Arithmetic Functions, $\phi(n)$, and Φ_n: Thoughts Surrounding Section 9.1

Definition. Let $\mathbb{N} = \{1, 2, 3, \ldots\}$. An *arithmetic function* is a function $f : \mathbb{N} \to \mathbb{C}$. We say an arithmetic function is *multiplicative* if $f(1) = 1$ and

$$\text{for all } m, n \in \mathbb{N} \text{ with } \gcd(m, n) = 1, \text{ we have } f(mn) = f(m)f(n).$$

Note that a multiplicative function f is completely determined by its values $f(p^n)$ on prime powers.

Simple Examples: You can easily check that the following arithmetic functions are multiplicative:

- Define $1(n) = 1$ for all $n \in \mathbb{N}$.
- Define $\epsilon(n)$ by $\epsilon(1) = 1$, and $\epsilon(n) = 0$ for $n \geq 2$.
- Define $\mathrm{id}(n) = n$.

They're simple, but all three of 1, ϵ, and id will be important on the next page.

The following function we've seen before is important in Chapter 9:
Definition. The *Euler phi-function* ϕ, also known as the Euler *totient* function, is

$$\phi : \mathbb{N} \to \mathbb{C} \qquad \text{by} \qquad \boxed{\phi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \left|\left\{j \in \{0, 1, \ldots, n-1\} \mid \gcd(j, n) = 1\right\}\right|}$$

Lemma [Lemma 9.1.1 in Cox.] Let ϕ denote the Euler ϕ-function. Then:
(a) ϕ is a multiplicative function with image contained in $\mathbb{N}$.
(b) $\phi(n) = n \prod_{p|n \text{ prime}} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1)$, where we factor $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ into distinct primes $p_1, \ldots p_k$, with integer powers $e_i \geq 1$.

Proof We have $\phi(1) = 1$ since $\mathbb{Z}/1\mathbb{Z} = (\mathbb{Z}/1\mathbb{Z})^\times = \{0\} = \{1\}$. [Or, if you prefer, since $\gcd(0, 1) = 1$.] By Exercise 9.1#2 (i.e., Homework 13, Problem 2), for $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, we have $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$, and hence

$$\phi(mn) = \left|(\mathbb{Z}/mn\mathbb{Z})^\times\right| = \left|(\mathbb{Z}/m\mathbb{Z})^\times\right| \cdot \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \phi(m)\phi(n).$$

Let p be a prime and $e \in \mathbb{N}$. Then for any $j = 0, 1, \ldots, p^e - 1$, we have $\gcd(j, p^e) \neq 1 \Leftrightarrow p|j$. Thus,

$$\phi(p^e) = \left|\{0, 1, \ldots, p^e - 1\}\right| - \left|\left\{pi \mid i \in \{0, 1, \ldots, p^{e-1} - 1\}\right\}\right| = p^e - p^{e-1} = p^{e-1}(p - 1).$$

Since ϕ is multiplicative, the second equation in (b) follows immediately; and the first follows by rewriting the second. □

FYI's on $\mathbb{Z}/n\mathbb{Z}$ and Exercise 9.1#2:
1. Exercise 9.1#2 allows you to assume that $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for $\gcd(m, n) = 1$. This is Lemma A.5.2, also known as the Chinese Remainder Theorem, since a version of it is originally due to the 4th century CE Chinese mathematician Sun Tzu (not to be confused with the far more famous 6th century BCE Chinese general Sun Tzu, author of *The Art of War*, a millennium earlier).

The isomorphism is given by $j + mn\mathbb{Z} \mapsto (j + m\mathbb{Z}, j + n\mathbb{Z})$. It's not hard to show that this map is a ring homomorphism and (using the fact that $\gcd(m, n) = 1$) injective. Since both rings have order mn, then by the pigeonhole principle, it's also surjective. What Sun Tzu did was give an explicit formula for the *inverse* isomorphism, at least for $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/105\mathbb{Z}$.

2. For $p \geq 3$, it is a fact that $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is a **cyclic** group (of order $p^{e-1}(p-1)$). [When $p = 2$, $(\mathbb{Z}/2\mathbb{Z})^\times$ and $(\mathbb{Z}/4\mathbb{Z})^\times$ are also cyclic, since they are of order 1 and 2, respectively.] However, for $p = 2$ and $e \geq 3$, we have $(\mathbb{Z}/2^e\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z})$, which is not cyclic.

Definition. Let f and g be arithmetic functions. The (*Dirichlet*) *convolution* $f * g$ of f and g is

$$f * g(n) = \sum_{d|n} f(d) g\left(\frac{d}{n}\right), \quad \text{where the sum is over all positive integers } d \text{ dividing } n.$$

Theorem. Arithmetic functions form a commutative ring with unity under the operations of $+$ and $*$. That is, $*$ is commutative, associative, and distributive ($f*(g+h) = f*g + f*h$), with multiplicative identity ϵ from the previous page ($f * \epsilon = f$). Moreover, if f and g are multiplicative, then so is $f * g$.

Proof. Left to reader. (It's really just a matter of rearranging sums, recognizing that d is a divisor of n if and only if n/d is also an integer and a divisor of n, and that kind of thing.) □

Fact: $\boxed{\phi * 1 = \mathrm{id}}$ That is, for all $n \in \mathbb{N}$, we have $\boxed{\sum_{d|n} \phi(d) = n}$ (This is challenge Exercise 9.1#11.)

Proof. (Sketch). Prove it for $n = p^e$ by hand; then we're done since $\phi * 1$ is multiplicative. □

Definition The *Möbius mu-function* is the multiplicative function $\mu : \mathbb{N} \to \mathbb{C}$ given by

$$\mu\left(p_1^{e_1} \cdots p_s^{e_s}\right) = \begin{cases} 0 & \text{if any } e_i \geq 2 \\ (-1)^s & \text{otherwise,} \end{cases} \qquad \text{where } p_1, \ldots, p_s \text{ are distinct primes.}$$

That is, $\mu(n)$ is 1 if n is a product of an even number of distinct primes, or -1 if n is a product of an odd number of distinct primes, of 0 if n has any repeated primes in its factorization.

Theorem. (Möbius Inversion Formula): Let f be an arithmetic function, and define $g = f * 1$, i.e., $g(n) = \sum_{d|n} f(d)$. Then $f = \mu * g$, i.e., $\boxed{g(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)}$

Proof. (Sketch). First, prove that $\mu * 1 = \epsilon$. (This is challenge Exercise 9.1#14.)
Thus, $f = f * \epsilon = \epsilon * f = (\mu * 1) * f = \mu * (1 * f) = \mu * (f * 1) = \mu * g$. □

Theorem. Let $n \geq 1$. Then the cyclotomic polynomial Φ_n is $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$.

Proof. This is Exercise 9.1#15 (Homework 13, Problem 4). LTR □

Example. The divisors of $n = 12$ are $d = 1, 2, 3, 4, 6, 12$. So

$$\begin{aligned} \Phi_{12}(x) &= (x-1)^{\mu(12)} (x^2-1)^{\mu(6)} (x^3-1)^{\mu(4)} (x^4-1)^{\mu(3)} (x^6-1)^{\mu(2)} (x^{12}-1)^{\mu(1)} \\ &= \frac{(x^{12}-1)(x^2-1)}{(x^6-1)(x^4-1)} = \frac{x^6+1}{x^2+1} = x^4 - x^2 + 1 \end{aligned}$$

As an aside for those who have seen some complex analysis: for an arithmetic function $a(n)$, one can form a **Dirichlet series** $\boxed{L(s) = \sum_{n \geq 1} \frac{a(n)}{n^s}}$ where $s \in \mathbb{C}$ is a complex variable. In many situations, this series converges (to an analytic function) on a complex half-plane $\mathrm{Re}(s) > c$.

If $a(n)$ is multiplicative, then the Dirichlet series can be rewritten as $\sum_{n \geq 1} \frac{a(n)}{n^s} = \prod_p \left(\sum_{j \geq 0} \frac{a(p^j)}{p^{js}} \right)$. This product, which is over all prime numbers $p \geq 2$, is called an **Euler product**.

For example, if $a(n) = 1$ for all n, then $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ is the **Riemann zeta-function**, which converges on the half-plane $\mathrm{Re}(s) > 1$, with Euler product $\zeta(s) = \prod_p \left(\sum_{j \geq 0} \frac{1}{p^{js}} \right) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$.