INFORMATION & COMPUTER SCIENCES
UNIVERSITY of HAWAI'I at MĀNOA

Ch 4.1: Divisibility and Modular Arithmetic

ICS 141: Discrete Mathematics for Computer Science I

KYLE BERNEY
DEPARTMENT OF ICS, UNIVERSITY OF HAWAII AT MANOA

Divisibility

- Let $a, b \in \mathbb{Z}$ such that $a \neq 0$.
- We say a divides b, denoted $a \mid b$, if there exists an integer c such that

$$b = ac$$

  or equivalently, if $b/a \in \mathbb{Z}$.
- When a divides b
  - a is a factor (or divisor) of b
  - b is a multiple of a
- If a does not divide b, we use the notation $a \nmid b$

Properties of Divisibility

- Theorem 1: Let a, b, and c be integers, such that $a \neq 0$.

  1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  2. If $a \mid b$, then $a \mid bc$, for all integers c.
  3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Properties of Divisibility

- Theorem 1: Let a, b, and c be integers, such that $a \neq 0$.

  1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  2. If $a \mid b$, then $a \mid bc$, for all integers c.
  3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

- Proof of 1: By definition of divisibility, there exists integers x and y such that

$$b = ax \quad \text{and} \quad c = ay \ .$$

  Hence,

$$b + c = ax + ay = a(x + y) \ .$$

  Therefore, by definition of divisibility, $a \mid (b + c)$.

Properties of Divisibility

- Theorem 1: Let a, b, and c be integers, such that $a \neq 0$.

  1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  2. If $a \mid b$, then $a \mid bc$, for all integers c.
  3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

- Proof of 2: Let c be an arbitrary integer. By definition of divisibility, there exists an integers x such that

  $$b = ax \ .$$

  Hence,

  $$bc = (ax)c = a(xc) \ .$$

  Therefore, by definition of divisibility, $a \mid bc$.

Properties of Divisibility

- Theorem 1: Let a, b, and c be integers, such that $a \neq 0$.

  1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  2. If $a \mid b$, then $a \mid bc$, for all integers c.
  3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

- Proof of 3: By definition of divisibility, there exists integers x and y such that

$$b = ax \quad \text{and} \quad c = by \ .$$

  Hence,

$$c = by = (ax)y = a(xy) \ .$$

  Therefore, by definition of divisibility, $a \mid c$.

Properties of Divisibility

- Corollary: Let a, b, and c be integers, such that $a \neq 0$. If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for all integers x and y.

Properties of Divisibility

- Corollary: Let a, b, and c be integers, such that $a \neq 0$. If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for all integers x and y.

- Proof: It follows from part 2 of Theorem 1 that $a \mid bx$ and $a \mid cy$ for all integers x and y. And from part 1 of Theorem 1, $a \mid (bx + cy)$.

The Division Algorithm

- Theorem 2: Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. There exists unique integers q and r, where $0 \leq r < d$, such that

$$a = dq + r \ .$$

- a is called the dividend
- d is called the divisor
- q is called the quotient
- r is called the remainder

The Division Algorithm

- Theorem 2: Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. There exists unique integers q and r, where $0 \leq r < d$, such that

$$a = dq + r \ .$$

- a is called the dividend
- d is called the divisor
- q is called the quotient
- r is called the remainder

- This theorem is known as the division algorithm, despite it not being an algorithm

Modular Arithmetic

- Theorem 3: Let $m \in \mathbb{Z}^+$. The integers a and b are congruent modulo m if and only if there exists an integer k such that

$$a = b + km \ .$$

  Or equivalently, m is a divisor of the difference $a - b$ and $b - a$.

- If a is congruent to b modulo m, we write

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

- m is called the modulus of the congruence relation

Residue Class

- Definition: The set of integers congruent to $a \pmod{m}$ is called the residue class (or congruence class) of a and is denoted by $[a]_m$.

- The elements of $[a]_m$ are called residues
- The least non-negative element of $[a]_m$ is called the reduced residue of a

Residue Class

- Definition: The set of integers congruent to $a \pmod{m}$ is called the residue class (or congruence class) of a and is denoted by $[a]_m$.

- The elements of $[a]_m$ are called residues
- The least non-negative element of $[a]_m$ is called the reduced residue of a

- Ex: For $m = 4$,

$$[8]_4 = \{\ldots, -8, -4, 0, 4, 8, \ldots\} = [0]_4$$

Reduced Residue

- Proposition: Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. The reduced residue of a modulo m is the remainder of a/m.

Reduced Residue

- Proposition: Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. The reduced residue of a modulo m is the remainder of a/m.

- Proof: Let r be the remainder of a/m, i.e., using the division algorithm

$$a = mq + r$$

where $0 \leq r < m$. Assume for the sake of contradiction that r is not the reduced residue of a modulo m. Hence, there must exist another member of the residue class $[r]_m$ that is both smaller than r and non-negative.

Reduced Residue

- Proposition: Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. The reduced residue of a modulo m is the remainder of a/m.

- Proof: Consider the next smallest member of $[r]_m$, which is $r - m$.

$$0 - m \leq r - m < m - m = 0$$

A contradiction, since we assumed there existed a smaller member of $[r]_m$ that is also non-negative. Therefore, r is the reduced residue of a modulo m. ■

Modular Arithmetic

- Theorem 4: Let $m \in \mathbb{Z}^+$ and $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

  1. $a + c \equiv b + d \pmod{m}$
  2. $ac \equiv bd \pmod{m}$
  3. $a^k \equiv b^k \pmod{m}$, for all $k \in \mathbb{N}$

Modular Arithmetic

- Theorem 4: Let $m \in \mathbb{Z}^+$ and $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

  1. $a + c \equiv b + d \pmod{m}$
  2. $ac \equiv bd \pmod{m}$
  3. $a^k \equiv b^k \pmod{m}$, for all $k \in \mathbb{N}$

- Proof of 1: Let m be an arbitrary positive integer and let a, b, c, and d be arbitrary integers such that $a \equiv \pmod{m}$ and $c \equiv d \pmod{m}$. From Theorem 3, there exists integers x and y such that

$$a = b + xm$$

$$\text{and} \quad c = d + ym\ .$$

Modular Arithmetic

- Theorem 4: Let $m \in \mathbb{Z}^+$ and $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

  1. $a + c \equiv b + d \pmod{m}$
  2. $ac \equiv bd \pmod{m}$
  3. $a^k \equiv b^k \pmod{m}$, for all $k \in \mathbb{N}$

- Proof of 1: Hence,

$$\begin{aligned} a + c &= (b + xm) + (d + ym) \\ &= (b + d) + m(x + y) \ . \end{aligned}$$

  It follows from Theorem 3 that

$$a + c \equiv b + d \pmod{m} \ .$$

Modular Arithmetic

- Theorem 4: Let $m \in \mathbb{Z}^+$ and $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

  1. $a + c \equiv b + d \pmod{m}$
  2. $ac \equiv bd \pmod{m}$
  3. $a^k \equiv b^k \pmod{m}$, for all $k \in \mathbb{N}$

- Proof of 2: Let m be an arbitrary positive integer and let a, b, c, and d be arbitrary integers such that $a \equiv \pmod{m}$ and $c \equiv d \pmod{m}$. From Theorem 3, there exists integers x and y such that

$$a = b + xm$$

$$\text{and} \quad c = d + ym\ .$$

Modular Arithmetic

- Theorem 4: Let $m \in \mathbb{Z}^+$ and $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

  1. $a + c \equiv b + d \pmod{m}$
  2. $ac \equiv bd \pmod{m}$
  3. $a^k \equiv b^k \pmod{m}$, for all $k \in \mathbb{N}$

- Proof of 2: Hence,

$$\begin{aligned} a &= (b + xm)(d + ym) \\ &= bd + bym + dxm + xym^2 \\ &= bd + m(by + dx + xym) \ . \end{aligned}$$

It follows from Theorem 3 that

$$ac \equiv bd \pmod{m} \ .$$

Modular Arithmetic

- Theorem 4: Let $m \in \mathbb{Z}^+$ and $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

  1. $a + c \equiv b + d \pmod{m}$
  2. $ac \equiv bd \pmod{m}$
  3. $a^k \equiv b^k \pmod{m}$, for all $k \in \mathbb{N}$

- Proof of 3: Let m be an arbitrary positive integer and let a, b, c, and d be arbitrary integers such that $a \equiv \pmod{m}$ and $c \equiv d \pmod{m}$. From Theorem 3, there exists integers x and y such that

$$a = b + xm$$

$$\text{and} \quad c = d + ym\ .$$

  Let k be an arbitrary positive integer. (If $k = 0$, the proof is trivial.)

Modular Arithmetic

- Theorem 4: Let $m \in \mathbb{Z}^+$ and $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

  1. $a + c \equiv b + d \pmod{m}$
  2. $ac \equiv bd \pmod{m}$
  3. $a^k \equiv b^k \pmod{m}$, for all $k \in \mathbb{N}$

- Proof of 3: Consider the identity that for any integers x and y,

$$\begin{aligned} & x^k - y^k \\ =& (x-y)(x^{k-1} + x^{k-2}y + x^{k-3}y^2 + \ldots + xy^{k-2} + y^{k-1}) \,. \end{aligned}$$

  Setting $x = a$ and $y = b$.

Modular Arithmetic

- Theorem 4: Let $m \in \mathbb{Z}^+$ and $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,

  1. $a + c \equiv b + d \pmod{m}$
  2. $ac \equiv bd \pmod{m}$
  3. $a^k \equiv b^k \pmod{m}$, for all $k \in \mathbb{N}$

- Proof of 3: Consider the identity that for any integers x and y,

$$\begin{aligned} & a^k - b^k \\ =&(a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + a^{k-1}) \\ =&xm(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + a^{k-1}) \,. \end{aligned}$$

  It follows from Theorem 3 that $a^k \equiv b^k \pmod{m}$.

Modular Arithmetic

- Corollary: Let $m \in \mathbb{Z}^+$ and let $a, b \in \mathbb{Z}$. Then,

  1. $(a + b) \pmod{m} \equiv (a \pmod{m}) + (b \pmod{m}) \pmod{m}$
  2. $ab \pmod{m} \equiv (a \pmod{m})(b \pmod{m}) \pmod{m}$