ALGEBRAIC AND TRANSCENDENTAL NUMBERS

FROM *AN INVITATION TO MODERN NUMBER THEORY*

STEVEN J. MILLER AND
RAMIN TAKLOO-BIGHASH

CONTENTS

1. INTRODUCTION

These notes are from *An Invitation to Modern Number Theory*, by Steven J. Miller and Ramin Takloo-Bighash (Princeton University Press, 2006). PLEASE DO NOT DISTRIBUTE THESE NOTES FURTHER. As this is an excerpt from the book, there are many references to other parts of the book; these appear as ?? in the text below.

We have the following inclusions: the natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ are a subset of the integers $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$ are a subset of the rationals $\mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$ are a subset of the real numbers $\mathbb{R}$ are a subset of the complex numbers $\mathbb{C}$. The notation $\mathbb{Z}$ comes from the German zahl (number) and $\mathbb{Q}$ comes from quotient. Are most real numbers rational? We show that, not only are rational numbers "scarce," but irrational numbers like $\sqrt{n}$ or $\sqrt[m]{n}$ are also scarce.

Definition 1.1 (Algebraic Number)**.** *An $\alpha \in \mathbb{C}$ is an algebraic number if it is a root of a polynomial with finite degree and integer coefficients.*

Definition 1.2 (Transcendental Number)**.** *An $\alpha \in \mathbb{C}$ is a transcendental number if it is not algebraic.*

Later (Chapters **??**, **??** and **??**) we see many properties of numbers depend on whether or not a number is algebraic or transcendental. We prove in this chapter that most real numbers are transcendental *without ever constructing a transcendental number!* We then show that e is transcendental but only later in §7.2 will we explicitly construct infinitely many transcendental numbers.

The main theme of this chapter is to describe a way to compare sets with infinitely many elements. In Chapter **??** we compared subsets of the natural numbers. For any set A, let $A_N = A \cap \{1, 2, \ldots, N\}$, and consider $\lim_{N\to\infty} \frac{A_N}{N}$. Such comparisons allowed us to show that in the limit zero percent of all integers are prime (see Chebyshev's Theorem, Theorem **??**), but there are far more primes than perfect squares. While such limiting arguments work well for subsets of the integers, they completely fail for other infinite sets and we need a new notion of size.

For example, consider the closed intervals $[0, 1]$ and $[0, 2]$. In one sense the second set is larger as the first is a proper subset. In another sense they are the same size as each element $x \in [0, 2]$ can be paired with a unique element $y = \frac{x}{2} \in [0, 1]$. The idea of defining size through such correspondences has interesting consequences. While there are as many perfect squares as primes as integers as algebraic numbers, such numbers are rare and in fact essentially all numbers are transcendental.

2. Russell's Paradox and the Banach-Tarski Paradox

The previous example, where in some sense the sets $[0, 1]$ and $[0, 2]$ have the same number of elements, shows that we must be careful with our definition of counting. To motivate our definitions we give some examples of paradoxes in set theory, which emphasize why we must be so careful to put our arguments on solid mathematical ground.

Russell's Paradox: Assume for any property P the collection of all elements having property P is a set. Consider $\mathcal{R} = \{x : x \notin x\}$; thus $x \in \mathcal{R}$ if and only if $x \notin x$. Most objects are not elements of themselves; for example, $\mathbb{N} \notin \mathbb{N}$ because the set of natural numbers is not a natural number. If $\mathcal{R}$ exists, it is natural to ask whether or not $\mathcal{R} \in \mathcal{R}$. Unwinding the definition, we see $\mathcal{R} \in \mathcal{R}$ if and only if $\mathcal{R} \notin \mathcal{R}$! Thus the collection of all objects satisfying a given property is not always a set. This strange situation led mathematicians to reformulate set theory. See, for example, [HJ, Je].

Banach-Tarski Paradox: Consider a solid unit sphere in $\mathbb{R}^3$. It is possible to divide the sphere into 5 disjoint pieces such that, by simply translating and rotating the 5 pieces, we can assemble 3 into a solid unit sphere and the other 2 into a disjoint solid unit sphere. But translating and rotating should not change volumes, yet we have doubled the volume of our sphere! This construction depends on the (Uncountable) Axiom of Choice (see §4.4). See, for example, [Be, Str].

Again, the point of these paradoxes is to remind ourselves that plausible statements need not be true, and one must be careful to build on firm foundations.

3. Definitions

We now define the terms we will use in our counting investigations. We assume some familiarity with set theory; we will not prove all the technical details (see [HJ] for complete details).

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 $b \in B$ there exists $a \in A$ with $f(a) = b$. A **bijection** is a one-to-one and onto function.

Exercise 3.1. *Show $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is not a bijection, but $g : [0, \infty) \to \mathbb{R}$ given by $g(x) = x^2$ is. If $f : A \to B$ is a bijection, prove there exists a bijection $h : B \to A$. We usually write f^{-1} for h.*

We say two sets A and B **have the same cardinality** (i.e., 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), then there is a bijection from A to $\{1, \dots, n\}$. We say A is **finite** and $|A| = n < \infty$.

Exercise 3.2. *Show two finite sets have the same cardinality if and only if they have the same number of elements.*

Exercise 3.3. *Suppose A and B are two sets such that there are onto maps $f : A \to B$ and $g : B \to A$. Prove $|A| = |B|$.*

Exercise 3.4. *A set A is said to be 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 3.5. *Show that the cardinality of the positive even integers is the same as the cardinality of the positive integers is the same as the cardinality of the perfect squares is the same as the cardinality of the primes.*

Remark 3.6. Exercise 3.5 is surprising. Let E_N be all positive even integers at most N. The fraction of positive integers less than $2M$ and even is $\frac{M}{2M} = \frac{1}{2}$, yet the even numbers have the same cardinality as $\mathbb{N}$. If S_N is all perfect squares up to N, one can similarly show the fraction of perfect squares up to N is approximately $\frac{1}{\sqrt{N}}$, which goes to zero as $N \to \infty$. Hence in one sense there are a lot more even numbers or integers than perfect squares, but in another sense these sets are the same size.

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. A is **uncountable** if A is not at most countable

Definition 3.7 (Equivalence Relation)**.** *Let R be a binary relation (taking values true and false) on a set S. We say R is an equivalence relation if the following properties hold:*

(1) Reflexive: $\forall x \in S$, $R(x, x)$ is true;
(2) Symmetric: $\forall x, y \in S$, $R(x, y)$ is true if and only if $R(y, x)$ is true;
(3) Transitive: $\forall x, y, z \in S$, $R(x, y)$ and $R(y, z)$ are true imply $R(x, z)$ is true.

Exercise 3.8.

(1) *Let S be any set, and let $R(x, y)$ be $x = y$. Prove that R is an equivalence relation.*
(2) *Let $S = \mathbb{Z}$ and let $R(x, y)$ be $x \equiv y \bmod n$. Prove R is an equivalence relation.*
(3) *Let $S = (\mathbb{Z}/m\mathbb{Z})^*$ and let $R(x, y)$ be xy is a quadratic residue modulo m. Is R an equivalence relation?*

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

Exercise 3.9. *Let $S = \mathbb{N} \times (\mathbb{N} - \{0\})$. For $(a, b), (c, d) \in S$, we define $R((a, b), (c, d))$ to be true if $ad = bc$ and false otherwise. Prove that R is an equivalence relation. What type of number does a pair (a, b) represent?*

Exercise 3.10. *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.*

4. Countable and Uncountable 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 4.1. *To show a set S is countable, it is sufficient to find a bijection from S to either $\mathbb{W}$ or $\mathbb{N}$ or $\mathbb{Z}$.*

We need the intuitively plausible

Lemma 4.2. *If $A \subset B$, then $|A| \le |B|$.*

Lemma 4.3. *If $f : A \to C$ is a one-to-one function (not necessarily onto), then $|A| \le |C|$. Further, if $C \subset A$ then $|A| = |C|$.*

Theorem 4.4 (Cantor-Bernstein)**.** *If $|A| \le |B|$ and $|B| \le |A|$, then $|A| = |B|$.*

Exercise 4.5. *Prove Lemmas 4.2 and 4.3 and Theorem 4.4.*

Theorem 4.6. *If A and B are countable then 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

$$\begin{aligned} A &= \{a_0, a_1, a_2, a_3, \dots\} \\ B &= \{b_0, b_1, b_2, b_3, \dots\}. \end{aligned} \tag{1}$$

Assume $A \cap B$ is empty. Define $h : \mathbb{N} \to A \cup B$ by $h(2n) = a_n$ and $h(2n+1) = b_n$. As h is a bijection from $\mathbb{N}$ to $A \cup B$, this proves $A \cup B$ is countable. We leave to the reader the case when $A \cap B$ is not empty. To prove $A \times B$ is countable, consider the following function $h : \mathbb{N} \to A \times B$ (see Figure 1):

$$\begin{aligned} &h(1) = (a_0, b_0) \\ &h(2) = (a_1, b_0), h(3) = (a_1, b_1), h(4) = (a_0, b_1) \\ &h(5) = (a_2, b_0), h(6) = (a_2, b_1), h(7) = (a_2, b_2), h(8) = (a_1, b_2), h(9) = (a_0, b_2) \end{aligned}$$

and so on. For example, at the n^{th} stage we have

$$\begin{aligned} h(n^2+1) = (a_n, b_0), h(n^2+2) = (a_n, b_{n-1}), \dots \\ h(n^2+n+1) = (a_n, b_n), h(n^2+n+2) = (a_{n-1}, b_n), \dots \\ \dots, h((n+1)^2) = (a_0, b_n). \end{aligned}$$

We are looking at all pairs of integers (a_x, b_y) in the first quadrant (including those on the axes). 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 and then restarting on the x-axis. $\square$

Corollary 4.7. *Let $(A_i)_{i \in \mathbb{N}}$ be a collection of sets such that A_i is countable for all $i \in \mathbb{N}$. 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[(h)] 4.8. *Prove Corollary 4.7.*

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 4.9. *$\mathbb{N}^n$, $\mathbb{Z}^n$ and $\mathbb{Q}^n$ are countable.*

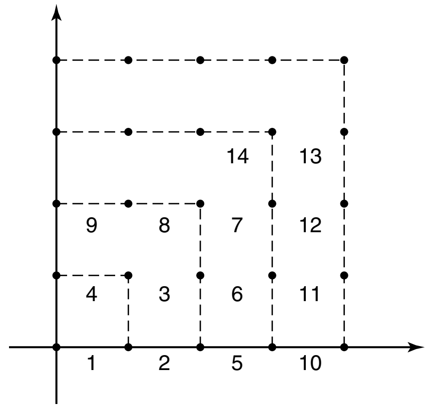

FIGURE 1. $A \times B$ is countable

Proof. Proceed by induction; for example write $\mathbb{Q}^{n+1}$ as $\mathbb{Q}^n \times \mathbb{Q}$. □

Exercise 4.10. *Prove that there are countably many rationals in the interval* $[0, 1]$.

Exercise(hr) 4.11. *Consider N points in the plane. For each point, color every point an irrational distance from that point blue. What is the smallest N needed such that, if the points are properly chosen, every point in the plane is colored blue? If possible, give a constructive solution (i.e., give the coordinates of the points).*

4.1. **Irrational Numbers.** If $\alpha \notin \mathbb{Q}$, we say α is **irrational**. Clearly, not all numbers are rational (for example, $\sqrt{-1}$). Are there any real irrational numbers? The following example disturbed the ancient Greeks:

Theorem 4.12. *The square root of two is irrational.*

Proof. Assume not. Then we have $\sqrt{2} = \frac{p}{q}$, and we may assume p and q are relatively prime. Then $2q^2 = p^2$. We claim that $2|p^2$. While this appears obvious, this must be proved. If p is even, this is clear. If p is odd, we may write $p = 2m + 1$. Then $p^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$, which is clearly not divisible by 2. Thus p is even, say $p = 2p_1$. Then $2q^2 = p^2$ becomes $2q^2 = 4p_1^2$, and a similar argument yields q is even. Hence p and q have a common factor, contradicting our assumption. □

This construction was disturbing for the following reason: consider an isosceles right triangle with bases of length 1. By the Pythagorean theorem, the hypotenuse has length $\sqrt{2}$. Thus, using a straight edge and compass, one easily constructs a non-rational length from rational sides and a right angle.

The above proof would be faster if we appealed to unique factorization: any positive integer can be written uniquely as a product of powers of primes. If one does not use unique factorization, then for $\sqrt{3}$ one must check p of the form $3m, 3m + 1$ and $3m + 2$.

Exercise 4.13. *If n is a non-square positive integer, prove $\sqrt{n}$ is irrational.*

Exercise 4.14. *Using a straight edge and compass, given two segments (one of unit length, one of length r with $r \in \mathbb{Q}$), construct a segment of length $\sqrt{r}$.*

Exercise(h) 4.15. *Prove the Pythagorean theorem: if a right triangle has bases of length a and b and hypotenuse c then $a^2 + b^2 = c^2$.*

4.2. **Algebraic Numbers.** Let $f(x)$ be a polynomial with rational coefficients. By multiplying by the least common multiple of the denominators, we can clear the fractions. Thus without loss of generality it suffices 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 4.16. *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 4.17. *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 4.7 $\mathcal{A}$ is at most countable. The proof proceeds by finding a bijection from the set of all roots of polynomials of degree n with a subset of the countable set $\mathbb{Z}^n$.

Recall the **Fundamental Theorem of Algebra:** Let $f(x)$ be a polynomial of degree n with complex coefficients. Then $f(x)$ has n (not necessarily distinct) roots. Actually, we only need a weaker version, namely that a polynomials with integer coefficients has at most countably many roots.

Fix an $n \in \mathbb{N}$. We 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 4.9, 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 $a \in \mathbb{Z}^{n+1}$

$$\{a : a \in \mathbb{Z}^{n+1}\} \;=\; \bigcup_{i=1}^{\infty} \{\alpha_i\}, \tag{2}$$

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 to the corresponding polynomial. Let R_{α_i} be the set of 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 $P_n = \{x \in \mathbb{C} : x \text{ is a root of a degree } n \text{ polynomial}\}$. One can show that

$$P_n \;=\; \bigcup_{i=1}^{\infty} R_{\alpha_i} \;\supset\; \mathcal{A}_n. \tag{3}$$

By Lemma 4.7, P_n is at most countable. Thus by Lemma 4.2, as P_n is at most countable, $\mathcal{A}_n$ is at most countable. By Corollary 4.7, $\mathcal{A}$ 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 countable. As $\mathcal{A}$ is at most countable, this implies $\mathcal{A}$ is countable. $\square$

Exercise 4.18. *Show the full force of the Fundamental Theorem of Algebra is not needed in the above proof; namely, it is enough that every polynomial have finitely many (or even countably many!) roots.*

Exercise 4.19. *Prove $R_n \supset \mathcal{A}_n$.*

Exercise 4.20. *Prove any real polynomial of odd degree has a real root.*

Remark 4.21. The following argument allows us to avoid using the Fundamental Theorem of Algebra. Let $f(x)$ be a polynomial of degree n with real coefficients. If $\alpha \in \mathbb{C}$ is such that $f(\alpha) = 0$, prove $f(\overline{\alpha}) = 0$, where $\overline{\alpha}$ is the complex conjugate of α ($\alpha = x + iy$, $\overline{\alpha} = x - iy$). Using polynomial long division, divide $f(x)$ by $h(x) = (x - \alpha)$ if $\alpha \in \mathbb{R}$ and $h(x) = (x - \alpha)(x - \overline{\alpha})$ otherwise. As both of these polynomials are real, $\frac{f(x)}{h(x)} = g(x) + \frac{r(x)}{h(x)}$ has all real coefficients, and the degree of $r(x)$ is less than the degree of $h(x)$. As $f(x)$ and $h(x)$ are zero for $x = \alpha$ and $\overline{\alpha}$, $r(x)$ is identically zero. We now have a polynomial of degree $n-1$ (or $n-2$). Proceeding by induction, we see f has at most n roots. Note we have not proved f *has* n roots. Note also the use of the Euclidean algorithm (see §**??**) in the proof.

Exercise 4.22 (Divide and Conquer)**.** *For $f(x)$ continuous, if $f(x_l) < 0 < f(x_r)$ then there must be a root between x_l and x_r (Intermediate Value Theorem, Theorem* **??***); look at the midpoint $x_m = \frac{x_l+x_r}{2}$. If $f(x_m) = 0$ we have found the root; if $f(x_m) < 0$ (> 0) the root is between x_m and x_r (x_m and x_l). Continue subdividing the interval. Prove the division points converge to a root.*

Remark 4.23. By completing the square, one can show that the roots of $ax^2 + bx + c = 0$ are given by $x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$. More complicated formulas exist for the general cubic and quartic; however, there is no such formula which gives the roots of a general degree 5 (or higher) polynomial in terms of its coefficients (see [Art]). While we can use Newton's Method (see §**??**) or Divide and Conquer to approximate a root, we do not have a procedure in general to give an exact answer involving radicals and the coefficients of the polynomial.

Exercise 4.24 (Rational Root Test)**.** *Let $f(x) = a_nx^n + \cdots + a_0$ be a polynomial with integer coefficients, $a_n, a_0 \neq 0$ and coprime. Let $p, q \in \mathbb{Z}$, $q \neq 0$. If $f(p/q) = 0$, show $q|a_n$ and $p|a_0$. Thus given a polynomial one can determine all the rational roots in a finite amount of time. Generalize this by finding a criterion for numbers of the form $\sqrt{p/q}$ to be a root. Does this work for higher powers, such as $\sqrt[m]{p/q}$? Does this contradict the claim in Remark 4.23 about degree 5 and higher polynomials?*

4.3. **Transcendental Numbers.** A set is **uncountable** if it is infinite and there is no bijection between it and the rationals (or the integers, or any countable set). We prove

Theorem 4.25 (Cantor)**.** *The set of all real numbers is uncountable.*

Cantor's Theorem is an immediate consequence of

Lemma 4.26. *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 listing of the elements of $\mathcal{S}$:

$$\begin{aligned} x_1 &= .x_{11}x_{12}x_{13}x_{14}\cdots \\ x_2 &= .x_{21}x_{22}x_{23}x_{24}\cdots \\ x_3 &= .x_{31}x_{32}x_{33}x_{34}\cdots \\ &\vdots \\ x_n &= .x_{n1}x_{n2}x_{n3}x_{n4}\cdots x_{nn}\cdots \\ &\vdots \end{aligned} \tag{4}$$

Define an element $\theta = (\theta_i)_{i\in\mathbb{N}} \in \mathcal{S}$ by $\theta_i = 1 - x_{ii}$. Note θ cannot be in the list; it is not x_N because $1 - x_{NN} \neq x_{NN}$. But our list was supposed to be a complete enumeration of $\mathcal{S}$, contradiction. □

Proof[Proof of Cantor's Theorem] Consider all numbers in the interval $[0, 1]$ whose decimal expansion (see §**??** or §**??**) consists entirely of 0's and 1's. 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, and is uncountable.

Exercise 4.27. *Instead of using decimal expansions one could use binary expansions. Unfortunately there is the problem that some rationals have two expansions, a finite terminating and* *an infinite non-terminating expansion. For example,* $.001 = .0001111111\ldots$ *in base two, or* $.1 = .0999\cdots$ *in base ten. Using binary expansions, prove there are uncountably many reals. Prove* $.001 = .0001111111\ldots$ *in base two.*

Exercise 4.28. *Prove* $|[0,1]| = |\mathbb{R}| = |\mathbb{R}^n| = |\mathbb{C}^n|$*. Find a set with strictly larger cardinality than* $\mathbb{R}$*.*

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 does not tell us *which* numbers are transcendental. We can easily show many numbers (such as $\sqrt{3+\sqrt[5]{2^3}\sqrt[11]{5}+\sqrt{7}}$) are algebraic. What of other numbers, such as π and e?

Lambert (1761), Legendre (1794), Hermite (1873) and others proved π irrational and Lindemann (1882) proved π transcendental (see [HW, NZM]); in Exercise **??**, we showed that $\pi^2 \notin \mathbb{Q}$ implies there are infinitely many primes! 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; see Theorem 7.1 as well as Exercise 7.9.

4.4. **Axiom of Choice and the Continuum Hypothesis.**

Let $\aleph_0 = |\mathbb{Q}|$. Cantor's diagonalization argument can be interpreted as saying that $2^{\aleph_0} = |\mathbb{R}|$. As there are more reals than rationals, $\aleph_0 < 2^{\aleph_0}$. Does there exist a subset of $\mathbb{R}$ with strictly larger cardinality than the rationals, yet strictly smaller cardinality than the reals? Cantor's **Continuum Hypothesis** says that there are no subsets of intermediate size, or, equivalently, that $\aleph_1 = 2^{\aleph_0}$ (the reals are often called the continuum, and the $\aleph_i$ are called cardinal numbers).

The standard axioms of set theory are known as the Zermelo-Fraenkel axioms. A more controversial axiom is the **Axiom of Choice**, which states given any collection of sets $(A_x)_{x\in J}$ indexed by some set J, then there is a function f from J to the disjoint union of the A_x with $f(x) \in A_x$ for all x. Equivalently, this means we can form a new set by choosing an element a_x from each A_x; f is our choice function. If we have a countable collection of sets this is quite reasonable: a countable set is in a one-to-one correspondence with $\mathbb{N}$, and "walking through" the sets we know exactly when we will reach a given set to choose a representative. If we have an uncountable collection of sets, however, it is not clear "when" we would reach a given set to choose an element.

Exercise 4.29. *The construction of the sets in the Banach-Tarski Paradox uses the Axiom of Choice; we sketch the set* $\mathcal{R}$ *that arises. For* $x, y \in [0,1]$ *we say* x *and* y *are equivalent if* $x - y \in \mathbb{Q}$*. Let* $[x]$ *denote all elements equivalent to* x*. We form a set of representatives* $\mathcal{R}$ *by choosing one element from each equivalence class. Prove there are uncountably many distinct equivalence classes.*

Kurt Gödel [Gö] 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 [Coh] 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 axioms of set theory! See [HJ] for more details.

Exercise 4.30. *The cardinal numbers have strange multiplication properties. Prove* $\aleph_0^{\aleph_0} = 2^{\aleph_0}$ *by interpreting the two sides in terms of operations on sets.*

5. Properties of e

In this section we study some of the basic properties of the number e (see [Rud] for more properties and proofs). One of the many ways to define the number e, the base of the natural logarithm, is to write it as the sum of the following infinite series:

$$e \;=\; \sum_{n=0}^{\infty} \frac{1}{n!}. \tag{5}$$

Denote the partial sums of the above series by

$$s_m \;=\; \sum_{n=0}^{m} \frac{1}{n!}. \tag{6}$$

Hence e is the limit of the convergent sequence s_m. This representation is one of the main tool in analyzing the nature of e.

Exercise^(h) 5.1. *Define*

$$e^x \;=\; \sum_{n=0}^{\infty} \frac{x^n}{n!}. \tag{7}$$

Prove $e^{x+y} = e^x e^y$. Show this series converges for all $x \in \mathbb{R}$; in fact, it makes sense for $x \in \mathbb{C}$ as well. One can define a^b by $e^{b \ln a}$.

Exercise^(h) 5.2. *An alternate definition of e^x is*

$$e^x \;=\; \lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n. \tag{8}$$

Show this definition agrees with the series expansion, and prove $e^{x+y} = e^x e^y$. This formulation is useful for growth problems such as compound interest or radioactive decay; see for example [BoDi].

Exercise 5.3. *Prove $\frac{d}{dx} e^x = e^x$. As $e^{\ln x} = x$, the chain rule implies $\frac{d}{dx} \ln x = \frac{1}{x}$ ($\ln x$ is the inverse function to e^x).*

From the functions e^x and $\ln x$, we can interpret a^b for any $a > 0$ and $b \in \mathbb{R}$: $a^b = e^{b \ln a}$. Note the series expansion for e^x makes sense for all x, thus we have a well defined process to determine numbers such as $3^{\sqrt{2}}$. We cannot compute $3^{\sqrt{2}}$ directly because we do not know what it means to raise 3 to the $\sqrt{2}$-power; we can only raise numbers to *rational* powers.

Exercise^(hr) 5.4. *Split 100 into smaller integers such that each integer is two or more and the product of all these integers is as large as possible.*

Suppose now N is a large number and we wish to split N into smaller pieces, but all we require is that each piece be positive. How should we break up a large N?

Exercise^(hr) 5.5. *Without using a calculator or computer, determine which is larger: e^π or π^e.*

5.1. Irrationality of e.

Theorem 5.6 (Euler, 1737)**.** *The number e is irrational.*

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

$$\begin{aligned}
e - s_m \;&=\; \sum_{n=m+1}^{\infty} \frac{1}{n!} \\
&=\; \frac{1}{(m+1)!}\left(1 + \frac{1}{m+2} + \frac{1}{(m+2)(m+3)} + \cdots\right) \\
&<\; \frac{1}{(m+1)!}\left(1 + \frac{1}{m+1} + \frac{1}{(m+1)^2} + \frac{1}{(m+1)^3} + \cdots\right) \\
&=\; \frac{1}{(m+1)!}\frac{1}{1 - \frac{1}{m+1}} \;=\; \frac{1}{m!m}.
\end{aligned} \tag{9}$$

Hence we obtain

$$0 \ < \quad e - s_m \quad < \ \frac{1}{m!m}. \tag{10}$$

In particular, taking $m = q$ we and multiplying (10) by $q!$ yields

$$0 \ < \quad q!e - q!s_q \quad < \ \frac{1}{q}, \tag{11}$$

which is clearly impossible since $q!e - q!s_q$ would have to be an integer between 0 and 1. This contradicts our assumption that e was rational. □

The key idea in the above proof is the simple fact that there are no integers between 0 and 1. We use a variant of this argument to prove e is transcendental.

5.2. **Transcendence of e.** We know there are more transcendental numbers than algebraic numbers. We finally show a specific number is transcendental; see [**?**] for an alternate proof of the transcendence of e, π and many other numbers.

Theorem 5.7 (Hermite, 1873)**.** *The number e is transcendental.*

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

$$a_n X^n + \cdots + a_1 X + a_0 \ = \ 0, \tag{12}$$

where $a_0, a_1, \dots, a_n$ are integers. The existence of such a polynomial leads to an integer greater than zero but less than one; and this contradiction proves the theorem. This is a common technique for proving such results; see also Remark **??**.

Exercise 5.8. *Prove one may assume without loss of generality that $a_0, a_n \neq 0$.*

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

$$F(X) \ = \ f(X) + f'(X) + \cdots + f^{(r)}(X). \tag{13}$$

Exercise 5.9. *Prove the polynomial $F(X)$ has the property that*

$$\frac{d}{dx}\left[e^{-x}F(x)\right] \ = \ -e^{-x}f(x). \tag{14}$$

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

$$e^{-k}F(k) - F(0) \ = \ -ke^{-c_k}f(c_k) \text{ for some } c_k \in (0,k), \tag{15}$$

or equivalently

$$F(k) - e^k F(0) \ = \ -ke^{k-c_k}f(c_k) \ = \ \epsilon_k. \tag{16}$$

Substituting $k = 0, 1, \dots, n$ into (16), we obtain the following system of equations:

$$\begin{array}{rcrcrcl} F(0) & - & F(0) & = & 0 & = & \epsilon_0 \\ F(1) & - & eF(0) & = & -e^{1-c_1}f(c_1) & = & \epsilon_1 \\ F(2) & - & e^2F(0) & = & -2e^{2-c_2}f(c_2) & = & \epsilon_2 \\ & & & \vdots & & & \\ F(n) & - & e^nF(0) & = & -ne^{n-c_n}f(c_n) & = & \epsilon_n. \end{array} \tag{17}$$

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

$$\sum_{k=0}^{n} a_k F(k) - \left(\sum_{k=0}^{n} a_k e^k\right) F(0) \ = \ \sum_{k=0}^{n} a_k \epsilon_k. \tag{18}$$

Notice that on the left hand side we have exactly the polynomial that we assume e satisfies:

$$\sum_{k=0}^{n} a_k e^k \;=\; 0; \tag{19}$$

this is the key step: we have now incorporated the (fictitious) polynomial. Hence (18) reduces to

$$\sum_{k=0}^{n} a_k F(k) \;=\; \sum_{k=0}^{n} a_k \epsilon_k. \tag{20}$$

We have used the hypothetical algebraicity of e to prove a certain integral combination of its powers vanish.

So far we had complete freedom in our choice of f, and (20) always holds for its associate F. In what follows we choose a special polynomial f in order to reach a contradiction. Choose a prime p large enough so that $p > |a_0|$ and $p > n$. Let f equal

$$\begin{aligned} f(X) &= \frac{1}{(p-1)!} X^{p-1}(1-X)^p(2-X)^p \cdots (n-X)^p \\ &= \frac{1}{(p-1)!}\left((n!)^p X^{p-1} + \text{higher order terms}\right) \\ &= \frac{b_{p-1}X^{p-1} + b_p X^p + \cdots + b_r X^r}{(p-1)!}. \end{aligned} \tag{21}$$

Though it plays no role in the proof, we note that the degree of f is $r = (n+1)p - 1$. We prove a number of results which help us finish the proof. Recall that $p\mathbb{Z}$ denotes the set of integer multiples of p.

Claim 5.10. *Let p be a prime number and m any positive integer. Then $(p-1)(p-2)\cdots 2 \cdot 1$ divides $(p-1+m)(p-2+m)\cdots(2+m)(1+m)$.*

Warning: It is clearly not true that any consecutive set of $p-1$ numbers divides any larger consecutive set of $p-1$ numbers. For example, $7\cdot 6\cdot 5\cdot 4$ does not divide $9\cdot 8\cdot 7\cdot 6$, and $8\cdot 7\cdot 6\cdot 5$ does not divide $14\cdot 13\cdot 12\cdot 11$. In the first example we have 5 divides the smaller term but not the larger; in the second we have 2^4 divides the smaller term but only 2^3 divides the larger.

Proof[Proof of Claim 5.10] Let $x = (p-1)!$ and $y = (p-1+m)\cdots(1+m)$. The claim follows by showing for each prime $q < p$ that if $q^a|x$ then $q^a|y$. Let k be the largest integer such that $q^k \le p-1$ and $\lfloor z \rfloor$ be the greatest integer at most z. Then there are $\lfloor \frac{p-1}{q} \rfloor$ factors of x divisible by q once, $\lfloor \frac{p-1}{q^2} \rfloor$ factors of x divisible by q twice, and so on up to $\lfloor \frac{p-1}{q^k} \rfloor$ factors of x divisible by q a total of k times. Thus the exponent of q dividing x is $\sum_{\ell=1}^{k} \lfloor \frac{p-1}{q^\ell} \rfloor$. The proof is completed by showing that for each $\ell \in \{1, \dots, k\}$ we have as many terms in y divisible by q^ℓ as we do in x; it is possible to have more of course (let $q = 5$, $x = 6 \cdots 1$ and $y = 10 \cdots 5$). Clearly it is enough to prove this for $m < (p-1)!$; we leave the remaining details to the reader in Exercise 5.17; see Exercise 5.18 for an alternate proof.

Claim 5.11. *For $i \ge p$ and for all $j \in \mathbb{N}$, we have $f^{(i)}(j) \in p\mathbb{Z}$.*

Proof. Differentiate (21) $i \ge p$ times. Consider any term which survives, say $\frac{b_k X^k}{(p-1)!}$ with $k \ge i$. After differentiating this term becomes $\frac{k(k-1)\cdots(k-(i-1))b_k X^{k-1}}{(p-1)!}$. By Claim 5.10 we have $(p-1)!|k(k-1)\cdots(k-(i-1))$. Further, $p|k(k-1)\cdots(k-(i-1))$ as we differentiated at least p times and any product of p consecutive numbers is divisible by p. As p does not divide $(p-1)!$, we see that all surviving terms are multiplied by p. □

Claim 5.12. *For $0 \le i < p$ and $j \in \{1, \dots, n\}$, we have $f^{(i)}(j) = 0$.*

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

Claim 5.13. *Let F be the polynomial associated to f. Then $F(1), F(2), \dots, F(n) \in p\mathbb{Z}$.*

Proof. Recall that $F(j) = f(j) + f'(j) + \cdots + f^{(r)}(j)$. By Claim 5.11, $f^{(i)}(j)$ is a multiple of p for $i \geq p$ and any integer j. By Claim 5.12, $f^{(i)}(j) = 0$ for $0 \leq i < p$ and $j = 1, 2, \dots, n$. Thus $F(j)$ is a multiple of p for these j. $\square$

Claim 5.14. *For $0 \leq i \leq p-2$, we have $f^{(i)}(0) = 0$.*

Proof. Similar to Claim 5.12, we note that $f^{(i)}(0) = 0$ for $0 \leq i < p-2$, because 0 is a root of $f(x)$ of multiplicity $p-1$. $\square$

Claim 5.15. *$F(0)$ is not a multiple of p.*

Proof. By Claim 5.11, $f^{(i)}(0)$ is a multiple of p for $i \geq p$; by Claim 5.14, $f^{(i)}(0) = 0$ for $0 \leq i \leq p-2$. Since

$$F(0) \ = \ f(0) + f'(0) + \cdots + f^{(p-2)}(0) + f^{(p-1)}(0) + f^{(p)}(0) + \cdots + f^{(r)}(0), \tag{22}$$

to prove $F(0)$ is a not multiple of p it is sufficient to prove $f^{(p-1)}(0)$ is not multiple of p because all the other terms *are* multiples of p. However, from the Taylor series expansion (see §**??**) of f in (21), we see that

$$f^{(p-1)}(0) \ = \ (n!)^p \ + \ \text{terms that are multiples of } p. \tag{23}$$

Since we chose $p > n$, $n!$ is not divisible by p, proving the claim. $\square$

We resume the proof of the transcendence of e. Remember we also chose p such that a_0 is not divisible by p. This fact plus the above claims imply first that $\sum_k a_k F(k)$ is an integer, and second that

$$\sum_{k=0}^{n} a_k F(k) \ \equiv \ a_0 F(0) \ \not\equiv 0 \mod p. \tag{24}$$

Thus $\sum_k a_k F(k)$ is a non-zero integer. Recall (20):

$$\sum_{k=0}^{n} a_k F(k) \ = \ a_1\epsilon_1 + \cdots + a_n\epsilon_n. \tag{25}$$

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

$$\epsilon_k \ = \ -ke^{k-c_k} f(c_k) \ = \ \frac{-ke^{k-c_k} c_k^{p-1}(1-c_k)^p \cdots (n-c_k)^p}{(p-1)!}. \tag{26}$$

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

$$|\epsilon_k| \quad \leq \quad \frac{e^k k^p (1 \cdot 2 \cdots n)^p}{(p-1)!} \ \leq \ \frac{e^n (n!n)^p}{(p-1)!} \ \longrightarrow \ 0 \ \text{ as } \ p \ \rightarrow \ \infty. \tag{27}$$

Exercise 5.16. *For fixed n, prove that as $p \to \infty$, $\frac{(n!n)^p}{(p-1)!} \to 0$. See Lemma* **??**.

Recall that n is fixed, as are the constants $a_0, \dots, a_n$ (they define the polynomial equation supposedly satisfied by e); in our argument only the prime number p varies. Hence, by choosing p sufficiently large, 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:

$$\left| \sum_{k=1}^{n} a_k \epsilon_k \right| \ < \ 1. \tag{28}$$

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

$$\frac{e^n (n!n)^p}{(p-1)!} \ < \ \frac{1}{\sum_{k=0}^n |a_k|}. \tag{29}$$

In this way we reach a contradiction in the identity (20) where the left hand side is a non-zero integer, while the right hand side is a real number of absolute value less than 1. □

This proof illustrates two of the key features of these types of arguments: considering properties of the "fictitious" polynomial, and finding an integer between 0 and 1. It is very hard to prove a given number is transcendental. Note this proof heavily uses special properties of e, in particular the derivative of e^x is e^x. The reader is invited to see Theorem 205 of [HW] where the transcendence of π is proved. It is known that $\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$ is transcendental for k even (in fact, it is a rational multiple of π^k); very little is known if k is odd. If $k = 3$, Apery [Ap] proved $\zeta(3)$ is irrational (see also [Mill]), though it is not known if it is transcendental. For infinitely many odd k, $\zeta(k)$ is irrational ([BR]), and at least one of $\zeta(5), \zeta(7), \zeta(9)$ or $\zeta(11)$ is irrational [Zu]. See also §**??**.

In field theory, one shows that if α, β are algebraic then so are $\alpha + \beta$ and $\alpha\beta$; if both are transcendental, at least one of $\alpha + \beta$ and $\alpha\beta$ is transcendental. Hence, while we expect both $e + \pi$ and $e\pi$ to be transcendental, all we know is at least one is! In §7.2 we construct uncountably many transcendentals. In §**??** we show the Cantor set is uncountable, hence "most" of its elements are transcendental.

Exercise 5.17. *Complete the proof of Claim 5.10.*

Exercise(hr) 5.18. *Alternatively, prove Claim 5.10 by considering the binomial coefficient* $\binom{p-1+m}{p-1}$*, which is an integer.*

Arguing similarly as in the proof of the transcendence of e, we can show π is transcendental. We content ourselves with proving π^2 is irrational, which we have seen (Exercises **??** and **??**) implies there are infinitely many primes. For more on such proofs, see Chapter 11 of [BB] (specifically pages 352 to 356, where the following exercise is drawn from).

Exercise 5.19 (Irrationality of π^2)**.** *Fix a large n (how large n must be will be determined later). Let $f(x) = \frac{x^n(1-x)^n}{n!}$. Show f attains its maximum at $x = \frac{1}{2}$, for $x \in (0,1)$, $0 < f(x) < \frac{1}{n!}$, and all the derivatives of f evaluated at 0 or 1 are integers. Assume π^2 is rational; thus we may write $\pi^2 = \frac{a}{b}$ for integers a, b. Consider*

$$G(x) \ = \ b^n \sum_{k=0}^{n} (-1)^k f^{(2k)}(x) \pi^{2n-2k}. \tag{30}$$

Show $G(0)$ and $G(1)$ are integers and

$$\frac{d}{dx}\left[G'(x)\sin(\pi x) - \pi G(x)\cos(\pi x)\right] \ \ = \ \ \pi^2 a^n f(x)\sin(\pi x). \tag{31}$$

Deduce a contradiction (to the rationality of π^2) by showing that

$$\pi \int_0^1 a^n f(x) \sin(\pi x) dx \ = \ G(0) + G(1), \tag{32}$$

which cannot hold for n sufficiently large. The contradiction is the usual one, namely the integral on the left is in $(0,1)$ and the right hand side is an integer.

6. Exponent (or Order) of Approximation

Let α be a real number. We desire a rational number $\frac{p}{q}$ such that $\left|\alpha - \frac{p}{q}\right|$ is small. Some explanation is needed. In some sense, the size of the denominator q measures the "cost" of approximating α, and we want an error that is small relative to q. For example, we could approximate π by $314159/100000$, which is accurate to 5 decimal places (about the size of q), or we could use $103993/33102$, which uses a smaller denominator and is accurate to 9 decimal places (about twice the size of q)! This ratio comes from the continued fraction expansion of π (see Chapter **??**). We will see later (present chapter and Chapters **??** and **??**) that many properties of numbers are related to how well they can be approximated by rationals. We start with a definition.

Definition 6.1 (Approximation Exponent)**.** *The real number ξ has approximation order (or exponent) $\tau(\xi)$ if $\tau(\xi)$ is the smallest number such that for all $e > \tau(\xi)$ the inequality*

$$\left|\xi - \frac{p}{q}\right| \; < \; \frac{1}{q^e} \tag{33}$$

has only finitely many solutions.

In Theorem **??** we shall see how the approximation exponent yields information about the distribution of the fractional parts of $n^k\alpha$ for fixed k and α. In particular, if α has approximation exponent greater than 4 then the sequence $n^k\alpha \bmod 1$ comes arbitrarily close to all numbers in $[0,1]$.

The following exercise gives an alternate definition for the approximation exponent. The definition below is more convenient for constructing transcendental numbers (Theorem 7.1).

Exercise$^{\text{(h)}}$ 6.2 (Approximation Exponent)**.** *Show ξ has approximation exponent $\tau(\xi)$ if and only if for any fixed $C > 0$ and $e > \tau(\xi)$ the inequality*

$$\left|\xi - \frac{p}{q}\right| \; < \; \frac{C}{q^e} \tag{34}$$

has only finitely many solutions with p, q relatively prime.

6.1. Bounds on the Order of Real Numbers.

Lemma 6.3. *A rational number has approximation exponent* 1.

Proof. If $\xi = \frac{a}{b}$ and $r = \frac{s}{t} \neq \frac{a}{b}$, then $sb - at \neq 0$. Thus $|sb - at| \geq 1$ (as it is integral). This implies

$$\left|\xi - \frac{s}{t}\right| \; = \; \left|\frac{a}{b} - \frac{s}{t}\right| \; = \; \frac{|sb - at|}{bt} \; \geq \; \frac{1}{bt}. \tag{35}$$

If the rational ξ had approximation exponent $e > 1$ we would find

$$\left|\xi - \frac{s}{t}\right| \; < \; \frac{1}{t^e}, \quad \text{which implies} \quad \frac{1}{t^e} \; > \; \frac{1}{bt}. \tag{36}$$

Therefore $t^{e-1} < b$. Since b is fixed, there are only finitely many such t. □

Theorem 6.4 (Dirichlet)**.** *An irrational number has approximation exponent at least* 2.

Proof. It is enough to prove this for $\xi \in (0,1)$. Let $Q > 1$ be an integer. Divide the interval $(0,1)$ into Q equal intervals, say $[\frac{k}{Q}, \frac{k+1}{Q})$. Consider the $Q+1$ numbers inside the interval $(0,1)$:

$$\{\xi\}, \; \{2\xi\}, \; \dots, \; \{(Q+1)\xi\}, \tag{37}$$

where $\{x\}$ denotes the fractional part of x. Letting $[x]$ denote the greatest integer less than or equal to x, we have $x = [x] + \{x\}$. As $\xi \notin \mathbb{Q}$, the $Q+1$ fractional parts are all different.

By Dirichlet's Pigeon-Hole Principle (§**??**), at least two of these numbers, say $\{q_1\xi\}$ and $\{q_2\xi\}$, belong to a common interval of length $\frac{1}{Q}$. Without loss of generality we may take $1 \le q_1 < q_2 \le Q+1$. Hence

$$|\{q_2\xi\} - \{q_1\xi\}| \ \le\ \frac{1}{Q} \tag{38}$$

and

$$|(q_2\xi - n_2) - (q_1\xi - n_1)| \ \le\ \frac{1}{Q}, \quad n_i = [q_i\xi]. \tag{39}$$

Now let $q = q_1 - q_2 \in \mathbb{Z}$ and $p = n_1 - n_2 \in \mathbb{Z}$. Note $1 \le q \le Q$ and

$$|q\xi - p| \ \le\ \frac{1}{Q} \tag{40}$$

and hence

$$\left|\xi - \frac{p}{q}\right| \ \le\ \frac{1}{qQ} \ \le\ \frac{1}{q^2}. \tag{41}$$

We leave the rest of the proof to the reader (Exercise 6.5). □

Exercise$^{(h)}$ 6.5. *Show the above argument leads to an infinite sequence of q with $q \to \infty$; thus there are infinitely many solutions to $\left|\xi - \frac{p}{q}\right| \le \frac{1}{q^2}$. Further, as $\frac{p}{q} \in \mathbb{Q}$ and $\xi \notin \mathbb{Q}$, we may replace the $\le$ with $<$, and ξ has approximation exponent at least 2.*

Exercise$^{(h)}$ 6.6. *Use Exercises 6.5 and 5.19 (where we prove π is irrational) to show that $\sum_{n=1}^{\infty}(\cos n)^n$ diverges; the argument of the cosine function is in radians. Harder: what about $\sum_{n=1}^{\infty}(\sin n)^n$?*

Exercise 6.7. *In Theorem 6.4, what goes wrong if $\xi \in \mathbb{Q}$? Is the theorem true for $\xi \in \mathbb{Q}$?*

Later we give various improvements to Dirichlet's theorem. For example, we use continued fractions to give constructions for the rational numbers $\frac{p}{q}$ (see the proof of Theorem **??**). Further, we show that any number $\frac{p}{q}$ that satisfies Dirichlet's theorem for an irrational ξ has to be a continued fraction convergent of ξ (§**??**). We also ask whether the exponent two can be improved. Our first answer to this question is Liouville's theorem (Theorem 7.1), which states that a real algebraic number of degree n *cannot* be approximated to order larger than n. In other words, if ξ satisfies a polynomial equation with integer coefficients of degree n, then $\tau(\xi) \le n$. Liouville's theorem provides us with a simple method to construct transcendental numbers: if a number can be approximated by rational numbers too well, it will have to be transcendental. We work out a classical example in 7.2.

Liouville's theorem combined with Dirichlet's theorem implies the interesting fact that a quadratic irrational number ξ has approximation exponent exactly 2. Roth's spectacular theorem (Theorem 8.1) asserts that this is in fact the case for all algebraic numbers: the approximation exponent of any real algebraic number is equal to two, regardless of the degree! We will see that the order of approximation of numbers has many applications, for example in digit bias of sequences (Chapter **??**) and Poissonian behavior of the fractional parts of $n^k\alpha$ (Chapter **??**).

Exercise 6.8. *Let α (respectively β) be approximated to order n (respectively m). What is the order of approximation of $\alpha + \frac{a}{b}$ ($\frac{a}{b} \in \mathbb{Q}$), $\alpha + \beta$, $\alpha \cdot \beta$, and $\frac{\alpha}{\beta}$.*

6.2. **Measure of Well Approximated Numbers.** We assume the reader is familiar with the notions of lengths or measures of sets; see §**??**. In loose terms, the following theorem states that almost all numbers have approximation exponent equal to two.

Theorem 6.9. *Let C, ϵ be positive constants. Let S be the set of all points $x \in [0,1]$ such that there are infinitely many relatively prime integers p, q with*

$$\left|x - \frac{p}{q}\right| \ \le\ \frac{C}{q^{2+\epsilon}}. \tag{42}$$

Then the length (or measure) of S, denoted $|S|$, equals 0.

Proof. Let $N > 0$. Let S_N be the set of all points $x \in [0,1]$ such that there are $p, q \in \mathbb{Z}$, $q > N$ for which

$$\left|x - \frac{p}{q}\right| \ \leq\ \frac{C}{q^{2+\epsilon}}. \tag{43}$$

If $x \in S$ then $x \in S_N$ for every N. Thus if we can show that the measure of the sets S_N becomes arbitrarily small as $N \to \infty$, then the measure of S must be zero. How large can S_N be? For a given q there are at most q choices for p. Given a pair (p,q), we investigate how many x's are within $\frac{C}{q^{2+\epsilon}}$ of $\frac{p}{q}$. Clearly the set of such points is the interval

$$I_{p,q} \ =\ \left(\frac{p}{q} - \frac{C}{q^{2+\epsilon}},\ \ \frac{p}{q} + \frac{C}{q^{2+\epsilon}}\right). \tag{44}$$

Note that the length of $I_{p,q}$ is $\frac{2C}{q^{2+\epsilon}}$. Let I_q be the set of all x in $[0,1]$ that are within $\frac{C}{q^{2+\epsilon}}$ of a rational number with denominator q. Then

$$I_q \ \subset\ \bigcup_{p=0}^{q} I_{p,q} \tag{45}$$

and therefore

$$|I_q| \quad\leq\quad \sum_{p=0}^{q} |I_{p,q}| \ =\ (q+1)\cdot\frac{2C}{q^{2+\epsilon}} \ =\ \frac{q+1}{q}\frac{2C}{q^{1+\epsilon}} \ <\ \frac{4C}{q^{1+\epsilon}}. \tag{46}$$

Hence

$$|S_N| \quad\leq\quad \sum_{q>N} |I_q| \ =\ \sum_{q>N} \frac{4C}{q^{1+\epsilon}} \ <\ \frac{4C}{1+\epsilon} N^{-\epsilon}. \tag{47}$$

Thus, as N goes to infinity, $|S_N|$ goes to zero. As $S \subset S_N$, $|S| = 0$. □

Remark 6.10. It follows from Roth's Theorem (Theorem 8.1) that the set S consists entirely of transcendental numbers; however, in terms of length, it is a small set of transcendentals.

Exercise 6.11. *Instead of working with $\left|x - \frac{p}{q}\right| \leq \frac{C}{q^{2+\epsilon}}$, show the same argument works for $\left|x - \frac{p}{q}\right| \leq \frac{C}{f(q)}$, where $\sum \frac{q}{f(q)} < \infty$.*

Exercise 6.12. *Another natural question to ask is what is the measure of all $x \in [0,1]$ such that each digit of its continued fraction is at most K? In Theorem* **??** *we show this set also has length zero. This should be contrasted with Theorem* **??***, where we show if $\sum_{n=1}^{\infty} \frac{1}{k_n}$ converges, then the set $\{x \in [0,1] : a_i(x) \leq k_i\}$ has positive measure. What is the length of $x \in [0,1]$ such that there are no 9's in x's decimal expansion?*

Exercise 6.13 (Hard)**.** *For a given C, what is the measure of the set of $\xi \in (0,1)$ such that*

$$\left|\xi - \frac{p}{q}\right| \ <\ \frac{C}{q^2} \tag{48}$$

holds only finitely often? What if $C < 1$? More generally, instead of $\frac{C}{q^2}$ we could have $\frac{1}{q^2 \log q}$ or any such expression. Warning: The authors are not aware of a solution to this problem!

7. Liouville's Theorem

7.1. Proof of Lioville's Theorem.

Theorem 7.1 (Liouville's Theorem)**.** *Let α be a real algebraic number of degree d. Then α is approximated by rationals to order at most d.*

Proof. Let

$$f(x) \ = \ a_d x^d + \cdots + a_1 x + a_0 \tag{49}$$

be the polynomial with relatively prime integer coefficients of smallest degree (called the **minimal polynomial**) such that $f(\alpha) = 0$. The condition of minimality implies that $f(x)$ is irreducible over $\mathbb{Z}$.

Exercise[(h)] 7.2. *Show that a polynomial irreducible over $\mathbb{Z}$ is irreducible over $\mathbb{Q}$.*

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 $(x - \frac{a}{b})$. Therefore f is non-zero at every rational. Our plan is to show the existence of a rational number $\frac{p}{q}$ such that $f(\frac{p}{q}) = 0$. Let $\frac{p}{q}$ be such a candidate. Substituting gives

$$f\left(\frac{p}{q}\right) \ = \ \frac{N}{q^d}, \quad N \in \mathbb{Z}. \tag{50}$$

Note the integer N depends on p, q and the a_i's. To emphasize this dependence we write $N(p, q; \alpha)$. As usual, the proof proceeds by showing $|N(p, q; \alpha)| < 1$, which then forces $N(p, q; \alpha)$ to be zero; this contradicts f is irreducible over $\mathbb{Q}$.

We find an upper bound for $N(p, q; \alpha)$ by considering the Taylor expansion of f about $x = \alpha$. As $f(\alpha) = 0$, there is no constant term in the Taylor expansion. We may assume $\frac{p}{q}$ satisfies $|\alpha - \frac{p}{q}| < 1$. Then

$$f(x) \ = \ \sum_{i=1}^{d} \frac{1}{i!} \frac{\mathrm{d}^i f}{\mathrm{d}x^i}(\alpha) \cdot (x - \alpha)^i. \tag{51}$$

Consequently

$$\begin{aligned} \left| f\left(\frac{p}{q}\right) \right| \ = \ \left| \frac{N(p, q; \alpha)}{q^d} \right| \ & \leq \ \left| \frac{p}{q} - \alpha \right| \cdot \sum_{i=1}^{d} \left| \frac{1}{i!} \frac{\mathrm{d}^i f}{\mathrm{d}x^i}(\alpha) \right| \cdot \left| \frac{p}{q} - \alpha \right|^{i-1} \\ & \leq \ \left| \frac{p}{q} - \alpha \right| \cdot d \cdot \max_i \left| \frac{1}{i!} \frac{\mathrm{d}^i f}{\mathrm{d}x^i}(\alpha) \cdot 1^{i-1} \right| \\ & \leq \ \left| \frac{p}{q} - \alpha \right| \cdot A(\alpha), \end{aligned} \tag{52}$$

where $A(\alpha) = d \cdot \max_i \left| \frac{1}{i!} \frac{\mathrm{d}^i f}{\mathrm{d}x^i}(\alpha) \right|$. If α were approximated by rationals to order greater than d, then (Exercise 6.2) for some $\epsilon > 0$ there would exist a constant $B(\alpha)$ and infinitely many $\frac{p}{q}$ such that

$$\left| \frac{p}{q} - \alpha \right| \ \leq \ \frac{B(\alpha)}{q^{d+\epsilon}}. \tag{53}$$

Combining yields

$$\left| f\left(\frac{p}{q}\right) \right| \ \leq \ \frac{A(\alpha) B(\alpha)}{q^{d+\epsilon}}. \tag{54}$$

Therefore

$$|N(p, q; \alpha)| \ \leq \ \frac{A(\alpha) B(\alpha)}{q^{\epsilon}}. \tag{55}$$

For q sufficiently large, $A(\alpha)B(\alpha) < q^\epsilon$. As we may take q arbitrarily large, for sufficiently large q we have $|N(p,q;\alpha)| < 1$. As the only non-negative integer less than 1 is 0, we find for q large that $f\left(\frac{p}{q}\right) = 0$, contradicting f is irreducible over $\mathbb{Q}$. □

Exercise 7.3. *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* $q_i \to \infty$.

7.2. **Constructing Transcendental Numbers.** 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 α can be approximated by rationals to an arbitrarily large order, then α must be transcendental! This provides us with a recipe for constructing transcendental numbers. Note the reverse need not be true: if a number x can be approximated to order at most n, it does not follow that x is algebraic of degree at most n (see Theorem 8.1); for example, Hata [Hata] showed the approximation exponent of π is at most 8.02; see Chapter 11 of [BB] for bounds on the approximation exponent for e, π, $\zeta(3)$ and $\log 2$. We use the definition of approximation exponent from Exercise 6.2.

Theorem 7.4 (Liouville)**.** *The number*

$$\alpha \ = \ \sum_{m=1}^{\infty} \frac{1}{10^{m!}} \tag{56}$$

is transcendental.

Proof. The series defining α 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 makes α transcendental. Fix N large and choose $n > N$. Write

$$\frac{p_n}{q_n} \ = \ \sum_{m=1}^{n} \frac{1}{10^{m!}} \tag{57}$$

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 α. In particular, all these rational numbers are distinct. Note also that q_n must divide $10^{n!}$, which implies that $q_n \leq 10^{n!}$. Using this, and the fact that $10^{-(n+1+k)!} < 10^{-(n+1)!}10^{-k}$, we obtain

$$\begin{aligned}
0 \ < \ \alpha - \frac{p_n}{q_n} \quad &= \quad \sum_{m>n} \frac{1}{10^{m!}} \\
&< \quad \frac{1}{10^{(n+1)!}}\left(1 + \frac{1}{10} + \frac{1}{10^2} + \cdots\right) \\
&= \quad \frac{1}{10^{(n+1)!}} \cdot \frac{10}{9} \\
&< \quad \frac{2}{(10^{n!})^{n+1}} \\
&< \quad \frac{2}{q_n^{n+1}} \ \leq \ \frac{2}{q_n^N}.
\end{aligned} \tag{58}$$

This gives an approximation by rationals of order N of α, in fact infinitely many such approximations (one for each $n > N$). Since N can be chosen arbitrarily large, this implies that α can be approximated by rationals to arbitrary order. By Theorem 7.1, if α were algebraic of degree m it could be approximated by rationals to order at most m; thus, α is transcendental. □

Numbers defined as in (56) are called Liouville numbers. The following exercise shows there are uncountably many Liouville numbers.

Exercise 7.5. *Consider the binary expansion for $x \in [0,1)$, namely*

$$x \ = \ \sum_{n=1}^{\infty} \frac{b_n(x)}{2^n}, \quad b_n(x) \in \{0,1\}. \tag{59}$$

For irrational x this expansion is unique. Consider the function

$$M(x) \ = \ \sum_{n=1}^{\infty} 10^{-(b_n(x)+1)n!}. \tag{60}$$

Prove for irrational x that $M(x)$ is transcendental. Thus the above is an explicit construction for uncountably many transcendentals! Investigate the properties of this function. Is it continuous or differentiable (everywhere or at some points)? What is the measure of these numbers? These are "special" transcendental numbers (compare these numbers to Theorem 6.9). See also Remark **??**.

The following example uses some results concerning continued fraction studied in Chapter **??**. The reader should return to this theorem after studying Chapter **??**.

Theorem 7.6. *The number*

$$\beta \ = \ [10^{1!}, 10^{2!}, \dots] \tag{61}$$

is transcendental.

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

$$\left|\beta - \frac{p_n}{q_n}\right| \ = \ \frac{1}{q_n q'_{n+1}} \ = \ \frac{1}{q_n(a'_{n+1}q_n + q_{n-1})} \ < \ \frac{1}{a_{n+1}} \ = \ \frac{1}{10^{(n+1)!}}. \tag{62}$$

Since $q_k = a_k q_{k-1} + q_{k-2}$, we have $q_k > q_{k-1}$ Also $q_{k+1} = a_{k+1}q_k + q_{k-1}$, so we obtain

$$\frac{q_{k+1}}{q_k} \ = \ a_{k+1} + \frac{q_{k-1}}{q_k} \ < \ a_{k+1} + 1. \tag{63}$$

Writing this inequality for $k = 1, \dots, n-1$ and multiplying yields

$$\begin{aligned} q_n \ = \ q_1 \frac{q_2}{q_1}\frac{q_3}{q_2} \cdots \frac{q_n}{q_{n-1}} \quad &< \quad (a_1+1)\,(a_2+1) \cdots (a_n+1) \\ &= \quad \left(1 + \frac{1}{a_1}\right) \cdots \left(1 + \frac{1}{a_n}\right) a_1 \cdots a_n \\ &< \quad 2^n a_1 \cdots a_n \ = \ 2^n 10^{1!+\cdots+n!} \\ &< \quad 10^{2\cdot n!} \ = \ a_n^2. \end{aligned} \tag{64}$$

Combining (62) and (64) gives

$$\left|\beta - \frac{p_n}{q_n}\right| \ < \ \frac{1}{a_{n+1}} \ = \ \frac{1}{a_n^{n+1}} \ < \ \left(\frac{1}{a_n^2}\right)^{\frac{n}{2}} \ < \ \left(\frac{1}{q_n^2}\right)^{\frac{n}{2}} \ = \ \frac{1}{q_n^n}. \tag{65}$$

In this way we get, just as in Liouville's Theorem, an approximation of β by rationals to arbitrary order. This proves that β is transcendental. □

Exercise 7.7. *Without using the factorial function, construct transcendental numbers (either by series expansion or by continued fractions). Can you do this using a function $f(n)$ which grows slower than $n!$?*

The following exercises construct transcendental numbers by investigating infinite products of rational numbers; see Exercise **??** for a review of infinite products. algebraic and which are transcendental.

Exercise 7.8. *Let a_n be a sequence of positive numbers such that $\sum_{n=1}^{\infty} a_n$ converges. Assume also for all $N > 1$ that $a_N > \sum_{n=N+1}^{\infty} a_n$. Let $(n_1, n_2, \dots)$ and $(m_1, m_2, \dots)$ be any two distinct infinite sequences of increasing positive integers; this means that there is at least one k such that $n_k \neq m_k$. Prove*

$$\sum_{k=1}^{\infty} a_{n_k} \neq \sum_{k=1}^{\infty} a_{m_k}, \tag{66}$$

and find three different sequences $\{a_n\}_{n=1}^{\infty}$ satisfying the conditions of this problem.

Exercise(h) 7.9. *Prove*

$$\prod_{n=2}^{\infty} \frac{n^2-1}{n^2} = \prod_{n=2}^{\infty} \left(1 - \frac{1}{n^2}\right) = \frac{1}{2}. \tag{67}$$

For each $\alpha \in [0,1]$, let $\alpha(n)$ be the n^{th} of α's binary expansion; if α has two expansions take the finite one. Consider the function

$$f(\alpha) = \prod_{n=2}^{\infty} \left(1 - \frac{\alpha(n)}{n^2}\right). \tag{68}$$

Prove $f(\alpha)$ takes on countably many distinct rational values and uncountably many distinct transcendental values. Hint: *one approach is to use the previous exercise. For a generic $\alpha \in [0,1]$, do you expect $f(\alpha)$ to be algebraic or transcendental? Note if $\alpha(n) = 1$ for n prime and 0 otherwise we get $\frac{6}{\pi^2}$; see Exercise* **??** *and* **??**.

8. Roth's Theorem

As we saw earlier, Liouville's Theorem asserts that there is a limit to the accuracy with which algebraic numbers can be approximated by rational numbers. There is a long list of improvements associated with Liouville's Theorem. More precise and more profound results were proved by Thue in 1908, Siegel in 1921, Dyson in 1947 and Roth in 1955, to mention but a few of the improvements. Thue proved that the exponent n can be replaced by $\frac{n}{2}+1$; Siegel proved

$$\min_{1 \leq s \leq n-1} \left(s + \frac{n}{s+1}\right) \tag{69}$$

works, and Dyson showed that $\sqrt{2n}$ is sufficient. It was, however, conjectured by Siegel that for any $\epsilon > 0$, $2+\epsilon$ is enough! Proving Siegel's conjecture was Roth's remarkable achievement that earned him a Fields medal in 1958. For an enlightening historical analysis of the work that led to Roth's Theorem see [Gel], Chapter I.

Theorem 8.1 (Roth's Theorem)**.** *Let α be a real algebraic number (a root of a polynomial equation with integer coefficients). Given any $\epsilon > 0$ there are only finitely many relatively prime pairs of integers (p,q) such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}. \tag{70}$$

Remark 8.2. We have seen for $\alpha \notin \mathbb{Q}$ that there are infinitely many pairs of relatively prime integers (p,q) such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{71}$$

Therefore any non-rational algebraic number has approximation exponent exactly 2.

Roth's Theorem has been generalized to more general settings. For a generalization due to Lang, and other historical remarks, see [HS]. For another generalization due to Schmidt see [B].

The remainder of this chapter is devoted to various applications of this fundamental theorem. For a proof, see Chapter **??**.

8.1. **Applications of Roth's Theorem to Transcendental Numbers.** In this section we indicate, without proof, some miscellaneous applications of Roth's Theorem to constructing transcendental numbers. From this theorem follows a sufficient, but not necessary, condition for transcendency: let ξ and $\tau > 2$ be real numbers. If there exists an infinite sequence of distinct rational numbers $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, \dots$ satisfying

$$0 \ < \ \left|\xi - \frac{p_r}{q_r}\right| \ \leq \ \frac{1}{q_r^\tau} \tag{72}$$

for $r = 1, 2, 3, \dots$, then ξ is transcendental.

Exercise 8.3. *Verify that the collection of all such ξ is an uncountable set of measure zero.*

The first application is a theorem due to Mahler which was originally proved by an improvement of Thue's result mentioned above. One can of course prove the same result using Roth's Theorem; the proof is easier, but still non-trivial. Let $P(x)$ be a polynomial with integral coefficients with the property that $P(n) > 0$ if $n > 0$. Let $q > 1$ be a positive integer. For any number n we let $l_q(n)$ be the string of numbers obtained from writing n in base q. Then Mahler's theorem [Mah] asserts that the number

$$\begin{aligned} \alpha(P;q) &= 0.l_q(P(1))l_q(P(2))l_q(P(3))\cdots \\ &= \sum_{n=1}^{\infty} \frac{P(n)}{\prod_{k=1}^{n} q^{\lceil \log_q P(k) \rceil}} \end{aligned} \tag{73}$$

is transcendental (see [Gel], page 6). For example, when $P(x) = x$ and $q = 10$, we obtain Champernowne's constant

$$0.123456789101112131415161718\dots. \tag{74}$$

Exercise 8.4. *Prove, using elementary methods, that the above number is irrational. Can you prove this particular number is transcendental?*

Another application is the transcendence of various continued fractions expansions (see Chapter **??** for properties of continued fractions). As an illustration we state the following theorem due to Okano [Ok]: let $\gamma > 16$ and suppose $A = [a_1, a_2, a_3, \dots]$ and $B = [b_1, b_2, b_3, \dots]$ are two simple continued fractions with $a_n > b_n > a_{n-1}^{\gamma(n-1)}$ for n sufficiently large. Then $A, B, A \pm B$ and $AB^{\pm 1}$ are transcendental. The transcendence of A, B easily follows from Liouville's theorem, but the remaining assertions rely on Roth's Theorem.

8.2. **Applications of Roth's Theorem to Diophantine Equations.** Here we collect a few applications of Roth's Theorem to Diophantine equations (mostly following [Hua], Chapter 17); see also Remark **??**. Before stating any hard theorems, however, we illustrate the general idea with an example (see pages 244–245 of [Sil1]).

Example 8.5. *There are only finitely many integer solutions $(x, y) \in \mathbb{Z}^2$ to*

$$x^3 - 2y^3 \ = \ a. \tag{75}$$

In order to see this, we proceed as follows. Let $\rho = e^{2\pi i/3} = (-1)^{1/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Then

$$x^3 - 2y^3 \ = \ (x - 2^{1/3}y)(x - \rho 2^{1/3}y)(x - \rho^2 2^{1/3}y), \tag{76}$$

and therefore

$$\begin{aligned}\left|\frac{a}{y^3}\right| &= \left|\frac{x}{y}-2^{1/3}\right|\left|\frac{x}{y}-\rho 2^{1/3}\right|\left|\frac{x}{y}-\rho^2 2^{1/3}\right| \\ &\geq \left|\frac{x}{y}-2^{1/3}\right|\left|\Im(\rho 2^{1/3})\right|\left|\Im(\rho^2 2^{1/3})\right| \\ &= \frac{3}{2^{4/3}}\left|\frac{x}{y}-2^{1/3}\right|. \end{aligned} \tag{77}$$

Hence every integer solution (x, y) *to* $x^3 - 2y^3 = a$ *is a solution to*

$$\left|2^{1/3}-\frac{x}{y}\right| \leq \frac{3\cdot 2^{-4/3}}{|y|^3}. \tag{78}$$

By Roth's Theorem there are only finitely many such solutions.

Note Liouville's Theorem is not *strong enough to allow us to conclude there are only finitely many integer solutions. As* $2^{1/3}$ *is an algebraic number of degree* 3*, Liouville's Theorem says* $2^{1/3}$ *can be approximated by rationals to order at most* 3*. Thus the possibility that* $2^{1/3}$ can *be approximated by rationals to order* 3 *is* not *ruled out by Liouville's Theorem.*

Remark 8.6. The reader should keep in mind that "finite" does not mean "a small number"; 10^{456} is still a finite number! In general, Roth's Theorem and other finiteness results of the same nature do not provide effective bounds. In some sense this is similar to the special value proofs of the infinitude of primes: $\pi^2 \notin \mathbb{Q}$ implies there are infinitely many primes, but gives no information on how many primes there are at most x (see Exercise **??**).

Building on the above example, we state the following important theorem.

Theorem 8.7. *Let* $n \geq 3$ *and let* $f(x, y)$ *be an irreducible homogeneous polynomial of degree* n *with integer coefficients. Suppose that* $g(x, y)$ *is a polynomial with rational coefficients of degree at most* $n - 3$*. Then the equation*

$$f(x,y) = g(x,y) \tag{79}$$

has only finitely many solutions in integers (x, y)*.*

Proof. Let us assume $a_0 \neq 0$. Without loss of generality we may also assume $|x| \leq |y|$. Suppose $y > 0$, the other cases being similar or trivial. Let $\alpha_1, \dots, \alpha_n$ be the roots of the equation $f(x, 1) = 0$, and let G be the maximum of the absolute values of the coefficients of $g(x, y)$. Then (79) implies

$$\begin{aligned}|a_0(x-\alpha_1 y)\dots(x-\alpha_n y)| &\leq G(1+2|y|+\dots+(n-2)|y|^{n-3}) \\ &< n^2 G|y|^{n-3}.\end{aligned} \tag{80}$$

Exercise 8.8. *Prove the above inequalities.*

Consequently

$$|(x-\alpha_1 y)\dots(x-\alpha_n y)| < \frac{n^2 G}{|a_0|}|y|^{n-3}. \tag{81}$$

As on the left hand side there are n factors, at least one the factors must be strictly less than the right hand side raised to the power $\frac{1}{n}$; there exist an index ν such that

$$|x-\alpha_\nu y| < \left(\frac{n^2 G}{|a_0|}\right)^{\frac{1}{n}} |y|^{1-\frac{3}{n}}. \tag{82}$$

Since there are infinitely many solutions (x, y), it is a consequence of the Pigeon-hole Principle that infinitely many of the pairs of solutions correspond to the same index ν. We fix one such index and denote it again by ν. Next let $\mu \neq \nu$ and $|y| > N$, N a large positive number whose size we will determine in a moment. Then

$$\begin{aligned} |x - \alpha_\mu y| &= |(\alpha_\nu - \alpha_\mu)y + (x - \alpha_\nu y)| \\ &> |(\alpha_\nu - \alpha_\mu)| \cdot |y| - \left(\frac{n^2 G}{|a_0|}\right)^{\frac{1}{n}} \cdot |y|^{1-\frac{3}{n}} \\ &> \frac{1}{2}|(\alpha_\nu - \alpha_\mu)| \cdot |y| \end{aligned} \tag{83}$$

for N sufficiently large. Next, 80 and 81 imply that for $|y| > N$ we have

$$\frac{n^2 G}{|a_0|}|y|^{n-3} > \left[\prod_{\mu \neq \nu} \frac{1}{2}|\alpha_\nu - \alpha_\mu|\right] \cdot |y|^{n-1} \left|x - \alpha_\nu y\right|. \tag{84}$$

Hence

$$\left|\frac{x}{y} - \alpha_\nu\right| < \frac{K}{|y|^3} \tag{85}$$

for infinitely many pairs of integers (x, y) for a fixed explicitly computable constant K. By Roth's Theorem, this contradicts the algebraicity of α_ν. □

Exercise 8.9. *In the proof of Theorem 8.7, handle the cases where* $|x| > |y|$.

Remark 8.10. In the proof of the above theorem, and also the example preceding it, we used the following simple, but extremely useful, observation: If $a_1, \dots, a_n, B$ are positive quantities subject to $a_1 \dots a_n < B$, then for some i, we have $a_i < B^{\frac{1}{n}}$.

An immediate corollary is the following:

Corollary 8.11 (Thue). *Let* $n \geq 3$ *and let* f *be as above. Then for any integer* a *the equation*

$$f(x, y) = a \tag{86}$$

has only finitely many solutions.

Exercise 8.12 (Thue). *Show that if* $a \neq 0$ *and* $f(x, y)$ *is not the* n^{th} *power of a linear form or the* $\frac{n}{2}^{\text{th}}$ *power of a quadratic form, then the conclusion of the corollary still holds.*

Example 8.13. *Consider Pell's Equation* $x^2 - dy^2 = 1$ *where* d *is not a perfect square. We know that if* $d > 0$ *this equation has infinitely many solutions in integers* (x, y). *Given integers* d *and* n, *we can consider the generalized Pell's Equation* $x^n - dy^n = 1$. *Exercise 8.12 shows that if* $n \geq 3$ *the generalized Pell's Equation can have at most finitely many solutions. See §**??** for more on Pell's Equation.*

Example 8.14. *We can apply the same idea to Fermat's equation* $x^n + y^n = z^n$. *Again, Exercise 8.12 shows that if* $n \geq 3$ *there are at most a finite number of solutions* (x, y, z), *provided that we require one of the variables to be a fixed integer. For example, the equation* $x^n + y^n = 1$ *cannot have an infinite number of integer solutions* (x, y). *This is of course not hard to prove directly (exercise!). Fermat's Last Theorem states that there are no rational solutions to the equation* $x^n + y^n = 1$ *for* n *larger than two except when* $xy = 0$ *(if* x *or* y *is zero, we say the solution is trivial). A deep result of Faltings, originally conjectured by Mordell, implies that for any given* $n \geq 3$ *there are at most a finite number of rational solutions to the equation. Incidently, the proof of Faltings' theorem uses a generalization of Roth's Theorem. Unfortunately, Faltings' theorem does not rule out the possibility of the existence of non-trivial solutions as conjectured by Fermat. This was finally proved by Wiles in 1995; see* [Acz, Maz3, Wi].

Exercise 8.15 (Hua). *Let $n \geq 3$, $b^2 - 4ac \neq 0$, $a \neq 0$, $d \neq 0$. Then a theorem of Landau, Ostrowski, and Thue states that the equation*

$$ay^2 + by + c \ = \ dx^n \tag{87}$$

has only finitely many solutions. Assuming this statement, prove the following two assertions:

(1) *Let n be an odd integer greater than 1. Arrange the integers which are either a square or an n^{th} power into an increasing sequence (z_r). Prove that $z_{r+1} - z_r \to \infty$ as $r \to \infty$.*
(2) *Let $\langle \xi \rangle = \min(\xi - [\xi], [\xi] + 1 - \xi)$. Prove that*

$$\lim_{x \to \infty, x \neq k^2} x^{\frac{n}{2}} \langle x^{\frac{n}{2}} \rangle \ = \ \infty, \tag{88}$$

where the conditions on the limit mean $x \to \infty$ and x is never a perfect square.

REFERENCES

Links to many of the references below are available online at
http://www.math.princeton.edu/mathlab/book/index.html

[Acz] A. Aczel, *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem*, Four Walls Eight Windows, New York, 1996.

[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.

[AgKaSa] M. Agrawal, N. Kayal and N. Saxena, *PRIMES is in P*, Ann. of Math. (2) **160** (2004), no. 2, 781–793.

[Al] L. Ahlfors, *Complex Analysis*, 3rd edition, McGraw-Hill, New York, 1979.

[AZ] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, Springer-Verlag, Berlin, 1998.

[AGP] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. Math. **139** (1994), 703–722.

[AMS] AMS MathSciNet, http://www.ams.org/msnmain?screen=Review

[AB] U. Andrews IV and J. Blatz, *Distribution of digits in the continued fraction representations of seventh degree algebraic irrationals*, Junior Thesis, Princeton University, Fall 2002.

[Ap] R. Apéry, *Irrationalité de $\zeta(2)$ et $\zeta(3)$*, Astérisque **61** (1979) 11–13.

[Apo] T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1998.

[ALM] S. Arms, A. Lozano-Robledo and S. J. Miller, *Constructing One-Parameter Families of Elliptic Curves over $\mathbb{Q}(T)$ with Moderate Rank*, preprint.

[Art] M. Artin, *Algebra*, Prentice-Hall, Englewood Cliffs, NJ, 1991.

[Ay] R. Ayoub, *Introduction to the Analytic Theory of Numbers*, AMS, Providence, RI, 1963.

[Bai] Z. Bai, *Methodologies in spectral analysis of large-dimensional random matrices, a review*, Statist. Sinica **9** (1999), no. 3, 611–677.

[B] A. Baker, *Transcendental Number Theory*, Cambridge University Press, Cambridge, 1990.

[BM] R. Balasubramanian and C. J. Mozzochi, *Siegel zeros and the Goldbach problem*, J. Number Theory **16** (1983), no. 3, 311–332.

[BR] K. Ball and T. Rivoal, *Irrationalité d'une infinité valeurs de la fonction zeta aux entiers impairs*, Invent. Math. **146** (2001), 193–207.

[BT] V. V. Batyrev and Yu. Tschinkel, *Tamagawa numbers of polarized algebraic varieties*, Nombre et répartition de points de hauteur bornée (Paris, 1996), Astérisque (1998), No. 251, 299–340.

[BL] P. Baxandall and H. Liebeck, *Vector Calculus*, Clarendon Press, Oxford, 1986.

[Be] R. Beals, *Notes on Fourier series*, Lecture Notes, Yale University, 1994.

[Bec] M. Beceanu, *Period of the continued fraction of $\sqrt{n}$*, Junior Thesis, Princeton University, 2003.

[Ben] F. Benford, *The law of anomalous numbers*, Proceedings of the American Philosophical Society **78** (1938) 551–572.

[BBH] A. Berger, Leonid A. Bunimovich, and T. Hill, *One-dimensional dynamical systems and Benford's Law*, Trans. Amer. Math. Soc. **357** (2005), no. 1, 197–219.

[BEW] B. Berndt, R. Evans, and K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Vol. 21, Wiley-Interscience Publications, John Wiley & Sons, New York, 1998.

[Ber] M. Bernstein, *Games, hats, and codes*, lecture at the SUMS 2005 Conference.

[BD] P. Bickel and K. Doksum, *Mathematical Statistics: Basic Ideas and Selected Topics*, Holden-Day, San Francisco, 1977.

[Bi] P. Billingsley, *Probability and Measure*, 3rd edition, Wiley, New York, 1995.

[Bl1] P. Bleher, *The energy level spacing for two harmonic oscillators with golden mean ratio of frequencies*, J. Stat. Phys. **61** (1990) 869–876.

[Bl2] P. Bleher, *The energy level spacing for two harmonic oscillators with generic ratio of frequencies*, J. Stat. Phys. **63** (1991), 261–283.

[Bob] J. Bober, *On the randomness of modular inverse mappings*, Undergraduate Mathematics Laboratory report, Courant Institute, NYU, 2002.

[Bol] B. Bollobás, *Random Graphs*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2001.

[BoLa] E. Bombieri and J. Lagarias, *Complements to Li's criterion for the Riemann ypothesis*, J. Number Theory **77** (1999), no. 2, 274–287.

[BP] E. Bombieri and A. van der Poorten, *Continued fractions of algebraic numbers*. Pages 137–152 in *Computational Algebra and Number Theory (Sydney, 1992)*, Mathematical Applications, Vol. 325, Kluwer Academic, Dordrecht, 1995.

[Bon] D. Boneh, *Twenty years of attacks on the RSA cryptosystem*, Notices of the American Mathematical Society, **46** (1999), no. 2, 203–213.

[BS] Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, New York, 1968.

[BB] J. Borwein and P. Borwein, *Pi and the AGM: A Study in Analytic Number Theory and Computational Complexity*, John Wiley and Sons, New York, 1987.

[BK] A. Boutet de Monvel and A. Khorunzhy, *Some elementary results around the Wigner semicircle law*, lecture notes.

[BoDi] W. Boyce and R. DiPrima, *Elementary differential equations and boundary value problems*, 7th edition, John Wiley & Sons, New York, 2000.

[Bre1] R. Brent, *The distribution of small gaps between successive primes*, Math. Comp. **28** (1974), 315–324.

[Bre2] R. Brent, *Irregularities in the distribution of primes and twin primes*, Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday, Math. Comp. **29** (1975), 43–56.

[BPR] R. Brent, A. van der Poorten, and H. te Riele, *A comparative study of algorithms for computing continued fractions of algebraic numbers*. Pages 35–47 in *Algorithmic number theory (Talence, 1996)*, Lecture Notes in Computer Science, Vol. 1122, Springer, Berlin, 1996.

[deBr] R. de la Bretèche, *Sur le nombre de points de hauteur bornée d'une certaine surface cubique singulière*. Pages 51–77 in *Nombre et répartition de points de hauteur bornée (Paris, 1996)*, Astérisque, (1998) no. 251, 51–77.

[BBD] R. de la Bretèche, T. D. Browning, and U. Derenthal, *On Manin's conjecture for a certain singular cubic surface*, preprint.

[BPPW] B. Brindza, A. Pintér, A. van der Poorten, and M. Waldschmidt, *On the distribution of solutions of Thue's equation*. Pages 35–46 in *Number theory in progress (Zakopane-Koscielisko, 1997)*, Vol. 1, de Gruyter, Berlin, 1999.

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

[BrDu] J. Brown and R. Duncan, *Modulo one uniform distribution of the sequence of logarithms of certain recursive sequences*, Fibonacci Quarterly **8** (1970) 482–486.

[Bro] T. Browning, *The density of rational points on a certain singular cubic surface*, preprint.

[BDJ] W. Bryc, A. Dembo, T. Jiang, *Spectral measure of large random Hankel, Markov and Toeplitz matrices*, preprint.

[Bry] A. Bryuno, *Continued frations of some algebraic numbers*, U.S.S.R. Comput. Math. & Math. Phys. **4** (1972), 1–15.

[Bur] E. Burger, *Exploring the Number Jungle: A Journey into Diophantine Analysis*, AMS, Providence, RI, 2000.

[BuP] E. Burger and A. van der Poorten, *On periods of elements from real quadratic number fields*. Pages 35–43 in *Constructive, Experimental, and Nonlinear Analysis (Limoges, 1999)*, CMS Conf. Proc., **27**, AMS, Providence, RI, 2000.

[CaBe] G. Casella and R. Berger, *Statistical Inference*, 2nd edition, Duxbury Advanced Series, Pacific Grove, CA, 2002.

[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.

[Car] L. Carleson, *On the convergence and growth of partial sums of Fourier series*, Acta Math. **116** (1966), 135–157.

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

[Ch] D. Champernowne, *The construction of decimals normal in the scale of ten*, J. London Math. Soc. 8 (1933), 254–260.

[Cha] K. Chang, *An experimental approach to understanding Ramanujan graphs*, Junior Thesis, Princeton University, Spring 2001.

[ChWa] J. R. Chen and T. Z. Wang, *On the Goldbach problem*, Acta Math. Sinica **32** (1989), 702–718.

[Chr] J. Christiansen, *An introduction to the moment problem*, lecture notes.

[Ci] J. Cisneros, *Waring's problem*, Junior Thesis, Princeton University, Spring 2001.

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

[CB] S. Chatterjee and A. Bose, *A new method for bounding rates of convergence of empirical spectral distributions*, J. Theoret. Probab. **17** (2004), no. 4, 1003–1019.

[CL1] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*. Pages 33–62 in *Number Theory*, Lecture Notes in Mathematics, Vol. 1068, Springer-Verlag, Berlin, 33–62.

[CL2] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups*, in *Number Theory*, Lecture Notes in Mathematics, Vol. 1052, Springer-Verlag, Berlin, 26–36.

[Coh] P. Cohen, *The independence of the continuum hypothesis*, Proc. Nat. Acad. Sci. U.S.A, **50** (1963), 1143–1148; **51** (1964), 105–110.

[Cohn] J. Cohn, *The length of the period of simple continued fractions*, Pacific Journal of Mathematics, **71** (1977), no. 1, 21–32.

[Con1] J. B. Conrey, *L-Functions and random matrices*. Pages 331–352 in *Mathematics unlimited — 2001 and Beyond*, Springer-Verlag, Berlin, 2001.

[Con2] J. B. Conrey, *The Riemann hypothesis*, Notices of the AMS, **50** (2003), no. 3, 341–353.

[CFKRS] B. Conrey, D. Farmer, P. Keating, M. Rubinstein and N. Snaith, *Integral moments of L-functions*, preprint.

[Conw] J. H. Conway, *The weird and wonderful chemistry of audioactive decay*. Pages 173–178 in *Open Problems in Communications and Computation*, ed. T. M. Cover and B. Gopinath, Springer-Verlag, New York, 1987.

[CG] J. H. Conway and R. Guy, *The Book of Numbers*, Springer-Verlag, Berlin, 1996.

[CS] J. H. Conway and N. J. A. Sloane, *Lexicographic Codes: Error-Correcting Codes from Game Theory*, IEEE Trans. Inform. Theory, **32** (1986), no. 3, 219–235.

[Corl] R. M. Corless,*Continued fractions and chaos*. Amer. Math. Monthly **99** (1992), no. 3, 203–215.

[Cor1] Cornell University, *arXiv*, http://arxiv.org

[Cor2] Cornell University, *Project Euclid*, http://projecteuclid.org/

[CFS] I. P. Cornfeld, S. V. Fomin, and I. G. Sinai, *Ergodic Theory*, Grundlehren Der Mathematischen Wissenschaften, Springer-Verlag, Berlin, 1982.

[Da1] H. Davenport, *The Higher Arithmetic: An Introduction to the Theory of Numbers*, 7th edition, Cambridge University Press, Cambridge, 1999.

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

[Da3] H. Davenport, *On the distribution of quadratic residues (mod p)*, London Math. Soc. **6** (1931), 49–54.

[Da4] H. Davenport, *On character sums in finite fields*, Acta Math. **71** (1939), 99–121.

[DN] H. A. David and H. N. Nagaraja, *Order Statistics*, 3rd edition, Wiley Interscience, Hoboken, NJ, 2003.

[DSV] G. Davidoff, P. Sarnak, and A. Valette, *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, London Mathematical Society, Student Texts, Vol. 55, Cambridge University Press, Cambridge 2003.

[Dev] R. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd edition, Westview Press, Cambridge, MA, 2003.

[Dia] P. Diaconis, *Patterns in eigenvalues: the 70^{th} Josiah Williard Gibbs lecture*, Bulletin of the American Mathematical Society, **40** (2003), no. 2, 155–178.

[Di] T. Dimofte, *Rational shifts of linearly periodic continued fractions*, Junior Thesis, Princeton University, 2003.

[DM] E. Dueñez and S. J. Miller, *The Low Lying Zeros of a $\mathrm{GL}(4)$ and a $\mathrm{GL}(6)$ family of L-functions*, preprint.

[Du] R. Durrett, *Probability: Theory and Examples*, 2nd edition, Duxbury Press, 1996.

[Dy1] F. Dyson, *Statistical theory of the energy levels of complex systems: I, II, III*, J. Mathematical Phys., **3** (1962) 140–156, 157–165, 166–175.

[Dy2] F. Dyson, *The threefold way. Algebraic structure of symmetry groups and ensembles in quantum mechanics*, J. Mathematical Phys., **3** (1962) 1199–1215.

[Edg] G. Edgar, *Measure, Topology, and Fractal Geometry*, 2nd edition, Springer-Verlag, 1990.

[Ed] H. M. Edwards, *Riemann's Zeta Function*, Academic Press, New York, 1974.

[EST] B. Elias, L. Silberman and R. Takloo-Bighash, *On Cayley's theorem*, preprint.

[EE] W. J. Ellison and F. Ellison, *Prime Numbers*, John Wiley & Sons, New York, 1985.

[Est1] T. Estermann, *On Goldbach's problem: Proof that almost all even positive integers are sums of two primes*, Proc. London Math. Soc. Ser. 2 **44** (1938) 307–314.

[Est2] T. Estermann, *Introduction to Modern Prime Number Theory*, Cambridge University Press, Cambridge, 1961.

[Fal] K. Falconer, *Fractal Geometry: Mathematical Foundations and Applications*, 2nd edition, John Wiley & Sons, New York, 2003.

[Fef] C. Fefferman, *Pointwise convergence of Fourier series*, Ann. of Math. Ser. 2 **98** (1973), 551–571.

[Fe] W. Feller, *An Introduction to Probability Theory and Its Applications*, 2nd edition, Vol. II, John Wiley & Sons, New York, 1971.

[Fi] D. Fishman, *Closed form continued fraction expansions of special quadratic irrationals*, Junior Thesis, Princeton University, 2003.

[Fol] G. Folland, *Real Analysis: Modern Techniques and Their Applications*, 2nd edition, Pure and Applied Mathematics, Wiley-Interscience, New York, 1999.

[For] P. Forrester, *Log-gases and random matrices*, book in progress.

[Fou] E. Fouvry, *Sur la hauteur des points d'une certaine surface cubique singulière*. In *Nombre et répartition de points de hauteur bornée (Paris, 1996)*, Astérisque, (1999) no. 251, 31–49.

[FSV] P. J. Forrester, N. C. Snaith, and J. J. M. Verbaarschot, *Developments in Random Matrix Theory*. In *Random matrix theory*, J. Phys. A **36** (2003), no. 12, R1–R10.

[Fr] J. Franklin, *Mathematical Methods of Economics: Linear and Nonlinear Programming, Fixed-Point Theorem*, Springer-Verlag, New York, 1980.

[Ga] P. Garrett, *Making, Breaking Codes: An Introduction to Cryptography*, Prentice-Hall, Englewood Cliffs, NJ, 2000.

[Gau] M. Gaudin, *Sur la loi limite de l'espacement des valeurs propres d'une matrice aléatoire*, Nucl. Phys. **25** (1961) 447–458.

[Gel] A. O. Gelfond, *Transcendental and Algebraic Numbers*, Dover, New York, 1960.

[Gl] A. Gliga, *On continued fractions of the square root of prime numbers*, Junior Thesis, Princeton University, 2003.

[Gö] K. Gödel, *On Formally Undecidable Propositions of Principia Mathematica and Related Systems*, Dover, New York, 1992.

[Gol1] D. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. 3, **4** (1976), 624–663.

[Gol2] D. Goldfeld, *The Elementary proof of the Prime Number Theorem, An Historical Perspective*. Pages 179–192 in *Number Theory, New York Seminar 2003*, eds. D. and G. Chudnovsky, M. Nathanson, Springer-Verlag, New York, 2004.

[Gold] L. Goldmakher, *On the limiting distribution of eigenvalues of large random regular graphs with weighted edges*, American Institute of Mathematics Summer REU, 2003.

[GV] D. A. Goldston and R. C. Vaughan, *On the Montgomery-Hooley asymptotic formula*. Pages 117–142 in *Sieve Methods, Exponential Sums and their Applications in Number Theory*, ed. G. R. H. Greaves, G. Harman, and M. N. Huxley, Cambridge University Press, Cambridge, 1996.

[GG] M. Golubitsky and V. Guillemin, *Stable Mappings and Their Singularities*, Graduate Texts in Mathematics, Vol. 14, Springer-Verlag, New York, 1973.

[GKP] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley, Reading, MA, 1988.

[GK] A. Granville and P. Kurlberg, *Poisson statistics via the Chinese remainder theorem*, preprint.

[GT] A. Granville and T. Tucker, *It's as easy as abc*, Notices of the AMS, **49** (2002), no. 10, 224–1231.

[GZ] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[Guy] R. Guy, *Unsolved Problems in Number Theory (Problem Books in Mathematics)*, 2nd edition, Springer-Verlag, New York, 1994.

[HM] C. Hammond and S. J. Miller, *Eigenvalue spacing distribution for the ensemble of real symmetric Toeplitz matrices*, Journal of Theoretical Probability **18** (2005), no. 3, 537–566.

[HL1] G. H. Hardy and J. E. Littlewood, *A new solution of Waring's problem*, Q. J. Math. **48** (1919), 272–293.

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

[HL3] G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio Numerorum." III. On the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.

[HL4] G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio Numerorum." IV. Further researches in Waring's problem*, Math. Z., **23** (1925) 1–37.

[HW] G. H. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Oxford Science Publications, Clarendon Press, Oxford, 1995.

[HR] G. H. Hardy and S. Ramanujan, *Asymptotic formulae in combinatorial analysis*, Proc. London Math. Soc. **17** (1918), 75–115.

[Hata] R. Hata, *Improvement in the irrationality measures of π and π^2*, Proc. Japan. Acad. Ser. A Math. Sci. **68** (1992), 283–286.

[Ha] B. Hayes, *The spectrum of Riemannium*, American Scientist, **91** (2003), no. 4, 296–300.

[He] R. Heath-Brown, *The density of rational points on Cayley's cubic surface*, preprint.

[Hei] H. Heillbronn, *On the average length of a class of finite continued fractions*. In *Number Theory and Analysis (A collection of papers in honor of E. Landau)*, VEB Deutscher Verlag, Berlin, 1968.

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

[Hil] D. Hilbert, *Beweis für die Darstellbarkeit der ganzen zahlen durch eine feste Anzahl n^{ter} Potenzen (Waringsches Problem)*, Mat. Annalen **67** (1909), 281–300.

[Hi1] T. Hill, *The first-digit phenomenon*, American Scientist **86** (1996), 358–363.

[Hi2] T. Hill, *A statistical derivation of the significant-digit law*, Statistical Science **10** (1996), 354–363.

[HS] M. Hindry and J. Silverman, *Diophantine Geometry: An Introduction*, Graduate Texts in Mathematics, Vol. 201, Springer-Verlag, New York, 2000.

[HJ] K. Hrbacek and T. Jech, *Introduction to Set Theory*, Pure and Applied Mathematics, Marcel Dekker, New York, 1984.

[Hua] Hua Loo Keng, *Introduction to Number Theory*, Springer-Verlag, New York, 1982.

[HuRu] C. Hughes and Z. Rudnick, *Mock Gaussian behaviour for linear statistics of classical compact groups*, J. Phys. A **36** (2003) 2919–2932.

[Hu] J. Hull, *Options, Futures, and Other Derivatives*, 5th edition, Prentice-Hall, Englewood Cliffs, NJ, 2002.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, Vol. 84, Springer-Verlag, New York, 1990.

[Iw] H. Iwaniec, *Topics in Classical Automorphic Forms*, Graduate Studies in Mathematics, Vol. 17, AMS, Providence, RI, 1997.

[IK] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, AMS Colloquium Publications, Vol. 53, AMS, Providence, RI, 2004.

[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.

[IS1] H. Iwaniec and P. Sarnak, *Dirichlet L-functions at the central point*. Pages 941–952 in *Number Theory in Progress, (Zakopane-Kościelisko, 1997)*, Vol. 2, de Gruyter, Berlin, 1999.

[IS2] H. Iwaniec and P. Sarnak, *The non-vanishing of central values of automorphic L-functions and Landau-Siegel zeros*, Israel J. Math. **120** (2000), 155–177.

[JMRR] D. Jakobson, S. D. Miller, I. Rivin, and Z. Rudnick, *Eigenvalue spacings for regular graphs*. Pages 317–327 in *Emerging Applications of Number Theory (Minneapolis, 1996)*, The IMA Volumes in Mathematics and its Applications, Vol. 109, Springer, New York, 1999.

[J] N. Jacobson, *Basic Algebra I*, 2nd edition, W H Freeman & Co, San Francisco, 1985.

[Je] R. Jeffrey, *Formal Logic: Its Scope and Limits*, McGraw-Hill, New York, 1989.

[Ka] S. Kapnick, *Continued fraction of cubed roots of primes*, Junior Thesis, Princeton University, Fall 2002.

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

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

[KeSn] J. P. Keating and N. C. Snaith, *Random matrices and L-functions*. In *Random Matrix Theory*, J. Phys. A **36** (2003), no. 12, 2859–2881.

[Kel] D. Kelley, *Introduction to Probability*, Macmillan Publishing Company, London, 1994.

[Kh] A. Y. Khinchin, *Continued Fractions*, 3rd edition, University of Chicago Press, Chicago, 1964.

[KSS] D. Kleinbock, N. Shah, and A. Starkov,*Dynamics of subgroup actions on homogeneous spaces of Lie groups and applications to number theory*. Pages 813–930 in *Handbook of Dynamical Systems*, Vol. 1A, North-Holland, Amsterdam, 2002.

[Kn] A. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, NJ, 1992.

[Knu] D. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd edition, Addison-Wesley, MA, 1997.

[Kob1] N. Koblitz, *Why study equations over finitess fields?*, Math. Mag. **55** (1982), no. 3, 144–149.

[Kob2] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), no. 177, 203–209.

[Kob3] N. Koblitz, *A survey of number theory and cryptography*. Pages 217-239 in *Number Theory*, Trends in Mathematics, Birkhäuser, Basel, 2000.

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

[KonMi] A. Kontorovich and S. J. Miller, *Benford's law, values of L-functions and the $3x+1$ problem*, Acta Arith. **120** (2005), 269–297.

[KonSi] A. Kontorovich and Ya. G. Sinai, *Structure theorem for (d,g,h)-maps*, Bull. Braz. Math. Soc. (N.S.) 33 (2002), no. 2, 213–224.

[Kor] A. Korselt, *Probléme chinois*, L'intermédiaire math. **6** (1899), 143–143.
[Kos] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, Wiley-Interscience, New York, 2001
[Kua] F. Kuan, *Digit distribution in the continued fraction of* $\zeta(n)$, Junior Thesis, Princeton University, Fall 2002.
[KN] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, John Wiley & Sons, New York, 1974.
[KR] P. Kurlberg and Z. Rudnick, *The distribution of spacings between quadratic residues*, Duke Math. J. **100** (1999), no. 2, 211–242.
[Ku] R. Kuzmin, *Ob odnoi zadache Gaussa*, Doklady Akad. Nauk, Ser. A (1928), 375–380.
[Lag1] J. Lagarias, *The* $3x+1$ *problem and its generalizations*. Pages 305-334 in *Organic mathematics (Burnaby, BC, 1995)*, CMS Conf. Proc., vol. 20, AMS, Providence, RI, 1997.
[Lag2] J. Lagarias, *The 3x+1 problem: An annotated bibliography*, preprint.
[LaSo] J. Lagarias and K. Soundararajan, *Benford's Law for the* $3x+1$ *function*, preprint.
[La1] S. Lang, *Diophantine Geometry*, Interscience Publishers, New York, 1962.
[La2] S. Lang, *Introduction to Diophantine Approximations*, Addison-Wesley, Reading, MA, 1966.
[La3] S. Lang, *Undergraduate Algebra*, 2nd edition, Springer-Verlag, New York, 1986.
[La4] S. Lang, *Calculus of Several Variables*, Springer-Verlag, New York, 1987.
[La5] S. Lang, *Undergraduate Analysis*, 2nd edition, Springer-Verlag, New York, 1997.
[La6] S. Lang, *Complex Analysis*, Graduate Texts in Mathematics, Vol. 103, Springer-Verlag, New York, 1999.
[LT] S. Lang and H. Trotter, *Continued fractions for some algebraic numbers*, J. Reine Angew. Math. **255** (1972), 112–134.
[LF] R. Larson and B. Farber, *Elementary Statistics: Picturing the World*, Prentice-Hall, Englewood Cliffs, NJ, 2003.
[LP] R. Laubenbacher and D. Pengelley, *Gauss, Eisenstein, and the "third" proof of the quadratic reciprocity theorem: Ein kleines Schauspiel*, Math. Intelligencer 16 (1994), no. 2, 67–72.
[Law1] J. Law, *Kuzmin's theorem on algebraic numbers*, Junior Thesis, Princeton University, Fall 2002.
[Law2] J. Law, *The circle method on the binary goldbach conjecture*, Junior Thesis, Princeton University, Spring 2003.
[Leh] R. Lehman, *First order spacings of random matrix eigenvalues*, Junior Thesis, Princeton University, Spring 2000.
[LS] H. Lenstra and G. Seroussi, *On hats and other covers*, 2002, preprint.
[Le] P. Lévy, *Sur les lois de probabilité dont dependent les quotients complets et incomplets d'une fraction continue*, Bull. Soc. Math. **57** (1929), 178–194.
[Lidl] R. Lidl, *Mathematical aspects of cryptanalysis*. Pages 86–97 in *Number Theory and Cryptography (Sydney, 1989)*, London Mathematical Society Lecture Note Series, vol. 154, Cambridge University Press, Cambridge, 1990.
[Li] R. Lipshitz, *Numerical results concerning the distribution of* $\{n^2\alpha\}$, Junior Thesis, Princeton University, Spring 2000.
[Liu] Y. Liu, *Statistical behavior of the eigenvalues of random matrices*, Junior Thesis, Princeton University, Spring 2000.
[Mah] K. Mahler, *Arithmetische Eigenschaften einer Klasse von Dezimalbrüchen*, Amsterdam Proc. Konin. Neder. Akad. Wet. **40** (1937), 421–428.
[Ma] E. S. Mahmoodian, *Mathematical Olympiads in Iran*, Vol. I, Sharif University Press, Tehran, Iran, 2002.
[Man] B. Mandelbrot, *The Fractal Geometry of Nature*, W. H. Freeman, New York, 1982.
[Mar] J. Marklof, *Almost modular functions and the distribution of* n^2x *modulo one*, Int. Math. Res. Not. (2003), no. 39, 2131–2151.
[MaMc] R. Martin and W. McMillen, *An elliptic curve over* $\mathbb{Q}$ *with rank at least* 24, Number Theory Listserver, May 2000.
[MMS] A. Massey, S. J. Miller, and J. Sinsheimer, *Eigenvalue spacing distribution for the ensemble of real symmetric palindromic Toeplitz matrices*, preprint.
[Maz1] B. Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math. **47** (1977), 33–186.
[Maz2] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.
[Maz3] B. Mazur, *Number Theory as Gadfly*, Amer. Math. Monthly, **98** (1991), 593–610.
[McK] B. McKay, *The expected eigenvalue distribution of a large regular graph*, Linear Algebra Appl. **40** (1981), 203–216.
[MW] B. McKay and N. Wormald, *The degree sequence of a random graph. I. The models*, Random Structures Algorithms **11** (1997), no. 2, 97–117.
[Meh1] M. Mehta, *On the statistical properties of level spacings in nuclear spectra*, Nucl. Phys. **18** (1960), 395–419.
[Meh2] M. Mehta, *Random Matrices*, 2nd edition, Academic Press, Boston, 1991.
[Met] N. Metropolis, *The beginning of the Monte Carlo method*, Los Alamos Science, No. 15, Special Issue (1987), 125–130.

[MU] N. Metropolis and S. Ulam, *The Monte Carlo method*, J. Amer. Statist. Assoc. **44** (1949), 335–341.

[Mic1] M. Michelini, *Independence of the digits of continued fractions*, Junior Thesis, Princeton University, Fall 2002.

[Mic2] M. Michelini, *Kuzmin's extraordinaty zero measure set*, Senior Thesis, Princeton University, Spring 2004.

[Mi1] N. Miller, *Various tendencies of non-Poissonian distributions along subsequences of certain transcendental numbers*, Junior Thesis, Princeton University, Fall 2002.

[Mi2] N. Miller, *Distribution of eigenvalue spacings for band-diagonal matrices*, Junior Thesis, Princeton University, Spring 2003.

[Mill] S. D. Miller, *A simpler way to show $\zeta(3)$ is irrational*, preprint.

[Mil1] S. J. Miller, 1*- and* 2*-level densities for families of elliptic curves: Evidence for the underlying group symmetries*, Compositio Mathematica **140** (2004), no. 4, 952–992.

[Mil2] S. J. Miller, *Density functions for families of Dirichlet characters*, preprint.

[Mil3] S. J. Miller, *The arithmetic mean and geometric inequality*, Class Notes from Math 187/487, The Ohio State University, Fall 2003.

[Mil4] S. J. Miller, *Differentiating identities*, Class Notes from Math 162: Statistics, Brown University, Spring 2005.

[Mil5] S. J. Miller, *The Pythagorean won-loss formula in baseball*, preprint.

[Mil6] S. J. Miller, *Investigations of zeros near the central point of elliptic curve L-functions*, to appear in Experimental Mathematics.

[Mil7] S. J. Miller, *Die battles and order statistics*, Class Notes from Math 162: Statistics, Brown University, Spring 2006.

[MN] S. J. Miller and M. Nigrini, *Differences of independent variables and almost Benford behavior*, preprint.

[M] V. Miller, *Use of elliptic curves in cryptography*. Pages 417–426 in *Advances in cryptology – CRYPTO '85 (Santa Barbara, CA, 1985)*, Lecture Notes in Computer Science, Vol. 218, Springer-Verlag, Berlin, 1986.

[Milne] J. S. Milne, *Elliptic Curves*, course notes.

[Min] S. Minteer, *Analysis of Benford's law applied to the $3x+1$ problem*, Number Theory Working Group, The Ohio State University, 2004.

[Mon1] H. Montgomery, *Primes in arithmetic progression*, Michigan Math. J. **17** (1970), 33–39.

[Mon2] H. Montgomery, *The pair correlation of zeros of the zeta function*. Pages 181–193 in *Analytic Number Theory*, Proceedings of Symposia in Pure Mathematics, vol. 24, AMS, Providence, RI, 1973.

[MoMc] D. Moore and G. McCabe, *Introduction to the Practice of Statistics*, W. H. Freeman and Co., London, 2003.

[MS] H. Montgomery and K. Soundararajan, *Beyond pair correlation*. Pages 507–514 in *Paul Erdös and His Mathematics, I (Budapest, 1999)*, Bolyai Society Mathematical Studies, Vol. 11, János Bolyai Math. Soc., Budapest, 2002.

[Moz1] C. J. Mozzochi, *An analytic sufficiency condition for Goldbach's conjecture with minimal redundancy*, Kyungpook Math. J. **20** (1980), no. 1, 1–9.

[Moz2] C. J. Mozzochi, *The Fermat Diary*, AMS, Providence, RI, 2000.

[Moz3] C. J. Mozzochi, *The Fermat Proof*, Trafford Publishing, Victoria, 2004.

[Mu1] R. Murty, *Primes in certain arithmetic progressions*, Journal of the Madras University, (1988), 161–169.

[Mu2] R. Murty, *Problems in Analytic Number Theory*, Springer-Verlag, New York, 2001.

[MM] M. R. Murty and V. K. Murty, *Non-Vanishing of L-Functions and Applications*, Progress in Mathematics, vol. 157, Birkhäuser, Basel, 1997.

[NS] K. Nagasaka and J. S. Shiue, *Benford's law for linear recurrence sequences*, Tsukuba J. Math. **11** (1987), 341–351.

[Nar] W. Narkiewicz, *The Development of Prime Number Theory*, Springer Monographs in Mathematics, Springer-Verlag, New York, 2000.

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

[NT] J. von Neumann and B. Tuckerman, *Continued fraction expansion of* $2^{1/3}$, Math. Tables Aids Comput. **9** (1955), 23–24.

[Ni1] T. Nicely, *The pentium bug*, http://www.trnicely.net/pentbug/pentbug.html

[Ni2] T. Nicely, *Enumeration to* 10^{14} *of the Twin Primes and Brun's Constant*, Virginia J. Sci. **46** (1996), 195–204.

[Nig1] M. Nigrini, *Digital Analysis and the Reduction of Auditor Litigation Risk*. Pages 69–81 in *Proceedings of the 1996 Deloitte & Touche / University of Kansas Symposium on Auditing Problems*, ed. M. Ettredge, University of Kansas, Lawrence, KS, 1996.

[Nig2] M. Nigrini, *The Use of Benford's Law as an Aid in Analytical Procedures*, Auditing: A Journal of Practice & Theory, **16** (1997), no. 2, 52–67.

[NZM] I. Niven, H. Zuckerman, and H. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition, John Wiley & Sons, New York, 1991.

[Nov] T. Novikoff, *Asymptotic behavior of the random* 3*-regular bipartite graph*, Undergraduate Mathematics Laboratory report, Courant Institute, NYU, 2002.

[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*. Pages 139–144 in *Procreedings of the Conference on Dynamical, Spectral and Arithmetic Zeta Functions*, ed. M. van Frankenhuysen and M. L. Lapidus, Contemporary Mathematics Series, AMS, Providence, RI, 2001.

[Ok] T. Okano, *A note on the transcendental continued fractions*, Tokyo J. Math, **10** (1987), no. 1, 151–156.

[Ol] T. Oliveira e Silva, *Verification of the Goldbach conjecture up to* $6 \cdot 10^{16}$, NMBRTHRY@listserv.nodak.edu mailing list, Oct. 3, 2003, http://listserv.nodak.edu/scripts/wa.exe?A2=ind0310&L=nmbrthry&P=168 and http://www.ieeta.pt/∼tos/goldbach.html

[Ols] L. Olsen, *Extremely non-normal continued fractions*, Acta Arith. **108** (2003), no. 2, 191–202.

[vdP1] A. van der Poorten, *An introduction to continued fractions*. Pages 99-138 in *Diophantine Analysis (Kensington, 1985)*, London Mathematical Society Lecture Note Series, Vol. 109, Cambridge University Press, Cambridge, 1986.

[vdP2] A. van der Poorten, *Notes on continued fractions and recurrence sequences*. Pages 86–97 in *Number theory and cryptography (Sydney, 1989)*, London Mathematical Society Lecture Note Series, Vol. 154, Cambridge University Press, Cambridge, 1990.

[vdP3] A. van der Poorten, *Continued fractions of formal power series*. Pages 453–466 in *Advances in Number Theory (Kingston, ON, 1991)*, Oxford Science Publications, Oxford University Press, New York, 1993.

[vdP4] A. van der Poorten, *Fractions of the period of the continued fraction expansion of quadratic integers*, Bull. Austral. Math. Soc. **44** (1991), no. 1, 155–169.

[vdP5] A. van der Poorten, *Continued fraction expansions of values of the exponential function and related fun with continued fractions*, Nieuw Arch. Wisk. (4) **14** (1996), no. 2, 221–230.

[vdP6] A. van der Poorten, *Notes on Fermat's Last Theorem*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Wiley-Interscience, New York, 1996.

[PS1] A. van der Poorten and J. Shallit, *Folded continued fractions*, J. Number Theory **40** (1992), no. 2, 237–250.

[PS2] A. van der Poorten and J. Shallit, *A specialised continued fraction*, Canad. J. Math. **45** (1993), no. 5, 1067–1079.

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

[Py] R. Pyke, *Spacings*, J. Roy. Statist. Soc. Ser. B **27** (1965), 395–449.

[QS1] R. Qian and D. Steinhauer, *Rational relation conjectures*, Junior Thesis, Princeton University, Fall 2003.

[QS2] R. Qian and D. Steinhauer, *Eigenvalues of weighted random graphs*, Junior Thesis, Princeton University, Spring 2003.

[Rai] R. A. Raimi, *The first digit problem*, Amer. Math. Monthly **83** (1976), no. 7, 521–538.

[Ra] K. Ramachandra, *Lectures on Transcendental Numbers*, Ramanujan Institute, Madras, 1969.

[Re] F. Reif, *Fundamentals of Statistical and Thermal Physics*, McGraw-Hill, New York, 1965.

[Ric] P. Richter, *An investigation of expanders and ramanujan graphs along random walks of cubic bipartite graphs*, Junior Thesis, Princeton University, Spring 2001.

[RDM] R. D. Richtmyer, M. Devaney, and N. Metropolis, *Continued fraction of algebraic numbers*, Numer. Math. **4** (1962), 68–84.

[Ri] G. F. B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monatsber. Königl. Preuss. Akad. Wiss. Berlin, Nov. 1859, 671–680 (see [Ed] for an English translation).

[RSA] R. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Comm. ACM **21** (1978), 120–126.

[Roc] D. Rockmore, *Stalking the Riemann Hypothesis: The Quest to Find the Hidden Law of Prime Numbers*, Pantheon, New York, 2005.

[Ro] K. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 1–20.

[Rub1] M. Rubinstein, *A simple heuristic proof of Hardy and Littlewood's conjecture B*, Amer. Math. Monthly **100** (1993), no. 5, 456–460.

[Rub2] M. Rubinstein, *Low-lying zeros of* L*-functions and random matrix theory*, Duke Math. J. **109** (2001), no. 1, 147–181.

[RubSa] M. Rubinstein and P. Sarnak, *Chebyshev's bias*, Experiment. Math. **3** (1994), no. 3, 173–197.

[Rud] W. Rudin, *Principles of Mathematical Analysis*, 3rd edition, International Series in Pure and Applied Mathematics, McGraw-Hill, New York, 1976.

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

[RS2] Z. Rudnick and P. Sarnak, *The pair correlation function of fractional parts of polynomials*, Comm. Math. Phys. **194** (1998), no. 1, 61–70.

[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.
[RZ1] Z. Rudnick and A. Zaharescu, *A metric result on the pair correlation of fractional parts of sequences*, Acta Arith. **89** (1999), no. 3, 283–293.
[RZ2] Z. Rudnick and A. Zaharescu, *The distribution of spacings between fractional parts of lacunary sequences*, Forum Math. **14** (2002), no. 5, 691–712.
[Sar] P. Sarnak *Some applications of modular forms*, Cambridge Trusts in Mathemetics, Vol. 99, Cambridge University Press, Cambridge, 1990.
[Sch] D. Schmidt, *Prime Spacing and the Hardy-Littlewood Conjecture B*, Junior Thesis, Princeton University, Spring 2001.
[Sc] P. Schumer, *Mathematical Journeys*, Wiley-Interscience, John Wiley & Sons, New York, 2004.
[Se] J. P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1996.
[Sh] A. Shidlovskii, *Transcendental Numbers*, Walter de Gruyter & Co., New York, 1989.
[ShTa] J. A. Shohat and J. D. Tamarkin, *The Problem of Moments*, AMS, Providence, RI, 1943.
[Sil1] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Vol. 106, Springer-Verlag, New York, 1986.
[Sil2] J. Silverman, *A Friendly Introduction to Number Theory*, 2nd edition, Prentice-Hall, Englewood Cliffs, NJ, 2001.
[ST] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.
[Si] B. Simon, *The classical moment problem as a self-adjoint finite difference operator*, Adv. Math. **137** (1998), no. 1, 82–203.
[SM] S. Simon and A. Moustakas, *Eigenvalue density of correlated complex random Wishart matrices*, Bell Labs Technical Memo, 2004.
[Sk] S. Skewes, *On the difference $\pi(x) - \mathrm{Li}(x)$*, J. London Math. Soc. **8** (1933), 277–283.
[Sl] N. Sloane, *On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/$\sim$njas/sequences/Seis.html
[Sn] N. Snaith, *Derivatives of random matrix characteristic polynomials with applications to elliptic curves*, preprint.
[SS1] E. Stein and R. Shakarchi, *Fourier Analysis: An Introduction*, Princeton University Press, Princeton, NJ, 2003.
[SS2] E. Stein and R. Shakarchi, *Complex Analysis*, Princeton University Press, Princeton, NJ, 2003.
[SS3] E. Stein and R. Shakarchi, *Real Analysis: Measure Theory, Integration, and Hilbert Spaces*, Princeton University Press, Princeton, NJ, 2005.
[StTa] I. Stewart and D. Tall, *Algebraic Number Theory*, 2nd edition, Chapman & Hall, London, 1987.
[St] Strang, *Linear Algebra and Its Applications*, 3rd edition, Wellesley-Cambridge Press, Wellesley, MA 1998.
[Str] K. Stromberg, *The Banach-Tarski paradox*, Amer. Math. Monthly **86** (1979), no. 3, 151–161.
[Sz] P. Szüsz, *On the length of continued fractions representing a rational number with given denominator*, Acta Arithmetica **37** (1980), 55–59.
[Ta] C. Taylor, *The Gamma function and Kuzmin's theorem*, Junior Thesis, Princeton University, Fall 2002.
[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995), 553–572.
[TrWi] C. Tracy and H. Widom, *Correlation functions, cluster functions, and spacing distributions for random matrices*, J. Statist. Phys., **92** (1998), no. 5–6, 809–835.
[Te] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press, Cambridge, 1995.
[Ti] E. C. Titchmarsh, *The Theory of the Riemann Zeta-function*, revised by D. R. Heath-Brown, Oxford University Press, Oxford, 1986.
[Va] R. C. Vaughan, *On a variance associated with the distribution of primes in arithmetic progression*, Proc. London Math. Soc. (3) **82** (2001), 533–553.
[VW] R. C. Vaughan and T. D. Wooley, *Waring's problem: a survey*. Pages 301–340 in *Number Theory for the Millennium, III (Urbana, IL, 2000)*, A. K. Peters, Natick, MA, 2002.
[Vin1] I. Vinogradov, *Representation of an odd number as the sum of three primes*, Doklady Akad. Nauk SSSR, **15** (1937), no. 6–7, 291–294.
[Vin2] I. Vinogradov, *Some theorems concerning the theory of primes*, Mat. Sbornik, **2** (1937), no. 44, 179–195.
[Vo] A. Voros, *A sharpening of Li's criterion for the Riemann hypothesis*, preprint.
[VG] W. Voxman and R. Goetschel, Jr., *Advanced Calculus*, Mercer Dekker, New York, 1981.
[Wa] L. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman & Hall / CRC, New York, 2003.
[Wed] S. Wedeniwski, *ZetaGrid*, http://www.zetagrid.net
[Wei1] A. Weil, *Numbers of Solutions of Equations in Finite Fields*, Bull. Amer. Math. Soc. **14** (1949), 497–508.
[Wei2] A. Weil, *Prehistory of the zeta-function*. Pages 1–9 in *Number Theory, Trace Formulas and Discrete Groups (Oslo, 1987)*, Academic Press, Boston, 1989.
[Weir] B. Weir, *The local behavior of Germain primes*, Undergraduate Mathematics Laboratory report, Courant Institute, NYU, 2002.

[We] E. Weisstein, *MathWorld — A Wolfram Web Resource*, http://mathworld.wolfram.com

[Weyl] H. Weyl, *The Classical Groups: Their Invariants and Representations*, Princeton University Press, Princeton, NJ, 1946.

[Wh] E. Whittaker, *A Treatise on the Analytical Dynamics of Particles and Rigid Bodies: With an Introduction to the Problem of Three Bodies*, Dover, New York, 1944.

[WW] E. Whittaker and G. Watson, *A Course of Modern Analysis*, 4th edition, Cambridge University Press, Cambridge, 1996.

[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, *Characteristic vectors of bordered matrices with infinite dimensions*, Ann. of Math. **2** (1955), no. 62, 548–564.

[Wig3] E. Wigner, *Statistical Properties of real symmetric matrices*. Pages 174–184 in *Canadian Mathematical Congress Proceedings*, University of Toronto Press, Toronto, 1957.

[Wig4] E. Wigner, *Characteristic vectors of bordered matrices with infinite dimensions. II*, Ann. of Math. Ser. 2 **65** (1957), 203–207.

[Wig5] E. Wigner, *On the distribution of the roots of certain symmetric matrices*, Ann. of Math. Ser. 2 **67** (1958), 325–327.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), 443–551.

[Wilf] H. Wilf, *Algorithms and Complexity*, 2nd edition, A. K. Peters, Natick, MA, 2002.

[Wir] E. Wirsing, *On the theorem of Gauss-Kuzmin-Lévy and a Frobenius-type theorem for function spaces*, Acta Arith. **24** (1974) 507–528.

[Wis] J. Wishart, *The generalized product moment distribution in samples from a normal multivariate population*, Biometrika **20 A** (1928), 32–52.

[Wor] N. C. Wormald, *Models of random regular graphs*. Pages 239–298 in *Surveys in combinatorics, 1999 (Canterbury)* London Mathematical Society Lecture Note Series, vol. 267, Cambridge University Press, Cambridge, 1999.

[Wo] T. Wooley, *Large improvements in Waring's problem*, Ann. of Math. (2), **135** (1992), no. 1, 131–164.

[Za] I. Zakharevich, *A generalization of Wigner's law*, preprint.

[Zu] W. Zudilin, *One of the numbers* $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ *is irrational*, Uspekhi Mat. Nauk **56** (2001), 149-150.

[Zy] A. Zygmund, *Trigonometrical Series*, vols. I and II, Cambridge University Press, Cambridge, 1968.

Index