MATH 300- Final Project
Lindsey Gordon

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.

  1 is neither prime nor composite. 1 is not prime since it does not have two distinct factors. The only factors that give you 1 are 1 and 1, thus it is not prime. 1 is not composite simply by definition: "if $n > 1$..." Since 1 is not greater than 1, it is not composite.

- **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).

  For natural numbers $n > 1$, $n = p_1 p_2 \cdots p_k$

Proof. : Let $n \in \mathbb{N}$ such that $n > 1$.
Let $P(n) :=$ "$p_1 p_2 \cdots p_k$ where each of $p_1, p_2, \cdots p_k$ is a prime number" for some $k \in \mathbb{N}$.
We proceed by complete induction.
Base Step: Let $n = 2$.
Since 2 is prime, $P(2)$ is true.
Inductive Step: Let $x \in \mathbb{N}$ and assume $P(x)$ is true.
If $x + 1$ is prime, then $p(x + 1)$ is true.
If $x+1$ is not prime, then $x+1 = ab$ where $a, b \in N$ and $1 < a, b < x+1$.
By inductive hypothesis, $P(a)$ and $P(b)$ are true.
Thus, $P(a) = p_1 p_2 \cdots p_k$ and $P(b) = q_1 q_2 \cdots q_k$.
Notice $x + 1 =$(p$_1 p_2 \cdots p_k)(q_1 q_2 \cdots q_k)$ where all p_i and q_i are prime.
Hence, $x + 1$ is a product of primes.
Thus, $P(x + 1)$ is true.
Therefore, by the PCMI, $P(n)$ is true for all natural numbers $n > 1$.//

□

- **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 $m = nq + r$.

$m = nq + r$
$27 = 5q + r$
$27 = 5(5) + 2$
q=5
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 $\gcd(54, 72)$.

$gcd(54, 72) = 18$
$54/18 = 3$

$72/18 = 4$
Thus, there are no larger gcd.

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

  gcd(5, 13)
  since 5 and 13 cannot be divided by a common divisor, they 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 $S = ps + at$ where $s, t \in \mathbb{Z}$ and $ps + at > 0$
  The set S is nonempty since when $s = 1$ and $t = 0$ $p(1) + a(0) = p > 0$ and p is prime.
  Notice S contains the set of natural numbers and has a smallest element.
  We let this smallest element be x.
  Notice $x \in S$, so there exists s, t where $ps + at = x$.
  By the division algorithm, $p = xq + r$ where $x, p \in \mathbb{N}$ and $q, r \in \mathbb{N}$ or 0 where $0 \leq r \leq x$.
  Notice $r \neq 0$ and $r = p - xq$.
  By substitution, $r = p - (ps + at)q$
  $r = p - psq - atq$
  $r = p(1 - sq) + a(-tq)$
  Since $1 - sq$ and $-tq$ are integers, $r \in S$.
  Recall $r < x$ and x is the smallest element in S, which cannot be true.
  Thus, $r = 0$.
  Hence $0 = p - xq$, so $p = xq$.
  Thus, $x|p$.
  Since p is prime, $x = 1$ or $x = p$.
  By the division algorithm, $a = xq_1 + r_1$ where $x, a \in \mathbb{N}$ and $q_1, r_1 \in \mathbb{N}$ or 0 where $0 \leq r_1 \leq x$.
  Notice $r_1 \neq 0$ and $r_1 = a - xq_1$.
  By substitution, $r_1 = a - (ps + at)q_1$
  $r_1 = a - psq_1 - atq_1$
  $r_1 = a(1 - tq_1) + p(-sq_1)$
  $r_1 = p(-sq_1) + a(1 - tq_1)$
  Since $1 - tq_1$ and $-sq_1$ are integers, $r \in S$.
  Recall $r_1 < x$ and x is the smallest element in S, which cannot be true.
  Thus, $r_1 = 0$.
  Hence $0 = a - xq_1$, so $a = xq_1$.
  Thus, $x|a$.

Since a is prime, $x = 1$ or $x = a$.
Notice $x = 1$, $x = p$, or $x = a$.
Since a, p are relatively prime, the only common divisor, x, is 1.
Therefore, there 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 $2s + 7t = 1$.

  $2s + 7t = 1$
  $2(-3) + 7(1) = 1$
  $-6 + 7 = 1$
  s=-3
  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 prime and $a, b \in \mathbb{N}$ where $p|ab$.
  Notice $ab = pk$ for some $k \in \mathbb{Z}$.
  Case 1: If $p|a$, then the statement is true.
  Case 2: If $p \nmid a$, by Theorem 5.10, gcd(a, p)=1 and there exists some $s, t \in \mathbb{Z}$ such that $ps + at = 1$.
  If we multiply both sides of the equation by b then
  $bps + bat = b$.
  By substitution, $bps + pkt = b$.
  Thus, $p(bs + kt) = b$.
  Since $bs + kt \in \mathbb{Z}, p|b$.
  Therefore, if p is prime and $p|ab$, then $p|a$ 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.

  let d divide ab
  notice 6 divides (4)(3)
  thus 6 divides 12
  let d not divide a
  notice 6 does not divide 4
  let d not divide b
  notice 6 does not divide 3
  therefore, a=4 and b=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 $n > 1$.
  Let $P(n) :=$ "Every natural number greater than 1 can be expressed uniquely as the product of primes"
  We proceed by complete induction.
  Base Step: Let $n = 2$.
  Since 2 is prime, $P(2)$ is true.
  Inductive Step: Let $x \in \mathbb{Z}$ and assume $P(x)$ is true.
  If $x + 1$ is prime then $p(x + 1)$ is true.
  Assume $x+1$ is not prime and $x+1 = p_1p_2 \cdots p_k$ and $x+1 = q_1q_2 \cdots q_j$ where $k, j \in \mathbb{Z}$.
  Notice $p_1p_2 \cdots p_k = q_1q_2 \cdots q_j$.
  Since $p_1p_2 \cdots p_k = q_1(q_2 \cdots q_j), q_1|p_1p_2 \cdots p_k$.
  By Theorem 5.12, $q_1|p_i$ for some $1 \leq i \leq k$.
  Thus, $p_1(p_2 \cdots p_k) = q_1q_2 \cdots q_j$, so $p_1|q_1q_2 \cdots q_j$.
  By Theorem 5.12, $p_1|q_i$ for some $1 \leq l \leq j$.
  Hence, $p_1 = q_1$.
  Thus, $k + 1 = p_1(p_2 \cdots p_k)$ and $k + 1 = p_1(q_2 \cdots q_j)$ where $p_2 \cdots p_k$ and $q_2 \cdots q_j \in \mathbb{N}$ and $< k + 1$.
  By the inductive hypothesis, $p_2 = q_2$ and $\cdots p_k = \cdots q_j$.
  Hence, $p_1p_2 \cdots p_k$ and $q_1q_2 \cdots q_j$ are equal, which proves $k + 1$ has its own unique element.
  Therefore, every natural number greater than 1 can be expressed uniquely as the product of primes.//

  □