Homework 2

Due: Friday, February 3

1. Fix an odd prime p, and let $\zeta = \exp(2\pi i/p)$. For $a \not\equiv 0 \bmod p$, define

$$\sum_{x\in\mathbb{F}_p} \zeta^{ax^2}.$$

   Prove the following assertions:

   (a) $\tau(a) = \left(\frac{a}{p}\right)\tau(1)$

   (b) $|\tau(a)|^2 = p$

   (c) $\tau(1)^2 = \left(\frac{-1}{p}\right)p$.

2. For an odd prime p an $a \in \mathbb{Z}$, let

$$N(a,p) = \#\{(x,y,z) \in \mathbb{F}_p^3 : x^2 + y^2 + z^2 \equiv a \bmod p\}.$$

   Find a formula for $N(a,p)$.

3. Find an example of the following situation: A finite field $\mathbb{F}_q$, a number $d \geq 2$ such that $d|(q-1)$, and polynomials $a(T)$, $P(T)$ and $Q(T)$ in $\mathbb{F}_q[T]$ such that: P and Q are monic and irreducible; $\deg P = \deg Q$; $PQ \nmid a$; $a(T)$ is a d^{th} power mod $P(T)$; and $a(T)$ is not d^{th} power mod $Q(T)$.

4. Let $P(T) \in \mathbb{F}_q[T]$ be irreducible. Give a criterion, in terms of q and $\deg P$, for

$$X^2 + 1 \equiv 0 \bmod P(T)$$

   to have a solution.

5. Suppose $d|(q-1)$ and $P(T) \in \mathbb{F}_q[T]$ is irreducible. SHow that the number of solutions to the congruence

$$X^d \equiv a \bmod P(T)$$

   is

$$1 + \left(\frac{a}{P}\right)_d + \left(\frac{a}{P}\right)_d^2 + \cdots + \left(\frac{a}{P}\right)_d^{d-1}.$$