# Lecture 13

## Arithmetic Functions

**Today** - Arithmetic functions, the Möbius function

**(Definition) Arithmetic Function:** An **arithmetic function** is a function $f : \mathbb{N} \to \mathbb{C}$

**Eg.**

$$\begin{aligned}
\pi(n) &= \text{ the number of primes } \leq n \\
d(n) &= \text{ the number of positive divisors of } n \\
\sigma(n) &= \text{ the sum of the positive divisors of } n \\
\sigma_k(n) &= \text{ the sum of the kth powers of } n \\
\omega(n) &= \text{ the number of distinct primes dividing } n \\
\Omega(n) &= \text{ the number of primes dividing } n \text{ counted with multiplicity}
\end{aligned}$$

**Eg.**

$$\begin{aligned}
&\sigma(1) = 1 \\
&\sigma(2) = 1 + 2 = 3 \\
&\sigma(3) = 1 + 3 = 4 \\
&\sigma(6) = 1 + 2 + 3 + 6 = 12
\end{aligned}$$

**(Definition) Perfect Number:** A **perfect number** $n$ is one for which $\sigma(n) = 2n$ (eg., $6, 28, 496$, etc.)

**Big open conjecture:** Every perfect number is even.

**Note:** One can show that if $n$ is an even perfect number, then $n = 2^{m-1}(2^m - 1)$ where $2^m - 1$ is a Mersenne prime (Euler)

**(Definition) Multiplicative:** If $f$ is an arithmetic function such that whenever $(m, n) = 1$ then $f(mn) = f(m)f(n)$, we say $f$ is **multiplicative**. If $f$ satisfies the stronger property that $f(mn) = f(m)f(n)$ for all $m, n$ (even if not coprime), we say $f$ is **completely multiplicative**

**Eg.**

$$f(n) = \begin{cases} 1 & n = 1 \\ 0 & n < 1 \end{cases}$$

is completely multiplicative. It's sometimes called $\mathbb{1}$ (we'll see why soon).

**Eg.** $f(n) = n^k$ for some fixed $k \in \mathbb{N}$ is also completely multiplicative

**Eg.** $\omega(n)$ is not multiplicative (adds, but $2^{\omega(n)}$ is multiplicative)

**Eg.** $\phi(n)$ is multiplicative (by CRT)

**Note:** If $f$ is a multiplicative function, then to know $f(n)$ for all $n$, it suffices to know $f(n)$ for prime powers $n$. This is why we wrote

$$\phi(p_1^{e_1} \dots p_r^{e_r}) = \prod p_i^{e_i - 1}(p_i - 1)$$

**(Definition) Convolution:** The **convolution** of two arithmetic functions $f$ and $g$ is $f * g$ defined by

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

(summing over positive divisors of $n$). Compare this to convolution from calculus or differential equations

$$\begin{aligned} (f * g)(x) &= \int_{t=-\infty}^{\infty} f(t) g(x-t) dt \\ \text{or } &\int_{t=0}^{x} f(t) g(x-t) dt \quad \text{ if } f(y), g(y) \text{ are } 0 \text{ for } y < 0 \end{aligned}$$

**Eg.**

$$f * \mathbb{1} = \mathbb{1} * f = f \text{ for every } f \text{ (check 1)}$$

$\mathbb{1}$ is the identity for convolution

**Theorem 48.** *If $f$ and $g$ are multiplicative then $f * g$ is multiplicative.*

*Proof.* Suppose $m$ and $n$ are coprime. Then any divisor of $mn$ is of the form

$d_1, d_2$, where $d_1|m$ and $d_2|n$, uniquely. So we have

$$\begin{aligned}
(f * g)(mn) &= \sum_{d|mn} f(d) g\left(\frac{mn}{d}\right) \\
&= \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) g\left(\frac{m}{d_1} \cdot \frac{n}{d_2}\right) \\
&= \sum_{d_1|m} \sum_{d_2|n} \underbrace{f(d_1) f(d_2)}_{\text{since } (d_1, d_2)=1} \underbrace{g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right)}_{\text{since } (\frac{m}{d_1}, \frac{n}{d_2})=1} \\
&= \left(\sum_{d_1|m} f(d_1) g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n} f(d_2) g\left(\frac{n}{d_2}\right)\right) \\
&= (f * g)(m)(f * g)(n)
\end{aligned}$$

■

**Eg.** Let $U(n) = 1$ for all $n$. Then for any arithmetic function $f$, we have

$$(f * U)(n) = \sum_{d|n} f(d) \underbrace{U\left(\frac{n}{d}\right)}_{=1} = \sum_{d|n} f(d)$$

This is usually called $F(n)$.

If $f$ is multiplicative, then $F$ is multiplicative, by theorem (since $U$ is obviously completely multiplicative) (that's theorem 4.4 in the book). In particular, we compute $U * U$

$$(U * U)(n) = \sum_{d|n} 1 \cdot 1 = \text{number of divisors of } n = d(n)$$

so $d(n)$ is multiplicative.

For a prime power $p^\alpha$, the number of divisors is $\alpha + 1$. So

$$d(p_1^{e_1} \dots p_r^{e_r}) = \prod_{i=1}^{r} (e_i + 1)$$

For the function $r_k(n) = n^k$, we have

$$(r_k * U)(n) = \sum_{d|n} d^k = \sigma_k(n)$$

which is therefore multiplicative.

Since

$$\sigma_k(p^\alpha) = 1 + p^k + \cdots + p^{k\alpha} = \frac{p^{k(\alpha+1)} - 1}{p^k - 1}$$

we get

$$\sigma_k\left(\prod p_i^{e_i}\right) = \prod_{i=1}^{r} \frac{p_i^{k(e_i+1)} - 1}{p_i^k - 1}$$

**Theorem 49.** *For any positive integer $n$, we have*

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

*In other words $\phi * U = r_1$.*

*Proof.* Since both sides are multiplicative, enough to show it for prime powers.

$$\begin{aligned}
r_1(p^\alpha) &= p^\alpha \\
\sum_{d|p^\alpha} \phi(d) &= \phi(1) + \phi(p) + \cdots + \phi(p^\alpha) \\
&= 1 + (p-1) + p(p-1) + \cdots + p^{\alpha-1}(p-1) \\
&= 1 + p - 1 + p^2 - p + p^3 - p^2 + \cdots + p^\alpha - p^{\alpha-1} \\
&= p^\alpha
\end{aligned}$$

■

**Eg.** What is $r_k * r_k$?

$$(r_k * r_k)(n) = \sum_{d|n} d^k \left(\frac{n}{d}\right)^k = \sum_{d|n} n_k = n^k d(n)$$

Other multiplicative functions: $(\frac{}{D})$ since $(\frac{mn}{D}) = (\frac{m}{D})(\frac{n}{D})$

There's an interesting multiplicative function - let $\tau(n)$ (Ramanujan's tau function) be the coefficient of $q^n$ in $q\prod_{i=1}^{\infty}(1-q^i)^{24}$. Then

$$\begin{aligned}
&\tau(1) = 1 \\
&\tau(2) = -24 \\
&\tau(3) = 252 \\
&\tau(6) = -6048 = -24 \cdot 252 = \tau(2)\tau(3) \\
&\qquad \text{etc.}
\end{aligned}$$

**Theorem 50.** *$\tau(n)$ is multiplicative (deep)*

Proof uses modular forms.

A famous open conjecture is **Lehmer's conjecture**: $\tau(n) \neq 0$ for every natural number $n$.

**Proposition 51.** *$f * g = g * f$ for any arithmetic functions $f, g$ (ie., convolution is commutative)*

*Proof.*
$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

as $d$ ranges over divisors of $n$, so does $\frac{n}{d} = d'$ so we write

$$(f * g)(n) = \sum_{d'|n} f(d')g(\frac{n}{d'}) = \sum_{d|n} f\left(\frac{n}{d}\right) g\left(\frac{n}{\frac{n}{d}}\right) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d) = (g * f)(n)$$

∎

**Proposition 52.**
$$f * (g * h) = (f * g) * h$$

*(ie., $*$ is associative)*

Proof left as exercise.

The Möbius mu function is defined to be

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

remembering that $\omega(n)$ was additive, it's easy to see $\mu(n)$ is a multiplicative function

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n = p_1 \dots p_r \text{ for distinct primes } p_i \\ 0 & \text{if some } p^2 \text{ divides } n \end{cases}$$

Remember the function $U(n) = 1$ for all $n$.

**Theorem 53.**
$$\mu * U = \mathbb{1} \begin{cases} 1 & \textit{if } n = 1 \\ 0 & \textit{otherwise} \end{cases}$$

*Proof.* $\mu, U$ are multiplicative, so $\mu * U$ is too. So enough to show that $(\mu * U)(1) = 1$ and $(\mu * U)(p^\alpha) = 0$ for prime powers $p^\alpha$.

The first is trivial:

$$\begin{aligned}
(\mu * U)(1) &= \sum_{d|1} \mu(1)U(1) = 1 \cdot 1 = 1 \\
(\mu * U)(p^\alpha) &= \sum_{d|p^\alpha} \mu(p^\alpha)U(p^\alpha) \\
&= \mu(1) + \mu(p) \\
&= 1 + (-1) \\
&= 0
\end{aligned}$$

So $\mu * U = 1$. ∎