Math 680 Fall 2017

Arithmetic Functions

This course is essentially the study of arithmetic functions and their statistical behavior.

Definition: An *arithmetic function* is a function $f\colon \mathbb{Z}^+ \to \mathbb{C}$. Such a function is called *multiplicative* if it isn't identically zero and $f(mn) = f(m)f(n)$ whenever m and n are relatively prime positive integers. A multiplicative function is called *totally multiplicative* if $f(mn) = f(m)f(n)$ for all positive integers m and n.

Example 1: The prime counting function is defined by

$$\pi(n) := \sum_{\substack{p \le n \\ p \text{ prime}}} 1.$$

As with many arithmetic functions, this function is extended to $[0, \infty)$ by setting $\pi(x) = \pi\big([x]\big)$, where $[\cdot]$ denotes the greatest integer (or "floor") function. Thus

$$\pi(x) := \sum_{\substack{p \le x \\ p \text{ prime}}} 1.$$

Example 2: Euler's phi function is given by

$$\phi(n) = \sum_{\substack{1 \le d \le n \\ \gcd(d,n)=1}} 1.$$

It isn't transparent from the definition that this function is multiplicative, but we'll soon see that it is.

Example 3: The Möbius mu function is given by

$$\mu(n) = \begin{cases} (-1)^m & \text{if } n \text{ is a product of } m \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

This function arises naturally when one attempts to "invert" (in a certain algebraic sense) arithmetic functions and certain sums of arithmetic functions. This function is clearly multiplicative.

Example 4: It is often useful to have a concise notation for the number of prime factors of a number; this is typically denoted

$$\omega(n) = \sum_{\substack{p \mid n \\ p \text{ prime}}} 1.$$

Example 5: One often is interested in the factors of a given positive integer, and sums involving these factors. The two most common associated functions here are

$$\tau(n) = \sum_{\substack{1 \le d \le n \\ d \mid n}} 1$$

and

$$\sigma(n) = \sum_{\substack{1 \le d \le n \\ d|n}} d.$$

Example 6: The following three multiplicative functions arise naturally when one considers the algebraic structure of the set of multiplicative functions (which we will do below):

$$U(n) = 1$$

$$E(n) = n$$

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

Definition: The *"Dirichlet product,"* or *convolution* is the binary operation on the set of arithmetic functions given by

$$f * g(n) = \sum_{\substack{1 \le d \le n \\ d|n}} f(d)g(n/d) = \sum_{\substack{1 \le d_1, d_2 \\ n = d_1 d_2}} f(d_1)g(d_2).$$

One notes immediately that this operation is commutative. A moment's reflection shows that it is associative as well. Moreover, $I * f = f$ for all arithmetic functions f. Thus, it is reasonable to wonder if the arithmetic functions form an abelian group under convolution, with I as the identity element. Indeed, this is almost the case.

Lemma 1: An arithmetic function f is invertible (i.e., there is an arithmetic function f^{-1} with $f * f^{-1} = I$) if and only if $f(1) \neq 0$, in which case the inverse is unique.

Proof: Suppose first that there is an f^{-1} with $f * f^{-1} = I$. Then $f * f^{-1}(1) = f(1)f^{-1}(1) = I(1) = 1$, so that $f(1) \neq 0$. Moreover, we see from this equation that $f^{-1}(1)$ is completely determined by $f(1)$.

Now assume $f(1) \neq 0$. We will construct f^{-1} by induction, that is, we will explicitly define $f^{-1}(n)$ by induction on n. As noted above, $f^{-1}(1)$ is given by $f(1)f^{-1}(1) = 1$. Now assume that $n > 1$ and that $f^{-1}(i)$ is defined for all $1 \le i < n$. Then the equation

$$0 = I(n) = f * f^{-1}(n) = f(1)f^{-1}(n) + \sum_{\substack{1 \le d < n \\ d|n}} f^{-1}(d)f(n/d)$$

determines $f^{-1}(n)$ uniquely.

Lemma 2: We have $\mu * U = I$.

Proof: This amounts to saying that

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

This is obviously the case when $n = 1$, so suppose that $n > 1$ and write $n = p^e m$ where p is a prime, e and m are positive integers and $p \nmid m$. Now we have

$$\sum_{\substack{1 \le d \le n \\ d|n}} \mu(d) = \sum_{\substack{1 \le d \le n \\ d|m}} \mu(d) + \sum_{\substack{1 \le d \le n \\ d|m}} \mu(dp) = 0.$$

Lemma 3 ("Möbius Inversion"): If f and g are arithmetic functions with $g = U * f$, then $f = \mu * g$. In other words, if

$$g(n) = \sum_{d|n} f(d),$$

then

$$f(n) = \sum_{d|n} \mu(d) g(n/d).$$

Proof: By associativity of convolution and Lemma 2,

$$\mu * \big(U * f\big) = \big(\mu * U\big) * f = I * f = f.$$

Theorem: The multiplicative functions form an abelian group under convolution.

Proof: All that remains is to show that the set of multiplicative functions is closed under convolution and taking inverses. Suppose f and g are multiplicative functions and m and n are relatively prime positive integers. Then

$$\begin{aligned} f * g(mn) &= \sum_{\substack{1 \le d \le mn \\ d|mn}} f(d) g(mn/d) \\ &= \sum_{\substack{1 \le d_1, d_2 \le mn \\ d_1|m \\ d_2|n}} f(d_1 d_2) g(mn/d_1 d_2) \\ &= \sum_{\substack{1 \le d_1, d_2 \le mn \\ d_1|m \\ d_2|n}} f(d_1) f(d_2) g(m/d_1) g(m/d_2) \\ &= \big(f * g(m)\big)\big(f * g(n)\big), \end{aligned}$$

since d_1 and d_2 are necessarily relatively prime above, as are m/d_1 and n/d_2.

Finally, since f is multiplicative we must have $f(1) = 1$, so that f^{-1} exists (and is unique) by Lemma 1. Set

$$g(n) := \prod_{\substack{p|n \\ p \text{ prime}}} f^{-1}(p^{\mathrm{ord}_p(n)}),$$

where $\mathrm{ord}_p(n)$ denotes the exact power of the prime p that divides n. This function g is multiplicative by definition and agrees with f^{-1} on prime powers. By what we have already shown, $f * g$ is multiplicative. Since $g(m) = f^{-1}(m)$ whenever m is a prime power, we immediately get $f * g(m) = f * f^{-1}(m) = I(m)$

whenever m is a prime power. But I is multiplicative, so the two multiplicative functions $f * g$ and I must be equal since they agree on prime powers. Since f^{-1} was unique, we must have $g = f^{-1}$, so that f^{-1} is multiplicative.

The Theorem can be a useful tool to show that a function is multiplicative. For example, we have

$$E * U(n) = \sum_{\substack{1 \le d \le n \\ d|n}} E(d)U(n/d) = \sum_{\substack{1 \le d \le n \\ d|n}} d = \sigma(n),$$

so that the divisor sum σ is multiplicative.

Lemma 4: We have $\phi = E * \mu$. In particular, ϕ is multiplicative.

Proof: We have $\phi * U(n) = \sum_{d|n} \phi(d)$. Consider the set of rational numbers $\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\}$. This is a set of n distinct elements, each of which has a unique representation of the form $\frac{a}{d}$, where $a < d$ is a positive integer relatively prime to d and $d|n$. Since there are exactly $\phi(d)$ such representations with a given denominator d, we get $\sum_{d|n} \phi(d) = n$. Hence $\phi * U = E$, so that $\phi = E * \mu$ by Lemma 2. Therefore ϕ is a multiplicative function, since it is the convolution of two multiplicative functions.

One last arithmetic function we'll define here is the *von Mangoldt Lambda function*. It is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^r \text{ for some prime } p \text{ and non-negative integer } r, \\ 0 & \text{otherwise.} \end{cases}$$

This function will be used extensively in our investigations into the prime counting function. Though it isn't multiplicative (since $\Lambda(1) = 0$), it still has some interesting convolution properties. To wit:

$$\begin{aligned} \Lambda * U(n) &= \sum_{\substack{1 \le d \le n \\ d|n}} \Lambda(d)U(n/d) \\ &= \sum_{\substack{1 \le d \le n \\ d|n}} \Lambda(d) \\ &= \sum_{\substack{p^r|d \\ p \text{ prime}}} \log p \\ &= \sum_{i=1}^{l} \sum_{r=1}^{e_i} \log p_i \qquad \text{where } n = p_1^{e_1} \cdots p_l^{e_l} \\ &= \sum_{i=1}^{l} e_i \log p_i \\ &= \log n. \end{aligned}$$

Therefore, by Möbius Inversion and Lemma 2

$$\begin{aligned}
\Lambda(n) &= \mu * \log(n) \\
&= \sum_{\substack{1 \le d \le n \\ d|n}} \mu(d) \log(n/d) \\
&= \sum_{\substack{1 \le d \le n \\ d|n}} \mu(d) \log n - \sum_{\substack{1 \le d \le n \\ d|n}} \mu(d) \log d \\
&= \log n \sum_{\substack{1 \le d \le n \\ d|n}} \mu(d) - \sum_{\substack{1 \le d \le n \\ d|n}} \mu(d) \log d \\
&= \log 1 - \sum_{\substack{1 \le d \le n \\ d|n}} \mu(d) \log d \\
&= - \sum_{\substack{1 \le d \le n \\ d|n}} \mu(d) \log d.
\end{aligned}$$