Math 342 Problem set 4 (due 2/2/09)

The natural numbers

1. Show, for all $a,b,c \in \mathbb{Z}$:
   (a) (cancellation from both sides) $(ac,bc) = c\,(a,b)$.
   (b) (cancellation from one side) If $(a,c) = 1$ then $(a,bc) = (a,b)$
   Hint: can either do these directly from the definition or using Prop. 2.5.7 from the notes.

2. ($\sqrt{6}$ and friends)
   (a) Show that $\sqrt{6}$ is not rational.
   (b) Show that $\sqrt{3}$ is not of the form $a + b\sqrt{6}$ for any $a,b \in \mathbb{Q}$.
   Hint: If $\sqrt{3} = a + b\sqrt{6}$ we square both sides and use part (a) and that $\sqrt{2} \notin \mathbb{Q}$.
   (b) For any $a,b \in \mathbb{Q}$ show that $a\sqrt{2} + b\sqrt{3}$ is irrational unless $a = b = 0$.

Factorization in the integers and the rationals

3. Let $r \in \mathbb{Q} \setminus \{0\}$ be a non-zero rational number.
   (a) Show that r can be written as a product $r = \varepsilon \prod_p p^{e_p}$ where $\varepsilon \in \{\pm 1\}$ is a sign, all $e_p \in \mathbb{Z}$, and all but finitely many of the e_p are zero.
   Hint: Write $r = \varepsilon a/b$ with $\varepsilon \in \{\pm 1\}$ and $a,b \in \mathbb{Z}_{\geq 1}$.
   (b) Prove that this representation is unique, in other words that if we also have $r = \varepsilon' \prod_p p^{f_p}$ for $\varepsilon' \in \{\pm 1\}$ and $f_p \in \mathbb{Z}$ almost all of which are zero, then $\varepsilon' = \varepsilon$ and $f_p = e_p$ for all p.
   Hint: On each side separate out the prime factors with positive and negative exponents.

Ideals

DEFINITION. Call a non-empty subset $I \subset Z$ an *ideal* if it is closed under addition (if $a,b \in I$ then $a+b \in I$) and under multiplication by elements of $\mathbb{Z}$ (if $a \in I$ and $b \in \mathbb{Z}$ then $ab \in I$).

7. For $a \in \mathbb{Z}$ let $(a) = \{ca \mid c \in \mathbb{Z}\}$ be the set of multiples of a. Show that (a) is an ideal. Such ideals are called *principal*.

8. Let $I \subset \mathbb{Z}$ be an ideal. Show that I is principal.
   Hint: Use the argument from the second proof of Bezout's Theorem.

9. For $a,b \in \mathbb{Z}$ let (a,b) denote the set $\{xa + yb \mid x,y \in \mathbb{Z}\}$. Show that this set is an ideal. By problem 8 we have $(a,b) = (d)$ for some $d \in \mathbb{Z}$. Show that d is the GCD of a and b. This justifies using (a,b) to denote both the gcd of the two numbers and the ideal generated by the two numbers.

10. Let $I,J \subset \mathbb{Z}$ be ideals. Show that $I \cap J$ is an ideal, that is that the intersection is non-empty, closed under addition, and closed under multiplication by elements of $\mathbb{Z}$.

11. For $a,b \in \mathbb{Z}$ show that the set of common multiples of a and b is precisely $(a) \cap (b)$. Use problem 8 to show that every common multiple is a divisible by the least common multiple.

Congruences

12. Using the fact that $10 \equiv -1\,(11)$, find a simple criterion for deciding whether an integer n is divisible by 11. Use your criterion to decide if 76443 and 93874 are divisible by 11.

Optional problems: The p-adic distance

For an rational number r and a prime p let $v_p(r)$ denote the exponent e_p in the unique factorization from problem 3. Also set $v_p(0) = +\infty$ (∞ is a formal symbol here).

A. For $r, s \in \mathbb{Q}$ show that $v_p(rs) = v_p(r) + v_p(s)$, $v_p(r+s) \geq \min\left\{v_p(r), v_p(s)\right\}$ (when r, s, or $r+s$ is zero you need to impose rules for arithmetic and comparison with ∞ so the claim continues to work).

For $a \neq b \in \mathbb{Q}$ set $|a-b|_p = p^{-v_p(a-b)}$ and call it the p-adic *distance* between a, b. For $a = b$ we set $|a-b|_p = 0$ (in other words, we formally set $p^{-\infty} = 0$). It measure how well $a-b$ is divisible by p.

B For $a, b, c \in \mathbb{Q}$ show the *triangle inequality* $|a-c|_p \leq |a-b|_p + |b-c|_p$.
Hint: $(a-c) = (a-b) + (b-c)$.

C. Show that the sequence $\{p^n\}_{n=1}^{\infty}$ converges to zero in the p-adic distance (that is, $|p^n - 0|_p \to 0$ as $n \to \infty$).

REMARK. The sequence $\{p^{-n}\}_{n=1}^{\infty}$ cannot converge in this notion of distance: if it converged to some A then, after some point, we'll have $|p^{-n} - A|_p \leq 1$. By the triangle inequality this will mean $|p^{-n}|_p \leq |A|_p + 1$. Since $|p^{-n}|_p$ is not bounded, there is no limit. The notion of p-adic distance is central to modern number theory.