Spring 2021, Math 522: Problem Set 13
Due: Thursday, April 29th, 2021
Quadratic Residues

(D1) *Jacobi symbols.* If c is odd and $c = p_1 p_2 \cdots p_k$ with each p_i prime, we define

$$\left(\frac{a}{c}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right),$$

called the *Jacobi symbol* of a and c.

(a) Find in $\left(\frac{a}{9}\right)$ for each $a = 0, 1, \ldots, 8$.

(b) Prove if c and c' are odd, then

$$\left(\frac{a}{c}\right)\left(\frac{a}{c'}\right) = \left(\frac{a}{cc'}\right).$$

(c) Prove if c is odd, then

$$\left(\frac{a}{c}\right)\left(\frac{b}{c}\right) = \left(\frac{ab}{c}\right).$$

(d) Prove that if c is odd and $a \equiv b \bmod c$, then

$$\left(\frac{a}{c}\right) = \left(\frac{b}{c}\right).$$

(e) Prove or disprove: for c odd, we have

$$\left(\frac{a}{c}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \bmod c \text{ has an integer solution for } x; \\ 0 & \text{if } c \mid a; \\ -1 & \text{otherwise.} \end{cases}$$

Hint: this holds by definition of c is prime.

(D2) *Using the reciprocity law.* Recall that for distinct primes p and q, we have

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

unless $p \equiv q \equiv 3 \bmod 4$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

(a) Using the piecewise formula for $\left(\frac{2}{p}\right)$ from class, prove that

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

(b) Find a formula for $\left(\frac{-1}{p}\right)$ in the spirit of part (a).

(c) Using the quadratic reciprocity law, prove

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

for any distinct odd primes p and q.

Homework problems. You must submit *all* homework problems in order to receive full credit.

Unless otherwise stated, $a, b, c, n, p \in \mathbb{Z}$ are arbitrary with $p > 1$ prime and $n \geq 2$.

(H1) Determine whether 70 is a quadratic residue modulo 101 without using a calculator.

Hint: use the property $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ of Legendre symbols and the quadratic reciprocity law to your advantage to compute $\left(\frac{70}{101}\right)$.

(H2) Prove that if p is an odd prime, then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 11 \bmod 12; \\ -1 & \text{if } p \equiv 5, 7 \bmod 12. \end{cases}$$

(H3) Prove that if a and c are odd and $\gcd(a, c) = 1$, then

$$\left(\frac{a}{c}\right)\left(\frac{c}{a}\right) = (-1)^{(a-1)(c-1)/4}.$$

(H4) Determine whether each of the following is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) Given a and n with $n \geq 2$, the equation

$$x^2 \equiv a \bmod n$$

has at most 2 incongruent solutions for x modulo n.

(b) For a and c odd with $\gcd(a, c) = 1$, we have

$$\left(\frac{a}{c}\right) = \left(\frac{c}{a}\right)$$

unless $a \equiv c \equiv 3 \bmod 4$.

(c) For c odd and $\gcd(a, c) = 1$, we have

$$\left(\frac{a}{c}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \bmod c \text{ has an integer solution for } x; \\ -1 & \text{otherwise.} \end{cases}$$