Modular Arithmetic

Definition 1 (Congruence Modulo n)**.** *Let n be a positive integer. We say that integers a and b are* congruent modulo n*, denoted $a \equiv b \mod n$ or $a \equiv_n b$, if $n|(b-a)$.*

Proposition 1. *If n is a fixed positive integer, then congruence modulo n is an equivalence relation.*

Since $\equiv_n$ is an equivalence, it induces a partition on the set $\mathbb{Z}$ of integers, $\mathbb{Z}/\equiv_n$. We will denote this partition using $\mathbb{Z}/(n)$, and refer to this set as the set of *modular integers.*

Theorem 2. *The elements of $\mathbb{Z}/(n)$ are sets of the form $[r]_n$, where $0 \leq r < n$; such r are called* residues *mod n. Moreover, any two such sets are distinct. In particular, $\mathbb{Z}/(n)$ is a finite set with precisely n elements, which are represented by the set of residues $\{0, 1, \ldots, n-1\}$.*

Proof. First we show that every class in $\mathbb{Z}/(n)$ has a representative r with $0 \leq r < n$. To this end, let $[a] \in \mathbb{Z}/(n)$. By the Division Algorithm, we have $a = qn + r$, where $0 \leq r < n$, and since $a - r = qn$, we have $a \equiv r \mod n$. Thus $[a] = [r]$ as needed.

Next we show that two such classes are distinct. To this end, suppose we have $[r_1] = [r_2]$, where $0 \leq r_1, r_2 < n$. By definition, we have that n divides $r_2 - r_1$; say $r_2 - r_1 = qn$. In particular, $r_2 = qn + r_1$. Note also that $r_2 = 0 \cdot n + r_2$. By the uniqueness of positive remainders given by the Division Algorithm, we have $r_1 = r_2$. □

Arithmetic in $\mathbb{Z}/(n)$

Theorem 3. *Let n be a positive integer. If a_1, a_2, b_1, and b_2 are integers such that $a_1 \equiv a_2 \mod n$ and $b_1 \equiv b_2 \mod n$, then we have the following.*

1. $a_1 + b_1 \equiv a_2 + b_2 \mod n$.

2. $a_1 b_1 \equiv a_2 b_2 \mod n$.

Corollary 4. *Let n be a positive integer. Then the operations $+$ and $\cdot$ on $\mathbb{Z}/(n)$ given by*

$$[a] + [b] = [a+b] \quad \text{and} \quad [a] \cdot [b] = [ab]$$

are well-defined.

Theorem 5 (Modular Arithmetic)**.** *Let n be a positive integer. Then $\mathbb{Z}/(n)$, with the operations $+$ and $\cdot$ defined as above, satisfy the following properties.*

A1. $([a] + [b]) + [c] = [a] + ([b] + [c])$ *for all a, b, and c.*

A2. There is a modular integer 0 with the property that $[a] + 0 = 0 + [a] = [a]$ for all a.

A3. *For every residue* $[a]$, *there is a unique residue* $[b]$ *with the property that* $[a]+[b]=[b]+[a]=0$. *We denote this residue by* $-[a]$.

A4. $[a]+[b]=[b]+[a]$ *for all* a *and* b.

M. $([a]\cdot[b])\cdot[c]=[a]\cdot([b]\cdot[c])$ *for all* a, b, *and* c.

D. $[a]\cdot([b]+[c])=[a]\cdot[b]+[a]\cdot[c]$ *and* $([b]+[c])\cdot[a]=[b]\cdot[a]+[c]\cdot[a]$ *for all* a, b, *and* c.

C. $[a]\cdot[b]=[b]\cdot[a]$ *for all* a *and* b.

U. *There is a modular integer* 1 *with the property that* $[a]\cdot 1=1\cdot[a]=[a]$ *for all* a.