MAT 311 Introduction to Number Theory

Problem Set 8

Solutions

Problem 2 sec 3.2 Quadratic reciprocity tell us in this case that $x^2 \equiv q \mod p$ is solvable; the only thing to check is that it has exactly two solutions. It cannot have more because the number of solutions modulo a prime number cannot exceed the degree of the congruence. A unique solution is not possible because if x is a solution, then $-x$ also is, and if these two solutions were the same, we'd have $x \equiv -x \mod p$, which implies $p|2x$ and, since p is odd, $p|x$, but then we'd have $x^2 \equiv q \equiv 0 \mod p$.

Problems 1,2 sec 3.3 are easy, just compute the Legendre symbol using the reciprocity law and other rules. Switch to Jacobi symbol if necessary.

Problem 9 sec 3.2 By the Gauss reciprocity,

$$\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right).$$

To compute the latter, we can reduce q mod 5 and check the residues modulo 5. Since 1 and 4 are squares mod 5, and 2 and 3 are not, we see that

$$\left(\frac{5}{q}\right) = -1 \text{ iff } q \equiv 2, 3 \mod 5.$$

Problem 10 sec 3.2

$$\left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = (-1)^{\frac{q-1}{2}}(-1)^{\frac{q^2-1}{8}} = 1$$

if either both $\frac{q-1}{2}$ and $\frac{q^2-1}{8}$ are even, or they both are odd. Write $q = 8k + a$, then $\frac{q^2-1}{8}$ is congruent to $\frac{a^2-1}{8}$ modulo 2. Then check the residues 1,3,5,7 mod 8 to get the answer: $q \equiv 1, 3 \mod 8$.

Problem 8 sec 5.3 If n is even, we can find a Pythagorean triple $x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$ with $n = y = 2rs$. If n is odd, we can find a triple with $n = x = r^2 - s^2$, representing the odd number n as a difference of two squares as explained in the next solution.

The extra question: Since a^2 and b^2 can only be congruent to 0 or 1 mod 4, $n = a^2 - b^2$ can be congruent mod 4 to 0, 1 or 3, but not to 2. If n is odd, $n = 2k + 1$, then $n = (k + 1)^2 - k^2$ is a difference of two squares. Otherwise n must be a multiple of 4, and if $n = 4k$, then $n = (k + 1)^2 - (k - 1)^2$.