9. Arithmetic functions

**Definition 9.1.** A function $f : \mathbb{N} \to \mathbb{C}$ is called an arithmetic function.

Some examples of arithmetic functions include:

1. the identity function
   $$I(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1; \end{cases}$$

2. the constant function $1(n) = 1$;

3. the divisor function, $d(n) = \#\{d \in \mathbb{N} : d \mid n\}$ (sometimes denoted $\tau(n)$);

4. the Euler totient function $\varphi(n) = \#\{a \in \mathbb{N} : a \leq n \text{ and } (a, n) = 1\}$;

5. the Möbius function,
   $$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n = p_1 \cdots p_r \text{ for distinct primes } p_i, \\ 0 & \text{otherwise}; \end{cases}$$

6. the von Mangoldt function $\Lambda(n)$;

7. the function $N(n) = n$.

**Definition 9.2.** Let $f, g$ be arithmetic functions. Then their *Dirichlet convolution* is the arithmetic function $f \ast g$ defined by

$$f \ast g(n) = \sum_{d \mid n} f(d)g(n/d).$$

For example we have $d = 1 \ast 1$. Let $\mathcal{A}$ denote the set of arithmetic functions. It is straightforward to see $\mathcal{A}$ is a commutative ring with respect to Dirichlet convolution (and the usual $+$), with identity element $I(n)$. In fact:

**Lemma 9.3.** $\mathcal{A}$ is an integral domain.

*Proof.* Exercise. (Show that $f \ast g = g \ast f$ and that $\mathcal{A}$ has no zero divisors.) \qed

**Lemma 9.4.** $\mu \ast 1 = I$.

*Proof.* We have $(\mu \ast 1)(1) = \mu(1) = 1$. Let $n > 1$ with $n = p_1^{a_1} \cdots p_r^{a_r}$ and $p_1 < \cdots < p_r$. Then

$$(\mu \ast 1)(n) = \sum_{d \mid n} \mu(d) = \sum_{J \subseteq \{1, \ldots, r\}} \mu \left( \prod_{j \in J} p_j \right) = \sum_J (-1)^{\#J} = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = (1 - 1)^r = 0.$$

This means that $\mu$ is the inverse of $1$ under Dirichlet convolution. As a simple corollary, we obtain:
Theorem 9.5 (Möbius inversion). Let $f \in \mathcal{A}$ and define $g(n) = \sum_{d|n} f(d)$. Then

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

Proof. We have $g = f \ast 1$ if and only if $f = g \ast \mu$. \qed

Definition 9.6. An arithmetic function $f$ has at most polynomial growth if there exists $\sigma \in \mathbb{R}$ such that $f(n) = O(n^{\sigma})$.

Let us denote by $\mathcal{A}^\text{poly}$ the set of $f \in \mathcal{A}$ of at most polynomial growth. Then one can show that $\mathcal{A}^\text{poly}$ is a subring of $\mathcal{A}$ (exercise). For $f \in \mathcal{A}^\text{poly}$, the associated Dirichlet series $\sum_{n=1}^{\infty} f(n)n^{-s}$ defines an analytic function on some half plane $\Re(s) > \sigma + 1$. This turns out to be a very useful device for understanding the ring structure of $\mathcal{A}^\text{poly}$:

Theorem 9.7. Let $f, g \in \mathcal{A}^\text{poly}$. Then

$$\sum_{n=1}^{\infty} \frac{f \ast g(n)}{n^s} = \left( \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \right) \left( \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \right).$$

Proof. Expanding the right-hand side, we obtain

$$\sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{f(m)g(n)}{(mn)^s} = \sum_{r=1}^{\infty} \sum_{mn=r} \frac{f(m)g(n)}{r^s} = \sum_{r=1}^{\infty} \frac{f \ast g(r)}{r^s},$$

which is the left-hand side. \qed

In other words, the map $f \mapsto \sum_{n=1}^{\infty} f(n)n^{-s}$ is a ring homomorphism from $\mathcal{A}^\text{poly}$ to the ring of functions that are analytic on a right half plane, and in fact this map is injective (exercise).

We have

$$\sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \sum_{n=1}^{\infty} \frac{(1 \ast 1)(n)}{n^s} = \zeta(s)^2.$$

Definition 9.8. An arithmetic function $f$ is multiplicative (resp. completely multiplicative) if $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$ (resp. for all $m,n$).

If $f \in \mathcal{A}^\text{poly}$ is multiplicative and non zero then, generalising the proof of the Euler product formula for $\zeta$, one finds that

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

If $f$ is completely multiplicative then the inner series is geometric, so that

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p} \frac{1}{1 - f(p)p^{-s}}.$$

Example. $\mu$ is multiplicative. Thus

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

for $\Re(s) > 1$. 

37
Lemma 9.9. If \( f, g \in \mathcal{A} \) are multiplicative then \( f \ast g \) is multiplicative.

Proof. Let \((m, n) = 1\). Then
\[
(f \ast g)(mn) = \sum_{d | mn} f(d)g(mn/d) = \sum_{d_1 | m} \sum_{d_2 | n} f(d_1d_2)g\left(\frac{mn}{d_1d_2}\right),
\]
where
\[
d_1 = \prod_{p | m, p \parallel d} p^r \quad \text{and} \quad d_2 = \prod_{p' | n, p' \parallel d} p'^r.
\]
(Here \(p \parallel d\) means \(p | d\) but \(p + 1 \nmid d\).) But then it follows from multiplicativity that
\[
(f \ast g)(mn) = \sum_{d_1 | m} \sum_{d_2 | n} f(d_1)d_1g\left(\frac{n}{d_2}\right) = (f \ast g)(m)(f \ast g)(n).
\]
\[\square\]

Remark. If \( f \in \mathcal{A} \) is not the zero function and \( f \) is multiplicative then \( f(1) = 1 \). Indeed, we have
\[
f(n) = f(n \cdot 1) = f(n)f(1).
\]

There are lots of identities between elements of \( \mathcal{A} \):

Lemma 9.10. \( \varphi = \mu \ast N \) where \( N(n) = n \).

Proof. We have
\[
\varphi(n) = \sum_{a \leq n \atop (a, n) = 1} 1 = \sum_{a \leq n} \sum_{d | (a, n)} \mu(d) = \sum_{a \leq n} \sum_{d | a} \mu(d),
\]
since \( \mu \ast 1 = I \). Switching the order of summation we get
\[
\varphi(n) = \sum_{d | n} \mu(d) \sum_{a \leq n, d | a} 1 = \sum_{d | n} \mu(d) \frac{n}{d} = (\mu \ast N)(n).
\]
\[\square\]

It follows from this result that \( \varphi \) is multiplicative (since both \( \mu \) and \( N \) are). If \( n = p^r \) is a prime power then
\[
\varphi(p^r) = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right).
\]
Hence it follows that
\[
\varphi(n) = n \prod_{p | n} \left(1 - \frac{1}{p}\right).
\]
Applying Möbius inversion to \( \varphi = \mu \ast N \) we deduce that \( \varphi \ast 1 = N \); i.e.
\[
\sum_{d | n} \varphi(d) = n
\]
for any \( n \in \mathbb{N} \).

Since \( \varphi = \mu \ast N \), we can easily calculate the Dirichlet series associated to the Euler totient function as
\[
\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{(\mu \ast N)(n)}{n^s} = \left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{1}{n^s-1}\right) = \zeta(s-1) / \zeta(s).
\]
In particular we have $\sigma_a = \sigma_c = 2$ for this Dirichlet series.

**Lemma 9.11.** $\Lambda \ast 1 = \log$.

**Proof.** Recall that $\Lambda(1) = 0$ and

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \\ 0 & \text{otherwise}. \end{cases}$$

Write $n = p_1^{a_1} \ldots p_r^{a_r}$. Then

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

Next we claim that

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

This obviously true for $n = 1$. For $n > 1$, Möbius inversion gives

$$\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d) = \sum_{d|n} \mu(d) (\log n - \log d) = - \sum_{d|n} \mu(d) \log d,$$

as required, since $\mu \ast 1 = I$.

More examples of arithmetic functions:

1. If $n = p_1^{a_1} \ldots p_r^{a_r}$ with $p_1 < \cdots < p_r$ then $\omega(n) = r$ and $\Omega(n) = a_1 + \cdots + a_r$.

2. The sum of divisors function is $\sigma_s(n) = \sum_{d|n} d^s$ for $s \in \mathbb{R}$. (Note that $d = \sigma_0$ and one usually writes $\sigma$ for $\sigma_1$.)

Returning to the divisor function, we have already seen that $d = 1 \ast 1$. Hence Lemma 9.9 implies that $d(n)$ is a multiplicative arithmetic function. It is not completely multiplicative (why?). It is easy to see that $2^{\omega(n)} \leq d(n) \leq 2^{\Omega(n)}$ (exercise).

Arithmetic functions can be quite erratically behaved and in the next section we will study their behaviour on average. By multiplicativity we have $d(n) = (a_1 + 1) \ldots (a_r + 1)$ if $n = p_1^{a_1} \ldots p_r^{a_r}$. In particular $d(p) = 2$ for all primes $p$, but sometimes $d(n)$ can be much bigger:

**Lemma 9.12.** Let $k \in \mathbb{N}$. Then $d(n) \geq (\log n)^k$ for infinitely many $n \in \mathbb{N}$.

**Proof.** Let $p_1 = 2, p_2 = 3, \ldots, p_{k+1}$ be the first $k + 1$ primes. Put $n = (p_1 p_2 \ldots p_{k+1})^m$. Then

$$d(n) = (m + 1)^{k+1} > m^{k+1} = \left( \frac{\log n}{\log p_1 p_2 \ldots p_{k+1}} \right)^{k+1} \geq (\log n)^k,$$

if $\log n \geq (\log p_1 p_2 \ldots p_{k+1})^{k+1}$. Thus, providing that $m \geq (\log p_1 p_2 \ldots p_{k+1})^k$, we have $d(n) \geq (\log n)^k$. \hfill \Box

On the other hand $d(n)$ can’t be too big. The following result shows, in particular, that the divisor function belongs to $\mathcal{A}^{\text{poly}}$.

**Lemma 9.13.** We have $d(n) = O_\varepsilon(n^\varepsilon)$ for any $\varepsilon > 0$. 

39
Proof. Given $\varepsilon > 0$, we have to show that there is a positive constant $C(\varepsilon)$ such that $d(n) \leq C(\varepsilon)n^{\varepsilon}$ for every $n \in \mathbb{N}$. By multiplicativity we have

$$
\frac{d(n)}{n^{\varepsilon}} = \prod_{p^a \mid n} \frac{a + 1}{p^{\varepsilon a}}.
$$

We decompose the product into two parts according to whether $p < 2^{1/\varepsilon}$ or $p \geq 2^{1/\varepsilon}$. In the second part $p^a \geq 2$, so that

$$
\frac{a + 1}{p^{\varepsilon a}} \leq \frac{a + 1}{2^a} \leq 1.
$$

Thus we must estimate the first part. Notice that

$$
\frac{a + 1}{p^{\varepsilon a}} \leq 1 + \frac{a}{p^{\varepsilon a}} \leq 1 + \frac{1}{\varepsilon \log 2},
$$

since $a \varepsilon \log 2 \leq e^{a \varepsilon \log 2} = 2^{a \varepsilon} \leq p^{a \varepsilon}$. Hence

$$
\prod_{p < 2^{1/\varepsilon}} \left( 1 + \frac{1}{\varepsilon \log 2} \right) = C(\varepsilon).
$$

□