Session 54: Congruence

- Congruences
- Properties of congruences

Congruence Relation

Definition: If a and b are integers and m is a positive integer, then ***a* is congruent to *b* modulo *m*** if m divides $a - b$.

Notations

- The notation $a \equiv b \pmod{m}$ says that a is congruent to b modulo m.
- We say that $a \equiv b \pmod{m}$ is a **congruence** and that m is its **modulus**.
- If a is not congruent to b modulo m, we write $a \not\equiv b \pmod{m}$

Example

Determine whether 17 is congruent to 5 modulo 6

Determine whether 24 and 14 are congruent modulo 6.

(mod *m*) and mod *m* Notations

The notations $a \equiv b$ (**mod** m) and a **mod** $m = b$ are different.

- $a \equiv b$ (**mod** m) is a ***relation*** on the set of integers.
- In a **mod** $m = b$, the notation **mod** denotes a ***function***.

Theorem 3: Let a and b be integers, and let m be a positive integer. Then $a \equiv b$ (**mod** m) if and only if a **mod** $m = b$ **mod** m.

Corollary: Two integers are congruent **mod** m if and only if they have the same remainder when divided by m.

Theorem on Congruences

Theorem 4: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Congruences of Sums and Products

Theorem 5: Let m be a positive integer.

If $a \equiv b$ (**mod** m) and $c \equiv d$ (**mod** m),

then $a + c \equiv b + d$ (**mod** m) and $ac \equiv bd$ (**mod** m).

Example

Because $7 \equiv 2 \ (\mathbf{mod}\ 5)$ and $11 \equiv 1 \ (\mathbf{mod}\ 5)$

Algebraic Manipulation of Congruences

Multiplying both sides of a valid congruence by an integer preserves validity.

If $a \equiv b \ (\mathbf{mod}\ m)$ then $c \cdot a \equiv c \cdot b \ (\mathbf{mod}\ m)$, where c is any integer.

Proof: by Theorem 5 with $d = c$.

Adding an integer to both sides of a valid congruence preserves validity.

If $a \equiv b \ (\mathbf{mod}\ m)$ then $c + a \equiv c + b \ (\mathbf{mod}\ m)$, where c is any integer

Proof: by Theorem 5 with $d = c$.

Example

Since $14 \equiv 8 \ (\mathbf{mod}\ 6)$ also

Dividing both sides by 2 does not produce a valid congruence:

Dividing a congruence by an integer does not always produce a valid congruence!

Summary

- Definition of congruences
- **mod** m relation vs. **mod** function
- Congruences of arithmetic operations