MTHSC 412 Section 2.6 –Congruence Classes

Kevin James

Definition

Given an integer $n > 1$ we denote the set of congruence classes modulo n as

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

Note

It is also common to omit the brackets and simply write

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

Fact

Under the equivalence relation $\equiv \pmod{n}$ *on* $\mathbb{Z}$, $[a] = [b]$ *if and only if* $a \equiv b \pmod{n}$.

Proof.

First, suppose that $[a] = [b]$.
Then, we have $a \in [a] = [b] \Rightarrow a \equiv b \pmod{n}$.

Now suppose that $a \equiv b \pmod{n}$.
$x \in [a] \Rightarrow x \equiv a \pmod{n}$.
Since, we also have $a \equiv b \pmod{n}$, it follows from transitivity that $x \equiv b \pmod{n}$.
Thus $x \in [b]$.
So, $[a] \subseteq [b]$.
Similarly, we can show that $[b] \subseteq [a]$ and thus $[a] = [b]$. $\square$

Definition

We define addition on $\mathbb{Z}_n$ as $[a] + [b] = [a + b]$.

Note

We must take care that this is a well-defined operation since the set $[a]$ has many different names.

Example

Let's consider $\equiv \pmod 4$ on the integers.
Recall that $[1] = [5]$ and $[2] = [6]$.
From our definition of addition, we have
$[1] + [2] = [3]$ while,
$[5] + [6] = [11]$.
Luckily $[3] = [11]$.
We must make sure that this is always the case for addition to be *well defined*.

Theorem

1. *Addition is a well defined binary operation on* $\mathbb{Z}_n$.
2. *Addition on* $\mathbb{Z}_n$ *is associative.*
3. *Addition on* $\mathbb{Z}_n$ *is commutative.*
4. $[0]$ *is the additive identity for* $\mathbb{Z}_n$.
5. *Each* $a \in \mathbb{Z}_n$ *has an additive inverse,* $[-a]$ *in* $\mathbb{Z}_n$.

PROOF.

(1.) Suppose that $[a] = [c]$ and $[b] = [d]$.
$[a] = [c] \Rightarrow a \equiv c \pmod{n}$ and
$[b] = [d] \Rightarrow b \equiv d \pmod{n}$.
Thus $a + b \equiv c + d \pmod{n}$ from results of section 2.4.
$\Rightarrow [a + b] = [c + d]$.

(2.) Suppose that $[a], [b]$ and $[c] \in \mathbb{Z}_n$. Then
$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)]$
$= [a] + [b + c] = [a] + ([b] + [c])$.

(3.) $[a] + [b] = [a + b] = [b + a] = [b] + [a]$.

(4.) Suppose that $[a] \in \mathbb{Z}_n$.
Then $[0] + [a] = [a] + [0] = [a + 0] = [a]$.

(5.) Note that $[-a] = [n - a] \in \mathbb{Z}_n$ and
$[a] + [-a] = [a + (-a)] = [0]$. □

Definition (Multiplication in $\mathbb{Z}_n$)

$$[a][b] = [ab].$$

Theorem

1. *Multiplication is a well defined binary operation on* $\mathbb{Z}_n$.
2. *Multiplication on* $\mathbb{Z}_n$ *is associative.*
3. *Multiplication on* $\mathbb{Z}_n$ *is commutative.*
4. $[1]$ *is the multiplicative identity for* $\mathbb{Z}_n$.

Proof.

1. Suppose that $[a] = [c]$ and $[b] = [d]$.
   Then $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$.
   Thus $ab \equiv cd \pmod{n}$.
   So, $[ab] = [cd]$.
2. $([a][b])[c] = [ab]\,[c] = [(ab)c] = [a(bc)] = [a]\,[bc] = [a]\,([b][c])$.
3. $[a][b] = [ab] = [ba] = [b][a]$.
4. Let $[a] \in \mathbb{Z}_n$. Then, $[a][1] = [1][a] = [(1)(a)] = [a]$.

$\square$

Example

Consider the multiplication table for $\mathbb{Z}_6$.

$\times$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Definition

Suppose $[0] \neq [a] \in \mathbb{Z}_n$. $[a]$ is a *zero diviosr* if there is $[0] \neq [b] \in \mathbb{Z}_n$ such that $[a][b] = [0]$

Example

From the multiplication table for $\mathbb{Z}_6$, we see that $[2], [3]$ and $[4]$ are zero divisors in $\mathbb{Z}_6$.

Theorem

$[a] \in \mathbb{Z}$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if $(a, n) = 1$.

Proof.

Suppose first that $(a, n) = 1$ then there is a solution s to $ax \equiv 1 \pmod{n}$.
Thus, $[a][s] = [as] = [1]$.
Now suppose that $[a]$ has an inverse $[b]$.
Then $[a][b] = [1] \Rightarrow ab \equiv 1 \pmod{n}$.
So, $ab - 1 = kn$ for some $k \in \mathbb{Z}$.
$\Rightarrow ab + (-k)n = 1$
$\Rightarrow (a, n) = 1$. $\square$

Corollary

Every nonzero element of $\mathbb{Z}_n$ has a multiplicative inverse if and only if n is prime.

Proof.

From our last result, every element of $\mathbb{Z}_n$ has a multiplicative inverse
$\Leftrightarrow (a, n) = 1$ for all $1 \leq a \leq n - 1$.
$\Leftrightarrow$ n has no divisors between 2 and $(n - 1)$.
$\Leftrightarrow$ n is prime. $\square$