13. Arithmetic functions

13.1 Arithmetic functions

In the previous lectures, we have witnessed functions like the “sum-of-squares” functions $r_k(n)$ that are defined on the positive integers. Such functions are of particular interest in the study of number theory.

Definition 13.1 An *arithmetic function* is a complex-valued function that is defined on the positive integers.

R In G. H. Hardy and E. M. Wright’s *Introduction*, they also include in their definition the requirement that an arithmetical function “expresses some arithmetical property of n.”

Recall that we have also encountered multiplicative functions such as Euler’s totient function $\phi(n)$.

Definition 13.2 An arithmetic function f is

(i) *multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all positive integers m and n with $(m,n) = 1$;

(ii) *completely multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all positive integers m and n.

Analogously, we may replace the above multiplicative condtion with an additive condition.

Definition 13.3 An arithmetic function f is

(i) *additive* if $f(mn) = f(m) + f(n)$ for all positive integers m and n with $(m,n) = 1$;

(ii) *completely additive* if $f(mn) = f(m) + f(n)$ for all positive integers m and n.

We list here several simple but important arithmetic functions:

- the *constant function* $\mathbf{1}(n)$, defined by $\mathbf{1}(n) = 1$ for all n — *completely multiplicative*;
- the *identity function* $\mathrm{id}(n)$, defined by $\mathrm{id}(n) = n$ for all n — *completely multiplicative*;
- the *unit function* $\varepsilon(n)$, defined by $\varepsilon(n) = 1$ if $n = 1$, and 0 otherwise — *completely multiplicative*;
- the function $\Omega(n)$, defined by the total number of prime factors of n (e.g. $\Omega(1) = 0$, $\Omega(2) = 1$, $\Omega(4) = 2$, $\Omega(6) = 2$, $\Omega(12) = 3$, etc.) — *completely additive*;

▷ the function $\omega(n)$, defined by the number of distinct prime factors of n (e.g. $\omega(1)=0$, $\omega(2)=1$, $\omega(4)=1$, $\omega(6)=2$, $\omega(12)=2$, etc.) — *additive*.

13.2 Divisor functions

Definition 13.4 For real or complex s, the *divisor functions* are defined $\sigma_s(n)$ by

$$\sigma_s(n) := \sum_{d|n} d^s,$$

where the summation runs over all positive divisors of n. In particular, we define

$$d(n) = \sigma_0(n) = \sum_{d|n} 1 \qquad \text{and} \qquad \sigma(n) = \sigma_1(n) = \sum_{d|n} d.$$

Theorem 13.1 Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be in the canonical form. Then

$$d(n) = \prod_{k=1}^{r} (a_k + 1) \tag{13.1}$$

and for $s \neq 0$,

$$\sigma_s(n) = \prod_{k=1}^{r} \frac{p_k^{(a_k+1)s} - 1}{p_k^s - 1}. \tag{13.2}$$

Proof. Noting that all divisors of n are of the form $p_1^{\beta_1} \cdots p_r^{\beta_r}$ with $0 \leq \beta_k \leq \alpha_k$ for all k, we have

$$\sigma_s(n) = \sum_{d|n} d^s = \sum_{\beta_1=0}^{\alpha_1} \cdots \sum_{\beta_r=0}^{\alpha_r} \left(p_1^{\beta_1} \cdots p_r^{\beta_r}\right)^s = \prod_{k=1}^{r} \left(1 + p_k^s + p_k^{2s} + \cdots + p_k^{\alpha_k s}\right).$$

We further get (13.1) and (13.2) by using the fact that $1 + p^s + \cdots + p^{\alpha s}$ equals $\alpha + 1$ if $s = 0$, and $\frac{p^{(\alpha+1)s}-1}{p-1}$ if $s \neq 0$. ■

Corollary 13.2 For any s, the divisor function $\sigma_s(n)$ is multiplicative.

Proof. This is a direct implication of Theorem 13.1. ■

13.3 Möbius function

Recall that $\omega(n)$ counts by the number of distinct prime factors of n.

Definition 13.5 An positive integer n is *squarefree* if no squares other than 1 divide n; otherwise, we say n is *squareful*.

▪ **Example 13.1** The first several squarefree integers are $1, 2, 3, 5, 6, 7, 10, 11, \ldots$ and the first several squareful integers are $4, 8, 9, 12, 16, 18, 20, 24 \ldots$ ▪

Definition 13.6 The *Möbius function* $\mu(n)$ is defined by

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

R The Möbius function was introduced by the German mathematician August Ferdinand Möbius (*J. Reine Angew. Math.* **9** (1832), 105–123).

Example 13.2 We have $\mu(1)=1$, $\mu(2)=-1$, $\mu(3)=-1$, $\mu(4)=0$, $\mu(5)=-1$, $\mu(6)=1$, etc.

Theorem 13.3 The Möbius function $\mu(n)$ is multiplicative.

Proof. First, we have $\mu(1)=1$. Let us assume that m and n are such that $(m,n)=1$. If one of m and n is squareful, so is mn, and hence $\mu(mn)=0=\mu(m)\mu(n)$. Further, $\mu(mn)=(-1)^{\omega(mn)}=(-1)^{\omega(m)+\omega(n)}=\mu(m)\mu(n)$ since $\omega(n)$ is additive. ■

Theorem 13.4 For $n\geq 1$,

$$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{if } n=1,\\ 0 & \text{if } n>1.\end{cases} \tag{13.3}$$

Proof. The formula is trivial when $n=1$. For $n>1$, we write n in the canonical form $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$. Note that if suffices to consider squarefree divisors d of n in the sum $\sum_{d|n}\mu(d)$. We have

$$\begin{aligned}\sum_{d|n}\mu(d)&=\mu(1)+\mu(p_1)+\cdots+\mu(p_r)+\mu(p_1p_2)+\cdots+\mu(p_{r-1}p_r)+\cdots+\mu(p_1\cdots p_r)\\ &=\binom{r}{0}-\binom{r}{1}+\binom{r}{2}+\cdots+(-1)^r\binom{r}{r}=(1-1)^r=0,\end{aligned}$$

as required. ■

R Recalling the definition of the unit function ε, i.e., $\varepsilon(n)=1$ if $n=1$, and 0 otherwise, we have

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

13.4 Euler's totient function revisited

Recall that Euler's totient function $\phi(n)$ was well studied in Sect. 4.2 and later lectures. In particular, we know that $\phi(n)$ is multiplicative. Also, we have shown in Theorem 4.5 that

$$\sum_{d|n}\phi(d)=n. \tag{13.4}$$

Now, we establish a formula connecting Euler's totient function and the Möbius function.

Theorem 13.5 For $n\geq 1$,

$$\phi(n)=\sum_{d|n}\mu(d)\frac{n}{d}. \tag{13.5}$$

Proof. By the definition of $\phi(n)$, we have, with (13.3) applied, that

$$\phi(n) = \sum_{k=1}^{n} \varepsilon\big((k,n)\big) = \sum_{k=1}^{n} \sum_{d|(k,n)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|k \\ d|n}} \mu(d) = \sum_{d|n} \sum_{\substack{k=1 \\ d|k}}^{n} \mu(d) = \sum_{d|n} \mu(d) \frac{n}{d},$$

as required. ■

13.5 Mangoldt function

In this part, we introduct the Mangoldt function $\Lambda(n)$ which plays a crucial role in the distribution of primes.

Definition 13.7 The *Mangoldt function* $\Lambda(n)$ is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^\alpha \text{ with } p \text{ a prime and } \alpha \text{ a positive integer,} \\ 0 & \text{otherwise.} \end{cases}$$

R The Mangoldt function is named after the German mathematician Hans von Mangoldt.

Example 13.3 We have $\Lambda(1) = 0$, $\Lambda(2) = \log 2$, $\Lambda(3) = \log 3$, $\Lambda(4) = \log 2$, $\Lambda(5) = \log 5$, $\Lambda(6) = 0$, etc.

R The Mangoldt function $\Lambda(n)$ is neither multiplicative nor additive, for $\Lambda(6) \neq \Lambda(2)\Lambda(3)$ and $\Lambda(6) \neq \Lambda(2) + \Lambda(3)$.

Theorem 13.6 For $n \geq 1$,

$$\log n = \sum_{d|n} \Lambda(d). \tag{13.6}$$

Proof. The formula is trivial when $n = 1$. For $n > 1$, we write n in the canonical form $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Then

$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^{r} \left(\Lambda(p_k) + \Lambda(p_k^2) + \cdots + \Lambda(p_k^{\alpha_k})\right) = \sum_{k=1}^{r} \alpha_k \log p_k = \sum_{k=1}^{r} \log p_k^{\alpha_k} = \log n,$$

as deseried. ■

Theorem 13.7 For $n \geq 1$,

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d. \tag{13.7}$$

Proof. The formula is trivial when $n = 1$. Also, if $n = p^\alpha$ with p a prime and α a positive integer, we have

$$-\sum_{d|p^\alpha} \mu(d) \log d = -\mu(1) \log 1 - \mu(p) \log p = \log p = \Lambda(p^\alpha).$$

Now, we assume that n is written in the canonical form $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with $r \geq 2$. Then

$$-\sum_{d|n} \mu(d) \log d = \sum_{1 \leq i \leq r} \log p_i - \sum_{1 \leq i < j \leq r} \log p_i p_j$$

$$+ \sum_{1 \le i < j < k \le r} \log p_i p_j p_k - \cdots + (-1)^{r-1} \log p_1 p_2 \cdots p_r.$$

Note that $\log xy = \log x + \log y$. We find that in the summation $\sum_{1 \le i \le r} \log p_i$, each $\log p_\ell$ appears $1 = \binom{r-1}{0}$ time; in the summation $\sum_{1 \le i < j \le r} \log p_i p_j$, each $\log p_\ell$ appears $r - 1 = \binom{r-1}{1}$ times; in the summation $\sum_{1 \le i < j \le r} \log p_i p_j$, each $\log p_\ell$ appears $\binom{r-1}{2}$ times, etc. Hence,

$$\begin{aligned} -\sum_{d \mid n} \mu(d) \log d &= \sum_{\ell=1}^{r} \left(\binom{r-1}{0} - \binom{r-1}{1} + \binom{r-1}{2} - \cdots + (-1)^{r-1} \binom{r-1}{r-1} \right) \log p_\ell \\ &= \sum_{\ell=1}^{r} (1-1)^{r-1} \log p_\ell = 0. \end{aligned}$$

However, for $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with $r \ge 2$, we also have $\Lambda(n) = 0$ by definition. The desired identity holds true. ∎

Corollary 13.8 For $n \ge 1$,

$$\Lambda(n) = \sum_{d \mid n} \mu(d) \log \frac{n}{d}. \tag{13.8}$$

Proof. Note that

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

Since $(\log n) \sum_{d \mid n} \mu(d) = 0$ for $n \ge 1$ by (13.3), we arrive at the required result by recalling (13.7). ∎