Multiplicative Number Theoretic Functions

1 Introduction to Multiplicative Functions

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 $\mathbb{N}$ (whose definition will appear in a subsequent section), 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.

Borrowing a method from the Ross Mathematics Program at The Ohio State University, we shall include some "PODASIP" exercises, an acronym for "Prove Or Disprove, And Salvage If Possible".[1] That is, you will be given an assertion, and you will have to determine whether it is true. If it is true, provide a proof justifying why. If it is false, provide a counterexample to demonstrate the assertion's falsity, and *salvage* the original statement by amending it to a true statement relevant to the original—then prove the newly-salvaged statement.

Example 1.1. PODASIP: If p is a positive prime, then p is odd.

This is *false*: $p = 2$ is both prime, but 2 is even.

Possible Salvage: If p is a positive prime and $p > 2$, then p is odd.

Proof of Salvage:

It suffices to prove that if $n > 2$ is even, then n is *not* a prime number. If $n > 2$ is even, then by definition of being even, $n = 2k$ for some integer k. Further, since $n > 2$, we must have $k > 1$. Then $n = 2k$ is a nontrivial factorization of n, so n must be composite, whence n is not prime. □

Remark. Note that there is no *unique* salvage for a given false assertion. As a general rule, though, try to find a salvage that is relevant to the original statement and ideally one whose truth is as ambitious to prove as you can manage. A salvage like "If $p := 2$, then p is even" is certainly true, but it is not in the spirit of being a meaningful salvage to the original—false–statement in Example #1.1.

[1] The "If" in "Salvage If Possible" is a bit misleading, since it is understood at the Ross program that *every* false statement admits a relevant, nontrivial salvage.

Other exercises will simply as you to make a *conjecture*. If you can prove your conjecture, great! The purpose here of forming conjectures, though, is more for you to experiment with these ideas and concepts.

2 Counting Units Modulo n

Most of you should be familiar with modular arithmetic, something we've explored in many previous Math Circle sessions. (*Note:* If you are unfamiliar with modular arithmetic, that's fine! Just get the attention of a volunteer quickly so we can get you caught up.)

Let $\mathbb{Z}/n\mathbb{Z}$ denote the system of integers modulo n (or, more simply, "mod n"). We shall typically represent this as $\mathbb{Z}/n\mathbb{Z} := \{0, 1, \ldots, n-1\}$.[2] We begin this session by considering units modulo n:

Definition 2.1. 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.

Example 2.2. We have that 2 is a unit modulo 5, since $2 \cdot 3 = 6 \equiv 1 \pmod{5}$. That is, for $n := 5$ and $a := 2$, we have that $b := 3$ is a multiplicative inverse for 2 modulo 5.

Further, one can verify that writing $\mathbb{Z}/n\mathbb{Z}$ as $\{0, 1, 2, 3, 4\}$, we have that $U(\mathbb{Z}/n\mathbb{Z}) = \{1, 2, 3, 4\}$.

Example 2.3. Conversely, 2 is *not* a unit modulo 10 because there is no way to solve the congruence $2b \equiv 1 \pmod{10}$ for an integer b. (Can you see why?)

Further, with the standard notation above for $\mathbb{Z}/10\mathbb{Z}$, we have $U(\mathbb{Z}/12\mathbb{Z}) = \{1, 3, 7, 9\}$. (Try to verify that each of these is a unit mod 10, and that nothing else is a unit mod 10.)

To build our understanding and intuition about units modulo n, we shall begin with some basic numerical examples:

2.1. What are all the units modulo 3? How many distinct units (modulo 3 are there?

[2] 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.

2.2. What are all the units modulo 5? How many distinct units (mod 5) are there?

2.3. Repeat the questions for Exercises #2.1 and #2.2 for $n = 9$, $n = 11$, $n = 12$, and $n = 15$, respectively.

2.4. *Notation:* For a positive integer $n \geq 2$, let $U(\mathbb{Z}/n\mathbb{Z})$ denote the collection of all units modulo n (which are themselves distinct mod n). Compute the sizes $|U(\mathbb{Z}/n\mathbb{Z})|$ for all positive integers n with $2 \leq n \leq 24$. What patterns do you notice?

2.5. PODASIP: Let n be a positive integer with $n \geq 2$. Then $|U(\mathbb{Z}/n\mathbb{Z})|$ is always even.

2.6. Let n be a positive integer with $n \geq 2$, and let a be any integer. Can you provide a criterion—at least as a conjecture—which characterizes precisely when a is a unit modulo n? (Even better: can you *prove* your conjecture is valid?)

2.7. *Conjectures:* Let p be a positive prime integer. What is $|U(\mathbb{Z}/p\mathbb{Z})|$? (That is, how many distinct units are there modulo p?) Can you generalize to compute $|U(\mathbb{Z}/n\mathbb{Z})|$ for composite values of n? (For example: what if $n = p^k$, where p is a positive prime and k is a positive integer with $k \geq 2$? What if $n = pq$, where p, q are *distinct* positive primes?)

3 Fractions with Denominator n

The following section will explore what appears to be a different question concerning finite sequences of fractions. We shall later see, however, that the results from this section are closely related to those in Section 2.

Definition 3.1. Let n be a positive integer. We define the set F_n by

$$F_n := \left\{ \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n} \right\}. \tag{3.1}$$

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).

Example 3.2. For $n := 6$, we have

$$\begin{aligned} F_n &= \left\{ \frac{1}{6}, \frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{5}{6}, \frac{6}{6} \right\} \\ &= \left\{ \frac{1}{6}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{5}{6}, \frac{6}{6} \right\}. \end{aligned}$$

In this section's exercises, we are interested in what happens when, for a fixed positive integer n, we take all the fractions in F_n and reduce them to lowest terms.

3.1. Write down F_{12}, both as a list of fractions with denominator 12 and reduced to lowest terms. What denominators appear in the lowest-terms representation of F_{12}? How many times does each denominator appear?

3.2. Repeat the above for F_{13} and F_{15}, respectively

3.3. Let n be a positive integer. Which positive integers d appear as denominators in the lowest-terms representation of F_n? Try to give a criterion which says which d *do* appear as a lowest-terms denominator in F_n, and which d *do not* appear as a lowest-terms denominator.

Suggestion: Consider some simple examples. Is it possible, say, for 4 to appear as a lowest-terms denominator in F_{10}? What about F_8?

3.4. Let n be a fixed positive integer, and for any positive integer, let $\text{denom}(d)$ denote the number of elements in F_n of lowest-terms denominator d. (If we wish to emphasize that we are considering how $\text{denom}(d)$ might, *a priori*, depend upon n, we may use the more explicit notation $\text{denom}_n(d)$.)

If $\text{denom}(d) \neq 0$, does the value of $\text{denom}(d)$ depend upon n? Why or why not?

3.5. Compute, with justification,

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

Here, we are summing the values $\text{denom}_n(d)$ over all positive integers d such that $d \mid n$. (This notation means that d divides n; equivalently, d is a factor of n, or n is a multiple of d.)

3.6. Let n be a positive d and n be positive integers. How can we express $\text{denom}_n(d)$ in terms of the size of the unit groups in Section #2? Make a conjecture.

4 Multiplicative Functions: Definition and Classical Examples

Here, we define a multiplicative function, present a number of the classical examples of multiplicative functions, and explore their properties.

Definition 4.1. 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*).

Example 4.2. Let $\mathbf{1} : \mathbb{N} \to \mathbb{C}$ be the constant function $f(n) := 1$ for all $n \in \mathbb{N}$. Then f is totally multiplicative.

Example 4.3. Let $\mathrm{id} : \mathbb{N} \to \mathbb{N}$ 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 $f_k : \mathbb{N} \to \mathbb{N}$, defined by $f_k(n) := n^k$, is also totally multiplicative.

Example 4.4. Let $I : \mathbb{N} \to \mathbb{C}$ be the function defined by

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

Then I is also totally multiplicative.

Example 4.5. Let $\varphi : \mathbb{N} \to \mathbb{N}$ be the function defined by

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

(Compare this to results from Section #3.) 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.)

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

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

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \tag{4.1}$$

[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.

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

$$f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k}). \tag{4.2}$$

Further, if f is totally multiplicative, then

$$f(n) = f(p_1)^{a_1} f(p_2)^{a_2} \cdots f(p_k)^{a_k}. \tag{4.3}$$

4.2. PODASIP: If f is a multiplicative function, then $f(1) = 1$.

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

$$S_f(n) := \sum_{d|n} f(d) \tag{4.4}$$

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

Note: We are summing over only the positive divisors of n, not all positive integers from 1 to n.

4.4. Let $k \in \mathbb{N}$. Define the functions $\tau, \sigma, \sigma_k: \mathbb{N} \to \mathbb{N}$ by

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

(Compute values of $\tau(n)$ and $\sigma(n)$ for sample small values of n to ensure you understand these definitions.)

PODASIP: τ, σ, and σ_k are all multiplicative functions.

4.5. Produce formulas for τ and σ.

4.6. 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?

Next, we consider some new operations on functions.

Definition 4.6. 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

$$f * g(n) := \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right). \tag{4.5}$$

Definition 4.7. 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

$$\sum_{d \mid n} f(d) \mu\left(\frac{n}{d}\right). \tag{4.6}$$

Example 4.8. Consider $f := \mathrm{id}$, $g := \mu$. Let's compute $f * g(12)$.

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

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

4.1. 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.

4.2. 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

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

4.4. Let φ be as in Example #4.5. Prove that $\varphi = \mathrm{id} * \mu$. That is, for all $n \in \mathbb{N}$,

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

4.5. PODASIP: φ is a multiplicative function.

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