Theorem 1. The identity element in $\mathbb{Z}_n$ is unique.

Proof. Let $e, e' \in \mathbb{Z}_n$ be the two identity elements such that $e \neq e'$. Then

$$e = e \circ e' = e' \implies e = e' \ .$$

$\square$

Theorem 2. The inverse of $a \in \mathbb{Z}_n$ is unique.

Proof. Let $a \in \mathbb{Z}_n$, and let a' and a'' be its inverse elements. Then

$$a \circ a' = e = a \circ a'' \implies a' \circ a \circ a' = a' \circ a \circ a'' \implies e \circ a' = e \circ a'' \implies a' = a'' \ .$$

$\square$

Theorem 3. Every element $a \in \mathbb{Z}_n$ has an additive inverse $-a \in \mathbb{Z}_n$.

Proof.

$$\forall a \in \mathbb{Z}_n \ \exists n - a \in \mathbb{Z}_n : a + n - a = n \equiv 0 = e \pmod{n} \ .$$

$\square$

Theorem 4. An element $a \in \mathbb{Z}_n$ has multiplicative inverse a^{-1} iff $\gcd(a, n) = 1$.

Proof. First, we show that $\gcd(a, n) = 1 \implies \exists a^{-1} \in \mathbb{Z}_n : aa^{-1} = 1$. By the Bezout identity,

$$\gcd(a, n) = 1 \implies \exists \alpha, \beta \in \mathbb{Z} : \alpha a + \beta n = 1 \implies \alpha a \equiv 1 \pmod{n} \implies a^{-1} = \alpha \ .$$

Finally, we show that $\exists a^{-1} \in \mathbb{Z}_n : aa^{-1} = 1 \implies \gcd(a, n) = 1$.

$$aa^{-1} \equiv 1 \pmod{n} \implies \exists \beta \in \mathbb{Z} : aa^{-1} + \beta n = 1 \implies \gcd(a, n) = 1 \ .$$

$\square$

Theorem 5. The equation $ax \mod n = c$ is solvable iff $\gcd(a, n) | c$.

Proof. First, we show that $ax \mod n = c \implies \gcd(a, n) | c$.

$$ax \mod n = c \implies \exists k \in \mathbb{Z} : ax - kn = c \ .$$

Let $\gcd(a, n) = d$. Then $d | a \implies \exists a' \in \mathbb{Z} : a = a'd$ and $d | n \implies \exists n' \in \mathbb{Z} : n = n'd$. Then

$$ax - kn = c \implies a'dx - kn'd = c \implies d \cdot (a'x - kn') = c \implies d | c \ .$$

Finally, we show that $\gcd(a, n) | c$ implies that the equation $ax \mod n = c$ is solvable. Let $\gcd(a, n) = d$. Then

$$\gcd(a, n) = d \implies \gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1 \implies \exists \left(\frac{a}{d}\right)^{-1} \in \mathbb{Z}_{\frac{n}{d}} \ .$$

Since element $\frac{1}{d}$ is invertible modulo $\frac{n}{d}$, the equation $\frac{a}{d}x \mod \frac{n}{d} = \frac{c}{d}$ is solvable. This means that

$$\exists k \in \mathbb{Z} : \frac{a}{d}x - k \cdot \frac{n}{d} = \frac{c}{d} \implies ax - kn = c \implies ax \mod n = c \ .$$

Therefore, the equation $ax \mod n = c$ is solvable. $\square$

Lemma 1. Every composite number $m \geqslant 2$ is a product of primes.

Proof. Let m be the least composite number that is not a product of primes. The existence of such m is guaranteed by the well-ordering principle, which states that every non-empty set of positive integers contains a least element. Since m is a composite number, there exist numbers $m_1, m_2 < m$ such that $m = m_1 \cdot m_2$. Since m was the least integer that is not a product of primes, every integer less than m must be a product of primes. Since $m_1, m_2 < m$, they must be products of primes, which in turn means that $m_1 \cdot m_2$ is also a product of primes, and so is m. A contradiction. □

Lemma 2. If $\gcd(a, n) = \gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.

Proof. By the Bezout identity

$$\gcd(a,n) = 1 \implies \exists \alpha, \beta \in \mathbb{Z} : \alpha a + \beta n = 1 \ ,$$
$$\gcd(b,n) = 1 \implies \exists \gamma, \delta \in \mathbb{Z} : \gamma b + \delta n = 1 \ .$$

In turn, this implies that

$$(\alpha a + \beta n)(\gamma b + \delta n) = \underbrace{\alpha\gamma}_{\varphi} ab + \underbrace{(\alpha\delta a + \beta\gamma b + \beta\delta n)}_{\vartheta} \cdot n = 1 \implies \varphi ab + \vartheta n = 1 \implies \gcd(ab, n) = 1 \ .$$

□

Theorem 6 (Fundamental Theorem of Arithmetics)**.** Every composite number $m \geqslant 2$ has a unique prime-factorization $p_1 \cdot p_2 \cdot \ldots p_k$, where $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k$.

Proof. Let m be the least number that has two different prime factorizations:

$$p_1 \cdot p_2 \cdot \ldots \cdot p_k = m = q_1 \cdot q_2 \cdot \ldots \cdot q_l \ .$$

$p_i \neq q_j$, because otherwise there existed other integer $m' = \frac{m}{p_i} < m$ that also has two different factorizations. Therefore

$$\gcd(p_1, q_1) = \gcd(p_1, q_2) = \ldots = \gcd(p_1, q_l) = 1 \ ,$$

By Lemma 2, the previous result implies that

$$\gcd(p_1, \underbrace{q_1 \cdot q_2 \cdot \ldots \cdot q_l}_{m}) = 1 \implies \gcd(p_1, m) = 1 \ ,$$

and it in turn is a contradiction, since $p_1 | m$. □

Theorem 7. Let $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k \in \mathbb{Z}$ and $n > 0$. Then $\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right)$

Proof. Let $M = \mathbb{Z}_m$, where $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$. Let $P_n = \{x \in \mathbb{Z}_n : p_n | x\}$. Then $\phi(n) = |M \setminus \cup_n P_n|$.

If $k = 1$, then $|M \setminus \cup_n P_n| = |M| - |P_1| = m - \frac{m}{p_1}$.
If $k = 2$, then $|M \setminus \cup_n P_n| = |M| - |P_1| - |P_2| + |P_1 \cap P_2| = m - \frac{m}{p_1} - \frac{m}{p_2} + \frac{m}{p_1 p_2}$.
If $k = 3$, then $|M \setminus \cup_n P_n| = |M| - |P_1| - |P_2| - |P_3| + |P_1 \cap P_2| + |P_1 \cap P_3| + |P_2 \cap P_3| - |P_1 \cap P_2 \cap P_3| =$

$m - \frac{m}{p_1} - \frac{m}{p_2} - \frac{m}{p_3} + \frac{m}{p_1p_2} + \frac{m}{p_1p_3} + \frac{m}{p_2p_3} - \frac{m}{p_1p_2p_3}$.

In the general case:

$$|M \setminus \cup_n P_n| = |M| - \Sigma_1 + \Sigma_2 - \Sigma_3 + \ldots + (-1)^i \Sigma_i \ \ ,$$

where $\Sigma_i = \sum\limits_{(j_1,\ldots,j_i)\in c(i)} |P_{j_1} \cap \ldots P_{j_i}|$, and the summation is over the set $c(i)$ of all i-combinations of indices. There are $\binom{k}{i}$ of them. And hence:

$$\begin{aligned}
\phi(n) &= m - \frac{m}{p_1} - \frac{m}{p_2} - \ldots - \frac{m}{p_k} + \frac{m}{p_1p_2} + \ldots + \frac{m}{p_1p_k} + \ldots + \frac{m}{p_2p_k} - \ldots - \frac{m}{p_1p_2p_k} - \ldots \\
&= m \cdot \left(1 - \frac{1}{p_1} - \frac{1}{p_2} - \ldots - \frac{1}{p_k} + \frac{1}{p_1p_2} + \ldots + \frac{1}{p_1p_k} + \ldots + \frac{1}{p_2p_k} - \ldots - \frac{1}{p_1p_2p_k} - \ldots\right) \\
&= m \cdot \left[\left(1 - \frac{1}{p_2} - \ldots - \frac{1}{p_k} + \ldots + \frac{1}{p_2p_k} + \ldots\right) - \frac{1}{p_1} \cdot \left(1 - \frac{1}{p_2} - \ldots - \frac{1}{p_k} + \ldots + \frac{1}{p_2p_k} + \ldots\right)\right] \\
&= m \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2} - \ldots - \frac{1}{p_k} + \ldots + \frac{1}{p_2p_k} + \ldots\right) \\
&= m \cdot \left(1 - \frac{1}{p_1}\right)\left[\left(1 - \ldots - \frac{1}{p_k}\right) - \frac{1}{p_2} \cdot \left(1 - \ldots - \frac{1}{p_k}\right)\right] = m \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) \ \ .
\end{aligned}$$

□