Due Date: Thursday, September 22 at 5PM EDT

Carefully read and provide solutions to the problems below, showing all work required to justify any conclusions you make. You are encouraged to collaborate with your classmates, but all solutions turned in should be your own work. If you do collaborate, please record the names of those other students on your submitted work. Finally, your work should be submitted as a PDF on Gradescope before the listed due date.

Textbook problems: 9.1, 9.2, 10.2

Problem 1. Fix $a, n \in \mathbb{N}$. The **order** of a mod n is the smallest $k \in \mathbb{N}$ such that $a^k \equiv 1 \pmod{n}$, if such a k exists.

(a) Show that a has an order mod n if and only if $\gcd(a, n) = 1$.

(b) Show that if $\gcd(a, n) = 1$ and a has order k mod n, the powers $a, a^2, \ldots, a^k$ are pairwise incongruent mod n.

(c) Let k be the order of a mod n. Show that for any $m \in \mathbb{N}$, $a^m \equiv 1 \pmod{n}$ if and only if k divides m.

(d) Show that if p is prime and $\gcd(a, p) = 1$, then the order of a mod p divides $p - 1$.

Problem 2. Let $a, n \in \mathbb{N}$ with $\gcd(a, n) = 1$.

(a) Show that the order of a mod n divides $\phi(n)$.

(b) Can you find any a and n such that the order of a mod n is less than $\phi(n)$? Describe any patterns you observe.

Problem 3. Let p be a prime. Show that for every $1 \leq a < p$, there is a unique $1 \leq b < p$ such that $ab \equiv 1 \pmod{p}$. *Hint: FLT.*