Lecture 15: Modular Congruence

Summary:
We continue our study of modular arithmetic, examining the structure of integers modulo m. We prove that the invertible group of integers modulo m consists of integers coprime to m, and establish conditions for the existence of multiplicative inverses.

Topics Covered: modular congruence relation, modular congruence ring

For a positive integer m, we define

$$\mathbb{Z}_m = \{[a]_m \ : \ a \in \mathbb{Z}\} = \{[0]_m, [1]_m, \ \ldots \ , [m-1]_m\}$$

to be the set of equivalence classes of $\mathbb{Z}$ under the equivalence relation

$$a \sim b \iff m \mid a - b$$

We checked last class that addition and multiplication defined on $\mathbb{Z}$ in the obvious way

$$[a]_m + [b]_m = [a+b]_m$$

$$[a]_m \cdot [b]_m = [ab]_m$$

is well-defined.

Lemma:

$(\mathbb{Z}_m, +)$ is a group

Example:

The addition table for $(\mathbb{Z}_3, +)$ is

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

Example:

The addition table for $(\mathbb{Z}_4, +)$ is

$$\begin{array}{c|cccc} + & [0]_4 & [1]_4 & [2]_4 & [3]_4 \\ \hline [0] & [0] & [1] & [2] & [3] \\ [1] & [1] & [2] & [3] & [0] \\ [2] & [2] & [3] & [0] & [1] \\ [3] & [3] & [0] & [1] & [2] \end{array}$$

Lemma:

The cyclic group $(\mathbb{Z}_m, +)$ is generated by $[a]_m \iff \gcd(a, m) = 1$.

Proof:

If $\gcd(a, m) = 1$, then we can use Bezout's theorem to write 1 as a linear combination of a and m. This shows that $[1]_m \in \langle [a]_m \rangle$, so $[a]_m$ generates all of $\mathbb{Z}_m$.

Conversely, if $\gcd(a, b) = d > 1$, then everything generated by $[a]_m$ is a multiple of d. In particular, you cannot reach $[1]_m$.

$$\text{QED}$$

Lemma:

$$(\mathbb{Z}_m, \cdot)$$

is a monoid.

Note that $[0]_m$ is never invertible in $(\mathbb{Z}_m, \cdot)$.

Recall that the grou pof units in a monoid $(M, \cdot)$ is the set

$$M^\times = \{x \in M \ : \ x \text{ is invertible}\}$$

We saw many lectrues ago that $(M^\times, \cdot)$ is always a group, What does that group look like for $\mathbb{Z}_m$?

Lemma:

$$\mathbb{Z}_m^\times = \{[a]_m \ : \ \gcd(a, b) = 1\}$$

Here, we are looking for elements $[a]_m$ which are invertible. In particular, these are the elements such that there exists $x \in \mathbb{Z}$ with $[a]_m[x]_m = [1]_m$.

This is the same as requiring $[ax]_m = [1]_m$, which in trun is the same as

$$ax \equiv 1 \pmod{m}$$

Proposition:

Let $a \in \mathbb{Z}$. Then,

1. $\exists x \in \mathbb{Z}$ such that $ax \equiv 1 \pmod{m} \iff \gcd(a, b) = 1$ and
2. Such an x is unique modulo m