MATH 3345 HOMEWORK 6

**Problem 1.** Falkner Section 5 Exercise 23
For this problem, you can also do the following:
Recall $F_1 = F_2 = 1$, and for $n \geq 2$, $F_{n+1} = F_n + F_{n-1}$. For $n \in \mathbb{N}$, let $P(n)$ be the statement

- $F_n$ is even if and only if 3 divides $n$.

Use the Principle of Strong Mathematical Induction to prove that for all $n \in \mathbb{N}$, $P(n)$ holds. To do so, you'll need to prove *two* base cases before your inductive step.

**Problem 2.** Falkner Section 7 Exercise 4
*Read Definition 7.11 and Examples 7.12*

**Problem 3.** Falkner Section 7 Exercise 14

We showed in class that if $d, n \in \mathbb{N}$ such that $d$ divides $n$, then $d \leq n$. If $a, b \in \mathbb{N}$, we say that their *greatest common divisor* is the largest $d \in \mathbb{N}$ such that $d$ divides $a$ and $d$ divides $b$. We denote the greatest common divisor of $a$ and $b$ by $\gcd(a, b)$. The greatest common divisor is well-defined, since 1 always divides $a$ and $b$, and the largest $\gcd(a, b)$ can be is $\min\{a, b\}$.

**Problem 4.** Fix $p \in \mathbb{N}$ with $p \geq 2$. Prove the following two conditions are equivalent.

(a) $p$ is prime.

(b) For all $d \in \{1, \ldots, p-1\}$, $\gcd(d, p) = 1$.

**Problem 5.** Falkner Section 7 Exercise 15

**Optional problem 1.** Suppose $a, b, q, r \in \mathbb{N}$ such that $a = bq + r$. (In particular, $r \neq 0$.) Show that $\gcd(a, b) = \gcd(b, r)$.
*Hint: Use Problem 3.*

**Optional problem 2.** Show that for every $a, b \in \mathbb{N}$, there are integers $k, \ell \in \mathbb{Z}$ such that $ak + b\ell = \gcd(a, b)$.
*Hint: Proceed as follows:*

*(1) For $a \in \mathbb{N}$, let $P(a)$ be the statement*

- *For each $b \in \mathbb{N}$, there are $k, \ell \in \mathbb{Z}$ such that $ak + b\ell$ is a common divisor of $a$ and $b$.*

*Use the Principal of Strong Mathematical Induction to prove for all $a \in \mathbb{N}$, $P(a)$ holds.*

*(2) Prove that if $d = ak + b\ell$ is a common divisor of $a$ and $b$, and if $d > 0$, then $d = \gcd(a, b)$.*

**Optional problem 3.** Fix $m \in \mathbb{N}$.

(a) Suppose $a \in \{1, \ldots, m-1\}$ with $\gcd(a, m) = 1$. Show there is a $b \in \{1, \ldots, m-1\}$ such that $\overline{a} \cdot \overline{b} = \overline{1}$.
*Hint: Use Optional Problem 2 to write $1 = ak + m\ell$ for some $k, \ell \in \mathbb{Z}$. Now pick $b$ carefully.*

(b) Suppose there is an $a \in \{1, \ldots, m-1\}$ such that there is no $b \in \{1, \ldots, m-1\}$ with $\overline{a} \cdot \overline{b} = \overline{1}$. Prove that $m$ is not prime.