MATH 772
SPRING 2011
HOMEWORK 1

Due Wednesday September 14, 2011.

1. In this problem, we will find all solutions to the equations $x^2 + y^2 = z^2$ with $x, y, z \in \mathbb{N}$ and look at some of the properties of the solutions.

a) (5 pt) Show that if $(a, b, c), (u, v, w) \in \mathbb{Z}^3$ are solutions to $x^2+y^2 = z^2$, then so are (ta, tb, tc) and $(au - bv, av + bu, cw)$ (so the set of integral solutions forms a monoid with identity $(1, 0, 1)$).

b) (5 pt) Find all rational solutions to the equations $u^2 + v^2 = 1$ (hint: use the point $(-1, 0)$ on the unit circle to parametrize the set of these solutions, or perhaps examine the Weierstrauss substitution from Calculus II).

c) (5 pt) Show that the set of solutions to $x^2 + y^2 = z^2$ (with $x, y, z \in \mathbb{N}$) can be parametrized as follows

$$x = n^2 - m^2$$
$$y = 2nm$$
$$z = n^2 + m^2$$

with x, y, z pairwise relatively prime.

d) (5 pt) Show that exactly one of n, m is odd and the other is even.

2. (*Infinite Descent*) The objective of this problem is to show that the equation $x^4 + y^4 = z^4$ has no solutions for $x, y, z \in \mathbb{Z} \setminus \{0\}$. Note first that by the symmetry of this equation, we can assume that $x, y, z > 0$.

a) (5 pt) Consider first the equation $x^4 + y^4 = Z^2$. Use the results of the first problem to write x^2, y^2, and Z parametrically. Then find a Pythagorean triple involving y.

b) (5 pt) Use the Pythagorean triple to find a square smaller than Z^2 that is the sum of two fourth powers.

c) (5 pt) Derive a contradiction and explain why the equation $x^4 + y^4 = z^4$ has no nontrivial solution.

3. (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?

4. (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 mod(p). What happens if $p = 2$?