Rational Numbers: Everywhere but Nowhere
From Ancient Mathematics to Modern Cryptography

Vu Hung Nguyen

2025-11-21

Abstract

This document explores one of the most counter-intuitive properties in mathematics: the paradoxical nature of rational numbers. While rational numbers (fractions like $\frac{1}{2}$, $\frac{5}{9}$) are *dense* in the real numbers—meaning you can find one in any interval, no matter how small—they essentially take up *no space* on the number line. Through the lens of measure theory, we discover that the total "length" of all rational numbers combined is actually zero, despite their infinite abundance.

This paradox, often described as "everywhere but nowhere," has profound implications not only in pure mathematics but also in modern cryptography. The concepts of density, countability, and measure zero provide the mathematical foundation for understanding random number generation, lattice-based cryptography, and cryptographic attacks such as Wiener's attack on RSA.

Target Audience: This document is designed for maths enthusiasts and cryptography practitioners, with content structured to be accessible at multiple levels—from high school students exploring the basics to researchers investigating advanced cryptographic applications.

Contents

1 Introduction to Rational Numbers **4**
- 1.1 What Are Rational Numbers? . . . 4
- 1.2 Document Roadmap . . . 4
- 1.3 Historical Review: From Ancient Greek Mathematics to Modern Post-Quantum Computing . . . 5
  - 1.3.1 Ancient Greek Mathematics . . . 5
  - 1.3.2 Evolution of Number Systems . . . 5
  - 1.3.3 Modern Applications: Post-Quantum Cryptography . . . 6
- 1.4 Basic Properties of Rational Numbers . . . 6
- 1.5 Notation . . . 7

2 Density (Everywhere) **7**
- 2.1 The Density Property . . . 8
- 2.2 Visualizing Density . . . 8
- 2.3 Constructive Proof: Finding Rationals Between Reals . . . 9

3 Countability **10**
3.1 Countable Sets . . . 10
3.2 Cantor's Enumeration of Rational Numbers . . . 10
3.3 Uncountability of Real Numbers . . . 11
3.4 Paradoxes of Infinite Sets . . . 12
3.5 Implications of Countability . . . 15

4 Measure Zero (Nowhere) **15**
4.1 Introduction to Lebesgue Measure . . . 16
4.2 Countable Sets Have Measure Zero . . . 18
4.3 The Rational Numbers Have Measure Zero . . . 18
4.4 Properties of Measure Zero . . . 19

5 The Paradox: Everywhere but Nowhere **19**
5.1 Understanding the Paradox . . . 19
5.2 The Microscope Analogy . . . 20
5.3 Why Both Can Be True . . . 20
5.4 The Complete Picture . . . 21

6 Probability Implications **21**
6.1 Geometric Probability . . . 22
6.2 Almost Surely . . . 22
6.3 Implications for Random Number Generation . . . 23
6.4 The Intuition . . . 24

7 Cryptography Connections: An Overview **24**
7.1 Why Rational Numbers Matter in Cryptography . . . 24
7.2 Key Cryptographic Applications . . . 25
7.2.1 1. Random Number Generation and Key Security . . . 25
7.2.2 2. Lattice-Based Cryptography . . . 25
7.2.3 3. Wiener's Attack on RSA . . . 25
7.2.4 Security Proofs and Distinguishing Sets . . . 26
7.3 The Mathematical Bridge . . . 26
7.4 Organization of Remaining Sections . . . 26

8 Random Number Generation and Key Security **27**
8.1 Keyspaces and Weak Keys . . . 27
8.2 Weak Keys as a Measure Zero Set . . . 27
8.3 Probability of Generating a Weak Key . . . 28
8.4 Implications for Cryptographic Security . . . 28
8.4.1 Security Guarantees . . . 28
8.4.2 Random Number Generation Requirements . . . 29
8.5 The Analogy to Rational Numbers . . . 29
8.6 Practical Considerations . . . 30

9 Lattice-Based Cryptography and Diophantine Approximation **30**
9.1 Introduction to Lattices . . . 30
9.2 Diophantine Approximation . . . 31
9.3 Continued Fractions . . . 32

9.4 Connection to Lattice Problems . . . 32
9.5 Cryptographic Applications . . . 33
9.5.1 Learning With Errors (LWE) . . . 33
9.5.2 Post-Quantum Security . . . 33
9.6 The Rational Number Connection . . . 34

10 Wiener's Attack on RSA: A Concrete Example 34
10.1 RSA Key Generation Recap . . . 34
10.2 The Vulnerability: Small Private Exponent . . . 35
10.3 The Mathematical Foundation . . . 35
10.4 The Attack Algorithm . . . 36
10.5 Why This Works . . . 36
10.6 Continued Fraction Approximation Process . . . 37
10.7 Defenses Against Wiener's Attack . . . 37
10.8 Connection to Rational Number Properties . . . 38

11 Problems: Mathematical and Cryptographic Challenges 38
11.1 Level 1: High School Accessible . . . 38
11.2 Level 2: More Depth . . . 39
11.3 Level 3: Crypto + Maths High Level . . . 40
11.4 Level 4: Research Level . . . 41
11.5 Additional Challenge Problems . . . 42
11.6 Further Reading and Exploration . . . 42

12 Conclusion 43
12.1 Key Takeaways . . . 43
12.1.1 Mathematical Foundations . . . 43
12.1.2 Cryptographic Connections . . . 43
12.2 The Unifying Theme . . . 44
12.3 Implications for Cryptography . . . 44
12.4 Future Directions . . . 45
12.5 Final Thoughts . . . 45

13 Glossary 46
13.1 Mathematical Terms . . . 46
13.2 Cryptographic Terms . . . 46

Part I: Mathematical Foundations

1 Introduction to Rational Numbers

1.1 What Are Rational Numbers?

Definition 1.1: Rational Numbers

A **rational number** is any number that can be expressed as the ratio of two integers, where the denominator is not zero. Formally, the set of rational numbers is:

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\}$$

where $\mathbb{Z}$ denotes the set of integers.

Rational numbers include familiar fractions like $\frac{1}{2}$, $\frac{3}{4}$, and $\frac{22}{7}$, as well as integers (which can be written as $\frac{n}{1}$) and terminating or repeating decimals (e.g., $0.5 = \frac{1}{2}$, $0.\overline{3} = \frac{1}{3}$).

Example 1.2

Examples of rational numbers:

- $\frac{1}{2} = 0.5$ (terminating decimal)
- $\frac{1}{3} = 0.\overline{3}$ (repeating decimal)
- $\frac{22}{7} \approx 3.142857...$ (approximation of π)
- $-5 = \frac{-5}{1}$ (integer)
- $0 = \frac{0}{1}$ (zero)

1.2 Document Roadmap

This document is organized into three main parts, designed to guide readers from fundamental mathematical concepts to advanced cryptographic applications:

- **Part I: Mathematical Foundations** (Sections 1–5) introduces rational numbers, explores their density and countability properties, establishes measure theory concepts, and reconciles the "everywhere but nowhere" paradox. This part is accessible to readers with high school mathematics background.
- **Part II: Cryptographic Applications** (Sections 6–10) connects the mathematical properties of rational numbers to modern cryptography, covering probability implications, random number generation, lattice-based cryptography, and Wiener's attack on RSA. This part requires more advanced mathematical and cryptographic knowledge.
- **Part III: Practice and Synthesis** (Sections 11–12) provides problems at various difficulty levels (from high school to research level) and concludes with key takeaways

and future directions.

Target Audience Levels:

- **Level 1 (High School Accessible)**: Sections 1–3
- **Level 2 (More Depth)**: Sections 4–6
- **Level 3 (Crypto + Maths High Level)**: Sections 7–10
- **Level 4 (Research Level)**: Section 11 problems

1.3 Historical Review: From Ancient Greek Mathematics to Modern Post-Quantum Computing

The study of rational numbers has a rich history spanning millennia, from ancient mathematical discoveries to cutting-edge cryptographic applications.

1.3.1 Ancient Greek Mathematics

The ancient Greeks made fundamental contributions to number theory. Pythagoras and his followers discovered that not all numbers could be expressed as ratios of integers—the discovery of irrational numbers (like $\sqrt{2}$) was revolutionary and initially disturbing to their worldview. The Euclidean algorithm, developed around 300 BCE, provided a method to find the greatest common divisor of two integers, which is essential for working with rational numbers in their simplest form.

1.3.2 Evolution of Number Systems

The development of number systems followed a natural progression:

1. **Natural Numbers ($\mathbb{N}$)**: The counting numbers $1, 2, 3, \ldots$ used by ancient civilizations for basic arithmetic and counting.
2. **Integers ($\mathbb{Z}$)**: The extension to include zero and negative numbers, enabling subtraction without restrictions. This was formalized by mathematicians like Brahmagupta (7th century CE).
3. **Rational Numbers ($\mathbb{Q}$)**: Fractions and ratios, allowing division to be meaningful for any pair of integers (except division by zero). The Greeks extensively studied these.
4. **Real Numbers ($\mathbb{R}$)**: The completion of the rationals, including irrational numbers like $\sqrt{2}$, π, and e. This was rigorously developed in the 19th century by mathematicians like Dedekind and Cantor.
5. **Complex Numbers ($\mathbb{C}$)**: Numbers of the form $a + bi$ where $i^2 = -1$, extending the reals to solve equations like $x^2 + 1 = 0$. First systematically studied by Cardano and Bombelli in the 16th century.

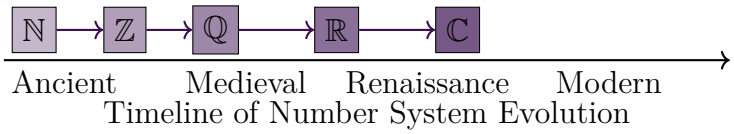


Figure 1: Evolution of number systems from natural numbers to complex numbers

1.3.3 Modern Applications: Post-Quantum Cryptography

In the 21st century, rational numbers and their properties have found crucial applications in cryptography, particularly in the development of post-quantum cryptographic systems. Lattice-based cryptography, which relies on the hardness of problems involving rational approximations, is one of the leading candidates for secure communication in the quantum computing era.

The connection between rational numbers and cryptography stems from:

- **Diophantine Approximation**: Finding rational numbers close to irrational numbers, which underlies lattice problems
- **Measure Zero Properties**: Understanding that "weak" cryptographic keys form a set of measure zero, ensuring security
- **Countability**: Distinguishing between countable and uncountable sets in security proofs

1.4 Basic Properties of Rational Numbers

Theorem 1.3: Closure Properties

The set of rational numbers $\mathbb{Q}$ is closed under addition, subtraction, multiplication, and division (by non-zero rationals). That is, if $a, b \in \mathbb{Q}$ and $b \neq 0$, then:

$$\begin{aligned} a + b &\in \mathbb{Q} \\ a - b &\in \mathbb{Q} \\ a \cdot b &\in \mathbb{Q} \\ \frac{a}{b} &\in \mathbb{Q} \end{aligned}$$

Proof. If $a = \frac{p}{q}$ and $b = \frac{r}{s}$ where $p, q, r, s \in \mathbb{Z}$ and $q, s \neq 0$, then:

$$\begin{aligned} a + b &= \frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs} \in \mathbb{Q} \\ a \cdot b &= \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} \in \mathbb{Q} \end{aligned}$$

Similar arguments hold for subtraction and division. □

Remark 1.4

The closure properties ensure that rational numbers form a *field*, making them suitable for algebraic operations without leaving the set. This property is fundamental to their use in cryptography, where operations must remain within well-defined mathematical structures.

1.5 Notation

Throughout this document, we use the following mathematical notation:

$\mathbb{N}$ The set of natural numbers: $\{1, 2, 3, \ldots\}$

$\mathbb{Z}$ The set of integers: $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{Q}$ The set of rational numbers: $\{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$

$\mathbb{R}$ The set of real numbers

$\mathbb{C}$ The set of complex numbers

μ Lebesgue measure

$\mu(A)$ The Lebesgue measure of set A

$P(\cdot)$ Probability function

$\gcd(a, b)$ Greatest common divisor of a and b

$\phi(n)$ Euler's totient function

$|A|$ Cardinality (size) of set A

$\in$ Element of (membership)

$\subseteq$ Subset of

$\cup$ Union of sets

$\cap$ Intersection of sets

$\setminus$ Set difference

$\approx$ Approximately equal to

$\equiv$ Congruent to (modular arithmetic)

2 Density (Everywhere)

The property of *density* is what makes rational numbers seem to be "everywhere" on the number line. This section explores this fundamental property and its implications.

2.1 The Density Property

Definition 2.1: Dense Set

A set $A \subseteq \mathbb{R}$ is said to be **dense** in $\mathbb{R}$ if for any two distinct real numbers $a < b$, there exists an element $x \in A$ such that $a < x < b$.

In other words, a dense set has elements in every interval, no matter how small. The rational numbers have this remarkable property.

Theorem 2.2: Density of Rational Numbers

The set of rational numbers $\mathbb{Q}$ is dense in $\mathbb{R}$. That is, between any two distinct real numbers, there exists a rational number.

Proof. Let $a, b \in \mathbb{R}$ with $a < b$. We need to show there exists $r \in \mathbb{Q}$ such that $a < r < b$.

Since $b - a > 0$, by the Archimedean property, there exists a positive integer n such that $n(b - a) > 1$, which means $b - a > \frac{1}{n}$.

Now consider the set of integers m such that $m > na$. By the Archimedean property, this set is non-empty. Let m_0 be the smallest such integer. Then:

$$m_0 - 1 \leq na < m_0$$

Dividing by n:

$$\frac{m_0 - 1}{n} \leq a < \frac{m_0}{n}$$

Since $m_0 \leq na + 1 < nb + 1$ and $na < m_0$, we have:

$$a < \frac{m_0}{n} \leq a + \frac{1}{n} < a + (b - a) = b$$

Therefore, $r = \frac{m_0}{n}$ is a rational number satisfying $a < r < b$. □

Corollary 2.3

Between any two distinct rational numbers, there are infinitely many rational numbers.

Proof. If $r_1 < r_2$ are rational numbers, by the density theorem, there exists a rational r_3 such that $r_1 < r_3 < r_2$. Applying the theorem again, we can find rationals $r_4, r_5, \ldots$ between r_1 and r_3, and between r_3 and r_2, and so on. This process can be repeated infinitely many times. □

2.2 Visualizing Density

The density property means that no matter how small an interval you choose on the real number line, it will always contain rational numbers. This is illustrated in the following figure, which shows multiple levels of zooming.

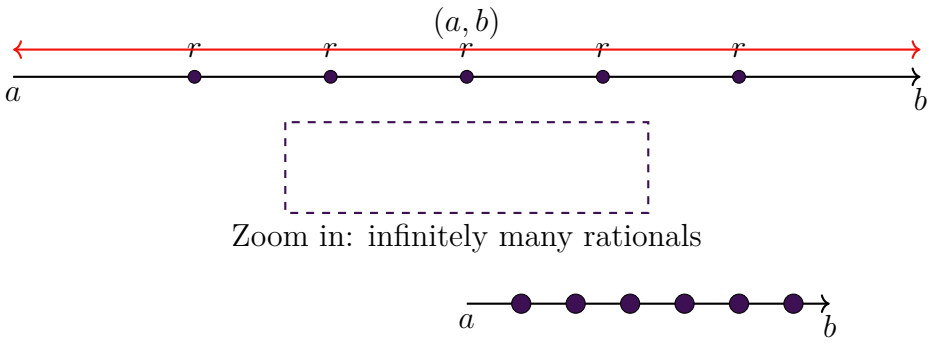


Figure 2: Number line showing rational numbers densely packed between any two reals a and b

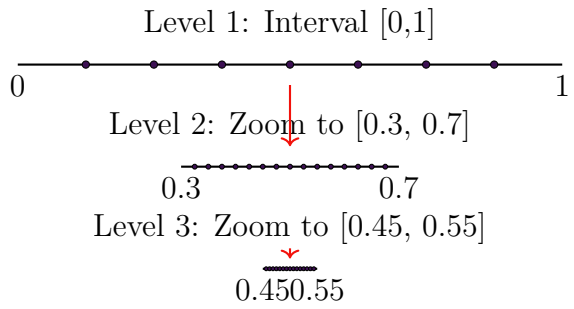


Figure 3: Progressive zooming reveals infinitely many rational numbers in any interval

2.3 Constructive Proof: Finding Rationals Between Reals

The proof of the density theorem is *constructive*—it actually shows us how to find a rational number between any two reals. This has practical applications in numerical analysis and cryptography.

Example 2.4: Finding a Rational Between $\sqrt{2}$ and $\sqrt{3}$

We know $\sqrt{2} \approx 1.414$ and $\sqrt{3} \approx 1.732$. To find a rational between them:
Since $1.732 - 1.414 = 0.318 > \frac{1}{4}$, we can use $n = 4$. Then:

$$4 \cdot 1.414 = 5.656 < 6 < 7.328 = 4 \cdot 1.732$$

So $\frac{6}{4} = \frac{3}{2} = 1.5$ is a rational number between $\sqrt{2}$ and $\sqrt{3}$.

Remark 2.5

The density property is what makes rational numbers seem "everywhere." However, as we will see in later sections, this intuitive sense of "everywhere" is misleading when we consider measure theory. The rationals are dense, but they occupy zero "space" in a precise mathematical sense.

3 Countability

While rational numbers are dense (appearing everywhere), they are fundamentally different from real numbers in terms of their "size" or cardinality. This section explores the concept of countability and shows that rational numbers, despite being infinite, are in a sense "smaller" than the real numbers.

3.1 Countable Sets

Definition 3.1: Countable Set

A set A is called **countable** if there exists a bijection (one-to-one correspondence) between A and the set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$. If a set is countable and infinite, we say it is **countably infinite**.

In simpler terms, a countable set can be "listed" or enumerated—we can assign each element a natural number index, even if the set is infinite.

Example 3.2

The set of even positive integers $\{2, 4, 6, 8, \ldots\}$ is countable because we can list them as:

$$\begin{aligned} 1 &\mapsto 2 \\ 2 &\mapsto 4 \\ 3 &\mapsto 6 \\ 4 &\mapsto 8 \\ &\vdots \end{aligned}$$

The bijection is $f(n) = 2n$.

3.2 Cantor's Enumeration of Rational Numbers

The remarkable fact that rational numbers are countable was first proven by Georg Cantor in the 19th century. His proof uses a clever enumeration method.

Theorem 3.3: Countability of Rational Numbers

The set of rational numbers $\mathbb{Q}$ is countably infinite.

Proof. We will show that the positive rationals are countable by arranging them in a grid and enumerating them systematically.

Consider the infinite grid where row i contains all fractions with numerator i:

$$\begin{matrix} \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \cdots \\ \frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \cdots \\ \frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \cdots \\ \frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{matrix}$$

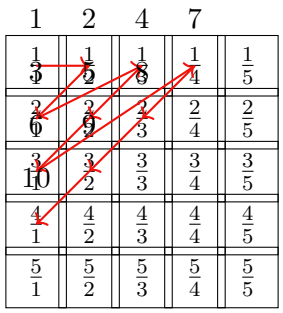
We enumerate by following diagonal paths:

1. Start with $\frac{1}{1}$ (position 1)
2. Move diagonally: $\frac{1}{2}, \frac{2}{1}$ (positions 2, 3)
3. Next diagonal: $\frac{1}{3}, \frac{2}{2}, \frac{3}{1}$ (positions 4, 5, 6)
4. Continue this pattern...

When we encounter a fraction that is not in lowest terms (like $\frac{2}{2} = 1$), we skip it since we've already counted its reduced form. This gives us an enumeration of all positive rationals.

To include negative rationals and zero, we can interleave: $0, \frac{1}{1}, -\frac{1}{1}, \frac{1}{2}, -\frac{1}{2}, \frac{2}{1}, -\frac{2}{1}, \ldots$

Therefore, $\mathbb{Q}$ is countable. □



Cantor's diagonal enumeration of rational numbers

Figure 4: Grid showing Cantor's enumeration method for rational numbers

3.3 Uncountability of Real Numbers

In contrast to rational numbers, the real numbers are *uncountable*—they cannot be put into a one-to-one correspondence with the natural numbers.

Theorem 3.4: Uncountability of Real Numbers

The set of real numbers $\mathbb{R}$ is uncountable.

Cantor's Diagonal Argument. Assume for contradiction that $\mathbb{R}$ is countable. Then we can list all real numbers between 0 and 1:

$$\begin{aligned} r_1 &= 0.d_{11}d_{12}d_{13}d_{14}\ldots \\ r_2 &= 0.d_{21}d_{22}d_{23}d_{24}\ldots \\ r_3 &= 0.d_{31}d_{32}d_{33}d_{34}\ldots \\ r_4 &= 0.d_{41}d_{42}d_{43}d_{44}\ldots \\ &\vdots \end{aligned}$$

where each d_{ij} is a digit.

Now construct a number $s = 0.s_1s_2s_3s_4\ldots$ where $s_i \neq d_{ii}$ (and $s_i \neq 9$ to avoid the $0.999\ldots = 1$ issue). Then s differs from every r_i in at least one decimal place, so s is not in our list—a contradiction.

Therefore, $\mathbb{R}$ is uncountable. □

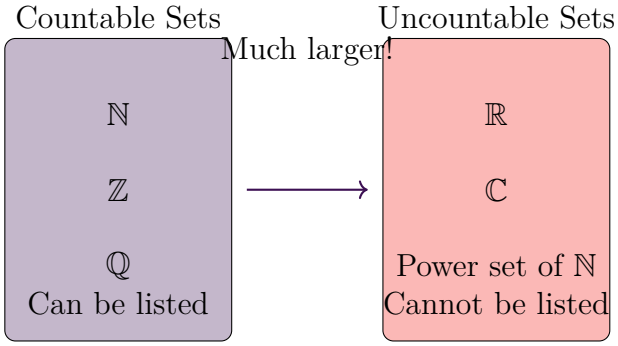


Figure 5: Comparison of countable and uncountable sets

3.4 Paradoxes of Infinite Sets

The concept of infinity leads to many counterintuitive results that challenge our everyday intuition. These paradoxes help illustrate the strange and fascinating properties of infinite sets, including the countably infinite set of rational numbers.

Example 3.5: Hilbert's Grand Hotel

Imagine a hotel with infinitely many rooms, numbered $1, 2, 3, \ldots$, and suppose every room is occupied. One might think the hotel is full and cannot accommodate any new guests. However, this is not the case!

When a new guest arrives, the hotel manager can accommodate them by asking each current guest in room n to move to room $2n$. This frees up all the odd-numbered rooms $(1, 3, 5, 7, \ldots)$, allowing the new guest to take room 1. In fact, the hotel can accommodate infinitely many new guests by having guest in room n move to room $2n$, freeing up all odd-numbered rooms.

This paradox illustrates a fundamental property of countably infinite sets: they can be "rearranged" to accommodate additional elements while maintaining the same cardinality. Just as the rational numbers can be enumerated (listed) in different ways, the hotel's guests can be reassigned to different rooms. This property is unique to infinite sets—a finite hotel with all rooms occupied truly cannot accommodate new guests, but an infinite hotel always can.

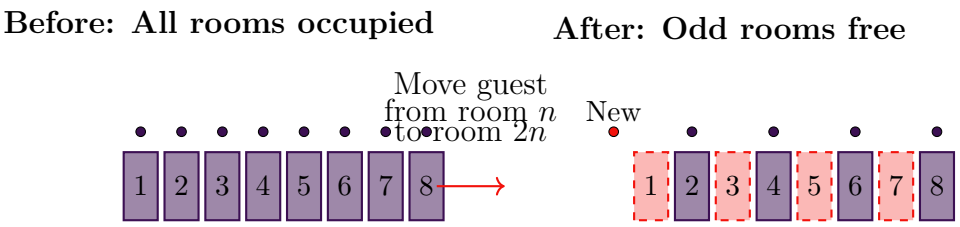


Figure 6: Hilbert's Grand Hotel: Rearranging guests to free up infinitely many rooms

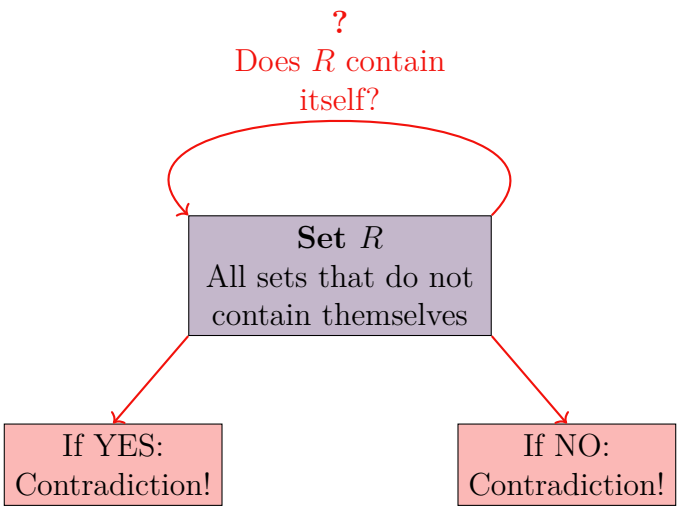
Example 3.6: Russell's Paradox

Consider the set R of all sets that do not contain themselves as an element. Does R contain itself?

If R contains itself, then by definition it should not contain itself (since R only contains sets that don't contain themselves). But if R does not contain itself, then it should contain itself (since it's a set that doesn't contain itself). This creates an inescapable contradiction.

This paradox, discovered by Bertrand Russell in 1901, revealed a fundamental flaw in naive set theory and led to the development of axiomatic set theory (such as Zermelo-Fraenkel set theory with the Axiom of Choice, or ZFC). The resolution required restricting what can be considered a "set" and introducing careful axioms to prevent such self-referential contradictions.

While Russell's paradox doesn't directly involve rational numbers, it highlights the importance of rigorous foundations in set theory. Our understanding of number systems, including the rational numbers $\mathbb{Q}$, rests on these carefully constructed foundations. The fact that we can rigorously define and work with infinite sets like $\mathbb{Q}$ is a testament to the success of modern set theory in resolving such paradoxes.



Russell's Paradox: An inescapable logical contradiction

Figure 7: Russell's Paradox: The self-referential set that leads to contradiction

Example 3.7: Tristram Shandy's Paradox

In Laurence Sterne's novel *The Life and Opinions of Tristram Shandy, Gentleman*, the protagonist takes two years to write the history of the first two days of his life. He laments that he will never finish his autobiography because he cannot keep up with the accumulating events—as he writes about day n, days $n+1, n+2, \ldots$ continue to pass.

At first glance, this seems like an impossible task. However, if we assume Tristram lives forever and continues writing at the same pace (one day's history per year), he will eventually complete his autobiography! After year 1, he has written about day 1. After year 2, he has written about days 1 and 2. After year n, he has written about days 1 through n. Since there are infinitely many natural numbers, he can eventually cover all days of his infinite life.

This paradox relates to the nature of countably infinite processes. Just as we can enumerate the rational numbers (assigning each rational a natural number index), Tristram can enumerate the days of his life. The key insight is that with infinite time, a countably infinite task can be completed, even if the task grows over time. This mirrors how we can "complete" the enumeration of all rational numbers, despite there being infinitely many of them.

Remark 3.8

These paradoxes demonstrate that infinite sets behave in ways that defy our finite intuition. The counterintuitive nature of infinity helps explain why the properties of rational numbers—being both dense (everywhere) and having measure zero (nowhere)—can seem paradoxical at first. Understanding these paradoxes of infinity provides valuable intuition for appreciating the deeper mathematical structures we explore in this document.

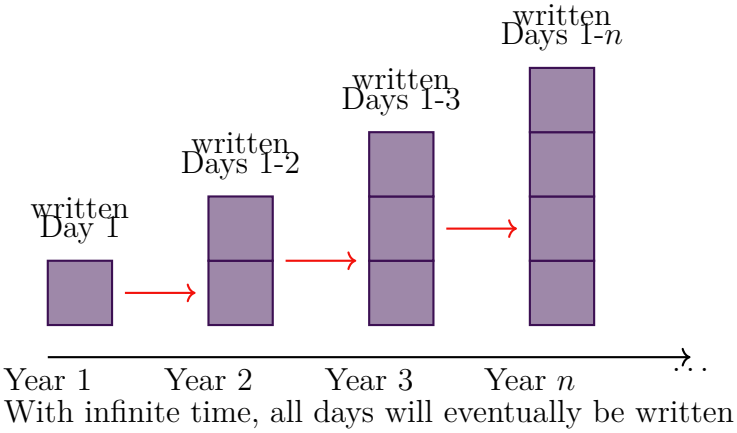


Figure 8: Tristram Shandy's Paradox: The infinite autobiography can be completed

3.5 Implications of Countability

The fact that rational numbers are countable while real numbers are uncountable has profound implications:

1. **Size Difference**: Even though both sets are infinite, there are "more" real numbers than rational numbers in a precise mathematical sense.
2. **Probability**: As we'll see in Section 6, if you pick a real number at random, the probability it's rational is 0, even though rationals are dense.
3. **Cryptography**: The distinction between countable and uncountable sets is crucial in security proofs, where we need to show that "weak" keys form a negligible (measure zero) set.

Remark 3.9

The countability of rational numbers, combined with their density, creates the paradox we explore in later sections: they are "everywhere" (dense) but "nowhere" (measure zero) at the same time.

4 Measure Zero (Nowhere)

While rational numbers are dense and appear "everywhere," measure theory reveals that they actually occupy "no space" on the number line. This section introduces Lebesgue measure and explains why countable sets have measure zero.

4.1 Introduction to Lebesgue Measure

Definition 4.1: Lebesgue Measure

The **Lebesgue measure** of an interval $[a, b]$ (where $a \leq b$) is defined as its length:

$$\mu([a, b]) = b - a$$

For more general sets, the Lebesgue measure extends this notion of "length" in a consistent way.

The Lebesgue measure generalizes our intuitive notion of length, area, and volume to more complicated sets. For intervals, it simply gives the length, but it can also measure sets that are not intervals.

Example 4.2: Riemann Integral vs Lebesgue Measure

To understand how Lebesgue measure relates to integration, consider calculating the integral of the constant function $f(x) = 1$ from 0 to 1 using the traditional Riemann integral.
The Riemann integral partitions the *domain* (the x-axis) into subintervals and approximates the area under the curve using rectangles. For $f(x) = 1$ on $[0, 1]$, we have:

$$\int_0^1 1 \, dx = [x]_0^1 = 1 - 0 = 1$$

The Riemann approach works by:

1. Dividing the interval $[0, 1]$ into smaller subintervals
2. Approximating the function value on each subinterval
3. Summing the areas of rectangles: $\sum f(x_i) \cdot \Delta x_i$
4. Taking the limit as the partition becomes finer

The **Lebesgue integral** (which uses Lebesgue measure) takes a different approach:

1. It partitions the *range* (the y-axis) instead of the domain
2. For each value y in the range, it considers the set $\{x : f(x) \geq y\}$
3. It uses the *measure* of these sets (their "length") rather than just their endpoints
4. For $f(x) = 1$, the set $\{x : 1 \geq y\}$ equals $[0, 1]$ when $y \leq 1$ (with measure 1), and is empty when $y > 1$ (with measure 0)
5. The Lebesgue integral becomes: $\int_0^1 1 \, d\mu = \mu([0, 1]) = 1$

For this simple function, both methods give the same result (1), but the Lebesgue approach is more powerful because:

- It can integrate functions that Riemann integration cannot handle (e.g., functions with many discontinuities)
- It provides better convergence theorems (e.g., the dominated convergence theorem)
- It naturally extends to higher dimensions and more abstract spaces

The key insight is that Lebesgue measure allows us to measure the "size" of sets (like $\{x : f(x) \geq y\}$) even when they are not simple intervals, which makes the Lebesgue integral more general and powerful than the Riemann integral.

Proof. For any $\epsilon > 0$, the point $\{x\}$ is contained in the interval $[x - \frac{\epsilon}{2}, x + \frac{\epsilon}{2}]$, which has measure ϵ. Since we can make ϵ arbitrarily small, the measure of $\{x\}$ must be zero. □

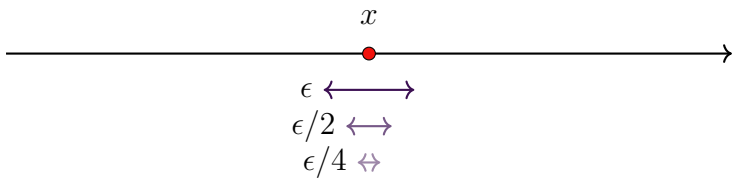


Figure 9: Visualization that a single point has measure zero

4.2 Countable Sets Have Measure Zero

The key result connecting countability to measure is the following theorem.

Theorem 4.4: Countable Sets Have Measure Zero

If A is a countable set, then $\mu(A) = 0$.

Proof. Since A is countable, we can list its elements: $A = \{a_1, a_2, a_3, \ldots\}$.

For any $\epsilon > 0$, cover each point a_i with an interval of length $\frac{\epsilon}{2^i}$:

$$I_i = \left[a_i - \frac{\epsilon}{2^{i+1}}, a_i + \frac{\epsilon}{2^{i+1}}\right]$$

The total measure of these intervals is:

$$\sum_{i=1}^{\infty} \frac{\epsilon}{2^i} = \epsilon \sum_{i=1}^{\infty} \frac{1}{2^i} = \epsilon \cdot 1 = \epsilon$$

Since $A \subseteq \bigcup_{i=1}^{\infty} I_i$ and we can make ϵ arbitrarily small, we conclude that $\mu(A) = 0$. □

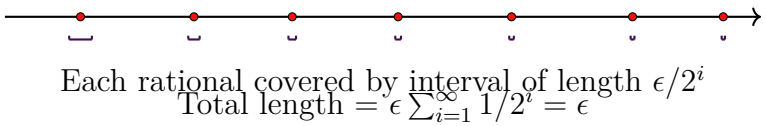


Figure 10: Visual representation of covering countable set with intervals of decreasing size

4.3 The Rational Numbers Have Measure Zero

Proof. Since $\mathbb{Q}$ is countable (as shown in Section 3), the theorem immediately implies that $\mu(\mathbb{Q}) = 0$. □

This is the "nowhere" part of our paradox! Even though rational numbers are dense (everywhere), they take up zero total "space" on the number line.

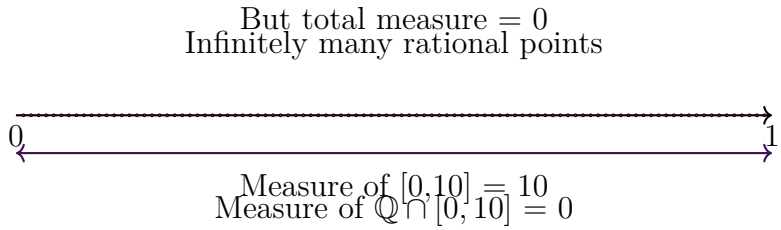


Figure 11: Number line showing rationals as "dust" with zero total length

4.4 Properties of Measure Zero

Theorem 4.6: Properties of Measure Zero

1. If $A \subseteq B$ and $\mu(B) = 0$, then $\mu(A) = 0$.
2. If $A_1, A_2, A_3, \ldots$ are sets with measure zero, then $\bigcup_{i=1}^{\infty} A_i$ also has measure zero.
3. Any finite set has measure zero.

These properties help us understand why countable unions of measure zero sets (like individual rational numbers) still have measure zero.

Remark 4.7

The concept of measure zero is fundamental in analysis and probability theory. Sets of measure zero are often called "negligible" because they don't affect integrals or probabilities in most practical situations.

5 The Paradox: Everywhere but Nowhere

We have now established two seemingly contradictory facts about rational numbers:

1. They are *dense* in $\mathbb{R}$ (Section 2)—you can find a rational in any interval.
2. They have *measure zero* (Section 4)—they take up no space on the number line.

This section reconciles this apparent paradox and provides intuition for how both can be true simultaneously.

5.1 Understanding the Paradox

The paradox arises from conflating two different notions of "size":

- **Topological size (density)**: Rationals are "everywhere" in the sense that every neighborhood of every real number contains rationals.
- **Measure-theoretic size**: Rationals are "nowhere" in the sense that their total Lebesgue measure is zero.

These are not contradictory—they measure different aspects of the set!

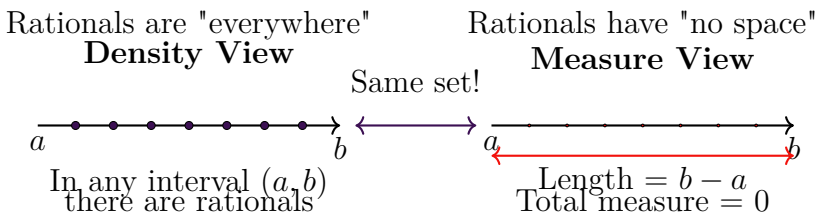


Figure 12: Side-by-side comparison: density vs measure zero

5.2 The Microscope Analogy

A helpful analogy is to think of rational numbers like "mathematical dust":

Remark 5.1: Microscope Analogy

Imagine you have a microscope that can zoom in on any part of the number line. No matter how much you zoom in, you'll always see rational numbers scattered throughout. However, if you were to "sweep" the number line with a ruler, the total length covered by all these rational points would be zero—they are like infinitely fine dust particles that take up no volume.
This is different from physical objects: if you zoom in on a physical object, you eventually reach atoms that have actual size. But with rational numbers, no matter how much you zoom, you see infinitely many points, yet they still amount to "dust" with no total width.

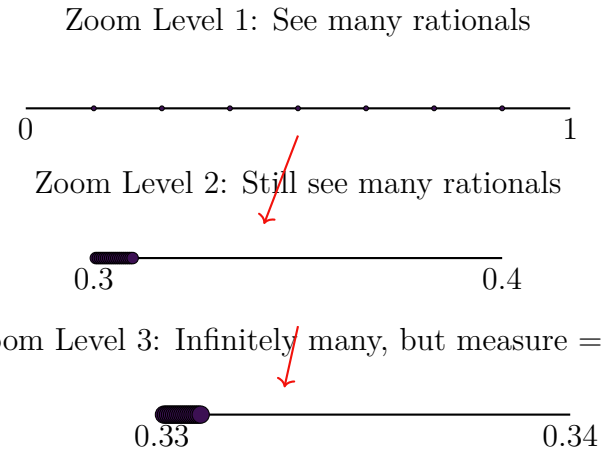


Figure 13: Progressive zoom showing infinite points but zero measure

5.3 Why Both Can Be True

The resolution of the paradox lies in understanding that:

1. **Density is about topology**: It concerns the *structure* of the set—how its elements are distributed relative to other points. Density means that rationals are "close" to every real number in a topological sense.

2. **Measure is about size**: It concerns the *volume* or *length* of the set. Measure zero means that if you tried to "paint" all the rationals, you'd use zero paint.

These are independent properties! A set can be dense but have measure zero, just as a set can have positive measure but not be dense (think of a single interval).

Example 5.2

Consider the set $A = [0, 1] \cup \{2\}$. This set:

- Has positive measure (measure of $[0, 1]$ is 1)
- Is *not* dense in $\mathbb{R}$ (there's a gap between 1 and 2)

This shows that density and measure are independent concepts.

5.4 The Complete Picture

Theorem 5.3: Rational Numbers: Dense but Measure Zero

The set of rational numbers $\mathbb{Q}$ satisfies:

1. $\mathbb{Q}$ is dense in $\mathbb{R}$
2. $\mu(\mathbb{Q}) = 0$

This theorem perfectly captures the "everywhere but nowhere" nature of rational numbers. They are simultaneously:

- **Everywhere**: Topologically dense, appearing in every interval
- **Nowhere**: Measure-theoretically negligible, taking up zero space

Remark 5.4

This paradox is not a contradiction but rather a beautiful illustration of how different mathematical perspectives (topology vs measure theory) can reveal different aspects of the same mathematical object. Understanding this duality is crucial for appreciating both pure mathematics and its applications in fields like cryptography.

6 Probability Implications

The measure-theoretic properties of rational numbers have direct implications for probability theory. This section explores what it means to "pick a number at random" and why the probability of selecting a rational number is zero, despite their density.

6.1 Geometric Probability

Definition 6.1: Geometric Probability

If we pick a real number uniformly at random from an interval $[a, b]$, the probability that it falls in a subset $A \subseteq [a, b]$ is:

$$P(x \in A) = \frac{\mu(A)}{b - a}$$

where $\mu(A)$ is the Lebesgue measure of A.

This definition makes intuitive sense: the probability is proportional to the "size" (measure) of the set.

Theorem 6.2: Probability of Picking a Rational

If a real number is chosen uniformly at random from any interval $[a, b]$ (where $a < b$), the probability that it is rational is zero:

$$P(x \in \mathbb{Q} \cap [a, b]) = 0$$

Proof. Since $\mu(\mathbb{Q} \cap [a, b]) = 0$ (rationals have measure zero), we have:

$$P(x \in \mathbb{Q} \cap [a, b]) = \frac{\mu(\mathbb{Q} \cap [a, b])}{b - a} = \frac{0}{b - a} = 0$$

□

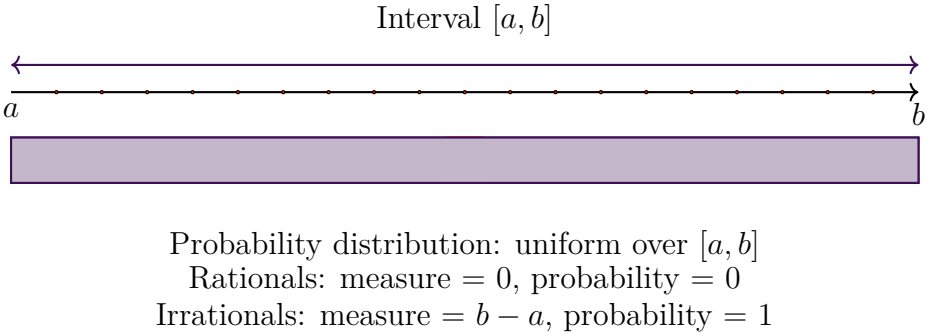


Figure 14: Geometric probability on number line showing rationals vs irrationals

6.2 Almost Surely

Definition 6.3: Almost Surely

An event is said to occur **almost surely** (a.s.) if it occurs with probability 1. Equivalently, the set of outcomes where it does *not* occur has measure zero.

Corollary 6.4

A randomly chosen real number is almost surely irrational.

Proof. Since $P(x \in \mathbb{Q}) = 0$, we have $P(x \notin \mathbb{Q}) = 1 - 0 = 1$. Therefore, x is irrational almost surely. □

This is a striking result: even though rational numbers are dense (you can find one arbitrarily close to any real number), if you pick a number "at random," you will *almost never* get a rational number!

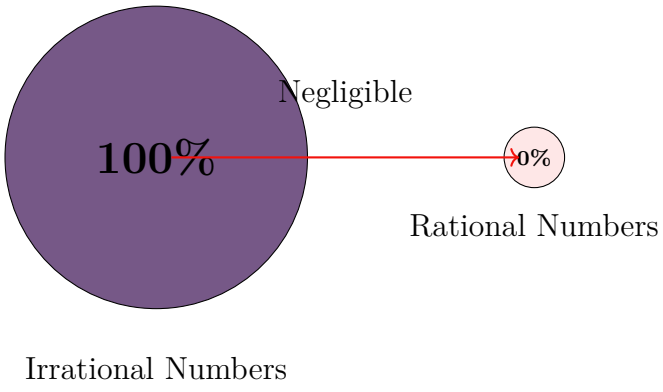


Figure 15: Probability distribution: 0% rationals, 100% irrationals

6.3 Implications for Random Number Generation

This mathematical fact has profound implications for cryptography and random number generation:

1. **Weak Keys Form Measure Zero**: In cryptographic systems, "weak" keys (those that can be easily broken) typically form a countable set, hence have measure zero. This means that if you generate keys "at random," you will almost surely avoid weak keys.

2. **Negligible Probability**: The concept of "negligible probability" in cryptography is directly related to measure zero. An event with measure zero has probability zero, making it statistically impossible.

3. **Security Guarantees**: Security proofs often rely on showing that the set of "bad" outcomes (weak keys, successful attacks under certain conditions) has measure zero, ensuring they occur with probability zero.

Remark 6.5

The connection between measure zero and negligible probability is fundamental to modern cryptography. When cryptographers say that a certain attack succeeds with "negligible probability," they mean (in a precise mathematical sense) that the set of successful outcomes has measure zero in the space of all possible outcomes.

6.4 The Intuition

Why does this make sense? Think of it this way:

- There are *infinitely many* rational numbers, but they are "countable" infinity.
- There are *infinitely many* irrational numbers, but they are "uncountable" infinity—a much larger infinity.
- When picking "at random," you're essentially sampling from the uncountable set, which dominates the countable set.

The countable set of rationals is "swallowed up" by the uncountable set of irrationals, just as a single point is swallowed up by a line segment.

Example 6.6

Consider picking a number uniformly from $[0, 1]$. The probability of picking exactly $\frac{1}{2}$ is zero (it's a single point). Similarly, the probability of picking *any* rational number is zero, because the set of all rationals, while infinite, is still "too small" compared to the uncountable set of all reals.

Part II: Cryptographic Applications

7 Cryptography Connections: An Overview

The mathematical properties of rational numbers—their density, countability, and measure zero—have deep connections to modern cryptography. This section provides an overview of these connections, which will be explored in detail in subsequent sections.

7.1 Why Rational Numbers Matter in Cryptography

Cryptography relies on mathematical structures and properties to ensure security. The properties of rational numbers provide:

1. **Theoretical Foundations**: Understanding countable vs uncountable sets helps define security in terms of computational vs information-theoretic security.
2. **Probability Guarantees**: Measure zero provides the mathematical basis for "negligible probability" in security proofs.
3. **Approximation Theory**: Rational approximations to irrational numbers underlie lattice-based cryptography and certain attacks.
4. **Key Space Analysis**: The structure of key spaces and the probability of weak keys can be understood through measure theory.

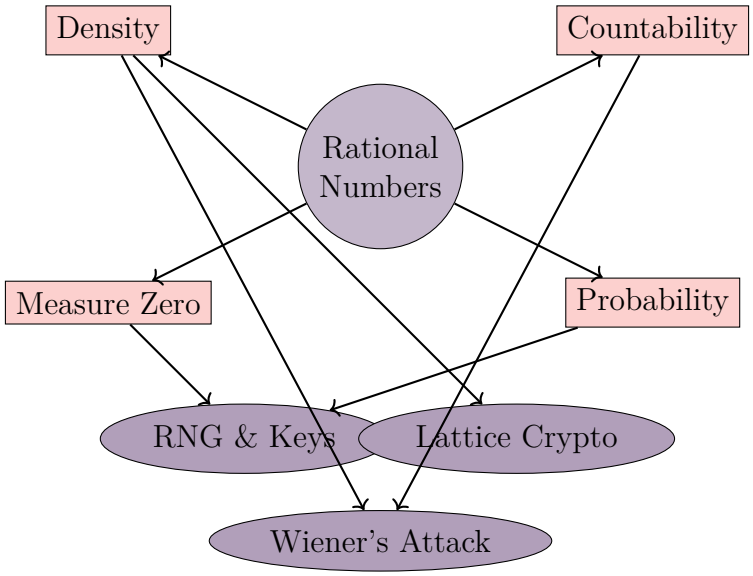


Figure 16: Concept map linking rational number properties to cryptographic applications

7.2 Key Cryptographic Applications

7.2.1 1. Random Number Generation and Key Security

The measure zero property of rational numbers (and more generally, countable sets) provides the mathematical foundation for understanding why "weak" cryptographic keys are statistically impossible to generate randomly.

- Weak keys typically form a countable set
- Countable sets have measure zero
- Random key generation samples from the full keyspace
- Probability of hitting a weak key is zero

7.2.2 2. Lattice-Based Cryptography

Lattice-based cryptography, a leading candidate for post-quantum security, relies on the hardness of problems involving rational approximations:

- Finding rational numbers close to irrational numbers (Diophantine approximation)
- Lattice problems reduce to approximation problems
- Security depends on the difficulty of these approximations

7.2.3 3. Wiener's Attack on RSA

A famous cryptographic attack exploits the fact that if an RSA private key is "too small," it can be found by finding a rational approximation to a certain fraction derived from the public key.

- Public key gives a fraction $\frac{e}{n}$

- Private key appears in continued fraction expansion
- If key is small, rational approximation reveals it

7.2.4 Security Proofs and Distinguishing Sets

The distinction between countable and uncountable sets is crucial in security proofs:

- Adversaries try to distinguish between different distributions
- Countable "bad" sets have measure zero
- Security guarantees rely on negligible probability (measure zero)

7.3 The Mathematical Bridge

The connection between rational numbers and cryptography is not merely coincidental—it reflects deep mathematical structures:

Theorem 7.1: Bridge Principle

Properties of rational numbers (density, countability, measure zero) provide the mathematical language for:

1. Defining security in terms of negligible probabilities
2. Analyzing key spaces and weak key sets
3. Understanding approximation problems in cryptography
4. Proving security guarantees

Remark 7.2

This connection illustrates how pure mathematics (the study of rational numbers and measure theory) directly informs applied mathematics (cryptography and security). The "everywhere but nowhere" paradox of rationals becomes a powerful tool for understanding cryptographic security.

7.4 Organization of Remaining Sections

The following sections will explore these connections in detail:

- **Section 8**: Random Number Generation—how measure zero ensures weak keys are negligible
- **Section 9**: Lattice-Based Cryptography—Diophantine approximation and post-quantum security
- **Section 10**: Wiener's Attack—a concrete example of rational approximation in cryptanalysis

Each section will build on the mathematical foundations established in the first six sections, showing how abstract mathematical concepts translate into practical cryptographic insights.

8 Random Number Generation and Key Security

The measure zero property of rational numbers provides crucial mathematical intuition for understanding cryptographic key generation and security. This section explores how measure theory guarantees that "weak" keys are statistically impossible to generate randomly.

8.1 Keyspaces and Weak Keys

Definition 8.1: Keyspace

A **keyspace** is the set of all possible keys that can be used in a cryptographic system. For a key of length n bits, the keyspace has size 2^n.

Definition 8.2: Weak Key

A **weak key** is a key that, due to its mathematical properties, makes the cryptographic system vulnerable to attack or easier to break than intended.

Example 8.3

In RSA, a weak key might be one where:

- The private exponent d is too small
- The prime factors p and q are too close together
- The key has some special mathematical structure that enables attacks

8.2 Weak Keys as a Measure Zero Set

Theorem 8.4: Weak Keys Have Measure Zero

Under reasonable assumptions, the set of weak keys in a cryptographic system forms a countable set, hence has Lebesgue measure zero in the keyspace.

Sketch. Weak keys typically have specific mathematical properties that can be enumerated:

- Keys with $d < \sqrt[4]{n}$ (for Wiener's attack)
- Keys where $|p - q| < k$ for some small k
- Keys with specific bit patterns
- Keys that are powers of small integers

Each of these conditions defines a countable set. The union of countably many countable sets is countable, hence has measure zero. □

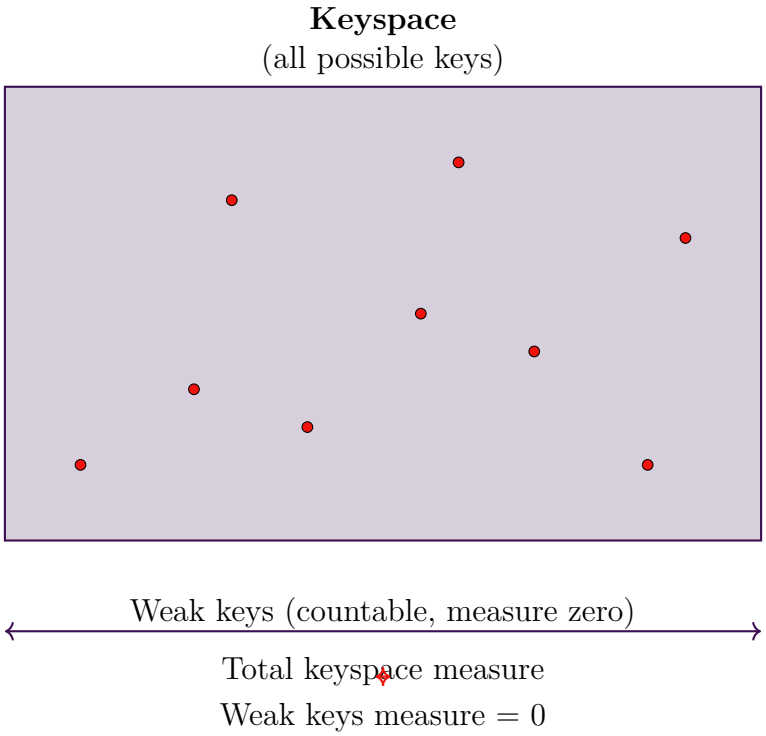


Figure 17: Keyspace visualization showing weak keys as measure zero set

8.3 Probability of Generating a Weak Key

Theorem 8.5: Negligible Probability of Weak Keys

If keys are generated uniformly at random from the keyspace, the probability of generating a weak key is zero.

Proof. Let W be the set of weak keys. Since $\mu(W) = 0$ and the keyspace has positive measure, we have:

$$P(\text{key} \in W) = \frac{\mu(W)}{\mu(\text{keyspace})} = \frac{0}{\mu(\text{keyspace})} = 0$$

□

This is the cryptographic significance of measure zero: it ensures that weak keys are not just rare, but *statistically impossible* to generate randomly.

8.4 Implications for Cryptographic Security

8.4.1 Security Guarantees

The measure zero property provides a strong security guarantee:

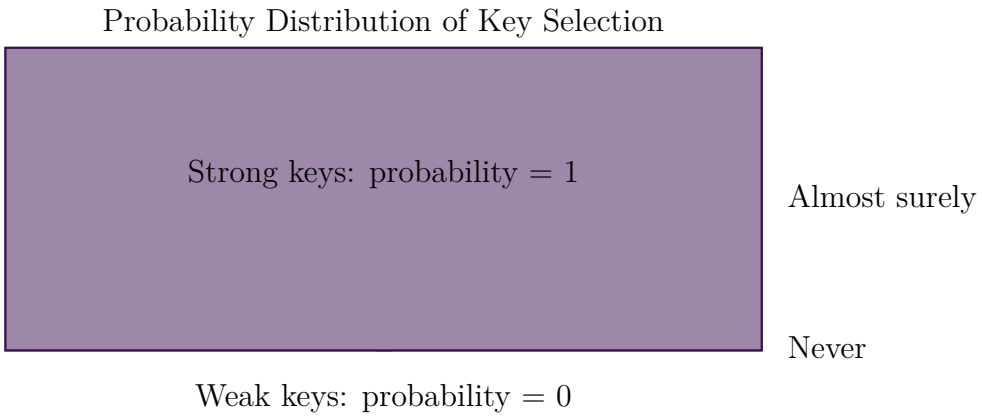


Figure 18: Probability distribution showing negligible probability of weak keys

Theorem 8.6: Security Guarantee

If a cryptographic system's security depends on avoiding weak keys, and weak keys form a measure zero set, then random key generation provides security with probability 1.

This means that as long as keys are generated using a proper random number generator, the system is secure *almost surely*.

8.4.2 Random Number Generation Requirements

This mathematical fact imposes requirements on random number generators:

1. **Uniform Distribution**: Keys must be sampled uniformly from the keyspace
2. **True Randomness**: The generator must not have biases that could concentrate probability on weak keys
3. **Sufficient Entropy**: The generator must have enough randomness to avoid predictable patterns

Remark 8.7

The measure zero property of weak keys is what makes cryptographic systems secure in practice. Without this mathematical guarantee, we would need to explicitly check every generated key for weakness, which would be computationally infeasible.

8.5 The Analogy to Rational Numbers

The connection to rational numbers is direct:

- **Rational numbers** are countable, hence have measure zero in $\mathbb{R}$
- **Weak keys** are countable, hence have measure zero in the keyspace
- **Picking a random real** almost surely gives an irrational

- **Generating a random key** almost surely gives a strong key

Both rely on the same mathematical principle: countable sets are "swallowed up" by uncountable sets when sampling uniformly.

Example 8.8: RSA Key Generation

When generating RSA keys:

- The keyspace is the set of all valid (n, e, d) tuples
- Weak keys (e.g., small d) form a countable subset
- Random generation samples from the full uncountable keyspace
- Probability of weak key $= 0$ (almost surely strong)

8.6 Practical Considerations

While the mathematical guarantee is strong, practical implementation matters:

1. **Implementation Bugs**: A buggy RNG might not sample uniformly
2. **Entropy Sources**: Insufficient entropy can create biases
3. **Timing Attacks**: Even with secure keys, implementation can leak information

The measure zero property provides a *theoretical* guarantee; proper implementation ensures this guarantee holds in practice.

9 Lattice-Based Cryptography and Diophantine Approximation

Lattice-based cryptography is one of the most promising approaches for post-quantum cryptography. It relies fundamentally on the difficulty of finding good rational approximations to certain numbers, directly connecting to the properties of rational numbers we've explored.

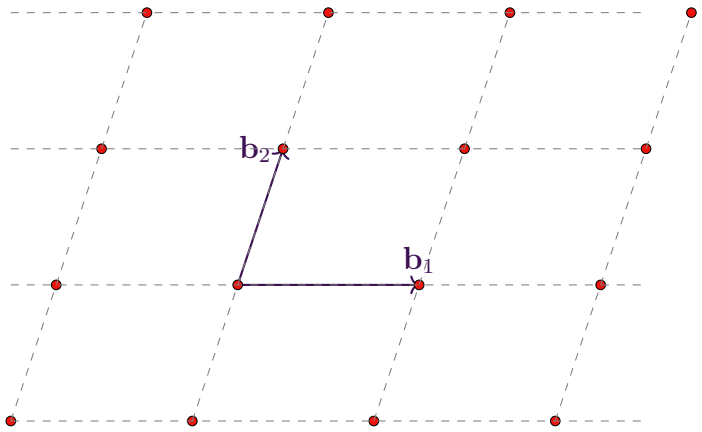
9.1 Introduction to Lattices

Definition 9.1: Lattice

A **lattice** $\mathcal{L}$ in $\mathbb{R}^n$ is the set of all integer linear combinations of linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$:

$$\mathcal{L} = \left\{ \sum_{i=1}^{k} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\}$$

The vectors $\mathbf{b}_1, \ldots, \mathbf{b}_k$ form a **basis** of the lattice.



2D Lattice: integer combinations of basis vectors

Figure 19: Visualization of a 2D lattice

9.2 Diophantine Approximation

Definition 9.2: Diophantine Approximation

Diophantine approximation is the study of how well real numbers can be approximated by rational numbers. Given an irrational number α and an error bound $\epsilon > 0$, we seek rational numbers $\frac{p}{q}$ such that:

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

The density of rational numbers (Section 2) guarantees that such approximations always exist, but finding *good* approximations (with small denominators) is computationally hard.

Theorem 9.3: Dirichlet's Approximation Theorem

For any irrational number α and any positive integer N, there exist integers p and q with $1 \leq q \leq N$ such that:

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

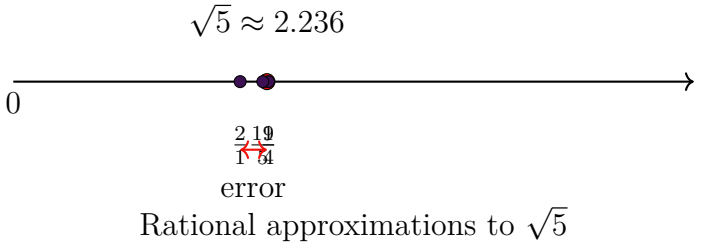


Figure 20: Number line showing rational approximation to irrational number

9.3 Continued Fractions

Continued fractions provide the best rational approximations to irrational numbers.

Definition 9.4: Continued Fraction

A **continued fraction** is an expression of the form:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

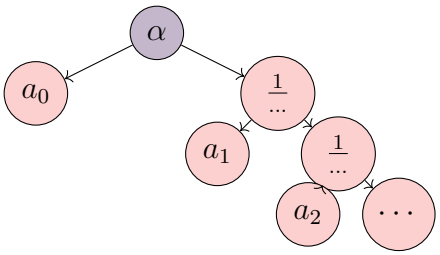
where a_0 is an integer and $a_1, a_2, a_3, \ldots$ are positive integers.

Example 9.5

The continued fraction for $\sqrt{2}$ is:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}$$

The convergents (rational approximations) are: $\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \ldots$



Continued fraction tree structure

Figure 21: Tree structure of continued fraction expansion

9.4 Connection to Lattice Problems

Lattice-based cryptography relies on the computational hardness of certain lattice problems, which are closely related to Diophantine approximation:

Theorem 9.6: Lattice Problems and Approximation

The following problems are computationally equivalent (up to polynomial factors):

1. **Shortest Vector Problem (SVP)**: Find the shortest non-zero vector in a lattice
2. **Closest Vector Problem (CVP)**: Find the lattice point closest to a given target vector
3. **Approximate SVP**: Find a vector within a factor of the shortest vector

These problems reduce to finding good rational approximations.

Remark 9.7

The security of lattice-based cryptosystems depends on the assumption that these approximation problems are computationally hard, even for quantum computers. This is why lattice-based cryptography is a leading candidate for post-quantum security.

9.5 Cryptographic Applications

9.5.1 Learning With Errors (LWE)

The Learning With Errors problem, a foundation of lattice-based cryptography, can be viewed as an approximation problem:

Definition 9.8: Learning With Errors

Given a matrix $\mathbf{A}$ and a vector $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$ (where $\mathbf{e}$ is a small error vector), recover the secret vector $\mathbf{s}$.

This is essentially finding a "close" solution to a system of equations, which relates to approximation problems.

9.5.2 Post-Quantum Security

Lattice-based cryptography is considered secure against quantum attacks because:

- Quantum algorithms (like Shor's algorithm) don't provide speedups for lattice problems
- The approximation problems remain hard even with quantum computation
- The security relies on the structure of rational approximations, which quantum computers don't help with

Example 9.9

NIST's post-quantum cryptography standardization includes several lattice-based schemes:

- CRYSTALS-Kyber (key encapsulation)
- CRYSTALS-Dilithium (digital signatures)
- FALCON (digital signatures)

All rely on the hardness of lattice approximation problems.

9.6 The Rational Number Connection

The connection to rational numbers is fundamental:

1. **Density**: Rationals are dense, so approximations always exist
2. **Countability**: There are only countably many "good" approximations (with bounded denominators)
3. **Hardness**: Finding the best approximation is computationally difficult
4. **Security**: Cryptographic security relies on this computational difficulty

The "everywhere but nowhere" nature of rationals—dense yet measure zero—ensures that while approximations exist, finding them is hard, providing the foundation for cryptographic security.

10 Wiener's Attack on RSA: A Concrete Example

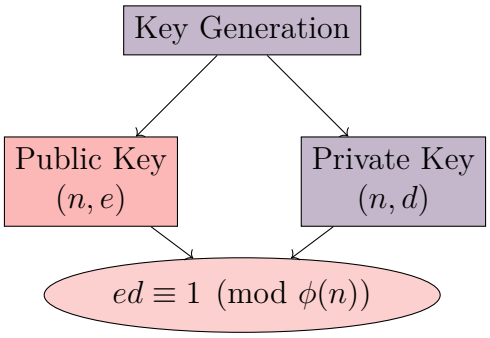
Wiener's attack on RSA provides a concrete and elegant example of how rational approximation theory can be used in cryptanalysis. This attack exploits the fact that if an RSA private key is "too small," it can be recovered by finding a rational approximation to a fraction derived from the public key.

10.1 RSA Key Generation Recap

In RSA cryptography:

- Choose two large primes p and q
- Compute $n = pq$ (the modulus)
- Choose public exponent e such that $\gcd(e, \phi(n)) = 1$ where $\phi(n) = (p-1)(q-1)$
- Compute private exponent d such that $ed \equiv 1 \pmod{\phi(n)}$
- Public key: (n, e)
- Private key: (n, d)

The security of RSA relies on the difficulty of factoring n or computing d from (n, e).



RSA key relationship

Figure 22: RSA key generation and relationship

10.2 The Vulnerability: Small Private Exponent

Theorem 10.1: Wiener's Condition

If the private exponent d satisfies:

$$d < \frac{1}{3}n^{1/4}$$

then d can be efficiently recovered from the public key (n, e) using continued fractions.

This means that if d is "too small" relative to n, the RSA system is vulnerable to attack, even without factoring n.

10.3 The Mathematical Foundation

The attack relies on a key mathematical relationship. Since $ed \equiv 1 \pmod{\phi(n)}$, there exists an integer k such that:

$$ed = 1 + k\phi(n)$$

Rearranging:

$$\frac{e}{n} = \frac{k}{d} + \frac{1 + k(\phi(n) - n)}{dn}$$

If d is small, then $\frac{k}{d}$ is a good rational approximation to $\frac{e}{n}$.

Theorem 10.2: Approximation Quality

If $d < \frac{1}{3}n^{1/4}$ and p, q are balanced (similar size), then:

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

This means $\frac{k}{d}$ appears as a convergent in the continued fraction expansion of $\frac{e}{n}$!

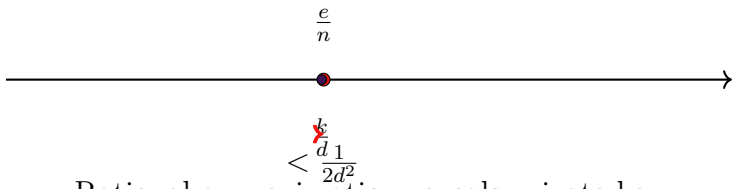


Figure 23: Number line showing how $\frac{k}{d}$ approximates $\frac{e}{n}$

10.4 The Attack Algorithm

Algorithm 1 Wiener's Attack on RSA

Compute the continued fraction expansion of $\frac{e}{n}$
for each convergent $\frac{k_i}{d_i}$ of the continued fraction **do**
  if d_i is odd and $d_i < \frac{1}{3}n^{1/4}$ **then**
    Try d_i as the private exponent
    Check if d_i works (verify with a test message)
    if verification succeeds **then**
      return d_i (private key found!)
    end if
  end if
end for

10.5 Why This Works

The attack succeeds because:

1. **Continued fractions give best approximations**: The convergents of a continued fraction are the best rational approximations (in a precise sense).
2. **Small d ensures good approximation**: If d is small, then $\frac{k}{d}$ must be a convergent.
3. **Efficient computation**: Continued fractions can be computed efficiently using the Euclidean algorithm.
4. **Verification is easy**: Once we guess d, we can verify it by testing encryption/decryption.

Example 10.3: Concrete Example

Suppose:

- $n = 10000019$ (product of two primes)
- $e = 65537$ (common public exponent)
- d is small (violating Wiener's condition)

The continued fraction expansion of $\frac{65537}{10000019}$ will have $\frac{k}{d}$ as a convergent, revealing the private key.

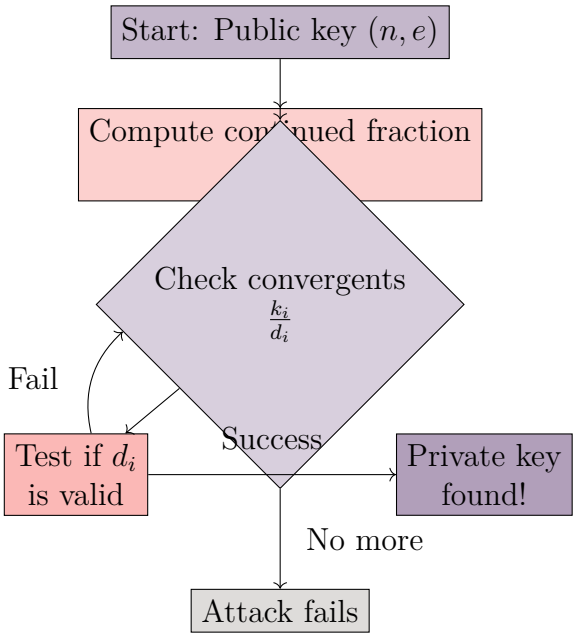


Figure 24: Wiener's attack flowchart

10.6 Continued Fraction Approximation Process

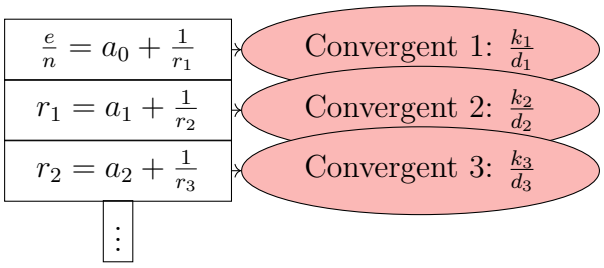


Figure 25: Visualization of continued fraction approximation algorithm

10.7 Defenses Against Wiener's Attack

To prevent Wiener's attack:

1. **Large private exponent**: Ensure $d > \frac{1}{3}n^{1/4}$
2. **Use d' instead of d**: Compute a larger equivalent private exponent
3. **CRT-based decryption**: Use Chinese Remainder Theorem, which doesn't require small d

Remark 10.4

Wiener's attack beautifully illustrates how the mathematical theory of rational approximation (rooted in the properties of rational numbers) directly applies to cryptanalysis. The "everywhere" nature of rationals (density) ensures approximations exist, while the computational difficulty of finding the *right* approximation provides security—until the key is too small, making the approximation too easy to find.

10.8 Connection to Rational Number Properties

This attack directly connects to our earlier discussions:

- **Density**: Rationals are dense, so good approximations to $\frac{e}{n}$ exist
- **Countability**: There are only countably many "small" private keys
- **Measure Zero**: Small private keys form a measure zero set in the keyspace
- **Probability**: Random key generation almost surely avoids this vulnerability

The attack succeeds precisely when we're in the "measure zero" set of weak keys—the same mathematical structure we explored in Section 8.

Part III: Practice and Synthesis

11 Problems: Mathematical and Cryptographic Challenges

This section presents problems at various difficulty levels, from high school accessible to research level. Each problem connects to the themes explored in this document: rational numbers, measure theory, and cryptography.

11.1 Level 1: High School Accessible

Exercise 11.1: Density Exercise

Show that between any two rational numbers $\frac{a}{b}$ and $\frac{c}{d}$ (where $a, b, c, d \in \mathbb{Z}$ and $b, d > 0$), there exists another rational number.

Hint: Consider the average of the two rational numbers. Is it rational? Where does it lie relative to the original two numbers?

Solution Outline:

The number $\frac{\frac{a}{b}+\frac{c}{d}}{2} = \frac{ad+bc}{2bd}$ is rational and lies strictly between the two given rationals.

Exercise 11.2: Countability Practice

Show that the set of integers $\mathbb{Z}$ is countable by explicitly constructing a bijection with $\mathbb{N}$.

Hint: Try mapping: $1 \mapsto 0, 2 \mapsto 1, 3 \mapsto -1, 4 \mapsto 2, 5 \mapsto -2, \ldots$ Can you find the pattern?

Solution Outline:

Define $f : \mathbb{N} \to \mathbb{Z}$ by $f(1) = 0$ and for $n > 1$, $f(n) = (-1)^n \lfloor n/2 \rfloor$. This gives a bijection.

11.2 Level 2: More Depth

Exercise 11.3: Measure of Finite Sets

Prove that any finite set of real numbers has Lebesgue measure zero.

Hint: Cover each point with an interval of length ϵ/n where n is the number of points. What is the total measure?

Solution Outline:

If $A = \{a_1, a_2, \ldots, a_n\}$, cover each a_i with interval $I_i = [a_i - \frac{\epsilon}{2n}, a_i + \frac{\epsilon}{2n}]$. Then $\mu(\bigcup I_i) \leq n \cdot \frac{\epsilon}{n} = \epsilon$. Since ϵ is arbitrary, $\mu(A) = 0$.

Exercise 11.4: Uncountability of Irrationals

Prove that the set of irrational numbers is uncountable.

Hint: Use the fact that $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$. What do you know about the cardinalities of these sets?

Solution Outline:

Since $\mathbb{R}$ is uncountable and $\mathbb{Q}$ is countable, if $\mathbb{R} \setminus \mathbb{Q}$ were countable, then $\mathbb{R}$ would be countable (union of two countable sets). Contradiction.

11.3 Level 3: Crypto + Maths High Level

Exercise 11.5: Weak Keys in Simplified RSA

Consider a simplified RSA system where $n = pq$ with p, q primes, and the private exponent d satisfies $d < \sqrt{n}/10$. Show that the set of such weak keys has measure zero in an appropriate keyspace.

Hint: How many pairs (p, q) with $pq = n$ exist? How many values of p satisfy the condition for a given n?

Solution Outline:

For each n, there are at most $O(\sqrt{n})$ valid d values. The number of possible n is countable. Therefore, the set of weak keys is countable, hence has measure zero.

Exercise 11.6: Continued Fraction Convergence

Show that if $\frac{p}{q}$ is a convergent of the continued fraction expansion of an irrational number α, then:

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

Hint: Use properties of continued fractions: convergents are best approximations, and they satisfy a recurrence relation.

Solution Outline:

This follows from the theory of continued fractions. Convergents satisfy $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$, and the error bound can be derived from this relationship.

Exercise 11.7: Lattice Basis and Approximation

Given a 2D lattice with basis vectors $\mathbf{b}_1 = (1, 0)$ and $\mathbf{b}_2 = (\alpha, 1)$ where α is irrational, show that finding the shortest vector in this lattice is equivalent to finding a good rational approximation to α.

Hint: A lattice point has the form $m\mathbf{b}_1 + n\mathbf{b}_2 = (m + n\alpha, n)$. What is the length of this vector?

Solution Outline:

The length is $\sqrt{(m+n\alpha)^2+n^2}$. Minimizing this is equivalent to finding m, n such that $|m+n\alpha|$ is small, i.e., finding a rational approximation $\frac{m}{n} \approx -\alpha$.

11.4 Level 4: Research Level

Exercise 11.8: Measure-Theoretic Security

Formalize the following security guarantee in measure-theoretic terms: "A cryptographic scheme is secure if the set of keys that allow an efficient attack has measure zero in the keyspace."

Hint: Define the keyspace as a measure space, define "efficient attack" precisely, and show that the set of vulnerable keys is measurable with measure zero.

Solution Outline:

1. Define keyspace K with measure μ
2. Define attack function $A : K \to \{0, 1\}$ (1 if attack succeeds)
3. Show $V = \{k \in K : A(k) = 1\}$ is measurable
4. Prove $\mu(V) = 0$ under security assumptions
5. Conclude $P(\text{random key} \in V) = 0$

Exercise 11.9: Optimal Approximation Bounds

For a given irrational α and bound B, what is the maximum number of rational approximations $\frac{p}{q}$ with $q \leq B$ that can satisfy $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$? How does this relate to cryptographic security?

Hint: Use the theory of continued fractions and the fact that convergents are the best approximations. Consider the growth rate of denominators in continued fraction expansions.

Solution Outline:

By Hurwitz's theorem and properties of continued fractions, there are at most $O(\log B)$ such approximations. This bounds the number of "good" keys an attacker needs to check, relating to security parameters in lattice-based cryptography.

Exercise 11.10: Quantum Resistance of Lattice Problems

Investigate why lattice problems (and the underlying Diophantine approximation problems) are believed to be resistant to quantum attacks, unlike factoring and discrete log.

Hint: Consider what makes Shor's algorithm work for factoring (period finding) and why this doesn't apply to lattice problems. Look into the structure of lattice problems vs. the structure of problems with efficient quantum algorithms.

Solution Outline:

1. Shor's algorithm relies on finding periods in abelian groups
2. Lattice problems don't have this algebraic structure
3. Best known quantum algorithms for lattices provide only polynomial speedups
4. The approximation structure doesn't yield to quantum period finding
5. This is why lattice-based crypto is post-quantum secure

11.5 Additional Challenge Problems

Exercise 11.11: Density in Higher Dimensions

Generalize the density of rationals to $\mathbb{Q}^n$ (rational points in n-dimensional space). Is $\mathbb{Q}^n$ dense in $\mathbb{R}^n$? What is its measure?

Exercise 11.12: Computational Complexity of Approximation

What is the computational complexity of finding the best rational approximation to an irrational number with denominator bounded by B? How does this relate to cryptographic assumptions?

Exercise 11.13: Measure Zero in Practice

In cryptographic implementations, "measure zero" sets might still cause problems due to implementation bugs or side channels. Discuss the gap between theoretical measure zero and practical security.

11.6 Further Reading and Exploration

For readers interested in deeper exploration:

- **Number Theory**: Hardy and Wright's "An Introduction to the Theory of Numbers" for continued fractions and Diophantine approximation

- **Measure Theory**: Royden's "Real Analysis" for rigorous treatment of Lebesgue measure
- **Lattice Cryptography**: Peikert's survey "A Decade of Lattice Cryptography" for modern developments
- **Cryptanalysis**: Boneh's "Twenty Years of Attacks on the RSA Cryptosystem" for various attacks including Wiener's

12 Conclusion

This document has explored one of mathematics' most beautiful paradoxes: rational numbers are simultaneously "everywhere" (dense) and "nowhere" (measure zero). We've seen how this seemingly abstract mathematical curiosity has profound implications for modern cryptography.

12.1 Key Takeaways

12.1.1 Mathematical Foundations

Density: Rational numbers are dense in the real numbers—between any two reals, there are infinitely many rationals. This topological property makes rationals appear "everywhere."

Countability: Despite being infinite, rational numbers are countable. They can be systematically enumerated, unlike the uncountable real numbers.

Measure Zero: Countable sets have Lebesgue measure zero. The total "length" of all rational numbers is zero, making them "nowhere" in a measure-theoretic sense.

Probability Zero: If you pick a real number at random, the probability it's rational is zero, even though rationals are dense.

12.1.2 Cryptographic Connections

Random Number Generation: Weak cryptographic keys typically form countable (hence measure zero) sets. Random key generation almost surely avoids weak keys.

Lattice-Based Cryptography: Post-quantum cryptographic systems rely on the hardness of finding good rational approximations to certain numbers—directly connecting to Diophantine approximation theory.

Cryptanalytic Attacks: Wiener's attack on RSA demonstrates how rational approximation theory can break cryptographic systems when keys are improperly chosen.

Security Proofs: The distinction between countable and uncountable sets, and the concept of measure zero, provides the mathematical language for formal security guarantees.

12.2 The Unifying Theme

The unifying theme throughout this document is the interplay between:

- **Topology** (density, "everywhere")
- **Measure Theory** (measure zero, "nowhere")
- **Probability** (almost surely, negligible probability)
- **Computation** (approximation algorithms, cryptographic security)

These different mathematical perspectives reveal different aspects of the same underlying structure, and their synthesis provides powerful tools for both pure mathematics and applied cryptography.

12.3 Implications for Cryptography

The properties of rational numbers teach us important lessons for cryptography:

1. **Theoretical Guarantees**: Measure zero provides rigorous mathematical guarantees about security, not just heuristic arguments.
2. **Key Generation**: Understanding measure zero helps design secure key generation algorithms that avoid weak keys.
3. **Post-Quantum Security**: The hardness of approximation problems (rooted in rational number theory) provides security even against quantum computers.
4. **Attack Analysis**: Understanding when and why attacks work (like Wiener's) helps design more secure systems.

12.4 Future Directions

The connections between rational numbers and cryptography continue to evolve:

- **Advanced Lattice Schemes**: New lattice-based cryptographic constructions continue to be developed, all relying on approximation hardness.
- **Quantum Algorithms**: Research into quantum algorithms for lattice problems may reveal new insights into the quantum resistance of these systems.
- **Implementation Security**: Bridging the gap between theoretical measure zero and practical implementation security remains an active area of research.
- **New Applications**: The mathematical structures explored here may find applications in other areas of cryptography and computer science.

12.5 Final Thoughts

The journey from ancient Greek mathematics—where the discovery of irrational numbers was revolutionary—to modern post-quantum cryptography demonstrates the remarkable unity of mathematics. What began as pure mathematical curiosity about the nature of numbers has become essential infrastructure for securing digital communication in the quantum era.

The "everywhere but nowhere" paradox of rational numbers is not a contradiction to be resolved, but rather a beautiful illustration of how different mathematical frameworks (topology, measure theory, probability) can reveal complementary truths about the same mathematical objects. This duality—far from being a weakness—is a source of strength, providing both theoretical guarantees and practical security.

As we move forward into an era of quantum computing and increasingly sophisticated cryptographic threats, the mathematical foundations explored in this document—rooted in the simple yet profound properties of rational numbers—will continue to guide the development of secure cryptographic systems.

Remark 12.1

The study of rational numbers, from their density to their measure zero property, exemplifies how pure mathematics provides the language and tools for understanding and securing our digital world. The "everywhere but nowhere" nature of rationals is not just a mathematical curiosity—it is a fundamental principle underlying modern cryptographic security.

Contact Information:

Website: https://vuhung16au.github.io/

GitHub: https://github.com/vuhung16au/

LinkedIn: https://www.linkedin.com/in/nguyenvuhung/

13 Glossary

This glossary provides definitions of key terms used throughout this document, organized alphabetically for easy reference.

13.1 Mathematical Terms

Almost Surely An event is said to occur almost surely if it occurs with probability 1. Equivalently, the set of outcomes where it does not occur has measure zero.

Countable Set A set is countable if it can be put into a one-to-one correspondence with the natural numbers. The rational numbers are countable, while the real numbers are uncountable.

Density A set A is dense in a set B if every point in B is either in A or is a limit point of A. Rational numbers are dense in the real numbers.

Diophantine Approximation The study of how well real numbers (especially irrational numbers) can be approximated by rational numbers. This is fundamental to lattice-based cryptography.

Lebesgue Measure A way of assigning a "size" or "length" to subsets of the real line. The Lebesgue measure of a countable set is zero.

Measure Zero A set has measure zero if it can be covered by a countable collection of intervals whose total length is arbitrarily small. Countable sets, including the rational numbers, have measure zero.

Topology The branch of mathematics concerned with properties of space that are preserved under continuous deformations. Density is a topological property.

Uncountable Set A set that cannot be put into a one-to-one correspondence with the natural numbers. The real numbers are uncountable.

13.2 Cryptographic Terms

Continued Fractions An expression of the form $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$, where a_0 is an integer and $a_1, a_2, \ldots$ are positive integers. Continued fractions provide the best rational approximations to irrational numbers.

Convergent In the context of continued fractions, a convergent is a rational approximation obtained by truncating the continued fraction expansion. Convergents are the best approximations.

Diophantine Approximation (See Mathematical Terms) Used in cryptography to find rational approximations that reveal private keys.

Keyspace The set of all possible keys that can be used in a cryptographic system. For a key of length n bits, the keyspace has size 2^n.

Lattice A discrete subgroup of $\mathbb{R}^n$ consisting of all integer linear combinations of linearly independent basis vectors. Lattice problems form the basis of post-quantum cryptography.

Lattice-Based Cryptography Cryptographic systems whose security relies on the computational hardness of lattice problems, such as finding short vectors in lattices.

Negligible Probability In cryptography, a probability that is smaller than any polynomial function of the security parameter. This concept is directly related to measure zero.

Post-Quantum Cryptography Cryptographic systems designed to be secure against attacks by quantum computers. Lattice-based cryptography is a leading candidate.

Weak Key A cryptographic key that, due to its mathematical properties, makes the cryptographic system vulnerable to attack or easier to break than intended. Weak keys typically form a countable (hence measure zero) set.

Wiener's Attack A cryptanalytic attack on RSA that exploits small private exponents by finding rational approximations to fractions derived from the public key using continued fractions.

References

[1] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 6th edition, 2008.

[2] National Institute of Standards and Technology (NIST). Post-quantum cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography, 2024. Accessed: 2024.

[3] C. Peikert. A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4):283–424, 2016.

[4] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):1–40, 2009.

[5] K. H. Rosen. *Elementary Number Theory and Its Applications*. Pearson, 6th edition, 2010.

[6] Chalk Talk. The rational numbers are not so 'rational' | everywhere but nowhere. YouTube video, 2024. Accessed: 2024.

[7] M. J. Wiener. Cryptanalysis of short rsa secret exponents. *IEEE Transactions on Information Theory*, 36(3):553–558, 1990.