Integers & Division (Lecture – 1)

Dr. Nirnay Ghosh

Integers and Division

- **Number theory** is a branch of mathematics that explores integers and their properties.
  - Has many applications within computer science including:
    - Storage and organization of data
    - Cryptology
    - Error correcting codes
    - Random numbers generators
- **Integers**: The set of **integers** consists of zero (0), the positive natural numbers (1, 2, 3, …), and their additive inverses (the negative **integers**, i.e., −1, −2, −3, …).
  - **Z : integers {…, -2,-1, 0, 1, 2, …}**
  - **Z^+ : positive integers {1, 2, …}**
  - **Z^-: negative integers {-1, -2,…}**

Division

- **Definition:** Assume two integers a and b, such that $a \neq 0$ (a is not equal 0). We say that ***a divides b*** if there is an integer c such that $b = ac$. If a divides b we say that **a is a *factor* of b** and that **b is *multiple* of a**.
  - We denote a divides b as $a \mid b$.
  - We write $a \nmid b$ when a does not divide b.
- **<u>Theorem 1</u>**:

Let a, b, and c be integers, where $a \neq 0$. Then

(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 $a \mid c$.

- **<u>Corollary 1</u>:**

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.

The Division Algorithm

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 $a = dq + r$.

- <u>**Definition**</u>

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*. This notation is used to express the quotient and remainder:

$$q = a \textbf{ div } d, \quad r = a \textbf{ mod } d.$$

Primes & Fundamental Theorem of Arithmetic

- **<u>Definition</u>:** A positive integer p that greater than 1 and that is divisible only by 1 and by itself (p) is called **a prime**. A positive integer that is greater than 1 and is not prime is called *composite*.
  - Example: 2, 3, 5, 7, …..
- **<u>Fundamental Theorem of Arithmetic</u>:** Every positive integer greater than 1 can be expressed as prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size.
  - **Examples:** $100 = 2*2*5*5 = 2^2 5^2$, $641 = 641$, $999 = 3*3*3*37 = 3^3 37$, $1024 = 2*2*2*2*2*2*2*2*2*2 = 2^{10}$

Process of finding out factors of the product: **factorization.**

Primes and Composites

- **How to determine whether the number is a prime or a composite?**
- **Theorem-2**: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.
- Example: Find the prime factorization of 7007.
  - $\sqrt{7007} \sim 83$. So if we do not find any prime number till 83 which divides 7007, then it has no factors.
  - Starting with 2, none of the prime factors 2, 3, 5 divides 7007. However, 7 divides 7007, with $7007/7 = 1001$.
  - $\sqrt{1001} \sim 31$. So we have to check primes till 31 to determine if 1001 can be factorized.
  - None of 2, 3, 5 divides 1001. Again 7 divides 1001, as $1001/7 = 143$.
  - $\sqrt{143} \sim 12$. So we have to check primes till 12. None of 2, 3, 5, 7 divides 143. However, 11 divides 143, with $143/11 = 13$.
  - In this way, we continue to find the prime factors of $7007 = 7*7*11*13 = 7^2*11*13$.

The Infinitude of Primes

- It has long been known that there are infinitely many primes. This means that whenever $p_1, p_2, \ldots, p_n$ are the n smallest primes, we know there is a larger prime not listed.
- **Theorem**: There are infinitely many primes.
  - Proof given by Euclid in his famous mathematics text, *The Elements*.
- Mersenne Prime:
  - The largest Mersenne prime known (again as of early 2011) is $2^{43,112,609} - 1$, a number with nearly 13 million decimal digits, which was shown to be prime in 2008.
  - Great Internet Mersenne Prime Search (GIMPS), is devoted to the search for new Mersenne primes.

Greatest Common Divisor (GCD)

- **<u>Definition #1</u>**: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by gcd (a, b).
- **<u>Definition #2</u>**: The integers a and b are *relatively prime* if their greatest common divisor is 1.
  - Example: integers 17 and 22 are relatively prime as gcd (17,22) = 1.
- **<u>Definition #3</u>**: 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 integers 10, 17, 21 are pairwise relatively prime as gcd (10, 17) = 1, gcd (17, 21) = 1, and gcd (10, 21) = 1.

Greatest Common Divisor (GCD)

- Finding gcd using prime factorization:
  - Suppose prime factorization of positive integers *a* and *b* are given as:

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

  - where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either *a* or *b* are included in both factorizations, with zero exponents if necessary.
- The gcd (a, b) is given by:

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

Least Common Multiple (LCM)

- **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*. The least common multiple of *a* and *b* is denoted by lcm*(a, b)*.
- Finding lcm by prime factorization method:
  - Suppose that the prime factorizations of *a* and *b* are as before. Then the least common multiple of *a* and *b* is given by

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

- Relationship between greatest common division and least common multiple:
- **Theorem 3**: Let *a* and *b* be positive integers. Then *ab* = gcd*(a, b)*. lcm*(a, b)*.

Euclid Algorithm for Finding GCDs

- Finding the greatest common divisor requires factorization
- Factorization can be cumbersome and time consuming since we need to find all factors of the two integers that can be very large
- A more efficient method for computing the gcd exists: **Euclid's Algorithm**
  - Successive divisions to reduce the problem of finding the greatest common divisor of two positive integers to the same problem with smaller integers, until one of the integers is zero.
- **Lemma:** Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

ALGORITHM 1 The Euclidean Algorithm.

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
  $r := x$ **mod** y
  $x := y$
  $y := r$
return $x\{\gcd(a, b)$ is $x\}$

GCDs as Linear Combinations

- GCD (a, b) can be expressed as a **linear combination** with integer coefficients of a and b.
  - For example, gcd $(6, 14) = 2$, and $2 = (-2)*6 + 1*14$.
- **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:** 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. Also, the equation $gcd(a, b) = sa + tb$ is called *Bézout's identity*.
- General Method to find linear combination of two integers equal to their gcd:
  - Proceed by working backward through the divisions of the Euclidean algorithm
  - Requires a forward pass and a backward pass through the steps of the Euclidean algorithm