Chapter 4, Number Theory (1)

Young-Rae Cho
Associate Professor
Department of Computer Science
Baylor University

4.1. Divisibility and Modular Arithmetic

Division
- Let \( a, b \in \mathbb{Z} \) where \( a \neq 0 \).
- "a divides b" if there is \( c \in \mathbb{Z} \) such that \( b = ac \) (if \( b/a \) is an integer).
- Notation: \( a \mid b \)
- \( a \) is a factor of \( b \).
- \( b \) is a multiple of \( a \).
- "a does not divide b" otherwise.

Theorems
- \( (a \mid b \land a \mid c) \rightarrow a \mid (b+c) \)
- \( a \mid b \rightarrow a \mid bc \), \( \forall c \in \mathbb{Z} \)
- \( (a \mid b \land b \mid c) \rightarrow a \mid c \)
- Corollary: \( (a \mid b \land a \mid c) \rightarrow a \mid (mb+nc) \), \( m, n \in \mathbb{Z} \)
The Division Algorithm

- **Theorem**
  - Let \( a \in \mathbb{Z} \) and \( d \in \mathbb{Z}^+ \).
  - There are unique \( q, r \in \mathbb{Z} \) (\( 0 \leq r < d \)) such that \( a = dq + r \).
  - \( d \): divisor, \( a \): dividend, \( q \): quotient, \( r \): remainder

- **div Operator**
  - The quotient \( q = a \div d \)
  - How to compute \((a \div d)\)?

- **mod Operator**
  - The remainder \( r = a \mod d \)
  - How to compute \((a \mod d)\)?

Modular Arithmetic

- **Modular Congruence**
  - Let \( a, b \in \mathbb{Z} \) and \( m \in \mathbb{Z}^+ \).
  - \( a \) is congruent to \( b \) modulo \( m \) if \( m | (a-b) \).
  - Notation: \( a \equiv b \pmod{m} \)

- **Theorems**
  - \( a \equiv b \pmod{m} \) \iff \( a \mod m = b \mod m \)
  - \( a \equiv b \pmod{m} \) \iff \( \exists k \in \mathbb{Z}, a = b + km \)
  - If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then
    - \( a+c \equiv b+d \pmod{m} \)
    - \( ac \equiv bd \pmod{m} \)
  - Corollary: \( (a+b) \mod m = ((a \mod m) + (b \mod m)) \mod m \)
  - Corollary: \( ab \mod m = ((a \mod m)(b \mod m)) \mod m \)
Questions?

- Lecture Slides are found on the Course Website, web.ecs.baylor.edu/faculty/cho/2350