MATH 300 - Final Project - Jessica Donahue

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.

  The number one is neither prime nor composite. It does not have more than one factor. Therefore, it is not composite. Furthermore, its only factor is itself. Thus, it cannot be prime as in order to be prime the number must have two factors: one AND itself. One is a special case scenario that is neither prime nor composite.

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

  The first ten prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, and 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 $n > 1$ and let $p(n) :=$ "n can be expressed as a product of primes." We proceed by induction.
  Base step: Let $n = 2$. Then $p(2)$ is true as 2 is a prime number.
  Inductive step: Let $k \in \mathbb{N}$. Suppose $p(j)$ is true for all $j \leq k$.
  Consider $k + 1$. If $k + 1$ is prime then $p(k + 1)$ is true. However, if $k + 1$ is not prime, then $k + 1 = a * b$ where a and b are not 1 or $k + 1$.Therefore, $1 < a, b < k + 1$. Hence, By the inductive hypothesis, $p(a)$ and $p(b)$ are true . Thus, $a = p_1 * p_2 * ... * P_k$ where all p_i are prime and $b = q_1 * q_2 * ... * q_l$ where all q_y are prime. Thus, by substitution $k+1 = a*b = (p_1*p_2*...*P_k)(q_1*q_2*...*q_l) = p_1*p_2*...*P_k*q_1*q_2*...*q_l$. Since all p_i and all q_y are prime, $p(k + 1)$ is true.

  Hence, by the PCMI, $p(n)$ is true for all natural number $n > 1$.

  □

- **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 $m = nq + r$.

  If $m = 27$ and $n = 5$, then the division algorith equals $27 = 5q + r$ for some unique $q, r \in \mathbb{N}$ such that $0 \leq r < 5$. Notice that $27 = 5(5) + 2$. Since $0 \leq 2 < 5$, the unique $q, r \in \mathbb{N}$ that satisfy $m = 27$ and $n = 5$ are $q = 5$ 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 $\gcd(54, 72)$.

  The factors of 54 and 72 are:
  54:1,2,3,6,9,18,27,54
  72:1,2,3,4,6,8,9,12,18,24,36,72.
  Thus, the $\gcd(54, 72)$ is 18.

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

  An example of two natural numbers that are relatively prime are 4 and 15 as the factors of 4 are 1, 2, and 4 and the factors of 15 are 1, 3, 5, and 15. Thus, the only factors they have in common are 1 making the $\gcd(4, 15) = 1$ which, by definition, makes them 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 $S = \{ps + at \mid s, t \in \mathbb{Z} and ps + at > 0\}$. Notice that S is a subset of the natural numbers. Therefore, S is well-ordered and there exists a smallest element in S.
  For the sake of contradiction let d be the smallest element in S. Since $d \in \mathbb{S}$, $\exists s, t \in \mathbb{Z}$ such that $ps + at = d$. Since $d, p \in \mathbb{N}$, by the division

algorithm $p = dq_1 + r_1$ where $0 \leq r_1 < d$. If $r_1 > 0$, then $r_1 \in \mathbb{N}$ and by substitution $r_1 = p - dq_1 = p - (ps + at)q_1 = p - psq_1 - atq_1 = p(1 - sq_1) + a(-tq_1)$. Since $(1 - sq_1), (-tq_1) \in \mathbb{Z}$, $r_1 \in \mathbb{S}$. Thus, $r_1 < d$ but d is the smallest element in S. This is a contradiction. Therefore $r_1 = 0$. Therfore, $p = dq_1$. Hence $d \mid p$. Thus, d is 1 or p since p is prime. Similarly notice that $d, a \in \mathbb{N}$. Thus by the division algorithm $a = dq_2 + r_2$ where $0 \leq r_2 < d$. If $r_2 > 0$, then $r_2 \in \mathbb{N}$ and by substituion $r_2 = a - dq_2 = a - (ps + at)q_2 = a - psq_2 - atq_2 = a(1 - tq_2) + p(-sq_2)$. Since $(1 - tq_2), (-sq_2) \in \mathbb{Z}$, $r_2 \in \mathbb{S}$. Thus, $r_2 < d$ but d is the smallest element in S. This is a contradiction. Therefore $r_2 = 0$. Thus, $a = dq_2$. Hence, $d \mid a$. Therefore, d is 1 or a since a is prime. However, d cannot be p and a. Therefore, d is 1. Since $d \in \mathbb{S}$, $\exists s, t \in \mathbb{Z}$ such that $ps + at = 1$. □

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

Let $s, t \in \mathbb{Z}$ such that $s = -10$ and $t = 3$. Then $2s + 7t = 2(-10) + 7(3) = (-20) + 21 = 21 - 20 = 1$. Therefore, $2s + 7t = 1$ when $s = -10$ and $t = 3$.

- **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 and let $a, b \in \mathbb{N}$ such that $p \mid ab$. Then $ab = pk$ for some $k \in \mathbb{Z}$. If $p \mid a$ then the statement above is true. However, if $p \nmid a$ then $\gcd(a, p) = 1$ as, by the definition of prime, p only has factors one and itself. Therefore, if $p \nmid a$ the only factor they can have in common is 1. Hence, a and p are relatively prime. By Bezout's Lemma, $\exists s, t \in \mathbb{Z}$ such that $ps + at = 1$. By the properties of equatily, $b(ps + at) = b(1)$. By the distributive property, $bps + bat = b$. By substitution, $bps + (ba)t = bps + (pk)t = b$. Thus, $p(bs + kt) = b$. By the definition of divides, $p \mid b$. Therefore, if p divides ab, where $a, b \in \mathbb{N}$, then either p divides a or p divides 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.

Let $a = 3, b = 4$, and $d = 6$. Then $ab = 3(4) = 12$. Notice that 6 divides 12, but 6 does not divide 3 nor does 6 divide 4.

- **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 $n > 1$ and let $p(n) :=$ "n can be uniquely written as a product of prime numbers." We proceed by induction. Base step: Let $n = 2$, then $p(2)$ is true as 2 is a prime number.
Inductive step: Let $k \in \mathbb{N}$. Suppose $p(j)$ is true for all $j \leq k$. Consider $k+1$. Notice that when $k+1$ is prime, $p(k+1)$ is true. However, $k+1$ can be composite. For the sake of contradiction assume $k+1 = p_1 * p_2 * ... * p_k$ and $k + 1 = q_1 * q_2 * ... * q_j$ where each $p_i.q_l$ is prime. Then, by substitution, $p_1 * p_2 * ... * p_k = q_1 * q_2 * ... * q_j$. By the associative property, $p_1(p_2 * ... * p_k) = q_1(q_2 * ... * q_j)$. Therefore, by Theorem 5.12, $q_1 \mid (p_1 * p_2 * ... * p_k)$ thus $q_1 \mid p_i$ for some p_i. Similarly, $p_1 \mid (q_1 * q_2 * ... * q_j)$ thus $p_1 \mid q_j$ for some q_j. Since every p_i and q_j is prime, $p_1 = q_1$. Thus $k + 1 = p_1(p_2 * p_3 * ... * p_k)$ and $k + 1 = p_1(q_2 * q_3 * ... * q_j)$ such that $(p_2 * p_3 * ... * p_k), (q_2 * q_3 * ... * q_j) \in \mathbb{N}$ and $(p_2 * p_3 * ... * p_k), (q_2 * q_3 * ... * q_j) < K + 1$. Thus, by the inductive hypothesis, $p(p_2 * p_3 * ... * p_k)$ is true and $p(q_2 * q_3 * ... * q_j)$ is true. Hence, $p_2 = q_2, p_3 = q_3, ..., p_k = q_j$. This is a contradiction as $k + 1 = p_1 * p_2 * ... * p_k$ and $k + 1 = q_1 * q_2 * ... * q_j$ are not uniquely written. Thus, $p(k + 1)$ is true.

Hence, by the PCMI, $p(n)$ if true for all natural numbers $n > 1$

□