

18.781 Problem Set 6 - Fall 2009

Due Thursday, Oct. 29 at 2:30

1. Evaluate the following Legendre symbols:

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

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

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

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

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

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

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

(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 $\left(\frac{7}{p}\right)$ based on the residue class of $p \pmod{28}$.

8. In this problem you will produce an alternative proof of the formula for $\left(\frac{2}{p}\right)$ 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 $\left(\frac{2}{p}\right)$; you will need to separate into cases based on the value of $p \pmod{8}$.

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

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

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

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

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

10. Is there a quadratic form of discriminant 11 representing 7? If so, find one.
Is there such a quadratic form representing 3? If so, find one.