Session 55: Modular Arithmetic

- Modular addition and multiplication
- Properties of modular arithmetic

mod *m* Function of Products and Sums

Corollary: Let *m* be a positive integer and let *a* and *b* be integers. Then

$(a + b)$ $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

and

$a \cdot b \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$.

Arithmetic Modulo *m*

Definitions: Let $\mathbf{Z}_m$ be the set of nonnegative integers less than *m*:

$\mathbf{Z}_m = \{0, 1, \ldots., m - 1\}$

The **addition modulo m** operation $+_m$ is defined as

$a +_m b = (a + b)$ **mod** m.

The **multiplication modulo m** operation $\cdot_m$ is defined as

$a \cdot_m b = (a \cdot b)$ **mod** m.

Using these operations is said to be doing **arithmetic modulo m**.

Example

Computing $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Arithmetic Modulo *m*

The operations $+_m$ and $\cdot_m$ satisfy many of the properties as ordinary addition and multiplication.

- **Closure**: If *a* and *b* belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.
- **Commutativity**: If *a* and *b* belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
- **Associativity**: If *a*, *b,* and *c* belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
- **Distributivity**: If *a*, *b,* and *c* belong to $\mathbf{Z}_m$, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Arithmetic Modulo *m*

The operations $+_m$ and $\cdot_m$ satisfy many of the properties as ordinary addition and multiplication.

- **Identity elements**: The elements 0 and 1 are identity elements for addition and multiplication modulo *m*, respectively.
  - If a belongs to $\mathbf{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.
- **Additive inverses**: If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse:
  - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$

Commutative Ring

Multiplicative inverses have not been included since they do not always exist.

Example: There is no multiplicative inverse of 2 modulo 6.

In the terminology of abstract algebra:

$\mathbf{Z}_m$ with $+_m$ is a **commutative group**

$\mathbf{Z}_m$ with $+_m$ and $\cdot_m$ is a **commutative ring**.

Summary

- Modular addition and multiplication
- Commutative Ring