Topics in Number Theory

Instructor : Dr. Kaneenika Sinha

Spring 2026

Contents

Chapter 1

Elementary Methods

1.1 Arithmetic Functions

Definition 1.1. A function is said to be arithmetic, if $f : \mathbb{N} \to \mathbb{C}$.

- f is said to be additive if $f(mn) = f(m)+f(n)\ \forall m, n$ such that $(m, n) = 1$.
- f is said to be multiplicative if $f(mn) = f(m)f(n)\ \forall m, n$ such that $(m, n) = 1$.
- f is said to be completely additive or multiplicative if additive or multiplicative property holds for all $m, n \in \mathbb{N}$

Examples. Some arithmetic functions:

1. $\omega : \mathbb{N} \to \mathbb{C}$, $\omega(n) =$ #distincty prime factors of n.
   Additive.
2. $\Omega : \mathbb{N} \to \mathbb{C}$, $\Omega(n) =$ #prime factors of n with multiplicity.
   Completely additive.
3. $\log : \mathbb{N} \to \mathbb{C}$
   Completely additive.
4. $\mu : \mathbb{N} \to \mathbb{C}$ - Mobius function

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & n \text{ is squarefree} \\ 0 & \text{otherwise} \end{cases}$$

   Multiplicative.

5. $\Lambda : \mathbb{N} \to \mathbb{C}$ - von Mongoldt function

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

Neither multiplicative nor additive.

6. $\lambda(n) : \mathbb{N} \to \mathbb{C}$ - Lioville's function

$$\lambda(n) = \begin{cases} 1 & n = 1 \\ (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_k} & \alpha_i \text{ such that } n = \prod_{i \leqslant k} p_i^{\alpha_i} \end{cases}$$

Completely multiplicative.

7. $\varphi : \mathbb{N} \to \mathbb{C}$ - Euler's totient function

$$\begin{aligned} \varphi(n) &= |\{1 \leqslant k \leqslant n : (n,k) = 1\}| \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right), \text{ and } \varphi(1) = 1. \end{aligned}$$

$\varphi(mn) = \varphi(m)\varphi(n)\frac{(m,n)}{\varphi(m,n)}$

8. $f : \mathbb{N} \to \mathbb{C}$, $f(n) = n^{-s}$, $s \in \mathbb{C}$.
Completely multiplicative.

Theorem 1.1. *If* $n \geqslant 1$, $\sum_{d|n} \mu(d) = I(n) := \left[\frac{1}{n}\right]$.

Proof. When $n = 1$, the summation is equal to $1 = I(1)$. Let $n = \prod_{i=1}^{m} p_i^{\alpha_i}$ for some $m \in \mathbb{N}$, and let $N = \prod_{i=1}^{m} p_i$. Now,

$$\begin{aligned} \sum_{d|n} \mu(d) = \sum_{d|N} \mu(d) &= 1 + \sum_{1 \leqslant i \leqslant m} \mu(p_i) + \sum_{1 \leqslant i,j \leqslant m} \mu(p_i p_j) + \cdots + \mu(N) \\ &= 1 - \binom{m}{1} + \binom{m}{2} - \cdots + (-1)^m \\ &= (1 + (-1))^m = 0 = I(n) \end{aligned}$$

■

Definition 1.2 (Number Field)**.** A finite field extension of Q is known as a number field.

Definition 1.3. An integer α is said to be algebraic if $f(\alpha) = 0$ for some monic irreducible $f \in \mathbb{Z}[x]$.

Definition 1.4. Given a number field K, the set

$$\theta_k := \{\alpha \in K : \alpha \text{ is an algebraic integer}\}$$

is known as its ring of integers.

Theorem 1.2. *Given $\zeta(s) > 0 \forall s > 1$, there are inifinetely many primes.*

Proof. By Euler product formula,

$$\begin{aligned}\log \zeta(s) &= \sum_p \log\left(1 - \frac{1}{p^s}\right) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{ns}} \\ &= \sum_p \frac{1}{p^s} + \sum_p \sum_{n \geqslant 2} \frac{1}{np^{ns}}\end{aligned}$$

If $s > 1$,

$$\begin{aligned}\sum_p \sum_{n \geqslant 2} \frac{1}{np^{ns}} &\leqslant \sum_p \sum_{n \geqslant 2} \frac{1}{p^n} \\ &= \sum_p \frac{1}{p(p-1)} \leqslant \sum_p \frac{2}{p^2} < \infty\end{aligned}$$

$$\begin{aligned}&\implies \lim_{s \to 1^+} \log \zeta(s) = +\infty \\ &\implies \sum_p \frac{1}{p} = +\infty\end{aligned}$$

Hence, there are infintely many primes. ∎

1.2 Infinite Products

Let $\alpha_1, \alpha_2, \ldots$ be a sequence in $\mathbb{R}$, and let $P(n) = \prod_{k=1}^{\infty} \alpha_k$. If $\lim_{k \to \infty} \prod_{k=1}^{\infty} \alpha_k$ converges, then we say that $\prod_{k=1}^{\infty} \alpha_k$ converges.

If $\prod_{k=1}^{\infty}(1+a_k)$ converges, then $\forall k$, $a_k \neq -1$, and for all $k \geqslant 2$,

$1 + a_k = \frac{P(k)}{P(k-1)} \implies \lim_{k\to\infty}(1+a_k) = 1$. Thus, if $\prod_{k=1}^{\infty}(1+a_k)$ converges, then $\lim_{k\to\infty}(a_k) = 0$

Theorem 1.3. *Given* $a_k \geqslant 0\ \forall k \geqslant 1$, $\prod_{k=1}^{\infty}(a_k+1)$ *converges iff* $\sum_{k=1}^{\infty} a_k < 0$.

Proof. Let $S(n) := \sum_{k=1}^{n} a_k$, and $p(n)) := \prod_{k=1}^{n}(1+a_k)$.

$$\begin{aligned} 0 \leqslant \sum_{k=1}^{n} a_k &\leqslant \prod_{k=1}^{n}(1+a_k) \\ &\leqslant \prod_{k=1}^{n} e^{a_k} \\ &= e^{\left(\sum_{k=1}^{n} a_k\right)} \end{aligned}$$

$$\implies 0 \leqslant S(n) \leqslant P(n) \leqslant e^{s(n)}$$

Since both $S(n)$ and $P(n)$ are monotonically increasing, $\lim_{n\to\infty} P(n)$ exists iff $\lim_{n\to\infty} S(n)$ exists and is nonzero. ■

Corollary. $\prod_{k=1}^{\infty}(1+|a_k|) < \infty \Leftrightarrow \sum_{k=1}^{\infty}|a_k| < \infty$.

Theorem 1.4. *If* $\prod_{k=1}^{\infty}(1+|a_k|)$ *converges, then* $\prod_{k=1}^{\infty}(1+a_k)$ *also converges.*

Proof. Let $P(n) = \prod_{k=1}^{n}(1+a_k)$, and $R(n) = \prod_{k=1}^{n}(1+|a_k|)$.

$\sum_{n=2}^{\infty}(R(n) - R(n-1)) < \infty$, since it is given that $\{R(n)\}_{n\geqslant 2}$ converges.

Now,

$$\begin{aligned} 0 \leqslant |P(n) - P(n-1)| &= |a_n P(n-1)| \\ &= \left| a_n \prod_{k=1}^{n-1} (1 + a_k) \right| \\ &\leqslant |a_n| \prod_{k=1}^{n-1} (1 + |a_k|) \\ &= R(n) - R(n-1) \end{aligned}$$

$$\therefore \sum_{n=2}^{\infty} |P(n) - P(n-1)| < \infty \implies \sum_{n=2}^{\infty} P(n) - P(n-1) < \infty$$

Further,

$$\begin{aligned} \sum_{n=2}^{\infty} P(n) - P(n-1) &= \lim_{n\to\infty} P(n) - P(1) \\ \implies \lim_{n\to\infty} P(n) &< \infty \end{aligned}$$

Since $a_k \to 0$ as $k \to \infty$, $|1 + a_k| \leqslant \frac{1}{2}$ for all $k \geqslant k_0$, for some large k_0,

$$\begin{aligned} \forall k \geqslant k_0, \ \left| \frac{-a_k}{1 + a_k} \right| &\leqslant 2|a_k| \\ \implies \prod_{k=1}^{\infty} \left(1 - \frac{a_k}{a_{k+1}} \right) &< \infty \\ \implies \prod_{k=1}^{\infty} \left(\frac{1}{1 + a_k} \right) &< \infty \end{aligned}$$

Hence, $\lim_{n\to\infty} P(n) \neq 0$ ■

1.3 Ordering of Arithmetical Functions

Definition 1.5. Take $f : \mathbb{R} \to \mathbb{C}$, and consider $g : \mathbb{R} \to \mathbb{R}$ such that $g(x) > 0$ for all $x \geqslant x_0$ for some $x_0 \in \mathbb{R}$.

- → If $\exists C > 0$ such that $|f(x)| \leqslant Cg(x)$ for all $x \geqslant x_0$ or as $x \to \infty$, we say $f \ll g$, and that $f = O(g)$.
- → If $\exists C > 0$ such that $|f(x)| \geqslant Cg(x)$ for all $x \geqslant x_0$ or as $x \to \infty$, we say $f \gg g$.

Definition 1.6. Given $f : \mathbb{N} \to \mathbb{C}$, and $g : \mathbb{R} \to \mathbb{R}$ such that $g(x) > 0$ for all $x \geqslant x_0$ for some $x_0 \in \mathbb{R}$, we say that $f = o(g)$ (as $n \to \infty$), if $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$.
$f = o(g) \implies f = O(g)$.

Proposition 1.1. $\log(n) = O(n^\varepsilon)$, *for all* $\varepsilon > 0$.

Proof. Let $g : [1, \infty) \to \mathbb{R}$, such that $g(x) = \frac{\log(x)}{x^\varepsilon}$.

$$\begin{aligned} g'(x) = 0 &\implies \frac{x^{\varepsilon-1} - \varepsilon \log(x) x^{\varepsilon-1}}{x^{2\varepsilon}} = 0 \\ &\implies \varepsilon \log(x) = 1 \\ &\implies x = e^{\frac{1}{\varepsilon}} \end{aligned}$$

That is, for all $x \geqslant 1$

$$\begin{aligned} g(x) \leqslant g(e^{\frac{1}{\varepsilon}}) &= \frac{1}{e\varepsilon} \\ \implies \log(x) &\leqslant \frac{x^\varepsilon}{e\varepsilon} \end{aligned}$$

■

Proposition 1.2. $d(n) = O(n^\varepsilon)$, *where* $d(n) :=$ *# of positive divisors of* n.

Proof. We know that $n = \prod_{p|n} p^{\alpha_p}$. Let $a|n$; then $a = \prod_{p|n} p^{b_p}$, where $0 \leqslant b_p \leqslant \alpha_p$. Thus, $d(n) = \prod_{p|n} (\alpha_p + 1)$.

$$\begin{aligned} \frac{d(n)}{n^\varepsilon} &= \prod_{p|n} \frac{\alpha_p + 1}{p^{\alpha_p \varepsilon}} \\ &= \prod_{\substack{p|n \\ p<2^{1/\varepsilon}}} \frac{\alpha_p + 1}{p^{\alpha_p \varepsilon}} \prod_{\substack{p|n \\ p\geqslant 2^{1/\varepsilon}}} \frac{\alpha_p + 1}{p^{\alpha_p \varepsilon}} \end{aligned}$$

When $\varepsilon \geqslant 1$, it is easy to see that the proposotion holds. Now we consider $0 < \varepsilon \leqslant 1$. Note that $\prod_{\substack{p|n \\ p\geqslant 2^{1/\varepsilon}}} \frac{\alpha_p + 1}{p^{\alpha_p \varepsilon}}$ has factors $\frac{\alpha_p+1}{p^{\alpha_p \varepsilon}} \leqslant \frac{\alpha_p+1}{2^{\alpha_p \varepsilon}} \leqslant 1$.

$$\implies \frac{d(n)}{n^\varepsilon} \leqslant \prod_{p<2^{1/\varepsilon}} < \prod_{\substack{p|n \\ p<2^{1/\varepsilon}}} \frac{\alpha_p + 1}{p^{\alpha_p \varepsilon}}$$

Now since $p < 2^{1/\varepsilon}$,

$$\frac{\alpha_p + 1}{p^{\alpha_p \varepsilon}} \leqslant 1 + \frac{\alpha_p}{p^{\alpha_p \varepsilon}} \leqslant 1 + \frac{1}{\varepsilon \log p}$$

Hence,

$$\frac{d(n)}{n^{\varepsilon}} \leqslant \prod_{p < 2^{1/\varepsilon}} \left(1 + \frac{1}{\varepsilon \log p}\right) \implies d(n) \leqslant C(\varepsilon) n^{\varepsilon}$$

■

Theorem 1.5. $\forall \delta > 0\ \exists n_0 \in \mathbb{N}$, *such that* $d(n) < 2^{(1+\delta)\frac{\log n}{\log\log n}}, \forall n \geqslant n_0$

Proved in [Murty, 2008] Ex. 1.33

Remark. $2^{\omega(n)} \leqslant n$, as $\omega(n) \leqslant \frac{\log n}{\log 2}$, that is $\omega(n) = O(n)$. Further, $2^{\omega(n)} \leqslant d(n)$ gives $\omega(n) \leqslant \frac{\log d(n)}{\log 2}$, which implies that $\omega(n) \ll \frac{\log n}{\log\log n}$.

1.4 Summation Tools

1.4.1 Abel Summation

1.5 Finite Abelian Groups

Definition 1.7. A function of the form $\chi : G \to S^1$ such that $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in G$, where G is a finite abelian group is known as a character.

The set of all characters of G is usually denoted as $\widehat{G}$. It can be shown that $\widehat{G}$ is a group with the binary operation $\chi\psi(g) := \chi(g)\phi(g)$. The trivial character χ_0 such that $\chi_0(g) = 1$ for all $g \in G$ will act as the identity of the group. The group $\widehat{G}$ will be abelian if G is abelian.

Proposition 1.3. *If* $f \in \widehat{G}$, *then* $f = e_l$ *for some* $l \in G$, *where* $e_l(k) := e^{2\pi i \frac{lk}{q}}$ *for* $G = \mathbb{Z}/q\mathbb{Z}$.

Lemma 1.1. *Suppose* $e : G \to \mathbb{C}^{\times}$ *is a function such that* $e(ab) = e(a)e(b)$ *for all* $a, b \in G$. *Then* $e \in \widehat{G}$.

Proof. Let $|G| = n$. We know that $e(a^n) = 1$ for all $a \in G$. Hence $|e(a) = 1|$ for all $a \in G$. ■

Lemma 1.2. *If* $e \in \widehat{G}$ *is not the identity, then* $\sum_{a \in G} e(a) = 0$.

Proof. Choose a $b \in G$ such that $e(b) \neq 0$.

$$\begin{aligned} e(b)\sum_{a\in G} e(a) &= \sum_{a\in G} e(ab) \\ &= \sum_{a\in G} e(a) \\ \implies (e(b)-1)\sum_{a\in G} e(a) &= 0 \\ \implies \sum_{a\in G} e(a) &= 0 \end{aligned}$$

■

Let $V = \{f : G \to \mathbb{C}\}$. V forms a finite dimensional vector space over $\mathbb{C}$. Define inner product on V: $\langle f_1, f_2\rangle := \frac{1}{|G|}\sum_{a\in G} f_1(a)\overline{f_2(a)}$

Theorem 1.6. $\widehat{G}$ *forms an orthonormal set in* V.

Proof. For any $e_l, e_k \in \widehat{G}$,

$$\begin{aligned} \langle e_l, e_k\rangle &= \frac{1}{|G|}\sum_{a\in G} e^{2\pi i\frac{l-k}{q}a} \\ &= \begin{cases} 1 & l = k \\ 0 & l \neq k \end{cases} \end{aligned}$$

■

Thus, $|\widehat{G}| \leqslant |G|$. By carefully constructing maps from $\widehat{G}$ to G, it can be shown that $|\widehat{G}| \geqslant |G|$. Hence the theorem:

Theorem 1.7. $|\widehat{G}| = |G|$

Using the results proved above, we can state the orothogonality principles:

1. Let $e \in \widehat{G}$.
$$\sum_{g\in G} e(g) = \begin{cases} |G| & \text{if } e \text{ is the identity} \\ 0 & \text{otherwise} \end{cases}$$
2. Let $x \in G$.
$$\sum_{e\in \widehat{G}} e(x) = \begin{cases} |G| & \text{if } x \text{ is the identity} \\ 0 & \text{otherwise} \end{cases}$$

▲▼▲

Chapter 2

Analytic Theory

▲▼▲

Chapter 3

Advanced Topics

▲▼▲

References

[Apostol, 1976] Apostol, T. M. (1976). *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. Springer.

[Murty, 2008] Murty, M. R. (2008). *Problems in Analytic Number Theory*. Graduate Texts in Mathematics. Springer.

[Nathonson, 2000] Nathonson, M. B. (2000). *Elementary Methods in Number Theory*. Graduate Texts in Mathematics. Springer.