Transcendence of e

Gerald Huang

UNSW Mathematics Society

June 13, 2023

Algebraic and Transcendental Numbers

Proof of transcendence
- Part I
- Part II

Lindemann-Weierstrass Theorem

Algebraic and Transcendental Numbers

Algebraic and Transcendental Numbers

- **Algebraic**: can be generated from *algebraic* equations.

Algebraic and Transcendental Numbers

- **Algebraic**: can be generated from *algebraic* equations.

An *algebraic number* is a number that is the root of some polynomial with integer coefficients; that is, α is algebraic if there exist a polynomial $f \in \mathbb{Z}[x]$ such that

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

where $\alpha_i \in \mathbb{Z}$ for each $i = 0, \ldots, n$ and $a_n \neq 0$.

Algebraic and Transcendental Numbers

- **Algebraic**: can be generated from *algebraic* equations.

An *algebraic number* is a number that is the root of some polynomial with integer coefficients; that is, α is algebraic if there exist a polynomial $f \in \mathbb{Z}[x]$ such that

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

where $\alpha_i \in \mathbb{Z}$ for each $i = 0, \ldots, n$ and $a_n \neq 0$.

- A number is said to be *transcendental* if it is not algebraic.

Algebraic and Transcendental Numbers

- Any rational number $k = p/q$ is algebraic because it is the root of the equation
$$f(x) = qx - p.$$

Algebraic and Transcendental Numbers

- Any rational number $k = p/q$ is algebraic because it is the root of the equation
$$f(x) = qx - p.$$
- $\sqrt{2}$ is algebraic because it is a root of the equation
$$f(x) = x^2 - 2.$$

Algebraic and Transcendental Numbers

- Any rational number $k = p/q$ is algebraic because it is the root of the equation
$$f(x) = qx - p.$$
- $\sqrt{2}$ is algebraic because it is a root of the equation
$$f(x) = x^2 - 2.$$
- i is algebraic because it is a root of the equation
$$f(x) = x^2 + 1.$$

Algebraic and Transcendental Numbers

- Any rational number $k = p/q$ is algebraic because it is the root of the equation
$$f(x) = qx - p.$$
- $\sqrt{2}$ is algebraic because it is a root of the equation
$$f(x) = x^2 - 2.$$
- i is algebraic because it is a root of the equation
$$f(x) = x^2 + 1.$$
- Let ζ_n be a primitive n-th root of unity. Then ζ_n is algebraic because it is a root of the equation
$$f(x) = x^n - 1.$$

Existence of Transcendental Numbers

Do transcendental numbers even exist in the first place?

Existence of Transcendental Numbers

Do transcendental numbers even exist in the first place? (Yes!)

The algebraic numbers form a *countable* set.

Existence of Transcendental Numbers

Do transcendental numbers even exist in the first place? (Yes!)

The algebraic numbers form a *countable* set.

Proof.

Given an integer N and integer coefficients $a_0, a_1, \ldots, a_N$, we see that the polynomial

$$a_N x^N + \cdots + a_1 x + a_0 \tag{1}$$

has at most N many solutions (from the Fundamental Theorem of Algebra).

Existence of Transcendental Numbers

Do transcendental numbers even exist in the first place? (Yes!)

The algebraic numbers form a *countable* set.

Proof.

Given an integer N and integer coefficients $a_0, a_1, \ldots, a_N$, we see that the polynomial

$$a_N x^N + \cdots + a_1 x + a_0 \tag{1}$$

has at most N many solutions (from the Fundamental Theorem of Algebra). Denote $A_{N,a_0,\ldots,a_N}$ to be the set of roots of (1), so that $|A_{N,a_0,\ldots,a_N}| \leq N$, which is clearly countable. $\square$

Existence of Transcendental Numbers

Proof continued...

Let B_N be the set of roots of polynomials of degree N.

Existence of Transcendental Numbers

Proof continued...

Let B_N be the set of roots of polynomials of degree N. Therefore, it is easy to see that

$$B_N = \bigcup_{(a_N, a_{N-1}, \ldots, a_0) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \times \cdots \times \mathbb{Z}} A_{N, a_0, \ldots, a_N},$$

which is a countable union of countable sets.

Existence of Transcendental Numbers

Proof continued...

Let B_N be the set of roots of polynomials of degree N. Therefore, it is easy to see that

$$B_N = \bigcup_{(a_N, a_{N-1}, \ldots, a_0) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \times \cdots \times \mathbb{Z}} A_{N, a_0, \ldots, a_N},$$

which is a countable union of countable sets. Therefore, B_N is also countable.

Finally, the set of algebraic numbers is exactly

$$\mathbb{A} = \bigcup_{n \in \mathbb{N}} B_n,$$

which is, again, a countable union of countable sets. So, $\mathbb{A}$ is countable. □

Existence of Transcendental Numbers

- Since $\mathbb{R}$ is uncountable, this implies that the set of transcendental numbers must be uncountable.

In other words, if you were to draw a real number out of a hat, it is more likely to be transcendental than algebraic!

Proof of transcendence

Proof outline

We outline the proof with two main steps that we will explore in greater detail.

1. Show that

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

   and consider a suitable function for $f(t)$ to define another series of functions $F(x)$.

2. By choosing a suitable function for $f(t)$, arrive at a contradiction that shows that e must indeed be transcendental.

Proof (part I)

Proof (part I)

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

Proof (part I)

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

We begin with integration by parts on the integral.

Proof (part I)

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

We begin with integration by parts on the integral.

$$\begin{aligned}\int_0^x e^{-t} \cdot f(t)\,dt &= \left(\int e^{-t}\right) \cdot f(t)\Big|_0^x + \int_0^x e^{-t} \cdot f'(t)\,dt \\ &= f(0) - e^{-x} \cdot f(x) + \int_0^x e^{-t} \cdot f'(t)\,dt.\end{aligned}$$

Proof (part I)

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

We begin with integration by parts on the integral.

$$\int_0^x e^{-t} \cdot f(t)\,dt = \left(\int e^{-t}\right) \cdot f(t)\Big|_0^x + \int_0^x e^{-t} \cdot f'(t)\,dt$$

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

Therefore,

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

as required.

Proof (part I)

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

We can see that by replacing $f(t)$ on the left hand side with $f'(t)$, we indeed obtain the middle expression. In other words, we have that

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

Proof (part I)

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

Let's explore this relation a little bit. By replacing $f^{(i)}$ with $f^{(i+1)}$, we can see that

$$e^x \left(\int_0^x e^{-t} \cdot f(t)\, dt - \int_0^x e^{-t} \cdot f'(t)\, dt \right) = e^x \cdot f(0) - f(x),$$

$$e^x \left(\int_0^x e^{-t} \cdot f'(t)\, dt - \int_0^x e^{-t} \cdot f''(t)\, dt \right) = e^x \cdot f'(0) - f'(x),$$

$$\dots$$

$$e^x \left(\int_0^x e^{-t} \cdot f^{(k)}(t)\, dt - \int_0^x e^{-t} \cdot f^{(k+1)}(t)\, dt \right) = e^x \cdot f^{(k)}(0) - f^{(k)}(x).$$

Proof (part I)

Therefore, we see that

$$e^x\left(\int_0^x e^{-t}\cdot f(t)\,dt-\int_0^x e^{-t}\cdot f^{(k+1)}(t)\,dt\right)=e^x\sum_{i=0}^{k}f^{(i)}(0)-\sum_{i=0}^{k}f^{(i)}(x).$$

Proof (part I)

Therefore, we see that

$$e^x\left(\int_0^x e^{-t}\cdot f(t)\,dt - \int_0^x e^{-t}\cdot f^{(k+1)}(t)\,dt\right) = e^x\sum_{i=0}^{k} f^{(i)}(0) - \sum_{i=0}^{k} f^{(i)}(x).$$

We make two observations:

- If we can freely choose f, ideally we want to choose f in such a way where taking high enough derivatives eventually land us at 0.

Proof (part I)

Therefore, we see that

$$e^x \left(\int_0^x e^{-t} \cdot f(t)\, dt - \int_0^x e^{-t} \cdot f^{(k+1)}(t)\, dt \right) = e^x \sum_{i=0}^{k} f^{(i)}(0) - \sum_{i=0}^{k} f^{(i)}(x).$$

We make two observations:

- If we can freely choose f, ideally we want to choose f in such a way where taking high enough derivatives eventually land us at 0.
- By letting $F(x) = \sum_{i=0}^{\infty} f^{(i)}(x)$, we can re-express the equality above.

Proof (part I)

Therefore, we see that

$$e^x \left(\int_0^x e^{-t} \cdot f(t)\, dt - \int_0^x e^{-t} \cdot f^{(k+1)}(t)\, dt \right) = e^x \sum_{i=0}^{k} f^{(i)}(0) - \sum_{i=0}^{k} f^{(i)}(x).$$

We make two observations:

- If we can freely choose f, ideally we want to choose f in such a way where taking high enough derivatives eventually land us at 0.
- By letting $F(x) = \sum_{i=0}^{\infty} f^{(i)}(x)$, we can re-express the equality above.

Therefore, we will define f to be some polynomial; the construction of f is yet to be determined but we just know that it is some polynomial.

Proof (part I)

Therefore, as $k \longrightarrow \infty$, $\int_0^x e^{-t} \cdot f^{(k+1)}(t)\, dt \longrightarrow 0$.

Proof (part I)

Therefore, as $k \longrightarrow \infty$, $\int_0^x e^{-t} \cdot f^{(k+1)}(t)\, dt \longrightarrow 0$. We let $F(x) = \sum_{i=0}^{\infty} f^{(i)}(x)$ such that we can write the previous expression exactly as

$$e^x \cdot \int_0^x e^{-t} \cdot f(t)\, dt = e^x \cdot F(0) - F(x).$$

Proof (part I)

Therefore, as $k \longrightarrow \infty$, $\int_0^x e^{-t} \cdot f^{(k+1)}(t)\,dt \longrightarrow 0$. We let $F(x) = \sum_{i=0}^{\infty} f^{(i)}(x)$ such that we can write the previous expression exactly as

$$e^x \cdot \int_0^x e^{-t} \cdot f(t)\,dt = e^x \cdot F(0) - F(x).$$

This finishes the first part of the proof; we now proceed with the proof.

Proof (part II)

Proof (part II)

As with most (if not all) transcendental proofs, we assume that e is *algebraic*. Therefore, there exist some polynomial $A(t)$ with integer coefficients a_j (with $a_0, a_n \neq 0$) such that $A(e) = 0$; that is,

$$a_0 + a_1 e + a_2 e^2 + \cdots + a_n e^n = 0.$$

Proof (part II)

As with most (if not all) transcendental proofs, we assume that e is *algebraic*. Therefore, there exist some polynomial $A(t)$ with integer coefficients a_j (with $a_0, a_n \neq 0$) such that $A(e) = 0$; that is,

$$a_0 + a_1 e + a_2 e^2 + \cdots + a_n e^n = 0.$$

Here, we can generate a series of equalities by setting $x = k$ for each $k = 0, 1, 2, \ldots, n$; that is,

$$a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt = a_k e^k \cdot F(0) - a_k \cdot F(k)$$

or

$$\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt = F(0) \sum_{k=0}^{n} a_k e^k - \sum_{k=0}^{n} a_k \cdot F(k).$$

Proof (part II)

This is equivalent to saying

$$\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt = -\sum_{k=0}^{n} a_k \cdot F(k)$$

since $\sum_{k=0}^{n} a_k e^k = 0$.

Proof (part II)

This is equivalent to saying

$$\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt = -\sum_{k=0}^{n} a_k \cdot F(k)$$

since $\sum_{k=0}^{n} a_k e^k = 0$.
We are now in a position to carefully choose f. How could we choose such a polynomial?
Let's explore the left side a little bit first! Our goal is to find some insight into how big the left side grows.

Proof (part II)

$$\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt = -\sum_{k=0}^{n} a_k \cdot F(k)$$

We see that

$$\left| \sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt \right| \leq \sum_{k=0}^{n} |a_k e^k| \cdot \left| \int_0^k e^{-t} \cdot f(t)\, dt \right|.$$

Proof (part II)

$$\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt = -\sum_{k=0}^{n} a_k \cdot F(k)$$

We see that

$$\left|\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt\right| \leq \sum_{k=0}^{n} |a_k e^k| \cdot \left|\int_0^k e^{-t} \cdot f(t)\, dt\right|.$$

- How big does the integral grow? Since $k \leq n$, then we have that

$$\left|\int_0^k e^{-t} \cdot f(t)\, dt\right| \leq \left|\int_0^n e^{-t} \cdot f(t)\, dt\right| \leq \int_0^n \left|e^{-t} \cdot f(t)\right|\, dt.$$

Proof (part II)

Let's try bounding $\left|e^{-t} \cdot f(t)\right|$ on the interval $[0, n]$.

Proof (part II)

Let's try bounding $\left|e^{-t} \cdot f(t)\right|$ on the interval $[0, n]$.

- Since e^{-t} is continuous on the closed interval $[0, n]$, we know that e^{-t} attains a maximum on this interval. Let's call it M.

Proof (part II)

Let's try bounding $\left|e^{-t} \cdot f(t)\right|$ on the interval $[0, n]$.

- Since e^{-t} is continuous on the closed interval $[0, n]$, we know that e^{-t} attains a maximum on this interval. Let's call it M.
- Therefore, $|e^{-t} \cdot f(t)| \leq M \cdot |f(t)|$.

Proof (part II)

Let's try bounding $\left|e^{-t} \cdot f(t)\right|$ on the interval $[0, n]$.

- Since e^{-t} is continuous on the closed interval $[0, n]$, we know that e^{-t} attains a maximum on this interval. Let's call it M.
- Therefore, $|e^{-t} \cdot f(t)| \leq M \cdot |f(t)|$.
- In other words, we obtain the bound

$$\left|\int_0^k e^{-t} \cdot f(t)\, dt\right| \leq \int_0^n M \cdot |f(t)|\, dt.$$

Proof (part II)

Let's try bounding $\left|e^{-t} \cdot f(t)\right|$ on the interval $[0, n]$.

- Since e^{-t} is continuous on the closed interval $[0, n]$, we know that e^{-t} attains a maximum on this interval. Let's call it M.
- Therefore, $|e^{-t} \cdot f(t)| \leq M \cdot |f(t)|$.
- In other words, we obtain the bound

$$\left|\int_0^k e^{-t} \cdot f(t)\, dt\right| \leq \int_0^n M \cdot |f(t)|\, dt.$$

Thus, if we can force f to have a maximum on the interval $[0, n]$, then we can achieve a nice bound on the overall integral.
What about the right hand side?

Proof (part II)

$$\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt = -\sum_{k=0}^{n} a_k \cdot F(k)$$

Recall that $F(k) = \sum_{i=0}^{\infty} f^{(i)}(k)$. Can we make this sum arbitrarily large?

Proof (part II)

$$\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt = -\sum_{k=0}^{n} a_k \cdot F(k)$$

Recall that $F(k) = \sum_{i=0}^{\infty} f^{(i)}(k)$. Can we make this sum arbitrarily large?

- Firstly, we see that k ranges from 0 to n. This tells us that we might want to consider a product of linear polynomials; that is, consider

  $$g(x) = x(x-1)(x-2)\cdots(x-n)$$

  since $g(k) = 0$ for each $k = 0, \ldots, n$.

Proof (part II)

$$\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt = -\sum_{k=0}^{n} a_k \cdot F(k)$$

Recall that $F(k) = \sum_{i=0}^{\infty} f^{(i)}(k)$. Can we make this sum arbitrarily large?

- Firstly, we see that k ranges from 0 to n. This tells us that we might want to consider a product of linear polynomials; that is, consider

$$g(x) = x(x-1)(x-2)\cdots(x-n)$$

  since $g(k) = 0$ for each $k = 0, \ldots, n$.
- Can we say anything about $f^{(i)}(k)$?

Proof (part II)

- If we differentiate $x(x-1)(x-2)\cdots(x-n)$ once, then $g'(0)$ simply depends on one term since every other term must contain a factor of x.

Proof (part II)

- If we differentiate $x(x-1)(x-2)\cdots(x-n)$ once, then $g'(0)$ simply depends on one term since every other term must contain a factor of x.
- If we differentiate $x^2(x-1)^2\cdots(x-n)^2$ once, then $g'(0) = g'(1) = \cdots = g'(n)$.

Proof (part II)

- If we differentiate $x(x-1)(x-2)\cdots(x-n)$ once, then $g'(0)$ simply depends on one term since every other term must contain a factor of x.
- If we differentiate $x^2(x-1)^2\cdots(x-n)^2$ once, then $g'(0) = g'(1) = \cdots = g'(n)$.
- If we differentiate $x^3(x-1)^3\cdots(x-n)^3$ once, then $g'(0) = g'(1) = \cdots = g'(n)$.

Proof (part II)

- If we differentiate $x(x-1)(x-2)\cdots(x-n)$ once, then $g'(0)$ simply depends on one term since every other term must contain a factor of x.
- If we differentiate $x^2(x-1)^2\cdots(x-n)^2$ once, then $g'(0)=g'(1)=\cdots=g'(n)$.
- If we differentiate $x^3(x-1)^3\cdots(x-n)^3$ once, then $g'(0)=g'(1)=\cdots=g'(n)$.
  - However, if we differentiate $x^3(x-1)^3\cdots(x-n)^3$ twice, then we also get $g''(0)=g''(1)=\cdots=g''(n)$.

Proof (part II)

- If we differentiate $x(x-1)(x-2)\cdots(x-n)$ once, then $g'(0)$ simply depends on one term since every other term must contain a factor of x.
- If we differentiate $x^2(x-1)^2\cdots(x-n)^2$ once, then $g'(0)=g'(1)=\cdots=g'(n)$.
- If we differentiate $x^3(x-1)^3\cdots(x-n)^3$ once, then $g'(0)=g'(1)=\cdots=g'(n)$.
  - However, if we differentiate $x^3(x-1)^3\cdots(x-n)^3$ twice, then we also get $g''(0)=g''(1)=\cdots=g''(n)$.

Perhaps, we'd want to set $f(x)=x^q(x-1)^q\ldots(x-n)^q$ for some large enough q that we can freely choose...

Proof (part II)

- Since $x(x-1)\cdots(x-n)$ is continuous on the interval $[0, n]$, then such a function attains a maximum – say N.

Proof (part II)

- Since $x(x-1)\cdots(x-n)$ is continuous on the interval $[0, n]$, then such a function attains a maximum – say N.
- Therefore, we can place a bound on the previous integral to get

$$\left| \int_0^k e^{-t} \cdot f(t)\, dt \right| \leq \int_0^n M \cdot N^q \, dt = M \cdot N^q n.$$

Proof (part II)

- Since $x(x-1)\cdots(x-n)$ is continuous on the interval $[0, n]$, then such a function attains a maximum – say N.
- Therefore, we can place a bound on the previous integral to get

$$\left|\int_0^k e^{-t} \cdot f(t)\, dt\right| \leq \int_0^n M \cdot N^q \, dt = M \cdot N^q n.$$

Hmm... ideally, we want this bound to be arbitrarily small. We can adjust this such that

$$f(x) = \frac{x^q (x-1)^q \cdots (x-n)^q}{q!}$$

since the factorial function grows much faster than the exponential functions. Thus, as $q \longrightarrow \infty$, the bound approaches 0.

Proof (part II)

$$f(x) = \frac{x^q(x-1)^q \ldots (x-n)^q}{q!}$$

Now, what about $f^{(i)}(k)$?

Proof (part II)

$$f(x) = \frac{x^q(x-1)^q \dots (x-n)^q}{q!}$$

Now, what about $f^{(i)}(k)$?

- For each k, $f^{(i)}(k) = 0$ if $i < q - 1$.

Proof (part II)

$$f(x) = \frac{x^q(x-1)^q \dots (x-n)^q}{q!}$$

Now, what about $f^{(i)}(k)$?

- For each k, $f^{(i)}(k) = 0$ if $i < q - 1$.
- If $i = q - 1$, we also see that $f^{(q-1)}(k) = 0$ for each $k = 0, \dots, n$.

Proof (part II)

$$f(x) = \frac{x^q(x-1)^q \dots (x-n)^q}{q!}$$

Now, what about $f^{(i)}(k)$?

- For each k, $f^{(i)}(k) = 0$ if $i < q - 1$.
- If $i = q - 1$, we also see that $f^{(q-1)}(k) = 0$ for each $k = 0, \dots, n$.
  - This doesn't give us much to work with. But removing one of the powers of x gives us a nice characterisation: it turns out that

$$f^{(q-1)}(0) = \frac{(q-1)! \cdot (-1)^q(-2)^q \cdots (-n)^q}{q!}.$$

Proof (part II)

$$f(x) = \frac{x^q(x-1)^q \dots (x-n)^q}{q!}$$

Now, what about $f^{(i)}(k)$?

- For each k, $f^{(i)}(k) = 0$ if $i < q - 1$.
- If $i = q - 1$, we also see that $f^{(q-1)}(k) = 0$ for each $k = 0, \dots, n$.
    - This doesn't give us much to work with. But removing one of the powers of x gives us a nice characterisation: it turns out that

      $$f^{(q-1)}(0) = \frac{(q-1)! \cdot (-1)^q(-2)^q \cdots (-n)^q}{q!}.$$

    - To clean this up, we can refine the denominator to be $(q-1)!$ so that $f^{(q-1)}(0)$ gives a nice expression.

Proof (part II)

$$f(x) = \frac{x^q(x-1)^q \ldots (x-n)^q}{q!}$$

Now, what about $f^{(i)}(k)$?

- For each k, $f^{(i)}(k) = 0$ if $i < q - 1$.
- If $i = q - 1$, we also see that $f^{(q-1)}(k) = 0$ for each $k = 0, \ldots, n$.
  - This doesn't give us much to work with. But removing one of the powers of x gives us a nice characterisation: it turns out that
  $$f^{(q-1)}(0) = \frac{(q-1)! \cdot (-1)^q(-2)^q \cdots (-n)^q}{q!}.$$
  - To clean this up, we can refine the denominator to be $(q-1)!$ so that $f^{(q-1)}(0)$ gives a nice expression.
- Therefore, refining f gives us
$$f(x) = \frac{x^{q-1}(x-1)^q \cdots (x-n)^q}{(q-1)!}.$$

Proof (part II)

We want to now focus on making some ground with $F(k)$ using our refined formulation for $f(k)$.

Proof (part II)

We want to now focus on making some ground with $F(k)$ using our refined formulation for $f(k)$. We saw that

- $f^{(q-1)}(0) = (-1)^q(-2)^q \dots (-n)^q$.

Proof (part II)

We want to now focus on making some ground with $F(k)$ using our refined formulation for $f(k)$. We saw that

- $f^{(q-1)}(0) = (-1)^q(-2)^q \dots (-n)^q$.
- $f^{(i)}(k) = 0$ for all $i < q - 1$.

Proof (part II)

We want to now focus on making some ground with $F(k)$ using our refined formulation for $f(k)$. We saw that

- $f^{(q-1)}(0) = (-1)^q(-2)^q \ldots (-n)^q$.
- $f^{(i)}(k) = 0$ for all $i < q - 1$.
- What about for all other values of i and k?

Proof (part II)

We want to now focus on making some ground with $F(k)$ using our refined formulation for $f(k)$. We saw that

- $f^{(q-1)}(0) = (-1)^q(-2)^q \dots (-n)^q$.
- $f^{(i)}(k) = 0$ for all $i < q - 1$.
- What about for all other values of i and k?
  - If $k \neq 0$, then clearly $f^{(q-1)}(k) = 0$.

Proof (part II)

We want to now focus on making some ground with $F(k)$ using our refined formulation for $f(k)$. We saw that

- $f^{(q-1)}(0) = (-1)^q(-2)^q \dots (-n)^q$.
- $f^{(i)}(k) = 0$ for all $i < q - 1$.
- What about for all other values of i and k?
    - If $k \neq 0$, then clearly $f^{(q-1)}(k) = 0$.
    - If $i \geq q$ and $k \neq 0$, then the term that remains must have had $(x - k)^q$ differentiated q times, leaving us with a factor of $q!$ in the numerator.

Proof (part II)

We want to now focus on making some ground with $F(k)$ using our refined formulation for $f(k)$. We saw that

- $f^{(q-1)}(0) = (-1)^q(-2)^q \dots (-n)^q$.
- $f^{(i)}(k) = 0$ for all $i < q - 1$.
- What about for all other values of i and k?
  - If $k \neq 0$, then clearly $f^{(q-1)}(k) = 0$.
  - If $i \geq q$ and $k \neq 0$, then the term that remains must have had $(x - k)^q$ differentiated q times, leaving us with a factor of $q!$ in the numerator. But this implies that

$$f^{(q)}(k) = \frac{q! \cdot X}{(q-1)!},$$

for some integer X. In other words, $f^{(i)}(k)$ is an integer multiple of q.

Proof (part II)

Therefore, what we have in $F(k)$ are some integral terms that is divisible by q and $f^{(q-1)}(0)$.

Proof (part II)

Therefore, what we have in $F(k)$ are some integral terms that is divisible by q and $f^{(q-1)}(0)$.

- This tells us that $F(k)$ is an integer and so, $a_k \cdot F(k)$ is also an integer.

Proof (part II)

Therefore, what we have in $F(k)$ are some integral terms that is divisible by q and $f^{(q-1)}(0)$.

- This tells us that $F(k)$ is an integer and so, $a_k \cdot F(k)$ is also an integer. If we can now show that the sum is necessarily non-zero for large enough q, then we are done (why?).

Proof (part II)

Therefore, what we have in $F(k)$ are some integral terms that is divisible by q and $f^{(q-1)}(0)$.

- This tells us that $F(k)$ is an integer and so, $a_k \cdot F(k)$ is also an integer. If we can now show that the sum is necessarily non-zero for large enough q, then we are done (why?).
- Note that

$$\sum_{k=0}^{n} a_k \cdot F(k)$$

  is composed of terms that are divisible by q and $f^{(q-1)}(0)$. If we can enforce $f^{(q-1)}(0)$ to not be divisible by q, then we are effectively there!

Proof (part II)

Therefore, what we have in $F(k)$ are some integral terms that is divisible by q and $f^{(q-1)}(0)$.

- This tells us that $F(k)$ is an integer and so, $a_k \cdot F(k)$ is also an integer. If we can now show that the sum is necessarily non-zero for large enough q, then we are done (why?).
- Note that

$$\sum_{k=0}^{n} a_k \cdot F(k)$$

  is composed of terms that are divisible by q and $f^{(q-1)}(0)$. If we can enforce $f^{(q-1)}(0)$ to not be divisible by q, then we are effectively there!
  - Recall that $f^{(q-1)}(0) = (-1)^q \cdot (n!)^q$. If $q > n$ and prime, then q cannot appear in the prime factorisation of $n!$ which implies that it cannot appear in the factorisation of $(n!)^q$. Thus, we let $q > n$ be prime.

Proof (part II)

How do we ensure that $a_0 \cdot F(k)$ is not a multiple of q?

Proof (part II)

How do we ensure that $a_0 \cdot F(k)$ is not a multiple of q?

- We first showed that $F(k)$ could not be a multiple of q.

Proof (part II)

How do we ensure that $a_0 \cdot F(k)$ is not a multiple of q?

- We first showed that $F(k)$ could not be a multiple of q.
- It is still possible that a_0 is a multiple of q. The easy fix is to enforce $q > |a_0|$.

Proof (part II)

How do we ensure that $a_0 \cdot F(k)$ is not a multiple of q?

- We first showed that $F(k)$ could not be a multiple of q.
- It is still possible that a_0 is a multiple of q. The easy fix is to enforce $q > |a_0|$.

Putting these together, we see that $f^{(q-1)}(0)$ is never a multiple of q; this implies that the sum $\sum_{k=0}^{n} a_k \cdot F(k)$ is non-zero for large enough q.

The contradiction!

- On the one hand, we said that

$$\left|\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt\right| \to 0$$

as $q \to \infty$.

The contradiction!

- On the one hand, we said that

$$\left|\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt\right| \longrightarrow 0$$

  as $q \longrightarrow \infty$.

- On the other hand, we also said that

$$\sum_{k=0}^{n} a_k F(k)$$

  is a non-zero integer as $q \longrightarrow \infty$.

The contradiction!

- On the one hand, we said that

$$\left|\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt\right| \longrightarrow 0$$

  as $q \longrightarrow \infty$.
- On the other hand, we also said that

$$\sum_{k=0}^{n} a_k F(k)$$

  is a non-zero integer as $q \longrightarrow \infty$.

This is the contradiction! Therefore, our assumption (that e is algebraic) must have been incorrect; thus, e is transcendental.

Putting everything together...

That was a lot to work through, so let's summarise everything here!

- Suppose that e is *algebraic*; then there exist a polynomial with integer coefficients a_j (with $a_0, a_n \neq 0$) such that

$$a_0 + a_1 e + \cdots + a_n e^n = 0.$$

Putting everything together...

That was a lot to work through, so let's summarise everything here!

- Suppose that e is *algebraic*; then there exist a polynomial with integer coefficients a_j (with $a_0, a_n \neq 0$) such that

$$a_0 + a_1 e + \cdots + a_n e^n = 0.$$

- Let $p > n, a_0$ be prime and consider the function

$$f(x) = \frac{x^{p-1}(x-1)^p(x-2)^p \cdots (x-n)^p}{(p-1)!}.$$

Putting everything together...

That was a lot to work through, so let's summarise everything here!

- Suppose that e is *algebraic*; then there exist a polynomial with integer coefficients a_j (with $a_0, a_n \neq 0$) such that

$$a_0 + a_1 e + \cdots + a_n e^n = 0.$$

- Let $p > n, a_0$ be prime and consider the function

$$f(x) = \frac{x^{p-1}(x-1)^p(x-2)^p \cdots (x-n)^p}{(p-1)!}.$$

- Letting $F(x) = \sum_{i=0}^{n} f^{(i)}(x)$, we can see that

$$\sum_{k=0}^{n} a_k e^k \int_0^k e^{-t} \cdot f(t)\, dt = -\sum_{k=0}^{n} a_k \cdot F(k).$$

Putting everything together...

- The contradiction comes from showing that the left side converges to 0 for large enough p, while the right side is a non-zero integer for large enough p.

Lindemann-Weierstrass Theorem

The Lindemann-Weierstrass Theorem

If $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a collection of *algebraic numbers* that is linearly independent over $\mathbb{Q}$, then the set $\{e^{\alpha_1}, e^{\alpha_2}, \ldots, \ldots, e^{\alpha_n}\}$ forms a set such that no element in the set is a root of any non-trivial polynomial equations with coefficients in $\mathbb{Q}$.

The Lindemann-Weierstrass Theorem

If $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a collection of *algebraic numbers* that is linearly independent over $\mathbb{Q}$, then the set $\{e^{\alpha_1}, e^{\alpha_2}, \ldots, \ldots, e^{\alpha_n}\}$ forms a set such that no element in the set is a root of any non-trivial polynomial equations with coefficients in $\mathbb{Q}$.

- But note that one can always transform a polynomial with rational coefficients to a polynomial with integer coefficients.

The Lindemann-Weierstrass Theorem

If $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a collection of *algebraic numbers* that is linearly independent over $\mathbb{Q}$, then the set $\{e^{\alpha_1}, e^{\alpha_2}, \ldots, \ldots, e^{\alpha_n}\}$ forms a set such that no element in the set is a root of any non-trivial polynomial equations with coefficients in $\mathbb{Q}$.

- But note that one can always transform a polynomial with rational coefficients to a polynomial with integer coefficients.
- Thus, the set $\{e^{\alpha_1}, \ldots, e^{\alpha_n}\}$ also forms a set such that no element in the set is a root of any non-trivial polynomial equations with coefficients in $\mathbb{Z}$.

The Lindemann-Weierstrass Theorem

If $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a collection of *algebraic numbers* that is linearly independent over $\mathbb{Q}$, then the set $\{e^{\alpha_1}, e^{\alpha_2}, \ldots, \ldots, e^{\alpha_n}\}$ forms a set such that no element in the set is a root of any non-trivial polynomial equations with coefficients in $\mathbb{Q}$.

- But note that one can always transform a polynomial with rational coefficients to a polynomial with integer coefficients.
- Thus, the set $\{e^{\alpha_1}, \ldots, e^{\alpha_n}\}$ also forms a set such that no element in the set is a root of any non-trivial polynomial equations with coefficients in $\mathbb{Z}$.
    - But this implies that each e^{α_i} is *transcendental*.

Proving that e and π are transcendental

- Proving that e and π are transcendental is a direct consequence of the theorem.

Proving that e and π are transcendental

- Proving that e and π are transcendental is a direct consequence of the theorem.
  - The set $\{1\}$ is a linearly independent set of a single algebraic number. Therefore, $e^1 = e$ is transcendental.

Proving that e and π are transcendental

- Proving that e and π are transcendental is a direct consequence of the theorem.
  - The set $\{1\}$ is a linearly independent set of a single algebraic number. Therefore, $e^1 = e$ is transcendental.
  - If π were algebraic, then πi is also algebraic. But this implies that the set $\{1, \pi i\}$ forms a linearly independent set of algebraic numbers, which implies that the elements of $\{e^1, e^{\pi i}\}$ are themselves transcendental. But $e^{\pi i} + 1 = 0$. Contradiction!

Concluding Remarks

- In this talk, we work exclusively with transcendence over $\mathbb{Q}$; we can extend this to other fields too!

Concluding Remarks

- In this talk, we work exclusively with transcendence over $\mathbb{Q}$; we can extend this to other fields too!
  - If we define polynomials whose coefficients come from $\mathbb{R}$, then e and π are no longer transcendental since $x - e$ and $x - \pi$ are polynomials in this polynomial ring.

Concluding Remarks

- In this talk, we work exclusively with transcendence over $\mathbb{Q}$; we can extend this to other fields too!
    - If we define polynomials whose coefficients come from $\mathbb{R}$, then e and π are no longer transcendental since $x - e$ and $x - \pi$ are polynomials in this polynomial ring.
- Proving transcendence is quite hard! We know that e and π are separately transcendental but we don't know whether $e + \pi$ is transcendental.