Dirichlet Convolution and Möbius Inversion

A. Anas Chentouf

May 21, 2022

This manuscript contains notes on arithmetic functions and Dirichlet convolutions, particularly aimed towards motivating the latter as well as demysifying the Möbius inversion. It was written in my capacity as an undergraduate assistant for the Spring 2022 offering of 18.781, MIT's elementary number theory class, taught by Prof. Ju-Lee Kim.

The notes arised because I found that the treatment of most textbooks on the subject is relatively unmotivated and confusing. I had struggled for years with fully grasping what Möbius inversion was really about, and so I hoped that this would help students avoid the issue.

As usual, these notes are by no means complete, and any error in them is on my part. If you do find any mistakes, please let me know at chentouf@mit.edu.

1 Notation and preliminary results

Definition 1 (Arithmetic Function)**.** An arithmetic function is a function $f : \mathbb{N} \to \mathbb{C}$.

Function	Definition
$\tau(n)$	Number of divisors of n
$\sigma_k(n)$	Sum of k-th powers of the positive divisors of n
$\phi(n)$	Number of integers in $[1, n]$ coprime to n
id_1	The function that is identically equal to 1
δ	The indicator function of the set $\{1\}$

Table 1: Table of some Arithmetic Functions

In addition to the above functions, the Möbius function plays a role so important that it deserves a definition of its own.

Definition 2 (Möbius Function)**.** The Möbius function is defined as

$$\mu(n) = \begin{cases} 1 & \text{if n=1} \\ 0 & \text{if p}^2|n \text{ for some prime } p \end{cases}$$

Definition 3 (Multiplicative)**.** We say that an arithmetic function f is multiplicative if $f(mn) = f(m)f(n)$ for all coprime natural numbers m, n.

We are particularly interested in multiplicative functions because they are uniquely determined by their values at prime powers - this follows from the fundamental theorem of arithmetic.

Exercise 1. *Prove the above fact: that a multiplicative function is uniquely determined by its values at prime powers.*

Many of the functions we see in introductory number theory are multiplicative: τ, μ, σ_k are all multiplicative. Even more restrictive than multiplicative function is the class of totally multiplicative functions.

Definition 4 (Totally multiplicative function)**.** We say that an arithmetic function f is multiplicative if $f(mn) = f(m)f(n)$ for all natural numbers m, n.

Exercise 2. *Prove that a totally multiplicative function is uniquely determined by its values at prime numbers.*

2 Dirichlet Convolution

Definition 5 (Dirichlet Convolution)**.** If f, g are two arithmetic functions, then we define their Dirichlet convolution, denoted by $f * g$, as the arithmetic function given by the sum

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

Fact 1. *Dirichlet convolution is commutative, that is, $f * g, g * f$ are equal as functions.*

Fact 2. *Dirichlet convolution is associative, that is, $(f * g) * h, f * (g * h)$ are equal as functions.*

Fact 3. *The equality of arithmetic functions $f * \delta = f = \delta * f$ holds.*

Proof. The first equality follows from the fact that

$$(f * \delta)(n) = \sum_{d|n} f(d)\delta(\frac{n}{d}),$$

but all the terms are zero except when $n = d$. This shoes that $(f * \delta)(n) = f(n)$, the second equality holds by commutativity. □

The following notes talks about viewing arithmetic functions as a ring. If you have not seen what a ring is before, feel free to skip the remainder of this section.

Note 1. *Note that the above three facts allow us to conclude that the set of arithmetic functions forms a commutative, associative, unital* [1] *ring under pointwise addition of functions and Dirichlet convolution, with the identity element being the δ function. We denote this ring as $\mathbb{A}$. In fact, we can go as far as exactly determining the invertible elements, as we shall do in the next few results.*

Lemma 1 (Invertibility of Arithmetic Functions)**.** *An arithmetic function $f \in \mathbb{A}$ is invertible, that is, there exists $g \in \mathbb{A}$ such that $f * g = \delta$, if and only if $f(1) \neq 0$.*

Note that from the properties of rings, if the inverse of an arithmetic function $f \in \mathbb{A}$ exists then it is unique.

Lemma 2. *The inverse of a multiplicative function is multiplicative.*

3 Möbius Inversion

Lemma 3.

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

Proof. If $n = 1$, then result clearly holds. Otherwise, consider the prime factorization $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Note that it suffices to consider $n = p_1 \cdots p_k$ since all other divisors will not be squarefree and will hence contribute nothing to the sum. Now by the inclusion-exclusion principle, we have that

$$\sum_{d|p_1 \cdots p_k} \mu(d) = \sum_{S \subset \{1,\ldots,k\}} (-1)^{|S|} = (1-1)^{|S|} = 0.$$

□

[1] I only placed these modifiers here for clarity, but see Bjorn Poonen's paper on why all rings should be unital.

In the notation we introduced earlier, we just proved that $\mu * u = \delta$.

Theorem 1 (Möbius Inversion Formula)**.** *Assume that $F(n) = \sum_{d|n} f(d)$. Then $f(n) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right)$. Alternatively, if $F = f * u$ then $f = F * \mu$.*

Proof. Note that

$$F = f * u \Rightarrow (F * \mu) = (f * u) * \mu = f * (u * \mu) = f * \delta = f.$$

□

4 Applications of Dirichlet Convolution

Lemma 4. *If f, g are multiplicative functions, then so is $f * g$.*

Proof. Let m, n be coprime natural numbers. Note that a divisor $d|mn$ can be expressed as ab where $a|m$, $b|n$ since m, n are coprime and hence their prime divisors

$$(f * g)(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{a|m,b|n} f(ab)g\left(\frac{mn}{ab}\right) = \sum_{a|m,b|n} \left(f(a)g\left(\frac{m}{a}\right)\right)\left(f(b)\left(\frac{n}{b}\right)\right)$$

$$= \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right) = (f * g)(m)(f * g)(n).$$

□

Corollary 1. *The functions τ, σ_k are all multiplicative.*

Proof. Note that $\tau = u * u$ and $\sigma_k = f_k * u$ where $f_k : n \mapsto n^k$. □

4.1 Example from Quiz 3

Problem 4.2 in the Quiz asked you to show that

$$\sum_{d|n} d\mu(d) = (-1)^{\omega(n)}\phi(n)\frac{s(n)}{n},$$

where $\omega(n)$ is the number of primes that divides n, and $s(n)$ is their product.

Note that the RHS is multiplicative, $\phi(n)$, $(-1)^{\omega}(n)$, $s(n)$, and $\frac{1}{n}$ are all multiplicative and so is their product. Moreover, the LHS can be written as

$$n\sum_{d|n} \mu(d)\frac{d}{n} = n\sum_{d|n} \mu(d) \cdot \frac{1}{\frac{n}{d}} = n \cdot (\mu * f)$$

where $f(n) = \frac{1}{n}$. note that by the above lemma, $\mu * f$ is multiplicative, and the pointwise product of two multiplicative functions is multiplicative, so the LHS is multiplicative too. As such, it suffices to prove the equality of both sides for all prime powers p^k.

However,

$$\sum_{d|p^k} d\mu(d) = 1\mu(1) + p\mu(p)$$

as $\mu(n)$ is zero when n is not square free. Hence,

$$\text{LHS}(p^k) = 1 - p,$$

and

$$\text{RHS}(p^k) = (-1)^1(p-1)\frac{p}{p} = 1 - p,$$

as desired.

5 More Exercises

Exercise 3. *Show that the convolution of two totally multiplicative functions need not be totally multiplicative.*

Exercise 4. *Is the convolution of a multiplicative function f and an arbitrary arithmetic function g necessarily multiplicative? Provide a proof for this statement, or a counterexample.*

Exercise 5. *Starting from the definition of the Euler totient function ϕ, show that $\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$. Use this to conclude that ϕ is multiplicative.*

Exercise 6. *Determine a closed form for $\sum_{d|n} |\mu(d)|$.*

Exercise 7. *Show that*

$$\sum_{m=1}^{n} \gcd(m, n) = (\mathrm{id} * \varphi)(n).$$

Exercise 8. *Use the above problem to determine an expression for $\sum_{m=1}^{n} \gcd(m, n)$.*

Exercise 9. *Prove that $\sigma(n) = \sum_{d|n} \phi(d)\tau\left(\frac{n}{d}\right)$.*

Exercise 10 (Invertibility of Arithmetic Functions)**.** *We say that an arithmetic function $f \in \mathbb{A}$ is invertible if there exists $g \in \mathbb{A}$ such that $f * g = \delta$. Show that f is invertible if and only if $f(1) \neq 0$.*

Exercise 11. *Show that the inverse of a multiplicative function is multiplicative.*

References

[1] Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, *An Introduction to the Theory of Numbers.*