Multiplicative Number Theoretic Functions, Part 2

0 Review of Previous Session

Let us review some of the material from Part 1, which we discussed in our previous session on January 26. We let $\mathbb{Z}/n\mathbb{Z}$ denote the system of integers modulo n (or, more simply, "mod n"). Identify this as $\mathbb{Z}/n\mathbb{Z} := \{0, 1, \ldots, n-1\}$.[1] We are interested in the *units* modulo n, and especially how many units mod n exist as a function of n:

Definition 0.1. Let n be a positive integer with $n \geq 2$. We say that an integer a is a *unit modulo n* if and only if there exists some integer b such that $ab \equiv 1 \pmod{n}$. We call b the *multiplicative inverse of a modulo n*.

Notation:. $U(\mathbb{Z}/n\mathbb{Z})$ shall denote the collection of all units modulo n. The size of $U(\mathbb{Z}/n\mathbb{Z})$ shall be denoted by $|U(\mathbb{Z}/n\mathbb{Z})|$. By convention, for $n := 1$, we set $|U(\mathbb{Z}/1\mathbb{Z})| := 1$.

We determined the following in our last session:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\lvert U(\mathbb{Z}/n\mathbb{Z})\rvert$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6

Proposition 0.2. *Let a, n be integers with $n > 1$. If $\gcd(a, n) > 1$, then a is* not *a unit mod n. That is, if a and n share a common factor greater than 1, then a cannot be a unit mod n.*

Conjecture 0.3. *Let a, n be integers with $n > 1$. If $\gcd(a, n) = 1$, then a is a unit mod n. That is, we conjecture that a is a unit mod n* if and only if $\gcd(a, n) = 1$.

Corollary 0.3(a). *Let p be a positive prime. Then $U(\mathbb{Z}/p\mathbb{Z}) = \{1, 2, \ldots, p-1\}$.*

Proposition 0.4. *If n is a positive integer with $n \geq 3$, then $|U(\mathbb{Z}/n\mathbb{Z})|$ must be even.*

Definition 0.5. Let n be a positive integer. We define the set F_n by

$$F_n := \left\{ \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n} \right\}. \tag{0.1}$$

That is, F_n consists of all fractions in the interval $(0, 1]$ with denominator n (with such fractions *not* necessarily reduced to lowest terms).

[1] The "proper" way to think of $\mathbb{Z}/n\mathbb{Z}$ is more nuanced than this. For example, we have $4 \equiv 9 \equiv -1 \pmod{5}$. Thinking of $\mathbb{Z}/n\mathbb{Z}$ as the set $\{0, 1, \ldots, n-1\}$, while an abuse of notation, avoids a digression that's unnecessary for our purposes here.

What happens when we take the fractions in F_n and reduce them to lowest terms?

Proposition 0.6. *Let n be a positive integer. If we take all the elements of F_n and reduce them to lowest terms, then a denominator d is represented if and only if $d|n$. That is, d is a lowest-terms denominator in F_n if and only if d divides n.*[2]

Proposition 0.7. *Let n be a positive integer, and let $\text{denom}_n(d)$ denote the number of elements in F_n have lowest-terms denominator d. Then*

$$\sum_{d|n} \text{denom}_n(d) = n. \tag{0.2}$$

Here, this notation means that we sum over all positive divisors d of n.

Conjecture 0.8. *Let d, n be positive integers. Then*

$$\text{denom}_n(d) = \begin{cases} 0, & \text{if } d \nmid n \\ |U(\mathbb{Z}/n\mathbb{Z})|, & \text{if } d \mid n. \end{cases} \tag{0.3}$$

1 Multiplicative Functions: Definition and Classical Examples

When considering a function f on $\mathbb{Z}$, the set of all integers, (or on $\mathbb{N}$, the set of all natural numbers,) it can often be illuminating to understand how to compute values like $f(p^k)$ for positive primes p and nonnegative integers k. For a *multiplicative* function f on $\mathbb{N}$, knowing just these values of $f(p^k)$ will completely determine the entire function. Put differently: multiplicative functions are *very* well-behaved with respect to prime factorizations, so it is worth understanding the properties of such functions. We shall motivate this by considering certain natural functions which, as we shall see, turn out to be multiplicative. We then consider more examples of classical functions, Dirichlet convolution, and Möbius inversion.

Definition 1.1. Let $f : \mathbb{N} \to \mathbb{C}$ be a function from the natural numbers to the complex numbers.[3] Then we say that f is *multiplicative* if and only if for every $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$, $f(mn) = f(m)f(n)$.

If $f(mn) = f(m)f(n)$ for *all* $m, n \in \mathbb{N}$, we say that f is *totally multiplicative* (or *strongly multiplicative*).

[2] Equivalently: d is a *divisor* of n, d is a *factor* of n, or n is a *multiple* of d.

[3] *Note:* Since $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{R} \subseteq \mathbb{C}$, such a function need not attain any nonreal complex values in principle. Letting the target of f be the complex numbers, though, allows for a more flexible definition.

Example 1.2. Let $\mathbf{1}\colon \mathbb{N} \to \mathbb{C}$ be the constant function $f(n) := 1$ for all $n \in \mathbb{N}$. Then f is totally multiplicative.

Example 1.3. Let $\mathrm{id}\colon \mathbb{N} \to \mathbb{N}$ be the *identity function* defined by $\mathrm{id}(n) := n$ for all $n \in \mathbb{N}$. Then id is multiplicative. More generally, for all $k \in \mathbb{N}$, the kth-power function function $f_k\colon \mathbb{N} \to \mathbb{N}$, defined by $f_k(n) := n^k$, is also totally multiplicative.

Example 1.4. Let $I\colon \mathbb{N} \to \mathbb{C}$ be the function defined by

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

Then I is totally multiplicative.

Example 1.5. Let $\varphi\colon \mathbb{N} \to \mathbb{N}$ be the function defined by

$$\varphi(n) := |\{k \in \mathbb{N} : 1 \le k \le n \text{ and } \gcd(k,n) = 1\}|. \tag{1.1}$$

(Compare this to the results for $|U(\mathbb{Z}/n\mathbb{Z})|$ and $\mathrm{denom}_n(d)$ in Section #0.) Then φ is multiplicative but not totally multiplicative. (We shall prove the former claim soon. You should be able to provide a counterexample to total multiplicativity yourself.)

Example 1.6. Let $k \in \mathbb{N}$. Define the functions $\tau, \sigma, \sigma_k\colon \mathbb{N} \to \mathbb{N}$ by

$$\begin{aligned} \tau(n) &:= \text{the number of positive integer} \\ &\quad\ \text{divisors of } n \text{ (including 1 and } n) \\ &= |\{d \in \mathbb{N} : d \mid n\}| \\ &= \sum_{d \mid n} 1 \\ \sigma(n) &:= \sum_{d \mid n} d \\ \sigma_k(n) &:= \sum_{d \mid n} d^k. \end{aligned}$$

Then each of these functions is multiplicative but not totally multiplicative.

We have, for example

$$\begin{aligned} \tau(12) &= |\{1,2,3,4,6,12\}| = 1+1+1+1+1+1 \\ &= 6 \\ \sigma(12) &= 1+2+3+4+6+12 = 28 \\ \sigma_3(12) &= 1^3+2^3+3^3+4^3+6^3+12^3 = 1+8+27+64+216+1728 \\ &= 2044. \end{aligned}$$

We now explore properties of multiplicative functions and deduce that certain classical number theoretic functions are multiplicative.

1.1. Let $n \in \mathbb{N}$. If $n \geq 2$, write the prime factorization of n as

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \tag{1.2}$$

where the p_j are distinct positive integer primes, and each a_k is a positive integer. Prove that if $f : \mathbb{N} \to \mathbb{C}$ is multiplicative, then

$$f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k}). \tag{1.3}$$

Further, if f is totally multiplicative, then

$$f(n) = f(p_1)^{a_1} f(p_2)^{a_2} \cdots f(p_k)^{a_k}. \tag{1.4}$$

1.2. PODASIP[4]: If f is a multiplicative function, then $f(1) = 1$.

1.3. PODASIP: Let f be a multiplicative function. Then the sum function S_f defined by

$$S_f(n) := \sum_{d|n} f(d) \tag{1.5}$$

is also multiplicative. If f is totally multiplicative, is S_f also totally multiplicative?

[4]Borrowed from the Ross Mathematics Program, “PODASIP” is an acronym for “Prove Or Disprove, And Salvage If Possible”. (The “If” in “Salvage If Possible” is a bit misleading, since it is understood that *every* false statement admits a relevant, nontrivial salvage.

1.4. Prove that τ, σ, and σ_k are all multiplicative functions.

1.5. Produce formulas for τ and σ. (*Note:* as is common with many functions arising in number theory, it will be natural to express your formulas for $\tau(n)$ and $\sigma(n)$ in terms of the prime factorization of n.)

1.6. Define the function $\mu\colon \mathbb{N} \to \mathbb{N}$ by

$$\mu(n) := \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if there exists a prime } p \text{ such that } p^2 \mid n \\ (-1)^k, & \text{if } n = p_1 p_2 \cdots p_k, \text{ where the } p_j \text{ are distinct positive primes.} \end{cases}$$

Compute the value of $\mu(n)$ for some sample values of n.

PODASIP: μ is a totally multiplicative function.

What is S_μ, the sum function of μ?

2 Dirichlet Convolution and Möbius Inversion

Next, we consider some new operations on functions.

Definition 2.1. Let $f, g\colon \mathbb{N} \to \mathbb{C}$ be functions. Then the *convolution* (or *Dirichlet convolution*) of f with g, denoted $f * g$, is a function defined by

$$f * g(n) := \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right). \tag{2.1}$$

Definition 2.2. Let $f\colon \mathbb{N} \to \mathbb{C}$ be a function. Then the *Möbius inversion function* of f is the function $f * \mu$. That is, the Möbius inversion is defined by

$$\sum_{d \mid n} f(d) \mu\left(\frac{n}{d}\right). \tag{2.2}$$

Example 2.3. Consider $f := \mathrm{id}$, $g := \mu$. Let's compute $f * g(12)$.

$$\begin{aligned}
f * g(12) &= \mathrm{id} * \mu(12) \\
&= \sum_{d|12} \mathrm{id}(d)\mu\left(\frac{n}{d}\right) \\
&= \sum_{d|12} d\mu\left(\frac{n}{d}\right) \\
&= 1 \cdot \mu(12) + 2 \cdot \mu(6) + 3 \cdot \mu(4) + 4 \cdot \mu(3) + 6 \cdot \mu(2) + 12 \cdot \mu(1) \\
&= 1 \cdot 0 + 2 \cdot 1 + 3 \cdot 0 + 4(-1) + 6(-1) + 12 \cdot 1 \\
&= 0 + 2 + 0 - 4 - 6 + 12 \\
&= 4.
\end{aligned}$$

That is, the Möbius inversion function of the identity function, evaluated at $n = 12$, yields 4.

2.1. PODASIP: For all $f, g, h \colon \mathbb{N} \to \mathbb{C}$, we have $f * g = g * f$, and $(f * g) * h = f * (g * h)$. That is, convolution is both commutative and associative.

   Note: We make no assumptions here about the multiplicativity of any of these functions.

2.2. PODASIP: Let $f \colon \mathbb{N} \to \mathbb{C}$. If I is as above, then $f * I = f$. That is, I is an identity for the convolution operation: convolve any function f with I, and you return the original function f.

2.3. Let $f \colon \mathbb{N} \to \mathbb{C}$, and define its sum function $S_f \colon \mathbb{N} \to \mathbb{C}$ via

$$S_f(n) := \sum_{d|n} f(d).$$

   Prove that for all $n \in \mathbb{N}$,

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

   That is, $S_f * \mu = f$.

2.4. PODASIP: If $f, g\colon \mathbb{N} \to \mathbb{C}$ are multiplicative, then their convolution $f * g$ is also multiplicative.

2.5. Let φ be as in Example #1.5. Prove that $\varphi = \mathrm{id} * \mu$. That is, for all $n \in \mathbb{N}$,

$$\begin{aligned}\varphi(n) &= \sum_{d|n} d\mu\left(\frac{n}{d}\right)\\ &= \sum_{d|n} \frac{n\mu(d)}{d}.\end{aligned}$$

2.6. PODASIP: φ is a multiplicative function.

Can you find a formula for $\varphi(n)$ in terms of its prime factorization?

2.7. For $n \in \mathbb{N}$, compute

$$s(n) := \sum_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} k.$$

in terms of n and the classical functions we have introduced thus far. That is, for a given positive integer we sum over all positive integers k between 1 and n (inclusive) such that k is relatively prime to n.

2.8. For $n \in \mathbb{N}$, compute

$$p(n) := \prod_{d|n} d$$

in terms of n and the classical functions we have introduced thus far.

3 Generalizations and Further Explorations

3.1. PODASIP: For all $n \in \mathbb{N}$, $\varphi(n^2) = n\varphi(n)$.

3.2. PODASIP: Let $n \in \mathbb{N}$ be a composite number. Then $\varphi(n) < n - \sqrt{n}$.

3.3. PODASIP: Let $f : \mathbb{N} \to \mathbb{C}$ be any function, and define its product function $P_f : \mathbb{N} \to \mathbb{C}$ by

$$P_f(n) := \prod_{d|n} f(n).$$

Then

$$\begin{aligned} f(n) &= \prod_{d|n} P_f(d)^{\mu(n/d)} \\ &= \prod_{d|n} P_f\left(\frac{n}{d}\right)^{\mu(d)}. \end{aligned}$$

4 Dirichlet Series of Multiplicative Functions

The following section, which is optional, will use some ideas concerning infinite series, providing one generalization of the Riemann zeta function. For this section, rigorous proofs about convergence will not be necessary. For those of you already familiar with these ideas, know that they can be made rigorous, subject to certain constraints on the domain. For our purpose, though, it will suffice to get the big-picture sense of how certain infinite series can be represented as infinite products, and we can use this equality to gain additional insight into the classical number theoretic functions.

Definition 4.1. The *Riemann zeta function* is the function

$$\begin{aligned}\zeta\colon (1,+\infty) &\to \mathbb{R} \\ \zeta(s) &:= \sum_{n=1}^{\infty} \frac{1}{n^s} \\ &= \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots\end{aligned}$$

Example 4.2. We have that

$$\begin{aligned}\zeta(2) &:= \sum_{n=1}^{\infty} \frac{1}{n^2} \\ &= \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \cdots \\ &= \frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots\end{aligned}$$

It is beyond the scope of this worksheet, but it can be shown that $\zeta(2) = \pi^2/6$.

Definition 4.3. Let $f\colon \mathbb{N} \to \mathbb{C}$ be a function. The *Dirichlet series for f* is the series

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} == \frac{f(1)}{1^s} + \frac{f(2)}{2^s} + \frac{f(3)}{3^s} + \frac{f(4)}{4^s} + \frac{f(5)}{5^s} + \cdots \tag{4.1}$$

Example 4.4. The Dirichlet series for φ is

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} &= \frac{\varphi(1)}{1^s} + \frac{\varphi(2)}{2^s} + \frac{\varphi(3)}{3^s} + \frac{\varphi(4)}{4^s} + \frac{\varphi(5)}{5^s} + \frac{\varphi(6)}{6^s} + \cdots \\ &= \frac{1}{1^s} + \frac{1}{2^s} + \frac{2}{3^s} + \frac{2}{4^s} + \frac{4}{5^s} + \frac{2}{6^s} + \cdots\end{aligned}$$

4.1. Show that

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}. \tag{4.2}$$

Hint: Use the geometric series

$$1 + r + r^2 + r^3 + r^4 + \cdots = \frac{1}{1-r}$$

for $|r| < 1$.

4.2. Let $f, g\colon \mathbb{N} \to \mathbb{C}$ be functions. Show that

$$\left(\sum_{n=1}^{\infty} \frac{f(n)}{n^s}\right) \cdot \left(\sum_{n=1}^{\infty} \frac{g(n)}{n^s}\right) = \sum_{n=1}^{\infty} \frac{f * g(n)}{n^s}. \tag{4.3}$$

Here, $f * g$ is the Dirichlet convolution as given in Definition #2.1.

4.3. let $f\colon \mathbb{N} \to \mathbb{C}$ be a multiplicative function. Then we have

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \text{ prime}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \frac{f(p^3)}{p^{3s}} + \cdots\right). \tag{4.4}$$

Note: Exercise #4.1 is a special case of this claim.

4.4. Show that

$$\sum_{n=1} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}. \tag{4.5}$$

That is, the Dirichlet series for μ is $\frac{1}{\zeta}$.

4.5. Show the following:

(a)

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

(b)

$$\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = [\zeta(s)]^2.$$

(c)

$$\sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}.$$