Math135 - November 2'nd, 2015

Integers Modulo M - Congruence Class Arithmetic

Recall:

$ax \equiv c \pmod{m}$ has a solution if $\gcd(a, m)|c$.

Congruence Classes

Let $a, m \in \mathbb{Z}$ where $m > 0$. The **Congruence Class Modulo** m of the integer a is the set of integers $[a] = x \in \mathbb{Z}|x \equiv a$

Example: Suppose $m = 5$

$[0] = \{\cdots - 10, -5, 0, 5, 10, \dots\} = \{5k : k \in \mathbb{Z}\}$
$[1] = \{\dots, -9, -4, 1, 6, 11, \dots\} = \{5k + 1 : k \in \mathbb{Z}\}$
And so on.

$\mathbb{Z}_\mathbf{m}$

Let m be a positive integer. We define $\mathbb{Z}_m$ to be the set of m congruence classes.

$\mathbb{Z}_m = \{[0], [1], [2], \dots, [m + 1]\}$

Congruence Class Arithmetic

We will define addition and multiplication of Congruence Classes as follows:

$[a] + [b] = [a + b]$
$[a][b] = [ab]$

Examples in $\mathbb{Z}_6$:

i) $[14] = [2]$
ii) $[13] = [5]$
iii) $[2][5] = [10] = [4]$
iv) $[14][-13] = [-182] = [-2] = [4]$

Addition and multiplication are well defined. That is, in any congruence class addition or multiplication, a congruence class can be replaced with an equivalent congruence class without disrupting the equality.

Identities

Given a set and an operation, an identity is "something that does nothing". More formally, given a set S, and an operation $\circ$, an identity is an element $e \in S$ such that $\forall a \in S, a \circ e = a$.

The additive identity is $[0]$ as $[a] + [0] = [a + 0] = [a]$.
The multiplicative identity is $[1]$ as $[a][1] = [1a] = [a]$.

Inverse

The element $b \in S$ is an inverse of $a \in S$ if $a \circ b = b \circ a = e$ where e is the corresponding identity for the operation $\circ$.

For example, the **additive** identity of $[5]$ is $[-5]$ as $[5] + [-5] = [0] = e$ (The additive identity).

We define subtraction as addition by the inverse. We will always be able to find an additive inverse.
We define division as multiplication by the inverse. We will **NOT** always be able to find the multiplicative inverse.
We denote the multiplicative inverse of some value $[a]$ as $[a]^{-1}$.

Examples in $\mathbb{Z}_4$:

i) $[3]^{-1} = [3]$ since $[3][3] = [9] = [1]$
ii) $[2]^{-1}$ does not exist since $[2][x] = 1$ has no solution in $\mathbb{Z}_4$

Practice:

Solve the following in $\mathbb{Z}_1 14$

i)

$$\begin{aligned} [75] - [x] &= [5] \\ [75] + [-x] &= [50] \textbf{ (We must express subtraction as addition)} \\ [75] &= [50] + [x] \textbf{ (By additive identity)} \\ [75] + [-50] &= [x] \textbf{ (By additive identity)} \\ [25] &= [x] \\ [11] &= [x] \textbf{ (Always reduce to lowest terms)} \end{aligned}$$

ii)

$$\begin{aligned} [10][x] &= [1] \\ 10x &= 1 \text{ (mod 14)} \\ 10x + 14y &= 1 \end{aligned}$$

Notice how this is a simple Linear Diophantine. We know how to solve for x and y.
$\gcd(10, 14) = 2$
$2 \nmid 1 \therefore$ There is no solution

iii)

$$\begin{aligned} [10][x] &= 2 \\ 10x &= 2 \text{ (mod 14)} \\ 10x + 14y &= 2 \\ \gcd(10, 14) &= 2 \end{aligned}$$

$2|2$ so there is a solution.
$x = -4, y = 3$ (By inspection) Just like when solving a Linear Diophantine, we now need to plug this into the general formula to get all values of x.

$x = -4 + 7n, n \in \mathbb{Z}$ (By LDET2)
$x \equiv -4 \pmod 7$
$x \equiv 3 \pmod 7$
$x \equiv 3, 10 \pmod 7$

$\therefore [x] = [3], [10]$