Homework 8 (due Dec. 2)

MATH 110 | Introduction to Number Theory | Fall 2022

Problem 1. Let p be an odd prime. Recall that a primitive root modulo p is an integer g such that $p-1$ is the smallest positive integer e such that

$$g^e \equiv 1 \pmod{p}.$$

(a) (5 pts) Consider $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{\overline{0}\}$. Show that there is an *isomorphism* (a bijective map preserving addition, multiplication, zero, and one) from $\mathbb{F}_p^\times$ to $\mathbb{Z}/(p-1)$.

Hint. First show that $\mathbb{F}_p^\times = \{g^e \mid 0 \leqslant e < p-1\}$, where g is a primitive root. (Why there is a primitive root?)

(b) (5 pts) Use a primitive root g to demonstrate that -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{4}$.

(c) (5 pts) Use a primitive root g to prove the *Wilson Theorem*: $(p-1)! \equiv -1 \pmod{p}$.

Hint. First show that $(p-1)! \equiv g^{1+2+\cdots+(p-2)} \pmod{p}$.

(d) (5 pts) Given a primitive root g, and an integer $a \in \Phi(p)$, prove that a is a quadratic residue modulo p if and only if $a \equiv g^e \pmod{p}$ for an even number e. Use this to prove the *Euler's Theorem on quadratic residues*:

$$a \text{ is a quadratic residue} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Problem 2 (10 pts)**.** Let p be an odd prime. Compute the Legendre symbols

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

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. Use the complete multiplicativity of Legendre symbol.

Problem 3. 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) (3 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) (3 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) (3 pts) Argue that $f(T)$ is irreducible if and only if q (the leftover term in 3.(b)) is a quadratic non-residue modulo p.

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

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

(d) (6 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.