Lecture 1: Introduction to Analytic Number Theory

Lanling King

University of HOK

April 2025

About These Slides

- I'll try to make the slides self-contained.
- A prior course in complex analysis is helpful, but not absolutely necessary — I'll review tools as we go.
- Suggested texts:
  - Tom M. Apostol – *Introduction to Analytic Number Theory*
  - M. Ram Murty – *Problems in Analytic Number Theory*
  - H. Iwaniec & E. Kowalski – *Analytic Number Theory* (advanced)

What is Analytic Number Theory?

- It's a branch of mathematics where we study properties of whole numbers using tools from calculus.
- Questions often involve primes — for example: "How many primes are less than a million?"
- We'll use ideas like limits, infinite series, and functions to explore these patterns.
- It turns out that some of the deepest results in number theory come from this approach.
- Many problems in analytic number theory are incredibly easy to state — but surprisingly difficult to solve.

The Riemann Zeta Function and Riemann Hypothesis

- The Riemann zeta function is defined (for $\Re(s) > 1$) by the infinite series:
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

The Riemann Zeta Function and Riemann Hypothesis

- The Riemann zeta function is defined (for $\Re(s) > 1$) by the infinite series:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

- The Riemann hypothesis states that all nontrivial zeros of the Riemann zeta function lie on the critical line $\Re(s) = \frac{1}{2}$.

The Riemann Zeta Function and Riemann Hypothesis

- The Riemann zeta function is defined (for $\Re(s) > 1$) by the infinite series:
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$
- The Riemann hypothesis states that all nontrivial zeros of the Riemann zeta function lie on the critical line $\Re(s) = \frac{1}{2}$.
- The Riemann Hypothesis remains unsolved — it is one of the 7 Clay Millennium Prize Problems, with a \$1,000,000 reward.

The Twin Prime Conjecture and Modern Breakthroughs

- The Twin Prime Conjecture states that there are infinitely many primes p such that $p + 2$ is also prime.

The Twin Prime Conjecture and Modern Breakthroughs

- The Twin Prime Conjecture states that there are infinitely many primes p such that $p + 2$ is also prime.
- It is easy to state, but remains unsolved after more than 2000 years.

The Twin Prime Conjecture and Modern Breakthroughs

- The Twin Prime Conjecture states that there are infinitely many primes p such that $p + 2$ is also prime.
- It is easy to state, but remains unsolved after more than 2000 years.
- In 2005, Goldston–Pintz–Yıldırım (GPY) developed a method showing primes often come unusually close together.

The Twin Prime Conjecture and Modern Breakthroughs

- The Twin Prime Conjecture states that there are infinitely many primes p such that $p + 2$ is also prime.
- It is easy to state, but remains unsolved after more than 2000 years.
- In 2005, Goldston–Pintz–Yıldırım (GPY) developed a method showing primes often come unusually close together.
- In 2013, Yitang Zhang proved that there are infinitely many pairs of primes less than 70,000,000 apart — the first bounded gap!

The Twin Prime Conjecture and Modern Breakthroughs

- The Twin Prime Conjecture states that there are infinitely many primes p such that $p + 2$ is also prime.
- It is easy to state, but remains unsolved after more than 2000 years.
- In 2005, Goldston–Pintz–Yıldırım (GPY) developed a method showing primes often come unusually close together.
- In 2013, Yitang Zhang proved that there are infinitely many pairs of primes less than 70,000,000 apart — the first bounded gap!
- Soon after, James Maynard simplified the method and improved the bound; Tao helped lead a massive online project (Polymath8) that brought it under 250.

The Twin Prime Conjecture and Modern Breakthroughs

- The Twin Prime Conjecture states that there are infinitely many primes p such that $p + 2$ is also prime.
- It is easy to state, but remains unsolved after more than 2000 years.
- In 2005, Goldston–Pintz–Yıldırım (GPY) developed a method showing primes often come unusually close together.
- In 2013, Yitang Zhang proved that there are infinitely many pairs of primes less than 70,000,000 apart — the first bounded gap!
- Soon after, James Maynard simplified the method and improved the bound; Tao helped lead a massive online project (Polymath8) that brought it under 250.
- The conjecture remains open, but these results showed that primes are much more clustered than we once knew.

Theorem 1 (Euclid)

There are infinitely many prime numbers.

Theorem 1 (Euclid)

There are infinitely many prime numbers.

Proof. Assume that there are only finitely many primes $p_1, p_2, \ldots, p_n$.

Theorem 1 (Euclid)

There are infinitely many prime numbers.

Proof. Assume that there are only finitely many primes $p_1, p_2, \ldots, p_n$.
Consider the number:

$$m = p_1 \cdot p_2 \cdots p_n + 1$$

Theorem 1 (Euclid)

There are infinitely many prime numbers.

Proof. Assume that there are only finitely many primes $p_1, p_2, \ldots, p_n$. Consider the number:

$$m = p_1 \cdot p_2 \cdots p_n + 1$$

Then m must be divisible by some prime p_k from our list (since every integer has a prime factor).

Theorem 1 (Euclid)

There are infinitely many prime numbers.

Proof. Assume that there are only finitely many primes $p_1, p_2, \ldots, p_n$. Consider the number:

$$m = p_1 \cdot p_2 \cdots p_n + 1$$

Then m must be divisible by some prime p_k from our list (since every integer has a prime factor). But then $p_k \mid m$ and $p_k \mid p_1 \cdot \cdots \cdot p_n$, so:

$$p_k \mid m - p_1 \cdots p_n = 1$$

Theorem 1 (Euclid)

There are infinitely many prime numbers.

Proof. Assume that there are only finitely many primes $p_1, p_2, \ldots, p_n$. Consider the number:

$$m = p_1 \cdot p_2 \cdots p_n + 1$$

Then m must be divisible by some prime p_k from our list (since every integer has a prime factor). But then $p_k \mid m$ and $p_k \mid p_1 \cdot \cdots \cdot p_n$, so:

$$p_k \mid m - p_1 \cdots p_n = 1$$

This is a contradiction — no prime divides 1.

Theorem 1 (Euclid)

There are infinitely many prime numbers.
Proof. Assume that there are only finitely many primes $p_1, p_2, \ldots, p_n$. Consider the number:

$$m = p_1 \cdot p_2 \cdots p_n + 1$$

Then m must be divisible by some prime p_k from our list (since every integer has a prime factor). But then $p_k \mid m$ and $p_k \mid p_1 \cdot \cdots \cdot p_n$, so:

$$p_k \mid m - p_1 \cdots p_n = 1$$

This is a contradiction — no prime divides 1. Therefore, there must be infinitely many primes. $\square$

Theorem 2: Bounding the kth Prime

Definition. Let $\pi(x)$ be the number of primes $\leq x$.

Theorem 2: Bounding the kth Prime

Definition. Let $\pi(x)$ be the number of primes $\leq x$.
Theorem 2.

$$p_k \leq 2^{2^k} \quad \text{for all } k \geq 1$$

Theorem 2: Bounding the kth Prime

Definition. Let $\pi(x)$ be the number of primes $\leq x$.
Theorem 2.

$$p_k \leq 2^{2^k} \quad \text{for all } k \geq 1$$

Idea: We adapt Euclid's proof to build increasingly large primes, using induction.

Proof by Induction

Base case: $k = 1$

$$p_1 = 2 \leq 2^2 = 4$$

Proof by Induction

Base case: $k = 1$

$$p_1 = 2 \leq 2^2 = 4$$

Inductive step: Assume $p_j \leq 2^{2^j}$ for all $1 \leq j < k$

Proof by Induction

Base case: $k = 1$

$$p_1 = 2 \leq 2^2 = 4$$

Inductive step: Assume $p_j \leq 2^{2^j}$ for all $1 \leq j < k$
Then by Euclid's idea:

$$p_k \leq p_1 \cdots p_{k-1} + 1$$

Proof by Induction

Base case: $k = 1$

$$p_1 = 2 \leq 2^2 = 4$$

Inductive step: Assume $p_j \leq 2^{2^j}$ for all $1 \leq j < k$

Then by Euclid's idea:

$$p_k \leq p_1 \cdots p_{k-1} + 1$$

Using the inductive bounds:

$$p_k \leq 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^{k-1}} + 1 = 2^{2^1+2^2+\cdots+2^{k-1}} + 1$$

Proof by Induction

Base case: $k = 1$

$$p_1 = 2 \leq 2^2 = 4$$

Inductive step: Assume $p_j \leq 2^{2^j}$ for all $1 \leq j < k$
Then by Euclid's idea:

$$p_k \leq p_1 \cdots p_{k-1} + 1$$

Using the inductive bounds:

$$p_k \leq 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^{k-1}} + 1 = 2^{2^1+2^2+\cdots+2^{k-1}} + 1$$

But $2^1 + 2^2 + \cdots + 2^{k-1} = 2^k - 2$, so:

$$p_k \leq 2^{2^k-2} + 1 \leq 2^{2^k}$$

$\therefore$ The bound holds. $\square$

Theorem 3: Lower Bound for $\pi(x)$

Theorem. For $x \geq 2$, we have:

$$\pi(x) \geq \log\log x$$

Theorem 3: Lower Bound for $\pi(x)$

Theorem. For $x \geq 2$, we have:

$$\pi(x) \geq \log \log x$$

Proof.

- First, check that the inequality holds for $2 \leq x \leq 4$ (e.g., $\pi(4) = 2 \geq \log \log 4 \approx 0.83$).

Theorem 3: Lower Bound for $\pi(x)$

Theorem. For $x \geq 2$, we have:

$$\pi(x) \geq \log \log x$$

Proof.

- First, check that the inequality holds for $2 \leq x \leq 4$ (e.g., $\pi(4) = 2 \geq \log \log 4 \approx 0.83$).
- Now let $x > 4$, and choose $s \in \mathbb{N}$ such that:

$$2^{2^s} \leq x < 2^{2^{s+1}}$$

Theorem 3: Lower Bound for $\pi(x)$

Theorem. For $x \geq 2$, we have:

$$\pi(x) \geq \log \log x$$

Proof.

- First, check that the inequality holds for $2 \leq x \leq 4$ (e.g., $\pi(4) = 2 \geq \log \log 4 \approx 0.83$).
- Now let $x > 4$, and choose $s \in \mathbb{N}$ such that:

$$2^{2^s} \leq x < 2^{2^{s+1}}$$

- By Theorem 2, $x \geq 2^{2^s} \Rightarrow \pi(x) \geq s$.

Theorem 3: Lower Bound for $\pi(x)$

Theorem. For $x \geq 2$, we have:

$$\pi(x) \geq \log\log x$$

Proof.

- First, check that the inequality holds for $2 \leq x \leq 4$ (e.g., $\pi(4) = 2 \geq \log\log 4 \approx 0.83$).
- Now let $x > 4$, and choose $s \in \mathbb{N}$ such that:

$$2^{2^s} \leq x < 2^{2^{s+1}}$$

- By Theorem 2, $x \geq 2^{2^s} \Rightarrow \pi(x) \geq s$.
- Taking logs twice:

$$x < 2^{2^{s+1}} \Rightarrow \log x < 2^{s+1}\log 2 \Rightarrow \frac{\log\log x}{\log 2} < s + 1$$

Theorem 3: Lower Bound for $\pi(x)$

Theorem. For $x \geq 2$, we have:

$$\pi(x) \geq \log \log x$$

Proof.

- First, check that the inequality holds for $2 \leq x \leq 4$ (e.g., $\pi(4) = 2 \geq \log \log 4 \approx 0.83$).
- Now let $x > 4$, and choose $s \in \mathbb{N}$ such that:

$$2^{2^s} \leq x < 2^{2^{s+1}}$$

- By Theorem 2, $x \geq 2^{2^s} \Rightarrow \pi(x) \geq s$.
- Taking logs twice:

$$x < 2^{2^{s+1}} \Rightarrow \log x < 2^{s+1} \log 2 \Rightarrow \frac{\log \log x}{\log 2} < s + 1$$

- Thus:

$$\pi(x) \geq s > \frac{\log \log x}{\log 2} - 1 > \log \log x \quad \text{for } x > 4.$$

Theorem 3: Lower Bound for $\pi(x)$

Theorem. For $x \geq 2$, we have:

$$\pi(x) \geq \log\log x$$

Proof.

- First, check that the inequality holds for $2 \leq x \leq 4$ (e.g., $\pi(4) = 2 \geq \log\log 4 \approx 0.83$).
- Now let $x > 4$, and choose $s \in \mathbb{N}$ such that:

$$2^{2^s} \leq x < 2^{2^{s+1}}$$

- By Theorem 2, $x \geq 2^{2^s} \Rightarrow \pi(x) \geq s$.
- Taking logs twice:

$$x < 2^{2^{s+1}} \Rightarrow \log x < 2^{s+1}\log 2 \Rightarrow \frac{\log\log x}{\log 2} < s+1$$

- Thus:

$$\pi(x) \geq s > \frac{\log\log x}{\log 2} - 1 > \log\log x \quad \text{for } x > 4.$$

Theorem 3: Lower Bound for $\pi(x)$

Theorem. For $x \geq 2$, we have:

$$\pi(x) \geq \log\log x$$

Proof.

- First, check that the inequality holds for $2 \leq x \leq 4$ (e.g., $\pi(4) = 2 \geq \log\log 4 \approx 0.83$).
- Now let $x > 4$, and choose $s \in \mathbb{N}$ such that:

$$2^{2^s} \leq x < 2^{2^{s+1}}$$

- By Theorem 2, $x \geq 2^{2^s} \Rightarrow \pi(x) \geq s$.
- Taking logs twice:

$$x < 2^{2^{s+1}} \Rightarrow \log x < 2^{s+1} \log 2 \Rightarrow \frac{\log\log x}{\log 2} < s + 1$$

- Thus:

$$\pi(x) \geq s > \frac{\log\log x}{\log 2} - 1 > \log\log x \quad \text{for } x > 4.$$

$\therefore$ The inequality holds for all $x \geq 2$. $\square$

Fermat Primes

Definition. The nth **Fermat number** is defined as:

$$F_n = 2^{2^n} + 1$$

Fermat Primes

Definition. The *n*th **Fermat number** is defined as:

$$F_n = 2^{2^n} + 1$$

Examples:

$$F_0 = 3$$
$$F_1 = 5$$
$$F_2 = 17$$
$$F_3 = 257$$
$$F_4 = 65537$$

Fermat Primes

Definition. The nth **Fermat number** is defined as:

$$F_n = 2^{2^n} + 1$$

Examples:

$$F_0 = 3$$
$$F_1 = 5$$
$$F_2 = 17$$
$$F_3 = 257$$
$$F_4 = 65537$$

These five numbers are all prime — they are known as the **Fermat primes**.

Fermat Primes

Definition. The *n*th **Fermat number** is defined as:

$$F_n = 2^{2^n} + 1$$

Examples:

$$\begin{aligned} F_0 &= 3 \\ F_1 &= 5 \\ F_2 &= 17 \\ F_3 &= 257 \\ F_4 &= 65537 \end{aligned}$$

These five numbers are all prime — they are known as the **Fermat primes**. However, it is conjectured that no other Fermat numbers are prime.

Fermat Primes

Definition. The nth **Fermat number** is defined as:

$$F_n = 2^{2^n} + 1$$

Examples:

$$F_0 = 3$$
$$F_1 = 5$$
$$F_2 = 17$$
$$F_3 = 257$$
$$F_4 = 65537$$

These five numbers are all prime — they are known as the **Fermat primes**.
However, it is conjectured that no other Fermat numbers are prime.
In fact, it is known that F_n is composite for $5 \leq n \leq 32$ (and beyond!).

Fermat Primes

Definition. The nth **Fermat number** is defined as:

$$F_n = 2^{2^n} + 1$$

Examples:

$$F_0 = 3$$
$$F_1 = 5$$
$$F_2 = 17$$
$$F_3 = 257$$
$$F_4 = 65537$$

These five numbers are all prime — they are known as the **Fermat primes**.
However, it is conjectured that no other Fermat numbers are prime.
In fact, it is known that F_n is composite for $5 \leq n \leq 32$ (and beyond!).
Fermat originally believed that all F_n would be prime — Euler disproved this by showing F_5 is divisible by 641.

Theorem 4 (Polya)

Theorem. If n and m are integers with $1 \leq n < m$, then:

$$\gcd(F_n, F_m) = 1 \quad \text{where } F_k = 2^{2^k} + 1$$

Theorem 4 (Polya)

Theorem. If n and m are integers with $1 \leq n < m$, then:

$$\gcd(F_n, F_m) = 1 \quad \text{where } F_k = 2^{2^k} + 1$$

Proof.

- Let $m = n + k$ for some $k \geq 1$.

Theorem 4 (Polya)

Theorem. If n and m are integers with $1 \leq n < m$, then:

$$\gcd(F_n, F_m) = 1 \quad \text{where } F_k = 2^{2^k} + 1$$

Proof.

- Let $m = n + k$ for some $k \geq 1$.
- We will show that $F_n \mid F_m - 2$.

Theorem 4 (Polya)

Theorem. If n and m are integers with $1 \leq n < m$, then:

$$\gcd(F_n, F_m) = 1 \quad \text{where } F_k = 2^{2^k} + 1$$

Proof.

- Let $m = n + k$ for some $k \geq 1$.
- We will show that $F_n \mid F_m - 2$.
- Note: $F_m - 2 = 2^{2^m} - 1$

Theorem 4 (Polya)

Theorem. If n and m are integers with $1 \leq n < m$, then:

$$\gcd(F_n, F_m) = 1 \quad \text{where } F_k = 2^{2^k} + 1$$

Proof.

- Let $m = n + k$ for some $k \geq 1$.
- We will show that $F_n \mid F_m - 2$.
- Note: $F_m - 2 = 2^{2^m} - 1$
- Let $x = 2^{2^n}$. Then:

$$F_n = x + 1, \quad F_m - 2 = x^{2^k} - 1$$

Theorem 4 (Polya)

Theorem. If n and m are integers with $1 \leq n < m$, then:

$$\gcd(F_n, F_m) = 1 \quad \text{where } F_k = 2^{2^k} + 1$$

Proof.

- Let $m = n + k$ for some $k \geq 1$.
- We will show that $F_n \mid F_m - 2$.
- Note: $F_m - 2 = 2^{2^m} - 1$
- Let $x = 2^{2^n}$. Then:

$$F_n = x + 1, \quad F_m - 2 = x^{2^k} - 1$$

- So:

$$\frac{F_m - 2}{F_n} = \frac{x^{2^k} - 1}{x + 1} \in \mathbb{Z} \Rightarrow F_n \mid F_m - 2$$

Theorem 4 (Polya)

Theorem. If n and m are integers with $1 \leq n < m$, then:

$$\gcd(F_n, F_m) = 1 \quad \text{where } F_k = 2^{2^k} + 1$$

Proof.

- Let $m = n + k$ for some $k \geq 1$.
- We will show that $F_n \mid F_m - 2$.
- Note: $F_m - 2 = 2^{2^m} - 1$
- Let $x = 2^{2^n}$. Then:

$$F_n = x + 1, \quad F_m - 2 = x^{2^k} - 1$$

- So:

$$\frac{F_m - 2}{F_n} = \frac{x^{2^k} - 1}{x + 1} \in \mathbb{Z} \Rightarrow F_n \mid F_m - 2$$

- If $d \mid F_n$ and $d \mid F_m$, then $d \mid 2$.

Theorem 4 (Polya)

Theorem. If n and m are integers with $1 \leq n < m$, then:

$$\gcd(F_n, F_m) = 1 \quad \text{where } F_k = 2^{2^k} + 1$$

Proof.

- Let $m = n + k$ for some $k \geq 1$.
- We will show that $F_n \mid F_m - 2$.
- Note: $F_m - 2 = 2^{2^m} - 1$
- Let $x = 2^{2^n}$. Then:

$$F_n = x + 1, \quad F_m - 2 = x^{2^k} - 1$$

- So:

$$\frac{F_m - 2}{F_n} = \frac{x^{2^k} - 1}{x + 1} \in \mathbb{Z} \Rightarrow F_n \mid F_m - 2$$

- If $d \mid F_n$ and $d \mid F_m$, then $d \mid 2$.
- But all Fermat numbers are odd, so $d = 1$.

Theorem 4 (Polya)

Theorem. If n and m are integers with $1 \leq n < m$, then:

$$\gcd(F_n, F_m) = 1 \quad \text{where } F_k = 2^{2^k} + 1$$

Proof.

- Let $m = n + k$ for some $k \geq 1$.
- We will show that $F_n \mid F_m - 2$.
- Note: $F_m - 2 = 2^{2^m} - 1$
- Let $x = 2^{2^n}$. Then:

$$F_n = x + 1, \quad F_m - 2 = x^{2^k} - 1$$

- So:

$$\frac{F_m - 2}{F_n} = \frac{x^{2^k} - 1}{x + 1} \in \mathbb{Z} \Rightarrow F_n \mid F_m - 2$$

- If $d \mid F_n$ and $d \mid F_m$, then $d \mid 2$.
- But all Fermat numbers are odd, so $d = 1$.

Theorem 4 (Polya)

Theorem. If n and m are integers with $1 \leq n < m$, then:

$$\gcd(F_n, F_m) = 1 \quad \text{where } F_k = 2^{2^k} + 1$$

Proof.

- Let $m = n + k$ for some $k \geq 1$.
- We will show that $F_n \mid F_m - 2$.
- Note: $F_m - 2 = 2^{2^m} - 1$
- Let $x = 2^{2^n}$. Then:

$$F_n = x + 1, \quad F_m - 2 = x^{2^k} - 1$$

- So:

$$\frac{F_m - 2}{F_n} = \frac{x^{2^k} - 1}{x + 1} \in \mathbb{Z} \Rightarrow F_n \mid F_m - 2$$

- If $d \mid F_n$ and $d \mid F_m$, then $d \mid 2$.
- But all Fermat numbers are odd, so $d = 1$.

$\therefore$ $\gcd(F_n, F_m) = 1$. $\square$