,

Final Project

Molly Desque

Math 300

Spring 2020

Section 5.1: The Fundamental Theorem of Arithmetic

- **Definition 5.1** Let $n \in Z$.

  [(a)]If $a \in Z$ such that a divides n, then we say a is a **factor** of n. If $n \in N$ such that n has exactly two distinct positive factors (namely, 1 and n itself), then n is called **prime**. If $n > 1$ such that n is not prime, then n is called **composite**.

- **Exercise 5.2** Is 1 a prime number or composite number? Explain your answer.

- **Solution** The integer one is neither prime nor composite based off of definition 5.1, and if we define distinct as recognizably different in nature. Definition 5.1 states that a number must have exactly two distinct positive factors. Since one can not be distinct from itself, it is not prime. In addition, for a number n to be composite $n > 1$, therefore one can not be composite.

- **Exercise 5.3** List the first 10 prime numbers.

- **Solution** The first ten prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$

- **Lemma 5.4** Let n be a natural number greater than 1. Then n can be expressed as a product of primes. That is, we can write

$$n = p_1 p_2 \cdots p_k$$

  where each of $p_1, p_2, \ldots, p_k$ is a prime number (not necessarily distinct).

- **Proof** Let $n \in N$, such that $n > 1$ and n can be expressed uniquely as the product of one or more primes. For the sake of contradiction, assume n can not be written as a product of primes. Let S be the set of all integers that can not be written as a prime number. Let a be the smallest prime integer in S. Notice that if the only factors of a are 1 and a, then a is prime, which is a contradiction. Therefore, $a = a_1 a_2$, where $1_a < a$ and $a_2 < a$. Since a is the smallest element in S, neither a_1,$a_2 \in S$. Therefore $a_1 = p_1 p_2 ... p_r$ and $a_2 = q_1 q_2 ... q_j$. Therefore $a = a_1 a_2 = p_1 p_2 ... p_r q_1 q_2 q_j$. So $a \notin S$, which is a contradiction. Thus n can be expressed as the product of one or more primes.

- **Theorem 5.5** (Division Algorithm) If $m, n \in N$, then there exists unique $q, r \in N \cup \{0\}$ such that $m = nq + r$ with $0 \leq r < n$.

  (Note: You do not have to prove this theorem.)

  The numbers q and r from the Division Algorithm are referred to as **quotient** and **remainder**, respectively.

- **Exercise 5.6** Suppose $m = 27$ and $n = 5$. Find the quotient and the remainder that are guaranteed to exist by the Division Algorithm. That is, find the unique $q, r \in N$ such that $0 \leq r < n$ and $m = nq + r$.

- **Solution** In order for $27 = 5q + r$ to be true, $q = 5$ and $r = 2$. Therefore, $27 = 5(5) + 2$. Which is equal to $27 = 27$.

- **Definition 5.7** Let $m, n \in Z$ such that at least one of m or n is nonzero. The **greatest common divisor** (gcd) of m and n, denoted $\gcd(m, n)$, is the largest positive integer that is a factor of both m and n. If $\gcd(m, n) = 1$, we say that m and n are **relatively prime**.

- **Exercise 5.8** Find $\gcd(54, 72)$.

- **Solution** The greatest common divider of $(54, 72)$ is 18. Notice $18(3) = 54$ and $18(4) = 72$.

- **Exercise 5.9** Provide an example of two natural numbers that are relatively prime.

- **Solution** Two natural numbers, 7 and 12, are relatively prime.

- **Lemma 5.10** (Special Case of Bezout's Lemma). If $p, a \in Z$ such that p is prime and p and a are relatively prime, then there exists $s, t \in Z$ such that $ps + at = 1$.

- **Proof** Let $p, a \in Z$, such that p, a are relatively prime. Let $S = [\ ps + at\ | s, t \in Z$ and $ps + at > 0\ ]$. Notice, S is a subset of natural numbers. Let d be the smallest element in S. Hence $d = 1$. Since $d \in S$ there exist an $s, t \in Z$ such that $ps + at = d$. Since $d, p \in N$ by theorem 5.5, $p = dq + r$, such that $q, r \in N \cup \{0\}$. Notice $r < d$, since $d = 1$, $r = 0$. Therefore, $p = dq$. Notice p is prime, therefore $d = 1$ and $q = p$. Thus, $ps + at = 1$.

- **Exercise 5.11** Consider the natural numbers 2 and 7, which happen to be relatively prime. Find integers s and t guaranteed to exist according to Lemma 5.10. That is, find $s, t \in Z$ such that $2s + 7t = 1$.

- **Solution** In order for $2s + 7t = 1$, $s = 4$ and $t = -1$. Therefore $2(4) + 7(-1) = 8 - 7$, thus $1 = 1$.

- **Theorem 5.12** (Euclid's Lemma). Assume that p is prime. If p divides ab, where $a, b \in N$, then either p divides a or p divides b.

- **Proof** Let $a, b, p \in Z$, such that p is prime. Let $p|ab$, and let p not divide a. Therefore, the gcd(a,p) = 1. Since a,p are relatively prime, by theorem 5.10 $ps + at = 1$ for some $s, t \in Z$. Notice that by the multiplicative identity property $b = b(1)$. By substitution, $b = b(ps + at)$. By the distributive property, $b(ps + at) = p(sb) + t(ab)$. Therefore, $p|p(sb)$ and $p|t(ab)$. Hence $p|b$. In addition, if we let p not divide b. Therefore, the gcd(b,p) = 1. Since b,p are relatively prime, by theorem 5.10 $ps + bt = 1$ for some $s, t \in Z$. Notice that by the multiplicative identity property $a = a(1)$. By substitution, $a = a(ps + bt)$. By the distributive property, $a(ps + bt) = p(sa) + t(ab)$. Therefore, $p|p(sa)$ and $p|t(ab)$. Hence $p|a$.

- **Problem 5.13** Provide an example of integers a, b, d such that d divides ab yet d does not divide a and d does not divide b.

- **Solution** Let $a = 3, b = 10$ and $d = 6$. Notice, $3(10) = 30$ and $6(5) = 30$, thus $6|30$. However, $6 \not| 3$ and $6 \not| 10$.

- **Theorem 5.14** (Fundamental Theorem of Arithmetic) Every natural number greater than 1 can be expressed uniquely (up to the order in which they appear) as the product of one or more primes.

- **Proof** Let $n \in N$, such that $n > 1$and n can be expressed uniquely as the product of one or more primes. Due to Theorem 5.4, any natural number can be expressed as the product of one or more primes. Therefore to prove uniqueness, we proceed by induction. Let P(n) = the statement "n can be expressed uniquely as the product of one or more primes."

- **Base case** Let $n = 2$, thus $P(n) = 2^1$, and $2 = 2$. Therefore, P(2) is true.

- **Inductive Step** Assume n is true, and let all integers m, such that $m \leq 1 < n$. Also, let $n = p_1p_2...p_k = q_1q_2...q_l$, where $p_1 \leq 2... \leq_p k$ and $q_1 \leq_2 ... \leq_l$. By theorem 5.12, notice $p_1|q_i$ and $q_1 = p_j$. Hence, $p_1 = q_1$, since $p_1 \leq_q j = q_1 \leq_q i = p_1$. Thus by the PMI $n = p_2...p_k = q_2...ql$ has a unique factorization. Therefore,$k = l$ and $q_i = p_i$ for $i = 1, ...k$.