Math 435 Number Theory I
Problem Set 4

Due: Friday September 23:

1) We showed that (x, y) is a rational solution to $X^2 + Y^2 = 1$ if and only if $(x, y) = (-1, 0)$

or there is $\lambda \in \mathbb{Q}$ such that

$$(x, y) = \left(\frac{1 - \lambda^2}{1 + \lambda^2}, \frac{2\lambda}{1 + \lambda^2} \right).$$

a) Suppose $\lambda = \frac{m}{n}$, where $m, n \in \mathbb{N}$. Show that $(n^2 - m^2, 2mn, n^2 + m^2)$ is an integral solution to

$X^2 + Y^2 = Z^2$.

b) Under what conditions on m and n is $(n^2 - m^2, 2mn, n^2 + m^2)$ a primitive solution in $\mathbb{N}$

[Recall that it is enough to have $\gcd(n^2 - m^2, 2mn) = 1$.]

2) Find a formula as in 1) for all rational points on the hyperbola $X^2 - Y^2 = 1$.

3) Solve the following congruences. Give the general solution.

a) $616x \equiv 144 (\text{mod } 780)$

b) $x \equiv 3 (\text{mod } 5)$ and $x \equiv 4 (\text{mod } 8)$ and $x \equiv 2 (\text{mod } 3)$.