Arithmetic Functions, $\phi(n)$, and $\Phi_n$: 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 $\text{id}(n) = n$.

They’re simple, but all three of 1, $\epsilon$, and $\text{id}$ will be important on the next page.

The following function we’ve seen before is important in Chapter 9:

**Definition.** The *Euler-phi* function $\phi$, also known as the Euler *totient* function, is
\[
\phi : \mathbb{N} \to \mathbb{C} \quad \text{by} \quad \phi(n) = \left|\left\{(\mathbb{Z}/n\mathbb{Z})^\times\right\}\right| = \left|\left\{j \in \{0, 1, \ldots, n-1\} : \gcd(j, n) = 1\right\}\right|.
\]

**Lemma** Let $\phi$ denote the Euler $\phi$ function. Then:
- (a) $\phi$ is a multiplicative function with image contained in $\mathbb{N}$.
- (b) $\phi(n) = n \prod_{p \mid n \text{ prime}} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1)$, 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.** (Sketch; see also Lemma 9.1.1.) A quick check shows $\phi(1) = 1$. [Yes, really, it does, because $\mathbb{Z}/1\mathbb{Z} = (\mathbb{Z}/1\mathbb{Z})^\times = \{0\} = \{1\}$, and alternatively because $\gcd(0,1) = 1$.] By Exercise 9.1#2, for $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, we have $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$, 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 $\gcd(j, p^e) \neq 1 \iff p|j$. Thus,
\[
\phi(p^e) = \left|\{0, 1, \ldots, p^e - 1\}\right| = \left|\{pi : i \in \{0, 1, \ldots, p^{e-1} - 1\}\}\right| = p^e - p^{e-1} = p^{e-1}(p-1).
\]
Since $\phi$ is multiplicative, the second equation in (b) follows immediately; and the first follows by rewriting the second. □

**Notes on $\mathbb{Z}/n\mathbb{Z}$ and Exercise 9.1#2:**
1. (including a hint): Recall that if $R$ is a ring with 1, then $R^\times$ denotes the set of *units* of $R$, i.e., those elements of $R$ which have a multiplicative inverse. It is a simple fact, which you may assume, that $R^\times$ forms a group under multiplication. (This is Saracino Exercise 16.23, for example.) To do Exercise 9.1#2, I’d suggest you prove two basic facts about unit groups:
   - a. If $R \simeq S$, then $R^\times \simeq S^\times$.
   - b. $(R \times S)^\times = R^\times \times S^\times$.
   [To be clear, please prove these facts when you solve Exercise 9.1#2; do not assume them. Then use them to do the rest of the proof of the Exercise.]

2. Just FYI: Exercise 9.1#2 allows you to assume that $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ 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 \( \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/105\mathbb{Z} \).

3. Another FYI: As I mentioned in class some weeks ago when going off on a tangent, it is a fact that \((\mathbb{Z}/p^{e}\mathbb{Z})^*\) is a **cyclic** group (of order \( p^{e-1}(p - 1) \), provided \( p \geq 3 \), or provided \( p = 2 \) with \( e \leq 2 \). However, for \( p = 2 \) and \( e \geq 3 \), we have \((\mathbb{Z}/2^{n}\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z})\), which is not cyclic.

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

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

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

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

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

**Definition** The M"{o}bius-mu function is the multiplicative function \( \mu : \mathbb{N} \to \mathbb{C} \) given by

\[
\mu(p_1^{e_1} \cdots p_k^{e_k}) = \begin{cases} 
0 & \text{if any } e_i \geq 2 \\
(-1)^k & \text{otherwise},
\end{cases}
\]

where \( p_1, \ldots, p_k \) 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 \( g = f \ast 1 \), i.e.,

\[
g(n) = \sum_{d|n} f(d). \text{ Then } f = \mu \ast g, \text{ i.e., } g(n) = \sum_{d|n} \mu(d)g\left(\frac{n}{d}\right)
\]

**Proof.** (Sketch). We claim that \( \mu \ast 1 = \epsilon \). The proof of the claim is left to the reader. (See challenge Exercise 9.1#14; it’s not too hard, just a matter of good bookkeeping after writing \( n = p_1^{e_1} \cdots p_k^{e_k} \).) Thus, \( f = f \ast \epsilon = \epsilon \ast f = (\mu \ast 1) \ast f = \mu \ast (1 \ast f) = \mu \ast (f \ast 1) = \mu \ast g \).

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

**Proof.** (Idea; see challenge Exercise 9.1#15). Proposition 9.1.5 says \( x^n - 1 = \prod_{d|n} \Phi_d(x) \). Now apply ideas similar to Möbius inversion.

**Example.** The divisors of \( n = 12 \) are \( d = 1, 2, 3, 4, 6, 12 \). So

\[
\Phi_{12}(x) = (x - 1)^{\mu(12)}(x^2 - 1)^{\mu(6)}(x^3 - 1)^{\mu(4)}(x^4 - 1)^{\mu(3)}(x^6 - 1)^{\mu(2)}(x^{12} - 1)^{\mu(1)}
\]

\[
= \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = \frac{x^6 + 1}{x^2 + 1} = x^4 - x^2 + 1
\]