Discrete Structures | Homework 8
CS2800 Spring 2015 | Number theory

Note: Some of these proofs are very easy to find online. Try doing the problems before referring to other sources. If you do refer to online sources, try to write up the proofs without having looked at any notes for the past few hours.

1. Euclid's algorithm for finding the greatest common divisor $g(a,b)$ of two positive integers a and b is defined inductively as follows (assuming $a \geq b$):

   - If b is zero, then $g(a,b) = a$.
   - Otherwise, we know there exists some q, r such that $a = qb + r$ and $r < b$. In this case, $g(a,b)$ is defined as $g(b,r)$. This is well defined because $0 \leq r < b$.

   Prove the following statements by (strong) induction on b. Use the definition of a divisor: x is a divisor of y if and only if there exists a z such that $xz = y$.

   (a) $g(a,b)$ is a divisor of both a and b.

   (b) If c is any other divisor of both a and b, then c divides $g(a,b)$.

   (c) There are integers n and m such that $g(a,b) = na + mb$ (this is known as Bézout's identity).

2. Show that if x and y are coprime (that is, if $gcd(x,y) = 1$), that x has an inverse mod y. That is, there exists some z such that $xz \equiv 1 \mod y$. Hint: use question 1.

3. Prove that the base-b representation of a number is unique. That is, if

$$\sum_{i=0}^{n} a_i b^i = \sum_{i=0}^{n} a_i' b^i$$

   and if $0 \leq a_i < b$ and $0 \leq a_i' < b$, then for all i, $a_i = a_i'$. Hint: use induction on n, and write

$$a_0 + a_1 b + a_2 b^2 + a_3 b^3 \cdots = a_0 + (a_1 + a_2 b + a_3 b^2 + \cdots) b$$