

Homework 6

(The Legendre symbol and Gauss's Lemma.)

Due Friday, November 8 at 11:30am in class.

Note: Be sure to justify your answers. No credit will be given for answers without work/justification. In addition, all written homework assignments should be neat and well-organized; **this assignment has only one part and can be submitted as a single packet.**

- (1) Find $\left(\frac{a}{11}\right)$ for each $a \in \mathbb{Z}$.
- (2) Let p be an odd prime and $[g]$ and $[h]$ be primitive roots mod p .
 - (a) Show that $[g], [h] \notin Q_p$.
 - (b) Show that $[gh] \in Q_p$.
- (3) Let p be an odd prime. Show that
$$[-50] \in Q_p \text{ if and only if } p \equiv 1 \text{ or } 3 \pmod{8}.$$
- (4) Suppose that q is a prime number such that $q \equiv 1 \pmod{4}$ and suppose that the number $p = 2q + 1$ is also a prime number. Show that $[2]$ is a primitive root mod p .
- (5)
 - (a) Use Euler's Criterion to determine if $[5]$ is a quadratic residue mod 23.
 - (b) Use Gauss's Lemma to determine if $[5]$ is a quadratic residue mod 23.

Fun problem (will not be graded):