Chapter 2

Arithmetic functions

2.1 Multiplicative and additive functions

A complex-valued function defined on $\mathbb{N}^*$ is called an **arithmetic function**.

Definition 2.1 (Multiplicative/Additive functions)**.** *Let* $f : \mathbb{N}^* \to \mathbb{C}$ *be an arithmetic function. We say* f *is* ***multiplicative*** *if* f *is not identically zero and satisfies*

$$f(mn) = f(m)f(n) \tag{2.1}$$

whenever $(m, n) = 1$. *If* (2.1) *holds unconditionally for all* m, n, *we say* f *is* ***completely multiplicative****.*

Similarly, an arithmetic funtion f *is* ***additive*** *if*

$$f(mn) = f(m) + f(n) \tag{2.2}$$

whenever $(m, n) = 1$. *Moreover, if* (2.2) *holds unconditionally for all* m, n, *we say* f *is* ***completely additive****.*

A multiplicative function f satisfies $f(1) = 1$. In fact, since a multiplicative function is not identically zero, there exists some $n \in \mathbb{N}^*$ s.t. $f(n) \neq 0$. Then we can deduce $f(1) = 1$ from $f(n) = f(n)f(1)$.

A multiplicative function reflects the multiplicative structure of $\mathbb{N}^*$. Let f be a multiplicative function and let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the prime factorization of n. Then we have

$$f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k}). \tag{2.3}$$

Conversely, by assigning a value for each $f(p^\alpha)$, we can uniquely define a multiplicative function by (2.3).

If we further assume that f is completely multiplicative, then we have

$$f(n) = f(p_1)^{\alpha_1} \cdots f(p_k)^{\alpha_k}.$$

So a completely multiplicative function is determined by its value on each prime number.

2.2 Examples

The following arithmetic functions are classical and define fundamental concepts attached to the multiplicative structure of $\mathbb{N}^*$.

1). The divisor function, counting the number of positive divisors of n, is traditionally denoted by

$$\tau(n) = \sum_{d|n} 1.$$

Similarly, we can define the function of the sum of k-th power divisors of n, which is denoted by

$$\sigma_k(n) = \sum_{d|n} d^k, \quad k \in \mathbb{C}.$$

Thus $\tau(n) = \sigma_0(n)$ and usually we write $\sigma(n)$ for $\sigma_1(n)$. The function $\sigma_k(n)$ is multiplicative. In fact, assuming that $(m, n) = 1$, any divisor d of mn can be uniquely decomposed into $d = d_1 d_2$ with $d_1 \mid m$ and $d_2 \mid n$. So

$$\sigma_k(mn) = \sum_{d|mn} d^k = \sum_{d_1|m} \sum_{d_2|n} d_1^k d_2^k = \left(\sum_{d_1|m} d_1^k \right) \left(\sum_{d_2|n} d_2^k \right) = \sigma_k(m)\sigma_k(n).$$

By (2.3), if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, we have

$$\tau(n) = (1 + \alpha_1) \cdots (1 + \alpha_k)$$

2). Euler's totient function $\varphi(n)$, counting the number of invertible residues modulo n, is denoted by

$$\varphi(n) = \left| (\mathbb{Z}/n\mathbb{Z})^\times \right| = \sum_{\substack{1 \le d \le n \\ (d,n)=1}} 1.$$

For $(m,n)=1$, we have

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \quad \Rightarrow \quad (\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \oplus (\mathbb{Z}/n\mathbb{Z})^\times.$$

By considering the cardinal of both sides, we get $\varphi(mn)=\varphi(m)\varphi(n)$. Thus $\varphi(n)$ is multiplicative.

3). Suppose that $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$. Define

$$\omega(n) = k, \quad \Omega(n) = \alpha_1 + \cdots + \alpha_k.$$

That is, $\Omega(n)$ is the number of primes factors of n and $\omega(n)$ is the number of distinct prime factors of n. Clearly, $\omega(n)$ is additive and $\Omega(n)$ is completely additive.

4). The Liouville function is defined by

$$\lambda(n) = (-1)^{\Omega(n)}.$$

Since $\Omega(n)$ is completely additive, $\lambda(n)$ is completely multiplicative.

5). The Möbius function is defined by

$$\mu(n) = \begin{cases} (-1)^k, & n = p_1\cdots p_k, \quad p_1,\ldots,p_k \text{ are distinct prime numbers} \\ 0, & \text{otherwise (i.e. } n \text{ is not square-free).} \end{cases}$$

Note that for coprime m,n, mn is square-free if and only if both m and n are square-free. So it is not hard to see that $\mu(n)$ is multiplicative. The Möbius function plays an important role in the distribution of prime numbers.

6). The Von Mangoldt function $\Lambda(n)$ is defined by

$$\Lambda(n) = \begin{cases} \log p, & n = p^k, p \text{ is prime}, \ k \in \mathbb{N}^* \\ 0, & \text{otherwise.} \end{cases}$$

Roughly speaking, $\Lambda(n)$ is a weighted characteristic function of the set of prime numbers.

2.3 The Dirichlet convolution

For an arithmetic function f, define the **formal Dirichlet series** associated with f by the formal series

$$D(f;s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}.$$

Let f and g be arithmetic functions. A formal computation gives

$$\begin{aligned} D(f;s)D(g;s) &= \left(\sum_{m_1=1}^{\infty}\frac{f(m_1)}{m_1^s}\right)\left(\sum_{m_2=1}^{\infty}\frac{g(m_2)}{m_2^s}\right)=\sum_{m_1=1}^{\infty}\sum_{m_2=1}^{\infty}\frac{f(m_1)g(m_2)}{m_1^s m_2^s} \\ &= \sum_{n=1}^{\infty}\frac{1}{n^s}\left(\sum_{m_1m_2=n}f(m_1)g(m_2)\right). \end{aligned}$$

So the product of $D(f;s)$ and $D(g;s)$ should be defined as the formal Dirichlet series $D(h;s)$ associated with h where h is the arithmetic function given by

$$h(n)=\sum_{m_1m_2=n}f(m_1)g(m_2)=\sum_{d|n}f(d)g\left(\frac{n}{d}\right)=\sum_{d|n}g(d)f\left(\frac{n}{d}\right).$$

This arithmetic function h is called the **Dirichlet convolution** of f and g and is denoted by $f*g$.

For arithmetic functions f and g, we define

$$\begin{cases} D(f;s)+D(g;s)=D(f+g;s) \\ D(f;s)D(g;s)=D(f*g;s). \end{cases} \tag{2.4}$$

It is not hard to see that the set of all formal Dirichlet series equipped with these two operation has the structure of commutative ring with unity given by the series $D(\delta;s)$ associated with the arithmetic function

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

A formal Dirichlet series $D(f;s)$ is uniquely determined by the arithmetic function f. So we see from (2.4) that the set of arithmetic functions, equipped with the usual addition operation and the Dirichlet convolution, has the structure of a commutative ring isomorphic to that of formal Dirichlet series.

Proposition 2.1. *The group of units in the ring of arithmetic functions consists of arithmetic functions f such that $f(1) \neq 0$.*

Proof. If f is invertible with the convolution inverse g, then we have

$$f(1)g(1) = \delta(1) = 1.$$

So $f(1) \neq 0$. Conversely, if $f(1) \neq 0$, we can recursively calculate the convolution inverse g of f. In fact, the arithmetic function g defined by

$$g(1) = f(1)^{-1}, \quad g(n) = -f(1)^{-1} \sum_{\substack{d|n \\ d<n}} g(d) f\left(\frac{n}{d}\right), \quad n > 1 \tag{2.5}$$

clearly satisfies $f * g = \delta$. □

Proposition 2.2. *The set of multiplicative functions is a subgroup of the group of units in the ring of arithmetic functions.*

Proof. We need to show that

1). The Dirichlet convolution of multiplicative functions is multiplicative.

2). The convolution inverse of a multiplicative function is multiplicative.

Proof of 1). Let f and g be multiplicative functions. Suppose that $(m, n) = 1$. Then

$$\begin{aligned}(f * g)(mn) &= \sum_{d|mn} f(d) g\left(\frac{mn}{d}\right) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) g\left(\frac{mn}{d_1 d_2}\right) \\ &= \left(\sum_{d_1|m} f(d_1) g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n} f(d_2) g\left(\frac{n}{d_2}\right)\right) \\ &= (f * g)(m) \cdot (f * g)(n).\end{aligned}$$

Proof of 2). Let f be a multiplicative function. Then we have $f(1) = 1$ (see the dicussion under the definition of multiplicative functions). Thus f is invertible by Proposition 2.1. Let g be the inverse of f. We should prove that

$$(m, n) = 1 \quad \Rightarrow \quad g(mn) = g(m)g(n).$$

We prove by induction on mn. For $mn = 1$, it suffices to show that $g(1) = 1$. This is quite obvious since we have

$$f(1)g(1) = \delta(1) = 1.$$

Now assume that $mn > 1$ and the multiplicativity of g holds for smaller mn. Then we have

$$\begin{aligned}
0 = \delta(mn) &= (f * g)(mn) \\
&= \sum_{d \mid mn} f(d) g\left(\frac{mn}{d}\right) \\
&= \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1 d_2) g\left(\frac{mn}{d_1 d_2}\right) \\
&= \sum_{\substack{d_1 \mid m \\ d_1 d_2 > 1}} \sum_{d_2 \mid n} f(d_1) f(d_2) g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right) + g(mn) \\
&= \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1) f(d_2) g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right) - g(m)g(n) + g(mn) \\
&= \delta(m)\delta(n) - g(m)g(n) + g(mn).
\end{aligned}$$

Since $mn > 1$, we have $\delta(m)\delta(n) = 0$. So $g(mn) = g(m)g(n)$. □

Example 2.1. *Let* $\mathbb{1}$ *denote the function* $\mathbb{1}(n) = 1$. *Then we have* $\tau = \mathbb{1} * \mathbb{1}$ *and* $\sigma_k = n^k * \mathbb{1}$. *So we regain the multiplicativity of* τ *and* σ_k.

Theorem 2.3. *Let* f *be a multiplicative function. Then we have*

$$\sum_{d \mid n} f(d) = \prod_{p^\alpha \| n} \left(1 + f(p) + \cdots + f(p^\alpha)\right),$$

where the notation $\prod_{p^\alpha \| n}$ *means taking the product of all prime factor* p *of* n *and* $v_p(n) = \alpha$.

Proof. By Proposition 2.2,

$$\sum_{d \mid n} f(d) = (f * \mathbb{1})(n)$$

is a multiplicative function in n. So we have

$$\sum_{d \mid n} f(d) = \prod_{p^\alpha \| n} \sum_{d \mid p^\alpha} f(d) = \prod_{p^\alpha \| n} \left(1 + f(p) + \cdots + f(p^\alpha)\right).$$

□

2.4 The Möbius inversion formula

Proposition 2.4. *The Möbius function is the convolution inverse of* $\mathbb{1}$*, that is,* $\mathbb{1} * \mu = \delta$*. In other words,*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n > 1. \end{cases}$$

Proof. Suppose that $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $n > 1$ (i.e. $k \neq 0$). Then

$$(\mu * \mathbb{1})(n) = \sum_{d|n} \mu(d) = \sum_{j=0}^{k} \binom{k}{j} (-1)^j = (1-1)^k = 0.$$

We explain the occurance of binomial numbers. In the sum $\sum_{d|n}$, given $0 \leq j \leq k$, there are exactly $\binom{k}{j}$ choices of square-free d such that d has exactly j distinct prime factors. These d contributes $\binom{k}{j}(-1)^j$. □

We provide an alternative proof. This method is useful in checking an identity of multiplicative functions.

Proof. By Proposition 2.2, both $\delta * \mathbb{1}$ and δ are multiplicative. So we need only to verify

$$(\mu * \mathbb{1})(p^\alpha) = \delta(p^\alpha) = 0$$

for each prime power p^α. In fact, we have

$$(\mu * \mathbb{1})(p^\alpha) = 1 + (-1) + 0 + \cdots + 0 = 0.$$

□

For a completely multiplicative functions, its Dirichlet inverse can be easily computed:

Theorem 2.5. *Let* f *be a multiplicative function. Then* f *is completely multiplicative if and only if*

$$f^{-1}(n) = \mu(n) f(n),$$

where $f^{-1}(n)$ *is the Dirichlet inverse of* f *(should not be confused with* $f(n)^{-1} = 1/f(n)$*).*

Proof. Recall that $f(1) = 1$ since f is multiplicative. Suppose that f is completely multiplicative, then we have

$$(f * \mu f)(n) = \sum_{d|n} \mu(d) f(d) f\left(\frac{n}{d}\right) = f(n) \sum_{d|n} \mu(d) = f(n)\delta(n) = \delta(n).$$

Conversely, suppose

$$f^{-1}(n) = \mu(n) f(n).$$

To show f is completely multiplicative, it suffices to prove

$$f(p^\alpha) = f(p)^\alpha$$

for any prime power p^α. By taking $n = p^\alpha$ in

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

we obtain

$$f(p^\alpha) = f(p) f(p^{\alpha-1}).$$

Hence

$$f(p^\alpha) = f(p) f(p^{\alpha-1}) = f(p)^2 f(p^{\alpha-2}) = \cdots = f(p)^\alpha.$$

□

Theorem 2.6 (Möbius inversion formula)**.** *Let f and g be arithmetic functions. Then the following statements are equivalent:*

1). $g(n) = \sum_{d|n} f(d)$, $\forall n \geq 1$.

2). $f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$, $\forall n \geq 1$.

Proof. We need to show that

$$g = f * \mathbb{1} \quad \Leftrightarrow \quad f = g * \mu.$$

By Proposition 2.4, we have

$$g = f * \mathbb{1} \quad \Leftrightarrow \quad g * \mu = f * \mathbb{1} * \mu = f * \delta = f.$$

This completes the proof. □

Remark. Certainly, we can replace the function $\mathbb{1}$ by any other completely multiplicative function, and apply Theorem 2.5 to get other inversion formulas. Specifically, suppose $w(n)$ is a completely multiplicative function. By Theorem 2.5, we have $w^{-1} = \mu w$. So for any arithmetic funtions f and g, we have

$$g = f * w \quad \Leftrightarrow \quad f = g * \mu w.$$

That is,

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

is equivalent to

$$f(n) = \sum_{d|n} \mu(d) w(d) g\left(\frac{n}{d}\right).$$

Taking $w = \mathbb{1}$, we get Theorem 2.6.

Theorem 2.7 (Generalized Möbius inversion formula)**.** *Let F and G be functions on $[1, +\infty)$. Then the following statements are equivalent:*

i). $G(x) = \sum_{n \le x} F\left(\frac{x}{n}\right)$, $\forall x \ge 1$.

ii). $F(x) = \sum_{n \le x} \mu(n) G\left(\frac{x}{n}\right)$, $\forall x \ge 1$.

Proof. i) $\Rightarrow$ ii). Suppose that $G(x) = \sum_{n \le x} F\left(\frac{x}{n}\right)$. Then we have

$$\sum_{n \le x} \mu(n) G\left(\frac{x}{n}\right) = \sum_{n \le x} \mu(n) \sum_{m \le \frac{x}{n}} F\left(\frac{x}{mn}\right) = \sum_{k \le x} F\left(\frac{x}{k}\right) \sum_{mn=k} \mu(n),$$

where we have rearraged the sum by putting together those m, n with the same product. By Proposition 2.4, we have

$$\sum_{mn=k} \mu(n) = \delta(k).$$

So we finally obtain that

$$\sum_{n \le x} \mu(n) G\left(\frac{x}{n}\right) = \sum_{k \le x} F\left(\frac{x}{k}\right) \delta(k) = F(x).$$

A similar argument gives ii) $\Rightarrow$ i), which is left as an exercise for readers. □

Corollary 2.8. *We have*

$$\sum_{n \le x} \mu(n) \left[\frac{x}{n}\right] = 1.$$

2.5 Applications

Theorem 2.9. *We have*

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n\prod_{p|n}\left(1 - \frac{1}{p}\right).$$

Hence by the Möbius inversion formula, we obtain the well-known fact that

$$\sum_{d|n} \varphi(d) = n.$$

Proof. The relation $\mu * \mathbb{1} = \delta$ provides a useful trick to deal with the condition $(m, n) = 1$:

$$\begin{aligned}\varphi(n) = \sum_{\substack{m=1\\(m,n)=1}}^{n} 1 = \sum_{m=1}^{n} \delta((m,n)) &= \sum_{m=1}^{n} \sum_{d|(m,n)} \mu(d)\\ &= \sum_{m=1}^{n} \sum_{\substack{d|m\\d|n}} \mu(d) = \sum_{d|n} \mu(d) \sum_{\substack{m=1\\d|m}}^{n} 1\\ &= \sum_{d|n} \mu(d)\frac{n}{d}.\end{aligned}$$

Since $\mu(n)/n$ is multiplicative, we have

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n}\frac{\mu(d)}{d} = n\prod_{p|n}\left(1 - \frac{1}{p}\right).$$

□

Remark. We provide an alternative way to derive the identity

$$\sum_{d|n} \varphi(d) = n.$$

Notice that each rational fraction in $(0, 1]$ with denominator n can be written in the form $h/n = a/d$ with $(a, d) = 1$. Thus

$$n = \sum_{1\le h\le n} 1 = \sum_{d|n} \sum_{\substack{1\le a\le d\\(a,d)=1}} 1 = \sum_{d|n} \varphi(d).$$

Theorem 2.10. *Let Λ be the Von Mangoldt function. Then we have*

$$\sum_{d|n} \Lambda(d) = \log n.$$

As a consequence,

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d.$$

Proof. Suppose that $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Note that $\Lambda(d) = \log p$ if d is a power of the prime p and $\Lambda(d) = 0$ otherwise. So

$$\sum_{d|n} \Lambda(d) = \sum_{j=1}^{k} \alpha_j \log p_j = \sum_{j=1}^{k} \log p_j^{\alpha_j} = \log n.$$

The second assertion follows from the Möbius inversion formula. □

Theorem 2.11. *Let $\mathbb{1}_\square$ denote the characteristic function of squares, i.e.*

$$\mathbb{1}_\square(n) = \begin{cases} 1, & n = k^2 \text{ for some } k \in \mathbb{N}^*, \\ 0, & \text{otherwise.} \end{cases}$$

Then we have $\mathbb{1}_\square = \lambda * \mathbb{1}$, where λ is the Liouville function. As a consequence, we have

$$\lambda(n) = \sum_{d|n} \mu(d) \mathbb{1}_\square \left(\frac{n}{d}\right).$$

Proof. Since $\lambda * \mathbb{1}$ is multiplicative, it suffices to consider the value of $\lambda * \mathbb{1}$ at each prime powers. By the definition of λ, we have

$$(\lambda * \mathbb{1})(p^\alpha) = \begin{cases} 1, & \alpha \text{ is even} \\ 0, & \alpha \text{ is odd.} \end{cases}$$

The desired result follows. □

We have defined the formal Dirichlet series in Section 2.3. We call

$$D(f; s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

the **Dirichlet series** associated with f if it is convergent. The Dirichlet series associated with $\mathbb{1}$ is called the **Riemann** ζ-function:

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

It is absolutely convergent for $\operatorname{Re} s > 1$.

Theorem 2.12. *For* $\operatorname{Re} s > 1$*, we have*

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

Hence $\zeta(s) \neq 0$ *for* $\operatorname{Re} s > 1$.

Proof. It follows from $\mu^{-1} = \mathbb{1}$ and $|\mu(n)| \leq 1$. □

Theorem 2.13. *For* $\operatorname{Re} s > 1$*, we have*

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

Proof. The series

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

is convergent uniformly in any compact subset of the set $\{s \in \mathbb{C} : \operatorname{Re} s > 1\}$. Thus we can take the derivative term by term. So we have

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

By Theorem 2.12 and Theorem 2.10,

$$-\frac{\zeta'(s)}{\zeta(s)} = \left(\sum_{n=1}^{\infty} \frac{\log n}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right) = \sum_{n=1}^{\infty} \frac{(\mu * \log)(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

□