Discrete Structures

Integers and Division

Chapter 2, Sections 2.3 - 2.5

Dieter Fox

Integers

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

◇ $a \mid b$: a divides b if there is an integer c such that $b = ac$. When a divides b we say that a is a factor of b and that b is a multiple of a.

◇ **Theorem:**

1. if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
2. if $a \mid b$, then $a \mid bc$;
3. if $a \mid b$ and $b \mid c$, then $a \mid c$.

◇ **Prime:** 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.

◇ **Fundamental Theorem of Arithmetic:** Every positive integer can be written uniquely as the product of primes, where the prime factors are written in order of increasing size.

Division algorithm

- ♢ **Division algorithm:** Let a be an integer and d a poisitive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

- ♢ 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.

gcd and lcm

- ◊ **gcd**(a, b)**:** 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 integers a and b are relatively prime if gcd$(a, b) = 1$.

- ◊ The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if gcd$(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

- ◊ **lcm**(a, b)**:** The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b.

- ◊ **Theorem:** Let a and b be positive integers. Then $ab =$ gcd$(a, b) \cdot$ lcm(a, b).

Modular Arithmetic

- a **mod** m**:** Let a be an integers and m be a positive integer. We denote by a mod m the remainder when a is divided by m.

- $a \equiv b$ (**mod** m) If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$.

- **Theorem:** Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

- **Theorem:** Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d$ (mod m)) and $ac \equiv bd \pmod{m}$.

Euclidean Algorithm

◇ **Lemma:** Let $a = bq + r$, where a, b, q, and r are integers. Then gcd$(a, b) =$ gcd(b, r).