Day 3

# Discrete Mathematics

## Number theory

Dr. Abhijit Debnath

University of Engineering and Management

Reference book for this material is

Rosen, K. H., & Krithivasan, K. (1999). *Discrete mathematics and its applications* (Vol. 6). New York: McGraw-hill.

# THE DIVISION ALGORITHM

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

In the equality given in the division algorithm, d is called the *divisor*, a is called the *dividend*, q is called the *quotient*, and r is called the *remainder*.

# Congruent modulo

If $a$ and $b$ are integers and $m$ is a positive integer, then $a$ is *congruent to b modulo m*, if $m$ divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate 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** (plural **moduli**). If $a$ and $b$ are not congruent modulo $m$, we write $a \not\equiv b \pmod{m}$.

# Congruent modulo

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. We use the notation $a \equiv b \pmod{m}$ to indicate 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** (plural **moduli**). If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

# Congruent modulo

## Theorem:

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 $a = b + km$.

***Proof:*** If $a \equiv b \pmod{m}$, by the definition of congruence (Definition 3), we know that $m \mid (a - b)$. This means that there is an integer $k$ such that $a - b = km$, so that $a = b + km$.
Conversely, if there is an integer $k$ such that $a = b + km$, then $km = a - b$. Hence, $m$ divides $a - b$, so that $a \equiv b \pmod{m}$.

# Congruent modulo

## Theorem:

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

***Proof:*** We use a direct proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 4 there are integers s and t with $b = a + sm$ and $d = c + tm$. Hence, $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$

and

$bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$.

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

# Congruent modulo

**1.** What are the quotient and remainder when
**a)** 19 is divided by 7?
**b)**$-111$ is divided by 11?
**c)** 789 is divided by 23?
**d)** 1001 is divided by 13?
**e)** 0 is divided by 19?
**f )** 3 is divided by 5?
**g)**$-1$ is divided by 3?
**h)** 4 is divided by 1?
**2.** What are the quotient and remainder when
**a)** 44 is divided by 8?
**b)** 777 is divided by 21?
**c)**$-123$ is divided by 19?
**d)**$-1$ is divided by 23?
**e)**$-2002$ is divided by 87?
**f )** 0 is divided by 17?
**g)** 1,234,567 is divided by 1001?
**h)**$-100$ is divided by 101?

# Congruent modulo

Suppose that a and b are integers, $a \equiv 11 \pmod{19}$, and $b \equiv 3 \pmod{19}$. Find the integer c with $0 \leq c \leq 18$ such that

**a)** $c \equiv 13a \pmod{19}$.

**b)** $c \equiv 8b \pmod{19}$.

**c)** $c \equiv a - b \pmod{19}$.

**d)** $c \equiv 7a + 3b \pmod{19}$.

**e)** $c \equiv 2a2 + 3b2 \pmod{19}$.

**f )** $c \equiv a3 + 4b3 \pmod{19}$.

# Congruent modulo

Evaluate these quantities.

**a)** $-17$ **mod** $2$ **c)** $-101$ **mod** $13$ **b)** $144$ **mod** $7$

**d)** $199$ **mod** $19$

Evaluate these quantities.

**a)** $13$ **mod** $3$ **c)** $155$ **mod** $19$ **b)** $-97$ **mod** $11$

**d)** $-221$ **mod** $23$

# Congruent modulo

Evaluate these quantities.

**a)** $-17$ **mod** 2 **c)** $-101$ **mod** 13 **b)** 144 **mod** 7

**d)** 199 **mod** 19

Evaluate these quantities.

**a)** 13 **mod** 3 **c)** 155 **mod** 19 **b)** $-97$ **mod** 11

**d)** $-221$ **mod** 23

# Thank you



UNIVERSITY OF ENGINEERING & MANAGEMENT
Good Education, Good Jobs