Math 105: Homework 6

Due November 14, 2025

Most questions are from the textbook but have been copied here for your convenience.

1. Use the fact that
$$p - j \equiv -j \pmod{p}$$
to show that if p is an odd prime $p = 2k + 1$, then
$$(p-1)! \equiv (-1)^k [(\frac{p-1}{2})!]^2 \pmod{p}.$$

2. Use the result of the previous problem to show that if $p \equiv 1 \pmod{4}$ is a prime, then $(\frac{p-1}{2})!$ is a solution to the congruence equation
$$x^2 + 1 \equiv 0 \pmod{p}.$$

3. Use the congruence equation $x^2 \equiv 1 \pmod{p}$ to show that if $(a, p) = 1$, then
$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

4. Show that if $p \equiv 1 \pmod{4}$ is a prime and g is a primitive root of p, then $g^{\frac{p-1}{4}}$ is a solution to the equation
$$x^2 \equiv -1 \pmod{p}.$$

5. There are four solutions to the equation
$$x^2 + 1 \equiv 0 \pmod{65}.$$
Find them by solving this equation $\pmod{5}$ and $\pmod{13}$ and then using the Chinese remainder theorem.

6. $g = 5$ is a primitive root modulo $p = 73$ (you may take this as a given). Using this, compute the orders modulo 73 of 5^4, 5^5, and 5^{20}.