3. Arithmetic functions

3.1. **Arithmetic functions.** These are functions $f : \mathbb{N} \to \mathbb{N}$ or $\mathbb{Z}$ or maybe $\mathbb{C}$, usually having some arithmetic significance. An important subclass of such functions are the multiplicative functions: such an f is *multiplicative* if

$$f(nn') = f(n)f(n')$$

for all $n, n' \in \mathbb{N}$ with n and n' coprime ($\gcd(n, n') = 1$).

Proposition 3.1. *If f is multiplicative and $n_1, \dots, n_k$ are pairwise coprime ($\gcd(n_i, n_j) = 1$ for all $i \neq j$) then*

$$f(n_1 n_2 \dots n_k) = f(n_1)f(n_2)\dots f(n_k).$$

This is readily proved by induction.

Corollary 3.2. *If n factorises into distinct prime powers as $n = p_1^{e_1} \dots p_k^{e_k}$ then*

$$f(n) = f(p_1^{e_1}) \dots f(p_k^{e_k}).$$

So multiplicative functions are completely determined by their values on prime powers. Some examples of multiplicative functions are

- The '1-detecting' function $\Delta(n)$, equal to 1 at $n = 1$ and 0 elsewhere – obviously multiplicative;
- $\tau(n) = \sum_{d|n} 1$, the number of divisors of n;
- $\sigma(n) = \sum_{d|n} d$, the sum of the divisors of n.

Proposition 3.3. *The functions $\tau(n)$ and $\sigma(n)$ are both multiplicative.*

Proof. Take n and n' coprime, with $\ell_1, \dots, \ell_{\tau(n)}$ the divisors of n, and $\ell'_1, \dots, \ell'_{\tau(n')}$ the divisors of n'. Then all the $\tau(n)\tau(n')$ numbers $\ell_i \ell'_j$ are all divisors of nn'. Conversely, if m divides nn' then $m = \ell\ell'$, where $\ell \mid n$ and $\ell' \mid n'$. (Write m as a product of prime powers, and then ℓ will be the product of the prime powers where the prime divides n, while ℓ' will be the product of the prime powers where the prime divides n'. Note that n and n', being coprime, have no prime factors in common.) So ℓ is some ℓ_i and ℓ' is some ℓ'_j, so all factors of nn' are of the form $\ell_i \ell'_j$. Thus $\tau(nn') = \tau(n)\tau(n')$, and

$$\sigma(nn') = \sum_{i,j} \ell_i \ell'_j = \left(\sum_i \ell_j\right)\left(\sum_j \ell'_j\right) = \sigma(n)\sigma(n').$$

□

Given an arithmetic function f, define its 'sum over divisors' function $F(n) = \sum_{d|n} f(d)$.

Proposition 3.4. *If f is multiplicative, and $n = \prod_p p^{e_p}$ then*

$$F(n) = \prod_{p|n} \left(1 + f(p) + f(p^2) + \dots + f(p^{e_p})\right). \tag{1}$$

Further, F is also multiplicative.

Proof. Expanding the RHS of (1), a typical term is $\prod_{p|n} f(p^{e'_p})$, where $0 \le e'_p \le e_p$. But, by the multiplicivity of f, this is simply $f(d)$, where $d = \prod_{d|n} p^{e'_p}$ is a divisor of n. Conversely, every divisor of n is of this form, for some choice of exponents e'_p. Hence the RHS of (1) is equal to $\sum_{d|n} f(d)$, which is $F(n)$.

Next, taking n and n' coprime, we see that (1) immediately implies that $F(n)F(n') = F(nn')$, i.e., that F is multiplicative. □

Proposition 3.5. *Euler's φ-function $\varphi(m)$ is multiplicative.*

Proof. Take n and n' coprime, and let

$$\{i : 1 \le i \le n, \gcd(i,n) = 1\} = \{a_1 < a_2 < \cdots < a_{\varphi(n)}\},$$

the *reduced residue classes* $\bmod n$. Similarly, let

$$\{j : 1 \le j \le n', \gcd(j,n') = 1\} = \{a'_1 < a'_2 < \cdots < a'_{\varphi(n')}\}.$$

If $x \in \{1, 2, \ldots, nn'\}$ and $\gcd(x, nn') = 1$ then certainly $\gcd(x,n) = \gcd(x,n') = 1$, so that

$$x \equiv a_i \pmod{n} \qquad x \equiv a'_j \pmod{n'} \tag{2}$$

for some pair a_i, a'_j. Conversely, given such a pair a_i, a'_j we can solve (2) using the CRT to get a solution $x \in \{1, 2, \ldots, nn'\}$ with $\gcd(x, nn') = 1$. Thus we have a bijection between such x and such pairs a_i, a'_j. Hence

$$\#\{\text{such } x\} = \varphi(nn') = \#\{a_i, a'_j\} = \varphi(n)\varphi(n').$$

□

In passing, mention

Proposition 3.6 (Euler's Theorem)**.** *If $a, n \in \mathbb{N}$ and $\gcd(a,n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Proof. This is because the reduced residue classes $\bmod n$ form a multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ of size(order) $\varphi(n)$. So, in this group, $a^{\varphi(n)} = 1$. □

Note that on putting $n = p$ prime we retrieve Fermat's Little Theorem $a^{p-1} \equiv 1 \pmod{p}$.

[In fact the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is usually smaller than $\varphi(n)$. To give the exponent, we need to define a new function ψ on prime powers by $\psi = \varphi$ on odd prime powers, and at 2 and 4, while $\psi(2^e) = \frac{1}{2}\varphi(2^e)$ if $e \ge 3$. Then the exponent of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\mathrm{lcm}_{p:p^{e_p}||n} \psi(p^{e_p})$. This follows from the isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{p:p^{e_p}||n} (\mathbb{Z}/p^{e_p}\mathbb{Z})^\times$$

and the fact that $(\mathbb{Z}/p^{e_p}\mathbb{Z})^\times$ has exponent $\psi(p^{e_p})$.]

Proposition 3.7. *We have $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$.*

Proof. Now $\varphi(p^k) = p^k - p^{k-1}$ (why?), which $= p^k \left(1 - \frac{1}{p}\right)$, so the result follows from Corollary 3.2. □

The *Möbius function* $\mu(n)$ is defined as

$$\mu(n) = \begin{cases} 0 \text{ if } p^2 \mid n \text{ for some prime } p; \\ (-1)^k \text{ if } n = p_1 p_2 \dots p_k \text{ for distinct primes } p_i. \end{cases}$$

In particular, $\mu(1) = 1$ and $\mu(p) = -1$ for a prime p. It is immediate from the definition that μ is multiplicative. Then, applying (1), we see that $\sum_{d|n} \mu(d) = \Delta(n)$.

Integers with $\mu(n) = \pm 1$ are called *squarefree*.

The Möbius function arises in many kinds of *inversion* formulae. The fundamental one is the following.

Proposition 3.8 (Möbius inversion)**.** *If* $F(n) = \sum_{d|n} f(d) \quad (n \in \mathbb{N})$ *then for all* $n \in \mathbb{N}$ *we have* $f(n) = \sum_{d|n} \mu(n/d) F(d)$.

Proof. Simplify $\sum_{d|n} \mu(n/d) F(d) = \sum_{d|n} \mu(n/d) \sum_{k|d} f(k) \quad (n \in \mathbb{N})$ by interchanging the order of summation to make $\sum_{k|n}$ the outer sum. But a simpler proof is given below. □

3.2. **Dirichlet series.** For an arithmetic function f, define its *Dirichlet series* $D_f(s)$ by

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

Here $s \in \mathbb{C}$ is a parameter. Typically, such series converge for $\Re s > 1$, and can be meromorphically continued to the whole complex plane. However, we will not be concerned with analytic properties of Dirichlet series here, but will regard them only as generating functions for arithmetic functions, and will manipulate them formally, without regard to convergence.

The most important example is for $f(n) = 1 \quad (n \in \mathbb{N})$, which gives the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Also, taking $f(n) = n \quad (n \in \mathbb{N})$ gives $\zeta(s-1)$. (Check!).

Proposition 3.9. *If* f *is multiplicative then*

$$D_f(s) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots + \frac{f(p^k)}{p^{ks}} + \dots \right) = \prod_p D_{f,p}(s), \tag{3}$$

say.

Proof. Expanding the RHS of (3), a typical term is

$$\frac{f(p_1^{e_1}) f(p_2^{e_2}) \dots f(p_r^{e_r})}{p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}} = \frac{f(n)}{n^s}$$

for $n = \prod_{i=1}^r p_i^{e_i}$, using the fact that f is multiplicative. □

Such a product formula $D_f(s) = \prod_p D_{f,p}(s)$ over all primes p is called an *Euler product* for $D_f(s)$.

For example

$$\zeta(s) = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots + \frac{1}{p^{ks}} + \dots \right) = \prod_p \left(\frac{1}{1 - p^{-s}} \right),$$

on summing the Geometric Progression (GP). Hence also

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

on expanding out the product.

Proposition 3.10. *We have*

$$\left(\sum_k \frac{a_k}{k^s}\right) \cdot \left(\sum_\ell \frac{b_\ell}{\ell^s}\right) = \left(\sum_n \frac{c_n}{n^s}\right),$$

where $c_n = \sum_{k|n} a_k b_{n/k}$.

Proof. On multiplying out the LHS, a typical term is

$$\frac{a_k}{k^s} \cdot \frac{b_\ell}{\ell^s} = \frac{a_k b_{n/k}}{n^s},$$

where $k\ell = n$. So all pairs k, ℓ with $k\ell = n$ contribute to the numerator of the term with denominator n^s. □

Corollary 3.11. *We have* $D_F(s) = D_f(s)\zeta(s)$.

Proof. Apply the Proposition with $a_k = f(k)$ and $b_\ell = 1$. □

Corollary 3.12 (Möbius inversion again)**.** *We have* $f(n) = \sum_{d|n} \mu(n/d)F(d)$ *for all* $n \in \mathbb{N}$.

Proof. From Corollary 3.11 we have

$$D_f(s) = D_F(s) \cdot \frac{1}{\zeta(s)} = \left(\sum_k \frac{F(k)}{k^s}\right) \cdot \left(\sum_\ell \frac{\mu(\ell)}{\ell^s}\right) = \left(\sum_n \frac{c_n}{n^s}\right),$$

where $c_n = \sum_{k|n} F(k)\mu(n/k)$. But $D_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$, so, on comparing coefficients, $f(n) = \sum_{k|n} F(k)\mu(n/k)$. □

We now compute the Dirichlet series for a few standard functions. [Part (a) is already proved above.]

Proposition 3.13. *We have*

(a) $D_\mu(s) = \frac{1}{\zeta(s)}$;
(b) $D_\varphi(s) = \frac{\zeta(s-1)}{\zeta(s)}$;
(c) $D_\tau(s) = \zeta(s)^2$;
(d) $D_\sigma(s) = \zeta(s-1)\zeta(s)$.

Proof. (b) Now

$$\begin{aligned} D_\varphi(s) &= \prod_p \left(1 + \frac{\varphi(p)}{p^s} + \frac{\varphi(p^2)}{p^{2s}} + \cdots + \frac{\varphi(p^k)}{p^{ks}} + \dots\right) \\ &= \prod_p \left(1 + \frac{p-1}{p^s} + \frac{p^2-p}{p^{2s}} + \cdots + \frac{p^k - p^{k-1}}{p^{ks}} + \dots\right) \\ &= \prod_p \left(1 + \frac{p-1}{p^s} \cdot \frac{1}{1-p^{1-s}}\right), \qquad \text{on summing the GP} \\ &= \prod_p \left(\frac{1-p^{-s}}{1-p^{-(s-1)}}\right), \qquad \text{on simplification} \\ &= \frac{\zeta(s-1)}{\zeta(s)}. \end{aligned}$$

(c) Now

$$\begin{aligned} D_\tau(s) &= \prod_p \left(1 + \frac{\tau(p)}{p^s} + \frac{\tau(p^2)}{p^{2s}} + \cdots + \frac{\tau(p^k)}{p^{ks}} + \dots\right) \\ &= \prod_p \left(1 + \frac{2}{p^s} + \frac{3}{p^{2s}} + \cdots + \frac{k+1}{p^{ks}} + \dots\right) \\ &= \prod_p \frac{1}{(1-p^{-s})^2} \qquad \text{using } (1-x)^{-2} = \sum_{k=0}^{\infty} (k+1)x^k \\ &= \zeta(s)^2 \end{aligned}$$

(d) This can be done by the same method as (b) or (c) – a good exercise! But, given that we know the answer, we can work backwards more quickly:

$$\zeta(s-1)\zeta(s) = \left(\sum_k \frac{k}{k^s}\right) \cdot \left(\sum_\ell \frac{1}{\ell^s}\right) = \sum_n \frac{\sum_{k|n} k \cdot 1}{n^s} = D_\sigma(s),$$

using Prop. 3.10

□

3.3. **Perfect numbers.** A positive integer n is called *perfect* if it is the sum of its proper (i.e., excluding n itself) divisors. Thus $\sigma(n) = 2n$ for n perfect.

Proposition 3.14. *An even number n is perfect iff it of the form $n = 2^{p-1}(2^p - 1)$ for some prime p with the property that $2^p - 1$ is also prime.*

Prime numbers of the form $2^p - 1$ are called *Mersenne primes*. (Unsolved problem: are there infinitely many such primes?)

It is easy to check that $\sigma(2^{p-1}(2^p - 1)) = 2^p(2^p - 1)$ when $2^p - 1$ is prime. The converse is more difficult — I leave this as a tricky exercise: you need to show that if $k \geq 2$ and

$2^{k-1}p_1 \dots p_\ell$ is perfect then $\ell = 1$ and $p_1 = 2^k - 1$. (It's easy to prove that if $2^k - 1$ is prime then so is k.)

It is an unsolved problem as to whether there are any odd perfect numbers. See e.g., `http://en.wikipedia.org/wiki/Perfect_number` for lots on this problem.