

Homework Set Six

Due Thursday, June 9.

Question 1. Calculate the following Jacobi/Legendre symbols.

(a) $\left(\frac{7}{787}\right)$

(b) $\left(\frac{55}{179}\right)$

Question 2. Suppose p is a prime congruent to 3 modulo 4. Additionally, suppose a is a quadratic residue modulo p .

(a) Show that $x = a^{\frac{p+1}{4}}$ is a solution to the congruence

$$x^2 \equiv a \pmod{p}.$$

(b) Find a solution (between 1 and 786) to the congruence $x^2 \equiv 7 \pmod{787}$.

Question 3. Suppose p is an odd prime and a is a quadratic residue modulo p . Show that $p - a$ is a quadratic residue if $p \equiv 1 \pmod{4}$ and is a quadratic nonresidue if $p \equiv 3 \pmod{4}$.

Question 4.

(a) Suppose $p > 2$ is a prime and $a, b \in \mathbb{Z}$ are such that $\gcd(ab, p) = 1$. Prove that at least one of a , b , or ab is a quadratic residue modulo p .

(b) Suppose p is any prime. Show that for some $n > 0$, p divides

$$(n^2 - 2)(n^2 - 3)(n^2 - 6).$$