# Analytic Number Theory

Daniel Naylor

March 3, 2025

## Contents



Lecture 1

What is analytic number theory?

- Study of number-theoretic problems using analysis (real, complex, Fourier, …)
- Also tools from combinatorics, probability, …

What kind of problems are studied?

A variety of problems about integers, especially primes.

- Are there infinitely many primes? (Euclid, 300BC)
- Are there infinitely many primes starting with 7 in base 10? (follows from prime number theorem)
- Are there infinitely many primes ending with 7 in base 10? (follows from Dirichlet's theorem)
- Are there infinitely many primes with 49% of the digits being 7 in base 10? would follow from the Riemann hypothesis
- Are there infinitely many pairs of primes differing by 2? (twin prime conjecture)

Key feature: To show that a set (of primes) is infinite, want to estimate the number of elements $\leq x$.

**Definition.** Define

$$\pi(x) = |\{\text{primes} \leq x\}| = \sum_{p \leq x} 1.$$

Euclid showed: $\lim_{x\to\infty} \pi(x) = \infty$.

**Theorem** (Prime number theorem)**.**

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$$

$\pi(x) \sim \frac{x}{\log x}$. (Conjectured: Legendre, Gauss. Proved: Hadamard, de la Vallée Poussin)

# 1 Estimating Primes

**Theorem** (Euler). $\sum_p \frac{1}{p} = \infty$.

*Proof.* Consider $p_N = \prod_p^N \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^N}\right)$, for $N \in \mathbb{N} = \{1, 2, 3, \ldots\}$. We have:

$$\begin{aligned}
p_N &\geq \sum_{n=1}^{N} \frac{1}{n} \\
&\geq \sum_{n=1}^{N-1} \int_n^{n+1} \frac{\mathrm{d}t}{t} \\
&= \int_1^{N-1} \frac{\mathrm{d}t}{t} \\
&= \log(N-1)
\end{aligned}$$

On the other hand, using $1 + x \leq e^x$, so

$$\begin{aligned}
p_N &\leq \prod_{p \leq N} \exp\left(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^N}\right) \\
&= \exp\left(\sum_{p \leq N} \left(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^N}\right)\right) \\
&\leq \exp\left(\sum_{p \leq N} \left(\frac{1}{p} + \frac{1}{p^2 - p}\right)\right) \\
&\leq \exp\left(C + \sum_{p \leq N} \frac{1}{p}\right)
\end{aligned}$$

Comparing these two bounds gives

$$\sum_{p \leq N} \frac{1}{p} \geq \log\log(N-1) - C.$$

Then letting $N \to \infty$ gives the desired result. □

**Theorem** (Chebyshev's Theorem).

$$\pi(x) \leq \frac{cx}{\log x}$$

(for $x \geq 2$, where $c$ is an absolute constant).

*Proof.* Consider

$$\begin{aligned} S_N &= \binom{2N}{N} \\ &= \frac{(2N)!}{(N!)^2} \end{aligned}$$

for $N \in \mathbb{N}$. We have

$$S_N \leq \sum_{j=0}^{2N} \binom{2N}{j} = (1+1)^{2N} = 4^N.$$

On the other hand,

$$S_N = \prod_{p \leq 2N} p^{\alpha^p(N)}$$

where $\alpha_p(N)$ is the largest $j$ such that $p^j \mid \binom{2N}{N}$. We have $\alpha_p(N) = 1$ for $p \in (N, 2N]$. So

$$(\log 4)N \geq \sum_{N < p \leq 2N} \log p.$$

Take $N = \lceil \frac{x}{2} \rceil$, for $x \geq 2$. Hence

$$\sum_{x < p \leq 2x} \log p \leq (\log 4) \left\lceil \frac{x}{2} \right\rceil + \log x \leq (\log 4)\frac{x}{2} + \log 4 + \log x.$$

Then

$$\begin{aligned} \sum_{p \leq x} &\leq \sum_{0 \leq j \leq \frac{\log x}{\log 2}} \left( (\log 4)\frac{x}{2^{j+2}} + \log x \right) \qquad \text{(telescoping summation, take } \frac{x}{2}, \frac{x}{2^2}, \frac{x}{2^3}, \ldots) \\ &\leq (\log 4)x + (\log x)^2 + 1 \end{aligned}$$

Lecture 2

So for $x \geq 2$ and a suitable large enough constant $c'$, we have

$$\sum_{p \leq x} \leq (\log 4)x + c'(\log x)^2.$$

Hence

$$\sum_{\frac{x}{(\log x)^2}<p\le x} \log p \le (\log 4)x + c'(\log x)^2$$

$$\implies \log \frac{x}{(\log x)^2}\left(\pi(x) - \pi\left(\frac{x}{(\log x)^2}\right)\right) \le (\log 4)x + c'(\log x)^2$$

$$\implies \pi(x) \le \frac{x}{(\log x)^2} + (\log 4)\frac{x}{\log \frac{x}{(\log x)^2}} + c'\frac{(\log x)^2}{\log \frac{x}{(\log x)^2}}$$

$$\le (\log 4 + \varepsilon)\frac{x}{\log x}$$

for any $\varepsilon$, as long as $x \ge x(\varepsilon)$.

Take $\varepsilon = 1$. Choose $c > 0$ large enough. □

## 1.1 Asymptotic Notation

**Definition 1.1** (Big $O$ and little $o$ notation)**.** Let $f, g, h : S \to \mathbb{C}$, $S \subseteq \mathbb{C}$.
Write $f(x) = O(g(x))$ if there is $c > 0$ such that $|f(x)| \le c|g(x)|$ for all $x \in S$.
Write $f(x) = o(g(x))$ if for any $\varepsilon > 0$ there is $x_\varepsilon > 0$ such that $|f(x)| \le \varepsilon|g(x)|$ for $x \in S$, $|x| \ge x_\varepsilon$.
Write $f(x) = g(x) + O(h(x))$ if $f(x) - g(x) = O(h(x))$ and write $f(x) = g(x) + o(h(x))$ if $f(x) - g(x) = o(h(x))$.

**Definition 1.2** (Vinogradov notation)**.** Let $f, g, h : S \to \mathbb{C}$, $S \subseteq \mathbb{C}$.
Write $f(x) \ll g(x)$ or $g(x) \gg f(x)$ if $f(x) = O(g(x))$.

**Example.**

- $(\log x)^1 00 \ll \exp(\sqrt{\log x}) \ll x^{\frac{1}{100}}$ $(x \le 1)$, since $\lim_{x\to\infty} \frac{(\log x)^{100}}{\exp(\sqrt{\log x})} = 0$, $\lim_{x\to\infty} \frac{\exp(\sqrt{\log x})}{x^{\frac{1}{100}}} = 0$.
- $100x + 100 \ll x \ll \frac{x}{100}$ (for $x \ge 1$).
- $e^x = 1 + x + O(x^2)$ for $x \in [-10, 10]$, since $e^x = 1 + x + \sum_{n=2}^{\infty} \frac{x^n}{n!}$.
- $\lfloor x \rfloor = x + O(1)$ for $x \in \mathbb{R}$ (since $\lfloor x \rfloor \in (x - 1, x]$).
- $\frac{x+1}{x} = 1 + o(1)$ (for $x \ge 1$).

**Lemma.** Let $f, g, h, u : S \to \mathbb{C}$.

(i) If $f(x) = O(g(x))$ and $g(x) = O(h(x))$, then $f(x) = O(h(x))$ (transitivity).

(ii) If $f(x) = O(h(x))$ and $g(x) = O(u(x))$, then $f(x) + g(x) = O(|h(x)| + |u(x)|)$.

(iii) If $f(x) = O(h(x))$ and $g(x) = O(u(x))$, then $f(x)g(x) = O(h(x)u(x))$.

*Proof.* Follows from the definition in a straightforward way. Example:

(iii) $|f(x)| \leq c_1|h(x)|$, $|g(x)| \leq c_2|u(x)|$. Then $|f(x)g(x)| \leq c_1c_2|h(x)u(x)|$, so $f(x)g(x) = O(h(x)u(x))$. □

## 1.2 Partial Summation

**Lemma 1.3** (Partial Summation)**.** Assuming that:

- $(a_n)_{n\in\mathbb{N}}$ are complex numbers
- $x \geq y \geq 0$
- $f : [y, x] \to \mathbb{C}$ is continuously differentiable

Then

$$\sum_{y<n\leq x} a_n f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)\mathrm{d}t,$$

where for $t \geq 1$, we define

$$A(t) = \sum_{n\leq t} a_n = \sum_{n=1}^{\lfloor t\rfloor} a_n.$$

*Proof.* It suffices to prove the $y = 0$ case, since then

$$\sum_{y<n\leq x} a_n f(n) = \sum_{0<n\leq x} a_n f(n) - \sum_{0<n\leq y} a_n f(n).$$

Suppose $y = 0$. By the fundamental theorem of calculus,

$$f(n) = f(x) - \int_n^x f'(t)\mathrm{d}t = \int_0^x f'(t)\mathbb{1}_{[n,x]}(t)\mathrm{d}t.$$

Summing over $n \le x$, we get

$$\sum_{n\le x} a_n f(n) = A(x)f(x) - \int_0^x f'(t)\left(\sum_{n\le x} \mathbb{1}_{[n,x]}(t) a_n\right)\mathrm{d}t$$
$$= A(x)f(x) - \int_0^x f'(t)A(t)\mathrm{d}t \qquad \square$$

Lecture 3

**Lemma.** If $x \ge 1$, then

$$\sum_{n\le x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right),$$

where $\gamma \in \mathbb{R}$ is Euler's constant, which is given by $\gamma = \lim_{N\to\infty} \sum_{k=1}^{N} \frac{1}{k} - \log N$.

*Proof.* Apply Partial Summation with $a_n = 1$, $f(t) = \frac{1}{t}$, $y = \frac{1}{2}$. Clearly $A(t) = \lfloor t \rfloor$. Then,

$$\sum_{n\le x} \frac{1}{n} = \frac{\lfloor x \rfloor}{x} + \int_1^x \frac{\lfloor t \rfloor}{t^2}\mathrm{d}t$$
$$= \frac{x + O(1)}{x} + \int_1^x \frac{t - \{t\}}{t^2}\mathrm{d}t$$
$$= 1 + O\left(\frac{1}{x}\right) + \log x - \int_1^x \frac{\{t\}}{t^2}\mathrm{d}t$$
$$= 1 + \log x - \int_1^\infty \frac{\{t\}}{t^2}\mathrm{d}t + O\left(\frac{1}{x}\right)$$

The last equality is true since $\int_x^\infty \frac{\{t\}}{t^2}\mathrm{d}t \le \int_x^\infty \frac{1}{t^2}\mathrm{d}t = \frac{1}{x}$.

Let $\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2}\mathrm{d}t$. Then we have the asymptotic equation as desired.

Taking $x \to \infty$ in the formula, we see that $\gamma$ is equal to the formula for Euler's constant, as desired. $\square$

**Lemma.** For $x \ge 1$,

$$\sum_{p\le x} \frac{1}{p} = \int_1^x \frac{\pi(t)}{t^2}\mathrm{d}t + O(1).$$

*Proof.* Apply Lemma 1.3 with $a_n = \mathbb{1}_{\mathbb{P}}(n)$ (where $\mathbb{P}$ is the set of primes), $f(t) = \frac{1}{t}$, and $y = 1$.

We get $A(t) = \pi(t)$, and then

$$\sum_{p \le x} \frac{1}{p} = \frac{\pi(x)}{x} + \int_1^x \frac{\pi(t)}{t^2} \mathrm{d}t$$
$$= \int_1^x \frac{\pi(t)}{t^2} \mathrm{d}t + O(1)$$

□

## 1.3 Arithmetic Functions and Dirichlet convolution

**Definition** (Arithmetic function)**.** An *arithmetic function* is a function $f : \mathbb{N} \to \mathbb{C}$.

**Definition** (Multiplicative)**.** An arithmetic function $f$ is *multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ whenever $m, n \in \mathbb{N}$ are coprime.
Moreover, $f$ is *completely multiplicative* if $f(mn) = f(m)f(n)$ for all $m, n$.

**Example.**

- $f(n) = n^s$ for $s \in \mathbb{C}$ is completely multiplicative.
- Möbius function

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \\ 0 & n \text{ is divisible by a square of a prime} \end{cases}$$

  This is multiplicative:

  - If $\mu(mn) = 0$ and $m$, $n$ are coprime, then we must have had at least one of $\mu(m) = 0$ or $\mu(n) = 0$.
  - If $\mu(mn) = 1$, then say $m$ is a product of $k$ distinct primes and $n$ is a product of $l$ distinct primes. Then $\mu(mn) = (-1)^{k+l} = (-1)^k(-1)^l = \mu(m)\mu(n)$.
  - $\tau(n) = \sum_{n=ab} 1$ (divisor function) and $\tau_k(n) = \sum_{n=n_1 n_2 \cdots n_k} 1$ (generalised divisor function). $\tau$ and $\tau_k$ are multiplicative.

On the space of arithmetic functions, we have operations:

$$(f + g)(n) = f(n) + g(n)$$
$$(fg)(n) = f(n)g(n)$$
$$(f * g)(n) = \text{Dirichlet convolution}$$

**Definition** (Dirichlet convolution)**.** For $f, g : \mathbb{N} \to \mathbb{C}$, we define

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right),$$

where $\sum_{d|n}$ means sum over the divisors of $n$.

**Lemma 1.4.** The space of arithmetic functions with operations $+$, $*$ is a commutative ring.

*Proof.* Since arithmetic functions with $+$ form an abelian group, it suffices to show:

(i) $(f * g) * h = f * (g * h)$

(ii) $f * g = g * f$

(iii) $f * I = f$

(iv) $f * (g + h) = f * g + f * h$

Proofs:

(i) Follows from $(f * g)(n) = \sum_{n=ab} f(a)g(b)$.

(ii) Follows from $(f * g)(n) = \sum_{n=ab} f(a)g(b)$.

(iii) Take

$$I(n) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 0 \end{cases}.$$

Then one can check that $f * I = f$.

(iv) From definition. □

**Lemma.** The set of arithmetic functions $f$ with $f(1) \neq 0$ form an abelian group with operation $*$.

*Proof.* Need $g$ such that $f * g = I$.

$$(f * g)(1) = f(1)g(1) = 1 \implies g(1) = \frac{1}{f(1)}.$$

Assume $g(m)$ defined for $m < n$. We will defined $g(n)$.

$$
\begin{aligned}
(f * g)(n) &= g(n)f(1) + \sum_{\substack{d|n \\ d \neq 1}} f(d) g\left(\frac{n}{d}\right) \\
\implies g(n) &= -\frac{1}{f(1)} \sum_{\substack{d|n \\ d \neq 1}} f(d) g \underbrace{\left(\frac{n}{d}\right)}_{<n}
\end{aligned}
$$

□

Lecture 4

**Lemma.** Multiplicative arithmetic functions form an abelian group with $*$. Moreover, for completely multiplicative $f$, the Dirichlet inverse is $\mu f$.

*Proof.* For the first part, suffices to show closedness. Let $f, g : \mathbb{N} \to \mathbb{C}$ be multiplicative, and $m, n$ coprime.

If $mn = ab$, we can write $a = a_1 a_2$, $b = b_1 b_2$ where $a_1 = (a, m)$, $a_2 = (a, n)$, $b_1 = (b, m)$ and $b_2 = (b, n)$. Therefore we have:

$$
\begin{aligned}
(f * g)(mn) &= \sum_{mn = ab} f(a) g(b) \\
&= \sum_{\substack{m = a_1 b_1 \\ n = a_2 b_2}} f(a_1 a_2) g(b_1 b_2) && \text{(above observation)} \\
&= \sum_{\substack{m = a_1 b_1 \\ n = a_2 b_2}} f(a_1) f(a_2) g(b_1) g(b_2) && \text{(by multiplicativity)} \\
&= (f * g)(m)(f * g)(n)
\end{aligned}
$$

(also need to check that inverses are multiplicative).

Now, remains to show that for completely multiplicative $f$, $f * \mu f = I$.

Note that $f * \mu f$ is multiplicative by the first part. So enough to show $(f * \mu f)(p^k) = I(p^k)$ for prime powers $p^k$. Calculate:

$$
\begin{aligned}
f * \mu f(p) &= f(p) + \mu f(p) \\
&= f(p) - f(p) \\
&= 0 \\
&= I(p)
\end{aligned}
$$

and for $k \geq 2$:

$$\begin{aligned} f * \mu f(p^k) &= f(p^k) + \mu f(p) f(p^{k-1}) \\ &= f(p^k) - f(p) f(p^{k-1}) \\ &= f(p)^k - f(p) f(p)^{k-1} \\ &= 0 \\ &= I(p^k) \end{aligned}$$

□

**Example.** $\tau_k(n) = \sum_{n=n_1 \cdots n_k} 1$. Then

$$\tau_k = \underbrace{1 * 1 * \cdots * 1}_{k \text{ times}}.$$

So $\tau_k$ is multiplicative by the previous result.

**Definition** (von Mangoldt function)**.** The *von Mangoldt function* $\Lambda : \mathbb{N} \to \mathbb{R}$ is

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \\ 0 & \text{otherwise} \end{cases}$$

Then $\log = 1 * \Lambda$ since

$$\log n = \log \prod_{p|n} p^{\alpha_p(n)} = \sum_{p|n} \alpha_p(n) \log p = 1 * \Lambda(n).$$

Since $\mu$ is the inverse of 1, we have

$$\log * \mu = 1 * \Lambda * \mu = \Lambda * 1 * \mu = \Lambda * I = \Lambda.$$

## 1.4 Dirichlet Series

For a sequence $(a_n)_{n \in \mathbb{N}}$, we want to associate a generating function that gives information of $(a_n)_{n \in \mathbb{N}}$. Might consider

$$(a_n)_{n \in \mathbb{N}} \leftrightarrow \sum_{n=1}^{\infty} a_n x^n.$$

If we do this, then $\sum_p x^p$ is hard to control. So this is not very useful.

The following series has nicer number-theoretic properties:

**Definition** (Formal series)**.** For $f : \mathbb{N} \to \mathbb{C}$, define a (formal) series

$$D_f(s) = \sum_{n=1}^{\infty} f(n) n^{-s}$$

for $s \in \mathbb{C}$.

**Lemma.** Assuming that:

- $f : \mathbb{N} \to \mathbb{C}$ satisfying $|f(n)| \le n^{o(1)}$

Then $D_f(s)$ converges absolutely for $\mathrm{Re}(s) > 1$ and defines an analytic function for $\mathrm{Re}(s) > 1$.

*Proof.* Let $\varepsilon > 0$ (fixed), $n \in \mathbb{N}$ and $\mathrm{Re}(s) > 1 + 2\varepsilon$.

Then

$$\begin{aligned}
\sum_{n=N}^{\infty} |f(n) n^{-s}| &= \sum_{n=N}^{\infty} |f(n)| n^{-\mathrm{Re}(s)} \\
&\ll \sum_{n=N}^{\infty} n^{\varepsilon - \mathrm{Re}(s)} \\
&\le \sum_{n=N}^{\infty} n^{-1-\varepsilon} \\
&\le N^{-1-\varepsilon} + \sum_{n=N+1}^{\infty} \int_{n-1}^{n} t^{-1-\varepsilon} \mathrm{d}t \\
&\le N^{-1-\varepsilon} + \int_{N}^{\infty} t^{-1-\varepsilon} \mathrm{d}t \\
&\ll N^{-\varepsilon}
\end{aligned}$$

Hence we have absolute convergence for $\mathrm{Re}(s) > 1 + 2\varepsilon$. Also, $D_f(s)$ is a uniform limit of the functions $\sum_{n=1}^{N} f(n) n^{-s}$. From complex analysis, a uniform limit of analytic functions is analytic. Hence $D_f(s)$ is analytic for $\mathrm{Re}(s) > 1 + 2\varepsilon$.

Now let $\varepsilon \to 0$. □

Lecture 5

**Theorem** (Euler product)**.** Assuming that:

- $f : \mathbb{N} \to \mathbb{C}$ be bounded ($|f(n)| \ll 1$) and multiplicative

Then

$$D_f(s) = \prod_p \left(1 + \frac{f(p)}{p^2} + \frac{f(p^2)}{p^{2s}} + \cdots\right),$$

for $\mathrm{Re}(s) > 1$. Furthermore, if $f$ is completely multiplicative, then

$$D_f(s) = \prod_p \left(1 - \frac{f(p)}{p^s}\right)^{-1},$$

for $\mathrm{Re}(s) > 1$.

*Proof.* Let $N \in \mathbb{N}$, $\mathrm{Re}(s) = \sigma > 1$. Let

$$D_f(s, N) = \prod_{p \le N} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\right).$$

Note that the series defining the factors are absolutely convergent, since

$$\sum_{k=1}^{\infty} \frac{|f(p^k)|}{|p^{ks}|} \ll \sum_{k=1}^{\infty} \frac{1}{p^{ks}} < \infty$$

(geometric series).

Therefore, multiplying out,

$$D_f(s, N) = \sum_{n=1}^{\infty} a(n, N) f(n) n^{-s}$$

where

$$a(n, N) = \#\{\text{ways to write } n \text{ as a product of prime powers, where the primes are } \le N\}.$$

The fundamental theorem of arithmetic tells us that $a(n, N) \in \{0, 1\}$ and $a(n, N) = 1$ for $n \le N$.

Now,

$$\begin{aligned} |D_f(S) - D_f(s, N)| &\le \sum_{n=N+1}^{\infty} |f(n)||n^{-s}| \\ &\ll \sum_{n=N+1}^{\infty} n^{-\sigma} \\ &\overset{N\to\infty}{\longrightarrow} 0 \end{aligned}$$

(since $\sum_{n=1}^{\infty} n^{-\sigma} < \infty$). Hence $D_f(s) = \lim_{N\to\infty} D_f(s, N)$.

Finally, for $f$ completely multiplicative, use geometric formula:

$$\sum_{k=1}^{\infty} \frac{f(p)^k}{p^{ks}} = \frac{1}{1 - \frac{f(p)}{p^s}}.$$ □

**Lemma.** Assuming that:

- $f, g : \mathbb{N} \to \mathbb{C}$
- $|f(n)|, |g(n)| \le n^{o(1)}$

Then

$$D_{f*g}(s) = D_f(s) D_g(s)$$

for $\mathrm{Re}(s) > 1$.

*Proof.* We know $D_f(s)$ and $D_g(s)$ are absolutely convergent, so can expand out the product.

$$\begin{aligned} D_f(s) D_g(s) &= \sum_{a,b=1}^{\infty} f(a) g(b) (ab)^{-s} \qquad = \sum_{n=1} \sum_{n=ab} f(a) g(b) n^{-s} \\ &= \sum_{n=1}^{\infty} (f * g)(n) n^{-s} \\ &= D_{f*g}(s) \end{aligned}$$

□

**Definition** (Riemann zeta function)**.** For $\mathrm{Re}(s) > 1$, define

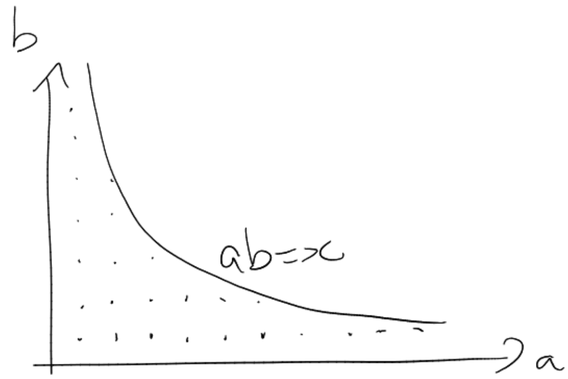
$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

**Example.**

- $\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \zeta(s)^2$ for $\mathrm{Re}(s) > 1$ (since $\tau = 1 * 1$).
- $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$ for $\mathrm{Re}(s) > 1$ (since $\mu$ is the Dirichlet inverse of 1, so $\mu * 1 = I$).
- $\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s}$ for $\mathrm{Re}(s) > 1$, since $\frac{\mathrm{d}}{\mathrm{d}s} n^{-s} = -(\log n) n^{-s}$. Can differentiate termwise, since if $F_n$ analytic and $F_n \to F$ uniformly, then $F$ is analytic and $F_n' \to F'$. We know that $\sum_{n=1}^{\infty} f(n) n^{-s}$ converges uniformly for $\mathrm{Re}(s) > 1$ if $|f(n)| \le n^{o(1)}$.
- $\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$ for $\mathrm{Re}(s) > 1$. This is because $-\log = -1 * \Lambda$ – see the definition of the von Mangoldt function.

### Dirichlet hyperbola method

Problem: How many lattice points $(a, b) \in \mathbb{N}^2$ satisfy $ab \le x$?




Note that this number is $\sum_{n \le x} \tau(n) = \sum_{ab \le x} 1$.

Dirichlet proved that for $x \ge 2$,

$$\sum_{n \le x} \tau(n) = x \log x + (2\gamma - 1)x + O(x^{1/2})$$

where $\gamma$ is Euler's constant.

We will see a proof of this shortly.

Conjecture: Can have $O_\varepsilon(x^{\frac{1}{4}+\varepsilon})$. Current best exponent is 0.314.

First, we prove a lemma:

**Lemma** (Dirichlet hyperbola method)**.** Assuming that:

- $f, g : \mathbb{N} \to \mathbb{C}$
- $x \ge y \ge 1$

Then

$$\sum_{n \le x} (f * g)(n) = \sum_{d \le y} f(d) \sum_{m \le \frac{x}{d}} g(m) + \sum_{m \le \frac{x}{y}} g(m) \sum_{y < d \le \frac{x}{m}} f(d).$$

*Proof.* $\sum_{n \le x} (f * g)(n) = \sum_{dm \le x} f(d)g(m)$. Split this sum into parts with $d \le y$ and $d > y$ to get the conclusion. □

Lecture 6

**Theorem 1.5** (Dirichlet's divisor problem)**.** For $x \geq 2$,

$$\sum_{n \leq x} \tau(n) = x \log x + (2\gamma - 1)x + O(x^{1/2})$$

where $\gamma$ is Euler's constant.

*Proof.* We use the Dirichlet hyperbola method, with $y = x^{\frac{1}{2}}$. Note that $\tau = 1 * 1$. Then,

$$\begin{aligned}\sum_{n \leq x} \tau(n) &= \sum_{d \leq x^{\frac{1}{2}}} \sum_{m \leq \frac{x}{d}} 1 + \sum_{m \leq x^{\frac{1}{2}}} \sum_{x^{\frac{1}{2}} < d \leq \frac{x}{m}} 1 \\ &= \sum_{x \leq x^{\frac{1}{2}}} \left(\frac{x}{d} + O(1)\right) + \sum_{m \leq x^{\frac{1}{2}}} \left(\frac{x}{m} - x^{\frac{1}{2}} + O(1)\right) \\ &= x \sum_{d \leq x^{\frac{1}{2}}} \frac{1}{d} + x \sum_{m \leq x^{\frac{1}{2}}} \frac{1}{m} - \sum_{m \leq x^{\frac{1}{2}}} x^{\frac{1}{2}} + O(x^{\frac{1}{2}})\end{aligned}$$

Recall from Lecture 2 that

$$\sum_{d \leq y} \frac{1}{d} = \log y + \gamma + O\left(\frac{1}{y}\right).$$

Taking $y = x^{\frac{1}{2}}$, the previous expression becomes

$$2 \times \left(\frac{1}{2} \log x + \gamma + O\left(\frac{1}{x^{\frac{1}{2}}}\right)\right) - x + O(x^{\frac{1}{2}}) = x \log x + (2\gamma - 1)x + O(x^{\frac{1}{2}}).$$ □

# 2 Elementary Estimates for Primes

Recall from Lecture 1:

- $\sum_p \frac{1}{p} = \infty$ (Euler's Theorem)
- $\pi(x) \ll \frac{x}{\log x}$ (Chebyshev's Theorem)

## 2.1 Merten's Theorems

**Theorem 2.1** (Merten's Theorem)**.** Assuming that:

- $x \geq 3$

Then

(i) $\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1)$

(ii) $\sum_{p \leq x} \frac{1}{p} = \log\log x + M + O\left(\frac{1}{\log x}\right)$ (for some $M \in \mathbb{R}$)

(iii) $\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{c + o(1)}{\log x}$ (for some $c > 0$)

**Remark.** Can show $c = e^{-\gamma}$.

*Proof.*

(i) Let $N = \lfloor x \rfloor$. Consider $N!$. We have

$$N^N \leq N^N$$
$$N! \geq N^N e^{-N}$$

(the second inequality cn be proved by induction, using $\left(1 + \frac{1}{N}\right)^N \leq e$).

Let $v_p(k)$ be the largest power of $p$ dividing $k$. Then

$$N! = \prod_{p \leq N} p^{v_p(N!)} \qquad \text{(fundamental theorem of arithmetic)}$$
$$\implies \log N! = \sum_{p \leq N} v_p(N!) \log p$$

We have $v_p(N!) = \sum_{j=1}^{\infty} \left\lfloor \frac{N}{p^j} \right\rfloor$. Indeed,

$$\begin{aligned} v_p(N!) &= \sum_{k=1}^{N} v_p(k) \\ &= \sum_{k=1}^{N} \sum_{j=1}^{\infty} \mathbb{1}_{v_p(k) \geq j} \\ &= \sum_{j=1}^{\infty} \sum_{k=1}^{N} \mathbb{1}_{v_p(k) \geq j} \\ &= \sum_{j=1}^{\infty} \left\lfloor \frac{N}{p^j} \right\rfloor \end{aligned}$$

Now,

$$\begin{aligned} \log N! &= \sum_{p \leq N} \left\lfloor \frac{N}{p} \right\rfloor \log p + \sum_{p \leq N} (\log p) \sum_{j=2}^{\infty} \left\lfloor \frac{N}{p^j} \right\rfloor \\ &= \sum_{p \leq N} \left( \frac{N}{p} + O(1) \right) \log p + O\left( \sum_{p \leq N} \frac{\log p}{p^2} \cdot N \right) && \text{(geometric series)} \\ &= N \sum_{p \leq N} \frac{\log p}{p} + \underbrace{O\left( \sum_{p \leq N} \log p \right)}_{\leq (\log N)\pi(N) \ll N (Chebyshev)} + O(N) && \left(\text{since } \sum_{p} \frac{\log p}{p^2} < \infty\right) \\ &= N \sum_{p \leq N} \frac{\log p}{p} + O(N) \end{aligned}$$

Combine with $\log N! = N \log N + O(N)$ to get

$$N \log N + O(N) = N \sum_{p \leq N} \frac{\log p}{p} + O(N).$$

Divide by $N$ to get the result.

(ii) By Partial Summation, this is

$$1 + O\left( \frac{1}{\log x} \right) + \int_2^x \frac{\sum_{p \leq t} \frac{\log p}{p}}{t (\log t)^2} \mathrm{d}t.$$

Writing $\varepsilon(t) = \sum_{p \leq t} \frac{\log p}{p} - \log t$, we get

$$\begin{aligned} &1 + O\left( \frac{1}{\log x} \right) + \int_2^x \frac{\mathrm{d}t}{t \log t} + \int_2^x \frac{\varepsilon(t)}{t (\log t)^2} \mathrm{d}t \\ &= 1 + O\left( \frac{1}{\log x} \right) + \log \log x - \log \log 2 + \int_2^{\infty} \frac{\varepsilon(t)}{t (\log t)^2} \mathrm{d}t + O\left( \int_x^{\infty} \frac{|\varepsilon(t)|}{t (\log t)^2} \mathrm{d}t \right) \end{aligned}$$

By part (i),

$$\int_x^\infty \frac{|\varepsilon(t)|}{t(\log t)^2}\mathrm{d}t \ll \int_x^\infty \frac{1}{t(\log t)^2}\mathrm{d}t \ll \frac{1}{\log x}$$

Take $M = 1 - \log\log 2 + \int_2^\infty \frac{\varepsilon(t)}{t(\log t)^2}\mathrm{d}t$.

(iii) Use Taylor expansion

$$\log(1-y) = -\sum_{j=1}^\infty \frac{y^j}{j}$$

to get

$$\log\prod_{p\le x}\left(1-\frac{1}{p}\right) = \sum_{p\le x}\log\left(1-\frac{1}{p}\right) = -\sum_{p\le x}\frac{1}{p} - \sum_{p\le x}\sum_{j=2}^\infty \frac{p-j}{j}$$

Write $H = \sum_p \sum_{j=2}^\infty \frac{p-j}{j}$. We get

$$= -\sum_{p\le x}\frac{1}{p} - H + O\left(\sum_{p>x}\underbrace{\sum_{j=2}^\infty \frac{p-j}{j}}_{\ll p^{-2}}\right) = -\sum_{p\le x}\frac{1}{p} - H + O\left(\frac{1}{x}\right) \overset{\text{(ii)}}{=} -\log\log x - H + O\left(\frac{1}{x}\right)$$

Taking exponentials,

$$\prod_{p\le x}\left(1-\frac{1}{p}\right) = \frac{c+o(1)}{\log x}.$$

□

Lecture 7

## 2.2 Sieve Methods

- General tools for estimating the number of primes (or products of a few primes in a set).
- Need information on the distribution of the set in residue classes.

**Definition** (Sieve problem)**.** Let $\mathcal{P} \subseteq \mathbb{P}$. Let

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p \le z}} p,$$

and let $A \subseteq \mathbb{Z}$. Denote

$$S(A, \mathcal{P}, z) = |\{n \in A : (n, P(z)) = 1\}|.$$

Problem: Estimate $S(A, \mathcal{P}, z)$.

Note that if $A \subseteq \left[\frac{x}{2}, x\right] \cap \mathbb{Z}$,

$$S(A, \mathbb{P}, x^{\frac{1}{2}}) = |A \cap \mathbb{P}|$$
$$S(A, \mathbb{P}, x^{\frac{1}{3}}) = |A \cap (\mathbb{P} \cup \{p_1 p_2 : p_1 p_2 > x^{\frac{1}{3}}\})|$$

**Sieve hypothesis:** There exists a multiplicative $g : \mathbb{N} \to [0, 1]$ and $R_d \in \mathbb{R}$ such that

$$|\{n \in A : n \equiv 0 \pmod d\}| = g(d)|A| + R_d$$

for all square-free $d$ (no repeated prime factors).

**Example.**

- $A = [1, x]$, $\mathcal{P} = \mathbb{P}$.

  $$|A_d| = \left\lfloor \frac{x}{d} \right\rfloor = \frac{x}{d} + O(1)$$

  Then $g(d) = \frac{1}{d}$, $|R_d| \ll 1$.

  $$S(A, \mathbb{P}, x^{\frac{1}{2}}) = |\{p \in \mathbb{P} : p \in [x^{\frac{1}{2}}, x]\}| = \pi(x) + O(x^{\frac{1}{2}}).$$

- $A = \{n(n+2) : n \le x\}$, $\mathcal{P} = \mathbb{P}$. Let $d = p_1 \cdots p_r$, where $p_i$ are distinct primes. Then

  $$\begin{aligned} |A_d| &= |\{n \le x : n \equiv 0 \text{ or } -2 \pmod{p_i} \forall i \le r\}| \\ &= \begin{cases} \frac{2^r}{d} x & \text{if } d \text{ odd} \\ \frac{2^{r-1}}{d} x + O(2^r) & \text{if } d \text{ even} \end{cases} \end{aligned}$$

  (by Chinese Remainder Theorem).

  $$\begin{aligned} S(A, \mathbb{P}, (2x)^{\frac{n}{2}}) &= |\{p \in ((2x)^{\frac{1}{2}}, x] : p + 2 \in \mathbb{P}\}| \\ &= |\{p \le x : p + 2 \in \mathbb{P}\}| + O(x^{\frac{1}{2}}) \end{aligned}$$

  Here,

  $$g(p) = \begin{cases} \frac{1}{p} & p = 2 \\ \frac{2}{p} & p > 2 \end{cases}$$

  and $R_d = O(2^{w(d)})$, where $w(d)$ is the number of prime factors of $d$ (distinct).

**Lemma.** We have
$$S(A, \mathcal{P}, z) = \sum_{d|P(z)} \mu(d)|A_d|.$$

*Proof.* Recall that
$$\mathbb{1}_{n=1} = (\mu * 1)(n)$$
(since $\mu$ is the inverse of 1). Hence,
$$\begin{aligned} S(A, \mathcal{P}, z) &= \sum_{n \in A} \mathbb{1}_{(n, P(z))=1} \\ &= \sum_{n \in A} \sum_{\substack{d|P(z) \\ d|n}} \mu(d) \\ &= \sum_{d|P(z)} \mu(a)|A_d| \end{aligned}$$
□

**Example.** Let
$$\pi(x, z) = |\{n \le x : (n, P(z)) = 1\}|.$$
Let $\mathcal{P} = \mathbb{P}$. Let $A = [1, x] \cap \mathbb{Z}$. Then
$$|A_d| = \frac{x}{d} + O(1).$$
By the previous lemma,
$$\begin{aligned} \pi(x, z) &= S(A, \mathbb{P}, z) \\ &= \sum_{d|P(z)} \mu(d) \left(\frac{x}{d} + O(1)\right) \\ &= x \sum_{d|P(z)} \frac{\mu(d)}{d} + O\left(\sum_{d|P(z)} \underbrace{|\mu(d)|}_{\le 1}\right) \\ &= x \sum_{d|P(z)} \frac{\mu(d)}{d} + O(2^{\pi(z)}) && P(z) = p_1 \cdots p_{\pi(2)} \\ &= x \prod_{p \le z} \left(1 + \underbrace{\frac{\mu(p)}{p}}_{-1}\right) + O(2^{\pi(2)}) && \text{fundamental theorem of arithmetic} \\ &= \frac{c + o(1)}{\log z} x + O(2^z) && \text{Merten's theorem, for some } c > 0 \end{aligned}$$

For $2 \le z \le \log x$,

$$\pi(x,z) = \frac{c+o(1)}{\log z} x.$$

**Theorem** (Sieve of Erastothenes – Legendre)**.** Assuming that:

- $A \subseteq [1,x] \cap \mathbb{N}$
- $2 \le z \le x$
- Assume the Sieve Hypothesis

Then

$$S(A, \mathcal{P}, z) = |A| \prod_{\substack{p \le 2 \\ p \in \mathcal{P}}} (1 - g(p)) + O\left( x^{\frac{1}{2}} (\log x)^{\frac{1}{2}} 2^{-\frac{\log x}{4 \log z}} \left( \sum_{\substack{d \le x \\ d \mid P(z)}} |R_d|^2 \right)^{\frac{1}{2}} + |A| e^{\frac{\log x}{\log z}} \prod_{\substack{p \le z \\ p \in \mathcal{P}}} (1 + g(p))^e \right)$$

Lecture 8

*Proof.* Recall from previous lecture that

$$\begin{aligned}
S(A, \mathcal{P}, z) &= \sum_{\substack{d \mid P(z) \\ d \le x}} \mu(d) |A_d| && \text{(since } A_d = \emptyset \text{ for } d > x) \\
&= \sum_{\substack{d \mid P(z) \\ d \le x}} \mu(d) g(d) |A| + O\left( \sum_{\substack{d \le x \\ d \mid P(z)}} |R_d| \right) && \text{(sieve hypothesis)} \\
&= |A| \sum_{d \mid P(z)} \mu(d) g(d) + O\left( \sum_{\substack{d \le x \\ d \mid P(z)}} |R_d| + |A| \sum_{\substack{d \mid P(z) \\ d > x}} g(d) \right) \\
&= |A| \prod_{\substack{p \le z \\ p \in \mathcal{P}}} (1 - g(p)) + O\left( \sum_{\substack{d \le x \\ d \mid P(z)}} |R_d| + |A| \sum_{\substack{d \mid P(z) \\ d > x}} g(d) \right)
\end{aligned}$$

We estimate the first error term using Cauchy-Schwarz:

$$\sum_{\substack{d \le x \\ d \mid P(z)}} |R_d| \le \left( \sum_{\substack{d \le x \\ d \mid P(z)}} |R_d|^2 \right)^{\frac{1}{2}} \left( \sum_{\substack{d \le x \\ d \mid P(z)}} 1 \right)^{\frac{1}{2}}.$$

Note that if $d \mid P(z)$, $d > x^{\frac{1}{2}}$, then

$$\omega(d) \geq \frac{\log x^{\frac{1}{2}}}{\log z},$$

($\omega(d)$ – number of distinct prime factors of $d$), since $z^{\omega(d)} \geq d \geq x^{\frac{1}{2}}$.

Hence, $2^{\omega(d)} \geq 2^{\frac{\log x}{2\log z}}$, $d \mid P(z)$, $d > x^{\frac{1}{2}}$.

Now we get

$$\begin{aligned}\sum_{\substack{d\leq x\\ d\mid P(z)}} 1 &\leq 2^{-\frac{\log x}{2\log z}} \sum_{\substack{d\leq x\\ d\mid P(z)}} \underbrace{2^{\omega(d)}}_{=\tau(d)} \\ &\leq 2^{-\frac{\log x}{2\log z}} \sum_{d\leq x} \tau(d) \\ &\ll 2^{-\frac{\log x}{2\log z}} x\log x\end{aligned}$$

(the last step is by Dirichlet's divisor problem: $\sum_{d\leq x}\tau(d) = (1+o(1))\cdot x\log x$).

Substituting this in, the first error term becomes as desired.

Now we estimate the second error term. We have

$$\begin{aligned}\sum_{\substack{d\mid P(z)\\ d>x}} g(d) &\leq x^{-\frac{1}{\log z}} \sum_{d\mid P(z)} g(d) d^{\frac{1}{\log z}} && \text{(since } d > x \text{ in the sum: Rankin's trick)} \\ &= x^{-\frac{1}{\log z}} \prod_{\substack{p\leq z\\ p\in\mathcal{P}}} (1 + g(p) \underbrace{p^{\frac{1}{\log z}}}_{\leq z^{\frac{1}{\log z}} = e}) \\ &\leq x^{-\frac{1}{\log z}} \prod_{\substack{p\leq z\\ p\in\mathcal{P}}} (1 + eg(p)) \\ &\leq \underbrace{x^{-\frac{1}{\log z}}}_{=e^{-\frac{\log x}{\log z}}} \prod_{\substack{p\leq z\\ p\in\mathcal{P}}} (1+g(p))^e && (1+ey \leq (1+y)^e)\end{aligned}$$

Combining the error terms, the claim follows. □

**Example.** Take $A = [1, x] \cap \mathbb{Z}$, $\mathcal{P} = \mathbb{P}$. Then $g(d) = \frac{1}{d}$, $R_d = O(1)$, so the sieve gives us

$$\begin{aligned}S(A, P, z) &= \pi(x, z) \\ &= (x + O(1)) \prod_{p\leq z} \left(1 - \frac{1}{p}\right) \\ &\quad + O\left(x^{\frac{1}{2}} (\log x)^{\frac{1}{2}} 2^{-\frac{\log x}{4\log z}} x^{\frac{1}{2}} + (x + O(1)) e^{-\frac{\log x}{\log z}} \prod_{p\leq z} \left(1 + \frac{1}{p}\right)^e\right)\end{aligned}$$

By Merten's Theorem,

$$\prod_{p \le z}\left(1 - \frac{1}{p}\right) = \frac{C + o(1)}{\log z}$$

$$\prod_{p \le z}\left(1 + \frac{1}{p}\right) \le \prod_{p \le z}\left(1 - \frac{1}{p}\right)^{-1}$$

$$= \left(\frac{1}{C} + o(1)\right) \log z$$

Hence,

$$\pi(x, z) = \frac{c + o(1)}{\log z} + O\left(x(\log x)^{\frac{1}{2}} 2^{-\frac{\log x}{4 \log z}} + xe^{-\frac{\log x}{\log z}} (\log z)^e\right).$$

Hence, for $2 \le z \le \exp\left(\frac{\log x}{10 \log\log x}\right)$,

$$\pi(x, z) = \frac{c + o(1)}{\log z} x.$$

This asymptotic in fact holds for $z \le x^{o(1)}$.
In particular, the Erastothenes-Legendre sieve gives

$$\pi(x) \le \pi(x, z) + z \ll \frac{x}{\log x} \log\log x$$

for $z = \exp\left(\frac{\log x}{10 \log\log x}\right)$. Not quite the Chebyshev bound $\pi(x) \ll \frac{x}{\log x}$.

Lecture 9

## 2.3 Selberg Sieve

| | asymptotes | good upper bound for primes |
|---|---|---|
| Erastothenes-Legendre | ✓ | ✗ |
| Selberg | ✗ | ✓ |

**Theorem 2.2** (Selberg sieve)**.** Assuming that:

- $z \ge 2$
- $A \subseteq \mathbb{Z}$ finite
- $\mathcal{P} \subseteq \mathbb{P}$
- Assume the sieve hypothesis

- $h : \mathbb{N} \to [0, \infty)$ be the multiplicative function supported on square-free numbers, given on the primes by

$$h(p) = \begin{cases} \frac{g(p)}{1-g(p)} & p \in \mathcal{P} \\ 0 & p \notin \mathcal{P} \end{cases}$$

Then

$$S(A, \mathcal{P}, z) \leq \frac{|A|}{\sum_{d \leq z} h(d)} + \sum_{\substack{d \leq z^2 \\ d | P(z)}} \tau_3(d) |R_d|.$$

**Sieve hypothesis**: There is a multiplicative $g : \mathbb{N} \to [0, 1]$ and $R_d \in \mathbb{R}$ such that

$$|A_d| = g(d)|A| + R_d$$

for all square-free $d \geq 1$.

*Proof.* Let $(\rho_d)_{d \in \mathbb{N}}$ be real numbers with

$$\rho_1 = 1, \rho_d = 0, d > z \tag{$*$}$$

Then,

$$\mathbb{1}_{(n, P(z))=1} \leq \left( \sum_{\substack{d | n \\ d | P(z)}} \rho_d \right)^2 .$$

(If $(n, P(z)) = 1$, get $1 \leq \rho$ otherwise use $0 \leq x^2$).

Summing over $n \in A$,

$$\begin{aligned} S(A, \mathcal{P}, z) &= \sum_{n \in A} \mathbb{1}_{(n, P(z))=1} \\ &\leq \sum_{n \in A} \left( \sum_{\substack{d | n \\ d | P(z)}} \rho_d \right)^2 \\ &= \sum_{d_1 d_2 | P(z)} \rho_{d_1} \rho_{d_2} \sum_{\substack{n \in A \\ [d_1, d_2] | n}} 1 \\ &= |A| \sum_{d_1, d_2 | P(z)} \rho_{d_1} \rho_{d_2} g([d_1, d_2]) + \underbrace{\sum_{d_1, d_2 | P(z)} \rho_{d_1} \rho_{d_2} R_{[d_1, d_2]}}_{E} \qquad \text{(sieve hypothesis)} \end{aligned}$$

($[m, n]$ means $\text{lcm}(m, n)$).

We first estimate $E$:

$$\begin{aligned} E &\leq \max_k |\rho_k|^2 \sum_{d_1,d_2|P(z)} |R_{[d_1,d_2]}| \\ &= \max_k |\rho_k|^2 \sum_{\substack{d\leq z^k \\ d|P(z)}} \sum_{\substack{d_1,d_2\in\mathbb{N} \\ [d_1,d_2]=d}} |R_d| \qquad (d=[d_1,d_2]) \end{aligned}$$

We have

$$\begin{aligned} \sum_{\substack{d_1,d_2\in\mathbb{N} \\ d=[d_1,d_2]}} 1 &= \sum_{l\leq z} \sum_{\substack{d_1',d_2'\in\mathbb{N} \\ d=ld_1'd_2' \\ (d_1',d_2')=1}} 1 \qquad (l=(d_1,d_2), d_1'=d_1/l, [d_1,d_2]=ld_1'd_2') \\ &\leq \tau_3(d) \end{aligned}$$

Therefore

$$E \leq \sum_{\substack{d\leq z^z \\ d|P(z)}} \tau_3(d)|R_d| \cdot \max_k |\rho_k|^2.$$

Now it suffices to prove that there is a choice of $(\rho_d)_{d\in\mathbb{N}}$ satisfying $(*)$ such that

Claim 1: $\sum_{d_1,d_2|P(z)} \rho_{d_1}\rho_{d_2} g([d_1,d_2]) = \frac{1}{\sum_{d\leq z}} h(d)$.

Claim 2: $|\rho_k| \leq 1$ for all $k\in\mathbb{N}$.

Proof of claim 1:

We have, writing $k=(d_1,d_2)$, $d_i'=\frac{d_i}{k}$,

$$\begin{aligned} \sum_{d_1,d_2|P(z)} \rho_{d_1}\rho_{d_2} g([d_1,d_2]) &= \sum_{k|P(z)} \mu(k)^2 \sum_{\substack{d_1',d_2'|\frac{P(z)}{k} \\ (d_1',d_2')=1}} \rho_{kd_1'}\rho_{kd_2'} g(kd_1'd_2') \\ &= \sum_{k|P(z)} \mu(k)^2 g(k) \sum_{\substack{d_1',d_2'|\frac{P(z)}{k} \\ (d_1',d_2')=1}} \rho_{kd_1'}\rho_{kd_2'} g(d_1')g(d_2') \qquad \text{(multiplicativity)} \end{aligned}$$

We have

$$\mathbb{1}_{(d_1',d_2')=1} = \sum_{\substack{c|d_1' \\ c|d_2'}} \mu(c)$$

(since $\mu * 1 = I$) so the previous expression becomes

$$\sum_{k|P(z)} \mu(k)^2 g(k) \sum_{c|\frac{P(z)}{k}} \mu(c) \sum_{\substack{d_1',d_2'|P(z) \\ d_1'\equiv 0 \pmod{()c} \\ d_2'\equiv 0 \pmod{c}}} \rho_{kd_1'}\rho_{kd_2'} g(d_1')g(d_2')$$

$$= \sum_{k|P(z)} \mu(k)^2 g(k) \sum_{c|\frac{P(z)}{k}} \mu(k) \left( \sum_{\substack{d|\frac{P(z)}{k} \\ d\equiv 0 \pmod{c}}} \right)^2$$

$$= \sum_{k|P(z)} \mu(k)^2 g(k)^{-1} \sum_{c|\frac{P(z)}{k}} \mu(c) \left( \sum_{d'|\frac{P(z)}{ck}} \rho_{ckd'} g(ckd') \right)^2$$

$$= \sum_{n\le z} h(m)^{-1} \left( \sum_{\substack{d|P(z) \\ d\equiv 0 \pmod{n}}} \rho_d g(d) \right)^2$$

(multiplicativity, $d = cd'$, $m = ck$, $d = md'$) since $\frac{1}{h} = \frac{\mu^2}{g} * \mu$ (check on primes $\frac{1}{h(p)} = \frac{1}{g(p)} - 1$).

Now we get

$$\sum_{d_1,d_2|P(z)} \rho_{d_1}\rho_{d_2} g([d_1,d_2]) = \sum_{m\le z} h(m)^{-1}\zeta_m^2$$

where

$$\zeta_m = \sum_{\substack{d|P(z) \\ d\equiv 0 \pmod{m}}} \rho_d g(d).$$

Lecture 10 Want to minimise this subject to $(*)$.

We need to translate the condition $\rho_1 = 1$. Note that

$$\sum_{\substack{m\le z \\ m\equiv 0 \pmod{c}}} \mu(m)\zeta_m = \sum_{d|P(z)} \rho_d g(d) \underbrace{\sum_{\substack{m|d \\ c|m}} \mu(m)}_{\sum_{m'|\frac{d}{c}} \mu(c)\mu(m') = \mu(d)\mathbb{1}_{d=e}}$$

$$= \mu(e)\rho_e g(e)$$

Hence,

$$\rho_e = \frac{\mu(e)}{g(e)} \sum_{\substack{m\le 2 \\ m\equiv 0 \pmod{c}}} \mu(m)\zeta_m.$$

Now,

$$\rho_1 = 1 = \sum_{m\le z} \mu(m)\zeta_m.$$

By Cauchy-Schwarz, we then get

$$\left(\sum_{m\leq z} h(m)^{-1}\zeta_m^2\right)\left(\sum_{m\leq z}\mu(m)^2 h(m)\right) \geq \left(\sum_{m\leq z}\mu(m)\zeta_m\right)^2 = 1.$$

Hence

$$\sum_{m\leq z} h(m)^{-1}\zeta_m^2 \geq \frac{1}{\sum_{m\leq z}\mu(m)^2 h(m)} = \frac{1}{\sum_{m\leq z} h(m)}.$$

Equality holds for $T_m = \frac{h(m)}{G(z)}$, where $G(z) = \sum_{m\leq z} h(m)$. We now check that with these $\zeta_m$, $\rho_d = 0$ for $d > z$.

Note that

$$\rho_c = \frac{\mu(c)}{g(c)G(z)} \sum_{\substack{m\leq z \\ m\equiv \pmod c}} \mu(m)h(m).$$

Hence, $\rho_c = 0$ for $c > 2$.

This proves Claim 1.

Now we prove Claim 2 ($|\rho_c| \leq 1$).

Note that any $m$ has at most one representation as $m = em'$, where $e \mid d$, $(m', d) = 1$ (for any $d \in \mathbb{N}$).

Now,

$$\begin{aligned} G(z) &\geq \sum_{c|d} \sum_{\substack{m'\leq \frac{z}{c} \\ (m',d)=1}} h(cm') \\ &= \sum_{c|d} h(c) \sum_{\substack{m'\leq \frac{z}{c} \\ (m',d)=1}} h(m') \\ &\geq \sum_{c|d} h(e) \sum_{\substack{m'\leq \frac{z}{d} \\ (m',d)=1}} h(m') \end{aligned}$$

Now,

$$\rho_d = \frac{\mu(d)^2 h(d)}{g(d)G(z)} \sum_{\substack{m'\leq \frac{z}{d} \\ (m',d)=1}} \mu(m')h(m').$$

Substituting the lower bound for $G(z)$,

$$|\rho_d| \leq \frac{h(d)}{g(d)\sum_{c|d} h(e)} = 1,$$

since $1 * h = \frac{h}{g}$. □

**Lemma 2.3.** Assuming that:

- $z \geq 3$
- $g : \mathbb{N} \to [0, 1]$ multiplicative
- for some $K, A \in \mathbb{R}$ we have
$$\sum_{p \leq z} g(p) \log p \leq \kappa \log z + A.$$

Then
$$\frac{1}{\sum_{m \leq z} h(m)} \leq 2 \prod_{p \leq z^{1/(e\kappa+1)}} (1 - g(p)),$$
where $h$ is defined in terms of $g$ as in Selberg's sieve.

*Proof.* Note that for any $c \in (0, 1)$,
$$\sum_{m \leq z} h(m) \geq \sum_{\substack{m \leq z \\ m | P(z^c)}} h(m) = G(z, c).$$

Then
$$\begin{aligned}\prod_{\substack{p \leq z^c \\ p \in \mathcal{P}}} (1 - g(p))^{-1} - G(z, c) &= \prod_{\substack{p \leq z^c \\ p \in \mathcal{P}}} (1 + h(p)) - \sum_{\substack{m \leq z \\ m | P(z^c)}} h(m) \\ &= \sum_{\substack{m > z \\ m | P(z^c)}} h(m)\end{aligned}$$

By Rankin's trick,

$$\begin{aligned}
1 - \prod_{p \le z^c} (1 - g(p)) G(z, c) &= \prod_{p \le z^c} (1 - g(p)) \sum_{\substack{m > z \\ m \mid P(z^c)}} h(m) \\
&\le \prod_{p \le z^c} (1 - g(p)) z^{-\frac{\lambda}{\log z}} \sum_{m \mid P(z^c)} h(m) m^{\frac{\lambda}{\log z}} && \text{(for any } \lambda > 0\text{)} \\
&= \prod_{p \le z^c} (1 - g(p)) e^{-\lambda} \prod_{p \le z^c} (1 + h(p) p^{\frac{\lambda}{\log z}}) \\
&= e^{-\lambda} \prod_{p \le z^c} (1 - g(p) + g(p) p^{\frac{\lambda}{\log z}} \\
&\le e^{-\lambda} \exp \left( \sum_{p \le z^c} \underbrace{(p^{\frac{\lambda}{\log z}} - 1)}_{\le \frac{\lambda}{\log z} (\log p) p^{\frac{\lambda}{\log z}}} \right) \\
&\le \exp \left( -\lambda + \frac{\lambda}{\log z} \sum_{p \le z^c} g(p) (\log p) p^{\frac{\lambda}{\log z}} \right) && (1 + t \le e^t) \\
&\le \exp \left( -\lambda + c e^{c\lambda} \lambda \kappa + \lambda e^{c\lambda} \frac{A}{\log z} \right)
\end{aligned}$$

Choose $c = \frac{1}{\lambda}$ and $\lambda = e\kappa + 1$ to get the claim. □

Lecture 11

**The Brun-Titchmarsh Theorem**

**Theorem 2.4** (Brun-Titchmarsh Theorem)**.** Assuming that:

- $x \ge 0$, $y \ge 2$
- $\varepsilon > 0$ and $y$ is large in terms of $\varepsilon$

Then

$$\pi(x + y) - \pi(x) \le \frac{(2 + \varepsilon) y}{\log y}.$$

**Remark.** We expect

$$\pi(x + y) - \pi(x) = \frac{(n + o(1)) y}{\log x}$$

in a wide range of $y$ (e.g. $y \ge x^\varepsilon$ for some $\varepsilon > 0$ fixed). The prime number theorem gives this for $y \gg x$. The Brun-Titchmarsh Theorem gives an upper bound of the expected order for $y \ge x^\varepsilon$.

*Proof.* Apply the Selberg sieve with $A = [x, x+y] \cap \mathbb{N}$, $\mathcal{P} = \mathbb{P}$. Note that for any $d \geq 1$,

$$|\{a \in A : a \equiv 0 \pmod d\}| = \frac{y}{d} + O(1).$$

Hence, the sieve hypothesis holds with $g(d) = \frac{1}{d}$, $R_d = O(1)$.

Now, the function $h$ in Selberg sieve is given on primes by

$$h(p) = \frac{g(p)}{1 - g(p)} = \frac{1}{p-1} = \frac{1}{\varphi(p)},$$

where $\varphi$ is the Euler totient function. In general,

$$h(d) = \mu(d)^2 \cdot \frac{1}{\varphi(d)}$$

(since $\varphi$ is multiplicative). Now, for any $z \geq 2$, Selberg sieve yields

$$S(A, \mathbb{P}, z) \leq \frac{y}{\sum_{d \leq z} \frac{\mu(d)^2}{\varphi(d)}} + O\left(\sum_{d \leq z^2} \tau_3(d)\right).$$

By Problem 11 on Example Sheet 1, the error term is $O(z^2 (\log z)^2)$.

Take $z = y^{\frac{1}{2} - \frac{\varepsilon}{10}}$. Then

$$z^2 (\log z)^2 \ll (y^{\frac{1}{2} - \frac{\varepsilon}{10}})^2 (\log y)^2 \ll y^{1 - \frac{\varepsilon}{20}}$$

(for $y \geq y_0(\varepsilon)$). We estimate

$$\begin{aligned}
\sum_{d \leq z} \frac{\mu(d)^2}{\varphi(d)} &= \sum_{d \leq z} \frac{\mu(d)^2}{d} \frac{d}{\varphi(d)} \\
&= \sum_{d \leq z} \frac{\mu(d)^2}{d} \cdot \prod_{p \mid d} \underbrace{\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right)}_{= \frac{p}{p-1} = \frac{p}{\varphi(p)}} \\
&\geq \sum_{n \leq z} \frac{1}{n}
\end{aligned}$$

since any $n \leq z$ has at least one representation as

$$n = d p_1^{a_1} \cdots p_k^{a_k},$$

where $d \leq z$ is square-free and $p_i \mid d$ are primes and $a_1 \geq 0$.

We have proved

$$\sum_{n \leq z} \frac{1}{n} = \log z + O(1) \geq \left(1 - \frac{1}{10}\right) \log z$$

for $z \geq z_0(\varepsilon)$.

Putting everything together gives us

$$\begin{aligned}\pi(x+y)-\pi(x) &\le S(A,\mathbb{P},z)+z \\ &\le \frac{y}{\left(1-\frac{\varepsilon}{10}\right)\log z}+z+y^{1-\frac{\varepsilon}{20}} \\ &\le \frac{(2+\varepsilon)y}{\log y}\end{aligned}$$

for $y \ge y_0(\varepsilon)$. □

# 3 The Riemann Zeta Function

Recall that the Riemann zeta function is defined by

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

for $\mathrm{Re}(s) > 1$.

Remarkable properties:

(1) $\zeta(s)$ extends meromorphically to $\mathbb{C}$.

(2) A functional equation relating $\zeta(s) \leftrightarrow \zeta(1-s)$.

(3) All the (non-trivial) zeroes appear to be on the line $\mathrm{Re}(s) = \frac{1}{2}$ (Riemann hypothesis).

(4) $\zeta(s)$ closely relates to the distribution of primes.

**Notation.** $f(x) \asymp g(x)$ means $f(x) \ll g(x) \ll f(x)$. $\asymp_\sigma$ means that the constant in $\ll$ can depend on $\sigma$.

**Lemma 3.1.** Assuming that:

- $\sigma > 1$
- $t \in \mathbb{R}$

Then $|\zeta(\sigma + it)| \asymp_\sigma 1$.

*Proof.* By the Euler product formula,

$$\zeta(\sigma + it) = \prod_p (1 - p^{-\sigma - it})^{-1},$$

hence

$$|\zeta(\sigma + it)| = \prod_p |1 - p^{-\sigma - it}|^{-1}.$$

By the triangle inequality,

$$1 - p^{-\sigma} \le |1 - p^{-\sigma - it}| \le 1 + |p^{-\sigma - it}| = 1 + p^{-\sigma}.$$

Hence,

$$\prod_p (1 - p^{-\sigma})^{-1} \ge |\zeta(\sigma + it)| \ge \prod_p (1 = p^{-\sigma})^{-1}.$$

Note that these products converge if and only if $\sum_p p^{-\sigma}$ converges, and this sum converges by the comparison test. □

**Lemma 3.2** (Polynomial growth of *eta* in half-planes)**.**

(i) $f(\zeta)$ extends to a meromorphic function on $\mathbb{C}$, with the only pole being a simple pole which is at $s = 1$.

(ii) Let $k \geq 0$ be an integer. Then, for $\mathrm{Re}(s) \geq -k$ and $|s-1| \geq \frac{1}{10}$ we have $|\zeta(s)| \ll_k |s|^{k+2}+1$.

Lecture 12

*Proof.* Let $k \geq 0$ be an integer.

We claim that there exist polynomials $P_k$, $Q_k$ of degree $\leq k+1$ and such that for $\mathrm{Re}(s) > 1$,

$$\zeta(s) = \frac{1}{s-1} + Q_k(s) + s(s+1)\cdots(s+k)\int_1^\infty \frac{P_k(\{t\})}{t^{s+k+1}}\mathrm{d}t. \qquad (*)$$

First assume $(*)$ holds.

Then, since $P_k(\{t\}) \ll_k 1$, for $\mathrm{Re}(s) > -k - \frac{1}{2}$, $|s-1| \geq \frac{1}{10}$, $(*)$ gives $|\zeta(s)| \ll_k |s|^{k+2} + 1$. So (ii) follows.

For (i), using analytic continuation and $(*)$, it suffices to show that the RHS of $(*)$ is meromorphic for $\mathrm{Re}(s) > -k$, with the only pole a simple one at $s = 1$.

Suffices to show that

$$\int_1^\infty \frac{P_k(\{t\})}{t^{s+k+1}}\mathrm{d}t$$

is analytic for $\mathrm{Re}(s) > -k$.

This follows from the following criterion: If $U \subseteq \mathbb{C}$ is open, $f : U \times \mathbb{R} \to \mathbb{C}$ is piecewise continuous, and if $s \mapsto f(s,t)$ is analytic in $U$ for any $t \in \mathbb{R}$, then $\int_{\mathbb{R}} f(s,t)\mathrm{d}t$ is analytic in $U$, provided that $\int_{\mathbb{R}} |f(s,t)|\mathrm{d}t$ is bounded on compact subsets of $U$.

Applying this with $f(s,t) = \frac{P_k(\{t\})}{t^{s+k+1}}\mathbb{1}_{[1,\infty)}$ concludes the proof of (i) assuming $(*)$.

We are left with proving $(*)$. We use induction on $k$.

Case $k = 0$: By Partial Summation,

$$\begin{aligned}
\zeta(s) &= \sum_{n=1}^\infty \frac{1}{n^s} \\
&= s\int_1^\infty \frac{\lfloor u \rfloor}{u^{s+1}}\mathrm{d}u && \text{(apply partial summation to } \sum_{n\leq x} n^{-s} \text{ and let } x \to \infty) \\
&= s\int_1^\infty \frac{1}{u^s}\mathrm{d}u - \int_1^\infty \frac{\{u\}}{u^{s+1}}\mathrm{d}u \\
&= \frac{1}{s-1} + 1 - s\int_1^\infty \frac{\{u\}}{u^{s+1}}\mathrm{d}u
\end{aligned}$$

Take $P_0(u) = u$, $Q_0(u) = 1$.

Case $k+1$ assuming $k$: Let

$$c_k = \int_0^1 P_k(\{t\})\mathrm{d}t.$$

For $\mathrm{Re}(s) > 1$, we have

$$\zeta(s) = \frac{1}{s-1} + Q_k(s) + c_k s(s+1)\cdots(s+k-1) + s(s+1)\cdots(s+k)\int_1^\infty \frac{P_k(\{t\}) - c_k}{t^{s+k+1}}\mathrm{d}t.$$

Let

$$P_{k+1}(u) = -\int_0^u (P_k(t) - c_k)\mathrm{d}t.$$

This is a polynomial of degree $\le k+2$. By integration by parts,

$$\int_1^\infty \frac{P_t(\{t\}) - c_k}{t^{s+k+1}}\mathrm{d}t = (s+k+1)\int_1^\infty \frac{P_{k+1}(\{u\})}{u^{s+k+1}}\mathrm{d}u.$$

Substituting this into the previous equation, we get that case $k+1$ follows. □

### The Gamma function

**Definition** (Gamma function)**.** For $\mathrm{Re}(s) > 0$, let

$$\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}\mathrm{d}t.$$

**Lemma 3.3.** $\Gamma(s)$ is analytic for $\mathrm{Re}(s) > 0$.

*Proof.* Apply the same criterion for integral of analytic function being analytic as in the previous lemma, taking $f(s,t) = t^{s-1}e^{-t}\mathbb{1}_{[0,\infty)}(t)$.

Note that for $0 < \sigma_1 \le \mathrm{Re}(s) \le \sigma_2$,

$$\int_{\mathbb{R}} |f(s,t)|\mathrm{d}t \le \int_0^1 t^{\sigma_1 - 1}e^{-t}\mathrm{d}t + \int_1^\infty t^{\sigma_2-1}e^{-t}\mathrm{d}t < \infty.$$ □

Lecture 13

**Lemma** (Functional equation for $\Gamma$)**.** The $\Gamma$ function extends meromorphically to $\mathbb{C}$, with the only poles being simple poles at $s = 0, -1, -2, \dots$.
Moreover:

(i) $\Gamma(s+1) = s\Gamma(s)$ for $s \in \mathbb{C}$.

(ii) $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$ for all $s \in \mathbb{C}$ (Euler reflection formula).

*Proof.*

(i) For $\mathrm{Re}(s) > 0$, by integration by parts,

$$\int_0^\infty t^s e^{-t} \mathrm{d}t = s \int_0^\infty t^{s-1} e^{-t} \mathrm{d}t.$$

This proves (i) for $\mathrm{Re}(s) > 0$.

Now for any $k \in \mathbb{N}$, for $\mathrm{Re}(s) > 0$ we have

$$\Gamma(s) = \frac{\Gamma(s+k)}{(s+k-1)\cdots(s+1)s}.$$

The RHS is analytic for $\mathrm{Re}(s) > -k$, so can use analytic continuation to extend $\Gamma(s)$ meromorphically to $\mathrm{Re}(s) > -k$, with the only poles being simple poles at $s = 0, -1, \dots, -k, -1$.

Let $k \to \infty$.

(ii) Since both sides are analytic in $\mathbb{C} \setminus \mathbb{Z}$, by analytic continuation, it suffices to prove the formula for $0 < s < 1$.

Now, for any $t > 0$,

$$\begin{aligned} t^{s-1}\Gamma(s-1) &= t^{s-1} \int_0^\infty u^{-s} e^{-u} \mathrm{d}u \\ &= \int_0^\infty v^{-s} e^{-vt} \mathrm{d}t && (u = vt) \end{aligned}$$

Multiply by $e^{-t}$ and integrate, and use Fubini to get

$$\begin{aligned} \Gamma(s)\Gamma(s-1) &= \int_0^\infty \int_0^\infty v^{-s} e^{-vt} \mathrm{d}v e^{-t} \mathrm{d}t \\ &= \int_0^\infty \int_0^\infty e^{-(v+1)t} \mathrm{d}t v^{-s} \mathrm{d}v \\ &= \int_0^\infty \frac{v^{-s}}{1+v} \mathrm{d}v \\ &= \int_{-\infty}^\infty \frac{e^{(1-s)x}}{1+e^x} \mathrm{d}x && (v = e^x) \end{aligned}$$

Hence, the remaining task is to show

$$\int_{-\infty}^\infty \frac{e^{(1-s)x}}{1+e^x} \mathrm{d}x = \frac{\pi}{\sin(\pi s)}.$$

We will do this next time.

$\square$

Lecture 14

**Theorem 3.4** (Functional equation for *zeta*)**.** Assuming that:

- $\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{s}\right)\zeta(s)$ for $s \in \mathbb{C}$

Then $\xi$ is an entire function and $\xi(s) = \xi(1-s)$ for $s \in \mathbb{C}$. Hence

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

for $s \in \mathbb{C} \setminus \{0, 1\}$.

*Proof.* Let $\mathrm{Re}(s) > 1$. Then,

$$\Gamma\left(\frac{s}{2}\right) = \int_0^\infty t^{\frac{s}{2}-1}e^{-t}\mathrm{d}t.$$

Make the change of variables $f = \pi n^2 u$ to get

$$\Gamma\left(\frac{s}{2}\right) = \pi^{s/2}n^s \int_0^\infty u^{\frac{s}{2}-1}e^{-\pi n^2 u}\mathrm{d}u.$$

Hence

$$\pi^{-\frac{s}{2}}n^{-s}\Gamma\left(\frac{s}{2}\right) = \int_0^\infty u^{\frac{s}{2}-1}e^{-\pi n^2 u}\mathrm{d}u.$$

Summing over $n \in \mathbb{N}$ and using Fubini,

$$\begin{aligned}
\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \sum_{n=1}^\infty \int_0^\infty u^{\frac{s}{2}-1}e^{-\pi n^2 u}\mathrm{d}u \\
&= \frac{1}{2}\int_0^\infty u^{\frac{s}{2}-1}(\theta(u)-1)\mathrm{d}u \qquad \theta(u) = \sum_{n=-\infty}^\infty e^{-\pi n^2 u} \\
&= \frac{1}{2}\int_0^1 u^{\frac{s}{2}-1}(\theta(u)-1)\mathrm{d}u + \frac{1}{2}\int_1^\infty u^{\frac{s}{2}-1}(\theta(u)-1)\mathrm{d}u \qquad (*)
\end{aligned}$$

By the functional equation

$$\theta(u) = \frac{1}{\sqrt{u}}\theta\left(\frac{1}{u}\right),$$

we have

$$\begin{aligned}\int_0^1 u^{\frac{s}{2}-1}(\theta(u)-1)\mathrm{d}u &= \int_0^1 u^{\frac{s}{2}-\frac{3}{2}}\theta\left(\frac{1}{u}\right)\mathrm{d}u - \int_0^1 u^{\frac{s}{2}-1}\mathrm{d}u \\ &= \int_1^\infty v^{-\frac{s+1}{2}}\theta(v)\mathrm{d}v - \int_0^1 u^{\frac{s}{2}-1}\mathrm{d}u \qquad (u = \frac{1}{v}) \\ &= \int_1^\infty v^{-\frac{s+1}{2}}(\theta(v)-1)\mathrm{d}v + \underbrace{\int_1^\infty v^{-\frac{s+1}{2}}\mathrm{d}v}_{\frac{1}{\frac{s-1}{2}}} - \underbrace{\int_0^1 u^{\frac{s}{2}-1}\mathrm{d}u}_{\frac{1}{\frac{s}{2}}}\end{aligned}$$

Plugging this into $(*)$, we get

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \frac{1}{2}\int_1^\infty (u^{-\frac{s+1}{2}} + u^{\frac{s}{2}-1})(\theta(u)-1)\mathrm{d}u - \frac{1}{s(s-1)}.$$

Hence

$$\xi(s) = -\frac{1}{2} + \frac{1}{4}s(s-1)\int_1^\infty (u^{-\frac{s+1}{2}} + u^{\frac{s}{2}-1})(\theta(u)-1)\mathrm{d}u. \qquad (**)$$

Since $|\theta(u)-1| \ll e^{-\pi u}$, applying the criterion for integrals of analytic functions being analytic, we see that $\xi(s)$ is entire. So by analytic continuation, $(**)$ holds for all $s \in \mathbb{C}$.

Moreover, the expression for $\zeta(s)$ is symmetric with respect to $s \mapsto 1-s$, so $\xi(s) = \xi(1-s)$, $s \in \mathbb{C}$. □

**Corollary 3.5** (Zeroes and poles of *zeta*)**.** The $\zeta$ function extends to a meromorphic function in $\mathbb{C}$ and it has

(i) Only one pole, which is a simple pole at $s = 1$, residue 1.

(ii) Simple zeroes at $s = -2, -4, -6, \ldots$.

(iii) Any other zeroes satisfy $0 \leq \mathrm{Re}(s) \leq 1$.

*Proof.*

(ii) – (iii) Follows from the lemma on polynomial growth of $\zeta$ on vertical lines.

(ii) – (iii) We know $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$. We want to show that if $\zeta(s) = 0$ and $\mathrm{Re}(s) > 0$ then $s \in \{-2, -4, -6, \ldots\}$ and $s$ is a simple zero.

Let $\mathrm{Re}(s) > 0$. By the functional equation for $\zeta$,

$$\zeta(s) = \underbrace{\pi^{s-\frac{1}{2}}}_{\neq 0}\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}\zeta(1-s).$$

We claim that $\Gamma(s) \neq 0$ for all $s \in \mathbb{C}$. By the Euler reflection formula,

$$\Gamma(s)\Gamma(1-s)\sin(\pi s) = \pi,$$

for $s \in \mathbb{C}$.

If $\Gamma(s) = 0$, then $\Gamma$ has a pole at $1-s$. Hence, $1-s=-n$ for some $n \geq 0$ integer. But then $s = n+1$, and $\Gamma(n+1) = n! \neq 0$.

We conclude that for $\mathrm{Re}(s) < 0$,

$$\begin{aligned} \zeta(s) = 0 &\iff \frac{s}{2} \text{ is a pole of } \Gamma \\ &\iff s = -2n, n \in \mathbb{N} \end{aligned}$$

Since the poles of $\Gamma$ are simple, $\zeta$ has a simple zero at $s = -2n$, $n \in \mathbb{N}$. □

## 3.1 Partial fraction approximation of $\zeta$

This is a formula for $\frac{\zeta'(s)}{\zeta(s)}$.

For the proof we need a lemma. We write, for $z \in \mathbb{C}$, $r > 0$,

$$\begin{aligned} B(z_0, r) &= \{z \in \mathbb{C} : |z - z_0| < r\} \\ \overline{B(z_0, r)} &= \{z \in \mathbb{C} : |z - z_0| \leq r\} \\ \partial B(z_0, r) &= \{z \in \mathbb{C} : |z - z_0| = r\} \end{aligned}$$

**Lemma 3.6** (Borel-Caratheodory Theorem)**.** Assuming that:

- $0 < r < R$
- $f$ analytic in $\overline{B(0, R)}$, with $f(0) = 0$

Then

$$\sup_{|z| \leq r} |f(z)| \leq \frac{2r}{R-r} \sup_{|z|=R} \mathrm{Re}(f(z)).$$

*Proof.* This is Exercise 10 on Example Sheet 2. □

Lecture 15

**Lemma 3.7** (Landau)**.** Assuming that:

- $z_0 \in \mathbb{C}$ and $r > 0$
- $f$ analytic in $B(z_0, r)$
- for some $M > 1$ we have $|f(z)| < e^M |f(z_0)|$ for all $z \in B(z_0, r)$

Then for $z \in B(z_0, r/4)$,

$$\left|\frac{f'(z)}{f(z)} - \sum_{\rho \in Z} \frac{1}{z-\rho}\right| \leq \frac{96M}{r},$$

where $Z$ is the set of zeroes of $f$ in $\overline{B(z_0, r/2)}$, counted with multiplicities.

**Note.** If $f$ is a polynomial, we can factorise

$$f(z) = a \prod_{\rho} (z - \rho),$$

and then

$$\begin{aligned}\frac{f'(z)}{f(z)} &= (\log f(z))' \\ &= \left(\log a + \sum_{\rho} \log(z-\rho)\right)' \\ &= \sum_{\rho} \frac{1}{z-\rho}\end{aligned}$$

*Proof.* Let

$$g(z) = \frac{f(z)}{\prod_{\rho \in Z}(z-\rho)}.$$

Then $g$ is analytic and non-vanishing in $\overline{B(z_0, r/2)}$. Note that

$$\frac{g'(z)}{g(z)} = \frac{f'(z)}{f(z)} - \sum_{\rho \in Z} \frac{1}{z-\rho}$$

$(\frac{(f_1 - f_n)'}{f_1 - f_n} = \sum_{i=1}^n \frac{f_1'}{f_1})$.

Hence, it suffices to prove

$$\left|\frac{g'(z)}{g(z)}\right| \leq \frac{96M}{r}$$

for $z \in B(z_0, r/4)$. Write

$$h(z) = \frac{g(z_0 + z)}{g(z_0)}.$$

Then $h$ is analytic and non-vanishing in $\overline{B(0, r/2)}$, and $h(0) = 1$. We want to show

$$\left|\frac{h'(z)}{h(z)}\right| \leq \frac{96M}{r}$$

for $z \in B(0, r/4)$.

For all $z_0 \in \partial B(0, r)$ we have

$$|h(z)| = \left| \frac{f(z_0 + z)}{f(z_0)} \prod_{\rho \in Z} \frac{z_0 - \rho}{z_0 + z - \rho} \right| \leq \left| \frac{f(z_0 + z)}{f(z_0)} \right| < e^M$$

since

$$|z_0 - \rho| \leq \frac{r}{2} = r - \frac{r}{2} \leq |z_0 + z - \rho|$$

for $z \in \partial B(0, r)$.

By the maximum modulus principle, $|h(z)| < e^M$ for $z \in \overline{B(0, r/2)}$, so

$$\operatorname{Re} \log h(z) = \log |h(z)| < M.$$

By the Borel-Caratheodory Theorem with radii $\frac{3r}{8}$, $\frac{r}{4}$ we have for for $z \in B(0, 3r/8)$,

$$|\log h(z)| \leq \frac{2\frac{r}{4}}{\frac{3r}{8} - \frac{r}{4}} M = 4M.$$

Now, for $z \in B(0, r/4)$, Cauchy's theorem gives us

$$\begin{aligned} \left| \frac{h'(z)}{h(z)} \right| &= \left| \frac{1}{2\pi i} \int_{\partial B(0, 3r/8)} \frac{\log h(w)}{(z - w)^2} \mathrm{d}w \right| \\ &\leq \frac{1}{2\pi} \cdot 2\pi \frac{3r}{8} 4M \left( \frac{3r}{8} - \frac{r}{4} \right)^{-2} \\ &= \frac{96M}{r} \end{aligned}$$

□

**Theorem 3.8** (Partial Fraction approximation of $zeta'/zeta$)**.**

(i) Let $s = \sigma + it$ with $|\sigma| \leq 10$, $s \neq 1$ and $\zeta(s) \neq 0$. Then

$$\frac{\zeta'(s)}{\zeta(s)} = -\frac{1}{s - 1} + \sum_{|\rho - s| \leq \frac{1}{10}} \frac{1}{s - \rho} + O(\log(|t| + 2)).$$

where the sum is over the zeroes $\rho$ of $\zeta$ counted with multiplicity.

(ii) For any $T \geq 0$, there are $\ll \log(T + 2)$ many zeroes $\rho$ of $\zeta$ (counted with multiplicity) with $|\operatorname{Im}(\rho)| \in [T, T + 1]$.

*Proof.* We apply Landau with $z_0 = 2 + it$, $r = 50$, with $f(s) = (s - 1)\zeta(s)$.

By the lemma on polynomial growth of $\zeta$ on vertical lines, for $\sigma + it \in B(z_0, 50)$, we have

$$\begin{aligned}|f(s)| &\leq C(|t| + 52)(|t\ \ + 2)^{50} \\ &\leq C\exp(51\log(|t| + 52)) \\ &\ll C\exp(51\log(|t| + 52))|f(z)|\end{aligned}$$

$(|\zeta(z + it)| \asymp 1)$.

Let $s \in B\left(z_0, \frac{25}{2}\right)$. Then Landau gives us

$$\begin{aligned}\frac{f'(s)}{f(s)} &= \frac{1}{s-1} + \frac{\zeta'(s)}{\zeta(s)} \\ &= \sum_{|\rho - z_0| \leq 2S} \frac{1}{s - \rho} + O(\log(|t| + 2))\end{aligned} \tag{$*$}$$

Since $B\left(z_0, \frac{25}{2}\right)$ contains all the points $s = \sigma + it$ with $|\sigma| \leq 10$, it suffices to show

$$\sum_{\substack{|\rho - z_0| \leq 25 \\ |\rho - s| > \frac{1}{10}}} \frac{1}{s - \rho} = O(\log(|t| + 2)). \tag{$**$}$$

Substituting $s = z_0$ in $(*)$, we get

$$\begin{aligned}\sum_{|\rho - z_0| \leq 25} \frac{1}{z_0 - \rho} &= O\left(\left|\frac{\zeta'(z_0)}{\zeta(z_0)}\right| + 1 + \log(|t| + 2)\right) \\ &= O(\log(|t| + 2))\end{aligned}$$

since

$$\begin{aligned}\left|\frac{\zeta'(2 + it)}{\zeta(2 + it)}\right| &= \left|\sum_{n=1}^{\infty} \Lambda(n) n^{-2+it}\right| \\ &\leq \sum_{n=1}^{\infty} \Lambda(n) n^{-2} \\ &= -\frac{\zeta(2)}{\zeta(2)}\end{aligned}$$

Taking real parts,

$$\sum_{|\rho - z_0| \leq 25} \frac{2 - \mathrm{Re}(\rho)}{|z_0 - \rho|^2} = O(\log(|t| + 2)).$$

Since $\mathrm{Re}(\rho) \leq 1$,

$$\sum_{|\rho - z_0| \leq 25} \frac{1}{|z_0 - \rho|^2} = O(\log(|t| + 2)).$$

This proves part (ii). It gives also $(**)$ since the sum there contains $O(\log(|t| + 2))$ zeros. $\square$

Lecture 16

### 3.2 Zero-free region

**Proposition 3.9.** Assuming that:

- $\sigma > 1$ and $t \in \mathbb{R}$

Then

$$3\frac{\zeta'}{\zeta}(\sigma) + 4\operatorname{Re}\left(\frac{\zeta'}{\zeta}(\sigma + it)\right) + \operatorname{Re}\left(\frac{\zeta'}{\zeta}(\sigma + 2it)\right) \leq 0. \tag{$**$}$$

*Proof.* Recall that

$$\frac{\zeta'}{\zeta}(s) = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

where $\Lambda$ is the von Mangoldt function function, and $\operatorname{Re}(s) > 1$.

Taking linear combinations, the LHS of $(**)$ becomes

$$-\sum_{n=1}^{\infty} \Lambda(n) \frac{3 + 4\operatorname{Re}(n^{it}) + \operatorname{Re}(n^{-2it})}{n^\sigma} = -\sum_{n=1}^{\infty} \Lambda(n) \frac{3 + 4\cos(t\log n) + \cos(2 + \log n)}{n^\sigma}$$

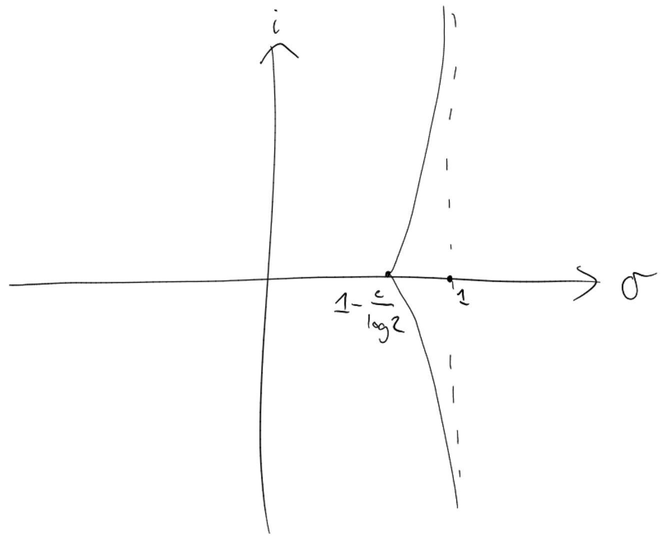
$(\operatorname{Re}(n^{iu}) = \cos(u \log n))$.

We are done by the inequality:

$$3 + 4\cos\alpha + \cos 2\alpha = 2(1 + \cos\alpha)^2 \geq 0$$

for $\alpha \in \mathbb{R}$. □

**Theorem 3.10** (Zero-free region)**.** There is a constant $c > 0$ such that $\zeta(\sigma + it) \neq 0$ whenever $\sigma > 1 - \frac{c}{\log(|t|+2)}$. In particular, $\zeta(s) \neq 0$ for $\operatorname{Re}(s) = 1$.




*Proof.* Let $\sigma \in [1,2]$ and $t \in \mathbb{R}$. Suppose $\zeta(\beta + it)$. uwe know that $\beta \leq 1$. We know that $\zeta$ has no zeroes in some ball $B(1,r)$ for some $r > 0$ (otherwise the entire function $(s-1)\zeta(s)$ would have an accumulation point for its zeros).

Choosing $c > 0$ small enough, we can assume that $|t| \geq r$. By the key inequality for $\frac{\zeta'}{\zeta}$,

$$3\frac{\zeta'}{\zeta}(\sigma) + 4\operatorname{Re}\left(\frac{\zeta'}{\zeta}(\sigma + it)\right). + \operatorname{Re}\left(\frac{\zeta'}{\zeta}(\sigma + 2it)\right). \leq 0.$$

Apply partial fraction decomposition of $\frac{\zeta'}{\zeta}$. So

$$\frac{\zeta'}{\zeta}(s) = -\frac{1}{s-1} + \sum_{|s-\rho| \leq \frac{1}{10}} \frac{1}{s-\rho} + O(\log(|t|+2)). \tag{$**$}$$

$(t = \operatorname{Im}(s))$.

Since $\operatorname{Re}(\rho) \leq 1$ for any zero $\rho$,

$$\operatorname{Re}\frac{1}{\sigma + iu - \rho} = \frac{\sigma - \operatorname{Re}(\rho)}{|\sigma + iu - \rho|^2} \geq 0$$

$(\sigma > 1)$.

Discarding terms, we get

$$-\frac{3}{\sigma - 1} + \frac{4}{\sigma - \beta} \leq C\log(|t|+2).$$

Take $\sigma = 1 + \frac{sc}{\log(|t|+2)}$, and assume $\beta \geq 1 - \frac{c}{\log(|t|+2)}$ to get

$$-3\frac{\log(|t|+2)}{5c} + 4\frac{\log(|t|+2)}{6c} \leq C(\log|t| + 2).$$

Take $c = \frac{1}{16C}$ to get a contradiction. □

**Theorem 3.11** (Bounding $zeta'/zeta$)**.** Assuming that:

- $c > 0$ sufficiently small
- $T \geq 0$
- $\mathrm{Re}(s) \geq -10$
- $|\,\mathrm{Im}(s)| \in [T, T+1]$
- $s$ is at least distance $\frac{c}{\log(T+2)}$ away from any zero or pole

Then

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \ll_c (\log(T+2))^2.$$

*Proof.* If $s = \sigma + it$ with $\sigma > 10$, then

$$\begin{aligned}\left|\frac{\zeta'(s)}{\zeta(s)}\right| &= \left|\sum_{n=1}^{\infty} \Lambda(n) n^{-s}\right| \\ &\leq \sum_{n=1}^{\infty} \Lambda(n) n^{-\sigma} \\ &\ll 1\end{aligned}$$

Assume then that $\mathrm{Re}(s) \in [-10, 10]$. Apply $(**)$. Each term satisfies

$$\begin{aligned}\frac{1}{|s-\rho|} &\leq \frac{\log(T+2)}{c} \\ \frac{1}{|s-1|} &\leq \frac{\log(T+2)}{c}\end{aligned}$$

We know that there are $O(\log(T+2))$ zeros with multiplicity having imaginary part $\in [T-2, T+2]$. The claim follows from triangle inequality. □

TODO

# Index