Midterm 1 Study Guide

1. Provide definitions for the terms and statements for the theorems:

   a. A number being prime
   b. A number being composite
   c. Fundamental Theorem of Arithmetic

2. State in mathematical terms and either prove or provide a counterexample:

   a. If two numbers are equal modulo n when multiplied by a third number, then the numbers are equal modulo n.
   b. Every natural number is either prime or composite (but not both)
   c. Every natural number greater than 1 is divisible by some prime number.
   d. A number is prime if and only if all primes not exceeding its square root don't divide it.
   e. Two distinct primes are relatively prime.
   f. If a prime number divides a product, then it must divide one of the factors.
   g. A power of a number divides the same power of another number if and only if the first number divides the second.
   h. There are natural numbers that solve the equation $6n^2 = m^2$.
   i. If two numbers divide a third, then their product also divides it.
   j. If two relatively prime numbers divide a third, then their product also divides it.
   k. If two numbers have the property that whenever they divide a third number then their product also divides it, then the numbers must be relatively prime.
   l. A prime number either divides another number or is relatively prime to it.
   m. If a number is relatively prime to two other numbers, then it is also relatively prime to their product.
   n. Any two consecutive integers are relatively prime.
   o. If two numbers are relatively prime, any divisors of them are also relatively prime.
   p. If two numbers are relatively prime, any multiples of them are also relatively prime.
   q. For every integer there is a prime larger than it.

3. Prove:

   a. The equation $ax + by = c$ has a solution in integer x, y if and only if $\gcd(a, b)$ divides c.
   b. If $ax_0 + by_0 = c$, then all the solutions to the equation $ax + by = c$ are given by the formulas $x = x_0 + k\frac{b}{\gcd(a,b)}$, $y = y_0 - k\frac{a}{\gcd a,b}$. (Two questions here: that all these pairs are solutions,for every k, and that any solution has this form).

c. If p and $q_1, \ldots, q_n$ are primes and $p|q_1 \cdots q_n$, then there is an i such that $p = q_i$.

d. If $n > 1$ is a number with the property that whenever $n|ab$ it follows that $n|a$ or $n|b$, then n must be prime.

e. If $\gcd(b, c) = 1$ then $\gcd(a, bc) = \gcd(a, b)\gcd(a, c)$.

f. If $a' = \frac{a}{\gcd(a,b)}$ and $b' = \frac{b}{\gcd(a,b)}$, then $\gcd(a', b') = 1$.