Math 11N
Homework 3
Due Thursday, January 27th, 2022

1. Recall from worksheet 3 the *least common multiple* of a and b, denoted $\text{lcm}(a, b)$. It is defined as the smallest positive integer ℓ such that:

   i. It's a common multiple of a and b, i.e. $a \mid \ell$ and $b \mid \ell$.

   ii. It's the smallest such common multiple, i.e. if $a \mid c$ and $b \mid c$, then $\ell \leq c$.

   Prove that if $\gcd(a, b) = 1$, then $\text{lcm}(a, b) = ab$.

2. Define a sequence of numbers F_n as follows:

$$F_0 = 1, \quad F_1 = 1$$
$$F_{n+1} = F_n + F_{n-1}, \quad n \geq 1$$

   This sequence starts $1, 1, 2, 3, 5, 8, 13, 21, \ldots$. This sequence is called the *Fibonacci sequence*, and the number F_n is called the n^{th} Fibonacci number. Prove by induction that for all $n \geq 1$, the number of steps required for the Euclidean algorithm on the pair (F_{n+1}, F_n) to terminate is exactly n.

3. In this problem, you will give a proof that $\sqrt{2}$ is irrational using the Euclidean algorithm. Suppose that $\sqrt{2}$ was rational, so it can be written as $\sqrt{2} = \frac{a}{b}$ for some positive integers a, b with $b \neq 0$.

   (a) Show that $a = b \cdot 1 + (a - b)$ with $0 \leq a - b < b$, so that this is the first step in the Euclidean algorithm on the pair (a, b) with $q_1 = 1$ and $r_1 = a - b$.

   (b) Write down the next step in the Euclidean algorithm by performing the division algorithm on the pair $(b, a - b)$. What is q_2? What is the ratio r_1/r_2? (Your answers should be *numbers*, not involving the letters a, b).

   (c) Prove that $q_n = q_2$ and $\frac{r_{n-1}}{r_n} = \frac{r_1}{r_2}$ for all $n \geq 2$. (*Hint: prove these both simultaneously via induction.*)

   (d) Explain why the truth of the statement in (c) yields a contradiction, therefore proving that $\sqrt{2}$ must not be rational.

4. For each of the pairs of integers (a, b) below, do the following:

   (i) Run the Euclidean algorithm to compute $\gcd(a, b)$.

   (ii) Use back substitution to find integers x, y such that $ax + by = \gcd(a, b)$.

   (a) $(504, 94)$

   (b) $(-1260, 816)$

The goal of the remaining problems is to determine when a linear equation $ax + by = c$ with $a, b, c \in \mathbb{Z}$ has integer solutions, and to classify the complete solution set. We'll continually assume that a, b are non-zero integers.

5. Let $c \in \mathbb{Z}$. Prove that $ax + by = c$ has integer solutions if and only if $\gcd(a, b) \mid c$.

6. Let $d = \gcd(a, b)$ and suppose that $d \mid c$, so that by the previous problem, the equation $ax+by = c$ has integer solutions. Suppose you are given $x_0, y_0 \in \mathbb{Z}$ such that $ax_0+by_0 = c$. Let $a = da'$ and $b = db'$ for some integers a', b'. Define, for any $k \in \mathbb{Z}$,

$$x_k = x_0 + b'k \qquad \text{and} \qquad y_k = y_0 - a'k.$$

   Note: Try to avoid the use of fractions throughout this problem! You don't actually need them anywhere!

   (a) Prove that for all $k \in \mathbb{Z}$, (x_k, y_k) is a solution to the equation $ax + by = c$.

   (b) Now assume that (x, y) is another solution to the equation $ax + by = c$. Prove that there is some $k \in \mathbb{Z}$ for which $x = x_k$ and $y = y_k$.

   (c) Find all integer solutions to the equation $37x + 47y = 103$.