Supplement 2

Arithmetic Functions and Dirichlet Convolution

A real (or complex) valued function defined on $\mathbb{N}$ is called <u>arithmetical</u>.

The Möbius function $\mu(n)$

The Möbius function μ is defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n \text{ is } \underline{\text{not}} \text{ squarefree} \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes.} \end{cases}$$

<u>Note:</u> $\mu(n) = 0 \Leftrightarrow n$ has a square factor > 1.

The Möbius function arises in many different places in number theory. One of its fundamental properties is the following "orthogonality" relation:

<u>Theorem 1:</u> If $n \geq 1$, then $\displaystyle\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$.

<u>Proof:</u> Clearly true for $n=1$. For $n>1$, write $n = p_1^{e_1} \cdots p_k^{e_k}$. In the sum $\displaystyle\sum_{d|n} \mu(d)$ the only non-zero terms come from $d=1$ and from those divisors of n which are products of distinct primes. Thus

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \cdots + \mu(p_k) + \mu(p_1 p_2) + \cdots + \mu(p_{k-1} p_k) + \cdots + \mu(p_1 p_2 \cdots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k \\ &= (1-1)^k \\ &= 0 \end{aligned}$$

$\square$

Dirichlet Convolution: If f and g are two arithmetical functions, we define their Dirichlet convolution to be the arithmetical function

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

Theorem 2: For any arithmetical functions f, g, h we have

$$f*g = g*f \qquad \text{(commutative)}$$
$$(f*g)*h = f*(g*h) \qquad \text{(associative)}$$

Proof: We first note that the definition of $f*g$ can be re-expressed

$$f*g(n) = \sum_{ab=n} f(a)\, g(b)$$

from which commutativity follows immediately. To prove associativity we let $A = g*h$ and note that

$$f*A(n) = \sum_{ad=n} f(a) A(d) = \sum_{ad=n} f(a) \sum_{bc=d} g(b) h(c) = \sum_{abc=n} f(a) g(b) h(c)$$

and similarly, if $B = f*g$ then $B*h(n) = \sum_{abc=n} f(a) g(b) h(c)$. □

We now introduce an identity element for this multiplication by defining

$$\delta(n) := \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}.$$

Theorem 3: For any arithmetical function f

$$\delta*f = f*\delta = f$$

Proof: $f*\delta(n) = \sum_{d|n} f(d)\, \delta\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \left\lfloor \frac{d}{n} \right\rfloor = f(n)$ □

Möbius Inversion

Theorem 1 (Restatement) $1 * \mu = \mu * 1 = \delta$

where $1(n) := 1$ for all $n \in \mathbb{N}$.

The following fundamental result follows immediately from Theorems 1, 2 & 3.

Corollary 1: (Möbius Inversion Formula)

$$F(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Proof: Since $\mu * 1 * f = \delta * f = f$ it follows that

$$F = 1 * f \iff \mu * F = f. \qquad \square$$

Examples

1. $$\log n = \sum_{d|n} \Lambda(d) \iff \Lambda(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right)$$

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

Lemma 2.1.

(Since $\sum_{d|n} \mu(d) = \delta$ & $\log 1 = 0$.)

2. $$n = \sum_{d|n} \varphi(d) \iff \varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

Euler Phi Function

Corollary 2 (later in this note)

Multiplicative Functions

An arithmetical function f is called multiplicative if $f(1) \neq 0$ and

$$f(mn) = f(m)f(n) \quad \text{whenever} \quad (m,n) = 1.$$

A multiplicative function f is called completely multiplicative if we also have

$$f(mn) = f(m)f(n) \quad \text{for all } m,n \in \mathbb{N}.$$

The following properties are easily verified:

- If f is multiplicative, then $f(1) = 1$
- f multiplicative $\iff f\left(\prod_{j=1}^{k} p_j^{\alpha_j}\right) = \prod_{j=1}^{k} f(p_j^{\alpha_j})$ for all primes p_j and $\alpha_j \in \mathbb{N}$.
- If f is multiplicative, then f completely multiplicative $\iff f(p^\ell) = f(p)^\ell$ for all primes p and $\ell \in \mathbb{N}$.

Examples

1. The identity function $\delta(n) = \lfloor \frac{1}{n} \rfloor$ is completely multiplicative.
2. The Möbius function is multiplicative, but not completely
   (Easy) $\mu(4) = 0$, but $\mu(2)\mu(2) = 1$.
3. The Euler Phi function is multiplicative, but not completely
   (Not so easy!) $\varphi(4) = 2$, but $\varphi(2) = 1$.

The Euler Phi Function

Recall that the Euler Phi Function $\varphi(n) = \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right| = \#\{1 \le m \le n : (m,n)=1\}$.

The multiplicativity of φ is closely related to

The Chinese Remainder Theorem

If $m_1, \dots, m_k \in \mathbb{N}$ are pairwise coprime and $b_1, \dots, b_k \in \mathbb{Z}$, then the system

$$x \equiv b_j \bmod m_j \quad 1 \le j \le k$$

has exactly one solution modulo $n = m_1 \cdots m_k$. In particular, if $n = p_1^{l_1} \cdots p_k^{l_k}$ then

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \cong \left(\mathbb{Z}/p_1^{l_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_k^{l_k}\right)^\times .$$

* Since $\varphi(n) = \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right|$ it follows immediately that φ is multiplicative.

<u>Theorem 4</u>: For $n \ge 1$, $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$.

<u>Proof</u>: Since the only numbers $1 \le m \le p^l$ <u>not</u> coprime to p^l are the multiples of p, we see that $\varphi(p^l) = p^l - p^{l-1} = p^l\left(1 - \frac{1}{p}\right)$. $\square$

<u>Corollary 2</u>:

$$\varphi(n) = \sum_{d} \mu(d) \frac{n}{d} \text{ and hence by Möbius inversion } \sum_{d \mid n} \varphi(d) = n$$

<u>Proof</u>: Clear for $n=1$ (empty products are assigned the value 1).

If $n = p_1^{l_1} \cdots p_k^{l_k} > 1$, then $\displaystyle\prod_{p \mid n} \left(1 - \frac{1}{p}\right) = \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right) \underset{(*)}{=} \sum_{d \mid n} \frac{\mu(d)}{d}$

$\square$

<u>Exercise 1</u>: Verify $(*)$.

Let $q \in \mathbb{N}$.

¿ How many numbers $1 \le n \le x$ are relatively prime to q ?

Since

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

it follows that

$$\#\{1 \le n \le x : (n,q) = 1\} = \sum_{n \le x} \sum_{d \mid (n,q)} \mu(d)$$

#{1 ≤ n ≤ x : d | n}

Since $d \mid (n,q)$ $\Updownarrow$ $d \mid n$ & $d \mid q$

$$= \sum_{d \mid q} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor$$

$$= x \sum_{d \mid q} \mu(d) \frac{1}{d} + \sum_{d \mid q} \mu(d) \underbrace{\left(\left\lfloor \frac{x}{d} \right\rfloor - \frac{x}{d} \right)}_{|\cdot| \le 1}$$

Since

$$\sum_{d \mid n} \frac{\mu(d)}{d} = \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = \frac{\varphi(n)}{n}$$

it follows that

divisor function

$$\#\{1 \le n \le x : (n,q) = 1\} = \frac{x\,\varphi(q)}{q} + O(\tau(q)) .$$