Chapter 11

Prime Numbers

Definition 11.1. The integers can be partitioned in to four types:

(1) zero: $a \mid 0$ for all $a \in \mathbb{Z}$;

(2) units $e = \pm 1$: $e \mid a$ for all $a \in \mathbb{Z}$;

(3) primes p: for any $a \in \mathbb{Z}$, if $a \mid p$ then $a = \pm p$ or ± 1.

(4) composites c: $\exists\, a, b \in \mathbb{Z}$ which are both neither zero or units such that $c = ab$.

Remark 11.2. Recall Corollary 10.12: if $a, b \in \mathbb{N}$ and $c \in \mathbb{Z}$ satisfy $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

Suppose that p is a prime, $b, c \in \mathbb{Z}$ and $p \mid bc$. Since $(p, b) \mid p$, $(p, b) = 1$ or p. If $(p, b) = p$, then $p \mid b$.

If $(p, b) = 1$, then (since $p \mid bc$) we have that $p \mid c$ by Corollary 10.12. Hence either $p \mid b$ or $p \mid c$ or both.

It follows by an inductive argument that if (a) p is a prime, (b) $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ and (c) $p \mid a_1 a_2 \ldots a_r$ then $p \mid a_i$ for at least one $i \in \{1, 2, \ldots, r\}$.

Theorem 11.3 (Unique Prime Factorization of Natural Numbers)**.** *Suppose that $n \in \mathbb{N}$ and $n > 1$. Then there exist primes $p_1, p_2, \ldots, p_r > 1$, which are unique up to order, such that*

$$n = p_1 p_2 \ldots p_r.$$

Proof If n is prime, then taking $r = 1$ and $p_1 = n$ gives the stated result.

Suppose now that n is composite. Take $b, c \in \mathbb{N}$ such that $1 < b, c < n$ and $n = bc$. If b and c are both primes, $n = bc$ is a (not necessarily unique) prime factorization of n. If either b or c is a composite, factorize it once again.

Proceeding inductively yields a finite process which results in a (not necessarily unique) prime factorization

$$n = p_1 p_2 \ldots p_r$$