Number Theory Notebook

Junchi Wang

September 2025

Contents

Notation

This section summarizes the main symbols and notations used throughout the thesis.

Symbol	**Meaning**
$d\|n$	d is a divisor of n
$\lfloor \cdot \rfloor$	floor function
$f = O(g)$	f is bounded by g, i.e. $\|f(x)\| \leq Cg(x)$
$f \sim g$	$\frac{f(x)}{g(x)} \to 1$
$n!$	$\prod_{1 \leq k \leq n} k$
$\binom{a}{b}$	binomial, i.e. $\frac{a!}{(a-b)!b!}$
(m, n)	greatest common divisor (gcd) of m, n
$[m, n]$	least common multiple (lcm) of m, n

1 Counting Prime Numbers

1.1 Introduction

It has been known since the time of Euclid that there are infinitely many prime numbers. Arguing by contradiction, suppose that there were only finitely many primes $p_1, \ldots, p_n$. Then the number $p_1 \cdots p_n + 1$ must have a prime divisor not equal to any of $p_1, \ldots, p_n$. In this course we will be interested in quantifying the infinitude of prime numbers. To do so, we define the prime counting function

$$\pi(x) = \#\{\, p \in \mathcal{P} : p \leq x \,\}.$$

Euclid's theorem therefore says that $\pi(x) \to \infty$ as $x \to \infty$, but the question is

at what rate?

Theorem 1 (Prime Number Theorem (PNT))**.** *As $x \to \infty$ we have*

$$\pi(x) \sim \frac{x}{\log x}.$$

1.2 Euler's Method

Zeta Function: For $s > 1$ one considers the convergent series

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

In terms of prime numbers:

$$\zeta_p(s) = 1 + \frac{1}{p^s} + \frac{1}{(p^2)^s} + \cdots + \frac{1}{(p^\alpha)^s} + \ldots.$$

As geometric series, we have

$$\zeta_p(s) = (1 - 1/p^s)^{-1}$$

Key observation:

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \zeta_p(s) = \prod_p (1 - 1/p^s)^{-1} \tag{1}$$

Assume there are finite primes, $\prod_p (1 - 1/p^s)^{-1}$ will be finite, but the $\sum_{n \geq 1} \frac{1}{n^s}$ will be infinite as $s \to 1$, which contradicts our assumption, thus the number of primes is infinite.

If we take logarithm on each side, the equation can be written as,

$$\log \zeta(s) = \log \prod_p (1 - 1/p^s)^{-1} = -\sum_p \log(1 - 1/p^s) \approx \sum_p 1/p^s \tag{2}$$

The $\zeta(s)$ is infinite as $s \to 1$, thus the series

$$\sum_p 1/p \tag{3}$$

is *divergent.*

1.3 Chebyshev's Method

Theorem 2. *There exist constants $0 < c < C$ such that for $x \geq 2$ one has*

$$c\frac{x}{\log x} \leq \pi(x) \leq C\frac{x}{\log x}.$$

Definition 1 (p-adic valuation)**.** *For $n \in \mathbb{Z} \setminus \{0\}$ and p a prime number, the p-adic valuation of n, written $v_p(n)$, is the largest integer $\alpha \geq 0$ such that p^α divides n. That is to say, such that $p^\alpha \mid n$ and $p^{\alpha+1} \nmid n$. In particular, one has*

$$n = \prod_{p|n} p^{v_p(n)} = \prod_{p \in \mathcal{P}} p^{v_p(n)}.$$

Define $\theta(x)$:

$$\theta(x) = \sum_{p \leq x} \log p$$

Theorem 3 (Mertens)**.** *We have*

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

Proof. **Key Observation:**

$$n! = \prod_{p \leq n} p^{v_p(n!)} \tag{4}$$

$$\log(n!) = \sum_{p \leq n} v_p(n!) \log p$$

The left hand side can be written as,

$$\log(n!) = \sum_{1 \leq x \leq n} \log x \approx \int_1^n \log x \mathrm{d}x = n \log(n) + O(n)$$

The right hand side can be written as

$$\sum_{p\leq n} v_p(n!)\log p = \sum_{p\leq n}\log p\sum_{x\leq n}\sum_{a\geq 1,p^a|x} 1 = \sum_{p\leq n}\log p\sum_{a\geq 1}\sum_{x\leq n,p^a|x} 1$$

Which can be expressed as,

$$= \sum_{p\leq n}\log p\sum_{a\geq 1}\lfloor\frac{n}{p^a}\rfloor = \sum_{p\leq n}\log p\frac{n}{p} + O(n)$$

Finally we have,

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

thus,

$$\sum_{p\leq n}\frac{\log p}{p} = \log(n) + O(1) \tag{5}$$

$\square$

2 Sums of arithmetic functions

2.1 arithmetic functions

Definition 2.1. *An arithmetic function is a complex-valued function on the positive integers,* $f : \mathbb{N}_{\geq 1} \to \mathbb{C}$*. We write* $\mathcal{A}$ *for the* $\mathbb{C}$*-vector space of arithmetic functions.*

The *von Mangoldt* function

$$\Lambda(n) = \begin{cases} \log p, & n = p^\alpha,\ \alpha \geq 1, \\ 0, & n \neq p^\alpha. \end{cases}$$

Definition 2.2. *Let* f *be an arithmetic function. The summation function of* f *is the function defined on* $\mathbb{R}_{\geq 0}$ *by*

$$x \mapsto M_f(x) = \sum_{1 \leq n \leq x} f(n).$$

The summation function of f is a piecewise constant function, and in this chapter, we will present methods to study the following question:

2.2 Approximation by integrals

If f is the restriction to $\mathbb{N}_{\geq 1}$ of a continuous function on $\mathbb{R}$, then $M_f(x)$ is often well approximated by

$$\int_1^x f(t)\, dt.$$

For example, if f is *monotone* we have

Theorem 4 (Monotone comparison)**.** *If* f *is monotone we have*

$$M_f(x) = \int_1^x f(t)\, dt + O(|f(1)| + |f(x)|). \tag{6}$$

2.3 Dirichlet convolution

The Dirichlet convolution is a composition law on the set of arithmetic functions that realizes the multiplicative structure of the integers.

Let $f, g \in \mathcal{A}$, and define $f * g \in \mathcal{A}$ by setting

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{d|n} f(d)g(n/d)\,.$$

Example:

$$\log = \Lambda * 1, \quad \text{i.e.} \quad \log(n) = \sum_{d|n} \Lambda(d).$$

Indeed, if $n = \prod_p p^{\alpha_p}$ then

$$\begin{aligned}
\log(n) &= \log\left(\prod_p p^{\alpha_p}\right) \\
&= \sum_p \alpha_p \log(p) \\
&= \sum_p \sum_{1 \le \alpha \le \alpha_p} \log(p) \\
&= \sum_{p^\alpha | n} \log(p) = \sum_{d|n} \Lambda(d).
\end{aligned}$$

2.4 Applications to Counting Prime Numbers

Theorem 5 (Mertens)**.** *We have*

$$\sum_{n \le x} \frac{\Lambda(n)}{n} = \log(x) + O(1). \tag{7}$$

Proof. start from

$$\sum_{n \le x} \log n = x \log x + O(x) \tag{8}$$

The left hand side can be written as,

$$\sum_{n \le x} \log n = \sum_{n \le x} \sum_{d|n} \Lambda(d) = \sum_{d \le x} \lfloor \frac{x}{d} \rfloor \Lambda(d) = \sum_{d \le x} \frac{x}{d} \Lambda(d) + O(x)$$

Finally we have,

$$\sum_{d \le x} \frac{x}{d} \Lambda(d) + O(x) = x \log x + O(x) \tag{9}$$

□

2.5 Multiplicative functions

Definition 2.16. *A non-zero arithmetic function f is called multiplicative if and only if for all $m, n \ge 1$ with $(m, n) = 1$ we have $f(mn) = f(m)f(n)$. A non-zero arithmetic function is called completely multiplicative if for all $m, n \ge 1$ we have $f(mn) = f(m)f(n)$.*

Proposition 2.1. *If f and g are multiplicative, then $f * g$ and $f^{(-1)}$ are as well.*

3 Dirichlet Series