18.781 Problem Set 8 - Fall 2008

Due Tuesday, Nov. 4 at 1:00

1. Evaluate the following Legendre symbols:

   (a) $\left(\frac{85}{101}\right)$

   (b) $\left(\frac{29}{541}\right)$

   (c) $\left(\frac{101}{1987}\right)$.

2. (Niven 3.2.4abce) Determine which of the following are solvable (the moduli are all primes):

   (a) $x^2 \equiv 5 \pmod{227}$

   (b) $x^2 \equiv 5 \pmod{229}$

   (c) $x^2 \equiv -5 \pmod{227}$

   (d) $x^2 \equiv 7 \pmod{1009}$.

3. Prove that if $p \mid (n^2 - 5)$ for some integer n, then $p \equiv 1$ or $4 \pmod 5$.

4. Show that if $p \equiv 3 \pmod 4$, then $x = a^{(p+1)/4}$ is a solution to $x^2 \equiv a \pmod p$.

5. (Niven 3.2.6) Determine whether $x^2 \equiv 150 \pmod{1009}$ is solvable.

6. (Niven 3.2.8 & 3.2.9)

   (a) Characterize all primes p such that $\left(\frac{10}{p}\right) = 1$.

   (b) Characterize all primes p such that $\left(\frac{5}{p}\right) = -1$.

7. Use quadratic reciprocity to evaluate $(\frac{7}{p})$ based on the residue class of p mod 28.

8. In this problem you will produce an alternative proof of the formula for $(\frac{2}{p})$ when p is an odd prime.

   (a) Prove that $2 \cdot 4 \cdots (p-3) \cdot (p-1) \equiv \left(\frac{2}{p}\right) \cdot \left(\frac{p-1}{2}\right)! \pmod p$.

   (b) If u is the number of terms in the product that are larger than $\frac{p-1}{2}$, prove that
   $$2 \cdot 4 \cdots (p-3) \cdot (p-1) \equiv (-1)^u \left(\frac{p-1}{2}\right)! \pmod p.$$

   (c) Compare (a) and (b) to derive the formula for $(\frac{2}{p})$; you will need to separate into cases based on the value of p mod 8.

9. (Niven 3.3.1) Evaluate using quadratic reciprocity for Jacobi symbols:

(a) $\left(\frac{-23}{83}\right)$

(b) $\left(\frac{51}{71}\right)$

(c) $\left(\frac{71}{73}\right)$

(d) $\left(\frac{-35}{97}\right)$.

10. (Niven 3.3.7, 3.3.8 & 3.3.9)

    (a) For which primes are there solutions to $x^2 + y^2 \equiv 0 \pmod{p}$ with $(x, p) = (y, p) = 1$?

    (b) For which prime powers are there solutions to $x^2 + y^2 \equiv 0 \pmod{p^n}$ with $(x, p) = (y, p) = 1$?

    (Bonus) For which integers n are there solutions to $x^2 + y^2 \equiv 0 \pmod{n}$ with $(x, n) = (y, n) = 1$?

(Bonus) (Niven 3.2.16) Show that if $p = 2^{2^n} + 1$ is prime, then 3 is a primitive root modulo p, and that 5 and 7 are primitive roots when $n > 1$.