

# Theorems on the Division of Integers

**Axiom.** Every non-empty set of natural numbers always contains a smallest element.

**Theorem** (Division Theorem). For any integer  $b$  and any positive integer  $a$ , there exist a unique pair of integers  $(q, r)$  such that  $0 \leq r < a$  and  $b = aq + r$ .

**Definition** (Divisibility Relation).  $a$  divides  $b$ ,  $a|b$ , if and only if the division theorem implies  $b = aq + r$  where  $r = 0$ .

**Theorem** (Division of a Linear Combination). If  $a$ ,  $b$ , and  $c$  are integers so  $c|a$  and  $c|b$ , then  $c|as + bt$  for any integers  $s$  and  $t$ .

**Definition** (GCD). The greatest common divisor of  $a$  and  $b$ ,  $\gcd(a, b) = \max\{d : d \in \mathbb{Z} \text{ and } d|a \text{ and } d|b\}$ .

**Theorem** (GCD bounds). For every pair of positive integers  $(a, b)$ ,  $1 \leq \gcd(a, b) \leq \min(a, b)$ , where  $\min(a, b)$  is the minimum of  $a$  and  $b$ .

**Theorem** (GCD Duality Theorem).  $\gcd(a, b) = \min\{as + bt : (s, t) \in \mathbb{Z} \times \mathbb{Z}, as + bt > 0\}$

**Theorem** (GCD--Divisibility equivalence).  $c|\gcd(a, b)$  if and only if  $(c|a \text{ and } c|b)$

**Theorem** (Euclidian Algorithm Theorem). If  $b = aq + r$  where  $q$  and  $r$  are given by the Division Theorem, then either

$$r = 0 \text{ and } \gcd(a, b) = a, \quad \text{or} \quad 0 < r \text{ and } \gcd(a, b) = \gcd(a, r).$$

**Theorem** (Associativity of GCD). Suppose we have an infinite sequence of positive integers,  $a_1, a_2, a_3, \dots$ ,

$$\gcd(a_1 \dots a_n) = \gcd(\gcd(a_1 \dots a_{n-1}), a_n).$$

**Definition** (Relatively Prime).  $x$  and  $y$  are relatively prime to each other if and only if  $\gcd(x, y) = 1$ .

**Theorem** (Division with Relative Primes). (1) If  $\gcd(a, b) = 1$  and  $a|bc$ , then  $a|c$ . (2) If  $\gcd(a, b) = 1$  and  $a|c$  and  $b|c$ , then  $ab|c$ .

**Definition** (Prime).  $p$  is prime if and only if  $\{x : x \in \mathbb{N} \text{ and } x|p\} = \{1, p\}$ .

**Theorem** (Euclid's lemma). If  $p$  is prime and  $p|ab$  then  $p|a$  or  $p|b$ .

**Theorem** (General Euclid's lemma). If  $p$  is prime and  $p|\prod_{k=1}^n a_k$ , then  $p|a_k$  for some  $k$ .

**Theorem** (Prime Factorization Theorem, Fundamental Theorem of Arithmetic). Every finite positive integer  $a$  can be written a product of prime numbers

$$a = \prod_{i=1}^n p_i.$$

This product is unique, except for the order of the primes.

**Theorem.** There are infinitely many prime numbers.

## Chapter 1 vocabulary terms you should know and be able to use

- well-ordering principle
- quotient
- remainder
- divisible
- division algorithm
- greatest common divisor (gcd)
- least common multiple (lcm)
- linear combination
- Euclidean algorithm
- reduced fraction
- prime
- relatively prime
- well-ordered
- argument by induction
- argument by contradiction
- factorization
- prime factorization
- $a$  modulo  $b$ ,  $a \bmod b$
- congruent mod  $n$
- congruence class
- partition
- linear congruence relation
- multiplication table
- zero-divisor
- binary operation
- commutative
- associative
- identity
- inverse
- invertible
- idempotent
- order
- totient
- $a|b$
- $a\%b$
- $a/b$
- $ar + sn$
- $\gcd(x, y)$
- $\text{lcm}(x, y)$
- $\sum_{x=1}^n u_x$
- $\prod_{x=1}^n u_x$
- $x!$
- $\mathbb{N}$
- $\mathbb{Z}$
- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{Z}_n$
- $\mathbb{Z}_n^\times, G_n$
- $[x]_n$
- $x \equiv_n y, x \equiv y \pmod n$
- $\phi(x)$
- $\mathcal{O}([x]_n)$