Math 1560 - Notes 3

Ian Benway

8 February 2022

1 Dirichlet Convolution

Let f and g be arithmetic functions. The **Dirichlet Convolution** (or Dirichlet Product) of f and g is

$$\begin{aligned}(f*g)(n) &= \sum_{d_1 d_2 = n} f(d_1)g(d_2) \\ &= \sum_{d|n} f(d)g(\frac{n}{d}).\end{aligned}$$

Let's quickly check some properties:

- Associativity holds:

$$\begin{aligned}((f*g)*h)(n) &= (f*(g*h))(n) \\ &= \sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3)\end{aligned}$$

- Commutitivity clearly holds.
- It has a multiplicative identity:
  Let $I : \mathbb{Z}_+ \to \{0, 1\}$ be given by

$$I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

  Then $f * I = I * f = f$.

- There are also *usually* Dirichlet inverses.

Lemma 1. *If f is an arithmetic function such that $f(1) \neq 0$, then there exists an arithmetic function g such that $f * g = I$. This inverse is given recursively by*

$$\begin{aligned}g(1) &= \frac{1}{f(1)} \\ \text{and } g(n) &= -\frac{1}{f(1)} \sum_{\substack{d|n \\ d<n}} g(d)f(\frac{n}{d}).\end{aligned}$$

Proof. We'll show that given f, g defined above, $f * g = I$.

$$n = 1: \qquad g(1)f(1) = \frac{1}{f(1)} f(1) = 1$$

$$\begin{aligned} n > 1: \qquad \sum_{d|n} g(n) f(\frac{n}{d}) &= g(n)f(1) + \sum_{\substack{d|n \\ d<n}} g(d) f(\frac{n}{d}) \\ &= -\frac{f(1)}{f(1)} \sum_{\substack{d|n \\ d<n}} g(d) f(\frac{n}{d}) + \sum_{\substack{d|n \\ d<n}} g(d) f(\frac{n}{d}) \\ &= 0. \end{aligned}$$

□

2 Möbius Inversion

The Möbius Mu Function $\mu : \mathbb{Z}_+ \to \{-1, 0, 1\}$ given by

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 p_2 ... p_k, \text{ each pairwise distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

Lemma 2. *μ is a multiplicative function.*

Proof. Let $m, n, \in \mathbb{Z}_+$ with $(m, n) = 1$. Write

$$\begin{aligned} m &= p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \\ n &= q_1^{f_1} q_2^{f_2} \dots q_l^{f_l}. \end{aligned}$$

We have two cases:
Case 1: Some e_i or $f_i \geq 2$. Then, $\mu(mn) = \mu(m)\mu(n) = 0$.
Case 2: All $e_i = f_i = 1$. Then $\mu(m) = (-1)^k$ and $\mu(n) = (-1)^l$, so $\mu(m)\mu(n) = (-1)^{k+l}$.
Since $(m, n) = 1$, we have $\mu(mn) = (-1)^{k+l}$. □

Lemma 3.

$$\sum_{d|n} \mu(d) = 0 \qquad \forall n \geq 2$$

i.e., the summatory function of μ is I.

Proof. $f(n) = \sum_{d|n} \mu(d)$ is multiplicative. So it suffices to check on prime powers:

$$\begin{aligned} f(p^e) &= \mu(1) + \mu(p) + (p^2) + \dots + \mu(p^e) \\ &= 1 - 1 + 0 + \dots + 0 = 0 \end{aligned}$$

□

Let $i : \mathbb{Z}_+ \to \{1\}$ bet the constant 1 function.

Lemma 4. $i * \mu = \mu * i = I$

Proof.

$$\begin{aligned} n = 1: &\quad i(1)\mu(1) = 1 \\ n > 1: &\quad (i*\mu)(n) = \sum_{d|n} \mu(d) = 0 \end{aligned}$$

□

Summatory functions can be seen as Dirichlet products: the summatory function F of f is $F = f * i$.

Recall summatory functions inherit multiplicativity. In fact, this holds for Dirichlet products: if f, g are multiplicative, then so is $f * g$.
The proof is parallel to the proof of summatory functions.

Theorem 1 (Möbius Inversion)**.** *Let* $F(n) = \sum_{d|n} f(d)$. *Then,*

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

Proof. $F = f * i$, thus $F * \mu = (f * i) * \mu = f * (i * \mu) = f * I = f$. □

Corollary 1. *If F is the summatory function of f, and F is multiplicative, then f is multiplicative, as $f = F * \mu$, and μ is multiplicative.*

Corollary 2. *Corollary 1 proves that the Euler ϕ function is multiplicative, as $\sum_{d|n} \phi(d) = \phi * i =$ the identity.*

Applications of Möbius Inversion

- Application 1: Cyclotomic Polynomials
  The nth cyclotomic polynomial $\Phi_n(x)$ is the unique irreducible polynomial in $\mathbb{Z}[x]$ dividing $x^n - 1$ but not $x^k - 1$ for $k < n$. Thus

  $$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ (k,n)=1}} (x - e^{2\pi i \frac{k}{n}}),$$

  as the roots of this polynomial are exactly the primitive nth roots of unity.
  We have $\prod_{d|n} \Phi_d(x) = x^n - 1$. By Möbius Inversion, if $G(n) = \prod_{d|n} g(d)$, then

$g(n) = \prod_{d|n} G(d)^{\mu(\frac{n}{d})}$.

In particular, taking $G(n) = x^n - 1$ ($x \in \mathbb{C}$) gets

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})} \qquad (x \in \mathbb{C}).$$

Applying this identity for enough $x \in \mathbb{C}$ yields this as an identity of polynomials.

- Application 2: Dynatomic Polynomials
  Dynatomic polynomials have as roots the periodic points (of certain periods) of a polynomial.
  Let K be a field, and let $f \in K[x]$ of degree $d \geq 2$. Let $f^n = f \circ f \circ \cdots \circ f$ (n times).
  $P \in \bar{K}$ is said to be periodic under f if $f^n(P) = P$ for some $n \geq 1$.

  For example: $f(x) = x^2 - 1$ has 0 as a periodic point: $0 \to -1 \to 0$.
  It's period is 2.

  Note: if n is the smallest possible integer such that $f^n(P) = P$ (for P periodic), then n is said to be the **exact period** of P.

  The nth dynatomic polynomial of f is

  $$\Phi_{f,n}(x) :=_{d|n} (f^d(x) - x)^{\mu(\frac{n}{d})}.$$

  Our hope is that $\Phi_{f,n}(x)$ has its roots as the point of exact period n. But our hope is brutally and violently ripped apart, as this is not the case; for example,

  $$f(x) = x^2 - 3/4$$
  $$f^2(x) - x = (x - 3/2)(x + 1/2)^3$$
  $$f(x) - x = (x - 3/2)(x + 1/2).$$

  Thus, $\frac{f^2(x)-x}{f(x)-x} = (x + 1/2)^2$. But $x = -1/2$ is fixed under f.