Homework 8 (due Mar. 19)

MATH 110 | Introduction to Number Theory | Winter 2023

Problem 1 (20 pts)**.** Let p be an odd prime. Compute the Legendre symbols

$$\left(\frac{\frac{p-1}{2}}{p}\right) \qquad \text{and} \qquad \left(\frac{\frac{p+3}{2}}{p}\right).$$

The results should be stated in language of congruence class of p modulo a certain modulus independent of p. Namely, the conditions in the results should be of the form:

$$p \equiv \underline{\qquad} \pmod{m},$$

where m is a modulus independent of p.

Hint. First use the complete multiplicativity of Legendre symbol and then apply the quadratic reciprocity.

Problem 2. Consider the polynomial $f(T) = T^2 + T + 1$. The purpose of this problem is to figure out for which prime p, $f(T)$ is irreducible modulo p.

(a) (5 pts) Show that $f(T)$ is irreducible modulo 2.

Hint. Use Problem 2 (a) from HW 6.

Hence, we may assume p is odd. In what follows, we keep this assumption.

(b) (5 pts) Find an integer polynomial of the form $(T + a)^2 - q$ such that

$$f(T) \equiv (T + a)^2 - q \pmod{p}.$$

Hint. Note that p is odd.

(c) (5 pts) Argue that $f(T)$ is irreducible if and only if q (the leftover term in 2.(b)) is a quadratic non-residue modulo p.

Equivalently, $f(T)$ is irreducible if and only if

$$\left(\frac{q}{p}\right) = -1.$$

(d) (10 pts) Conclude the condition for $f(T)$ being irreducible modulo p in language of congruence of p modulo a certain modulus independent of p. Namely, the condition should be of the form:

$$p \equiv \underline{\qquad} \pmod{m},$$

where m is a modulus independent of p.