Chapter 4, Number Theory (2)

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

4.3. Primes and Greatest Common Divisors

- **Primes**
  - An integer \( p > 1 \) is prime iff the only positive factors of \( p \) are 1 and \( p \).
  - For example, 2, 3, 5, 7, 11, 13, 17, ...
  - A non-prime integers \( c > 1 \) is called composite.

- **Theorem 1 (Prime Factorization)**
  - Every positive integer greater than 1 has a unique representation as a prime or as the product of a non-decreasing series of two or more primes.
  - For example,
    - \( 4 = 2^2 \)
    - \( 100 = 2^2 \cdot 5^2 \)
    - \( 999 = 3^3 \cdot 37 \)
    - \( 2001 = 3 \cdot 23 \cdot 29 \)
**Trial Division**

- **Theorem 2**
  - If \( n \) is a composite integer, \( n \) has a prime divisor less than or equal to \( \sqrt{n} \).
  - Example: Show that 101 is prime.
    - Primes not exceeding \( \sqrt{101} \) are 2, 3, 5, and 7.
    - 101 is not divisible by any of 2, 3, 5, or 7.
    - Therefore, 101 is a prime.

- **Theorem 3**
  - There are infinitely many primes.
  - Prove?

---

**Greatest Common Divisors**

- **Definition**
  - The greatest common divisor \( \text{gcd}(a,b) \) of integers \( a \) and \( b \) (not both 0) is the largest integer \( d \) that is a divisor both of \( a \) and of \( b \).
  - \( d = \text{gcd}(a,b) = \max(\{d| d|a \land d|b\}) \)
  - \( \Leftrightarrow d|a \land d|b \land \forall e \in \mathbb{Z}, (e|a \land e|b) \rightarrow (d \geq e) \)

- **Relative Primality**
  - Integers \( a \) and \( b \) are called relatively prime (co-prime) iff \( \text{gcd}(a,b) = 1 \).
  - Example: 10 and 21

- **Finding gcd using Prime Factorization**
  - When \( a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n} \) and \( b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n} \),
  
  \[
  \text{gcd}(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_n^{\min(a_n,b_n)}
  \]
Least Common Multiples

- **Definition**
  - The least common multiple \( \text{lcm}(a,b) \) of positive integers \( a \) and \( b \) is the smallest positive integer that is a multiple both of \( a \) and of \( b \).
  
  \[
  m = \text{lcm}(a,b) = \min\{m | a|m \land b|m\} \\
  \iff a|m \land b|m \land \forall n \in \mathbb{Z}: (a|n \land b|n) \rightarrow (m \leq n)
  \]

- **Finding lcm using Prime Factorization**
  - When \( a = p_1^{a_1}p_2^{a_2} \ldots p_n^{a_n} \) and \( b = p_1^{b_1}p_2^{b_2} \ldots p_n^{b_n} \),
  
  \[
  \text{lcm}(a,b) = p_1^{\max(a_1,b_1)}p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,b_n)}
  \]

- **Theorem**
  - Let \( a \) and \( b \) be positive integers. Then, \( ab = \gcd(a,b) \times \text{lcm}(a,b) \)

Euclidean Algorithm

- **Background**
  - Finding gcd by prime factorization is inefficient.

- **Euclid’s Theorem**
  - Let \( a = bq + r \) where \( a, b, q, \) and \( r \) are integers. Then, \( \gcd(a,b) = \gcd(b,r) \).
  
  Prove ?

- **Euclidean Algorithm**
  - To find \( \gcd(a,b) \), apply the Theorem repeatedly until the remainder of 0 occurs.
  
  Examples ?

  Pseudocode ?
gcd as Linear Combinations

- **Bezout’s Theorem**
  - Let $a$ and $b$ be positive integers. Then, there exist integers $s$ and $t$ such that $\text{gcd}(a,b) = sa + tb$.

- **Extended Euclidean Algorithm**
  - Expressing $\text{gcd}(a,b)$ as a linear combination of $a$ and $b$.
  - Examples?

- **Some Miscellaneous Lemmas**
  - $\forall a,b,c \in \mathbb{Z}^+, \text{if } \text{gcd}(a,b)=1 \land a \mid bc, \text{then } a \mid c$.
  - If $p$ is prime and $p | a_1 a_2 \ldots a_n$ (for integers $a_i$) then $\exists i, p | a_i$.
  - $m \in \mathbb{Z}^+, a,b,c \in \mathbb{Z}$, if $ac \equiv bc \pmod{m}$ $\land$ $\text{gcd}(c,m)=1$, then $a \equiv b \pmod{m}$.

4.4. Solving Congruences

- **Linear Congruences**
  - A congruence of the form $ax \equiv b \pmod{m}$ where $m \in \mathbb{Z}^+$, $a,b \in \mathbb{Z}$, and $x$ is a variable.
  - Example: Solve the linear congruence $3x \equiv 4 \pmod{7}$.
    (Find $x$'s that satisfy $3x \equiv 4 \pmod{7}$.)

- **Theorem**
  - If $a$ and $m$ are relatively prime integers and $m > 1$, then there is a unique $\bar{a} \in \mathbb{Z}^+$ that is an inverse of $a$ modulo $m$.
  - Prove?

  - Example: Find an inverse of 3 modulo 7.
Questions?

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