An Invitation to Modern Number Theory
Countable, Uncountable, Algebraic and Transcendentals

Steven J. Miller and
Ramin Takloo-Bighash

October 23, 2003

Contents

Chapter 1

Algebraic and Transcendental Numbers

Definition 1.0.1 (Algebraic Number). $\alpha \in \mathbb{C}$ *is an algebraic number if it is a root of a polynomial with finite degree and integer coefficients.*

Definition 1.0.2 (Transcendental Number). $\alpha \in \mathbb{C}$ *is a transcendental number if it is not algebraic.*

Thus, a transcendental number is a number that does not satisfy any polynomial equation with integer coefficients. Fortunately primitive man must have thought that every number is algebraic otherwise the development of mathematics would have suffered greatly. But transcendental numbers do exist. The mere existence of such numbers was a puzzling problem for hundreds of years. Remember that back in the Pythagorean era the existence of irrational numbers was quite a devastating event. The existence of transcendental numbers, however, must have brought a sense of relief to the mathematical psyche. For one, the transcendence of a certain number, π, settled the long-standing problem of proving the impossibility of squaring a circle. Also, it showed that the theory of equations is simply not enough, and hence it opened the door for the development of other branches of mathematics. The purpose of this chapter is to prove the existence of transcendental numbers. While it is possible to write down explicit examples of transcendental numbers (e, π, etc!), we prefer to show the existence using a different method. Here we will use Cantor's ingenious counting argument. The basic idea is to show that there are a lot more real numbers than there are algebraic numbers. This will then show that there must be a left-over set, entirely consisting of transcendental numbers. We will see from the proof, that are a lot more transcendental numbers than there are algebraic ones; in fact, if one chooses a random number, the chance of it being transcendental is effectively one hundred percent!

1.1 Definitions and Cardinalities of Sets

1.1.1 Definitions

A function $f : A \to B$ is **one-to-one** (or injective) if $f(x) = f(y)$ implies $x = y$; f is **onto** (or surjective) if given any $b \in B$, $\exists a \in A$ with $f(a) = b$. A **bijection** is a one-to-one and onto function.

We say two sets A and B **have the same cardinality** (ie, are the same size) if there is a bijection $f : A \to B$. We denote the common cardinality by $|A| = |B|$. If A has finitely many elements (say n elements), A is **finite** and $|A| = n < \infty$.

Exercise 1.1.1. *Show two finite sets have the same cardinality if and only if they have the same number of elements.*

Exercise 1.1.2. *If f is a bijection from A to B, prove there is a bijection $g = f^{-1}$ from B to A.*

Exercise 1.1.3. *Suppose A and B are two sets, and suppose we have two onto maps $f : A \to B$ and $g : B \to A$. Then show that $|A| = |B|$.* ***NOT AS EASY AS IT SEEMS***

Exercise 1.1.4. *A set A is called infinite if there is a one-to-one map $f : A \to A$ which is not onto. Using this definition, show that the sets $\mathbb{N}$ and $\mathbb{Z}$ are infinite sets. In other words, prove that an infinite set has infinitely many elements.*

Exercise 1.1.5. *Show that the cardinality of the even integers is the same as the cardinality of the integers.*

Remark 1.1.6. *The above example is surprising to many.* ***MAYBE ADD REMARK HERE ABOUT COUNTING INTEGERS UP TO X, AND LOOKING AT LIMITS****.*

A is **countable** if there is a bijection between A and the integers $\mathbb{Z}$. A is **at most countable** if A is either finite or countable.

Exercise 1.1.7. *Let x, y, z be subsets of X (for example, $X = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}^n$, et cetera). Define $R(x, y)$ to be true if $|x| = |y|$ (the two sets have the same cardinality), and false otherwise. Prove R is an equivalence relation.*

1.1.2 Countable Sets

We show that several common sets are countable. Consider the set of whole numbers $\mathbb{W} = \{1, 2, 3, \dots\}$. Define $f : \mathbb{W} \to \mathbb{Z}$ by $f(2n) = n - 1$, $f(2n + 1) = -n - 1$. By inspection, we see f gives the desired bijection between $\mathbb{W}$ and $\mathbb{Z}$.

Similarly, we can construct a bijection from $\mathbb{N}$ to $\mathbb{Z}$, where $\mathbb{N} = \{0, 1, 2, \dots\}$.

Thus, we have proved

Lemma 1.1.8. *To show a set S is countable, it is sufficient to find a bijection from S to either $\mathbb{W}$ or $\mathbb{N}$.*

We need the intuitively plausible

Lemma 1.1.9. *If $A \subset B$, then $|A| \leq |B|$.*

Definition 1.1.10. *If $f : A \to C$ is a one-to-one function (not necessarily onto), then $|A| \leq |C|$. Further, if $C \subset A$, then $|A| = |C|$.*

Exercise 1.1.11. *Prove Lemmas 1.1.9 and 1.1.10.*

If A and B are sets, the **cartesian product** $A \times B$ is $\{(a, b) : a \in A, b \in B\}$.

Theorem 1.1.12. *If A and B are countable, so is $A \cup B$ and $A \times B$.*

Proof. We have bijections $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to B$. Thus, we can label the elements of A and B by

$$\begin{aligned} A &= \{a_0, a_1, a_2, a_3, \dots\} \\ B &= \{b_0, b_1, b_2, b_3, \dots\}. \end{aligned} \tag{1.1}$$

Assume $A \cap B$ is empty. Define $h : \mathbb{N} \to A \cup B$ by $h(2n) = a_n$ and $h(2n+1) = b_n$. We leave to the reader the case when $A \cap B$ is not empty.

To prove the second claim, consider the following function $h : \mathbb{N} \to A \times B$:

$$\begin{aligned}
&h(1) = (a_0, b_0)\\
&h(2) = (a_1, b_0), h(3) = (a_1, b_1), h(4) = (a_0, b_1)\\
&h(5) = (a_2, b_0), h(6) = (a_2, b_1), h(7) = (a_2, b_2), h(8) = (a_1, b_2), h(9) = (a_0, b_2)\\
&\quad\vdots\\
&h(n^2+1) = (a_n, b_0), h(n^2+2) = (a_n, b_{n-1}), \dots,\\
&\qquad\qquad h(n^2+n+1) = (a_n, b_n), h(n^2+n+2) = (a_{n-1}, b_n), \dots,\\
&\qquad\qquad h((n+1)^2) = (a_0, b_n)\\
&\quad\vdots
\end{aligned}\tag{1.2}$$

Basically, look at all pairs of integers in the first quadrant (including those on the axes). Thus, we have pairs (a_x, b_y). The above function h starts at $(0, 0)$, and then moves through the first quadrant, hitting each pair once and only once, by going up and over. Draw the picture!

□

Corollary 1.1.13. *Let A_i be countable $\forall i \in \mathbb{N}$. Then for any n, $A_1 \cup \cdots \cup A_n$ and $A_1 \times \cdots \times A_n$ are countable, where the last set is all n-tuples $(a_1, \dots, a_n)$, $a_i \in A_i$. Further, $\cup_{i=0}^{\infty} A_i$ is countable. If each A_i is at most countable, then $\cup_{i=0}^{\infty} A_i$ is at most countable.*

Exercise 1.1.14. *Prove Corollary 1.1.13. Hint: for $\cup_{i=0}^{\infty} A_i$, mimic the proof used to show $A \times B$ is countable.*

As the natural numbers, integers and rationals are countable, by taking each $A_i = \mathbb{N}$, $\mathbb{Z}$ or $\mathbb{Q}$ we immediately obtain

Corollary 1.1.15. *$\mathbb{N}^n$, $\mathbb{Z}^n$ and $\mathbb{Q}^n$ are countable. Hint: proceed by induction. For example write $\mathbb{Q}^{n+1}$ as $\mathbb{Q}^n \times \mathbb{Q}$.*

Exercise 1.1.16. *Prove that there are countably many rationals in the interval* $[0, 1]$.

1.1.3 Algebraic Numbers

Consider a polynomial $f(x)$ with rational coefficients. By multiplying by the least common multiple of the denominators, we can clear the fractions. Thus, without loss of generality it is sufficient to consider polynomials with integer coefficients.

The set of **algebraic numbers**, $\mathcal{A}$, is the set of all $x \in \mathbb{C}$ such that there is a polynomial of finite degree and integer coefficients (depending on x, of course!) such that $f(x) = 0$. The remaining complex numbers are the **transcendentals**.

The set of **algebraic numbers of degree** n, $\mathcal{A}_n$, is the set of all $x \in \mathcal{A}$ such that

1. there exists a polynomial with integer coefficients of degree n such that $f(x) = 0$
2. there is no polynomial g with integer coefficients and degree less than n with $g(x) = 0$.

Thus, $\mathcal{A}_n$ is the subset of algebraic numbers x where for each $x \in \mathcal{A}_n$, the degree of the smallest polynomial f with integer coefficients and $f(x) = 0$ is n.

Exercise 1.1.17. *Show the following are algebraic: any rational number, the square-root of any rational number, the cube-root of any rational number, $r^{\frac{p}{q}}$ where $r, p, q \in \mathbb{Q}$, $i = \sqrt{-1}$, $\sqrt{3\sqrt{2} - 5}$.*

Theorem 1.1.18. *The algebraic numbers are countable.*

Proof. If we show each $\mathcal{A}_n$ is at most countable, then as $\mathcal{A} = \cup_{n=1}^{\infty} \mathcal{A}_n$, by Corollary 1.1.13 $\mathcal{A}$ is at most countable.

Recall the **Fundamental Theorem of Algebra (FTA):** Let $f(x)$ be a polynomial of degree n with complex coefficients. Then $f(x)$ has n (not necessarily distinct) roots. Of course, we will only need a weaker version, namely that the Fundamental Theorem of Algebra holds for polynomials with integer coefficients.

Fix an $n \in \mathbb{N}$. We now show $\mathcal{A}_n$ is at most countable. We can represent every integral polynomial $f(x) = a_n x^n + \cdots + a_0$ by an $(n+1)$-tuple $(a_0, \dots, a_n)$. By Corollary 1.1.15, the set of all $(n+1)$-tuples with integer coefficients ($\mathbb{Z}^{n+1}$) is countable. Thus, there is a bijection from $\mathbb{N}$ to $\mathbb{Z}^{n+1}$, and we can index each $(n+1)$-tuple $a \in \mathbb{Z}^{n+1}$:

$$\{a : a \in \mathbb{Z}^{n+1}\} \ = \ \bigcup_{i=1}^{\infty} \{\alpha_i\}, \tag{1.3}$$

where each $\alpha_i \in \mathbb{Z}^{n+1}$.

For each tuple α_i (or $a \in \mathbb{Z}^{n+1}$), there are n roots. Let R_{α_i} be the roots of the integer polynomial associated to α_i. The roots in R_{α_i} need not be distinct, and the roots may solve an integer polynomial of smaller degree. For example, $f(x) =$

$(x^2-1)^4$ is a degree 8 polynomial. It has two roots, $x=1$ with multiplicity 4 and $x=-1$ with multiplicity 4, and each root is a root of a degree 1 polynomial.

Let $R_n = \{x \in \mathbb{C} : x$ is a root of a degree n polynomial$\}$. One can show that

$$R_n \; = \; \bigcup_{i=1}^{\infty} R_{\alpha_i} \; \supset \; \mathcal{A}_n. \tag{1.4}$$

By Lemma 1.1.13, R_n is countable. Thus, by Lemma 1.1.9, as R_n is at most countable, A_n is at most countable.

Therefore, each $\mathcal{A}_n$ is at most countable, so by Corollary 1.1.13 $\mathcal{A}$ is at most countable. As $\mathcal{A}_1 \supset \mathbb{Q}$ (given $\frac{p}{q} \in \mathbb{Q}$, consider $qx - p = 0$), $\mathcal{A}_1$ is at least countable. As we've shown $\mathcal{A}_1$ is at most countable, this implies $\mathcal{A}_1$ is countable. Thus, $\mathcal{A}$ is countable.

□

Exercise 1.1.19. *Show the full force of the Fundamental Theorem of Algebra is not needed in the above proof; namely, that it is enough that every polynomial have finitely many roots.*

Exercise 1.1.20. *Prove $R_n \supset \mathcal{A}_n$.*

1.1.4 Transcendental Numbers

A set is **uncountable** if there is no bijection between it and the rationals (or the integers, or any countable set). The aim of this paragraph is to prove the following fundamental theorem:

Theorem 1.1.21. *The set of all real numbers is uncountable.*

We first state and prove a lemma.

Lemma 1.1.22. *Let $\mathcal{S}$ be the set of all sequences $(y_i)_{i\in\mathbb{N}}$ with $y_i \in \{0,1\}$. Then $\mathcal{S}$ is uncountable.*

Proof. We proceed by contradiction. Suppose there is a bijection $f : \mathcal{S} \to \mathbb{N}$. It is clear that this is equivalent to giving a list of the elements of $\mathcal{S}$:

$$\begin{array}{rcl} x_1 & = & x_{11}x_{12}x_{13}x_{14}\cdots \\ x_2 & = & x_{21}x_{22}x_{23}x_{24}\cdots \\ x_3 & = & x_{31}x_{32}x_{33}x_{34}\cdots \\ & \vdots & \\ x_n & = & x_{n1}x_{n2}x_{n3}x_{n4}\cdots x_{nn}\cdots \\ & \vdots & \end{array} \tag{1.5}$$

Define an element $\xi = (\xi_i)_{i\in\mathbb{N}} \in \mathcal{S}$ by $\xi_i = x_{ii}$, and another element $\bar{\xi} = (1-\xi_i)_{i\in\mathbb{N}}$. Now the element $\bar{\xi}$ cannot be in the list; it is not x_N because $1-x_{NN} \neq x_{NN}$! □

Proof of the theorem. Consider all those numbers in the interval $[0, 1]$ whose decimal expansion consists entirely of numbers $0, 1$. Clearly, there is a bijection between this subset of $\mathbb{R}$ and the set $\mathcal{S}$. We have established that $\mathcal{S}$ is uncountable. Consequently $\mathbb{R}$ has an uncountable subset. This gives the theorem. □

The above proof is due to Cantor ($1873 - 1874$), and is known as **Cantor's Diagonalization Argument**. Note Cantor's proof shows that *most* numbers are transcendental, though it doesn't tell us *which* numbers are transcendental. We can easily show many numbers (such as $\sqrt{3 + 2^{\frac{3}{5}}\sqrt{7}}$) are algebraic. What of other numbers, such as π and e?

Lambert (1761), Legendre (1794), Hermite (1873) and others proved π irrational. In 1882 Lindemann proved π transcendental.

What about e? Euler (1737) proved that e and e^2 are irrational, Liouville (1844) proved e is not an algebraic number of degree 2, and Hermite (1873) proved e is transcendental.

Liouville (1851) gave a construction for an infinite (in fact uncountable) family of transcendental numbers; we will discuss his construction later.

1.1.5 Continuum Hypothesis

We have shown that there are more transcendental numbers than algebraic numbers. Does there exist a subset of $[0, 1]$ which is strictly larger than the rationals, yet strictly smaller than the transcendentals?

Cantor's Continuum Hypothesis says that there are no subsets of intermediate size.

The standard axioms of set theory are known as the Zermelo-Fraenkel axioms (note to the expert: often the Axiom of Choice is assumed, and we talk of ZF $+$ Choice).

Kurt Gödel showed that if the standard axioms of set theory are consistent, so too are the resulting axioms where the Continuum Hypothesis is assumed true; Paul Cohen showed that the same is true if the negation of the Continuum Hypothesis is assumed.

These two results imply that the Continuum Hypothesis is independent of the other standard assumptions of set theory!

1.2 Properties of e

In this section, we study some of the basic properties of the number e. One of the many ways to define the number e, the base of the natural logarithms, is to write it as the sum of the following infinite series:

$$e = \sum_{n=1}^{\infty} \frac{1}{n!} \tag{1.6}$$

Now, let us denote the partial sums of the above series by

$$s_m = \sum_{n=1}^{m} \frac{1}{n!} \tag{1.7}$$

Hence e is the limit of the convergent sequence s_m. This idea will be the main tool in analyzing the nature of e.

Theorem 1.2.1 (Euler, 1737). *The number e is irrational.*

Proof. Assume that $e \in \mathbb{Q}$. Then we can write $e = \frac{p}{q}$, where p, q are positive integers.

Now,

$$\begin{aligned} e - s_m &= \sum_{n=m+1}^{\infty} \frac{1}{n!} \\ &= \frac{1}{(m+1)!}\left\{1 + \frac{1}{m+1} + \frac{1}{(m+1)(m+2)} + ...\right\} \\ &< \frac{1}{(m+1)!}\left\{1 + \frac{1}{m+1} + \frac{1}{(m+1)^2} + \frac{1}{(m+1)^3} + ...\right\} \\ &= \frac{1}{(m+1)!}\frac{1}{1-\frac{1}{m+1}} = \frac{1}{m!m} \end{aligned} \tag{1.8}$$

Hence we obtain

$$0 < e - s_m < \frac{1}{m!m}. \tag{1.9}$$

In particular, taking $m = q$ we get:

$$\begin{aligned} 0 \ &< \quad e - s_q \quad < \ \frac{1}{q!} \\ 0 \ &< \ q!e - q!s_q \ < \ 1 \end{aligned} \tag{1.10}$$

which is clearly impossible since the left hand side of the last equation, namely $q!e - q!s_q$, would have to be an integer between 0 and 1. This contradicts our assumption that e was rational. □

1.2.1 e is Transcendental

Here we prove the following beautiful fact:

Theorem 1.2.2 (Hermite,1873). *The number e is transcendental.*

Proof. The proof is again by contradiction. Assume that e is algebraic. Then it must satisfy a polynomial equation

$$a_n X^n + ... + a_1 X + a_0 = 0 \tag{1.11}$$

where $a_0, a_1, .., a_n$ are integer numbers, and we can assume without loss of generality that $a_0, a_n \neq 0$.

Now consider a polynomial $f(X)$ of degree r, and associate to it the following linear combination of its derivatives:

$$F(X) = f(X) + f'(X) + ... + f^{(r)}(X) \tag{1.12}$$

Now, the polynomial $F(X)$ has the property that

$$\frac{d}{dx}\left[e^{-x}F(x)\right] = e^{-x}f(x). \tag{1.13}$$

As $F(X)$ is differentiable, applying the Mean Value Theorem to $e^{-x}F(X)$ on the interval $[0,k]$ for k any integer gives

$$e^{-k}F(k) - F(0) = -ke^{-c_k}f(c_k), \quad \text{for some} \quad c_k \in (0,k), \tag{1.14}$$

or, equivalently

$$F(k) - e^kF(0) = -ke^{k-c_k}f(c_k) =: \epsilon_k. \tag{1.15}$$

Now, if we plug in the previous equation the values $k = 0, 1, ..., n$ we get the following system of equations:

$$\begin{aligned}
&F(0) - F(0) = 0 =: \epsilon_0 \\
&F(1) - eF(0) = -e^{1-c_1}f(c_1) =: \epsilon_1 \\
&F(2) - e^2F(0) = -2e^{2-c_2}f(c_2) =: \epsilon_2 \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
&F(n) - e^nF(0) = -ne^{n-c_n}f(c_n) =: \epsilon_n
\end{aligned} \tag{1.16}$$

We multiply the first equation by a_0, the second by $a_1, \ldots$, the $(n+1)^{st}$ by a_n. Adding the resulting equations gives

$$\sum_{k=0}^{n} a_kF(k) - \left(\sum_{k=0}^{n} a_ke^k\right)F(0) = \sum_{k=0}^{n} a_k\epsilon_k. \tag{1.17}$$

Notice that on the left hand side we have exactly the polynomial equation that is satisfied by e:

$$\sum_{k=0}^{n} a_k e^k = 0; \tag{1.18}$$

hence Equation 1.17 reduces to

$$\sum_{k=0}^{n} a_k F(k) = \sum_{k=0}^{n} a_k \epsilon_k. \tag{1.19}$$

So far we had complete freedom in our choice of f, and the previous equation always holds for its associate F. In what follows we choose a special polynomial f in order to reach a contradiction.

Take a large prime p, large enough such that $p > |a_0|$ and $p > n$. Let f equal

$$\begin{aligned} f(X) &= \frac{1}{(p-1)!} X^{p-1}(1-X)^p(2-X)^p \cdots (n-X)^p \\ &= \frac{1}{(p-1)!}\Big((n!)^p X^{p-1} + \text{higher order terms}\Big). \end{aligned} \tag{1.20}$$

Though it plays no role in the proof, we note that the degree of f is

$$\deg(f) := r = (n+1)p - 1. \tag{1.21}$$

In what follows we make a number of remarks which will help us finish the proof. By $p\mathbb{Z}$ we mean the set of integer multiples of p.

Remark 1.2.3. *For* $i \geq p, f^{(i)}(j) \in p\mathbb{Z}, \forall j \in \mathbb{N}$.

Proof. Differentiate Equation 1.20 $i \geq p$ times. The only terms which survive bring down at least a $p!$. As each term of $f(x)$ is an integer over $(p-1)!$, we see that all surviving terms are multiplied by p. □

Remark 1.2.4. *For* $0 \leq i < p, f^{(i)}(j) = 0, j = 1, 2, .., n$.

Proof. The multiplicity of a root of a polynomial gives the order of vanishing of the polynomial at that particular root. As $j = 1, 2, \ldots, n$ are roots of multiplicity p, differentiating $f(x)$ less than p times yields a polynomial which still vanishes at these j. □

Remark 1.2.5. *Let F be the polynomial associated to f. Then $F(1), F(2), \ldots, F(n) \in p\mathbb{Z}$.*

Proof. Recall that $F(j) = f(j) + f'(j) + .. + f^{(r)}(j)$. By the first remark, $f^{(i)}(j)$ is a multiple of p for $i \geq p$ and any integer j. By the second remark, $f^{(i)}(j) = 0$ for $0 \leq i < p$ and $j = 1, 2, \ldots, n$. Thus, $F(j)$ is a multiple of p for these j. □

Remark 1.2.6. *For $0 \leq i \leq p-2$, $f^{(i)}(0) = 0$.*

Proof. Similar to the second remark, we note that $f^{(i)}(0) = 0$ for $0 \leq i < p-2$, because 0 is a root of $f(x)$ of multiplicity $p-1$. □

Remark 1.2.7. *$F(0)$ is not a multiple of p.*

Proof. By the first remark, $f^{(i)}(0)$ is a multiple of p for $i \geq p$; by the fourth remark, $f^{(i)}(0) = 0$ for $0 \leq i \leq p-2$. Since

$$F(0) = f(0) + f'(0) + \cdots + f^{(p-2)}(0) + f^{(p-1)}(0) + f^{(p)}(0) + \cdots + f^{(r)}(0), \quad (1.22)$$

to prove $F(0)$ is a not multiple of p it is sufficient to prove $f^{(p-1)}(0)$ is not multiple of p (as all other terms *are* multiples of p).

However, from the Taylor Series expansion of f in Equation 1.20, we see that

$$f^{(p-1)}(0) \;=\; (n!)^p \;+\; \Big(\text{terms that are multiples of } p\Big). \quad (1.23)$$

Since we chose $p > n$, $n!$ is not divisible by p, proving the remark. □

We resume the proof of the transcendence of e.

We also chose p such that a_0 is not divisible by p. This fact plus the above remarks imply first that $\sum_k a_k F(k)$ is an integer, and second that

$$\sum_{k=0}^{n} a_k F(k) \equiv a_0 F(0) \not\equiv 0 \bmod p. \quad (1.24)$$

Thus, $\sum_k a_k F(k)$ is a non-zero integer.

Let us recall equation 1.19:

$$\sum_{k=0}^{n} a_k F(k) = a_1 \epsilon_1 + \cdots + a_n \epsilon_n. \quad (1.25)$$

We have already proved that the left hand side is a non-zero integer. We analyze the sum on the right hand side. We have

$$\epsilon_k = -ke^{k-c_k} f(c_k) = \frac{-ke^{k-c_k} c_k^{p-1}(1-c_k)^p \cdots (n-c_k)^p}{(p-1)1}. \tag{1.26}$$

As $0 \leq c_k \leq k \leq n$ we obtain

$$\begin{aligned} |\epsilon_k| &\leq \frac{e^k k^p (1 \cdot 2 \cdots n)^p}{(p-1)!} \\ &\leq \frac{e^n (n!n)^p}{(p-1)!} \to 0 \quad \text{as} \quad p \to \infty. \end{aligned} \tag{1.27}$$

Now recall that n is fixed, and so are the constants $a_0, \ldots, a_n$ (they define the polynomial equation supposedly satisfied by e), and the only thing that varies in our argument is the prime number p. Hence, by choosing a prime number p large enough, we can make sure that all ϵ_k's are uniformly small, in particular we can make them small enough such that the following holds:

$$\left| \sum_{k=1}^{n} a_k \epsilon_k \right| < 1 \tag{1.28}$$

To be more precise, we only have to choose p such that $p > n, |a_0|$ and:

$$\frac{e^n (n!n)^p}{(p-1)!} < \frac{1}{\sum_{k=0}^{n} |a_k|} \tag{1.29}$$

In this way we reach a contradiction in the identity 1.19 where the left hand side is a non-zero integer, while the right hand side is a real number of absolute value < 1. □

Exercise 1.2.8. *In the above proof, we assumed $a_0, a_n \neq 0$. Prove that if a non-zero number is algebraic, one can always find a polynomial such that the leading term and the constant term are both non-zero.*

Exercise 1.2.9. *For fixed n, prove that as $p \to \infty$, $\frac{(n!n)^p}{(p-1)!} \to 0$. Hint: Let $C = n!n$. Choose $p > 2(2C)^4$. Then $(p-1)! > (p-1)(p-2) \cdots (p - \frac{p}{2}) \approx (\frac{p}{2})^{\frac{p}{2}}$. Substitute and compare.*

1.3 Properties of Algebraic Numbers

Let α and β be two algebraic numbers. Is their sum algebraic? Is their product? What about a general linear combination? What if both are transcendental?

1.3.1 Symmetric Polynomials

Consider the set $\{1, \dots, n\}$. There are $n!$ ways to permute the n elements (where order counts). Let σ denote one of these permutations. Thus, $\{\sigma(1), \dots, \sigma(n)\}$ is the same set as $\{1, \dots, n\}$, with the elements (possibly) in a different order. Let the group of permutations of $\{1, \dots, n\}$ be denoted S_n, where the product of two permutations is given by composition.

Definition 1.3.1 (Symmetric Functions). *Let $f : \mathbb{R}^n \to \mathbb{C}$ and let σ be any permutation of the set $\{1, \dots, n\}$. Then f is symmetric if for any permutation $\sigma \in S_n$,*

$$f(x_1, x_2, \dots, x_{n-1}, x_n) \ = \ f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n-1)}, x_{\sigma(n)}). \tag{1.30}$$

For $n = 2$, there are two possible permutations, and we have

$$f(x_1, x_2) \ = \ f(x_2, x_1). \tag{1.31}$$

For $n = 3$, there are six possible permutations, and we have

$$f(x_1, x_2, x_3) = f(x_1, x_3, x_2) = f(x_2, x_1, x_3) = f(x_2, x_3, x_1) = f(x_3, x_1, x_2) = f(x_3, x_2, x_1). \tag{1.32}$$

Example 1.3.2. *For example, $f(x_1, x_2) = x_1 x_2$ or $\frac{x_1}{x_2} + \frac{x_2}{x_1}$ or $x_1^2 + x_2^2$ are symmetric, but $f(x_1, x_2) = x_1^2 x_2$ is not.*

If we have $n = 2$, we often denote the variables by x and y instead of x_1 and x_2.

In two variables, there are two basic symmetric polynomials:

1. $\sigma_1 = \sigma_1(x, y) = x + y$.
2. $\sigma_2 = \sigma_2(x, y) = xy$.

Theorem 1.3.3. *Let $f(x, y)$ be a symmetric polynomial in two variables. Then $f(x, y)$ can be expressed in terms of σ_1 and σ_2.*

For example,

$$\begin{aligned} x^2 + y^2 &= \sigma_1^2(x, y) - 2\sigma_2(x, y) \\ yx^4 + xy^4 &= \sigma_2(x, y) \cdot \left(\sigma_1^3(x, y) - 3\sigma_1(x, y)\sigma_2(x, y)\right). \end{aligned} \tag{1.33}$$

1.3.2 Needed Lemmas

Definition 1.3.4 (Zero Polynomial). *A polynomial f is the zero polynomial if it has no non-zero terms. In other words, if f is a function of $x_1, \dots, x_n$, it contains no monomials $Cx_1^{r_1} \cdots x_n^{r_n}$.*

Lemma 1.3.5. *Let $f(x, y)$ be a polynomial with at least one non-zero term. Then $f(x, y)$ is not identically zero. Equivalently, if $f(x, y) = 0$ for all complex x and y, $f(x, y)$ is the zero polynomial.*

FROM REVIEWER: FOR ANY INFINITE FIELD K, AN ELEMENT OF K(X1,...,XN) IS IDENTICALLY ZERO IF IT ONLY TAKES ZERO VALUES. BY INDUCTION IT'S ENOUGH TO PROVE FOR N=1, WHICH IS OBVIOUS.

Proof. Without loss of generality, we can assume there is at least one term containing a power of x, say x^a. We collect terms where x has the same degree, and write $f(x, y)$ as

$$f(x, y) = \sum_{i=0}^{n} g_i(y)x^i, \tag{1.34}$$

where each $g_i(y)$ is a polynomial in y of finite degree (not necessarily the same degree for each i). Clearly, $g_a(y)$ is not the zero polynomial (if it were, it would contradict our assumption that we have a term x^a).

By the Fundamental Theorem of Algebra, a polynomial in one variable with complex coefficients of degree m has at most m roots. Thus, there are only finitely many y such that $g_a(y) = 0$. Choose y_0 such that $g_a(y_0) \neq 0$. Then

$$F(x) = f(x, y_0) = \sum_{i=0}^{n} g(y_0)x^i \tag{1.35}$$

is not the zero polynomial, as $g_a(y_0) \neq 0$. Therefore, $F(x)$ is a finite polynomial of degree at least a. By the Fundamental Theorem of Algebra, $F(x)$ equals zero at most finitely often; therefore, $F(x)$ is not identically zero, which implies $f(x, y)$ is not identically zero.

□

Lemma 1.3.6. *Let $f(x_1, \dots, x_n)$ have at least one non-zero term. Then $f(x_1, \dots, x_n)$ is not the zero polynomial. Equivalently, if $f(x_1, \dots, x_n) = 0$ for all $(x_1, \dots, x_n)$, then f is the zero polynomial.*

The proof is by induction. The Fundamental Theorem of Algebra does the case where we have just one variable; we did two variables above. The general case is handled similarly. Briefly, we may assume without loss of generality that there is a term containing a power of x_1, say x_1^a. We may write

$$f(x_1, \dots, x_n) \ = \ \sum_{i=0}^{N} g_i(x_2, \dots, x_n) x_1^i. \tag{1.36}$$

$g_a(x_2, \dots, x_n)$ is not the zero polynomial (otherwise we would not have an x^a; by the inductive assumption (since g_a is a function of $n-1$ instead of n variables), there is a tuple $(x_{20}, \dots, x_{n0})$ such that $g_a(x_{20}, \dots, x_{n0}) \neq 0$.

We form

$$F(x) \ = \ f(x_1, x_{20}, \dots, x_{n0}) \ = \ \sum_{i=0}^{N} g_i(x_{20}, \dots, x_{n0}) x^i. \tag{1.37}$$

The rest of the proof is as before. □

Lemma 1.3.7. *If a symmetric polynomial contains a term $Cx^a y^b$, then it must contain the term $Cx^b y^a$.*

Clearly, we only need to check when $a \neq b$.

Assume $f(x, y)$ is symmetric, so $f(x, y) = f(y, x)$. Assume for some a and b, $Cx^a y^b$ occurs in $f(x, y)$ but $Cx^b y^a$ does not. Then $Cx^b y^a$ occurs in $f(y, x)$ but $Cx^a y^b$ does not.

Hence, if we look at $f(x, y) - f(y, x)$, we see the term $Cx^a y^b - Cx^b y^a$ occurs. Hence, $f(x, y) - f(y, x)$ is *not* the zero polynomial.

By Lemma 1.3.5, $f(x, y) - f(y, x)$ cannot be identically zero, which contradicts $f(x, y) = f(y, x)$ (as we assumed f was symmetric). □

Remark 1.3.8. *One could have defined symmetric polynomials slightly differently. Namely, we could say a polynomial $f(x,y)$ is symmetric if whenever f contains a term Cx^ay^b, it contains a term Cx^by^a. For polynomials with variables in $\mathbb{C}$, the two definitions are equivalent. Consider, however, the following:*

$$f(x,y) \;=\; e^{\frac{2\pi i y(x^3+1)}{3}} + e^{\frac{2\pi i x(y+1)^3}{3}},\; x,y \in \mathbb{Z}. \tag{1.38}$$

Then $f(x,y) = f(y,x)$ for all $x, y \in \mathbb{Z}$, but the two terms look different.

1.3.3 Proof of Theorem 1.3.3

The following is due to Newton. We proceed by induction on the number of terms of the symmetric polynomial f.

By Lemma 1.3.7, if a symmetric polynomial contains a term Cx^ay^b, then it must contain the term Cx^by^a.

Thus, the polynomial must contain $Cx^ay^b + Cx^by^a$; if we subtract this expression from the original polynomial, the remaining polynomial will still be symmetric, and it will have fewer terms.

Thus, it is sufficient to prove that we can express $x^ay^b + x^by^a$ in terms of $\sigma_1(x,y)$ and $\sigma_2(x,y)$.

Suppose $a > b$. Then

$$\begin{aligned} x^ay^b + x^by^a &= x^by^b(x^{a-b} + y^{a-b}) \\ &= \sigma_2(x,y)^b(x^{a-b} + y^{a-b}). \end{aligned} \tag{1.39}$$

Thus, to complete the proof, it suffices to show

Lemma 1.3.9. *Any polynomial $x^n + y^n$ can be expressed in terms of $\sigma_1(x,y)$ and $\sigma_2(x,y)$.*

We proceed by induction; the basis step $n = 1$ is clear. We also note that for $n = 2$, $x^2 + y^2 = \sigma_1(x,y)^2 - 2\sigma_2(x,y)$.

Look at

$$\begin{aligned} (X-x)(X-y) &= X^2 - (x+y)X + xy \\ &= X^2 - \sigma_1(x,y)X + \sigma_2(x,y). \end{aligned} \tag{1.40}$$

Setting $X = x$ gives

$$0 \;=\; x^2 - \sigma_1(x,y)x + \sigma_2(x,y). \tag{1.41}$$

Therefore, we find

$$x^2 \;=\; \sigma_1(x,y)x - \sigma_2(x,y). \tag{1.42}$$

Multiplying by x^n yields

$$\begin{aligned} x^{n+2} &= \sigma_1(x,y)x^{n+1} - \sigma_2(x,y)x^n \\ y^{n+2} &= \sigma_1(x,y)y^{n+1} - \sigma_2(x,y)y^n, \end{aligned} \tag{1.43}$$

where the second line follows from the symmetry of x and y (we can apply same type of argument with x replaced with y, as $\sigma_i(x,y) = \sigma_i(y,x)$). Adding the two equations above yields

$$x^{n+2} + y^{n+2} \;=\; \sigma_1(x,y)\left(x^{n+1} + y^{n+1}\right) - \sigma_2(x,y)(x^n + y^n). \tag{1.44}$$

By induction, we are done. Note that it was important to verify for $n = 1$ *and* $n = 2$.

1.3.4 Theory for More Variables

There is a theory of symmetric polynomials in any number of variables.

The basic symmetric functions in three variables are

1. $\sigma_1 = x + y + z$;
2. $\sigma_2 = xy + xz + yz$;
3. $\sigma_3 = xyz$;

in four variables, the basic symmetric functions are

1. $\sigma_1 = x + y + z + t$;
2. $\sigma_2 = xy + xz + xt + yz + yt + zt$;
3. $\sigma_3 = yzt + xzt + xyt + xyz$;

4. $\sigma_4 = xyzt$.

The main result, which we will not prove, is

Theorem 1.3.10 (Newton). *For each n, there are n basic symmetric functions $\sigma_1, \ldots, \sigma_n$ such that any symmetric polynomial P can be expressed in terms of σ_1 through σ_n. Furthermore, if P has rational coefficients, the expression of P in terms in the σ_i will have rational coefficients.*

FROM REVIEWER: UTE PROOF OF THIS USING GALOIS THEORY – SEE E. ARTIN'S GALOIS THEORY

1.3.5 Applications

The formula

$$\begin{aligned}(X-x)(X-y) &= X^2-(x+y)X+xy \\ &= X^2-\sigma_1(x,y)X+\sigma_2(x,y), \end{aligned} \qquad (1.45)$$

generalizes to

$$(X-x_1)\cdots(X-x_n) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n X^0. \qquad (1.46)$$

If we have any polynomial with coefficients in $\mathbb{C}$, it factors over $\mathbb{C}$ into a product of linear factors (the Fundamental Theorem of Algebra).

Thus, if we take a polynomial with rational coefficients,

$$a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 = a_n(X-\alpha_1)\cdots(X-\alpha_n), \qquad (1.47)$$

where the $\alpha_i \in \mathbb{C}$. A simple comparison combined with Newton's theorem implies

Lemma 1.3.11. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the solutions of an algebraic equation of degree n with rational coefficients. Then every symmetric polynomial expression with rational coefficients in terms of the α_i will be a rational number.*

This lemma has a number of interesting consequences.

Proposition 1.3.12. *If α and β are two algebraic numbers, then $\alpha + \beta$, $\alpha\beta$, and α/β will be algebraic numbers.*

Proof. We will prove this for $\alpha + \beta$; the others are similar. Let $\alpha_1, \ldots, \alpha_m$ ($\beta_1, \ldots, \beta_m$, resp.) be all the roots of the algebraic equation satisfied by α (β, resp.). Consider the polynomial

$$\prod_{1\leq i\leq n} \prod_{1\leq j\leq m} (x - \alpha_i - \beta_j).$$

It is clear that $(x-\alpha-\beta)|P(x)$. So our result will follow if we can show that $P(x)$ has rational coefficients. The coefficients of $P(x)$ are polynomials with integral coefficients in terms of the α_i and the β_j. Also they are separately symmetric in each set of the variables. The lemma then gives the result. □

Exercise 1.3.13. *Complete the details of the proof.*

Proposition 1.3.14. *A number that satisfies an equation with algebraic coefficients (not necessarily rational) is algebraic.*

Proof. Suppose our equation is

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

and suppose α is a solution of this equation. We will find an equation with integral coefficients that has α as a root. For this we proceed as follows. Take a typical coefficient of the above equation, say a_i. Since a_i is algebraic it will be the solution of an equation

$$b(i)_{m_i} x^{m_i} + b(i)_{m_i-1} x^{m_i-1} + \cdots + b(i)_1 x^1 + b(i)_0 = 0,$$

with $b(i)_j$'s rational. Let $c(i)_1, c(i)_2, \ldots, c(i)_{m_i}$ be all the roots of this equation. Notice that by definition a_i is one of the $c(i)_j$'s. Next we consider the product

$$\prod_{k=0}^{n} \prod_{1\leq j_k\leq m_k} \Big(c(n)_{j_n} x^n + c(n-1)_{j_{n-1}} x^{n-1} + \cdots + c(1)_{j_1} x + c(0)_{j_0} \Big).$$

This is an equation which has α as a solution. Also it has rational coefficients! This proves the claim. □

Exercise 1.3.15. *Fill in the missing steps.*

Remark 1.3.16. *The last two propositions imply that the set of algebraic numbers is an algebraically closed field.*

REVIEWER: PROBABLY WANT TO MENTION RESULTS ON ALGEBRAIC INTEGERS

Chapter 2

Liouville's Theorem Constructing Transcendentals

2.1 Review of Approximating by Rationals

Definition 2.1.1 (Approximated by rationals to order n). *A real number x is approximated by rationals to order n if there exist a constant $k(x)$ (possibly depending on x) such that there are infinitely many rational $\frac{p}{q}$ with*

$$\left|x - \frac{p}{q}\right| < \frac{k(x)}{q^n}. \tag{2.1}$$

Recall that Dirichlet's Box Principle gives us, for $\alpha \notin \mathbb{Q}$,

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^2} \tag{2.2}$$

for infinitely many fractions $\frac{p}{q}$. This was proved by choosing a large parameter Q, and considering the $Q+1$ fractionary parts $\{qx\} \in [0,1)$ for $q \in \{0,\dots,Q\}$. The box principle ensures us that there must be two different q's, say:

$$0 \le q_1 < q_2 \le Q \tag{2.3}$$

such that both $\{q_1 x\}$ and $\{q_2 x\}$ belong to the same interval $[\frac{a}{Q}, \frac{a+1}{Q})$, for some $0 \le a \le Q-1$. Note that there are exactly Q such intervals partitioning $[0,1)$, and $Q+1$ fractionary parts! Now, the length of such an interval is $\frac{1}{Q}$ so we get

$$|\{q_2 x\} - \{q_1 x\}| < \frac{1}{Q}. \tag{2.4}$$

There exist integers p_1 and p_2 such that

$$\{q_1 x\} = q_1 x - p,\ \{q_2 x\} = q_2 x - p. \tag{2.5}$$

Letting $p = p_2 - p_1$ we find

$$|(q_2 - q_1)x - p| \leq \frac{1}{Q} \tag{2.6}$$

Let $q = q_2 - q_1$, so $1 \leq q \leq Q$, and the previous equation can be rewritten as

$$\left| x - \frac{p}{q} \right| < \frac{1}{qQ} \leq \frac{1}{q^2} \tag{2.7}$$

Now, letting $Q \to \infty$, we get an infinite collection of rational fractions $\frac{p}{q}$ satisfying the above equation. If this collection contains only finitely many distinct fractions, then one of these fractions, say $\frac{p_0}{q_0}$, would occur for infinitely many choices Q_k of Q, thus giving us:

$$\left| x - \frac{p_0}{q_0} \right| < \frac{1}{qQ_k} \to 0, \tag{2.8}$$

as $k \to \infty$. This implies that $x = \frac{p_0}{q_0} \in \mathbb{Q}$. So, unless x is a rational number, we can find infinitely many *distinct* rational numbers $\frac{p}{q}$ satisfying Equation 2.7. This means that any real, irrational number can be approximated to order $n = 2$ by rational numbers.

2.2 Liouville's Theorem

Theorem 2.2.1 (Liouville's Theorem). *Let x be a real algebraic number of degree n. Then x is approximated by rationals to order at most n.*

Proof. Let

$$f(X) \ = \ a_n X^n + \cdots a_1 X + a_0 \tag{2.9}$$

be the polynomial with coprime integer coefficients of smallest degree (minimal polynomial) such that x satisfies

$$f(x) \;=\; 0. \tag{2.10}$$

Note that $\deg x = \deg f$ and the condition of minimality implies that $f(X)$ is irreducible over $\mathbb{Z}$. Further, a well known result from algebra states that a polynomial irreducible over $\mathbb{Z}$ is also irreducible over $\mathbb{Q}$.

Remark 2.2.2. ***FROM REVIEWER: LET** $f_1(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_n \in \mathbb{Q}[x]$**. Then it is irreducible over** $\mathbb{Q}$ **with no rational roots. Clear the denominators to get** f**.***

In particular, as $f(X)$ is irreducible over $\mathbb{Q}$, $f(X)$ does not have any rational roots. If it did, then $f(X)$ would be divisible by a linear polynomial $(X - \frac{a}{b})$. Let $G(X) = \frac{f(X)}{X - \frac{a}{b}}$. Clear denominators (multiply throughout by b), and let $g(X) = bG(X)$. Then $\deg g = \deg f - 1$, and $g(x) = 0$. This contradicts the minimality of f (we choose f to be a polynomial of smallest degree such that $f(x) = 0$). Therefore, f is non-zero at every rational.

Let

$$M \;=\; \sup_{|z-x|<1} |f'(z)|. \tag{2.11}$$

Let now $\frac{p}{q}$ be a rational such that $\left|x - \frac{p}{q}\right| < 1$. The Mean Value Theorem **GIVE REF** gives us that

$$\left| f\left(\frac{p}{q}\right) - f(x) \right| = \left| f'(c)\left(x - \frac{p}{q}\right) \right| \leq M \left| x - \frac{p}{q} \right| \tag{2.12}$$

where c is some real number between x and $\frac{p}{q}$; $|c - x| < 1$ for $\frac{p}{q}$ moderately close to x.

Now we use the fact that $f(X)$ does not have any rational roots:

$$0 \neq f\left(\frac{p}{q}\right) = a_n \left(\frac{p}{q}\right)^n + \cdots + a_0 = \frac{a_n p^n + \cdots a_1 p^{n-1} q + a_0 q^n}{q^n} \tag{2.13}$$

The numerator of the last term is a nonzero integer, hence it has absolute value at least 1. Since we also know that $f(x) = 0$ it follows that

$$\left| f\left(\frac{p}{q}\right) - f(x) \right| = \left| f\left(\frac{p}{q}\right) \right| = \frac{|a_n p^n + \cdots a_1 p^{n-1} q + a_0 q^n|}{q^n} \geq \frac{1}{q^n}. \tag{2.14}$$

Combining the equations 2.12 and 2.14, we get:

$$\frac{1}{q^n} \leq M\left|x-\frac{p}{q}\right| \;\Rightarrow\; \frac{1}{Mq^n} \leq \left|x-\frac{p}{q}\right| \tag{2.15}$$

whenever $|x-\frac{p}{q}|<1$. This last equation shows us that x can be approximated by rationals to order at most n. For assume it was otherwise, namely that x can be approximated to order $n+\epsilon$. Then we would have an infinite sequence of distinct rational numbers $\{\frac{p_i}{q_i}\}_{i\geq 1}$ and a constant $k(x)$ depending only on x such that

$$\left|x-\frac{p_i}{q_i}\right| \;<\; \frac{k(x)}{q_i^{n+\epsilon}}. \tag{2.16}$$

Since the numbers $\frac{p_i}{q_i}$ converge to x we can assume that they already are in the interval $(x-1,x+1)$. Hence they also satisfy Equation 2.15:

$$\frac{1}{q_i^n} \leq M\left|x-\frac{p_i}{q_i}\right|. \tag{2.17}$$

Combining the last two equations we get

$$\frac{1}{Mq_i^n} \leq \left|x-\frac{p_i}{q_i}\right| \;<\; \frac{k(x)}{q_i^{n+\epsilon}}, \tag{2.18}$$

hence

$$q_i^\epsilon \;<\; Mk(x) \tag{2.19}$$

and this is clearly impossible for arbitrarily large q since $\epsilon>0$ and $q_i\to\infty$.

□

Exercise 2.2.3. *Justify the fact that if $\{\frac{p_i}{q_i}\}_{i\geq 1}$ is a sequence of rational approximations to order $n\geq 1$ of x, then $q_i\to\infty$.*

Remark 2.2.4. *So far we have seen that the order to which an algebraic number can be approximated by rationals is bounded by its degree. Hence if a real, irrational number $\alpha\notin\mathbb{Q}$ can be approximated by rationals to an arbitrary large order, then α must be transcendental! This provides us with a recipe for constructing transcendental numbers.*

2.3 Constructing Transcendental Numbers

2.3.1 $\sum_m 10^{-m!}$

The following construction of transcendental numbers is due to Liouville.

Theorem 2.3.1. *The number*

$$x = \sum_{m=1}^{\infty} \frac{1}{10^{m!}} \tag{2.20}$$

is transcendental.

Proof. The series defining x is convergent, since it is dominated by the geometric series $\sum \frac{1}{10^m}$. In fact, the series converges very rapidly and it is this high rate of convergence that will yield x is transcendental.

Fix N large, and let $n > N$. Write

$$\frac{p_n}{q_n} = \sum_{m=1}^{n} \frac{1}{10^{m!}} \tag{2.21}$$

with $p_n, q_n > 0$ and $(p_n, q_n) = 1$. Then $\{\frac{p_n}{q_n}\}_{n \geq 1}$ is a monotone increasing sequence converging to x. In particular, all these rational numbers are distinct. Not also that q_n must divide $10^{n!}$, which implies

$$q_n \leq 10^{n!}. \tag{2.22}$$

Using this, we get

$$\begin{aligned} 0 < x - \frac{p_n}{q_n} &= \sum_{m>n} \frac{1}{10^{m!}} = \frac{1}{10^{(n+1)!}} \left(1 + \frac{1}{10^{n+2}} + \frac{1}{10^{(n+2)(n+3)}} + \cdots \right) \\ &< \frac{2}{10^{(n+1)!}} = \frac{2}{(10^{n!})^{n+1}} \\ &< \frac{2}{q_n^{n+1}} \leq \frac{2}{q_n^N}. \end{aligned} \tag{2.23}$$

This gives an approximation by rationals of order N of x. Since N can be chosen arbitrarily large, this implies that x can be approximated by rationals to arbitrary order. We can conclude, in view of our previous remark 2.2.4, that x is transcendental. □

2.3.2 $[10^{1!}, 10^{2!}, \dots]$

Theorem 2.3.2. *The number*

$$y = [10^{1!}, 10^{2!}, \dots] \tag{2.24}$$

is transcendental.

Proof. Let $\frac{p_n}{q_n}$ be the continued fraction of $[10^{1!} \cdots 10^{n!}]$. Then

$$\begin{aligned} \left| y - \frac{p_n}{q_n} \right| &= \frac{1}{q_n q'_{n+1}} = \frac{1}{q_n(a'_{n+1}q_n + q_{n-1})} \\ &< \frac{1}{a_{n+1}} = \frac{1}{10^{(n+1)!}}. \end{aligned} \tag{2.25}$$

Since $q_k = a_n q_{k-1} + q_{n-2}$, it implies that $q_k > q_{k-1}$ Also, $q_{k+1} = a_{k+1}q_n + q_{k-1}$, so we get

$$\frac{q_{k+1}}{q_k} = a_{k+1} + \frac{q_{k-1}}{q_k} < a_{k+1} + 1. \tag{2.26}$$

Hence writing this inequality for $k = 1, \cdots, n-1$ we obtain

$$\begin{aligned} q_n = q_1 \frac{q_2}{q_1} \frac{q_3}{q_2} \cdots \frac{q_n}{q_{n-1}} &< (a_1 + 1)(a_2 + 1) \cdots (a_n + 1) \\ &= (1 + \frac{1}{a_1}) \cdots (1 + \frac{1}{a_n}) a_1 \cdots a_n \\ &< 2^n a_1 \cdots a_n = 2^n 10^{1! + \cdots + n!} \\ &< 10^{2n!} = a_n^2 \end{aligned} \tag{2.27}$$

Combining equations 2.25 and 2.27 we get:

$$\begin{aligned} \left| y - \frac{p_n}{q_n} \right| &< \frac{1}{a_{n+1}} = \frac{1}{a_n^{n+1}} \\ &< \left(\frac{1}{a_n^2} \right)^{\frac{n}{2}} < \left(\frac{1}{q_n^2} \right)^{\frac{n}{2}} \\ &= \frac{1}{q_n^{n/2}}. \end{aligned} \tag{2.28}$$

In this way we get, just as in the previous theorem, an approximation of y by rationals to arbitrary order. This proves that y is transcendental.

$\square$

Bibliography

[AKS] R. Adler, M. Keane, and M. Smorodinsky, *A construction of a normal number for the continued fraction transformation*, J. Number Theory **13** (1981), no. 1, 95–105.

[BS] Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press.

[BFFMPW] T. Brody, J. Flores, J. French, P. Mello, A. Pandey, S. Wong, *Random-matrix physics: spectrum and strength fluctuations*, Rev. Mod. Phys. vol. **53**, no. 3, July 1981, $385 - 479$.

[CGI] G. Casati, I. Guarneri, and F. M. Izrailev, *Statistical Properties of the Quasi-Energy Spectrum of a Simple Integrable System*, Phys. Lett. A 124 (1987), $263 - 266$.

[Ca] J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge University Press, London 1957.

[CW] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnterton-Dyer*, Invent. Math. **39**, 1977, $43 - 67$.

[CFKRS] B. Conrey, D. Farmer, P. Keating, M. Rubinstein and N. Snaith, *Integral Moments of L-Functions*, http://arxiv.org/pdf/math.NT/0206018

[Da1] H. Davenport, *The Higher Arithmetic*.

[Da2] H. Davenport, *Multiplicative Number Theory, 2nd edition*, Graduate Texts in Mathematics **74**, Springer-Verlag, New York, 1980, revised by H. Montgomery.

[Fe] W. Feller, *An Introduction to Probability Theory and its Applications*, Vol. II. Second edition. John Wiley & Sons, Inc., New York-London-Sydney 1971.

[GT] A. Granville and T. Tucker, *It's as easy as abc*, Notices of the AMS, volume 49, number 10 (November 2002).

[HL1] G. Hardy and J. Littlewood, *A new solution of Waring's Problem,* Q. J. Math. 48: $272-293$, 1919.

[HL2] G. Hardy and J. Littlewood, *Some problems of "Partitio Numerorum". A new solution of Waring's problem,* Göttingen Nach., $33-54$, 1920.

[HL3] G. Hardy and J. Littlewood,

[HL4] G. Hardy and J. Littlewood,

[HW] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers,* fifth edition, Oxford Science Publications, Clarendon Press, Oxford, 1995.

[HR] G. Hardy and S. Ramanujan, *Asymptotic formulae in combinatorial analysis*, Proc. London Math. Soc. 17: $75-115$, 1918.

[Hej] D. Hejhal, *On the triple correlation of zeros of the zeta function*, Internat. Math. Res. Notices 1994, no. 7, $294-302$.

[HS] M. Hindry and J. Silverman, *Diophantine geometry: An introduction*, Graduate Texts in Mathematics, vol. 201, Springer, New York, 2000.

[Iw] H. Iwaniec, *Topics in Classical Automorphic Forms*, American Mathematical Society, Graduate Studies in Mathematics, vol. **17**, Providence, 1997.

[ILS] H. Iwaniec, W. Luo and P. Sarnak, *Low lying zeros of families of L-functions,* Inst. Hautes Études Sci. Publ. Math. **91**, 2000, $55-131$.

[JMRR] D. Jakobson, S. D. Miller, I. Rivin and Z. Rudnick, *Eigenvalue spacings for regular graphs*, Emerging applications of number theory (Minneapolis, MN, 1996), $317-327$.

[KS1] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Colloquium Publications **45**, AMS, Providence, 1999.

[KS2] N. Katz and P. Sarnak, *Zeros of zeta functions and symmetries*, Bull. AMS **36**, 1999, $1-26$.

[Kh] A. Y. Khinchin, *Continued Fractions*, Third Edition, The University of Chicago Press, Chicago 1964.

[Ko] V. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, $429-436$.

[Ku] R. Kuzmin, *Ob odnoi zadache Gaussa*, Doklady akad. nauk, ser A, 1928, $375-380$.

[La1] S. Lang, *Introduction to Diophantine Approximations*, Addison-Wesley, Reading, 1966.

[La2] S. Lang, *Undergraduate Algebra*, Springer-Verlag.

[LT] S. Lang and H. Trotter, *Continued fractions for some algebraic numbers*, J. Reine Angew. Math. **255**, 1972, $112-134$.

[Le] P. L$\acute{e}$vy, *Sur les lois de probabilit$\acute{e}$ dont dependent les quotients complets et incomplets d'une fraction continue*, Bull. Soc. Math., **57**, 1929, $178-194$.

[Mai] K. Mainzer, *Natural Numbers, Integers, and Rational Numbers*, Numbers, pp. 9-26.

[McK] B. McKay, *The expected eigenvalue distribution of a large regular graph*, Linear Algebra Appl. 40 (1981), $203-216$.

[Meh] M. Mehta, *Random Matrices,* 2*nd edition*, Academic Press Inc., Boston, 1991.

[Mil] S. J. Miller, 1- *and* 2-*Level Densities for Families of Elliptic Curves: Evidence for the Underlying Group Symmetries*, P.H.D. Thesis, Princeton University, 2002, http://www.math.princeton.edu/$\sim$sjmiller/thesis/thesis.pdf.

[Mon] H. Montgomery, *The pair correlation of zeros of the zeta function*, Analytic Number Theory, Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence, 1973, $181-193$.

[Na] M. Nathanson, *Additive Number Theory: The Classical Bases*, Springer-Verlag, Graduate Texts in Mathematics, 1996.‘

[Od1] A. Odlyzko, *On the distribution of spacings between zeros of the zeta function*, Math. Comp. **48**, 1987, no. 177, $273-308$.

[Od2] A. Odlyzko, *The* 10^{22}*-nd zero of the Riemann zeta function*, Proc. Conference on Dynamical, Spectral and Arithmetic Zeta-Functions, M. van Frankenhuysen and M. L. Lapidus, eds., Amer. Math. Soc., Contemporary Math. series, 2001, http://www.research.att.com/$\sim$amo/doc/zeta.html

[Po] C. Porter (editor), Statistical Theories of Spectra: Fluctuations, Academic Press, 1965.

[Ro] K. Roth, *Rational approximations to algebraic numbers*, Mathematika 2, 1955, $1-20$.

[Ru] M. Rubinstein, *Evidence for a spectral interpretation of the zeros of* L*-functions*, P.H.D. Thesis, Princeton University, 1998, http://www.ma.utexas.edu/users/miker/thesis/thesis.html.

[Rud] W. Rudin, *Principles of Mathematical Analysis*, third edition, International Series in Pure and Applied Mathematics, McGraw-Hill Inc., New York, 1976.

[RS] Z. Rudnick and P. Sarnak, *Zeros of principal* L*-functions and random matrix theory*, Duke Journal of Math. **81**, 1996, $269-322$.

[RSZ] Z. Rudnick, P. Sarnak, and A. Zaharescu, *The Distribution of Spacings Between the Fractional Parts of* $n^2\alpha$, Invent. Math. 145 (2001), no. 1, $37-57$.

[Vin1] I. Vinogradov, *Representation of an odd number as the sum of three primes*, Doklady Akad. Nauk SSSR, $15(6-7)$: $291-294$, 1937.

[Vin2] I. Vinogradov, *Some theorems concerning the theory of primes*, Mat. Sbornik, $2(44)$: $179-195$, 1937.

[Wig1] E. Wigner, *On the statistical distribution of the widths and spacings of nuclear resonance levels*, Proc. Cambridge Philo. Soc. **47**, 1951, $790-798$.

[Wig2] E. Wigner, *Statistical Properties of real symmetric matrices*, Canadian Mathematical Congress Proceedings, University of Toronto Press, Toronto, 1957, $174-184$.

[Wo] T. Wooley, *Large improvements in Waring's problem*, Ann. Math., 135, $131-164$.