Midterm 1 Study Guide

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

   a. An integer a *divides* another integer b.
   b. Two integers a and b are *congruent modulo* n.
   c. An integer d is a *common divisor* of a and b.
   d. The *greatest common divisor* of a and b.
   e. *Division Algorithm.*
   f. *Well-ordering axiom.*
   g. a and b are *relatively prime*.

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

   a. If a number divides two other numbers then it also divides their sum.
   b. If a number divides another number, then it also divides any multiple of that number.
   c. If a number divides the sum of two numbers then it also divides one of them.
   d. If a number divides the product of two numbers then it also divides one of them.
   e. 1 divides every number.
   f. Every number is divisible by 1.
   g. Every number divides 1.
   h. Every number divides 0.
   i. Congruence is a transitive relation.
   j. Congruence is a reflexive relation.
   k. Congruence is a symmetric relation.
   l. Divisibility is a symmetric relation.
   m. Divisibility is a transitive relation.
   n. Divisibility is a reflexive relation.
   o. If two numbers are congruent modulo n, then so are their k-th powers.
   p. Two numbers are relatively prime if and only if we can write 1 as a linear combination of them.
   q. a and b are both relatively prime to n if and only if their product ab also is.
   r. Two numbers can be relatively prime only if at least one of them is even.
   s. Two numbers can be relatively prime only if at least one of them is odd.
   t. If two relatively prime numbers both divide n then their product also divides n.
   u. If two numbers both divide n then their product also divides n.
   v. The relation of being relatively prime is reflexive.
   w. The relation of being relatively prime is symmetric.

x. The relation of being relatively prime is transitive.

3. Prove:

   a. If a is congruent to b modulo n, then $a+c$ is congruent to $b+c$ modulo n and ac is congruent to bd modulo n.
   b. If a is congruent to b modulo n, then $a-b$ is congruent to 0 modulo n.
   c. If a is congruent to b modulo n, and c is congruent to d modulo n, then ac is congruent to bd modulo n and $a+c$ is congruent to $b+d$ modulo n.
   d. For given integers n, m with n non-zero, there is at most one pair of integers q, r with r in the range from 0 to $n-1$ such that $m = nq + r$.
   e. If a divides bc, and a and b are relatively prime, then a must divide c.

4. Be able to follow the algorithm for finding the greatest common divisor of two numbers and express it as a linear combination of those numbers.