Number Theory Notebook

Junchi Wang

jw3724@ic.ac.uk

Based on course notes by Ian Petrow

Contents

Notation **3**

Notation **4**

1 Counting Prime Numbers **5**

1.1 Introduction 5

1.2 Euler's Method 5

1.3 Chebyshev's Method 6

2 Sums of arithmetic functions **8**

2.1 arithmetic functions 8

2.2 Approximation by integrals 8

2.3 Dirichlet convolution 8

2.4 Applications to Counting Prime Numbers 10

2.5 Multiplicative functions 10

3 Dirichlet Series **11**

3.1 Review of Power Series 11

3.2 Dirichlet Series 11

3.3 Dirichlet series and multiplicative functions 13

4 Primes in Arithmetic Progressions **15**

4.1 arithmetic progressions 15

4.2 abelian group 16

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
$a \equiv b \pmod q$	a and b are congruent modulo q

Function

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

Symbol	**Meaning**
$\pi(x)$	prime counting function
$\zeta(s)$	zeta function

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

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

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

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

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:

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

Assume there are finite primes, $\prod_p (1 - 1/p^s)^{-1}$ will be finite, but the $\sum_{n \ge 1} \frac{1}{n^s}$ 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,

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

□

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

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

Möbius inversion formula: The *Möbius function* is by definition the inverse of the constant function 1:

$$\mu = 1^{(-1)}, \quad \mu(1) = 1, \quad \mu(n) = -\sum_{\substack{d|n \\ d<n}} \mu(d) \quad \text{for } n \ge 2.$$

In the following section we will show that

1. If n is divisible by a square not equal to 1 (i.e. there exists a prime p such that $p^2 \mid n$), then $\mu(n) = 0$.

2. If n is square-free, and has r prime factors (i.e. $n = p_1 \cdots p_r$), then $\mu(n) = (-1)^r$.

The inverse of the constant function 1 indicates that

$$\mu * 1 = \delta$$

where $\delta(n) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$

Proof. when $n > 1$,

$$\begin{aligned}
\mu * 1(n) &= \sum_{d|n} \mu(d) \\
&= \sum_{d|n, p^2|d} \mu(d) + \sum_{d|n, p^2\nmid d} \mu(d) \\
&= 0 + \sum_{d|n, p^2\nmid d} \binom{r}{x} (-1)^x 1^{r-x} \\
&= 0 + 0 \\
&= 0
\end{aligned}$$

□

2.4 Applications to Counting Prime Numbers

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

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

Proof. start from

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

The left hand side can be written as,

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

Finally we have,

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

□

2.5 Multiplicative functions

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

3.1 Review of Power Series

For a sequence a_n, the power series is defined as,

$$F(a,q) = \sum_{n\geq 0} a_n q^n \tag{10}$$

The radius of convergence is defined as,

$$\frac{1}{\rho} = \limsup_{n\to\infty} |a_n|^{1/n} \tag{11}$$

Let b_n be another sequence with associated power series,

$$F(b,q) = \sum_{n\geq 0} b_n q^n$$

The product will be

$$F(a,q)F(b,q) = \sum_{n\geq 0} c_n q^n \quad c_n = \sum_{k+l=n} a_k b_l \tag{12}$$

3.2 Dirichlet Series

Dirichlet series are to arithmetic functions as power series are to sequences of numbers. Let $f \in \mathcal{A}$ be an arithmetic function. The *Dirichlet series* associated to f is the series in the complex variable s given by

$$s \mapsto L(s,f) = \sum_{n\geq 1} \frac{f(n)}{n^s}.$$

Definition 3.1. An arithmetic function $f : \mathbb{N}_{\geq 1} \to \mathbb{C}$ is of *polynomial growth* if it satisfies one of the following equivalent conditions.

- There exists a constant $A \in \mathbb{R}$ (depending on f) such that $|f(n)| = O(n^A)$.
- There exists $\sigma \in \mathbb{R}$ such that the series $L(\sigma, f)$ is absolutely convergent.

In this case we write

$$\sigma_f = \inf\{\sigma \in \mathbb{R} : L(\sigma, f) \text{ converges absolutely}\} \in \mathbb{R} \cup \{-\infty\};$$

The number σ_f is called the *abscissa of convergence* of $L(s,f)$.

Proof. Exercise. □

Proposition 3.1. *Let f be an arithmetic function with polynomial growth, and let σ_f be its abscissa of convergence. For all $\sigma > \sigma_f$, the series $L(s,f)$ converges absolutely and uniformly in the half-plane $\{s \in \mathbb{C} : \mathrm{Re}(s) \geq \sigma\}$. In this domain, the derivative of $L(s,f)$ is the Dirichlet series of the arithmetic function*

$$-\log f : n \mapsto -\log(n)f(n),$$

that is to say,

$$L'(s,f) = L(s, -\log f) = \sum_{n\geq 1} \frac{-\log(n)f(n)}{n^s},$$

which has abscissa of convergence σ_f as well.

Proof. To prove abscissa of convergence $\sigma_{-\log .f} = \sigma_f$, for $n \geq 3$,

$$\log n|f(n)| > |f(n)| \tag{13}$$

which indicates that $\sigma_{-\log .f} \geq \sigma_f$ On the other hand,

$$L'(s,f) = L(s, -\log f) = \sum_{n\geq 1} \frac{-\log(n)f(n)}{n^s},$$

which converges on $\mathrm{Re}(s) \geq \sigma_f$, the function $-\log .f$ have a convergence area greater or equal than $\mathrm{Re}(s) \geq \sigma_f$, i.e.

$$\sigma_{-\log .f} \leq \sigma_f$$

Thus we have $\sigma_{-\log .f} = \sigma_f$ □

The main reason to introduce Dirichlet series is the following.

Theorem 6. *Let $f, g \in \mathcal{A}$, with $\sigma_f, \sigma_g < \infty$. Then, $\sigma_{f*g} \leq \max(\sigma_f, \sigma_g)$, and for $\mathrm{Re}(s) > \max(\sigma_f, \sigma_g)$ we have*

$$L(s, f*g) = L(s,f)L(s,g).$$

Proof. Let $\mathrm{Re}(s) > \max(\sigma_f, \sigma_g)$, so that

$$\sum_{n=1}^{\infty} \frac{|f*g(n)|}{|n^s|} = \sum_{n=1}^{\infty} \frac{|\sum_{ab=n} f(a)g(b)|}{n^{\mathrm{Re}(s)}}$$

$$\leq \sum_{n=1}^{\infty} \sum_{ab=n} \frac{|f(a)||g(b)|}{(ab)^{\mathrm{Re}(s)}}$$

$$= \sum_{a,b=1}^{\infty} \frac{|f(a)||g(b)|}{(ab)^{\mathrm{Re}(s)}} = \left(\sum_{a=1}^{\infty} \frac{|f(a)|}{a^{\mathrm{Re}(s)}}\right)\left(\sum_{b=1}^{\infty} \frac{|g(b)|}{b^{\mathrm{Re}(s)}}\right) < \infty.$$

All of the above identities and swaps of order of summation above are justified by the fact that we are summing positive terms. We have thus shown that $\sigma_{f*g} \leq \max(\sigma_f, \sigma_g)$. Moreover, for $\mathrm{Re}(s) > \max(\sigma_f, \sigma_g)$, we have by absolute convergence that we can regroup the terms arbitrarily, and so we have

$$L(s,f)L(s,g) = L(s, f*g).$$

□

3.3 Dirichlet series and multiplicative functions

Theorem 7. *Let $f \in \mathcal{A}$ be a multiplicative function of polynomial growth, then for all $\sigma > \sigma_f$ we have*

1. *For all p prime, the series*

   $$L_p(s,f) := \sum_{a \geq 0} \frac{f(p^a)}{p^{as}}$$

   converges absolutely and uniformly in the half plane $\mathrm{Re}(s) \geq \sigma$. We call $L_p(s,f)$ the local factor of f at p.

2. *Moreover, we have*

   $$L(s,f) = \prod_p L_p(s,f) = \lim_{P \to \infty} \prod_{p \leq P} L_p(s,f),$$

   and the convergence is uniform in this half-plane.

3. *More precisely, if we write*

   $$L^{>P}(s,f) = \prod_{p>P} L_p(s,f),$$

   then as $P \to \infty$ we have

   $$L^{>P}(s,f) \to 1$$

   uniformly in every half-plane $\mathrm{Re}(s) \geq \sigma$, $\sigma > \sigma_f$.

4. *Conversely, if f is an arithmetic function such that $\sigma_f < \infty$ and $f(1) = 1$ and if $L(s, f)$ satisfies*

$$L(s,f) = \prod_p L_p(s,f) = \lim_{P\to\infty} \prod_{p\leq P} L_p(s,f)$$

for s sufficiently large, then f is multiplicative.

Proof.

$$\begin{aligned}
\prod_p L_p(s,f) &= \prod_p \sum_{a\geq 0} \frac{f(p^a)}{(p^a)^s} \\
&= \sum_{a_1\geq 0, a_2\geq 0,\ldots} \frac{f(p_1^{a_1})f(p_2^{a_2})\ldots}{(p_1^{a_1})^s(p_2^{a_2})^s\ldots} \\
&= \sum_{a_1\geq 0, a_2\geq 0,\ldots} \frac{f(p_1^{a_1}p_2^{a_2}\ldots)}{(p_1^{a_1}p_2^{a_2}\ldots)^s} \\
&= \sum_{n\geq 1} \frac{f(n)}{n^s} = L(s,f)
\end{aligned}$$

$\square$

Corollary 1. *If f is completely multiplicative, then for $\mathrm{Re}(s) > \sigma_f$ we have*

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

4 Primes in Arithmetic Progressions

4.1 arithmetic progressions

Definition 2. *An arithmetic progression is a doubly-infinite* ***subset*** *of* $\mathbb{Z}$ *satisfying the following property: There exists a positive integer* $q > 0$ *such that the distance between two consecutive integers of this subset is always* q*. The integer* q *is called the modulus of the arithmetic progression.*

It is easy to see that arithmetic progressions of modulus q are of the form

$$L_{q,a} = a + q\mathbb{Z} \subseteq \mathbb{Z},$$

where a is an integer. We remark that if $a \equiv a' \pmod{q}$, then we have $L_{q,a} = L_{q,a'}$. Thus arithmetic progressions of modulus q are indexed by the congruence classes modulo q (i.e. by the ring $\mathbb{Z}/q\mathbb{Z}$). There are therefore q of them. The integer a is called the class of the arithmetic progression.

Theorem 8 (Dirichlet's theorem on primes in arithmetic progressions)**.** *Let* $a, q > 0$ *be two relatively prime integers. Then, the set*

$$\mathcal{P}_{q,a} = \mathcal{P} \cap L_{q,a}$$

is infinite. Said differently, there exist infinitely many prime numbers $p \equiv a \pmod{q}$*.*

In the vein of the prime number theorem, we can pose more precise questions on the density of the set $\mathscr{P}_{q,a}$. We therefore set

$$\pi(x; q, a) = |\mathscr{P}_{q,a} \cap [1, x]| = |\{p \leq x : p \equiv a \pmod{q}\}| = \sum_{\substack{p \equiv a \pmod{q} \\ p \leq x}} 1$$

the counting function of the primes $p \equiv a \pmod{q}$. At the beginning of the 20th century, Landau showed this generalization of the prime number theorem:

Theorem 9. *(Landau). Let* $a, q > 0$ *be relatively prime integers. Then*

$$\pi(x; q, a) = \frac{1}{\varphi(q)}\pi(x)(1 + o(1)) = \frac{1}{\varphi(q)}\frac{x}{\log x}(1 + o(1)).$$

where $\varphi = \mu * Id$ *is the Euler function,* $\mu = 1^{(-1)}$ *is the Möbius function and* $Id(n) = n$ *is identity function.*

Merten's theorem is extended to intersection set of primes and arithmetic progressions.

Theorem 10. *We have*

$$\sum_{\substack{n\leq x \\ n\equiv a \pmod q}} \frac{\Lambda(n)}{n} = \frac{1}{\varphi(q)} \log(x) + O(1) \tag{4.1}$$

$$\sum_{\substack{p\leq x \\ p\equiv a \pmod q}} \frac{\log p}{p} = \frac{1}{\varphi(q)} \log(x) + O(1), \tag{4.2}$$

$$\sum_{\substack{p\leq x \\ p\equiv a \pmod q}} \frac{1}{p} = \frac{1}{\varphi(q)} \log\log(x) + O(1). \tag{4.3}$$

The crucial point is the group structure of the set $(\mathbb{Z}/q\mathbb{Z})$.

4.2 abelian group

The Abelian group is the group in which the group operation is commutative, meaning that the order of operation does not affect the results.

Let G be a finite abelian group, and $g \in G$ is an element in the group. The action of right translation is defined as,

$$T_g f : g' \mapsto T_g f(g') = f(g'g) \tag{14}$$

We can verify that,

$$T_g \circ T_{g'} = T_{gg'} \tag{15}$$

As the action is invertible, the inverse is defined as,

$$(T_g)^{-1} = T_{g^{-1}} \tag{16}$$

As G is abelian group, the action can commute,

$$T_g \circ T_{g'} = T_{g'} \circ T_g \tag{17}$$

The inner product is defined as,

$$\langle f, f' \rangle = \frac{1}{|G|} \sum_{g\in G} f(g)\, \overline{f'(g)}. \tag{18}$$