Math 40520 Theory of Number
Homework 9

Due Friday, 11/16, in class

Do 3 of the following problems.

1. Let p be an odd prime. Count the number of solutions to the equation $x^2 + ay^2 \equiv b \pmod{p}$, where $a, b \in \mathbb{Z}_p$.

2. Suppose $p \equiv 1 \pmod{4}$ is a prime. Count the number of solutions to
$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 \equiv 1 \pmod{p}.$$

3. Let p be an odd prime. Compute $\sum \left(\frac{(x_1+1)(x_2+1)(x_3+1)(x_4+1)(x_5+1)}{p}\right)$ mod 5, where the sum is taken over all tuples $(x_1, \ldots, x_5) \in \mathbb{Z}_p^5$ such that $x_1 + x_2 + x_3 + x_4 + x_5 \equiv 1 \pmod{p}$.

4. Let $p \equiv 5 \pmod{4}$ be a prime. Count the number of solutions to $x^2 - y^4 + z^6 \equiv 0 \pmod{p}$.

5. Let p be an odd prime. Show that the variance of the number of solutions to $y^2 \equiv x^3 + ax + b \pmod{p}$ is $p - 1$, i.e., show that
$$\frac{1}{p^2} \sum_{a,b \in \mathbb{Z}_p} \left(\sum_{x \in \mathbb{Z}_p} \left(\frac{x^3 + ax + b}{p} \right) \right)^2 = p - 1.$$