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). *An integer* \(a\) *divides* \(b\), *denoted* \(a|b\), *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* \(b\), *denoted* \(\gcd(a, b)\), *is the maximum* \(d \in \mathbb{Z}\) *such that* \(d|a\) *and* \(d|b\).

**Theorem** (GCD bounds). *For every pair of positive integers* \((a, b)\), *the greatest common divisor* \(\gcd(a, b)\) *satisfies* \(1 \leq \gcd(a, b) \leq \min(a, b)\), *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). *An integer* \(c\) *divides* \(\gcd(a, b)\) *if and only if* \(c|a\) *and* \(c|b\).

**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* \(p|\prod_{k=1}^{n} a_i\), *then* \(p|a_k\) *for some* \(k\).

**Theorem** (Prime Factorization Theorem, Fundamental Theorem of Arithmetic). *Every finite positive integer* \(a\) *can be written as 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.*