CS 2800: Discrete Structures

Homework 7

Due Monday, October 22, 2012

Please write your netid in sufficiently large font on the upper right corner of all pages. Grading for all problems will be based on neatness, style, and correctness.

1. Prove that if x and y are relatively prime and x divides yz, then x divides z.

2. State the fundamental theorem of arithmetic.

3. Let a and b be positive integers. Are the integers s and t satisfying $as+bt = \gcd(a, b)$ unique? Hint: Consider the homogenous equation $as + bt = 0$. If a and b are relatively prime, is the multiplicative inverse of a mod b unique. Give a careful explanation for your answer.

4. Given the encryption and decryption algorithms E and D such that $D(E(m)) = m$ and $E(D(m)) = m$ explain how to send an encrypted and digitally signed message to someone who you have never meet before.

5. Use Euclid's gcd algorithm to compute the gcd of $x^4 + 5x^3 + 8x^2 + 5x + 1$ and $x^3 + 5x^2 + 7x + 2$ and then factor the two polynomials.