Theorems and Corollaries of Chapter 1

Well-Ordering Axiom: Every nonempty subset of the set of nonnegative integers contains a smallest element.

Theorem 1.1 (The Division Algorithm): Let a and b be integers with $b > 0$. Then there exists unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Corollary 1.2: Let a and c be integers with $c \neq 0$. Then there exist unique integers q and r such that $a = cq + r$ and $0 \leq r < |c|$.

Theorem 1.3: Let a and b be integers, not both 0, and let $d = \gcd(a, b)$. Then there exist (not necessarily unique) integers u and v such that $d = au + bv$. Furthermore, d is the smallest positive integer that can be written in the form $au + bv$.

Corollary 1.4: Let a and b be integers, not both 0, and let d be a positive integer. Then $d = \gcd(a, b)$ if and only if d satisfies the following conditions:

i. $d|a$ and $d|b$;
ii. If $c|a$ and $c|b$, then $c|d$.

Theorem 1.5: Let a, b and c be integers. If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

Theorem 1.6 (The Euclidean Algorithm): Let a and b be positive integers with $a \geq b$. If $b|a$, then $\gcd(a, b) = b$. If $b \nmid a$, then apply the division algorithm repeatedly as follows:

$$\begin{aligned} a &= bq_0 + r_0 & 0 < r_0 < b \\ b &= r_0q_1 + r_1 & 0 \leq r_1 < r_0 \\ r_0 &= r_1q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 &= r_2q_3 + r_3 & 0 \leq r_3 < r_2 \\ &\cdots \end{aligned}$$

This process ends when a remainder of 0 is obtained. This must occur after a finite number of steps; that is for some integer t:

$$\begin{aligned} r_{t-2} &= r_{t-1}q_t + r_t & 0 < r_t < r_{t-1} \\ r_{t-1} &= r_tq_{t+1} + 0 \end{aligned}$$

Then r_t, the last nonzero remainder, is the greatest common divisor of a and b.

Theorems and Corollaries of Chapter 1

Lemma 1.7: Let $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

Theorem 1.8: Let b, c and p be integers with $p \neq 0, \pm 1$. Then p is prime if and only if p has the property that whenever $p|bc$, then $p|b$ or $p|c$.

Corollary 1.9: If p is prime and $p|a_1 a_2 \ldots a_n$, then p divides at least one of the a_i.

Theorem 1.10: Every integer n except $0, \pm 1$ is the product of primes.

Theorem 1.11 (The Fundamental Theorem of Arithmetic): Every integer n except $0, \pm 1$ is the product of primes. This prime factorization is unique in the following sense: if

$$n = p_1 p_2 \ldots p_r \quad and \quad n = q_1 q_2 \ldots q_s$$

with each p_i and q_j prime, then $r = s$ and after reordering and relabeling the q_j's,

$$p_1 = \pm q_1, \quad p_2 = \pm q_2, \quad \ldots \quad , p_r = \pm q_r$$

Corollary 1.12: Every integer $n > 1$ can be written uniquely in the form $n = p_1 p_2 \ldots p_r$, where the p_i are positive primes such that $p_1 \leq p_2 \leq \cdots \leq p_r$.