Congruences: If an integer $m \neq 0$ divides the difference $a-b$, we say that a is congruent to b modulo m and write $a \equiv b \pmod{m}$. If $a-b$ is not divisible by m, we say that a is not congruent to b modulo m, and in this case we write $a \not\equiv b \pmod{m}$.

Let a, b, c, d denote integers. Then:

1. $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $a-b \equiv 0 \pmod{m}$ are equivalent statements.
2. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$
3. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$.
4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
5. If $a \equiv b \pmod{m}$ and $d \mid m, d > 0$, then $a \equiv b \pmod{d}$.
6. If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{mc}$ for $c > 0$.

Let f denote a polynomial with integral coefficients. If $a \equiv b \pmod{m}$ then $f(a) \equiv f(b) \pmod{m}$.

If $x \equiv y \pmod{m}$ then y is called a residue of x modulo m. A set $x_1, x_2, \cdots, x_m$ is called a complete residue system modulo m if for every integer y there is one and only one x_j such that $y \equiv x_j \pmod{m}$.

If $b \equiv c \pmod{m}$, then $(b, m) = (c, m)$

Let $b = c + mx$, then $\underline{(b, m)} = (c+mx, m)$

$= (c+mx-mx, m) = \underline{(c, m)}$

A reduced residue system modulo m is a set of integers r_i such that $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ if $i \neq j$, and such that every x prime to m is congruent modulo m to some member r_i of the set. All reduced residue systems modulo m will contain the same number of members, a number that is denoted by $\phi(m)$. This function is called Euler's ϕ-function, sometimes the totient. The number $\phi(m)$ is the number of positive integers less than or equal to m that are relatively prime to m.

Let $(a, m) = 1$. Let $r_1, r_2, \ldots, r_n$ be a complete, or a reduced residue system modulo m. Then $ar_1, ar_2, \ldots, ar_n$ is a complete, or a reduced, residue system, respectively, modulo m.

$$(r_i, m) = 1 \Rightarrow (ar_i, m) = 1$$

$$r_i \equiv r_j \pmod{m} \Rightarrow ar_i \equiv ar_j \pmod{m}$$

$ar_i \equiv ar_j \pmod{m} \Rightarrow r_i \equiv r_j \pmod{m}$ since $(a, m) = 1$.

<u>Fermat's Theorem</u>: Let p denote a prime. If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$. For every integer a, $a^p \equiv a \pmod{p}$.

<u>Euler's theorem</u>: If $(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Let $r_1, r_2, \ldots, r_{\phi(m)}$ be a reduced residue system modulo m. Then $ar_1, ar_2, \ldots, ar_{\phi(m)}$ is also a reduced residue system modulo m.

$\Rightarrow \quad ar_i \equiv r_j \bmod (m)$ for unique j

$$\Rightarrow a^{\phi(m)} \prod r_i \equiv \prod r_j \pmod{m} \Rightarrow a^{\phi(m)} \equiv 1 \pmod{m}$$

If $(a, m) = 1$ then there is an x such that $ax \equiv 1 \pmod{m}$. Any two such x are congruent $(\bmod m)$. If $(a, m) > 1$ then there is no such x.

$(a, m) = 1 \Rightarrow ax + my = 1 \Rightarrow ax \equiv 1 \pmod{m}$

suppose $ax' \equiv 1 \pmod{m} \Rightarrow ax' \equiv ax \pmod{m}$

$\Rightarrow x' \equiv x \pmod{m}$,

$ax \equiv 1 \pmod{m} \Rightarrow m \mid (ax-1) \Rightarrow (a, m) \mid (ax-1)$

$\Rightarrow (a, m) \mid 1 \Rightarrow \underline{(a, m) = 1} \Rightarrow$ If $(a, m) > 1$ then there is no such x.

If m_1 and m_2 denote two positive, relatively prime integers, then $\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$. Moreover, if m has the canonical factorization $m = \prod p^\alpha$, then $\phi(m) = \prod_{p \mid m} (p^\alpha - p^{\alpha-1})$

$= m \prod_{p \mid m} (1 - 1/p)$

Applying inclusion-exclusion principle:

$$\phi(m) = m - \sum_i \frac{m}{p_i} + \sum_{i \neq j} \frac{m}{p_i p_j} - \sum_{i \neq j \neq k} \frac{m}{p_i p_j p_k} + \cdots$$

$$= m\left(1 - \sum_i \frac{1}{p_i} + \sum_{i \neq j} \frac{1}{p_i p_j} - \sum_{i \neq j \neq k} \frac{1}{p_i p_j p_k} + \cdots\right)$$

$$= m \prod_{p \mid m} \left(1 - \frac{1}{p}\right) = \prod_{p \mid m} \phi(p^\alpha)$$

$\Rightarrow \phi(m_1 m_2) = \phi(m_1)\phi(m_2)$ if $(m_1, m_2) = 1$