The Euler phi-function

**Definition:** The *Euler φ-function* is defined for an integer \( m \geq 1 \) by

\[
\phi(m) = |\{ a \in \mathbb{Z} : 1 \leq a \leq m, \gcd(a, m) = 1 \}|
\]

**Remarks:**

1) The Euler φ-function is frequently called the *totient function*. This name was introduced by Sylvester, who in 1879 called an integer \( a \) with \( 1 \leq a \leq m \) and \( \gcd(a, m) = 1 \) a *totative*. (Neither word seems to be found in the Oxford dictionary, and there is no equivalent name for this function in other languages.)

2) We have that

\[
\phi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|
\]

is the number of units in the ring \( \mathbb{Z}/m\mathbb{Z} \).

**Examples:**

1) If \( m = p \) is a prime, then

\[
\phi(p) = p - 1.
\]

2) More generally, if \( m = p^r \) is a prime power with \( r \geq 1 \), then

\[
\phi(p^r) = p^{r-1}(p - 1).
\]
Theorem 6: We have that

\[(1) \quad \phi(mn) = \phi(m)\phi(n), \quad \text{if } \gcd(m, n) = 1.\]

Thus, if \(m = p_1^{r_1} \cdots p_t^{r_t}\), where the \(p_i\)'s are distinct primes, then

\[(2) \quad \phi(m) = \prod_{i=1}^{t} p_i^{r_i-1}(p_i - 1) = m \prod_{p|m} \left(1 - \frac{1}{p}\right).\]

Remark: Although (2) gives us an explicit formula for \(\phi(m)\), this does not allow us to compute \(\phi(m)\) in polynomial time because the formula requires the prime decomposition of \(m\), and there is no (known) polynomial time algorithm for finding the prime divisors \(p|m\) of \(m\).

Theorem 7 (Fermat-Euler): We have

\[a^{\phi(m)} \equiv 1 \pmod{m}, \quad \text{if } \gcd(a, m) = 1.\]

Corollary (Fermat): If \(p\) is a prime, then

\[a^p \equiv a \pmod{p}, \quad \text{for all } a \in \mathbb{Z}.\]