CHAPTER 2

Arithmetic Functions

2.1. Examples

In this chapter, we discuss some basic arithmetic functions.

DEFINITION 2.1. A real or complex valued function defined on the positive integers (or all integers) is called an **arithmetic function** or a **number-theoretic function**.

We give some examples of arithmetic functions as follows and we will discuss their properties in the following sections.

EXAMPLE 2.2. We have the following simple but important arithmetic functions:

$$\text{The identity function } I(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise,} \end{cases}$$

$$\text{the unit function } u(n) \equiv 1, \quad n \geq 1,$$

$$N^s(n) = n^s, \quad n \geq 1,\ s \in \mathbb{C}.$$

DEFINITION 2.3. The divisor function $\tau(n)$ is defined as the number of positive divisors of n, i.e.,

$$\tau(n) = \sum_{d|n} 1. \tag{2.1}$$

DEFINITION 2.4. The divisor power sum function $\sigma_s(n)$ (with $s \in \mathbb{C}$) is defined as the sum of s power of all positive divisors of n, i.e.,

$$\sigma_s(n) = \sum_{d|n} d^s. \tag{2.2}$$

DEFINITION 2.5. The Euler totient function φ is defined as

$$\varphi(n) = \sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} 1.$$

DEFINITION 2.6. The Möbius function μ is defined as follows:

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ (-1)^r, & \text{if } n = p_1 p_2 \cdots p_r, \text{ with distint primes } p_i, \\ 0, & \text{otherwise.} \end{cases} \tag{2.3}$$

DEFINITION 2.7. The von Mangoldt function Λ is defined as follows:

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k,\ k \geq 1 \text{ and } p \text{ prime}, \\ 0, & \text{otherwise.} \end{cases} \tag{2.4}$$

DEFINITION 2.8. The omega function $\omega(n)$ is defined as the number of distinct prime factors of n, i.e.,

$$\omega(n) = r, \quad n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \text{ is the prime-power decomposition.} \tag{2.5}$$

DEFINITION 2.9. The Omega function $\Omega(n)$ is defined as the total number of prime factors of n, i.e.,

$$\Omega(n) = a_1 + a_2 + \cdots + a_r, \quad n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \text{ is the prime-power decomposition.} \tag{2.6}$$

DEFINITION 2.10. The Liouville function λ is defined as follows:

$$\lambda(n) = (-1)^{\Omega(n)}. \tag{2.7}$$

2.2. Multiplicative functions

An important class of arithmetic functions are multiplicative functions defined as follows.

DEFINITION 2.11. An arithmetic function f which is not identically zero is said to be **multiplicative** if

$$f(mn) = f(m)f(n) \tag{2.8}$$

whenever $(m, n) = 1$. Moreover, if (2.8) holds for all m, n, then f is called **completely multiplicative**.

We have the following property of all multiplicative functions

THEOREM 2.12. *If f is multiplicative then $f(1) = 1$.*

PROOF. Since f is not identically zero, there exists $n \in \mathbb{N}$ such that $f(n) \neq 0$. We have $f(n) = f(n)f(1)$ as f is multiplicative. Hence $f(1) = 1$. □

In this section, we will discuss some properties of some basic examples of multiplicative functions.

2.2.1. The divisor function τ.

THEOREM 2.13. *If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then*

$$\tau(n) = \prod_{i=1}^{r} (a_i + 1).$$

PROOF. By Corollary 1.8 we have

$$\tau(n) = \sum_{0 \leq c_1 \leq a_1} \sum_{0 \leq c_2 \leq a_2} \cdots \sum_{0 \leq c_r \leq a_r} 1 = \prod_{i=1}^{r} (a_i + 1). \qquad \square$$

As a simple consequence we have the following corollary.

COROLLARY 2.14. *The function τ is multiplicative.*

2.2.2. The divisor sum function σ.

THEOREM 2.15. *If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then*

$$\sigma_s(n) = \prod_{i=1}^{r} \frac{p_i^{(a_i+1)s} - 1}{p_i^s - 1}.$$

PROOF. By Corollary 1.8 we have

$$\sigma_s(n) = \sum_{0 \le c_1 \le a_1} \sum_{0 \le c_2 \le a_2} \cdots \sum_{0 \le c_r \le a_r} (p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r})^s$$
$$= \prod_{i=1}^{r} \sum_{0 \le c_i \le a_i} p_i^{c_i s} = \prod_{i=1}^{r} \frac{p_i^{(a_i+1)s} - 1}{p_i^s - 1}. \quad \square$$

As a simple consequence we have the following corollary.

THEOREM 2.16. *The function σ_s is multiplicative.*

We denote σ_1 by σ. We say $n \in \mathbb{N}$ is a **perfect number** if $\sigma(n) = 2n$, which means the number is equal to the sum of its proper divisors. For examples, 6 and 28. It was of great interest of the Greeks to determine all the perfect numbers. It was known as early as Euclid's time that every number of the form

$$n = 2^{p-1}(2^p - 1),$$

in which both p and $2^p - 1$ are prime, is perfect. Indeed we have

$$\sigma(n) = \frac{2^p - 1}{2 - 1} \cdot \frac{(2^p - 1)^2 - 1}{2^p - 1 - 1} = 2^p(2^p - 1) = 2n.$$

A partial converse of above holds: every even perfect number n is of the above type. To see this we put $n = 2^{k-1} \cdot n'$ such that $\sigma(n) = 2n$, where $k \ge 2$ and $2 \nmid n'$. Then we have

$$\sigma(n) = \sigma(2^{k-1})\sigma(n') = (2^k - 1)\sigma(n') = 2^k \cdot n'.$$

Since $(2^k - 1, 2) = 1$, we have $(2^k - 1) \mid n'$. Write $n' = (2^k - 1)n''$. Then we have $\sigma(n') = 2^k \cdot n''$. Note that

$$n'' + n' = 2^k n'' = \sigma(n').$$

Hence $n'' = 1$ and $n' = (2^k - 1)$ is prime. Note that if k is composite then $2^k - 1$ is also composite. Hence k is also prime. This proves the claim.

There are two open problems connected with perfect numbers. One is whether there are any odd perfect numbers. Various necessary conditions are known for an odd number to be perfect, which show that any such number must be extremely large, but no conclusive results have been obtained. The other question is about the primes p for which $2^p - 1$ is prime. These are Mersenne primes. They continue to occur, although with decreasing frequency, as far as computations have been pushed. There is no reason to suppose that there are only finitely many, but no proof that there are infinitely many.

2.2.3. The Möbius function μ. Note that $\mu(n) = 0$ if and only if n has a square factor > 1. Here is a short table of values of μ:

n:	1	2	3	4	5	6	7	8	9	10
$\mu(n)$:	1	-1	-1	0	-1	1	-1	0	0	1

It is easy to prove the following property of μ.

THEOREM 2.17. *The function μ is multiplicative.*

The Möbius function arises in many different places in number theory. One of its fundamental properties is a remarkably simple formula for the divisor sum $\sum_{d|n} \mu(d)$.

THEOREM 2.18. *If $n \geq 1$, then we have*

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

PROOF. If $n = 1$, then both sides are equal to 1. If $n > 1$, then we can write $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. By Corollary 1.8 and Theorem 2.17, we have

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{0 \leq c_1 \leq a_1} \sum_{0 \leq c_2 \leq a_2} \cdots \sum_{0 \leq c_r \leq a_r} \mu(p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}) \\ &= \sum_{0 \leq c_1 \leq 1} \sum_{0 \leq c_2 \leq 1} \cdots \sum_{0 \leq c_r \leq 1} \mu(p_1^{c_1}) \mu(p_2^{c_2}) \cdots \mu(p_r^{c_r}) \\ &= \prod_{i=1}^{r} \sum_{0 \leq c_i \leq 1} \mu(p_i^{c_i}) = \prod_{i=1}^{r} (1 - 1) = 0. \end{aligned}$$

This proves the theorem. □

THEOREM 2.19. *If $n \geq 1$, then we have*

$$\sum_{d^2|n} \mu(d) = |\mu|(n) = \mu(n)^2.$$

PROOF. If $n = 1$, then both sides are equal to 1. If $n > 1$, then we can write $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. By Corollary 1.8 and Theorem 2.17, we have

$$\begin{aligned} \sum_{d^2|n} \mu(d) &= \sum_{0 \leq c_1 \leq [\frac{a_1}{2}]} \sum_{0 \leq c_2 \leq [\frac{a_2}{2}]} \cdots \sum_{0 \leq c_r \leq [\frac{a_2}{2}]} \mu(p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}) \\ &= \sum_{0 \leq c_1 \leq [\frac{a_1}{2}]} \sum_{0 \leq c_2 \leq [\frac{a_2}{2}]} \cdots \sum_{0 \leq c_r \leq [\frac{a_2}{2}]} \mu(p_1^{c_1}) \mu(p_2^{c_2}) \cdots \mu(p_r^{c_r}) \\ &= \prod_{i=1}^{r} \sum_{0 \leq c_i \leq [\frac{a_i}{2}]} \mu(p_i^{c_i}). \end{aligned}$$

If there exists i such that $a_i \geq 2$ then $\sum_{0 \leq c_i \leq [\frac{a_i}{2}]} \mu(p_i^{c_i}) = 1 - 1 = 0$. Otherwise $a_i = 1$ for all i, and hence $\sum_{d^2|n} \mu(d) = |\mu|(n) = 1$. This proves the theorem. □

2.2.4. Euler's totient function φ. Note that $\varphi(p) = p - 1$ if p is prime. Here is a short table of values of φ:

n:	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$:	1	1	2	2	4	2	6	4	6	4

THEOREM 2.20. *If $n \geq 1$, then we have*

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

PROOF. By Theorem 2.18, we have

$$\varphi(n) = \sum_{\substack{1\leq k\leq n\\(k,n)=1}} 1 = \sum_{1\leq k\leq n} 1 \sum_{d|(n,k)} \mu(d).$$

Exchanging the order of the sums above, we get

$$\varphi(n) = \sum_{d|n} \mu(d) \sum_{\substack{1\leq k\leq n\\d|k}} 1 = \sum_{d|n} \mu(d)\frac{n}{d},$$

as claimed. □

THEOREM 2.21. *If $n \geq 1$, then we have*

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

PROOF. Assume $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. By Corollary 1.8 and Theorems 2.17 and 2.20, we have

$$\begin{aligned}
\varphi(n) &= n \sum_{d|n} \frac{\mu(d)}{d} = n \sum_{0\leq c_1\leq a_1} \sum_{0\leq c_2\leq a_2} \cdots \sum_{0\leq c_r\leq a_r} \frac{\mu(p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r})}{p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}} \\
&= n \sum_{0\leq c_1\leq 1} \sum_{0\leq c_2\leq 1} \cdots \sum_{0\leq c_r\leq 1} \frac{\mu(p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r})}{p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}} \\
&= \prod_{i=1}^{r} \sum_{0\leq c_i\leq 1} \frac{\mu(p_i^{c_i})}{p_i^{c_i}} = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).
\end{aligned}$$

□

THEOREM 2.22. *The function φ is multiplicative.*

PROOF. For any $m, n \in \mathbb{N}$ such that $(m, n) = 1$, we need to prove $\varphi(mn) = \varphi(m)\varphi(n)$. Assume $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$, with p_i, q_j are distinct primes and $a_i, b_j \in \mathbb{Z}_{\geq 0}$. By Theorem 2.21 we have

$$\varphi(mn) = mn \prod_{p|mn} \left(1 - \frac{1}{p}\right) = m \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) n \prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right) = \varphi(m)\varphi(n).$$

This completes the proof. □

THEOREM 2.23. *If $n \geq 1$, then we have*

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

PROOF. By Theorem 2.20 we have

$$\sum_{d|n}\varphi(d)=\sum_{d|n}\sum_{\ell|d}\mu(\ell)\frac{d}{\ell}=\sum_{d|n}\sum_{\ell|d}\mu\left(\frac{d}{\ell}\right)\ell=\sum_{\ell|n}\ell\sum_{\ell|d|n}\mu\left(\frac{d}{\ell}\right).$$

Making a change of variable $k=d/\ell$, we get

$$\sum_{d|n}\varphi(d)=\sum_{\ell|n}\ell\sum_{k|n/\ell}\mu\left(k\right).$$

By Theorem 2.18, we have

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

This completes the proof. □

2.3. Dirichlet convolution

2.3.1. Dirichlet convolution.

DEFINITION 2.24. Let f,g be two arithmetic functions. The **Dirichlet convolution** of f and g, denoted by $f*g$, is defined by

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

THEOREM 2.25. *Let f,g,h be three arithmetic functions. Then we have*

$$f*g=g*f\quad(\textit{commutative law}),$$

$$(f*g)*h=f*(g*h)\quad(\textit{associative law}).$$

PROOF. By definition, for any $n\geq 1$ we have

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

and

$$((f*g)*h)(n)=\sum_{mc=n}(f*g)(m)h(c)=\sum_{abc=n}f(a)g(b)h(c)=(f*(g*h))(n).\quad\square$$

In this notation, we have

$$I=\mu*u,\quad N=\varphi*u,\quad \varphi=\mu*N.$$

THEOREM 2.26. *For all f, we have $I*f=f*I=f$.*

PROOF. We have

$$(I*f)(n)=\sum_{d|n}f(d)I(n/d)=f(n).\qquad\square$$

2.3.2. Möbius transform.

DEFINITION 2.27. We define the **Möbius transform** of an arithmetic function f to be $F = f * u$, that is,

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

THEOREM 2.28 (Möbius inversion formula). *If $F = f * u$, then $f = F * \mu$. Conversely, if $f = F * \mu$, then $F = f * u$. We say f is the inverse Möbius transform of F.*

PROOF. If $F = f * u$, then by Theorem 2.18 and 2.26 we have $F * \mu = (f * u) * \mu = f * (u * \mu) = f * I = f$. Conversely, if $f = F * \mu$, then $f * u = F * \mu * u = F$. □

2.3.3. Dirichlet inverse.

THEOREM 2.29. *If f is an arithmetic function with $f(1) \neq 0$, then there is a unique arithmetic function f^{-1}, called the **Dirichlet inverse** of f, such that*

$$f * f^{-1} = f^{-1} * f = I.$$

Moreover, f^{-1} is given by the recursion formulas

$$f^{-1}(1) = \frac{1}{f(1)}, \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \quad \text{for } n > 1.$$

PROOF. It is clear that the function f^{-1} constructed above satisfies that $f * f^{-1} = f^{-1} * f = I$. So we prove the existence. Now we prove the uniqueness. Assume that g is a function such that $f * g = g * f = I$. Then we have $g = g * I = g * (f * f^{-1}) = (g * f) * f^{-1} = I * f^{-1} = f^{-1}$. This proves the theorem. □

REMARK 2.30. We have $(f * g)(1) = f(1)g(1)$. So if $f(1) \neq 0$, $g(1) \neq 0$, then $(f * g)(1) \neq 0$. The set of all arithmetic functions f with $f(1) \neq 0$ forms an abelian group with respect to the operation $*$. Since $(f^{-1} * g^{-1}) * (f * g) = I$, we get $(f * g)^{-1} = f^{-1} * g^{-1}$, if $f(1) \neq 0$, $g(1) \neq 0$.

EXAMPLE 2.31. Recall that $u * \mu = I$. We have $u^{-1} = \mu$ and $\mu^{-1} = u$.

THEOREM 2.32. *Let f be multiplicative. Then f is completely multiplicative if and only if*

$$f^{-1}(n) = \mu(n)f(n), \quad \text{for all } n \geq 1.$$

PROOF. If f is completely multiplicative, then we have

$$(\mu f * f)(n) = \sum_{ab=n} \mu(a)f(a)f(b) = f(n) \sum_{d|n} \mu(d) = I(n).$$

So $f^{-1} = \mu f$.

If $f^{-1} = \mu f$, then by Theorem 2.29 we have

$$f(n) = -\sum_{\substack{ab=n \\ a<n}} f^{-1}(b)\, f(a) = -\sum_{\substack{ab=n \\ a<n}} \mu(b) f(b)\, f(a), \quad \text{for } n > 1.$$

Let p be a prime and $k \geq 1$ be an integer. Then we have

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

Hence $f(p^k) = f(p)^k$. This shows that f is completely multiplicative. □

THEOREM 2.33. *We have* $\lambda^{-1} = |\mu|$.

PROOF. Note that λ is completely multiplicative. So we have $\lambda^{-1} = \mu\lambda$. Note that $\mu\lambda = |\mu|$. So we have $\lambda^{-1} = |\mu|$. □

THEOREM 2.34. *We have* $\varphi^{-1} = u * \mu N$.

PROOF. Note that we have $\varphi = \mu * N$. By Theorem 2.32 we have $N^{-1} = \mu N$. Hence $\varphi^{-1} = \mu^{-1} * N^{-1} = u * \mu N$. □

THEOREM 2.35. *We have* $\sigma_s^{-1} = \mu N^s * \mu$, *where* $N^s(n) = n^s$.

PROOF. Note that $\sigma_s = u * N^s$. By Theorem 2.32 we have $(N^s)^{-1} = \mu N^s$. Hence $\sigma^{-1} = u^{-1} * (N^s)^{-1} = \mu * \mu N^s$. □

2.3.4. Dirichlet convolution and multiplicative functions.

THEOREM 2.36. *If f and g are multiplicative, so is their Dirichlet convolution $f * g$.*

PROOF. By corollary 1.8, for any pair of positive integers m, n with $(m, n) = 1$, a divisor d of mn can be written uniquely as a product of a divisor d_1 of m and a divisor d_2 of n. So

$$(f * g)(mn) = \sum_{d|mn} f(d)g(mn/d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1d_2)g(mn/d_1d_2).$$

Note that $(d_1, d_2) = (m/d_1, n/d_2) = 1$. Since f and g are multiplicative, we have

$$(f * g)(mn) = \sum_{d_1|m} f(d_1)g(m/d_1) \sum_{d_2|n} f(d_2)g(n/d_2) = (f * g)(m)(f * g)(n).$$

So $f * g$ is multiplicative. □

THEOREM 2.37. *If both g and $f*g$ are multiplicative, then f is also multiplicative.*

PROOF. We should assume that f is not multiplicative and then find a contradiction. Assume that a pair of coprime positive integers (m, n) such that $f(mn) \neq f(m)f(n)$ and the product mn is smallest. Now we consider $(f * g)(mn)$. On the one hand, we have

$$(f * g)(mn) = \sum_{d|mn} f(d)g(mn/d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1d_2)g(mn/d_1d_2).$$

If $d_1d_2 < mn$ then we have $f(d_1d_2) = f(d_1)f(d_2)$. Since g is multiplicative, we get

$$(f * g)(mn) = \sum_{\substack{d_1|m \\ d_2|n \\ d_1d_2<mn}} f(d_1)f(d_2)g(m/d_1)g(n/d_2) + f(mn). \tag{2.9}$$

On the other hand, since $f*g$ is multiplicative, we have

$$(f*g)(mn) = (f*g)(m)(f*g)(n) = \sum_{d_1|m}\sum_{d_2|n} f(d_1)f(d_2)g(m/d_1)g(n/d_2)$$
$$= \sum_{\substack{d_1|m\\ d_2|n\\ d_1d_2<mn}} f(d_1)f(d_2)g(m/d_1)g(n/d_2) + f(m)f(n). \tag{2.10}$$

If $f(mn) \neq f(m)f(n)$, then (2.9) and (2.10) are contradicted to each other. □

COROLLARY 2.38. *If f is multiplicative, so is its Dirichlet inverse f^{-1}.*

PROOF. Since f and I are both multiplicative and $f*f^{-1} = I$. By Theorem 2.37, we conclude the proof. □

REMARK 2.39. These results together show that the set of multiplicative functions is a subgroup of the group of all arithmetic functions f with $f(1) \neq 0$.

THEOREM 2.40. *If f is multiplicative, then we have*

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n}(1-f(p)).$$

PROOF. Since μ and f are multiplicative, so is μf. Hence $g(n) = \sum_{d|n}\mu(d)f(d)$ is also multiplicative. Note that $h(n) = \prod_{p|n}(1-f(p))$ is multiplicative. So we only need to check $g(p^k) = h(p^k)$ for any prime p and integer $k \geq 1$. Indeed we have

$$g(p^k) = 1 - f(p) = h(p^k).$$

This completes the proof of Theorem 2.40. □

THEOREM 2.41. *We have $u*\lambda = \mathbb{1}_{\square}$, where*

$$\mathbb{1}_{\square}(n) = \begin{cases} 1, & \text{if } n \text{ is a square,} \\ 0, & \text{otherwise.} \end{cases}$$

PROOF. Note that both $u*\lambda$ and $\mathbb{1}_{\square}$ are multiplicative functions. We only need to check $(u*\lambda)(p^k) = \mathbb{1}_{\square}(p^k)$ for prime p and integer $k \geq 1$. If $2 \nmid k$, then we have

$$(u*\lambda)(p^k) = \sum_{d|p^k}\lambda(d) = \lambda(1)+\lambda(p)+\cdots+\lambda(p^k) = 1-1+1-\cdots-1 = 0.$$

So $\mathbb{1}_{\square}(p^k) = 0 = (u*\lambda)(p^k)$. If $2 \mid k$, then we have

$$(u*\lambda)(p^k) = \sum_{d|p^k}\lambda(d) = \lambda(1)+\lambda(p)+\cdots+\lambda(p^k) = 1-1+1-\cdots-1+1 = 1.$$

So $\mathbb{1}_{\square}(p^k) = 1 = (u*\lambda)(p^k)$. This proves the theorem. □

2.4. Generalized convolutions

In this section, F denotes a real or complex-valued function defined on the positive real axis $(0, +\infty)$ such that $F(x) = 0$ for $0 < x < 1$. Let g be an arithmetic function. Sums of the type

$$\sum_{n\le x} g(n)F\left(\frac{x}{n}\right)$$

arise frequently in number theory. The sum defines a new function H on $(0, +\infty)$ such that $G(x) = 0$ for $0 < x < 1$. We denote the function H by $g \circ F$, that is,

$$H(x) = (g \circ F)(x) = \sum_{n\le x} g(n)F\left(\frac{x}{n}\right).$$

If $F(x) = 0$ for all non-integer x, the restriction of F to the integers is an arithmetic function and we have

$$(g \circ F)(m) = (g * F)(m),$$

for all integers $m \ge 1$. So the operation $\circ$ can be regarded as a generalization fo the Dirichlet convolution $*$.

THEOREM 2.42. *For any arithmetic functions f and g, we have*

$$f \circ (g \circ H) = (f * g) \circ H.$$

PROOF. We have

$$\begin{aligned}(f \circ (g \circ H))(x) &= \sum_{a\le x} f(a)\left(\sum_{b\le x/a} g(b)H\left(\frac{x}{ab}\right)\right)\\ &= \sum_{n\le x}\left(\sum_{ab=n} f(a)g(b)\right)H\left(\frac{x}{n}\right) = ((f * g) \circ H)(x).\end{aligned}$$

This proves the theorem. □

THEOREM 2.43. *If g has a Dirichlet inverse g^{-1}, then the equation*

$$H(x) = \sum_{n\le x} g(n)F\left(\frac{x}{n}\right) \tag{2.11}$$

implies

$$F(x) = \sum_{n\le x} g^{-1}(n)H\left(\frac{x}{n}\right). \tag{2.12}$$

Conversely, (2.14) *implies* (2.13).

PROOF. If $H = g \circ F$, then by Theorem 2.42 we have

$$g^{-1} \circ H = g^{-1} \circ (g \circ F) = I \circ F = F.$$

Conversely, if $F = g^{-1} \circ H$, then we have $g \circ F = g \circ (g^{-1} \circ H) = I \circ H = H$. □

COROLLARY 2.44. *If g has a completely multiplicative function, then the equation*

$$H(x) = \sum_{n\le x} g(n)F\left(\frac{x}{n}\right) \tag{2.13}$$

if and only if

$$F(x) = \sum_{n \le x} \mu(n) g(n) H\left(\frac{x}{n}\right). \tag{2.14}$$

PROOF. By Theorem 2.32 we have $g^{-1} = \mu g$. □

2.5. The von Mangoldt function

The von Mangoldt function Λ plays a central role in the distribution of primes. Here is a table of values of $\Lambda(n)$:

n:	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$:	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0

THEOREM 2.45. *If $n \ge 1$ then we have*

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

That is, we have $\log = u * \Lambda$.

PROOF. If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then we have

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{r} \sum_{k=1}^{a_i} \Lambda(p_i^k) = \sum_{i=1}^{r} \sum_{k=1}^{a_i} \log p_i = \sum_{i=1}^{r} \log p_i^{a_i} = \log n$$

as claimed. □

THEOREM 2.46. *We have*

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

That is we have $\Lambda = \mu * \log = -u * \mu \log$.

PROOF. By Theorems 2.37 and 2.45, we have $\Lambda = \mu * \log$. Note that

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

Hence $\Lambda = -u * \mu \log$. This completes the proof. □

DEFINITION 2.47. For $k \ge 0$, the von Mangoldt function of degree k is defined as follows

$$\Lambda_k(n) = \sum_{d|n} \mu(d) \left(\log \frac{n}{d}\right)^k.$$

THEOREM 2.48 (Selberg's identity). *We have*

$$\Lambda_k = \Lambda_{k-1} \log + \Lambda_{k-1} * \Lambda.$$

PROOF. We have

$$\begin{aligned} \Lambda_k &= \mu * \log^k = (\mu * \log^{k-1}) \log - \mu \log * \log^{k-1} \\ &= \Lambda_{k-1} \log + (-\mu \log) * (\mu * u) * \log^{k-1} \\ &= \Lambda_{k-1} \log + \Lambda * \Lambda_{k-1}. \end{aligned}$$

This completes the proof. □

2.6. The Riemann zeta function and generating function

Let $s = \sigma + it \in \mathbb{C}$. For $\sigma > 1$, the Riemann zeta function $\zeta(s)$ is defined by the series

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

THEOREM 2.49 (Euler product). *For* $\mathrm{Re}(s) > 1$, *we have*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p=2}^{\infty} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

PROOF. By Taylor's series, we have

$$\prod_{p \le x} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p \le x} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right).$$

By Fundamental theorem of arithmetic, we have

$$\prod_{p \le x} \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{\substack{n \ge 1 \\ p|n \Rightarrow p \le x}} \frac{1}{n^s} =: \Sigma_1(x) + \Sigma_2(x),$$

where $\Sigma_1(x) = \sum_{n \le x} \frac{1}{n^s}$ and $\Sigma_2(x) = \sum_{p|n \Rightarrow p \le x}^{n > x} \frac{1}{n^s}$. Let $\sigma = \mathrm{Re}(s) > 1$. We have

$$\Sigma_2(x) \le \sum_{n > x} \frac{1}{n^\sigma} \le \int_x^\infty \frac{2}{u^\sigma} \mathrm{d}u \le \frac{2}{(1-\sigma)} \frac{1}{u^{\sigma-1}}\Big|_x^\infty = \frac{2}{(\sigma-1)x^{\sigma-1}}.$$

Hence $\lim_{x \to \infty} \Sigma_2(x) = 0$ and

$$\zeta(s) = \lim_{x \to \infty} \Sigma_1(x) = \lim_{x \to \infty} \prod_{p \le x} \left(1 - \frac{1}{p^s}\right)^{-1} - \lim_{x \to \infty} \Sigma_2(x) = \prod_{p \ge 2} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

This completes the proof. □

THEOREM 2.50. *We have* $\zeta(s) \neq 0$ *if* $\mathrm{Re}(s) > 1$, *and*

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \quad \mathrm{Re}(s) > 1.$$

PROOF. If $\mathrm{Re}(s) > 1$ then we have

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \le \sum_{n=1}^{\infty} \frac{1}{n^{\mathrm{Re}(s)}} < \infty.$$

By $u * \mu = I$, we have

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{m=1}^{\infty} \frac{1}{m^s} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{k=1}^{\infty} \frac{I(k)}{k^s} = 1, \quad \mathrm{Re}(s) > 1.$$

This completes the proof. □

COROLLARY 2.51. *We have*

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_{p=2}^{\infty} \left(1 - \frac{1}{p^s}\right),$$

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

PROOF. This follows from Theorems 2.49 and 2.50. □

THEOREM 2.52 (generating function of the divisor function). *We have*

$$\zeta^2(s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s},$$

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

PROOF. This follows from $\tau = u * u$. □

THEOREM 2.53 (generating function of the Euler totient function). *We have*

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

for $\mathrm{Re}(s) > 2$.

PROOF. This follows from $\varphi = \mu * N$. □

THEOREM 2.54 (generating function of the Mangoldt function). *We have*

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

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

PROOF. By the Euler product formula, we have

$$\log \zeta(s) = \log \sum_{n=1}^{\infty} \frac{1}{n^s} = \log \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1} = -\sum_{p} \log \left(1 - \frac{1}{p^s}\right).$$

Then by derivation on the both sides of the above equation, we get

$$\begin{aligned}
\frac{\zeta'(s)}{\zeta(s)} &= -\sum_{p} \frac{1}{\left(1 - \frac{1}{p^s}\right)} p^{-s} \log p \\
&= -\sum_{p} p^{-s} \log p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \\
&= -\sum_{p} \sum_{k=1}^{\infty} \frac{\log p}{p^{ks}} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.
\end{aligned}$$

Hence we have

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

□

2.7. Additive functions

DEFINITION 2.55. An arithmetic function f which is not identically zero is said to be **additive** if

$$f(mn) = f(m) + f(n) \tag{2.15}$$

whenever $(m, n) = 1$. Moreover, if (2.15) holds for all m, n, then f is called **completely additive**.

THEOREM 2.56. *The function ω is additive. The function Ω is completely additive.*

PROOF. Write $m = p_1^{a_1} \cdots p_r^{a_r}$ and $n = q_1^{b_1} \cdots q_s^{b_s}$ with prime p_i, q_j and positive integers a_i, b_j. We have $\Omega(mn) = \sum_i a_i + \sum_j b_j = \Omega(m) + \Omega(n)$. If $(m, n) = 1$, then $\omega(mn) = r + s = \omega(m) + \omega(n)$. □