MATH 772
SUMMER 2006
HOMEWORK 0

Due Wednesday June 14, 2006.

1. (5 pt) Let $\mathbb{F}$ be a field and let $\mathfrak{F}$ be a (multiplicative) subgroup of $\mathbb{F} \setminus \{0\}$. Show that if $\mathfrak{F}$ is finite, then $\mathfrak{F}$ is cyclic.

2. (5 pt) Let $\mathbb{F}$ be a finite field. Show that every element in $\mathbb{F}$ can be written as the sum of two squares (that is, if $a \in \mathbb{F}$ then $a = x^2 + y^2$ for some $x, y \in \mathbb{F}$). Is this result true if the word "finite" is removed?

3. (5 pt) Let p be an odd prime and $\mathbb{F}$ be the finite field of p^n elements. Show that -1 is a square in $\mathbb{F}$ (that is, $-1 = x^2$ for some $x \in \mathbb{F}$) if and only if $p^n \equiv 1 \bmod(4)$. Use this to find all odd primes for which -1 is a square $\bmod(p)$. What happens if $p = 2$?