MATH 270
SUMMER 2004
HOMEWORK 3

Due Friday June 22, 2007.

You may freely use the fact that any subset of $\mathbb{N}$ *has a minimal element.*

1. (5 pt) (*The Euclidean Algorithm*). Show that if $n, m \in \mathbb{Z}$ and $m \neq 0$ then there is an integer, q, and $r \in \mathbb{N}_0$ such that

$$n = qm + r$$

with $0 \leq r < |m|$.

2. We recall that if $m, n \in \mathbb{Z}$ then the *greatest common divisor* of m and n (we write $\gcd(m, n) = d$ or $(m, n) = d$) is a (positive) common divisor of m and n with the property that if d' is another common divisor of m and n then $d'|d$. Additionally the *least commmon multiple* of m and n (we write $\operatorname{lcm}(m, n) = L$) is a positive common multiple of m and n such that if L' is another common multiple of m and n then $L|L'$.

Prove the following.

a) (5 pt) If $m, n \in \mathbb{N}$ and $d = \gcd(m, n)$ then there exist $r, s \in \mathbb{Z}$ such that $rm + sn = d$. Your proof should demonstrate the existence of the greatest common divisor of m and n. (This is a very important property of the integers.)

b) (5 pt) If $m, n \in \mathbb{N}$, $d = \gcd(m, n)$, and $L = \operatorname{lcm}(m, n)$, then $mn = dL$.

3. A natural number p is said to be *prime* if its only (positive) factors are itself and 1.

a) (3 pt) Show that if $n > 1$ is a natural number, then n can be written as a product of primes.

b) (3 pt) Show that if p is prime, $a, b \in \mathbb{N}$, and $p|ab$ then $p|a$ or $p|b$.

c) (3 pt) Show that if $n > 1$ is a natural number, then n can be expressed *uniquely* as a product of primes (this is the "Fundamental Theorem of Arithmetic").

4. (*Properties of Divisibility.*) Let $n, m \in \mathbb{Z}$ with $n \neq 0$. We say that n divides m (and write $n|m$) if there is an integer k such that $m = kn$. Prove the following divisibility properties. For this problem $a, b, r, s, n, m \in \mathbb{Z}$.

a) (3 pt) Show that if $n|a$ and $n|b$ then $n|(ra + sb)$.

b) (3 pt) Show that if $\gcd(n, m) = 1$ and $n|am$ then $n|a$.

c) (3 pt) Show that if $\gcd(n, m) = 1$ and $n|a$ and $m|a$ then $mn|a$.

5. (5 pt) (it The Rational Root Test) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with each $a_i \in \mathbb{Z}$. Suppose that this polynomial has the rational root $\frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$. Show that $a|a_0$ and $b|a_n$. Use this to find all complex roots of the polynomial $14x^4 + x^3 + 25x^2 + 2x - 6$.