Math 412 Homework 9

your name

Due date: Nov 6, 2015

Solve the following problems. Please remember to use complete sentences and good grammar. Four points each.

1. (4 points) Show that there are infinite many primes of form $8k-1$. (hint: consider $N = (p_1p_2\dots p_n)^2 - 2$.)

2. (4 points) Compute the following Legendre symbols: $\left(\frac{13}{47}\right), \left(\frac{71}{73}\right)$.

3. (4 points) Find all prime p so that 3 is a quadratic nonresidue modulo p.

4. (4 points) Suppose that p is an odd prime with $\left(\frac{n}{p}\right) = -1$, where $n = k2^m + 1$ with $1 < k < 2^m$ for some integers k and m. Show that if n is a prime then $p^{(n-1)/2} \equiv -1 \pmod{n}$.

5. (12 points with 4 bonus points) The 221st proof of the quadratic reciprocity) Let p and q be distinct odd primes and R be the set of integers a such that $1 \le a \le \frac{pq-1}{2}$ and $(a, pq) = 1$, let S be the set of integers a with $1 \le a \le \frac{pq-1}{2}$ and $(a, p) = 1$, and let T be the set of integers $q \cdot 1, q \cdot 2, \dots, q \cdot \frac{p-1}{2}$. Finally, let $A = \prod_{a \in R} a$.

   (a) Show that T is a subset of S and that $R = S - T$.

   (b) Use part (a) and Euler's criterion to show that $A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}$.

   (c) Show that $A \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q}$ by switching the roles of p and q in parts (a) and (b).

   (d) Use part (b) and (c) to show that $(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)$ if and only if $A \equiv \pm 1 \pmod{pq}$.

   (e) Show that $A \equiv 1$ or $-1 \pmod{pq}$ if and only if $p \equiv q \equiv 1 \pmod{4}$.

   (f) Conclude from parts (d) and (e) that $(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)$ if and only if $p \equiv q \equiv 1 \pmod{4}$. Deduce the law of quadratic reciprocity from this congruence.