CS 1050 - Proofs
Homework 11
Assigned Saturday, November 13
Due <u>Thursday</u>, November 18

1. a) Prove that if d is a divisor of both a and b, then d is a divisor of $a - b$.

b) Now use that lemma to prove the following theorem

Theorem 1 *If $gcd(x, m) > 1$ then x has no multiplicative inverse* mod m.

2. Using Euclid's algorithm, find the gcd of

a) 1,575 and 231

b) 100,996 and 20,048

3. Use the extended-gcd algorithm to find a, b and d so that $d = \gcd(42, 98)$ and $d = a \cdot 42 + b \cdot 98$. Show the steps involved.

4. For all integers n between 5 and 9, and for all integers a such that $1 \leq a \leq n$, calculate $a^{n-1} (\text{mod } n)$. What do you find? Which answers were predicted by Fermat's little theorem?

5. a) Prove that $a^{\log_a x} = x$.

b) Prove that $\sqrt{2}^{\log_2 n} = n^{\frac{1}{2}}$.

c) Prove that $4^{\log_2 n} = n^2$.

d) Prove that $2^{\log_2^2 n} = n^{\log_2 n}$. (Recall that $\log_2^2 n = (\log_2 n)^2$.)

e) Prove that $\log_2^2 n = O(\log_e^2 n)$.