3.4 Multiplicative Functions

Question how to identify a multiplicative function? If it is the convolution of two other arithmetic functions we can use

Theorem 3.19 *If f and g are multiplicative then $f * g$ is multiplicative.*

Proof Assume $\gcd(m,n) = 1$. Then $d|mn$ if, and only if, $d = d_1 d_2$ with $d_1|m,\ d_2|n$ (and thus $\gcd(d_1,d_2) = 1$ and the decomposition is unique). Therefore

$$
\begin{aligned}
f * g(mn) &= \sum_{d|mn} f(d)\, g\left(\frac{mn}{d}\right) \\
&= \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2)\, g\left(\frac{m}{d_1}\frac{n}{d_2}\right) \\
&= \sum_{d_1|m} f(d_1)\, g\left(\frac{m}{d_1}\right) \sum_{d_2|n} f(d_2)\, g\left(\frac{n}{d_2}\right) \\
&\qquad \text{since } f \text{ and } g \text{ are multiplicative} \\
&= f * g(m)\, f * g(n)
\end{aligned}
$$

■

Example 3.20 *The divisor functions $d = 1 * 1$, and $d_k = 1 * 1 * ... * 1$ convolution k times, along with $\sigma = 1 * j$ and $\sigma_\nu = 1 * j^\nu$ are all multiplicative.*

Note 1 is completely multiplicative but d is not, so convolution does not preserve *complete* multiplicatively.

Question, was it obvious from its definition that σ was multiplicative? I suggest not.

Example 3.21 *For prime powers*

$$d(p^a) = a+1 \quad \textit{and} \quad \sigma(p^a) = \frac{p^{a+1}-1}{p-1}.$$

Hence

$$d(n) = \prod_{p^a \| n} (a+1) \quad \textit{and} \quad \sigma(n) = \prod_{p^a \| n} \left(\frac{p^{a+1}-1}{p-1}\right).$$

Recall how in Theorem 1.8 we showed that $\zeta(s)$ has a Euler Product, so for $\operatorname{Re} s > 1$,

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{7}$$

When convergent, an infinite product is non-zero. Hence (7) gives us (as already seen earlier in the course)

Corollary 3.22 *$\zeta(s) \neq 0$ for $\operatorname{Re} s > 1$.*

Thus for $\operatorname{Re} s > 1$ the inverse $1/\zeta(s)$ is well-defined and writing it as an Euler Product gives

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

where the arithmetic function μ is found by multiplying out the infinite product.

Definition 3.23 ***Möbius Function*** *$\mu(1) = 1$ and for $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r} > 1$, written as a product of distinct primes, then*

$$\mu(n) = \begin{cases} (-1)^r & \text{if } a_1 = a_2 = ... = a_r = 1, \\ 0 & \text{if some } a_i \geq 2. \end{cases}$$

Note

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2},$$

from the result for $\zeta(2)$ seen in Chapter 1.

It is easily seen that μ is multiplicative, but do convince yourself.

3.5 Möbius Inversion

Recall the definition of δ as $\delta(n) = 1$ if $n = 1$, 0 otherwise. Thus $D_\delta(s) = 1$ for all $s \in \mathbb{C}$. We also have

$$1 = \zeta(s) \frac{1}{\zeta(s)} = D_1(s) \, D_\mu(s) = D_{1*\mu}(s)$$

for $\operatorname{Re} s > 1$. Hence $D_\delta(s) = D_{1*\mu}(s)$, i.e.

$$\sum_{n=1}^{\infty} \frac{\delta(n)}{n^s} = \sum_{n=1}^{\infty} \frac{(1*\mu)(n)}{n^s} \tag{8}$$

for such s.

Important Observation In this course **we have not proved** that if $D_F(s) = D_G(s)$ for some domain of s then $F = G$.

This means that we can **not** conclude $\delta = 1 * \mu$ from (8). Instead I say that (8) "suggests" $\delta = 1 * \mu$ and we need to prove it true by alternative methods. Since both sides of the equality are multiplicative functions it suffices by Corollary 3.16 to prove equality on prime powers.

Important For a prime power

$$f * g(p^r) = \sum_{d|p^r} f(d)\, g\left(\frac{p^r}{d}\right).$$

Yet the only divisors d of p^r are of the form p^k with $0 \le k \le r$, thus

$$f * g\,(p^r) = \sum_{0\le k\le r} f\left(p^k\right) g\left(p^{r-k}\right) = \sum_{a+b=r} f(p^a)\, g\left(p^b\right). \tag{9}$$

We will use either of these without comment.

Theorem 3.24 ***Möbius Inversion***

$$1 * \mu = \delta,$$

i.e.

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

In other words, since δ is the identity under $*$ then μ is the **inverse** of 1 under $*$.

Proof The two functions 1 and μ are both multiplicative and thus, so is $1*\mu$. Since multiplicative functions are given by their values on prime powers it suffices to show that $1 * \mu\,(p^r) = \delta\,(p^r)$ for any prime p and all $r \ge 1$.

If $r = 0$ then $p^0 = 1$ and both $1 * \mu\,(1) = 1$ and $\delta\,(1) = 1$.

If $r \geq 1$ then

$$\begin{aligned}
(1 * \mu)(p^r) &= \sum_{d|p^r} \mu(d) = \sum_{0 \leq k \leq r} \mu\big(p^k\big) \quad \text{by } (9)\,, \\
&= \sum_{0 \leq k \leq 1} \mu\big(p^k\big) \quad \text{since } \mu\left(p^k\right) = 0 \text{ for } k \geq 2, \\
&= \mu(1) + \mu(p) \\
&= 1 - 1 \\
&= 0 = \delta(p^r)\,.
\end{aligned}$$

■

The following is also often called Möbius Inversion and looks more general than the previous result - but it is not!

Corollary 3.25 *For arithmetic functions f and g we have*

$$f = 1 * g \quad \textit{if, and only if,} \quad g = \mu * f.$$

Proof $(\Rightarrow)$ If $f = 1 * g$ then

$$\begin{aligned}
\mu * f &= \mu * (1 * g) \\
&= (\mu * 1) * g \quad \text{since } * \text{ is associative} \\
&= \delta * g \\
&= g
\end{aligned}$$

$(\Leftarrow)$ I leave the implication in the other direction to the student. ■

To give us arithmetic functions with which to give examples illustrating future results:

Definition 3.26 *An integer n is* ***square-free*** *if no square divides n. In fact, it suffices that no square of a prime divides n, i.e. $p|n \Rightarrow p^2 \nmid n$.*

Alternatively, if $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$, distinct primes, then no $a_i \geq 2$.

Define $Q_2(n) = 1$ if n square-free and 0 otherwise.

An integer n is ***k-power free****, or simply k*-***free*** *if $p|n \Rightarrow p^{k+1} \nmid n$. Alternatively, if $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$, distinct primes, then no $a_i \geq k$.*

Define $Q_k(n) = 1$ if n is k-free and 0 otherwise.

Careful, this notation is not universal. Also, $Q_2(n)$ is often written as $|\mu(n)|$ or $\mu^2(n)$. There are no such alternatives for $Q_k(n)$ when $k \geq 3$. It is easily seen that Q_2 and Q_k are multiplicative, but convince yourself.

The definition can be extended to $k = 1$, for the only integer that is 1-*free,* i.e. divisible by no first power of a prime, is $n = 1$. Thus $Q_1(n) = 1$ if $n = 1$, 0 otherwise, i.e. $Q_1 = \delta$.

Aside The definition of the Möbius function can be written as

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

The form $(-1)^{\omega(n)}$ suggests defining a further arithmetic function.

Definition 3.27 *The* ***Liouville Function*** λ *is defined by* $\lambda(1) = 1$ *and* $\lambda(n) = (-1)^{\Omega(n)}$ *for all* $n \geq 2$.

This is multiplicative since Ω is additive, and $\lambda(p^r) = (-1)^r$ for all powers of primes. This function is used a lot in the Problem Sheet to the section.