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

In-class Problem 1 Check Lemma 1 for

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

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

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

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

$$\begin{aligned} 3 \pmod 7,\ 3(2) \equiv -1 \pmod 7,\ 3(3) \equiv 2 \pmod 7,\\ 3(4) \equiv -2 \pmod 7,\ 3(5) \equiv 1 \pmod 7,\ 3(6) \equiv -3 \pmod 7, \end{aligned}$$

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

$$\begin{aligned} 5 \pmod{11},\ 5(2) \equiv -1 \pmod{11},\ 5(3) \equiv 4 \pmod{11},\\ 5(4) \equiv -2 \pmod{11},\ 5(5) \equiv 3 \pmod{11},\\ 5(6) \equiv -3 \pmod{11},\ 5(7) \equiv -2 \pmod{11},\ 5(8) \equiv -4 \pmod{11},\\ 5(9) \equiv 1 \pmod{11},\ 5(10) \equiv -5 \pmod{11}, \end{aligned}$$

(c) $a = 11, p = 23$

$$\begin{aligned} 11 \pmod{23},\ 11(2) \equiv -1 \pmod{23},\ 11(3) \equiv 10 \pmod{23},\\ 11(4) \equiv -2 \pmod{23},\ 11(5) \equiv 9 \pmod{23},\ 11(6) \equiv -3 \pmod{23},\\ 11(7) \equiv 8 \pmod{23},\ 11(8) \equiv -4 \pmod{23},\ 11(9) \equiv 7 \pmod{23},\\ 11(10) \equiv -5 \pmod{23},\ 11(11) \equiv 6 \pmod{23},\\ 11(12) \equiv -6 \pmod{23},\ 11(13) \equiv 5 \pmod{23},\\ 11(14) \equiv -7 \pmod{23},\ 11(15) \equiv 4 \pmod{23},\ 11(16) \equiv -8 \pmod{23},\\ 11(17) \equiv 3 \pmod{23},\ 11(18) \equiv -9 \pmod{23},\ 11(19) \equiv 2 \pmod{23},\\ 11(20) \equiv -10 \pmod{23},\ 11(21) \equiv 1 \pmod{23},\ 11(22) \equiv -11 \pmod{23}, \end{aligned}$$

Learning outcomes:
Author(s): Claire Merriman