Homework 2

Instructions: Complete each of the following on separate, stapled sheets of paper.

1. Let $f : A \to B$ be a function. Define a relation R on the set A by $x \; R \; y$ when $f(x) = f(y)$. Prove that R is an equivalence relation.

2. Let $\sim$ be an equivalence relation on set S. Recall that the *equivalence class* of $s \in S$ is the set $[s] = \{t \in S : s \sim t\}$. Prove that $[s_1] = [s_2]$ if and only if $s_1 \sim s_2$.

3. Let $f : X \to Y$ and $g : Y \to Z$ be functions. Prove the following.
   (a) If both f and g are injective, then $g \circ f$ is injective.
   (b) If $g \circ f$ is surjective, then g is surjective.

4. Prove each of the following:
   (a) $\sum_{k=1}^{n} 1 = n$ for all $n \in \mathbb{Z}_{>0}$.
   (b) $\sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3}$ for all $n \in \mathbb{Z}_{>0}$.
   (c) $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$ for all $n \in \mathbb{Z}_{>0}$.
   (d) $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$ for all $n \in \mathbb{N}_0$.

5. Let F_k denote the k^{th} Fibonacci Number. Prove that F_{4n} is divisible by 3 for all integers $n \geq 0$.

6. Let $a, b, c \in \mathbb{Z}$ be arbitrary. Prove the following.
   (a) If $a \mid b$ and $b \mid c$, then $a \mid c$.
   (b) If $a \mid b$ and $a \mid c$, then $a|(bs + ct)$ for all $s, t \in \mathbb{Z}$.

7. We proved the following in class:

   Proposition (Quotient-Remainder Theorem for $\mathbb{N}_0$)**.** *Let $n, d \in \mathbb{N}_0$ with $d \neq 0$. There exist unique $q, r \in \mathbb{N}_0$ such that $n = dq + r$ and $0 \leq r < d$.*

   Finish the proof of the Quotient-Remainder Theorem for $\mathbb{Z}$ using the proposition above.[1] In other words, prove that for all $n, d \in \mathbb{Z}$ with $d \neq 0$ there exist unique $q, r \in \mathbb{Z}$ such that $n = dq + r$ and $0 \leq r < |d|$.

8. Make Cayley tables for the operations indicated below.
   (a) addition and multiplication modulo 7
   (b) addition and multiplication modulo 8

9. Let $m, n \in \mathbb{Z}$ with $m \neq 0$. Prove that if $n = mq + r$ for some $q, r \in \mathbb{Z}$, then $\gcd(m, n) = \gcd(m, r)$.

10. Use Euclid's Extended Algorithm to write each of the following as linear combinations of their arguments.
    (a) $\gcd(87, 2500)$
    (b) $\gcd(85, 105)$

[1] This problem is optional, but it's a good idea to do it anyway.