Math 230 **Fall 2018**
Homework 6 **Drew Armstrong**

Problem 1. This problem is about the ring $\mathbb{Z}/17\mathbb{Z}$. Since $\gcd(8,17) = 1$ we know that the element $[8]_{17} \in \mathbb{Z}/17\mathbb{Z}$ has a multiplicative inverse.

(a) Use the Extended Euclidean Algorithm to find the inverse $[8^{-1}]_{17} \in \mathbb{Z}/17\mathbb{Z}$.
(b) Use your answer from part (a) to solve the following equations for $x, y, z \in \mathbb{Z}$:

$$[8x]_{17} = [2]_{17},$$
$$[8y]_{17} = [3]_{17},$$
$$[8z]_{17} = [4]_{17}.$$

Problem 2. In this problem you will give an induction proof of Fermat's Little Theorem. You may assume that the following statement, which we proved in class: For all $a, b, p \in \mathbb{Z}$ with p prime we have

$$[(a+b)^p]_p = [a^p]_p + [b^p]_p.$$

Now fix a prime p and for each integer $n \in \mathbb{Z}$ consider the following statement:

$$P(n) = \text{"}[n^p]_p = [n]_p.\text{"}$$

(a) Explain why the statements $P(0)$ and $P(1)$ are true.
(b) If $P(n)$ is true, prove that $P(-n)$ is true. [Hint: $p = 2$ is a special case.]
(c) If $P(n)$ is true, prove that $P(n+1)$ is true.

Problem 3. In this problem you will prove a formula related to the RSA Cryptosystem.

(a) Consider $a, b, c \in \mathbb{Z}$ with $\gcd(a,b) = 1$. If $a|c$ and $b|c$, prove that $ab|c$. [Hint: There exist integers $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Multiply both sides by c.]
(b) Consider $a, p \in \mathbb{Z}$ with p prime and with $\gcd(a,p) = 1$ (i.e., with $p \nmid a$). Prove that $[a^{p-1}]_p = [1]_p$. [Hint: Use Problem 2 and the fact that $[a^{-1}]_p$ exists.]
(c) Consider $m, p, q \in \mathbb{Z}$ with $p \neq q$ prime and with $\gcd(m, pq) = 1$ (i.e., with $p \nmid m$ and $q \nmid m$). Prove that

$$[m^{(p-1)(q-1)}]_{pq} = [1]_{pq}.$$

[Hint: Use part (b) to show that $p|(m^{(p-1)(q-1)} - 1)$ and $q|(m^{(p-1)(q-1)} - 1)$. You will need to mention the extended version of Euclid's Lemma. Then use part (a).]