**Important Concepts**

Given two integers \( n \) and \( m \), write \( n \mid m \) if \( n \) divides \( m \); that is, there exists another integer \( k \) such that \( nk = m \).

1. **Prime Numbers**
   - A natural number \( p \) is prime if \( p \neq 1 \) and the only natural numbers that divide \( p \) are 1 and \( p \).
   - (Prime Factorization) If \( n \neq 1 \) is a natural number, there is exactly one way to write \( n = p_1^{a_1} \cdots p_m^{a_m} \) where \( p_1, \ldots, p_m \) are prime numbers and \( a_1, \ldots, a_n \) are natural numbers.

2. **Greatest Common Divisor**
   - Given two natural numbers \( n \) and \( m \), the greatest common divisor of \( n \) and \( m \), denoted \( \gcd(n, m) \), is the largest natural number \( d \) such that \( d \mid n \) and \( d \mid m \), and the least common multiple of \( n \) and \( m \), denoted \( \text{lcm}(m, n) \), is the smallest (non-zero) natural number \( d \) such that \( n \mid d \) and \( m \mid d \).
   - (Euclidean Algorithm) Given two natural numbers \( n \) and \( m \), there exists integers \( s \) and \( t \) so that \( sn + tm = \gcd(n, m) \).
   - (Legendre Formula) Let \( p \) be a prime number and \( n \) be a positive integer. The largest power of \( p \) that divides \( n! \) is \( p^m \) where
     \[
     m = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots
     \]

3. **Modular Arithmetic**
   - Let \( n \) be a positive integer. Two integers \( m \) and \( k \) are said to be congruent modulo \( n \), written \( m \equiv k \mod n \) if \( n \mid (m - k) \).
   - Suppose \( m_1 \equiv m_2 \mod n \) and \( k_1 \equiv k_2 \mod n \). Then \( m_1 + k_1 \equiv m_2 + k_2 \mod n \) and \( m_1k_1 \equiv m_2k_2 \mod n \).
   - Often we use \( \mathbb{Z}/n\mathbb{Z} \) to denote \( \{0, 1, 2, \ldots, n - 1\} \) where arithmetic is done modulo \( n \).
   - (Wilson’s Theorem) If \( p \) is a prime number, then \( (p - 1)! = -1 \mod p \).
   - (Fermat’s Little Theorem) If \( p \) is a prime number, then for any integer \( n \) such that \( n \neq 0 \mod p \), we have that \( n^{p-1} = 1 \mod p \). In particular, \( n^p = n \mod p \) for all natural numbers \( n \).
   - (Chinese Remainder Theorem) Let \( k \) be a positive integer and \( n_1, \ldots, n_k \) be positive integers such that \( \gcd(n_i, n_j) = 1 \) for all \( i, j \in \{1, \ldots, k\} \) with \( i \neq j \). For any selection of integers \( a_1, \ldots, a_k \) the system of congruences
     \[
     \begin{align*}
     x & \equiv a_1 \mod n_1 \\
     x & \equiv a_2 \mod n_2 \\
     & \quad \vdots \\
     x & \equiv a_k \mod n_k
     \end{align*}
     \]
   has an infinite number of integer solutions, and a unique solution in \( \{1, 2, \ldots, n_1n_2\cdots n_k\} \).

4. **Euler Totient Function**
   - The Euler (pronounced ‘oiler’) totient function (also called the Euler phi function) is the function \( \varphi : \mathbb{N} \to \mathbb{N} \) such that for each \( n \in \mathbb{N} \), \( \varphi(n) \) is the number of elements \( k \in \{1, \ldots, n\} \) such that \( \gcd(k, n) = 1 \).
   - If \( n, m \in \mathbb{N} \) and \( \gcd(m, n) = 1 \), then \( \varphi(mn) = \varphi(m)\varphi(n) \).
• For all $n \in \mathbb{N}$,
  \[ \varphi(n) = n \prod_{ \substack{p \text{ prime} \backslash n} } \left( 1 - \frac{1}{p} \right). \]

• For all $n \in \mathbb{N}$,
  \[ \sum_{d \text{ such that } d|n} \varphi(d) = n. \]

• (Euler’s Theorem) If $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$, then $m^{\varphi(n)} \equiv 1 \pmod{n}$. 