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 $x, y, z \in \mathbb{Z}$:

$$\begin{aligned} [8x]_{17} &= [2]_{17}, \\ [8y]_{17} &= [3]_{17}, \\ [8z]_{17} &= [4]_{17}. \end{aligned}$$

(a) Consider the set of triples $k, \ell, m \in \mathbb{Z}$ such that $8k + 17\ell = m$. Starting with the easy triples $(0,1,17)$ and $(1,0,8)$, we have the following table:

k	ℓ	m
0	1	17
1	0	8
-2	1	1

It follows that $8(-2) + 17(1) = 1$, and hence

$$\begin{aligned} [8]_{17} \cdot [-2]_{17} + [17]_{17} \cdot [1]_{17} &= [1]_{17} \\ [8]_{17} \cdot [-2]_{17} + \cancel{[0]_{17} \cdot [1]_{17}} &= [1]_{17} \\ [8]_{17} \cdot [-2]_{17} &= [1]_{17}. \end{aligned}$$

In other words:

$$[8^{-1}]_{17} = [-2]_{17} = [15]_{17}.$$

(b) From part (a) we know that "dividing by 8" is the same as "multiplying by 15" mod 17. Thus we have

$$\begin{aligned} [8x]_{17} &= [2]_{17} \\ [15]_{17} \cdot [8x]_{17} &= [15]_{17} \cdot [2]_{17} \\ [x]_{17} &= [2 \cdot 15]_{17} = [30]_{17} = [13]_{17}, \end{aligned}$$

and

$$\begin{aligned} [8y]_{17} &= [3]_{17} \\ [15]_{17} \cdot [8y]_{17} &= [15]_{17} \cdot [3]_{17} \\ [y]_{17} &= [3 \cdot 15]_{17} = [45]_{17} = [11]_{17}, \end{aligned}$$

and

$$\begin{aligned} [8z]_{17} &= [4]_{17} \\ [15]_{17} \cdot [8z]_{17} &= [15]_{17} \cdot [4]_{17} \\ [z]_{17} &= [4 \cdot 15]_{17} = [60]_{17} = [9]_{17}. \end{aligned}$$

Problem 2. In this problem you will give an induction proof of Fermat's Little Theorem. You may assume 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.

(a) Since $0^p = 0$ and $1^p = 1$ we note that the following statements are true:

$$[0^p]_p = [0]_p,$$
$$[1^p]_p = [1]_p.$$

(b) Assuing that $[n^p]_p = [n]_p$, we will prove that $[(-n)^p]_p = [-n]_p$.

Proof. There are two cases. Case 1: If p is odd then we have

$$[(-n)^p]_p = [(-1)^p n^p]_p = [-n^p]_p = [-1]_p \cdot [n^p]_p = [-1]_p \cdot [n]_p = [-n]_p.$$

Case 2: If p is even then since p is prime we must have $p = 2$. Thus we want to show that $[(-n)^2]_2 = [-n]_2$. But note that $[-1]_2 = [1]_2$. Therefore we have

$$[(-n)^2]_2 = [(-1)^2 n^2]_2 = [n^2]_2 = [n]_2 = [-1]_2 \cdot [n]_2 = [-n]_2.$$

□

(c) Assuming that $[n^p]_p = [n]_p$, we will prove that $[(n + 1)^p]_p = [n + 1]_p$.

Proof. We assume that $[(a+b)^p]_p = [a^p]_p + [b^p]_p$ for all $a, b \in \mathbb{Z}$. (This is called the "Freshman's Dream." The proof uses the Binomial Theorem and we did it in class.) Thus we have

$$[(n + 1)^p]_p = [n^p]_p + [1^p]_p = [n]_p + [1]_p = [n + 1]_p,$$

as desired. □

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).]

(a) *Proof.* Consider $a, b, c \in \mathbb{Z}$ with $a|c$ and $b|c$, so that $c = ak$ and $c = b\ell$ for some $k, \ell \in \mathbb{Z}$. If $\gcd(a, b) = 1$ then we know that there exist some (non-unique) $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Multiplying both sides by c gives

$$\begin{aligned} c &= cax + cby \\ &= (b\ell)ax + (ak)by \\ &= ab(\ell x + ky), \end{aligned}$$

and hence $ab|c$. □

(b) *Proof.* Consider $a, p \in \mathbb{Z}$ with p prime and $p \nmid a$. From Problem 2 we know that

$$[a^p]_p = [a]_p.$$

But since $\gcd(a, p) = 1$ we also know that the inverse $[a^{-1}]_p$ exists. Multiplying both sides by the inverse gives

$$\begin{aligned} [a^p]_p &= [a]_p \\ [a^{-1}]_p \cdot [a^p]_p &= [a^{-1}]_p \cdot [a]_p \\ [a^{p-1}]_p &= [1]_p. \end{aligned}$$

□

Alternate Proof. Consider $a, p \in \mathbb{Z}$ with p prime and $p \nmid a$. From Problem 2 we know that $[a^p]_p = [a]_p$. By definition this means that

$$p|(a^p - a) \quad \text{or, in other words,} \quad p|a(a^{p-1} - 1).$$

Then since p is prime and $p \nmid a$ we have from Euclid's Lemma that

$$p|(a^{p-1} - a) \quad \text{or, in other words,} \quad [a^{p-1}]_p = [1]_p.$$

□

(c) *Proof.* 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 $q \nmid m$.) Since $p \nmid m$ we also have $p \nmid m^{(q-1)}$. Indeed, we have $p \nmid m^k$ for any power k. This follows from the contrapositive of Euclid's Lemma:

$$p|(m \cdot m \cdots m) \quad \Longrightarrow \quad (p|m \text{ or } p|m \text{ or } \cdots \text{ or } p|m) \quad \Longrightarrow \quad p|m.$$

By setting $a = m^{(q-1)}$ we have from part (b) that

$$[(m^{(q-1)})^{(p-1)}]_p = [1]_p \quad \Longrightarrow \quad [m^{(p-1)(q-1)}]_p = [1]_p \quad \Longrightarrow \quad p|(m^{(p-1)(q-1)} - 1).$$

The same proof also gives $q|(m^{(p-1)(q-1)} - 1)$. Then since $\gcd(p, q) = 1$ (because p, q are non-equal prime numbers), part (a) with $a = p$, $b = q$ and $c = m^{(p-1)(q-1)} - 1$ gives

$$pq|(m^{(p-1)(q-1)} - 1) \quad \text{and hence} \quad [m^{(p-1)(q-1)}]_{pq} = [1]_{pq}.$$

□