[CSED261] Discrete Mathematics for Computer Science

Lecture 10

Basic Number Theory

Suha Kwak

suha.kwak@postech.ac.kr

Dept. of Computer Science and Engineering

POSTECH

Divisibility and Modular Arithmetic

Division

- Definition
  - If a and b are integers with $a \neq 0$, then a divides b if there exists an integer c such that $b = ac$.
  - When a divides b, we say that a is a factor or divisor of b and that b is a multiple of a.

- Notation
  - The notation $a \mid b$ denotes that a divides b.
  - If $a \mid b$, then $\frac{b}{a}$ is an integer.
  - If a does not divide b, we write $a \nmid b$.

Properties of Divisibility

- Let a, b, and c be integers, where $a \neq 0$.
  - (i) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  - (ii) If $a \mid b$, then $a \mid bc$ for all integers c.
  - (iii) If $a \mid b$ and $b \mid c$, then $a \mid c$.

- If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Division Algorithm

- Division
  - When an integer is divided by a positive integer, there is a quotient and a remainder.
  - This is called the division algorithm, but is actually a theorem.

- Division algorithm
  - If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.
- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

Definitions of functions

div and mod

$$q = a \text{ div } d$$

$$r = a \text{ mod } d$$

Division Algorithm

- Examples
  - When 101 is divided by 11,
    - The quotient is $9 = 101 \text{ div } 11$, and
    - The remainder is $2 = 101 \bmod 11$.
  - When -11 is divided by 3,
    - The quotient is $-4 = -11 \text{ div } 3$, and
    - The remainder is $1 = -11 \bmod 3$.

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 $a - b$.
  - $a \equiv b \pmod{m}$
- We say that
  - $a \equiv b \pmod{m}$ is a congruence, and
  - m is the modulus of the congruence.
- Two integers are congruent $\bmod m$ if and only if they have the same remainder when divided by m.
- If a is not congruent to b modulo m, we write

$$a \not\equiv b \pmod{m}$$

Congruence Relation

- Example 1
  - Determine whether 17 is congruent to 5 modulo 6.
  - $17 \equiv 5 \pmod 6$ because 6 divides $17 - 5 = 12$.

- Example 2
  - Determine whether 24 and 14 are congruent modulo 6.
  - $24 \not\equiv 14 \pmod 6$ since $24 - 14 = 10$ is not divisible by 6.

$(\mathrm{mod}\ m)$ vs. $\mathrm{mod}\ m$

- The different use of mod:
  - $a \equiv b\ (\mathrm{mod}\ m)$
    - A relation on the set of integers
  - $a\ \mathrm{mod}\ m = b$
    - A function

- Theorem
  - Let a and b be integers, and let m be a positive integer.
  - Then $a \equiv b\ (\mathrm{mod}\ m)$ if and only if $a\ \mathrm{mod}\ m = b\ \mathrm{mod}\ m$.

Congruences of Sums and Products

- 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
  - Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, there are integers s and t with $b = a + sm$ and $d = c + tm$.
  - Therefore,
    - $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$
    - $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$
  - Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

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.
- 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.
- Dividing a congruence by an integer does not always produce a valid congruence.
  - $14 \equiv 8 \pmod{6}$, but $7 \not\equiv 4 \pmod{6}$.
  - See page 33.

$\mathrm{mod}\ m$ Function of Products and Sums

- Let m be a positive integer and let a and b be integers.
  - $(a + b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$
  - $ab \bmod m = \big((a \bmod m) \cdot (b \bmod m)\big) \bmod m$

Integer Representations

Representations of Integers

- Decimal (or base 10) notation
  - $965 = 9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$
- We can represent numbers using any base b, where b is a positive integer greater than 1.
- Important bases for computing and communications
  - $b = 2$ (*binary*)
  - $b = 8$ (*octal*)
  - $b = 16$ (*hexadecimal*)
- The ancient Mayans used base 20 and the ancient Babylonians used base 60.

Base b Representations

- Theorem
  - Let b be a positive integer greater than 1.
  - Then if n is a positive integer, it can be expressed

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

where k is a nonnegative integer, a_0, a_1, …, a_k are nonnegative integers less than b, and $a_k \neq 0$.

  - The a_i, $i = 0, \ldots, k$ are called the base-b digits of the representation.

- Base b expansion
  - The above representation of n is called the base-b expansion of n and is denoted by $(a_k a_{k-1} \cdots a_1 a_0)_b$.
  - We usually omit the subscript 10 for base 10 expansions.

Base b Representations

- Binary expansions
  - Most computers represent integers and do arithmetic with binary (base 2) expansions of integers.
  - In these expansions, the only digits used are 0 and 1.
  - Example
    - What is the decimal expansion of the integer that has $(101011111)_2$ as its binary expansion?

- Octal expansions
  - The octal expansion (base 8) uses the digits $\{0,1,2,3,4,5,6,7\}$.
  - Example
    - What is the decimal expansion of the number with octal expansion $(111)_8$?

Base b Representations

- Hexadecimal Expansions
  - The hexadecimal expansion needs 16 digits, but our decimal system provides only 10.
  - So letters are used for the additional symbols.
  - The hexadecimal system uses the digits $\{0,1, \ldots, 9, A, B, \ldots, F\}$.
    - The letters A through F represent the decimal numbers 10~15.
- Example
  - What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?
  - What is the decimal expansion of the number with hexadecimal expansion $(E5)_{16}$?

Base Conversion

- Base conversion algorithm

Procedure $base\_b(n, b$: positive integers with $b > 1)$

$q := n$

$k := 0$

while $(q \neq 0)$

$a_k := q \bmod b$

$q := q \operatorname{div} b$

$k := k + 1$

return $(a_{k-1}, a_{k-2}, \ldots, a_1, a_0)$

- q represents the quotient obtained by successive divisions by b, starting with $q = n$.
- The digits in the base b expansion are the remainders of the division given by $q \bmod b$.

Base Conversion

- Examples
  - Find the octal expansion of $(12345)_{10}$.
    - Successively dividing by 8 gives:

$$12345 = 8 \cdot 1543 + 1$$
$$1543 = 8 \cdot 192 + 7$$
$$192 = 8 \cdot 24 + 0$$
$$24 = 8 \cdot 3 + 0$$
$$3 = 8 \cdot 0 + 3$$

    - The remainders are the digits yielding $(30071)_8$.

  - Find the hexadecimal expansions of $(1111010111100)_2$.
    - Group the digits into blocks of four $(0011\ 1110\ 1011\ 1100)_2$ adding initial 0s as needed.
    - The blocks from left to right correspond to 3,E,B, and C.
    - Hence, the solution is $(3\mathrm{EBC})_{16}$.

Binary Addition of Integers

- Algorithm

Procedure $add(a, b$: positive integers$)$

binary expansions of $a := (a_{n-1}, a_{n-2}, \ldots, a_0)_2$

binary expansions of $b := (b_{n-1}, b_{n-2}, \ldots, b_0)_2$

$c := 0$

for $j := 1$ to $n - 1$

$d := \lfloor (a_j + b_j + c)/2 \rfloor$

$s_j := a_j + b_j + c - 2d$

$c := d$

$s_n := c$

return $(s_n, s_{n-1}, \ldots, s_1, s_0)_b$

- The number of additions of bits is $O(n)$.

Binary Multiplication of Integers

- Algorithm

Procedure $multiply(a, b$: positive integers$)$

  binary expansions of $a := (a_{n-1}, a_{n-2}, \ldots, a_0)_2$

  binary expansions of $b := (b_{n-1}, b_{n-2}, \ldots, b_0)_2$

  for $j := 0$ to $n - 1$

    if $b_j = 1$ **then** $c_j = a$ shifted j places.

    else $c_j := 0$

  $p := 0$

  for $j := 0$ to $n - 1$

    $p := p + c_j$

return p

- The number of additions of bits is $O(n^2)$.

Primes and Greatest Common Divisors

Primes

- Definition
  - A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p.
  - A positive integer that is greater than 1 and is not prime is called composite.

- Example
  - The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic

- Theorem
  - Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size.

- Examples
  - $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
  - $641 = 641$
  - $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
  - $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Prime Factorization

Greatest Common Divisor

- Definition
  - Let a and b be integers, not both zero.
  - The largest integer d such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of a and b.
  - The greatest common divisor of a and b is denoted by $\gcd(a, b)$.
- Examples
  - What is the greatest common divisor of 24 and 36?
    - $\gcd(24, 36) = 12$
  - What is the greatest common divisor of 17 and 22?
    - $\gcd(17, 22) = 1$

Greatest Common Divisor

- The integers a and b are relatively prime if their GCD is 1.
  - Example: 17 and 22

- The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
  - Example: Determine whether the integers 10, 17 and 21 are pairwise relatively prime.
    - $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$, and $\gcd(17, 21) = 1$.
    - Hence 10, 17, and 21 are pairwise relatively prime.
  - Example: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.
    - $\gcd(10,24) = 2$
    - 10, 19, and 24 are not pairwise relatively prime.

Finding GCD Using Prime Factorizations

- Suppose the prime factorizations of a and b are:

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n},$$

where each exponent is a non-negative integer. Then,

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}.$$

- This formula is valid since the integer on the right divides both a and b. No larger integer can divide both a and b.

- Example
  - $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^5$
  - $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 20.$

Finding GCD Using Euclidean Algorithm

- Euclidean algorithm for finding GCDs
  - An efficient method for computing the GCD of two integers.
  - Based on the idea that $\gcd(a, b) = \gcd(b, r)$ when $a > b$ and r is the remainder when a is divided by b.

- An example: Find $\gcd(91, 287)$.
  - $287 = 91 \cdot 3 + 14$
  - $91 = 14 \cdot 6 + 7$
  - $14 = 7 \cdot 2 + 0$ (Stopping condition: Found $r = 0$)
  - $\gcd(91, 287) = \gcd(91, 14) = \gcd(14, 7) = 7$

Finding GCD Using Euclidean Algorithm

- Pseudo-code

Procedure $gcd(a, b: \text{positive integers})$
  $x := a$
  $y := b$
  while $y \neq 0$
    $r := x \bmod y$
    $x := y$
    $y := r$
return x

Finding GCD Using Euclidean Algorithm

- Correctness of the algorithm
  - **Lemma**:
    Let $a = bq + r$, where a, b, q, and r are integers.
    Then $\gcd(a, b) = \gcd(b, r)$.
  - **Proof**:
    - Suppose that d divides both a and b.
      Then d also divides $a - bq = r$.
      Hence, any common divisor of a and b must also be a common divisor of b and r.
    - Suppose that d divides both b and r.
      Then d also divides $bq + r = a$.
      Hence, any common divisor of b and r must also be a common divisor of a and b.
    - Therefore, $\gcd(a, b) = \gcd(b, r)$.

Least Common Multiple

- Definition
  - The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b.
  - It is denoted by $\mathrm{lcm}(a, b)$.

- The least common multiple can also be computed from the prime factorizations.

$$\mathrm{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}.$$

  - This number is divided by both a and b, and no smaller number is divided by a and b.

- The GCD and the LCM of two integers are related by

$$ab = \gcd(a, b) \cdot \mathrm{lcm}(a, b)$$

GCD as Linear Combination

- Bézout's theorem
  - If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

- Definition: Bézout's identity
  - If a and b are positive integers, then integers s and t such that $\gcd(a, b) = sa + tb$ are called Bézout coefficients of a and b .
  - The equation $\gcd(a, b) = sa + tb$ is called Bézout's identity.

- Example
  - $\gcd(6,14) = 2 = (-2) \cdot 6 + 1 \cdot 14$

Dividing Congruence by an Integer

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence.
- However, dividing by an integer relatively prime to the modulus does produce a valid congruence.

- Theorem
  - Let m be a positive integer and let a, b, and c be integers.
  - If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.
- Proof
  - $ac \equiv bc \pmod{m} \Leftrightarrow m \mid (ac - bc) \Leftrightarrow m \mid c(a - b)$
  - Since $\gcd(c, m) = 1$, $m \mid (a - b)$.
  - Hence, $a \equiv b \pmod{m}$.

Solving Congruence

Linear Congruence

- Linear congruence
  - A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.
  - The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.
- Inverse
  - An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be "an inverse of a modulo m".
  - Example
    - 5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1 \pmod{7}$.

One method of solving linear congruence makes use of an inverse $\bar{a}$, if it exists.
Although we cannot divide both sides of the congruence by a,
we can multiply by $\bar{a}$ to solve for x.

Inverse of a modulo m

- Theorem
  - If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists.
- Proof
  - [Bézout's Theorem] Since $\gcd(a, m) = 1$, there are integers s and t such that $sa + tm = 1$.
  - Hence, $sa + tm \equiv 1 \pmod{m}$.
  - Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$.
  - Consequently, s is an inverse of a modulo m.

The theorem guarantees that
an inverse of a modulo m exists
whenever a and m are relatively prime.

Finding Inverses

- The Euclidean algorithm and Bézout coefficients give us a systematic approach to finding inverses.
  - Example
    - Find an inverse of 3 modulo 7.
  - Solution
    - Because $\gcd(3,7) = 1$, an inverse of 3 modulo 7 exists. [by the theorem in the previous page]
    - Using the Euclidian algorithm: $7 = 2 \cdot 3 + 1$.
    - From this equation, we get $-2 \cdot 3 + 1 \cdot 7 = 1$, and see that −2 and 1 are Bézout coefficients of 3 and 7.
    - Hence −2 is an inverse of 3 modulo 7.
    - Also, every integer congruent to −2 modulo 7 is an inverse of 3 modulo 7 (*i.e.*, 5, −9, 12, …).

Finding Inverses

- The Euclidean algorithm and Bézout coefficients give us a systematic approach to finding inverses.
  - Example: Find an inverse of 101 modulo 4620.
  - Solution

$$4620 = 45 \cdot 101 + 75$$
$$101 = 1 \cdot 75 + 26$$
$$75 = 2 \cdot 26 + 23$$
$$26 = 1 \cdot 23 + 3$$
$$23 = 7 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

$$\gcd(101, 4620) = 1$$

(1) Euclidean algorithm

$$1 = 3 - 1 \cdot 2$$
$$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$$
$$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$$
$$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$$
$$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$$
$$= 26 \cdot 101 - 35 \cdot 75$$
$$1 = 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$$
$$= -35 \cdot 4620 + 1601 \cdot 101$$

(2) Working backwards

Bézout coefficients = -35 and 1601 ➡ 1601 is an inverse of 101 modulo 4620.

Using Inverses to Solve Congruence

- What are the solutions of $3x \equiv 4 \pmod 7$?
  - We found that −2 is an inverse of 3 modulo 7 (two slides back).
  - We multiply both sides of the congruence by −2 giving
    $$-2 \cdot 3x \equiv -2 \cdot 4 \pmod 7$$
  - Because $-6 \equiv 1 \pmod 7$ and $-8 \equiv 6 \pmod 7$,
    it follows that if x is a solution, then $x \equiv -8 \equiv 6 \pmod 7$.
  - The solutions are the integers x such that $x \equiv 6 \pmod 7$,
    namely, $6, 13, 20, \ldots$ and $-1, -8, -15, \ldots$