Homework 1 : Due Wednesday, February 1

Problem 1: Suppose that $a, b \in \mathbb{Z}$ are relatively prime and that both $a \mid n$ and $b \mid n$.
a. Without using the Fundamental Theorem of Arithmetic, show that $ab \mid n$.
b. Using the Fundamental Theorem of Arithmetic, show that $ab \mid n$.

Problem 2: Let $p \in \mathbb{N}^+$ be prime. Define a function $ord_p \colon \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ as follows. Let $ord_p(0) = \infty$, and given $a \in \mathbb{Z} - \{0\}$, let $ord_p(a)$ be the largest $k \in \mathbb{N}$ such that $p^k \mid a$. Without using the Fundamental Theorem of Arithmetic, prove each of the following:
a. Show that $ord_p(ab) = ord_p(a) + ord_p(b)$ for all $a, b \in \mathbb{Z}$.
b. Show that $ord_p(a + b) \geq \min\{ord_p(a), ord_p(b)\}$ for all $a, b \in \mathbb{Z}$.
c. Show that $ord_p(a + b) = \min\{ord_p(a), ord_p(b)\}$ for all $a, b \in \mathbb{Z}$ with $ord_p(a) \neq ord_p(b)$.
Note: In these problems, you should interpret arithmetic with ∞ in the "obvious" ways. That is, let $k + \infty = \infty$ for all $k \in \mathbb{N} \cup \{\infty\}$ and $\min\{k, \infty\} = k$ for all $k \in \mathbb{N} \cup \{\infty\}$.

Problem 3: Give a characterization of the integers which can be written as the difference of two squares.

Problem 4: Let $E = \{2n : n \in \mathbb{Z}\}$ be the set of even integers. Notice that the sum and product of two elements of E is still an element of E, and that E is closed under additive inverses. Thus, E is almost a ring in that the only property it fails is the existence of a multiplicative identity. Call an element $a \in E$ *irreducible* if $a > 0$ and there is no way to write $a = bc$ with $b, c \in E$. Notice that 6 is irreducible in E even though it is not irreducible in $\mathbb{Z}$.
a. Give a characterization of the irreducible elements of E.
b. Show that the analogue of Fundamental Theorem of Arithmetic fails in E by finding a positive element of E which does *not* factor uniquely (up to order) into irreducibles.

Problem 5: Let R be a (commutative) ring and let I and J be ideals of R. Using these two ideals, there are (at least) three natural ways to build new ideals:

- $I \cap J$
- $I + J = \{a + b : a \in I, b \in J\}$
- $IJ = \{c_1d_1 + c_2d_2 + \cdots + c_kd_k : k \in \mathbb{N}^+, c_i \in I, d_i \in J\}$

You might have guessed that the definition of IJ should have been $\{cd : c \in I, d \in J\}$, but this is not generally closed under addition (which is why our definition is finite sums of such products). You should convince yourself that $I \cap J$ and $I + J$ are each ideals of R. Also, you should convince yourself that $I \cap J$ is the largest ideal contained in both I and J, while $I + J$ is the smallest ideal containing both I and J.
a. Prove that IJ is an ideal of R.
b. Prove that $IJ \subseteq I \cap J$.
c. Show that if $I = \langle a \rangle$ and $J = \langle b \rangle$, then $IJ = \langle ab \rangle$.
d. Find an example of ideals I and J of some commutative ring R for which $IJ \subsetneq I \cap J$.

Problem 6: Let R be a ring and let I and J be ideals of R. We say that I and J are *comaximal* if $I + J = R$ (this is equivalent to saying that there is no proper ideal containing both I and J). Give a characterization of the comaximal ideals of $\mathbb{Z}$.