MAT-255– Number Theory Spring 2024 In Class Work February 21

Your Name: _____ Group Members: _____ _____

In-class Problem 1 Let p be an odd prime. Use that $\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \pmod{p}$ to show

(a) If $p \equiv 1 \pmod 4$, then $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}$

(b) If $p \equiv 3 \pmod 4$, then $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod{p}$

Solution: (a) Let p be a prime with $p \equiv 1 \pmod 4$. Then $p = 4k+1$ for some $k \in \mathbb{Z}$. From part (a),

$$\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \equiv (-1)^{(4k+1+1)/2} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}.$$

(b) Let p be a prime with $p \equiv 3 \pmod 4$. Then $p = 4k+3$ for some $k \in \mathbb{Z}$. From part (a),

$$\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \equiv (-1)^{(4k+3+1)/2} \equiv (-1)^{2k+2} \equiv 1 \pmod{p}.$$

Learning outcomes:
Author(s): Claire Merriman