Joseph Liouville’s construction of a transcendental number

Legal information:
Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License
You are free:
to Share – to copy, distribute, display, and perform the work
to Remix – to make derivative works
Under the following conditions:
Attribution. You must attribute the work in the manner specified by the author or licensor.
Noncommercial. You may not use this work for commercial purposes.
Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under a license identical to this one.
Any of these conditions can be waived if you get permission from the copyright holder.

Images tend to be Wikipedia images, though I made all the graphs. If someone finds it useful, great. Send me an e-mail, dean at deanlm dot com, or if I made some typo, flub or used bad logic.

Top matter, inspiration


Here, we present a modified version of work of the French mathematician Joseph Liouville that explicitly made a transcendental number. The number here produced is Liouville’s Constant.

There are countless web references to transcendental numbers, a Wikipedia page. There are biographies of Joseph Liouville, discussions of transcendental numbers, and even a page on the “fifteen most famous transcendental numbers.” But could not find a good construction, though this page has some discussion on a higher level than this one, as does this link.

It is easy to say, “the number π is transcendental,” as it is easy to say, “The number e is transcendental.” Both proofs trace to the 19th century, and weren’t proving “The sum of the first n positive integers equals $\frac{n(n+1)}{2}$,” which is easy induction.

The beginning is long, as no familiarity with transcendental numbers is assumed; we build from rational numbers, to algebraic numbers, to transcendental numbers. There is some history.
Credit

Slowly typeset by Dean Moore, of Boulder, Colorado, USA.

In March 2009, for pure entertainment worked the proof, later typeset to slowly piece through, to understand the logic, fill in gaps. Parts are my revenge against math texts, where the passage “Thus it clearly follows …” was found, hours of work required to fill in the abyss between “clearly” and “follows.” Why in graduate school at CU – Boulder a mathematician studying analysis bought a book on Galois Theory—which is about solving polynomials, lands in the basket of field theory and group theory—is a lost mystery, though years later worked through it.

Fascinating material, Galois Theory. The Norwegian mathematician Niels Abel solved the same problem, in 1824, but Galois’s work of 1830 was more general. Abel solved the problem of the “insolvability” of fifth-degree polynomials. If Abel was first, Galois’s results proved that when \( n \geq 5 \), no single formula will find the roots of any polynomial of degree \( n \), some polynomials being “not solvable by radicals.”

Math knowledge needed

Knowledge of calculus, fields, a little set theory, limits of sequences and infinite sums are all musts.

Some mathematical notation used without reference

- For any number \( x \), the notation \(|x|\) denotes “absolute value,” so, \(|-9| = 9\).
- By the notation \( \mathbb{N} \) we denote the natural numbers, \( \{1, 2, 3, 4, \ldots\} \), not \( \{0, 1, 2, 3, \ldots\} \),
- The symbol \( \mathbb{Z} \) refers to the integers, \( \{-3, -2, -1, 0, 1, 2, 3, \ldots\} \),
- The symbol \( \mathbb{Q} \) refers to the rational numbers, in set notation (below), \( \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\} \),
- The symbol \( \mathbb{R} \) refers to the real numbers,
- The symbol \( \mathbb{R}^+ \) refers to positive real numbers, \( (0, \infty) = \{x \in \mathbb{R} \mid x > 0\} \),

\[ f(x) = 5x^7 - 48x^3 + 44x + 2 \]

By a result in Galois Theory, this polynomial is “insoluble.”

The polynomial cannot be factored over the rational numbers, and no formula for its roots exists.

By extracting roots of and performing algebra on rational numbers, the roots of this polynomial cannot be obtained. It is “insoluble.”
• The symbol \( \mathbb{Z}[x] \) refers to \textbf{polynomials}, with coefficients in \( \mathbb{Z} \),
• The symbol \( \mathbb{Q}[x] \) refers to polynomials, with coefficients in \( \mathbb{Q} \),
• For a polynomial \( f \), the terminology \( n = \deg(f) \) means “The parameter \( n \) is set equal to the degree of the polynomial, that is, to the highest non-zero power of \( f \).” So, \( \deg(-8x^7 + 9451x - 1023) = 7 \),
• The symbol \( \forall \) means “For all,”
• The symbol \( \exists \) means “There exists,”
• The symbol \( \epsilon \) means “Is an element of;” and,
• The notation \( \{0, 1, 2, \ldots n\} \) is a “set notation,” here means “The set of all integers from 0 to \( n \), inclusively.” So, \( \{1, 2, \ldots 7\} \) means \( \{1,2,3,4,5,6,7\} \),
• Of set notation, some sets are written like \( \left\{ \frac{p}{q} \right\} \), \( p, q \in \mathbb{Z}, q \neq 0 \), which means “The set of all fractions \( \frac{p}{q} \) such that \( p \) and \( q \) are integers, and \( q \neq 0 \),”
• Note \( i \) and \( f \) are always indices,
• The notation \( \Sigma \) denotes sum, as in, \( \sum_{i=1}^{3} \left( \frac{i+1}{i} \right) = \frac{2}{1} + \frac{2+1}{2} + \frac{3+1}{3} = 2 + \frac{3}{2} + \frac{4}{3} = \frac{29}{6} \),
• For an infinite sequence like \( \left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty} \) and some real number \( x_0 \), terminology like \( \lim_{i \to \infty} \left( \frac{p_i}{q_i} \right) = x_0 \) denotes a limit,
• Of \( \lim \sup \left( \frac{p_i}{q_i} - x_0 \right) \), remember, for a sequence \( \{x_i\}_{i=1}^{\infty} \), the definition of \textbf{limit supremum}, which is \( \lim \sup \left( x_i \right) = \lim_{i \to \infty} \left( \sup_{m \geq i} x_m \right) \). If \( \lim a_i = a \), then \( \lim \sup a_i = a \),
• By a \textbf{sequence} of rational numbers \( \left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty} \), the notations \( \frac{p_i}{q_i} - x_0 \rightarrow 0 \) and \( \frac{p_i}{q_i} \rightarrow x_0 \) is the same as \( \lim_{i \to \infty} \frac{p_i}{q_i} = x_0 \); all these notations are synonymous,
• \textbf{Topology, real analysis}: Brackets such as [ and ] mean, “Endpoint is included,” as in, a “\textbf{closed interval}.” Parentheses such as ( and ) mean “Endpoint is not included,” as in, an “open interval.” Of Calculus Result 11, below, it only holds on a “closed” interval like \([0,5]\), and is plain false, on an “open” interval such as \((0, 5)\) : for example, on \((0, 5)\), \( f(x) = x^2 \) takes neither a maximum nor a minimum value, though on \([0, 5]\), it takes both 0 and 25 as values.

The blue dots are a convergent sequence

On \((0, 5)\), \( f(x) = x^2 \) never takes on a value of 0, or of 25.
Background

Rational numbers, the ancient Greeks

Ancient Greek mathematicians assumed all numbers rational, i.e., ratios of integers as $\frac{p}{q}$ with $p, q \in \mathbb{Z}$, $q \neq 0$. Easy examples are

\[
0, 1, -4, -\frac{5}{9}, -\frac{4}{13}, -\frac{3^2 \cdot 7 \cdot 127 \cdot 7853}{28 \cdot 57} = 3.14159265, \ldots
\]

The Greeks knew about the square root of two, $\sqrt{2}$, from obvious considerations from the Pythagorean Theorem (diagram, right):

Note that $\sqrt{2}$ is the hypotenuse of the right triangle with both short legs of length 1, as $1^2 + 1^2 = 2$. Initially, they assumed $\sqrt{2}$ rational. Eventually, a Greek proved the square root of two was irrational, i.e., cannot be expressed as a fraction of two integers. This has been proven, in many ways.

Babylonian mathematics on $\sqrt{2}$.

One may use rational numbers to get arbitrarily “close” (i.e., limit), but equality cannot happen.

So, we wish to include the numbers $\pm \sqrt{2}$ in our number system, but it isn’t rational.

Notably for the polynomial $f(x) = x^2 - 2$, the numbers $x_2 = -\sqrt{2}$ and $x_3 = \sqrt{2}$ satisfy $f(x_2) = f(x_3) = 0$. So $\pm \sqrt{2}$ are the roots of a polynomial in integer coefficients.

So we have an simple way to include numbers like $\pm \sqrt{2}$ in our number system and in terms of simple familiar things: roots of polynomials of integer/rational coefficients, ideas studied since at least the ancient Egyptians and Babylonians. This is our next topic:
**Algebraic numbers**

Thus **algebraic numbers**: these are all numbers that are **roots** of some polynomial

\[ f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} + a_n x^n, \]

\( n \in \mathbb{N}; a_i \in \mathbb{Q}, \forall i \in \{0, \ldots, n\} \)

The coefficients are **rational**. Note as \( a_i \in \mathbb{Q}, \forall i \in \{0, \ldots, n\} \), and the polynomial \( f(x) \) is set equal to zero (that word “root” above), we can multiply \( f(x) \) by the least common denominator of the \( a_i \), and may as well assume

\[ f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} + a_n x^n, \]

\( n \in \mathbb{N}; a_i \in \mathbb{Z}, \forall i \in \{0, \ldots, n\} \)

As an example, a messy number such as

\[ \left( 3 + 9^{\frac{3}{5}} \right)^{\frac{11}{5}} + 1023 \]

\[ \left( \frac{7}{5^2 - 2^4 + 1} \right)^{\frac{82}{73}} - 109 \]

is algebraic, a root of some integer–coefficient polynomial. From **Galois Theory**, roots of polynomials of **degree** five and higher cannot, in general, be expressed as algebraic combinations of **radicals** of integers or rational numbers. Galois Theory gets a bit away from the subject matter of this discussion, if a book on Galois Theory inspired it.

As it’s impossible, no one **proved** all numbers are algebraic. After Liouville’s original work of 1844, in 1874 **Georg Cantor** proved the algebraic numbers a field of cardinality \( \aleph_0 \), actually small in a set–theoretic sense, the first infinity. The **real numbers** are a field of cardinality \( 2^{\aleph_0} \). Note \( 2^{\aleph_0} \) is sometimes equated to \( \aleph_1 \), but this enters set theory and gets afield for this discussion. Here \( 2^{\aleph_0} \) means “the second infinity,” which is strictly larger than \( \aleph_0 \).

Whenever \( a \) and \( b \) are integers, rational numbers, or irrational algebraic numbers, the number \( c \) is algebraic.
Transcendental numbers

Algebraic numbers led to the idea of the *transcendental number*: a number—real or complex—that is not the root of any polynomial with rational or algebraic coefficients.

The term *transcendental* goes back to at least Leibniz in 1704, if more modern formulations appear to trace to Euler in 1748.

Genesis

Transcendental numbers were first proven to exist in 1844 by the French mathematician Joseph Liouville, though he did not then construct an explicit decimal number but a continued fraction. The first decimal proven transcendental was the Liouville Constant which Liouville proved transcendental in 1850, not 1844 as stated in some web references. It belongs to a class of numbers, a “Liouville number,” is a bit odd, and never occurs in physics. The first “naturally” occurring transcendental numbers were later proven to be \( e \) (Hermite, 1873), and \( \pi \) (Lindemann, 1882).

When in 1882 the number \( \pi \) was proven transcendental, it proved that by the methods of ancient Greek geometers that it is impossible to square the circle. This question had been open for thousands of years.

After Liouville, Cantor discovered no transcendental numbers but proved they had to exist. Cantor showed the real numbers comprise a “big” **uncountable** \( 2^{\aleph_0} \) set. Cantor also showed the algebraic numbers are a **countable set**, that is, are of the cardinality called “countable infinity,” \( \aleph_0 \); see Result 2, below. As

- the algebraic numbers are **countable**, and no transcendental number is algebraic, and
- the real numbers are **uncountable**,

it follows that transcendental numbers must comprise an uncountable set of cardinality \( 2^{\aleph_0} \). Thus:

Because \( \pi \) is transcendental, it is impossible to square the circle.
Construction of a transcendental number

To do in detail, the construction is long with a few proofs. First a few preliminary results. Those who have studied a fair amount of mathematics can ignore all these results and go straight to the proofs.

Result 1

Let $x_0$ be any irrational real number. As the set of rational numbers are “dense” in the entire real line, there always exists a sequence of rational numbers $\left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty}$ such that $\frac{p_i}{q_i} \to x_0$. Such a sequence always exists, one proof here. The word “dense” is topological, and we avoid it.

Result 2

Intuitively, the cardinality of a set is the “size” of the set. For a set with a finite collection of elements, cardinality is a number.

It should be known that the integers $\mathbb{Z}$ and the rational numbers $\mathbb{Q}$ form a set of cardinality $\aleph_0$; the first infinity. This is proved countless places, here, here, here, and here. The algebraic numbers also form an $\aleph_0$ set. The real numbers form a larger set, of cardinality $2^{\aleph_0}$, the second infinity.
Result 3

It is well known, proven many places, that if \( \lim_{i \to \infty} a_i = a \), then for any subsequence \( \{a_{i_j}\}_{j=1}^{\infty} \), we have \( \lim_{j \to \infty} a_{i_j} = a \), that is, of convergent sequences, all subsequences have the same limit, proven various places. One example is the sequence \( \{a_i\}_{i=1}^{\infty} = \left\{ \frac{i+1}{i} \right\}_{i=1}^{\infty} \), which satisfies \( a_i \to 1 \), but so does the subsequence \( \{a_{i_j}\}_{j=1}^{\infty} = \left\{ \frac{ij+1}{ij} \right\}_{j=1}^{\infty} \), where \( i_j = 2i^2 \), doubling values of squares, which also satisfies \( a_{i_j} \to 1 \), really \( \lim_{j \to \infty} \left( \frac{2i^2+1}{2i^2} \right) = 1 \).

The phrase “Pass to a subsequence” is common, simply meaning, from \( \{a_i\}_{i=1}^{\infty} \) indexed by \( i \), we pass to \( \{a_{i_j}\}_{j=1}^{\infty} \), some subsequence, now indexed by \( j \).
Definition 4

Abstractly, our \( n_{th} \) - degree polynomial follows:

\[
f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} + a_n x^n,
\]

\( n \in \{0, 1, 2, 3, \ldots \}; \ a_i \in \mathbb{Q}, \forall \ i \in \{0, \ldots, n\}; \ a_n \neq 0\)

Most of our polynomials will have \( a_i \in \mathbb{Z} \), not \( a_i \in \mathbb{Q} \). The degree of a polynomial \( f(x) = \sum_{i=0}^{n} a_i x^i \) is the largest non-zero exponent; we ignore constant polynomials like \( f(x) = -5 \), so \( n \geq 1 \). Suppose we have

\[
f(x) = (6.626 \cdot 10^{-34}) \cdot x^{19} - 57x^{15} - 7x^4 + \frac{9}{2} x^2 - \frac{x}{57} + 8
\]

This is a 19\textsuperscript{th}-degree polynomial. Notably, Lemma 13 and all else below depends on the polynomial having coefficients in \( \mathbb{Z} \). This will cause no problems; see Definition 5, direct below.

The term degree deserves pointed out, as in this paper, the word degree has a second definition; see Definition 6. First, we need to define a monic polynomial.

Graph of \( f(x) = 2x^6 + 3x^5 - 3x^4 + 3x^3 + 3x^2 - 12x + 3 \), a sixth-degree polynomial. It has four real roots, two complex roots. Note \( f(x) \) cannot be factored over the rational numbers, though proving that goes outside this paper’s scope. All of its roots are irrational.
**Definition 5**

A *monic polynomial* has the coefficient of the highest exponent of $x$ equal to 1. So,

$$g(x) = x^3 - \frac{9}{2}x^2 - 3x + \frac{15}{6}$$

is monic, but

$$f(x) = 6 \cdot g(x) = 6x^3 - 27x^2 - 18x + 15$$

is not monic.

The word “monic” says nothing about if a polynomial can be factored, and nothing about the polynomial’s roots.

If we start with a monic polynomial $g(x) \in \mathbb{Q}[x]$, we can easily derive $f(x) \in \mathbb{Z}[x]$, simply by multiplying $g(x)$ by the least common denominator of all its denominators, and, $f(x)$ has the same degree and the same roots as $g(x)$; see graph, above right.

Monic polynomials are unavoidable, but all our proofs depend on polynomials with coefficients in $\mathbb{Z}$.

![Graph showing the relationship between $f(x)$ and $g(x)$](image)

An example, of a monic polynomial, also of a polynomial of integer coefficients, six times the monic polynomial. Both have the same degree and have the same roots.
**Definition 6**

Let $x_0$ be any algebraic number. We call $f(x)$ the *minimal polynomial* of $x_0$ when it is the monic polynomial of rational coefficients, of smallest degree of which $x_0$ is a root. In the last sentence the definite article *the* makes sense, as the minimal polynomial of any $x_0$ is unique, one proof [here](#).

Minimal polynomials are always what is called *irreducible*, which means, over the field $\mathbb{Q}$ they can’t be factored; a good example is $f(x) = x^2 + 2x + 7$, which has roots that are complex numbers, or perhaps $f(x) = 3x^5 - 4x + 2$, a fifth-order polynomial which has three roots that are irrational real numbers, and two that are complex, and cannot be factored. We won’t be using much of the word “irreducible,” but of polynomials, an irreducible polynomial is a bit like a prime number, which can’t be factored any further.

**Corollary 7.**

Let a minimal polynomial of an irrational root $x_0$ be $f(x) = \sum_{i=0}^{n} a_i x^i$, so, $f(x_0) = 0$. All of $f(x)$’s roots are irrational numbers.

*Proof.*

Note that if $f(x)$ has an irrational algebraic root $x_0$, then for $p, q \in \mathbb{Z}, q \neq 0$, the rational $\frac{p}{q}$ can’t be a root of $f(x)$, as if so, we can factor: There exists a $g(x)$, of degree $n - 1$, such that $f(x) = g(x) \cdot (qx - p)$, and for $x_0$ we would have a new minimal polynomial $g(x)$, of degree $n - 1$. This would violate the definition of minimal polynomial, stated in Definition 6.

So, an important corollary follows: If a minimal polynomial has one irrational root, then all its roots are irrational. □

Henceforth can avoid the word “minimal,” and all in this discussion will work, if some modifications are needed. But minimal polynomials are “nice,” as they are of lowest possible degree, so we use them.
**Definition 8**

When \( f(x) \in \mathbb{Q}[x] \) is the minimal polynomial of \( x_0 \), and \( f(x) \) is of degree \( n \), the number \( n \) is called the *degree* of the number \( x_0 \).

The last paragraph is the second definition of the word *degree*.

All rational numbers are of degree 1. We will be looking at irrational numbers, roots of polynomials like \( f(x) = x^2 + x - 3 \), so all our degrees of interest will be of at least degree 2.

We note, minimal polynomials are monic, hence are assumed to have coefficients in \( \mathbb{Q} \), not \( \mathbb{Z} \). If most of our polynomials are assumed to have coefficients in \( \mathbb{Z} \), this will cause no problems; see Definition 5.

**Definition 9**

All of our polynomial are over the *base field* of \( \mathbb{Q} \), which notably includes minimal polynomials. In this paper we are not going into the concept of a “base field,” but for our discussion, most polynomials will have coefficients in \( \mathbb{Z} \), but minimal polynomials have coefficients in \( \mathbb{Q} \). This will cause no problems; see Definition 5.

**Comment 10**

In any fraction \( \frac{p}{q} \), assume \( q \geq 1 \), as we can always move a negative sign to \( p \); note \( \frac{3}{-7} = -\frac{3}{7} \).

Whenever \( \frac{p_i}{q_i} \to x_0 \), after a finite point, all \( \frac{p_i}{q_i} \) are the same sign, so if needed, take a subsequence, and move all minus signs to \( p_i \). This avoids absolute values like \( |q_i| \), thus clogs proofs with less notation. Should you wish, fill them in mentally.
Calculus Result 11

Let \( f(x) \) be a polynomial, so its derivative is continuous. Let \( x_0 \) be an irrational root of \( f(x) \).

Now remember, absolute value function is continuous. Thus by the **extreme value theorem** of calculus, on a bounded, closed interval the continuous composition \( \left| \frac{df}{dx} \right| \) is bounded. So \( \exists M \in \mathbb{R}^+ \) such that \( \forall x \in [x_0 - 1, x_0 + 1] \) we have \( |f'(x)| \leq M \).

A graph of the irreducible function \( f(x) = 2x^5 - 9x + 3 \), plus \( \left| \frac{d}{dx} f(x) \right| \), shows why the Extreme Value Theorem works, if only for one function.
Convention 12

For $x_0$ any irrational root of the polynomial $f(x) \in \mathbb{Z}[x]$, assume $\frac{p}{q} \in \mathbb{Q}$ is “close” to $x_0$ in the sense of

$$x_0 - 1 \leq \frac{p}{q} \leq x_0 + 1$$

and that $\frac{p}{q}$ is closer to $x_0$ than to any other root of $f$. In a so–so graph, of a polynomial that cannot be factored over $\mathbb{Q}$:

We want $f\left(\frac{p}{q}\right) \neq 0$, why $\frac{p}{q}$ is closer to $x_0$ than to any other root of $f(x)$. Be $f(x)$ derived from a minimal polynomial, we note that $f\left(\frac{p}{q}\right) \neq 0$ is true for all $\frac{p}{q} \in \mathbb{Q}$; see Corollary 7.

Done with setup.

All further proofs depend on Lemma 13, direct below.
Proofs

**Lemma 13.**

Let $f(x) \in \mathbb{Z}[x]$ be of degree $n$, with $f(x) = \sum_{i=0}^{n} a_n x^n$. If $p \in \mathbb{Z}, q \in \mathbb{N},$ and $f \left( \frac{p}{q} \right) \neq 0$, then $|f \left( \frac{p}{q} \right)| \geq \frac{1}{q^n}$ is true.

Note if we specify that $f(x)$ is a constant multiple of the minimal polynomial of an irrational number $x_0$, then $f \left( \frac{p}{q} \right) \neq 0$ is automatic; see Corollary 7.

**Proof.**

Taking absolute values of both sides of $f \left( \frac{p}{q} \right) = \sum_{i=0}^{n} a_n \left( \frac{p}{q} \right)^i$, we have:

$$|f \left( \frac{p}{q} \right)| = \left| \sum_{i=0}^{n} a_i \left( \frac{p}{q} \right)^i \right|$$

Now multiply last equations by $q^n$, and as $q \in \mathbb{N}$ is assumed, – see Comment 10 – $q^n$ “filters through” the absolute value brackets:

$$q^n |f \left( \frac{p}{q} \right)| = q^n \left| \sum_{i=0}^{n} a_i p^i q^{-i} \right| = \left| \sum_{i=0}^{n} a_i p^i q^{n-i} \right|$$

In the right-side of the equation above, note that $i$ ranges from 0 to $n$, so

$$n - i \in \{n, n - 1, n - 2, ..., 2, 1, 0\}$$

and $q^{n-i} \in \mathbb{N}$ is always true. As for all $i$ we also have $a_i \in \mathbb{Z}$ and $p^i \in \mathbb{Z}$, all terms in the upper right sum are integers. As $f \left( \frac{p}{q} \right) \neq 0$, we have $q^n |f \left( \frac{p}{q} \right)| \geq 1$.

Dividing by $q^n$ we get $|f \left( \frac{p}{q} \right)| \geq \frac{1}{q^n}$. □
Comment 14

Math 101 error: Note that as \( f(x) \in \mathbb{Z}[x] \), we can’t “cheat our way out” of the lemma by dividing \( f(x) \) by “large” integers to reduce the magnitude of \(|f(x)|\), thus making \(|f\left(\frac{p}{q}\right)| < \frac{1}{q^n}\). If we get a new polynomial \( g(x) \) by dividing \( f(x) \) by the Greatest Common Factor of all of \( f(x) \)’s coefficients, the lemma is still true, but we can go no further, as we will get a \( g(x) \in \mathbb{Q}[x] \). We may as well have \( f(x) \) be the multiple of the Least Common Multiple of the denominators of a minimal polynomial, as this gives us the smallest values of \(|f(x)|\).

Also note, to use coprime \( p \) and \( q \) makes the most sense, gives the largest lower bound. This is not necessary for the proof.

Example 15

As an example of the last lemma, \( x = \sqrt{3} \) satisfies \( f(x) = x^2 - 3 \). While \( \sqrt{3} = 1.73205 \ldots \) is irrational, its digits having no known pattern and never ending, we can approximate it with

\[
\frac{p}{q} = \frac{173205}{10000} = \frac{3^3 \cdot 1283}{20000}
\]

(coprime form). So \( q = 20000 \). Note

\[
\left| f\left(\frac{p}{q}\right) \right| = \left| \left(\frac{3^3 \cdot 1283}{20000}\right)^2 - 3 \right| \approx 2.795 \cdot 10^{-6}
\]

Here, \( n = 2 \) (as \( \deg(x^2 - 3) = 2 \)), and \( \frac{1}{q^2} = \frac{1}{20000^2} = 2.5 \cdot 10^{-9} \), and as

\[
f\left(\frac{p}{q}\right) = 2.795 \cdot 10^{-6} \geq \frac{1}{q^2} = \frac{1}{20000^2} = 2.5 \cdot 10^{-9}
\]

that \( |f\left(\frac{p}{q}\right)| \geq \frac{1}{q^n} \) seems obvious, by about three orders of magnitude.
We note, the proof of Lemma 17 is a little easier, with a preliminary lemma.

**Lemma 16.**

Let \( x_0 \) be an irrational root of the \( n \)th-degree polynomial \( f(x) \). Let \( \frac{p}{q} \) be any rational number is “near” \( x_0 \) in the sense that \( \frac{p}{q} \in [x_0 - 1, x_0 + 1] \); see Convention 12.

**Conclusion:** There exists a \( c \in \left( \min \left\{ x_0, \frac{p}{q} \right\}, \max \left\{ x_0, \frac{p}{q} \right\} \right) \) such that

\[
f'(c) = \frac{f\left( \frac{p}{q} \right)}{\frac{p}{q} - x_0}
\]

**Proof.**

By the **Mean Value Theorem**, between \( \frac{p}{q} \) and \( x_0 \) there is a point \( c \in \left( \min \left\{ \frac{p}{q}, x_0 \right\}, \max \left\{ \frac{p}{q}, x_0 \right\} \right) \) such that the tangent line through \( (c, f(c)) \) with a slope of \( m = f'(c) \) is parallel to the secant line through \( \left( \frac{p}{q}, f\left( \frac{p}{q} \right) \right) \) and \( (x_0, f(x_0)) = (x_0, 0) \), explicitly, looking at slopes, we have

\[
f'(c) = \frac{f\left( \frac{p}{q} \right) - f(x_0)}{\frac{p}{q} - x_0}
\]

As \( f(x_0) = 0 \), we may restate the right side,

\[
f'(c) = \frac{f\left( \frac{p}{q} \right)}{\frac{p}{q} - x_0}
\]

For a perhaps easier “visual proof,” see illustration, right. □
Lemma 17.

Let $x_0$ be an irrational root of the $n^{th}$-degree minimal polynomial $g(x) \in \mathbb{Q}[x]$. Multiply $g(x)$ by the least common denominator of its denominators, deriving $f(x) \in \mathbb{Z}[x]$. Let $\frac{p}{q}$ be any rational number is “near” $x_0$ in the sense that $\frac{p}{q} \in [x_0 - 1, x_0 + 1]$; see Convention 12.

Conclusion: For all $\frac{p}{q} \in [x_0 - 1, x_0 + 1]$, there exists an $M \in \mathbb{R}^+$ such that

$$\frac{1}{M \cdot q^n} \leq \left| \frac{p}{q} - x_0 \right|$$

Proof.

We have a graph that looks vaguely like

$$f(x) = 2x^5 - 15x - 3$$

$$g(x) = x^5 - (15/2)x - 3/2$$
Let $M > 0$ be as in Calculus Result 11: $\forall x \in [x_0 - 1, x_0 + 1]$ we have $|f'(x)| \leq M$. Looking at the graphs, it is obvious by “visual proof” that such a constant as $M$ exists.

Note $x_0$ is irrational, so $\frac{p}{q} \neq x_0$ and $f\left(\frac{p}{q}\right) \neq 0$; see Corollary 7. Important, $\frac{p}{q} - x_0 \neq 0$, so we may divide by it.

By Lemma 16, choose $c \in \left(\min\{x_0, \frac{p}{q}\}, \max\{x_0, \frac{p}{q}\}\right)$ such that

$$f'(c) = \frac{f\left(\frac{p}{q}\right)}{\frac{p}{q} - x_0}$$

Taking absolute values, from our chosen value of $M$ this gives

$$M \geq |f'(c)| = \left|f\left(\frac{p}{q}\right)\right| \cdot \left|\frac{1}{\frac{p}{q} - x_0}\right|$$

Throw out the middle:

$$M \geq \left|f\left(\frac{p}{q}\right)\right| \cdot \left(\frac{1}{\left|\frac{p}{q} - x_0\right|}\right)$$
But from Lemma 13 we know that

\[ \left| f\left( \frac{p}{q} \right) \right| \geq \frac{1}{q^n} \]

Joining this with \( M \geq \left| f\left( \frac{p}{q} \right) \cdot \frac{1}{p-x_0} \right| \),

\[ M \geq \left| f\left( \frac{p}{q} \right) \cdot \frac{1}{p-x_0} \right| \geq \left( \frac{1}{q^n} \right) \cdot \left( \frac{1}{\left| \frac{p}{q} - x_0 \right|} \right) \]

Tossing the middle term,

\[ M \geq \left( \frac{1}{q^n} \right) \cdot \left( \frac{1}{\left| \frac{p}{q} - x_0 \right|} \right) \]

We divide by \( M \), multiply by \( p - x_0 \) and flip the inequality to derive

\[ \frac{1}{M \cdot q^n} \leq \left| \frac{p}{q} - x_0 \right| \]

This verifies our inequality. □
Corollary 18

Assume we have a sequence $\{\frac{p_i}{q_i}\}_{i=1}^{\infty}$ and an irrational algebraic number $x_0$ of degree $n$, such that $\frac{p_i}{q_i} \to x_0$. Take a subsequence $\{\frac{p_{ij}}{q_{ij}}\}_{j=1}^{\infty}$ within $[x_0 - 1, x_0 + 1]$. There exists a constant $M$ such that

$$\frac{1}{M \cdot (q_{ij})^n} \leq \left| \frac{p_{ij}}{q_{ij}} - x_0 \right|$$

is always true. □

The upcoming Proposition 21 shows that for only a finite set of rational numbers can $\left| \frac{p}{q} - x_0 \right|$ be less than a stronger bound and matters in Theorem 31 that proves the existence of a transcendental number.

We note of Proposition 21 below that for $f \in \mathbb{Z}[x]$, the minimal polynomial of an irrational root $x_0$, the Thue–Siegel–Roth Theorem gives stronger bounds. Its proof is not easy, and led to a Fields Medal.

Proposition 21 is our important “speed limit.” To prove Proposition 21, first we need a lemma.
Lemma 19.

Let \( \left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty} \), \( p_i, q_i \in \mathbb{Z} \), with \( q_i \neq 0 \ \forall \ i \in \mathbb{N} \) be a sequence of unique rational numbers, and let \( x_0 \) be an irrational number such that \( \frac{p_i}{q_i} \to x_0 \).

Then \( |p_i| \to \infty \) and \( |q_i| \to \infty \).

Proof.

Case 1: If \( \exists \ M_1, M_2 \in \mathbb{N} \) such that \( |q_i| \leq M_1 \) and \( |p_i| \leq M_2 \) for all \( i \), then \( \left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty} \) cannot be a unique set of rational numbers: there exist at most \( M_1 \cdot M_2 \) choices of rational numbers, and \( \left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty} \) is an infinite set.

Case 2: If \( |q_i| \leq M_1 \in \mathbb{N} \) but \( p_i \) is unbounded, then \( |p_i| \to \infty \) is forced, as the rational numbers in the set \( \left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty} \) are unique. By the Reverse Triangle Inequality, we have

\[
\left| \frac{p_i}{q_i} - x_0 \right| \geq \left| \left| \frac{p_i}{q_i} \right| - |x_0| \right| > \left| \frac{p_i}{q_i} \right| \geq \frac{|p_i|}{M_1} \to \infty
\]

But \( \left| \frac{p_i}{q_i} - x_0 \right| \to 0 \).

Case 3: If \( |p_i| \leq M_2 \in \mathbb{N} \) but \( q_i \) is unbounded, then \( |q_i| \to \infty \) is forced, as the set of rational numbers in \( \left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty} \) are unique. As \( q_i \to \infty \), we have \( \frac{M_2}{q_i} \to 0 \). Note \( \left| \frac{p_i}{q_i} \right| \leq \frac{M_2}{q_i} \to 0 \) implies \( \frac{p_i}{q_i} \to 0 \), and \( \frac{p_i}{q_i} \to 0 \) forces \( \left| \frac{p_i}{q_i} - x_0 \right| \to x_0 \), not \( \left| \frac{p_i}{q_i} - x_0 \right| \to 0 \).

Concluding, \( \frac{p_i}{q_i} \to x_0 \) forces \( |p_i| \to \infty \) and \( |q_i| \to \infty \). □
Comment 20

All we use in Proposition 21 below is that \( |q_i| \to \infty \). Out of Lemma 19, the fact that \( |p_i| \to \infty \) deserves to be known.

We reiterate: By Result 1, if \( x_0 \) is any irrational real number, a sequence of rational numbers \( \{ \frac{p_i}{q_i} \}_{i=1}^{\infty} \) with \( \frac{p_i}{q_i} \to x_0 \) always exists.

Thus, whenever \( \{ \frac{p_i}{q_i} \}_{i=1}^{\infty} \) is any infinite set of rational numbers converging to an irrational number \( x_0 \), as \( \left| \frac{p_i}{q_i} - x_0 \right| \to 0 \), to arrange for them to be unique is easy:

- A sequence \( \{ \frac{p_i}{q_i} \}_{i=1}^{\infty} \) of rational numbers can never limit on an irrational number \( x_0 \) at a finite point, so,
- throw out all repeated elements of \( \{ \frac{p_i}{q_i} \}_{i=1}^{\infty} \),

which after a finite point, can’t exist: if, say, for a fixed index \( j_0 \), we have \( \frac{p_{j_0}}{q_{j_0}} \) repeated infinite times, then

\[
\lim_{i \to \infty} \sup \left| \frac{p_i}{q_i} - x_0 \right| \geq \left| \frac{p_{j_0}}{q_{j_0}} - x_0 \right| > 0
\]

and \( \left| \frac{p_i}{q_i} - x_0 \right| \to 0 \) is impossible. So for some subsequence \( \{ \frac{p_{j_i}}{q_{j_i}} \}_{i=1}^{\infty} \), all \( \frac{p_{j_i}}{q_{j_i}} \) are unique.

The important “speed limit” follows. The next proposition is just as true, for an irrational algebraic number \( x_0 \) and any polynomial \( f(x) \in \mathbb{Z}[x] \) satisfying \( f(x_0) = 0 \), but a minimal polynomial is “nicer,” as it gives the best bound.
Proposition 21.

Let \( g(x) \in \mathbb{Q}[x] \) be of degree \( n \), and assume it the minimal polynomial of the irrational algebraic number \( x_0 \). Let \( f(x) \in \mathbb{Z}[x] \) be \( g(x) \) multiplied by the product of the least common denominator of the denominators of \( g(x) \).

Note \( g(x) \) has no roots that are rational numbers; see Corollary 7. Thus \( f(x) \) has no roots that are rational. Also, \( f(x) \) has integer coefficients, has the same degree as \( g(x) \), and has the same roots as \( g(x) \). A fifth-order example is graphed, above right.

Fix a real \( K > 0 \). Fix \( m \in \mathbb{N} \) such that \( m > n \).

Let \( \left\{ \frac{p_{ij}}{q_{ij}} \right\}_{i=1}^{\infty} \) be a set of unique rational numbers such that \( \frac{p_{i}}{q_{i}} \to x_0 \). For all \( i \), assume \( q_i \geq 1 \); see Comment 10.

Conclusion: There exists an at most finite sub-set \( S \) of \( \left\{ \frac{p_{i}}{q_{i}} \right\}_{i=1}^{\infty} \) of some of size \( N < \infty \), specifically, \( S = \left\{ \frac{p_{ij}}{q_{ij}} \right\}_{j=1}^{N} \), such that

\[
\left| \frac{p_{ij}}{q_{ij}} - x_0 \right| < \frac{K}{(q_{ij})^m}
\]

Proof.

We do a “proof by contradiction,” that is, assume the proposition’s statement false, and show it leads to a contradiction.
Assume there exists an infinite subsequence

$$S = \left\{ \frac{p_{ij}}{q_{ij}} \right\}_{j=1}^{\infty}$$

such that

$$\left| \frac{p_{ij}}{q_{ij}} - x_0 \right| < \frac{K}{(q_{ij})^m}$$

is true for all $j$, and, for all $j$ we have $\frac{p_{ij}}{q_{ij}} \in [x_0 - 1, x_0 + 1]$. As $x_0$ is an algebraic number, we may use Comment 18, and we may assume there exists an $M > 0$ such that for all $j$

$$\frac{1}{M \cdot (q_{ij})^n} \leq \left| \frac{p_{ij}}{q_{ij}} - x_0 \right|$$

Thus

$$\frac{1}{M \cdot (q_{ij})^n} \leq \left| \frac{p_{ij}}{q_{ij}} - x_0 \right| < \frac{K}{(q_{ij})^m}$$

is always true. Throwing out the middle of the last equation, we get

$$\frac{1}{M \cdot (q_{ij})^n} < \frac{K}{(q_{ij})^m}$$

is always true. Via algebra, the following is always true:

$$\left( q_{ij} \right)^{m-n} < M \cdot K \quad \text{(Equation 1)}$$

As $\frac{p_{ij}}{q_{ij}} \to x_0$ is clear, we can use Lemma 19. Thus, $\lim_{j \to \infty} q_{ij} = \infty$, and as $m - n \geq 1$, for all but at most a finite set of $j$ we have forced

$$\left( q_{ij} \right)^{m-n} > M \cdot K$$
violating the inequality \((q_i)^{m-n} < M \cdot K\) (Equation 1 above). Thus for an infinite set of \(j\), the subsequence \(\left\{\frac{p_{ij}}{q_{ij}}\right\}_{j=1}^{\infty}\) violates the inequality of Equation 1, and for an infinite set of \(i\), \(\left\{\frac{p_i}{q_i}\right\}_{l=1}^{\infty}\) violates the same inequality, and our initial assumption is false. Any set as in the proposition’s statement is necessarily \textit{finite}—this will be key to proving a number transcendental.

This verifies the proposition and is our “speed limit.” □

**Corollary 22**

Set \(K = 2\), and use \(n + 1 > n\). By passing to a new subsequence \(\left\{\frac{p_{ik}}{q_{ik}}\right\}_{k=1}^{\infty}\) and arranging for all \(j\) that \(\frac{p_{ij}}{q_{ij}} \epsilon [x_0 - 1, x_0 + 1]\), we can arrange that

\[
\left| \frac{p_{ik}}{q_{ik}} - x_0 \right| < \frac{2}{(q_{ik})^{n+1}}
\]

never happens. □

It is time to define our transcendental number.

**Definition 23**

We define a new number \(x_1\) in a special way:

\[
x_1 = \sum_{m=1}^{\infty} 10^{-m!}
\]

In the exponential we use \textit{factorial function}, as in \(5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120\).

**Definition 24**

Define a sequence of rational numbers, \(\left\{\frac{p_i}{q_i}\right\}_{n=1}^{\infty}\), by \(\frac{p_i}{q_i} = \sum_{m=1}^{i} 10^{-m!}\).

In the next lemma, we will prove that sequence converges, so \(x_1\) exists, as a single finite number.
Lemma 25.

The number we just defined exists and is finite.

Proof.

Apply a standard calculus test, the ratio test:

In a “generic” series \( \sum_{m=1}^{\infty} a_m \), we have \( a_m = 10^{-m!} \). First do some algebra:

\[
\left| \frac{a_{m+1}}{a_m} \right| = \frac{10^{-(m+1)!}}{10^{-m!}} = \frac{1}{(10^{-m!}) \cdot (10^{(m+1)!})} = \frac{1}{10^{-m!} \cdot (10^{(m+1)!})} = \frac{1}{10^{-m!} + 10^{(m+1)!}} = \frac{1}{10^{m!} (-1 + m+1)} = \frac{1}{10^{m!} m}
\]

Now apply the ratio test: It is easy that \( \lim_{m \to \infty} \sup_{m} \left| \frac{1}{10^{m!} m} \right| = 0 \), thus the condition of the ratio test is satisfied. We have \( x_1 = \sum_{m=1}^{\infty} 10^{-m!} \) is an absolutely convergent series, so is convergent. So, \( \frac{p_i}{q_i} \to x_0 \). □
Corollary 26.

Note for $j > i$ that $\frac{p_j}{q_j} > \frac{p_i}{q_i}$, so the sequence $\left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty}$ is strictly monotonically increasing, and, thus is a set of unique rational numbers; for “visual proof,” see the graph, right. □

Lemma 27.

We maintain that $p_i = \sum_{m=1}^{i} 10^{i-m}!$ and $q_i = \frac{1}{10^i}$

Proof.

The number $x_1$ is an infinite sum of rational numbers with no common denominator, but we need a set of unique, pure fractions $\left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty}$ such that $\lim_{i \to \infty} \left( \frac{p_i}{q_i} \right) = x_0$.

At each point $i$ we write the $i$th term of an infinite sequence of rational numbers $\left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty}$ as

$$\frac{p_i}{q_i} = \sum_{m=1}^{i} 10^{-m!} = 10^{-1!} + 10^{-2!} + 10^{-3!} + \cdots + 10^{-(i-1)!} + 10^{-i!}$$

Do some algebra to get a common denominator:

$$\frac{p_i}{q_i} = \left( \frac{10^{1l}}{10^{1l}} \right) \cdot \left( 10^{-1!} + 10^{-2!} + 10^{-3!} + \cdots + 10^{-(i-1)!} + 10^{-i!} \right) =$$

$$\left( \frac{10^{1l-1!} + 10^{1l-2!} + 10^{1l-3!} + \cdots + 10^{1l-(i-1)!} + 10^{1l-i!}}{10^{1l}} \right)$$

So, as formulas, $p_i = \sum_{m=1}^{i} 10^{i-m}!$ and $q_i = \frac{1}{10^i}$. □

We comment, the following lemma simplifies the proof of Lemma 29, which simplifies the proof of Theorem 31, our final, “big” theorem.
Lemma 28.

We maintain,

\[ \left| \frac{p_i}{q_i} - x_1 \right| = \sum_{m=i+1}^{\infty} \left( \frac{1}{10^m} \right) \]

Proof.

Go back to our definition of \( x_1 \). The second line of upcoming formulas requires small re-ordering, but that’s easy, inside the absolute value brackets. Note that at any finite point \( i \) that

\[ \left| \frac{p_i}{q_i} - x_1 \right| = \left| \sum_{m=1}^{i} 10^{-m!} - \sum_{m=1}^{\infty} 10^{-m!} \right| = \]

\[ \sum_{m=i+1}^{\infty} 10^{-m!} = \frac{1}{10^{(i+1)!}} + \frac{1}{10^{(i+2)!}} + \frac{1}{10^{(i+3)!}} + \cdots \]

Thus,

\[ \left| \frac{p_i}{q_i} - x_1 \right| = \sum_{m=i+1}^{\infty} \frac{1}{10^m} \]

We have our value. \( \square \)
Comment 29

Note $x_1$ is called a **Liouville Constant** (more than one exists) and

$$x_1 = 0.11000100000000000000001000...$$

with the 1s getting progressively farther and farther apart. As digits of $x_1$ have no repeating pattern, it is easily irrational.

Our “big” Theorem 31 is an easier proof, with a small lemma.

**Lemma 30.**

*From Lemma 76, we know that $\left| \frac{p_i}{q_i} - x_1 \right| = \sum_{m=1}^{\infty} \frac{1}{10^m}$ is true. The following inequality is also true:*

$$\left| \frac{p_i}{q_i} - x_1 \right| < \frac{2}{10^{(i+1)!}}$$

*Proof.*

From Lemma 28, we are really proving is

$$\left| \frac{p_i}{q_i} - x_1 \right| = \frac{1}{10^{(i+1)!}} + \frac{1}{10^{(i+2)!}} + \frac{1}{10^{(i+3)!}} + \cdots < \frac{2}{10^{(i+1)!}}$$

By canceling one term of $\frac{1}{10^{(i+1)!}}$, we simplify what we wish to prove:

$$\frac{1}{10^{(i+2)!}} + \frac{1}{10^{(i+3)!}} + \cdots < \frac{1}{10^{(i+1)!}} $$ (Equation 1)
Now look at individual terms of the left-hand side of Equation 1 and compare them to the right-hand side. Note that for any $j \geq 1$ that
\[
\frac{1}{10^{(i+1+j)!}} < \frac{1}{10^{(i+1)!}}
\]

The left-hand side of Equation 1 has nonzero digits in strictly increasing decimal positions $(i + 2)!$, $(i + 3)!$, ... that strictly progress to the right. Note that $\frac{1}{10^{(i+1)!}}$ has one non-zero digit at position $(i + 1)!$, strictly to the left of all non-zero digits on the left-hand side of Equation 1.

Thus,
\[
\left| \frac{p_i}{q_i} - x_1 \right| < \frac{2}{10^{(i+1)!}}
\]

Our inequality is verified. □

Now for our “big” theorem, up to which we have been building.
**Theorem 31.**

There does not exist a polynomial \( f(x) \in \mathbb{Z}[x] \) of which \( x_1 \) is a root.

*Proof.*

By Lemma 25 we have a sequence of rational numbers \( \left\{ \frac{p_i}{q_i} \right\}_{n=1}^{\infty} \) with \( \frac{p_i}{q_i} \to x_0 \).

Note by the definition of \( \left\{ \frac{p_i}{q_i} \right\}_{n=1}^{\infty} \), for any subsequence \( \left\{ \frac{p_i}{q_i} \right\}_{i=1}^{\infty} \) it is always true that

\[
\left| \frac{p_i}{q_i} - x_1 \right| < \frac{2}{10(i+1)!}
\]

and such may always be chosen. There is a conflict, between Corollary 22 and Lemma 30. We have

\[
\left| \frac{p_i}{q_i} - x_1 \right| < \frac{2}{10(i+1)!}
\]

is true for all \( j \geq 1 \), and \( \left\{ \frac{p_i}{q_i} \right\}_{j=1}^{\infty} \) is an infinite set, a direct contradiction to Proposition 21 and impossible if \( x_1 \) is an algebraic number. Thus \( x_1 \) is not an algebraic number. \( \square \)

**Final Conclusion 32**

By Theorem 31, one Liouville Constant \( x_1 = \sum_{m=1}^{\infty} 10^{-m!} \) cannot be the root of any polynomial with coefficients in \( \mathbb{Z} \) (equivalent, \( \mathbb{Q} \)), hence \( x_1 \) is not an algebraic number. That is to say, \( x_1 \) is a **transcendental number**. \( \square \)

**Final comment 33**

Again, just in the world of real numbers, as Cantor proved

- the algebraic numbers are **countable**, of cardinality \( \aleph_0 \), the first infinity, and
- the real numbers are **uncountable**, of cardinality \( 2^{\aleph_0} \), the second infinity,

it follows that transcendental numbers must be an uncountable set, that is, of cardinality \( 2^{\aleph_0} \). For such a large set, as of August 2020 precious few numbers have been **proven** transcendental.