MAT-255– Number Theory Spring 2024 In Class Work April 3

Your Name: _____ Group Members: _____ _____

Lemma 1. *Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Consider*

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a, \frac{p+1}{2}a, \ldots, (p-1)a.$$

The least absolute residues of ak and $a(p-k)$ differ by a negative sign. In other words,

$$ak \equiv -a(p-k) \pmod{p}.$$

Furthermore, for each $k = 1, 2, \ldots, \frac{p-1}{2}$, the exactly one of k and $-k$ is a least absolute residue of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$.

Problem 1 *Check Lemma 1 for*

(a) $a = 3, p = 7$

(b) $a = 5, p = 11$

(c) $a = 6, p = 11$