mathematics.

One way to do this is to build an integer $N$ using the coefficients of $p$ and $\alpha$. If we build a good integer $N$ using some properties of $\alpha$, we can provide lower and upper bounds on $N$. We can use these bounds to show that $N$ lies between consecutive integers or even conflicting bounds (ie $A < N$ and $N < B$ but $A > B$). Since $N$ is not an integer, we have reached a contradiction.

Now, (if all our statements directly follow from each other,) the only possible flaw in the argument is our assumption that $\alpha$ is algebraic. Thus, $\alpha$ is transcendental. See Table 4.1 for a condensed version of this subsection.

Building an integer $N$ which we can bound requires some helpful properties of $\alpha$. Therefore, to begin our journey to the transcendence of $e$, we state a few useful facts about $e$:

| | Steps |
|---|---|
| 1. | Assume on the contrary that $\alpha$ is a root of some polynomial $p$. |
| 2. | Build an integer $N$ using $\alpha$ and the coefficients of $p$. |
| 3. | Find a lower bound $A$ on $N$. |
| 4. | Find an upper bound $B$ on $N$. |
| 5. | Show that $N$ cannot be an integer using $A$ and $B$. |
| 6. | Conclude that since $N$ cannot be an integer, $\alpha$ must be transcendental! |

Table 4.1: Six Steps to Prove $\alpha$ is Transcendental

**Theorem 4.1.**

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = \frac{1}{0!} + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots.$$

**Theorem 4.2** (Gamma function)**.**

$$\Gamma(n) = \int_0^{\infty} x^{n-1} e^{-x} dx = (n-1)!.$$

**Theorem 4.3** (Euler)**.**

$$e^{i\theta} = \cos(\theta) + i\sin(\theta).$$

**Corollary 4.3.1.**

$$e^{i\pi} = -1.$$

## 4.2 The Irrationality of $e$

To motivate how we will approach the transcendence of $e$, let's start with a simpler problem. Instead of showing $e$ is not the solution to any polynomial with integer coefficients, we can consider only polynomials of degree 1. Namely, we will show that

**Theorem 4.4.** *$e$ is irrational.*

We present Fourier's remarkably quick proof.

*Proof.* Suppose, for the sake of contradiction, that $e$ is rational. Then, let the nonzero polynomial $p(x) = sx - r$ satisfy $p(e) = 0$. Then, it follows that $e = \frac{r}{s}$.

Following the strategy from the previous section, our next step is to build an integer which we can bound. Consider Theorem 4.1, which we restate:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = \frac{1}{0!} + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots.$$

If we substitute $x = 1$, we have

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \dots. \tag{1}$$

This allows us to produce very good approximations of $e$ by truncating the series. If we subtract the truncation at $s$ from $e$, we get

$$e - \sum_{n=0}^{s} \frac{1}{n!} = \frac{r}{s} - \sum_{n=0}^{s} \frac{1}{n!}.$$

This is evidently a positive number, so we have

$$0 < \frac{r}{s} - \sum_{n=0}^{s} \frac{1}{n!},$$

the foundation for our lower bound. We wish to build an integer, so we can multiply the inequality by $s!$ to cancel denominators.

$$0 < s!\left(\frac{r}{s} - \sum_{n=0}^{s} \frac{1}{n!}\right).$$

This gives us not only our desired integer, but the lower bound as well. All we have left to find is an upper bound. If we substitute (1) back in for $\frac{r}{s}$, we get

$$s!\left(\sum_{n=0}^{\infty} \frac{1}{n!} - \sum_{n=0}^{s} \frac{1}{n!}\right) = s!\left(\sum_{n=s+1}^{\infty} \frac{1}{n!}\right) = \frac{1}{(s+1)} + \frac{1}{(s+1)(s+2)} + \dots.$$

Since $s+1 > 2$, $\frac{1}{s+1} < \frac{1}{2}$. Thus, we have

$$\frac{1}{(s+1)} + \frac{1}{(s+1)(s+2)} + \frac{1}{(s+1)(s+2)(s+2)} + \dots < \frac{1}{(2)} + \frac{1}{2^2} + \frac{1}{2^3} = 1$$

by the formula for a geometric series. Combining our inequalities, we have

$$0 < s!\left(\frac{r}{s} - \sum_{n=0}^{s} \frac{1}{n!}\right) < 1.$$

Thus, our expression cannot be an integer, so $e$ must be irrational. □

It turns out that we cannot directly use $e$'s power series to prove its transcendence, but we have practiced the strategy from Table 4.1 effectively. The next course of action is to explore the property of $e$ that will help us do the job.

## 4.3 The Gamma Function and the Proof

We will present Hilbert's simplified and modified version (from [Hil32]) of Hermite's proof, rather than the original. The main ingenious ideas of Hermite's are in building the ideal integer $N$ to bound and construct a contradiction for. For a detailed exposition on why Hermite considered the specific integrals and auxiliary polynomial($f$) that we will utilize in the proof, see [Coh06] on the Padé approximations of irrational numbers. We turn to the gamma function to discover these same tools.

Recall Theorem 4.2, the gamma function:

$$\Gamma(n) = \int_0^{\infty} x^{n-1} e^{-x} dx = (n-1)!.$$

The second equality arises from integration by parts. We have little interest in the function $\Gamma$ itself, so we'll replace $n-1$ with $k$:

$$\int_0^\infty x^k e^{-x} dx = k!.$$

Note that for any polynomial $f \in \mathbb{Z}[x]$, we have

$$\int_0^\infty f(x) e^{-x} dx \in \mathbb{Z}. \tag{2}$$

This follows because $f(x)$ is a polynomial with integer coefficients, so we can represent the above expression as a sum of gamma integrals.

For some large prime $p$, we also notice that

$$\frac{1}{(p-1)!} \int_0^\infty x^k e^{-x} dx = \frac{k!}{(p-1)!} = \begin{cases} 1, & k = p-1 \\ \text{a multiple of } p, & k > p-1. \end{cases} \tag{3}$$

(The case where $k < p-1$ will not be significant in the future.) This will be of use to us when providing arguments for divisibility by $p$ and $p-1$.

We combine the integrals from (2) and (3) to get

$$\frac{1}{(p-1)!} \int_0^\infty f(x) e^{-x} dx,$$

which we will investigate in the proof. Using the above integral, let's construct an expression for $e^k$ where $k$ is an integer. With no effort, we have

$$e^k = \frac{e^k/(p-1)! \cdot \int_0^\infty f(x) e^{-x} dx}{1/(p-1)! \cdot \int_0^\infty f(x) e^{-x} dx}.$$

This seems to be useless. However, since $\frac{d}{dk} e^k = e^k$, we can put the $e^k$ into the integral to get

$$e^k = \frac{1/(p-1)! \int_0^\infty f(x) e^{k-x} dx}{1/(p-1)! \int_0^\infty f(x) e^{-x} dx}. \tag{4}$$

We are interested in an expression for $e^k$ because any polynomial in $e$ will have terms of the form $a_k e^k$. Notice that $f(x)$ remains unspecified; we will choose this auxiliary polynomial in the proof. With (3) and (4) in mind, we are ready to prove the transcendence of $e$, using our favorite six-step strategy (from Table 4.1).

**Theorem 4.5.** *$e$ is transcendental.*

*Proof.* We begin with the assumption that $e$ is algebraic. Let there be a nonzero polynomial

$$a(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

with integer coefficients such that $a(e) = 0$.

Our next step is to build an integer $N$. Let

$$f(x) = x^{p-1}(x-1)^p (x-2)^p \ldots (x-d)^p$$

for some large prime $p$. (This relates to (3).) The reasoning behind this choice of $f$ will become apparent later in the proof. Now, consider (4). We can split the integral in the numerator into two parts: from 0 to $k$ and $k$ to $\infty$. We have

$$\frac{1}{(p-1)!}\int_0^\infty f(x)e^{k-x}dx = \frac{1}{(p-1)!}\int_0^k f(x)e^{k-x}dx + \frac{1}{(p-1)!}\int_k^\infty f(x)e^{k-x}dx.$$

For all $1 \le k \le d$, define

$$\delta_k = \frac{1}{(p-1)!}\int_0^k f(x)e^{k-x}dx,$$
$$R_k = \frac{1}{(p-1)!}\int_k^\infty f(x)e^{k-x}dx.$$

Also, let

$$S = \frac{1}{(p-1)!}\int_0^\infty f(x)e^{-x}dx.$$

With these substitutions into (4), we have

$$e^k = \frac{R_k + \delta_k}{S}. \tag{5}$$

We claim that $S$ is an integer and $p \nmid S$. If we expand $f(x)$, all the terms are multiples of $x^{p-1}$, so it follows by (3) that $S$ is an integer. $p \nmid S$ because in the expansion of $f(x)$, there is only one term that is not divisible by $x^p$. We have

$$\begin{aligned} f(x) &= x^{p-1}(x-1)^p(x-2)^p\dots(x-d)^p \\ &= x^{p-1}(-1)^p(-2)^p\dots(-d)^p + \text{a huge multiple of } p. \end{aligned}$$

If $p$ is sufficiently large, the integral of this term cannot be a multiple of $p!$, so $p \nmid S$. The goal of making $S$ an integer while ensuring that $p \nmid S$ inspires the $x^{p-1}$ term in $f(x)$.

For all $1 \le k \le d$, $R_k$ is also an integer but $p \mid R_k$. If we substitute $t = x - k$ into the expression for $R_k$, we have

$$R_k = \frac{1}{(p-1)!}\int_k^\infty f(x)e^{k-x}dx = \frac{1}{(p-1)!}\int_0^\infty f(t+k)e^{-t}dx.$$

Since $1 \le k \le d$, there is a term $(x-k)^p$ in $f(x)$. Therefore, we will have a term $t^p$ in $f(t+k)$. If we expand $f(t+k)$, all the terms will be multiples of $t^p$, so $p \mid R_k$ by (3). The goal of making $R_k$ a multiple of $p$ motivates all the $(x-k)^p$ terms in $f(x)$.

Since both $R_k$ and $S$ are integers (and we can verify $\delta_k$ is a small number), we have constructed rational approximations $\frac{R_k}{S}$ of $e^k$. Notice that the approximations of $e^k$ for each $k$ have the same denominator $S$. Thus, to start building our integer, we consider $S \cdot a(e)$ and substitute (5) for all $1 \le k \le d$.

$$\begin{aligned} S \cdot a(e) &= S\left(a_0 + \sum_{k=1}^d a_k \frac{R_k + \delta_k}{S}\right) \\ &= Sa_0 + S\sum_{k=1}^d a_k(R_k + \delta_k) \\ &= Sa_0 + S\sum_{k=1}^d a_k R_k + S\sum_{k=1}^d a_k\delta_k \end{aligned}$$

Remember that we assumed that $a(e) = 0$, so $S \cdot a(e) = 0$. Let

$$R = S \sum_{k=1}^{d} a_k R_k,$$

and our desired integer

$$N = S \sum_{k=1}^{d} a_k \delta_k.$$

$N$ is an integer because $S \cdot a(e)$, $Sa_0$, and $R$ are integers.

For step 3 (in Table 4.1), we now provide the lower bound $0 < |N|$. Since $p \nmid S$ while $p \mid R_k$ and we can choose $p > a_0$,

$$p \mid S \cdot a(e) = 0,$$

$$p \nmid Sa_0,$$

$$p \mid R = S \sum_{k=1}^{d} a_k R_k.$$

Thus, we have

$$|N| = |S \cdot a(e) - Sa_0 - R| > 0,$$

because an integer multiple of $p$ minus an integer which is not a multiple of $p$ cannot be 0.

For step 4, We will show that $|N| < 1$ by providing an upper bound on $|N|$ involving $p$. Note that every term in $f(x)$ is of the form $x - k$ for $0 \leq k \leq d$. For all $1 \leq x \leq d$, Since $|x - k| \leq d$, we have

$$f(x) \leq d^{dp+p-1}$$

because the degree of $f$ is $dp + p - 1$. Plugging this into the expression for $\delta_k$ yields

$$\delta_k \leq \frac{e^d d^{(d+1)p}}{(p-1)!}.$$

Given $d$ and any $\epsilon > 0$, we can make $\delta_k < \epsilon$ with a sufficiently large $p$. Since $N$ is a linear combination of $\delta_k$'s, we can also ensure that $|N| < 1$ for a large enough $p$.

Thus, as long as $p$ is very large, $0 < |N| < 1$, so $N$ cannot be an integer. We have reached our contradiction, so $e$ is transcendental! □

We dealt with $e$ raised to integers in the above proof. Recall the famous relation Corollary 4.3.1, which we state here:

$$e^{i\pi} = -1.$$

Equivalently, we have

$$e^{i\pi} + 1 = 0.$$

This is a polynomial in $e$, just with complex exponents instead of integers. Is it possible to manipulate our special integrals to reveal the transcendence of $\pi$? With this in mind, our next venture is to tackle the transcendence of $\pi$ and search for a great generalization to Theorem 4.5.

# 5 Lindemann and $\pi$

In 1882, Ferdinand von Lindemann generalized Hermite's argument and showed that $\pi$ is transcendental with the following theorem:

**Theorem 5.1** (Hermite-Lindemann)**.** *$e^\alpha$ is transcendental for all algebraic nonzero $\alpha$.*

This establishes the transcendence of $\pi$ because if $\pi$ is algebraic and is a solution to some polynomial $p(x)$ with integer coefficients, then $i\pi$ is also algebraic because $q(i\pi) = p(i\pi)p(-i\pi) = 0$. If $i\pi$ is algebraic, $e^{i\pi}$ should be transcendental by Theorem 5.1. Since $e^{i\pi} = -1$ which is clearly not transcendental, we have a contradiction, so $\pi$ must be transcendental.

There are many other important corollaries to the Hermite-Lindemann theorem:

**Corollary 5.1.1.** *If $\alpha$ is a nonzero real algebraic number, $\sin(\alpha)$, $\cos(\alpha)$, and $\tan\alpha$ are transcendental.*

We provide an argument assuming that if we have polynomials $p, q \in \mathbb{Z}[x]$ satisfying $p(a) = 0$ and $q(b) = 0$, then we can construct a polynomial $r \in \mathbb{Z}[x]$ satisfying $r(a + b) = 0$ or $r(ab) = 0$.

*Proof.* Recall Theorem 4.3, which states that

$$e^{i\theta} = \cos(\theta) + i\sin(\theta).$$

Now, suppose on the contrary that $\cos(\alpha)$ is algebraic. Then, because

$$\cos^2(\alpha) + \sin^2(\alpha) = 1,$$

it follows that $\sin(\alpha)$ is algebraic. This means $i\sin(\alpha)$ is algebraic as well, so $e^{i\alpha}$ must be algebraic by Theorem 4.3. Since we know $e^{i\alpha}$ is transcendental by the Hermite-Lindemann theorem, we have reached a contradiction, so $\cos(\alpha)$ is transcendental. We can swap the sines and cosines to show the same for $\sin(\alpha)$.

To show that $\tan(\alpha)$ is transcendental, we provide the following formula:

$$\cos(\theta) = \frac{1}{\sqrt{1 + \tan^2(\theta)}}.$$

Thus, if $\tan(\alpha)$ is algebraic, $\cos(\alpha)$ must be algebraic. Since we have just shown $\cos(\alpha)$ to be transcendental, $\tan(\alpha)$ must be as well. □

**Corollary 5.1.2.** *If $\alpha \neq 0, 1$ is a real algebraic number, $\ln\alpha$ is transcendental.*

*Proof.* If $\ln\alpha$ is algebraic, then $e^{\ln\alpha}$ should be transcendental. But $e^{\ln\alpha}$ is simply equal to $\alpha$ (which we defined as algebraic), so $\ln\alpha$ is transcendental. □

We will not actually prove the Hermite-Lindemann theorem, but instead consider the case of $\pi$. To show that $\pi$ is transcendental, we will need to understand some important modifications to our proof of the transcendence of $e$ as well as a few results from the theory of symmetric polynomials.

## 5.1 The New Integral

In proving the transcendence of $e$, we used

$$\delta_k = \frac{1}{(p-1)!}\int_0^k f(x)e^{k-x}dx,$$

$$R_k = \frac{1}{(p-1)!}\int_k^\infty f(x)e^{k-x}dx,$$

$$S = \frac{1}{(p-1)!}\int_0^\infty f(x)e^{-x}dx,$$

to get

$$e^k = \frac{R_k + \delta_k}{S}.$$

$\frac{R_k}{S}$ were very good rational approximations of $e^k$. Therefore, we showed that if there exists a polynomial $a$ with integer coefficients such that $a(e) = 0$, the error of the linear combination of approximations

$$S\sum_{k=1}^{d} a_k\delta_k = S \cdot a(e) - Sa_0 - S\sum_{k=1}^{d} a_k R_k$$

is not an integer, where $a_i$ are the coefficients of $a$.

The main unique idea in Hilbert's proof (which we presented) as opposed to the original one is the phrasing of $\delta_k$ as the error term of a rational approximation of $e^k$. It turns out that we need not view $\delta_k$ from the perspective of rational approximations, which is what Hermite originally did. Hermite provided bounds on

$$\sum_{k=0}^{d}\left(a_k\int_0^k f(x)e^{k-x}dx\right),$$

which is just a simpler formation of the sum of $\delta_k$'s, without any reliance on the notion of rational approximations.

Although this method has less clear motivation, it will be much easier to generalize to $\pi$. Thus, we define

$$I(k,f) = \int_0^k f(x)e^{k-x}dx,$$

where $f$ is the auxiliary function with integer coefficients that we will choose later. Because we have abandoned our reliance on the framework of rational approximation, we must explore some new properties involving $I(k,f)$ to help build a good real number and form bounds on it.

First, with repeated integration by parts, we have

$$I(k,f) = e^k\sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(k), \tag{6}$$

where $m = \deg f$ and $f^{(j)}(x)$ is the $j$th derivative of $f(x)$.

If

$$f(x) = \sum_{i=0}^{m} b_i x^i,$$

then let

$$\bar{f}(x) = \sum_{i=0}^{m} |b_i| x^i.$$

With the help of norms, we have

$$|I(k,f)| \leq \int_0^k |f(x)e^{k-x}|dx \leq |k|e^{|k|}\bar{f}(|k|). \tag{7}$$

This will be our main mechanism for constructing an upper bound on $|I(k,f)|$.

## 5.2 Symmetric Polynomials

We now discuss the necessary background on symmetric polynomials.

**Definition 5.2.** A polynomial $P$ in $n$ variables is said to be *symmetric* if for all permutations $\sigma$ of $[n]$, we have

$$P(X_1, X_2, \ldots, X_n) = P(X_{\sigma_1}, X_{\sigma_2}, \ldots, X_{\sigma_n}).$$

In other words, changing the order of the variables does not affect the polynomial. Some examples of symmetric polynomials include $X_1^2 + 7X_1X_2 + X_2^2$ and

$$4X_1^3 + 4X_2^3 + 4X_3^3 + 2X_1X_2 + 2X_2X_3 + 2X_1X_3 + (X_1 + X_2 + X_3)^5.$$

**Definition 5.3.** The degree $d$ *elementary symmetric polynomial* of $(X_1, X_2, \ldots, X_n)$ is the sum of the distinct products of a subset of $d$ elements from $\{X_1, X_2, \ldots, X_n\}$. For $1 \leq d \leq n$, we have the elementary symmetric polynomials $e_d$:

$$\begin{aligned}
e_1(X_1, X_2, \ldots X_n) &= \sum_{1 \leq a \leq n} X_a, \\
e_2(X_1, X_2, \ldots X_n) &= \sum_{1 \leq a < b \leq n} X_a X_b, \\
e_3(X_1, X_2, \ldots X_n) &= \sum_{1 \leq a < b < c \leq n} X_a X_b X_c, \\
&\ldots \\
e_n(X_1, X_2, \ldots X_n) &= X_1 X_2 \ldots X_n.
\end{aligned}$$

For example, the elementary symmetric polynomials in 3 variables are

$$\begin{aligned}
e_1(X_1, X_2, X_3) &= X_1 + X_2 + X_3, \\
e_2(X_1, X_2, X_3) &= X_1X_2 + X_2X_3 + X_1X_3, \\
e_3(X_1, X_2, X_3) &= X_1X_2X_3.
\end{aligned}$$

**Proposition 5.4.** *The $d$ roots of a polynomial $a(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ with integer coefficients have elementary symmetric polynomials which are rational.*

*Proof.* Let the roots of $a(x)$ be $r_1, r_2, \ldots, r_d$. Then, by the fundamental theorem of algebra, we have

$$a_d(x - r_1)(x - r_2)\ldots(x - r_d) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0.$$

By considering the terms with $d-k$ $x$'s in the expansion of the LHS, we get

$$a_d(-1)^k e_k(r_1, r_2, \ldots, r_d) = a_{d-k}.$$

We can rearrange this to get

$$e_k(r_1, r_2, \ldots, r_d) = \frac{a_{d-k}(-1)^k}{a_d},$$

which is a rational number. □

**Theorem 5.5** (Fundamental Theorem of Elementary Symmetric Polynomials)**.** *Any symmetric polynomial $P(X_1, X_2, \ldots, X_n)$ can be expressed as a polynomial in the elementary symmetric polynomials $e_k(X_1, X_2, \ldots, X_n)$. We have*

$$P(X_1, X_2, \ldots, X_n) = Q\Big(e_1(X_1, X_2, \ldots, X_n), \ldots, e_n(X_1, X_2, \ldots, X_n)\Big).$$

Essentially, the elementary symmetric polynomials are the building blocks of all symmetric polynomials. Consider the example

$$P(X_1, X_2) = X_1^2 + X_2^3 - X_1X_2 = e_1(X_1, X_2)^2 - 3e_2(X_1, X_2).$$

See [Mac98] for a proof of Theorem 5.5. This concludes our discussion of symmetric polynomials, and we are ready to prove that $\pi$ is transcendental. The proofs in the next two subsections are taken from [Bak90].

## 5.3 The Transcendence of $\pi$

**Theorem 5.6.** *$\pi$ is transcendental.*

*Proof.* Recall that it suffices to show that $i\pi$ is transcendental. (If $i\pi$ is not algebraic, then $\pi$ cannot be algebraic.)

As usual, assume that $i\pi$ is the solution to some nonzero polynomial

$$a(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$$

with integer coefficients. Define $\theta_1 = i\pi$, and let $\theta_2, \theta_3, \ldots, \theta_d$ be the other roots of $a$. Since

$$e^{i\pi} + 1 = 0,$$

we have

$$(1 + e^{\theta_1})(1 + e^{\theta_2}) \ldots (1 + e^{\theta_d}) = 0.$$

Expanding this without any simplification yields $2^d$ terms of the form $e^{\alpha}$. We know that each exponent

$$\alpha = \epsilon_1\theta_1 + \epsilon_2\theta_2 + \cdots + \epsilon_d\theta_d,$$

where $\epsilon_j \in \{0, 1\}$. Since at least one $\alpha$ is 0, let the nonzero $\alpha$ be $\alpha_1, \alpha_2, \ldots, \alpha_n$, where $n$ is some number less than $2^d$. We have

$$2^d - n + e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_n} = 0. \tag{8}$$

For some large prime $p$, let our auxiliary function $f$ be

$$f(x) = a_d^{np} x^{p-1}(x-\alpha_1)^p(x-\alpha_2)^p \dots (x-\alpha_n)^p.$$

This is very similar to the $f$ we used in proving the transcendence of $e$. The main difference is that we multiply by $a_d$ a total of $np$ times, which will cancel some denominators in the future. Using $f$, we define our integer

$$N = I(\alpha_1, f) + I(\alpha_2, f) + \cdots + I(\alpha_n, f).$$

Unlike the case of $e$, it is not clear that $N$ is an integer. Therefore, we will show that $N \in \mathbb{Z}$ while simultaneously constructing the lower bound on $N$. By (6), we have

$$\begin{aligned} N &= \sum_{i=1}^{n} \left( e^k \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(k) \right) \\ &= \sum_{i=1}^{n} e^{\alpha_i} \sum_{j=0}^{m} f^{(j)}(0) - \sum_{i=1}^{n} \sum_{j=0}^{m} f^{(j)}(\alpha_i) \\ &= (n-2^d) \sum_{j=0}^{m} f^{(j)}(0) - \sum_{i=1}^{n} \sum_{j=0}^{m} f^{(j)}(\alpha_i) \\ &= (n-2^d) \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} \sum_{i=1}^{n} f^{(j)}(\alpha_i), \end{aligned}$$

where $m = \deg f = np - p - 1$. We know that $n - 2^d = \sum_{i=1}^{n} e^{\alpha_i}$ from (8).

Let's start making our lower bound by dealing with the double sum

$$\sum_{j=1}^{m} \sum_{i=1}^{n} f^{(j)}(\alpha_i).$$

We claim that

$$S_1 = \sum_{i=1}^{n} f^{(j)}(\alpha_i)$$

is an integer. To see this, notice that $S_1$ is a symmetric polynomial in all $2^r$ exponents of the form $\alpha$ (not just the $\alpha_i$'s), and therefore a symmetric polynomial in $\theta_1, \theta_2, \dots, \theta_d$. By Theorem 5.5 and Proposition 5.4, $S$ is rational. Since $f$ has a factor of $a_d^{np}$, the denominators of every $f^{(j)}\alpha_i$ will cancel out. (The proof of Proposition 5.4 states the denominators in question.) Thus, $S_1 \in \mathbb{Z}$, so the double sum is an integer.

Now, consider the derivatives $f^{(j)}(\alpha_i)$. If $j < p$, $f^{(j)}(\alpha_i) = 0$. If $j \geq p$, all the nonzero terms in the expansion have $(x-\alpha_i)^p$ differentiated into $p!$, so $p! \mid f^j(\alpha_i)$. Therefore, the double sum is an integer divisible by $p!$.

Next, we'll work with the remaining portion of $N$, namely

$$S_2 = (n-2^d) \sum_{j=0}^{m} f^{(j)}(0).$$

By similar reasoning to the consideration of $f^{(j)}(\alpha_i)$, we know that $p! \mid f^{(j)}(0)$ for all $j \neq p-1$. For $j = p-1$, however, we end up with

$$f^{(p-1)}(0) = (p-1)!(-a_d)^{np}(\alpha_1\alpha_2 \dots \alpha_n)^p,$$

because the remaining terms in $f^{(p-1)}(0)$ are equal to 0. Note that $f^{(p-1)}(0)$ is a nonzero integer multiple of $(p-1)!$, but it is not divisible by $p$ if $p$ is sufficiently large. Thus, if $p$ is also larger than $2^d - n = |n - 2^d|$, $S_2$ is a nonzero integer multiple of $(p-1)!$ but not $p!$. Combining this with our characterization of the double sum, we have that $N$ is a nonzero integer and $|N| \geq (p-1)!$.

We now use (7) to create an upper bound on $|N|$. We can show that

$$|N| \leq \sum_{i=1}^{n} |\alpha_i| e^{|\alpha_i|} \bar{f}(|\alpha_i|) \leq c_1 c_2^p,$$

where $c_1$ and $c_2$ are constants. One example that works is $c_1 = e^M$ and $c_2 = 2^n |\alpha_d|^n M^{n+1}$, where $M$ is the maximum value of $|\alpha_i|$. For sufficiently large $p$, however, $(p-1)! \geq c_1 c_2^p$, so we have contradictory bounds. Therefore, $N$ cannot be an integer, so $\pi$ is transcendental! $\square$

Having established the transcendence of $\pi$, Lindemann wondered if Hermite's proof could be extended even further.

## 5.4 The Lindemann-Weierstrass Theorem

We begin with a definition:

**Definition 5.7.** Two complex numbers $\alpha_1$ and $\alpha_2$ are *linearly independent* over the algebraic numbers if for all nonzero algebraic $\beta_1$ and $\beta_2$,

$$\beta_1 \alpha_1 + \beta_2 \alpha_2 \neq 0$$

In other words, there is no linear combination of $\alpha_1$ and $\alpha_2$ with algebraic coefficients equal to 0.

By Definition 5.7, the Hermite-Lindemann theorem (Theorem 5.1) is equivalent to the statement that for all nonzero algebraic numbers $\alpha$, we know that $e^{\alpha}$, $e^{2\alpha}$, $e^{3\alpha}, \ldots$ are linearly independent over the algebraic numbers.

A natural question arises from this phrasing: can we establish the linear independence of $n$ distinct numbers $e^{\alpha_1}, e^{\alpha_2}, e^{\alpha_3}, \ldots e^{\alpha_4}$, where the $\alpha_i$'s are algebraic? Lindemann pondered this generalization and managed a sketch of the proof. In 1885, Karl Weierstrass filled in most of the key details, along with David Hilbert among others. We have

**Theorem 5.8** (Lindemann-Weierstrass)**.** *Let $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ be distinct algebraic numbers. Then $e^{\alpha_1}, e^{\alpha_2}, e^{\alpha_3}, \ldots, e^{\alpha_n}$ are linearly independent over the algebraic numbers, or for all nonzero algebraic numbers $\beta_1, \beta_2, \beta_3, \ldots, \beta_n$,*

$$\beta_1 e^{\alpha_1} + \beta_2 e^{\alpha_2} + \beta_3 e^{\alpha_3} + \cdots + \beta_n e^{\alpha_n} \neq 0.$$

Before proving this theorem, we state one of its immediate consequences to transcendental number theory:

**Corollary 5.8.1.** *Let $\alpha_1, \alpha_2, \alpha_2, \ldots, \alpha_n$ be distinct algebraic numbers. Then for all nonzero algebraic numbers $\beta_1, \beta_2, \beta_3, \ldots, \beta_n$,*

$$\beta_1 e^{\alpha_1} + \beta_2 e^{\alpha_2} + \beta_3 e^{\alpha_3} + \cdots + \beta_n e^{\alpha_n}$$

*is transcendental.*

*Proof.* If $\beta_1 e^{\alpha_1} + \beta_2 e^{\alpha_2} + \cdots + \beta_n e^{\alpha_n}$ is equal to some algebraic number, say $\beta_0$, then we can simply add $\beta_0 e^0$ to our existing expression to derive a contradiction to the Lindemann-Weierstrass theorem. (If $\alpha_k = 0$ for some $k$, then add $\beta_0$ to $\beta_k$.) $\square$

Note that this corollary implies the transcendence of $e$, the transcendence of $\pi$, and the Hermite-Lindemann Theorem. Now that we understand the vast applications of Theorem 5.8, let's address a quick definition before jumping into the proof, which is quite similar that of the previous section.

**Definition 5.9.** An *algebraic integer* is a number which can be expressed as the solution to a polynomial $p(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$ with integer coefficients, where the leading coefficient of $p$, or $a_d$, is 1. The algebraic integers are a subset of the algebraic numbers.

*Proof of Theorem 5.8.* Suppose on the contrary that

$$\beta_1 e^{\alpha_1} + \beta_2 e^{\alpha_2} + \beta_3 e^{\alpha_3} + \cdots + \beta_n e^{\alpha_n} = 0, \tag{9}$$

for some distinct algebraic $\alpha_i$'s and nonzero algebraic $\beta_i$'s. We will reduce this assumption to a much simpler statement before building our integer $N$.

First, we may assume that all the $\beta_i$'s are integers without loss of generality. We prove this by constructing a new polynomial in $e$ with integer $\beta_i$'s from the existing one (provided in 9). Given (9), let there be $c(i)$ conjugates of $\beta_i$, namely $\beta_{i,1}, \beta_{i,2}, \ldots, \beta_{i,c(i)}$. Also, define $\beta_{i,0} = \beta_i$. Consider the product

$$\prod_{\substack{0 \le i_1 \le c(1) \\ 0 \le i_2 \le c(2) \\ \vdots \\ 0 \le i_n \le c(n)}} \left( \beta_{1,i_1} e^{\alpha_1} + \beta_{2,i_2} e^{\alpha_2} + \cdots + \beta_{n,i_n} e^{\alpha_n} \right).$$

Essentially, we take the product of all expressions formed by substituting some subsets of $\beta_i$ for some of their conjugates. The expansion of this product is equal to 0 and results in the creation of a new polynomial in $e$, where the new $\beta$ coefficients are rational. We can clear denominators to reach integer $\beta$'s, which proves the assumption.

Second, we may assume that if $\alpha_i$ is in $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, so are the conjugates of $\alpha_i$. Additionally, if $a_i$ and $a_j$ are conjugates in the expression, $\beta_i = \beta_j$. As with the previous assumption, we prove this by constructing a new polynomial in $e$ satisfying the desired constraints, using the existing polynomial (9). Consider the irreducible polynomial $q$ with integer coefficients. containing $\alpha_1, \alpha_2, \ldots, \alpha_n$ as roots. Since $q$ has integer coefficients, all the conjugates of the $\alpha_i$'s are also roots of $q$. Let the remaining roots of $q$ be $\alpha_{n+1}, \alpha_{n+2}, \ldots, \alpha_N$. With this definition, we construct

$$\prod_{\sigma} \beta_1 e^{\alpha_{\sigma(1)}} + \beta_2 e^{\alpha_{\sigma(2)}} + \cdots + \beta_n e^{\alpha_{\sigma(n)}} = 0,$$

where $\sigma$ is a permutation of $[n] = \{1, 2, \ldots, n\}$. We take the product across $N!$ such permutations $\sigma$. In the expansion of this product, each term is of the form

$$\beta e^{h_1 \alpha_1 + h_2 \alpha_2 + \cdots + h_N \alpha_N},$$

where $\beta$ is some product of $N!$ $B_i$'s and $h_1 + h_2 + \cdots + h_N = N!$. The possible exponents of e, namely $h_1\alpha_1 + h_2\alpha_2 + \cdots + h_N\alpha_N$, form a complete set of conjugates. We can verify with a symmetry argument that if two exponents are conjugates, their coefficients $\beta$ are equal. Also, our product is not identically zero because the $\alpha_i$'s are all distinct. This proves the second assumption.

From now onward, we assume once again that

$$\beta_1 e^{\alpha_1} + \beta_2 e^{\alpha_2} + \beta_3 e^{\alpha_3} + \cdots + \beta_n e^{\alpha_n} = 0,$$

but now we have the following conditions:

- $B_i \in \mathbb{Z}$ for all $1 \leq i \leq n$,
- if $\alpha_i$ is in $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, so are all the conjugates of $\alpha_i$,
- if $\alpha_i$ and $\alpha_j$ are conjugates, $\beta_i = \beta_j$.

For simplicity, let's order the terms such that conjugates are adjacent to each other. In other words, let there be integers $0 = n_0 < n_1 < \cdots < n_r = n$ such that for each $0 \leq t < r$, we have

$$\alpha_{n_t+1}, \alpha_{n_t+2}, \ldots, \alpha_{n_{t+1}} \text{ are conjugates,}$$

and

$$\beta_{n_t+1} = \beta_{n_t+2} = \cdots = \beta_{n_{t+1}}.$$

Equivalently,

$$\sum_{i=0}^{n} \beta_i e^{\alpha_i} = \sum_{n_i} \left( \beta_{n_{i+1}} e^{\alpha_{n_i+1}} + \beta_{n_{i+1}} e^{\alpha_{n_i+2}} + \cdots + \beta_{n_{i+1}} e^{\alpha_{n_{i+1}}} \right). \tag{10}$$

We would prefer to work with algebraic integers as opposed to algebraic numbers, because Proposition 5.4 will allow us to build an integer more easily with algebraic integers. Therefore, we make use of some integer $A$ satisfying $A\alpha_i$ and $A\beta_i$ are algebraic integers for all $1 \leq i \leq n$. With the help of $A$, we can define the auxiliary function:

$$f_i(x) = \frac{A^{np}(x - \alpha_1)^p \ldots (x - \alpha_n)^p}{(x - \alpha_i)}$$

for all $1 \leq i \leq n$, where $p$ is a large prime. The main motivation behind this function $f$ is that we have an exponent of $p-1$ only for the term $(x-\alpha_i)$, whereas the remaining exponents are $p$. This will help in our divisibility by $p$ argument, similar to the transcendence of $\pi$, when bounding $N$. Also, although $f$ does not have integer coefficients, it does have algebraic integer coefficients. Let our integer $N = N_1 N_2 \ldots N_n$, where

$$N_i = \beta_1 I(\alpha_1, f_i) + \beta_2 I(\alpha_2, f_i) + \cdots + \beta_n I(\alpha_n, f_i).$$

As with the proof that $\pi$ is transcendental, our next step is to provide a lower bound on

$N$ and show that $N$ is an integer. Substituting (6) into our definition for $N_i$, we have

$$\begin{aligned}
N_i &= \sum_{k=0}^{n} \beta_k I(\alpha_k, f_i) \\
&= \sum_{k=0}^{n} \left( \beta_k e^{\alpha_k} \sum_{j=0}^{m} f_i^{(j)}(0) \right) - \sum_{k=0}^{n} \left( \beta_k \sum_{j=0}^{m} f_i^{(j)}(\alpha_k) \right) \\
&= \left( \sum_{j=0}^{m} f_i^{(j)}(0) \right) \left( \sum_{k=0}^{n} \beta_k e^{\alpha_k} \right) - \sum_{k=0}^{n} \left( \beta_k \sum_{j=0}^{m} f_i^{(j)}(\alpha_k) \right) \\
&= -\sum_{k=0}^{n} \left( \beta_k \sum_{j=0}^{m} f_i^{(j)}(\alpha_k) \right) \\
&= -\sum_{k=0}^{n} \sum_{j=0}^{m} \left( \beta_k f_i^{(j)}(\alpha_k) \right),
\end{aligned}$$

where $m = \deg f_i = np - 1$. Consider $f_i^{(j)}(a_k)$. By arguments similar to those in the proof of the transcendence of $\pi$, we have

$$f_i^{(j)}(\alpha_k) = \begin{cases} 0, & j < p \\ \equiv 0 \mod p!, & j \geq p \end{cases}$$

if $i \neq k$. Otherwise,

$$f_i^{(j)}(\alpha_i) = \begin{cases} 0, & j < p-1 \\ A^{np}(p-1)! \prod_{l=1, l\neq i}^{n} (\alpha_i - \alpha_l)^p, & j = p-1 \\ \equiv 0 \mod p!, & j \geq p. \end{cases}$$

By combining these cases, we can show that $N_i$ is nonzero and $p \nmid N_i$ if $p$ is sufficiently large. Thus, $N_i$ is a nonzero algebraic integer divisible by $(p-1)!$ but not $p!$.

It remains to show that $N_i$ is an integer. By (10), we have

$$N_i = -\sum_{j=0}^{m} \sum_{t=0}^{r-1} \left( \beta_{n_{t+1}} \left( f_i^{(j)}(a_{n_t+1}) + f_i^{(j)}(a_{n_t+2}) + \cdots + f_i^{(j)}(a_{n_{t+1}}) \right) \right).$$

This is a symmetric polynomial in the $\alpha_i$'s. Since they form a complete set of conjugates and are algebraic integers, we can apply Theorem 5.5 and Proposition 5.4 to show that $N_i$ is an integer. Since $N_i$ is an integer and we have shown $N_i$ is divisible by $(p-1)!$ but not $p!$, $|N| = |N_1 N_2 \dots N_n| \in \mathbb{Z}$ and $|N| \geq (p-1)!$.

We now construct an upper bound on $N$ using 7. For each $i$,

$$|N_i| \leq \sum_{k=1}^{n} \left( |\beta_k| |I(a_k, f_i|) \right) \leq \sum_{k=1}^{n} \left( |\beta_k \alpha_k| e^{|\alpha_k|} \bar{f}_i(|\alpha_k|) \right).$$

Using this inequality, we can show that $N \leq c^p$ for some constant $c$. For sufficiently large $p$, $(p-1)! \geq c^p$, so we have contradictory bounds on $N$. Therefore, $N$ cannot be an integer, which is a contradiction and completes the proof. $\square$

The Lindemann-Weierstrass theorem expands the ideas of Hermite to reveal the transcendence of a vast set of numbers, parameterized by the form described in Corollary 5.8.1. We leave the reader with a conjecture involving our familiar friend $e$:

**Conjecture 5.10** (Four Exponentials)**.** *If $x_1, x_2$ and $y_1, y_2$ are two pairs of complex numbers, each pair linearly independent over the rationals, then at least one of*

$$e^{x_1 y_1}, e^{x_2 y_1}, e^{x_1 y_2}, e^{x_2 y_2}$$

*is transcendental.*


# Acknowledgements

I would like to thank Dr. Simon Rubinstein-Salzedo for providing this incredible opportunity at Euler Circle to study transcendental numbers. Additionally, a big thank you to Alex DeWeese for many helpful discussions and personal feedback. Finally, I would like to thank my family for their support.


# References


[Bak90] Alan Baker. *Transcendental Number Theory.* Cambridge University Press, United Kingdom, 1990.

[BT04] Edward B. Burger and Robert Tubbs. *Making Transcendence Transparent: An Intuitive Approach to Classical Transcendental Number Theory.* Springer, New York, 2004.

[Coh06] Henry Cohn. A short proof of the simple continued fraction expansion of e. 2006.

[Erd32] Paul Erdős. Representations of real numbers as sums and products of liouville numbers. *Michigan Mathematics Journal*, 9:59–60, 1932.

[Gra94] Robert Gray. Georg Cantor and transcendental numbers. *The American Mathematical Monthly*, 101(9):819–832, 1994.

[Hil32] David Hilbert. Über die transzendenz der zahlen e und $\pi$. 1932.

[Mac98] Ian G. Macdonald. *Symmetric Functions and Hall Polynomials.* Clarendon Press, United Kingdom, 1998.