Math 476 - Abstract Algebra 1
Day 4 Group Assignment **Name:**_____

The Euclidean Algorithm, Linear Combinations, and Prime Numbers

Example: Let $a = 11000$ and $b = 4950$. Our goal is to find $\gcd(a, b)$.

Using the Division Algorithm on a and b, we find that $11000 = 4950(2) + 1100$ [so $q = 2$ and $r = 1100$].

Recall: Theorem 3.4: Let a and b be integers, not both zero, and suppose that $b = aq + r$ for some integers q and r. Then $\gcd(b, a) = \gcd(a, r)$.

Applying this Theorem, we have that $\gcd(11000, 4950) = \gcd(4950, 1100)$.

Using the Division Algorithm again, we find that $4950 = 1100(4)+550$, so $\gcd(11000, 4950) = \gcd(4950, 1100) = \gcd(1100, 550)$.

Continuing this, we see that $1100 = 550(2) + 0$, so $\gcd(1100, 550) = \gcd(550, 0) = 550$. Hence $\gcd(11000, 4950) = 550$.

This method of using the Division Algorithm and Theorem 3.4 iteratively to find the gcd of a pair of integers is called **Euclid's Algorithm**.

1. Use Euclid's Algorithm to find the gcd for the following pairs of integers:

   (a) $a = 525$ and $b = 252$ (b) $a = 54321$ and $b = 12345$ (c) $a = 27182$ and $b = -3141$

Definition 3.8: Let a and b be integers. A **linear combination** of a and b is an integer that can be written as $ax + by$ for some integers x and y.

Notice that in our example of using Euclid's Algorithm above, we found that $4950 = 1100(4) + 550$. Rearranging this, we can write $550 = 4950(1) + 1100(-4)$. This shows that 550 can be written as a linear combination of $a = 4950$ and $b = 1100$ with $x = 1$ and $y = -4$.

Theorem 3.9 (Bezout's Identity) Let a and b be integers, not both zero. Then $\gcd(a, b)$ can be written as a linear combination of a and b. That is, there exist integers x and y such that $\gcd(a, b) = ax + by$.

Note: We will not prove this theorem formally, but to help convince us it is true and to demonstrate the core ideas from the proof, we return to the computations we used in our example of the Euclidean Algorithm above.

We know that $11000 = 4950(2) + 1100$, so $1100 = 4950(-2) + 11000(1)$. Also, we know that $550 = 4950(1) + 1100(-4)$.

Combining these, we have: $550 = 4950(1) + [4950(-2) + 11000(1)](-4) = 4950(1) + 4950(8) + 11000(-4)$.

Therefore, $550 = 4950(9) + 11000(-4)$.

Theorem 3.10 Let a and b be integers, not both zero. Then $\gcd(a, b)$ is equal to the smallest positive linear combination of a and b.

Corollary 3.11 Let a and b be integers, not both zero. Then $\gcd(a, b) = 1$ if and only if there exist integers x and y such that $ax + by = 1$.

Definition Let a and b be integers, not both zero. Then a and b are said to be **relatively prime** if and only if $\gcd(a, b) = 1$.

2. Express the gcd of each pair of integers as a linear combination of a and b.

   (a) $a = 525$ and $b = 252$

   (b) $a = 54321$ and $b = 12345$

3. **True or False:** Let a and b be positive integers. If $ax + by = 1$ for some integers x and y, then a and b are relatively prime. [Justify your answer.]

4. In your group, discuss and record answers to each of the following.

   (a) What does it mean for an integer p to be prime?

   (b) Write down the first 10 prime numbers.

   (c) Is 1 prime? Why or why not?

   (d) If possible, write 420 as a product of prime numbers.

Definition 4.2: A **prime number** is an integer $p > 1$ whose only positive divisors are 1 and p. A positive integer greater than one that is not prime is said to be **composite**.

The Fundamental Theorem of Arithmetic: Every integer greater than 1 is either a prime or can be expressed as a product of primes. Furthermore, this factorization is unique up to the order of the factors.

Euclid's Lemma: Let a and b be integers and let p be a prime. If $p|ab$, then $p|a$ or $p|b$.

5. Look up the statement of Theorem 4.5 in your textbook and copy it in the space below. Then, explain in your own words why Euclid's Lemma is a special case of Theorem 4.5.