Euler Phi-Function

In section 1.1.3 of the text-book, Definition 1.3, the Euler phi-function is defined as follows.

**Definition 1.3** (Stinson) Suppose \( a \geq 1 \) and \( m \geq 2 \) are integers. If \( \gcd(a, m) = 1 \) then we say that \( a \) and \( m \) are relatively prime. The number of integers in \( \mathbb{Z}_m \) that are relatively prime to \( m \) is denoted by \( \phi(m) \).

We set \( \phi(1) = 1 \). The function

\[
m \mapsto \phi(m), \quad m \geq 1
\]

is called the Euler phi-function, or Euler totient function. Clearly, for \( m \) prime, we have \( \phi(m) = m - 1 \). Further, we state the following fact without proof, and leave the proof as an easy exercise.
Fact. If $m$ is a prime power, say, $m = p^e$, where $p$ is prime and $p > 1$, then $\phi(m) = m\left(1 - \frac{1}{p}\right) = p^e - p^{e-1}$.

The main purpose of this section is to prove the multiplicative property of the Euler phi-function.

Proposition. Suppose that $m \geq 1$ and $n \geq 1$ are integers such that $\gcd(m, n) = 1$. Then $\phi(m \times n) = \phi(m) \times \phi(n)$.

Proof. If $m = 1$ or $n = 1$, then the claim holds. Suppose now that $m > 1$ and $n > 1$, and denote:

$$A = \{a | 1 \leq a < m, \gcd(a, m) = 1\}$$
$$B = \{b | 1 \leq b < n, \gcd(b, n) = 1\}$$
$$C = \{c | 1 \leq c < m \times n, \gcd(c, m \times n) = 1\}.$$ 

Then we have that $|A| = \phi(m)$, $|B| = \phi(n)$, and $|C| = \phi(m \times n)$. We show that $C$ has equally many elements as the set $A \times B = \{(a, b) | a \in A, b \in B\}$, from which the claim follows.

2
Since $\gcd(m, n) = 1$, we can use the Chinese Remainder Theorem, by which the mapping

$$\pi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \pi(x) = (x \mod m, x \mod n)$$

is bijective. Now we observe that $A \subset \mathbb{Z}_m$, $B \subset \mathbb{Z}_n$, and $C \subset \mathbb{Z}_{m \times n}$. Moreover, it holds that $x \in C$ if and only if $\pi(x) \in A \times B$, which we see by writing the following chain of equivalences:

$$\gcd(x, m \times n) = 1 \iff \gcd(x, m) = 1 \text{ and } \gcd(x, n) = 1$$
$$\iff \gcd(x \mod m, m) = 1 \text{ and } \gcd(x \mod n, n) = 1.$$

$\square$

3
As a corollary, we get Theorem 1.2 of the textbook.

**Theorem 1.2** Suppose

\[ m = \prod_{i=1}^{k} p_i^{e_i}, \]

where the integers \( p_i \) are distinct primes and \( e_i > 0, \ 1 \leq i \leq k \). Then

\[ \phi(m) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i-1}). \]