Modular Arithmetic

Noah Luntzlara & Annie Xu
nluntzla@umich.edu & wanqiaox@umich.edu

September 16, 2019

In this worksheet we introduce *modular arithmetic*. So far you have studied arithmetic in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{R}$, and maybe $\mathbb{C}$. We will look at a new "system of arithmetic", this time working with a finite set. However, it is very related to arithmetic in $\mathbb{Z}$.

Fix $n \in \mathbb{N}$. Define an equivalence relation on $\mathbb{Z}$ by

$$a \sim_n b \text{ provided that } \exists\ k \in \mathbb{Z} \text{ s.t. } a - b = k \cdot n.$$

Ex. Explain in regular language what this equivalence relation does.
Ex. Prove $\sim_n$ is an equivalence relation.
Ex. Prove that if $a \sim_n b$ and $c \sim_n d$, then $a + c \sim_n b + d$.
Ex. Prove that if $a \sim_n b$ and $c \sim_n d$, then $a \cdot c = b \cdot d$.
For $a \in \mathbb{Z}$, define $[a]_n$ to be the equivalence class of a under $\sim_n$, i.e. the set

$$\{z \in \mathbb{Z} \,|\, a \sim_n z\}.$$

Define $\mathbb{Z}_n$ to be the set of equivalence classes of $\sim_n$, i.e. the set

$$\{[z]_n \,|\, z \in \mathbb{Z}\}.$$

Ex. What is $|\mathbb{Z}_n|$?
Define the binary operations $+_n$ and $\times_n$ on $\mathbb{Z}_n$ by

$$[a]_n +_n [b_n] := [a + b]_n$$

and

$$[a]_n \times_n [b_n] := [ab]_n.$$

Ex. Verify that $+_n$ and $\times_n$ are well-defined binary operations on $\mathbb{Z}_n$. Verify that the left- and right-distributive properties hold.
Ex. Is there a $+_n$ identity in $\mathbb{Z}_n$? If so, which elements have $+_n$-inverses?
Ex. Is there a $\times_n$ identity in $\mathbb{Z}_n$? If so, which elements have $+_n$-inverses?
Ex. For which n is $(\mathbb{Z}_n, +_n, \times_n)$ a field?