March 15, 2019

Well Ordering Axiom Every non-empty subset of the non-negative integers contains a smallest element.

Theorem 17: Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$ (*b* is a positive integer), then there exist unique integers q, r such that $a = bq + r$ and $0 \le r < b$

Definition: Let *a* and *b* be integers where not both are zero, then $d = \gcd(a,b)$ is the greatest common divisor of *a* and *b*, which means:

- $d \mid a$ and $d \mid b$
- If $c \mid a$ and $c \mid b$ then $c \le d$

Note, our textbook writes $(a,b) = \gcd(a,b)$

Theorem 18 (1.2): Let *a* and *b* be integers where not both are zero, and $d = \gcd(a,b)$. There exist $u, v \in \mathbb{Z}$ such that $d = au + bv$

Theorem 19 (1.3): Let *a* and *b* be integers where not both are zero, and $d = \gcd(a,b)$. Then if $c \mid a$ and $c \mid b$ then $c \mid d$

Theorem 20 (1.4): Let $a, b, c \in \mathbb{Z}$ such that $a \mid bc$ and $\gcd(a,b) = 1$ then $a \mid c$

Definition: Let *p* be an integer such that $p \ne 0, \pm 1$, then *p* is **prime** means:

Given $b, c \in \mathbb{Z}$, if $p \mid bc$ then $p \mid b$ or $p \mid c$

Definition: Let *p* be an integer such that $p \ne 0, \pm 1$, then *p* is **irreducible** means the only divisors of p are ± 1 and $\pm p$

Theorem 21: An integer *p* be an integer such that $p \ne 0, \pm 1$ is prime if and only of it is irreducible.

Theorem 22 (1.6): Let *p* be a prime integer and let $p \mid a_1 a_2 ... a_n$ then *p* divides at least one of the factors a_i.

Theorem 23 (1.7): Every integer *n* except $0, \pm 1$ is a product of primes.

Theorem 21 (Fundamental Theorem of Arithmetic, 1.8): If $n \in \mathbb{Z}$ and $n \ne 0, \pm 1$ then *n* is a product of primes, and the prime factorization is unique in the sense that if

$n = p_1 p_2 ... p_r$ and $n = q_1 q_2 ... q_s$

such that all of the p_i and q_j are prime,

then $r = s$ and the q_j factors can be re-ordered such that $p_i = \pm q_i$

(We can use a permutation to write $f : \{1, 2, ... s\} \to \{1, 2, ... s\}$ is a permutation, and $p_i = \pm q_{f(i)}$)