Homework 1

Due: Friday, January 27

1. Don Zagier[1] has given the following argument to show that every prime $p \equiv 1 \bmod 4$ is a sum of two squares:

   > "The involution on the finite set $S = \{(x,y,z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by
   >
   > $$(x,y,z) \longmapsto \begin{cases} (x+2z, z, y-x-z) & \text{if } x < y-z \\ (2y-x, y, x-y+z) & \text{if } y-z < x < 2y \\ (x-2y, x-y+z, y) & \text{if } x > 2y \end{cases}$$
   >
   > has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x,y,z) \mapsto (x,z,y)$ also has a fixed point."

   Supply the necessary details to turn this into a readable proof. If you like, you may proceed as follows. Let ι be the involution Zagier defines.

   (a) Show that ι really is an involution. (HINT: *Let $A = \{(x,y,z) \in S : x < y-z\}$, and defined B and C similarly. Start by showing that $\iota(A) \subseteq C$, $\iota(C) \subseteq A$, and $\iota(B) \subseteq B$.*)
   (b) Find all fixed points of ι. (HINT: *Suppose $p = 4k+1$. Consider $(1,1,k)$.*)
   (c) Conclude that p is a sum of squares.

2. Let p be an odd prime. Show that

   $$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ 3 & p \equiv 3 \bmod 4 \end{cases}$$

   in two different ways:

   (a) Using the previous problem.
   (b) Using the fact that $\mathbb{F}_p^\times$ is cyclic.

3. Let p be an odd prime, and suppose $a \not\equiv 0 \bmod p$. Prove Euler's criterion:

   $$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p.$$

   The statement is of course true if $a \equiv 0 \bmod p$, too. If you like, you may proceed as follows.

   (a) Show that $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$.
   (b) Write down $\frac{p-1}{2}$ values of a such that $a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right)$.
   (c) Why is this list complete?

[1] D. Zagier, "A one-sentence proof that every prime $p \equiv 1 \bmod 4$ is a sum of two squares", American Mathematical Monthly, vol. 97, no. 2, Feb 1990, p.144