MATH 300- Final Project

One of the most important skills I want you to learn from this class is the ability to build new mathematics from previously proven results and new definitions. The goal of this project is for you to show me that you are able to produce mathematics that is new to you by using the skills and techniques we have covered this semester.

You will read Section 5.1 and fill in the solutions and proofs for each Exercise, Problem, Lemma, and Theorem (unless otherwise stated). You may bounce ideas off of each other, but you may not share your final solutions or proofs with anyone else from class. You also should not copy proofs or solutions from the internet. If you are taking this course for Honors credit, your solutions and proofs should be written in LaTex. If you are not taking this course for Honors credit, you may submit handwritten solutions.

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 1 is neither a prime nor a composite number, because for a number to be prime it must have exactly two positive factors, including 1 and the number itself. The number 1 only has 1 as a positive factor and therefore cannot be prime. The number 1 is not composite, because to be composite a number must have at least one positive factor other than 1 and the number itself. The number 1 only has 1 as a positive factor and therefore cannot be composite.

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

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

- **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 the set $S = \{n \neq p_1 p_2 \ldots p_k : n \in \mathbb{N} \text{ such that } n > 1 \text{ and each } p_i \text{ is prime for some } i = 1, \ldots k\}$ represent all the natural

numbers greater than 1 that cannot be expressed as a product of prime numbers. For the sake of contradiction, assume $S \neq \emptyset$. Notice that $S \subset N$. Thus, by the Well-Ordering Principal, S contains a smallest element. Let $j \in S$ such that j is the smallest element of S. j cannot be prime since $j \in S$. Thus, j is composite, and has a divisor other than 1 and j itself. This implies there are natural numbers a and b greater than 1 such that $n = ab$. Since j is the smallest element of S, both a and b must be prime. This contradicts the assumption that j is the smallest element in S. Thus, $\forall n \in \mathbb{N}$ such that $n > 1$ can be expressed as a product of prime numbers. □

- **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 $m = nq + r$.

  The unique $q, r \in \mathbb{N}$ are $q = 5$ and $r = 2$. Because $27 = 5(5) + (2) = 25 + 2 = 27$ and $0 \leq 2 < 5$.

- **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 $\gcd(54, 72) = 18$.

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

  A pair of relatively prime natural numbers are 7 and 12, because $\gcd(7, 12) = 1$.

- **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 $p, a \in \mathbb{N}$ such that p is prime and the $gcd(a, p) = 1$. Let the set $S = \{ps + at : s, t \in \mathbb{Z} \text{ and } ps + at > 0\}$ represent all possible positive outputs that can result from the expression $ps + at$. Notice that $S \subset N$. Therefore, By the Well-Ordering principal, there is a least

element in S. Let d be the least element in S. Since $d \in S$, $\exists s, t \in \mathbb{Z}$ such that $ps + at = d$. Since $a, p \in \mathbb{N}$, by the division algorithm, $p = dq + r$ such that $q, r \in \mathbb{N} \cup 0$ and $0 \leq r < d$. If $r > 0$, then $r \in \mathbb{N}$ and by substitution, $r = p - dq = p - (ps + at)q = p - psq - atq = p(1 - sq) + a(-tq)$. Since $(-tq), (1 - sq) \in \mathbb{Z}$, $r \in S$. Since $r < d$, this contradicts the assumption that d is the smallest element in S, thus r=0. So, $p = dq$, which means $d|p$. Hence, since p is prime, either $d = 1$ or $d = p$. By the division algorithm, $a = dj + b$ such that $j, b \in \mathbb{N} \cup 0$ and $0 \leq b < d$. If $b > 0$, then $b \in \mathbb{N}$ and by substitution, $b = a - dj = a - (ps + at)j = a - psj - atj = p(-sj) + a(1 - tj)$. Since $(1 - tj), (-sj) \in \mathbb{Z}$, $b \in S$. Since $b < d$, this contradicts the assumption that d is the least element in S, thus b=0. So, $a = dj$, which means $d|a$. Since $\gcd(a, p) = 1$, $d = 1$. So $1 \in S$. Hence, $\exists s, t$ 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 $2s + 7t = 1$.

  The integers are $s = -3$ and $t = 1$. Therefore, $2(-3) + 7(1) = -6 + 7 = 1$.

- **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 $a, b, p \in \mathbb{N}$ such that p is prime and $p|ab$. Then $ab = pk$ for some $k \in \mathbb{Z}$. Assume that $p \nmid a$. So p and a are relatively prime. Thus, by Lemma 5.10, $ps + at = 1$ for some $s, t \in \mathbb{Z}$. Notice $b(ps + at) = b$, so $bps + bat = b$. By substitution, $bps + pkt = p(bs + kt) = b$. Since $b, s, k, t \in \mathbb{Z}$, $p|b$. Assume that $p \nmid b$. So p and b are relatively prime. Thus, by Lemma 5.10, $pj + bf = 1$ for some $j, f \in \mathbb{Z}$. Notice $a(pj + bf) = a$, so $apj + abf = a$. By substitution, $apj + pkf = p(aj + kf) = a$. Since $a, j, k, f \in \mathbb{Z}$, $p|a$. Therefore, either $p|a$ or $p|b$. □

- **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.

  The integers are $a = 4$, $b = 3$, and $d = 6$. Because $(4)(3) = 12$ and $6|12$, but $6 \nmid 4$ and $6 \nmid 3$.

- **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 $n > 1$. By Lemma 5.4, n can be expressed as a product of prime numbers. Thus, let $F(n) :=$ "$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$ such that each factor is a prime number". We proceed by induction. Base Step: Let $n = 2$. Because 2 itself is prime, $F(2)$ is

true. Inductive Step: Assume that $F(m)$ is true $\forall m \in \mathbb{N}$ such that $1 \leq m < n$. Also, assume that $p_1 \leq p_2 \leq \ldots \leq p_k$ and $q_1 \leq q_2 \leq \ldots \leq q_l$. By Euclid's Lemma, $p_1 | q_i$ for some $i \in \mathbb{N}$ such that $i \leq l$ and $q_1 | p_j$ for some $j \in \mathbb{N}$ such that $j \leq k$. Because the factors are all prime, $p_1 = q_i$ and $q_1 = p_j$. Therefore, because $p_1 \leq p_j = q_1 \leq q_i = p_1$, $p_1 = q_1$. By the induction hypothesis, $p_2 \ldots p_k = q_2 \ldots q_l$, so n has a unique factorization. Thus, $k = l$ and $p_i = q_i$ for some $i \in \mathbb{N}$ such that $i \leq k$. Hence, by the PCMI, there is a unique prime factorization $\forall n \in \mathbb{N}$ such that $n > 1$. $\square$