The Ring $\mathbb{Z}/m\mathbb{Z}$ and the Field $\mathbb{F}_p$

Definition: The ring of integers modulo m is the set of remainders modulo m,

$$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\},$$

endowed with the following addition, subtraction and multiplication rules:

$$\begin{aligned} [a] \pm [b] &= [\mathrm{rem}(a \pm b, m)] \\ [a] \cdot [b] &= [\mathrm{rem}(a \cdot b, m)] \end{aligned}$$

Notes: 1) For $0 \leq k < m$, the symbol $[k] = [k]_m$ (which depends on m) is the integer k, but viewed as a remainder modulo m.

2) The above definitions make $\mathbb{Z}/m\mathbb{Z}$ into a ring: we can add, subtract and multiply (and these operations satisfy the usual rules).

3) If $m = p$ is a prime, then we can also divide in $\mathbb{F}_p := \mathbb{Z}/m\mathbb{Z}$, and so $\mathbb{F}_p$ is a (finite) field.

Extension: For any $k \in \mathbb{Z}$, put $[k]_m := [\mathrm{rem}(k, m)]_m$. (Thus $[k]_m \in \mathbb{Z}/m\mathbb{Z}$). Then we have

$$[k]_m = [k']_m \quad \Leftrightarrow \quad k \equiv k' \pmod{m}.$$