MATH 300- Final Project
Brooke Dippold

Section 5.1: The Fundamental Theorem of Arithmetic

- **Definition 5.1** Let $n \in \mathbb{Z}$.
  (a) If $a \in \mathbb{Z}$ such that a divides n, then we say a is a **factor** of n.
  (b) If $n \in \mathbb{N}$ such that n has exactly two distinct positive factors (namely, 1 and n itself), then n is called **prime**.
  (c) 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.

  One is neither prime nor composite. One cannot be prime because it does not have two distinct positive factors. Its only factor is itself. One is not composite because the definition of composite excludes one.

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

  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 $n \in \mathbb{N}$ such that $n \geq 2$. Let $P(n) :=$ "n can be expressed as the product of primes." We proceed by induction.
  Base Case: Notice that n=2 is prime. Therefore, $P(2)$ is true.
  Inductive Step: Let $k \in \mathbb{N}$ and assume $P(j)$ is true for all $j \leq k$. Notice if $k+1$ is prime, then $P(k+1)$ is true. If $k+1$ is not prime, then $k+1$ can be factored. Thus $k+1 = a * b$ where $a, b \in \mathbb{N}$. Because $k+1$ is not prime, $1 < a, b < k+1$. By the inductive hypothesis, a, b can be written as the product of primes. Thus $P(a)$ and $P(b)$ are true. Since $k+1$ can be written as the product of two products of primes, $P(k+1)$ is true. Therefore, by the PCMI $P(n)$ is true for all $n \in \mathbb{N}$. $\square$

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

  q=5 and r=2

- **Definition 5.7** Let $m, n \in \mathbb{Z}$ 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 $\gcd(54, 72)$.

  gcd(54, 72)=18

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

  28 and 81 are relatively prime.

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

  Proof. Let $S = [ps + at | s, t \in \mathbb{Z}$ and $ps + at > 0]$ where p is prime and p, a are relatively prime. S is the set of all possible outputs of $ps + at$. Since $ps + at > 0$, S is a subset of the natural numbers. Thus S is well ordered. So, there is a smallest element in S.
  Let d be the smallest element in S. Since d is in S, there exists $s, t \in \mathbb{Z}$ such that $ps + at = d$. Since $d, p \in \mathbb{N}$ by the division algorithm $p = qd + r$ where $0 \leq r < d$. If $r > 0$, $r \in \mathbb{N}$. Notice $p = qd + r$ can be rewritten as $r = p - qd$. By substitution, $r = p - qd = p - (ps + at)q = p - psq - qat = p(1 - sq) + a(-tq)$. Since $q, s, t \in \mathbb{Z}$, $(1 - sq), (-tq) \in \mathbb{Z}$ and $r \in S$. This is a contradiction because r must be smaller than d but d is the smallest element in S. Therefore r must be 0. So, $p = qd$, then $d | p$. Since p is prime, $d = 1$ or $d = p$.
  Since $d \in S$, there exists $s, t \in \mathbb{Z}$ such that $ps + at = d$. Since $d, a \in \mathbb{N}$ by the division algorithm, $a = dq + r$ where $0 \leq r < d$. If $r > 0, r \in \mathbb{N}$. Notice that $a = dq + r$ can be rewritten as $r = a - dq$. By substitution, $r = a - dq = a - (ps + at)q = a - qps - qat = a(1 - qt) + s(-qp)$. Since $q, t, p \in \mathbb{Z}$, $(1 - qt), (-qp) \in \mathbb{Z}$, $r \in \mathbb{Z}$. Then $r \in \mathbb{S}$. This is a contradiction because r must be smaller than d but d is the smallest element in S. Thus, $r = 0$. So, $a = dq$, then $d | a$. Since p, a are relatively prime, gcd(p,a)=1. Then, $d = 1$.
  Therefore, $1 \in S$. Thus, there exists s, t such that $ps + at = 1$.

  $\square$

- **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 $s, t \in \mathbb{Z}$ such that $2s + 7t = 1$.

$s = 4$ and $t = -1$

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

  Proof. Let p be a prime number where $p|ab$ $p, a, b \in \mathbb{N}$. Suppose p does not divide a. Thus p, a are relatively prime and gcd(a, p)=1. By Lemma 5.10, there exists $s, t \in \mathbb{Z}$ such that $ps+at = 1$. Notice, $b = b*1$. By substitution, $b = b(ps + at) = bps + bat = pbs + abt = p(bs) + (ab)t$. Since p divides ab and itself, $p|p(bs)$ and $p|(ab)t$. Algebraically, since p divides each part on the right hand side of the equation, p must divide the left hand side of the equation. Thus, $p|b$. □

- **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.

  $a = 4$ $b = 9$ and $d = 6$

- **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 $n \in \mathbb{N}$ such that $n \geq 2$. Let $P(n) :=$ "n can be expressed uniquely as the product of one or more primes." We proceed by induction.
  Base Case: Notice when $n = 2$, n is prime. Thus $P(2)$ is true.
  Inductive Step: Let $k \in \mathbb{N}$ such that $k \geq 2$ and assume $P(j)$ is true for all $j \leq k$. Notice if $k + 1$ is prime, the $P(k + 1)$ is true. By Lemma 5.4, if $k + 1$ is not prime, then it can be written as the product of primes. For the sake of contradiction, assume there exists two different products of primes that equal $k + 1$.
  That is, $k+1 = p_1p_2...p_r$ and $k+1 = m_1m_2...m_n$ where each individual element p_i and m_g, $1 \leq i \leq r$ and $1 \leq g \leq n$ is prime. Notice that $k + 1 = p_1p_2...p_r = m_1m_2...m_n$ can be rewritten as $k + 1 = p_1p_2...p_r = m_1(m_2...m_n)$. By Theorem 5.12, $m_1|p_1p_2...p_r$. Thus, $m_1|p_i$ for some p_i. Similarly, notice $k + 1 = m_1m_2...m_n = p_1(p_2...p_r)$. By Theorem 5.12, $p_1|m_1m_2...m_n$. Thus, $p_1|m_g$ for some m_g. Since p_1 and m_1 are prime, their only factors are 1 and p_1 or m_1 respectively. Since 1 is not prime, we can conclude that $p_1 = m_1$. Thus, $k + 1$ can be written as $k + 1 = p_1p_2...p_k = p_1(m_2...m_n)$.
  Notice that $m_2...m_n$ is an element of the set of natural numbers that is smaller than $k + 1$. Thus by the inductive hypothesis, $m_2...m_n$ can be expressed uniquely as a product of primes. Thus, $m_2...m_n = p_2...p_r$. Therefore, $p_1p_2...p_r = m_1m_2...m_n$. This is a contradiction. So, $k + 1$ can be expressed uniquely as a product of one or more primes. Therefore, by the PCMI, n can be expressed uniquely as the product of one or more primes is true for all $n \geq 2$. □