Modular Arithmetic

(Section 1.7)

Recall: Equivalence relations and classes

An equivalence relation on a set S is a subset R of $S \times S$ such that $\forall\ x, y, z \in S$,

1) $(x,x) \in R$
2) If $(x,y) \in R$, then $(y,x) \in R$.
3) If $(x,y) \in R$ and $(y,z) \in R$, then $(x,z) \in R$.

Usually, we dispense with the direct product and think of an equivalence relation as a relation "$\sim$" on S such that

$\forall \; x, y, z \in S$,

1) $x \sim x$ (reflexivity)

2) If $x \sim y$, then $y \sim x$ (symmetry)

3) If $x \sim y$ and $y \sim z$, then $x \sim z$. (transitivity)

If "$\sim$" is an equivalence relation on a set S and $x \in S$, we denote the equivalence class of x by $[x]$,

$$[x] = \{ y \in S \mid x \sim y \}$$

The Modulus

Let $S = \mathbb{Z}$. Let $n \in \mathbb{N}$, $n \geq 2$.

We define an equivalence relation "$\sim$" on $\mathbb{Z}$ by, if $a, b \in \mathbb{Z}$,

$$\boxed{a \sim b \quad \text{if} \quad n \mid (b-a)}.$$

The remainder of $a \in \mathbb{Z}$, upon division by n, is called the **modulus** of $a \in \mathbb{Z}$, and is denoted by

$$\boxed{a \bmod n}$$

This symbol will be used interchangeably (for the most part) with $[a]$ under this equivalence relation.

Example 1: (using mod) Let $n=7$.

Let $a=3845$.

Then

$3845 = 7\cdot(549)+2$,

so

$3845 \equiv 2 \mod 7$.

$3845 \mod 7 = 2$

is the same statement.