Definition: Let $m \in \mathbb{N} \setminus \{0\}$. The equivalence classes defined by the congruence relation \textit{modulo} $m$ are called \textbf{residue classes modulo} $m$. For any $a \in \mathbb{Z}$, $[a]$ denotes the equivalence class to which $a$ belongs, i.e.

$$[a] = \{b \in \mathbb{Z} | a \equiv b \mod m\}$$

Congruences as equivalence relation. Let $m \in \mathbb{N} \setminus \{0\}$. The congruence relation \textit{modulo} $m$ is an equivalence relation, i.e., it satisfies the following properties for any $a, b \in \mathbb{Z}$.

1. \textit{Reflexivity}: $a \equiv a \mod m$

2. \textit{Symmetry}: If $a \equiv b \mod m$, then $b \equiv a \mod m$

3. \textit{Transitivity}: If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.

\textbf{$\mathbb{Z}_p$ is the set of integers modulo $p$.}

In reality the elements of $\mathbb{Z}_p$ are equivalence classes, i.e.,

$$\mathbb{Z}_p = \{[0], [1], ..., [p - 1]\}.$$  

However, we often write

$$\mathbb{Z}_p = \{0, 1, ..., p - 1\}.$$ 

Consider $\mathbb{Z}_8$. Is it possible to have $a, b \in \mathbb{Z}_8$ with $a \neq 0$ and $b \neq 0$, but $a \cdot b = 0$?

Intuitively, a \textbf{field} is a set with two operations, denoted by “$+$” and “$\cdot$”, that has many of the properties that $\mathbb{Q}$ has.
Theorem.
Let $p$ be a prime number. Then $\forall x \in \mathbb{Z}_p \setminus \{0\}, \exists y \in \mathbb{Z}_p$, such that $x \cdot y \equiv 1$.

Is the assumption $p$-prime necessary?

Exercise.
Find the multiplicative inverse for each of the elements in $\mathbb{Z}_5$.
Can this be done for $\mathbb{Z}_6$?

Exercise.
Let $p$ be a prime integer. What is the multiplicative inverse of $x \in \mathbb{Z}_p \setminus \{0\}$?
Hint: Use Fermat’s Little Theorem.

Assume $p$ is prime. Can you show that the multiplicative inverse of every nonzero element $x \in \mathbb{Z}_p$ is unique?