MATH 3345 HOMEWORK 7

For Problem 1 below, you may use the following fact without proof:

Fact 1. For every $a, b \in \mathbb{N}$, there are integers $k, \ell \in \mathbb{Z}$ such that $ak + b\ell = \gcd(a, b)$.

If you wish to prove the above fact, you may do so below in Optional Problem 1.

Problem 1. Fix $m \in \mathbb{N}$ with $m \geq 2$.

(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 Fact 1 above.

(b) Deduce from part (a) that if m is prime and $a \in \{1, \ldots, m-1\}$, then there is a $b \in \{1, \ldots, m-1\}$ such that $\overline{a} \cdot \overline{b} = \overline{1}$.

Problem 2. Suppose A and B are sets. Show that the following are equivalent.

(a) $A \subseteq B$

(b) $A \cup B = B$

(c) $A \cap B = A$

(d) $A \setminus B = \emptyset$

Hint: To show they are all equivalent, you can prove (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d) $\Rightarrow$ (a), or any other cycle of your choice.

Problem 3.

(a) Falkner Section 10 Exercise 12

(b) Falkner Section 10 Exercise 13

Problem 4.

(a) Falkner Section 10 Exercise 14

(b) Falkner Section 10 Exercise 15

Problem 5. Falkner Section 10 Exercise 19

Optional problem 1. 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 $d = \gcd(a, b)$.