Modular Arithmetic

$a \bmod n$ is the remainder obtained when a is divided by n. For example, $100 \bmod 12 = 4$ (similar to % you encounter while programming). By Euclid's Division Lemma, $a \bmod n$ is unique. Some of it's properties are listed below :

- $(a + b) \bmod n = (a \bmod n + b \bmod n) \bmod n$
- $(a - b) \bmod n = (a + n - b) \bmod n$
- $(a * b) \bmod n = ((a \bmod n) * (b \bmod n)) \bmod n$

Euler's Totient function $\Phi(n)$

For any n, $\Phi(n) = \#\{x \in \{1, 2, \cdots, n-1\} | (x, n) = 1\}$ where (a, b) denotes the Greatest Common Divisor (GCD) of numbers a and b and # means the cardinality of the set.
eg: $\Phi(5) = 4, \Phi(2) = 1$

Some specific values of Euler's Totient function :

- $\Phi(p) = p - 1$ if p is Prime.
- $\Phi(p^n) = p^n - p^{n-1}$ if p is Prime.
- $\Phi(ab) = \Phi(a)\Phi(b)$ if $(a, b) = 1$.

In general, if $n = \prod_{i=1}^{r} p_i^{k_i}$ where p_i is a prime number, then :

$$\Phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Chinese Remainder Theorem (CRT)

Before moving directly to CRT we need to learn about some symbols.

$\mathbb{Z}_n$ represents the set of whole numbers less than n, i.e. the set $\{1, 2, \cdots, n-1\}$(this set is called **multiplicative group of integers modulo n**).

$\mathbb{Z}_n^*$ represents the set $\{a \in \mathbb{Z}_n | (a, n) = 1\}$. Note that cardinality of this group is $\Phi(n)$.

Definition a is said to be **congruent** to b module n if $n | (a - b)$. This is represented as $a \equiv b \bmod n$.

Theorem (CRT) For every element $x \in \mathbb{Z}_{pq}$, there exists a unique pair $(x \bmod p, x \bmod q)$ in $\mathbb{Z}_p \times \mathbb{Z}_q$ (this is cartesian product) where $(p, q) = 1$.

Conversely, for every (r, s) in $\mathbb{Z}_p \times \mathbb{Z}_q$, there exists a unique $x \in \mathbb{Z}_{pq}$ where $r = x \bmod p$ and $s = x \bmod q$.

Definition a is said to be **Modular Inverse** of another integer b modulo n if $ab \equiv 1 \bmod n$.

One can find modular inverse using **Extended Euclidean Algorithm**.

Euler's Totient Theorem

Theorem If n is a positive integer and $(a, n) = 1$, then $a^{\Phi(n)} \equiv 1 \bmod n$.