Math 1560 - Notes 2

Ian Benway

February 2022

1 Arithmetic Functions

An **arithmetic function** is a function $f : \mathbb{Z}_+ \to \mathbb{C}$. (Typically, these are integer-valued.)
Examples:

- Euler ϕ function
- $\tau(n) = \sum_{d|n} 1$
- $\sigma(n) = \sum_{d|n} d$

An arithmetic function f is **multiplicative** if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$.
f is said to be totally or completely multiplicative if $f(mn) = f(n)$ for all $m, n \in \mathbb{Z}_+$.

If f is multiplicative and $n_1, \ldots, n_k$ are positive pairwise coprime integers, then $f(n_1, \ldots, n_k) = f(n_1)f(n_2)(n_k)$.
A particularly useful case is when $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ so that we have $f(n) = f(p_1^{e_1})f(p_2^{e_2}) \ldots f(p_k^{e_k})$.

A common type of arithmetic function is a **summatory function**, namely of the form

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

where g is some arithmetic function.

Food for Thought: How special are summatory functions in the set of all arithmetic function?

A good slogan, which we formalize in the following lemma, is:

"Summatory functions inherit multiplicativity."

Lemma 1. *If g is a multiplicative function, and*

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

for all n, then f is multiplicative.

Proof. Suppose $m,n \in \mathbb{Z}$ are coprime. The divisors d of mn are the products $a \cdot b$ where $a|m$ and $b|n$. Each such pair (a,b) uniquely determines $d = a \cdot b$; conversely, since $(m,n) = 1$, each divisor d of mn determines a unique $a = (d,m)$ and $b = (d,n)$ so that $d = ab$. Thus, there exists a bijection

$$d|mn \overset{1\text{–}1}{\longleftrightarrow} (a|m, b|n).$$

Hence,

$$\begin{aligned} f(mn) &= \sum_{d|mn} g(d) \\ &= \sum_{d|m} \sum_{b|n} g(ab) \\ &= \sum_{a|m} \sum_{b|n} g(a)g(b) \\ &= (\sum_{a|m} g(a))(\sum_{b|n} g(b)) \\ &= f(m)f(n). \end{aligned}$$

□

Let's look again at our τ and σ functions.

$$\tau(n) = \sum_{d|n} 1 \qquad \sigma(n) = \sum_{d|n} d$$

So τ is the summatory function of the constant 1 function, and σ is the summatory function of the identity function. Hence, σ and τ are multiplicative functions.

Let p be a prime. Then $\tau(p^e) = e+1$ and $\sigma(p^e) = 1 + p + p^2 + \cdots + p^3 = \frac{p^{e+1}-1}{p-1}$. Therefore, if $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, then

$$\tau(n) = \prod_{i=1}^{k} (e_i + 1)$$

and

$$\sigma(n) = \prod_{i=1}^{k} (\frac{p_i^{e_{i+1}} - 1}{p_i - 1}).$$

Remark: There are higher order divisor functions:

$$\sigma_k(n) = \sum_{d|n} d^k$$

(so $\sigma_0 = \tau$, $\sigma_1 = \sigma$, etc.).

Review of $\mathbb{Z}/m\mathbb{Z}$

If $a,b,m \in \mathbb{Z}$ and $m \neq 0$, we say that a is congruent to b modulo m if $m|b-a$. We write $a \equiv b \mod m$.
Congruence mod m is an equivalence relation on $\mathbb{Z}$. If $a \in \mathbb{Z}$, $\bar{a}$ denotes the set of integers congruent to $a \mod m$, i.e. $\bar{a} = \{a+km | k \in \mathbb{Z}\}$.
The set of congruence classes mod m is denoted $\mathbb{Z}/m\mathbb{Z}$. If $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_m$ form a complete set of congruence classes mod m, then $\{a_1, a_2, \ldots, a_m\}$ is called a **complete set of residues mod** m.

$\mathbb{Z}/m\mathbb{Z}$ can be endowed with the structure of a commutative ring by setting

$$\bar{a} + \bar{b} = \overline{a+b}$$

and

$$\bar{a} \cdot \bar{b} = \overline{ab},$$

and proving this is well-defined.

Proposition 1. *The set of units in $\mathbb{Z}/m\mathbb{Z}$ is exactly $\{\bar{a} : (a,m) = 1\}$.*

Proof. Let $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$. Then the exists some $b \in \mathbb{Z}/m\mathbb{Z}$ such that $\bar{b} \cdot \bar{a} \equiv 1 \mod m \Leftrightarrow$ There exists some $b,n \in \mathbb{Z}$ such that $ba - mn = 1 \Leftrightarrow (a,m) = 1$ (by Bézout's Identity, see homework). □

The Euler ϕ Function
For $n \in \mathbb{Z}_+$, $\phi(n) =$ the number of integers $1 \leq m \leq n$ such that $(m,n) = 1$.
Examples:

- $\phi(1) = 1$
- $\phi(p) = p-1$ for any prime p
- $\phi(p^e) = p^e - p^{e-1}$ for prime p and $e \geq 1$

Theorem 1. *If $(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by the Chinese Remainder Theorem.

$$(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

Since $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$, the result follows. □

Here is an important fact about the Euler ϕ function:

Proposition 2.

$$\sum_{d|n} \phi(d) = n$$

Proof 1. Consider the n rational numbers $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}$ and reduce those to lowest terms so that the numerator and denominator are coprime.
Q: Given a positive divisor d of n, how many fractions have d as their denominator?
A: Exactly $\phi(d)$ of them.

Conversely, every denominator d is a divisor of n. Thus $n = \sum_{d|n} \phi(d)$. □

A good reflex for another proof:
Remember that summatory functions inherit multiplicity. So it suffices just to prove this holds for primes.
Let $n = p^k$. Let $f(n) = \sum_{d|n} \phi(d)$. Then $f(p^k) = \sum_{d|p^k} \phi(d) = 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) = p^k$.