COT 3100C: INTRODUCTION TO DISCRETE STRUCTURES

SUMMER 2024

Number Theory

Part-2

Mesut Ozdag, Ph.D.
mesut.ozdag@ucf.edu

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 $a - b$.

- The notation: $\boldsymbol{a \equiv b \ (\text{mod } m)}$
- $a \equiv b \ (\text{mod } m)$ is a ***congruence,*** and that m is its ***modulus***.
- Two integers are congruent mod m *iff* they have the same remainder when divided by m.
- If a is **not congruent** to b modulo m, $a \not\equiv b \ (\text{mod } m)$.

Example: Determine whether 17 is congruent to 5 modulo 6

and whether 24 and 14 are congruent to modulo 6.

$a \equiv_m b$ (modulo operator)
a % b == r (remainder operator)

Solution:

- $17 \equiv 5 \ (\text{mod } 6)$ because 6 divides $17 - 5 = 12$.
- $24 \not\equiv 14 \ (\text{mod } 6)$ since $24 - 14 = 10$ is not divisible by 6.

Example

Find the remainder when dividing $4^{25} / 10$.

More on Congruences

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

Proof:

- If $a \equiv b \pmod{m}$, (by the definition of congruence)

  $m \mid a - b$. Hence, there is an integer k

  such that $a - b = km$ and equivalently $a = b + km$.

- Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$.

  $m \mid a - b$

  and $a \equiv b \pmod{m}$.

Notations

They are different:

- $a \equiv b \pmod{m}$
- $a \bmod m = b$

$a \equiv b \pmod{m}$, is a relation on the set of integers.

$a \bmod m = b$, the notation **mod** denotes a function.

Theorem: Let a and b be integers, and let m be a positive integer. Then,

$a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$.

Congruences of Sums and Products

Theorem: Let m be a positive integer. If $\boldsymbol{a \equiv b \pmod{m}}$ and $\boldsymbol{c \equiv d \pmod{m}}$, then

$\boldsymbol{a + c \equiv b + d \pmod{m}}$ and $\boldsymbol{ac \equiv bd \pmod{m}}$

Proof:

Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, there are integers s and t with $\boldsymbol{b = a + sm}$ and $\boldsymbol{d = c + tm}$.

Therefore,

- $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$
- $b\,d = (a + sm)\,(c + tm) = ac + m(at + cs + stm)$.

Hence, $\boldsymbol{a + c \equiv b + d \pmod{m}}$ and $\boldsymbol{ac \equiv bd \pmod{m}}$.

Example: $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$,

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$$

Algebraic Manipulation of Congruences

- **Multiplying** both sides of a valid congruence by an integer preserves validity. If $a \equiv b \pmod{m}$ holds then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer, holds by congruence of products Theorem with $d = c$.

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

If $a \equiv b \pmod{m}$ holds then $c + a \equiv c + b \pmod{m}$, where c is any integer, holds by the Theorem with $d = c$.

- **Dividing** a congruence by an integer does not always produce a valid congruence.

Example: The congruence $14 \equiv 8 \pmod{6}$ holds. But dividing both sides by 2 does not produce a valid congruence since $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod{6}$.

Computing the **mod** m Function of Products and Sums

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

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

and

ab **mod** m = ((a **mod** m) (b **mod** m)) **mod** m.

Proof: By the definitions of mod m and of congruence modulo m, we know that:

- $a \equiv (a \bmod m) \pmod{m}$
- $b \equiv (b \bmod m) \pmod{m}$. Hence, from the previous theorem:
- $a + b \equiv (a \bmod m) + (b \bmod m) \pmod{m}$
- $ab \equiv (a \bmod m)(b \bmod m) \pmod{m}$.

Arithmetic Modulo m 1

Definitions: Let $\mathbf{Z}_m$ be the set of nonnegative integers less than m: $\{0,1, \ldots, m-1\}$

- The operation $+_m$ is defined as $a +_m b = (a+b)$ **mod** m. *(addition modulo m)*
- The operation $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b)$ **mod** m. *(multiplication modulo m)*
- Using these operations is said to be doing ***arithmetic modulo m.***

Example: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution:

- $7 +_{11} 9 = (7+9)$ **mod** 11 = 16 **mod** 11 = 5.
- $7 \cdot_{11} 9 = (7 \cdot 9)$ **mod** 11 = 63 **mod** 11 = 8.

Arithmetic Modulo m_2

Closure: If a and b belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.

Associativity: If a, b, and c belong to Z_m,

$$(a +_m b) +_m c = a +_m (b +_m c)$$

$$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$$

Commutativity: If a and b belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.

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 $a \cdot_m 1 = a$.

Arithmetic Modulo m_3

Additive inverses: If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $\boldsymbol{m-a}$ is the additive inverse of a module m.

- 0 is its own additive inverse.
- $a +_m (m-a) = 0$ and $0 +_m 0 = 0$

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 $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

MESUT OZDAG, PH.D.
MESUT.OZDAG@UCF.EDU