Homework 10, Math 310, due November 14th, 2011

(1) Define a number $a \in \mathbb{Z}$ to be *even* if 2 divides a. Define a number to be *odd*, if it is not even.
  (a) Show that a is odd if and only if there exists an integer b such that $a = 2b + 1$.
  (b) Show that for any integer a, $a^2 + a + 1$ is odd.
  (c) If p is an odd prime (that is, p is a prime and $p \neq 2$) and if $p = a^2 + b^2$ for some integers a, b, show that there exists an integer c such that $p = 4c + 1$. (The converse is also true, but much harder and related to a very important theorem called *Gauss's law of quadratic reciprocity*).

(2) Let p be a prime and let $a \geq 0$ be a non-negative integer. Prove that there exists unique integers $a_0, a_1, \ldots, a_k$ for some k with $0 \leq a_i < p$ for all i and $a = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$. (This is called the p-adic expansion). (Hint: It might be easier to use the third alternate form of induction in the notes).

(3) Let p be a prime and let $\mathbb{N}' = \{0\} \cup \mathbb{N} \cup \{\infty\}$, where ∞ is just a symbol. We may define addition in $\mathbb{N}'$ as usual for all elements in $\mathbb{N} \cup \{0\}$ and with the rule $a + \infty = \infty$ for all $a \in \mathbb{N}'$. We also have the usual inequality in all of $\mathbb{N}'$, if we define $a < \infty$ for all $a \in \mathbb{N} \cup \{0\}$.
  (a) If $0 \neq a \in \mathbb{Z}$ show that there exists an $n \in \mathbb{N} \cup \{0\}$ such that p^n divides a and p^{n+1} does not divide a. Define $v_p(a) = n$.
  (b) If we define $v_p(0) = \infty$, we get a function $v_p : \mathbb{Z} \to \mathbb{N}'$. Prove that $v_p(ab) = v_p(a) + v_p(b)$ for all $a, b \in \mathbb{Z}$.
  (c) Prove that $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$ for all $a, b \in \mathbb{Z}$.

  This function (or some its variants) is called the *valuation at p*.

(4) Let $A = \mathbb{Z} \times \mathbb{Z}$. Then we can define an addition in A by component wise addition. That is, if $a = (a_1, a_2) \in A$ with $a_1, a_2 \in \mathbb{Z}$ and similarly if $b = (b_1, b_2)$, define $a+b = (a_1+b_1, a_2+b_2)$. For any two integers r, s, we define a map $\phi_{r,s} : A \to \mathbb{Z}$ as $\phi_{r,s}(a_1, a_2) = ra_1 + sa_2$.
  (a) Show that if $a, b \in A$, then $\phi_{r,s}(a + b) = \phi_{r,s}(a) + \phi_{r,s}(b)$.
  (b) If $f : A \to \mathbb{Z}$ is any function with $f(a + b) = f(a) + f(b)$ for all $a, b \in A$, show that there exists $r, s \in \mathbb{Z}$ such that $f = \phi_{r,s}$.
  (c) Show that $\phi_{r,s}$ is surjective if and only if $\gcd(r, s) = 1$.