CS 1050 - Proofs
Homework 12
Assigned Sunday, November 21
Due Tuesday, November 30

1. Solve the following equations for x and y modulo the indicated modulus, or show that no solutions exists. Show your work.

a) $7x = 1 \pmod{15}$.

b) $10x + 20 = 11 \pmod{23}$.

c) $5x + 15 = 4 \pmod{20}$.

d) The system of simultaneous equations $3x + 2y = 0 \pmod{7}$ and $2x + y = 4 \pmod{7}$.

2. Given that a and d are relatively prime, prove that $ab = cd$ implies that d is a divisor of b.

3. a) Prove that the equation $ax = ay \pmod{n}$ implies that $x = y \pmod{n}$ whenever $\gcd(a, n) = 1$.

b) Show that the condition $\gcd(a, n) = 1$ is necessary by supplying a counterexample when $\gcd(a, n) > 1$.

4. Let $p = 17$, $q = 11$ be a RSA private key and $n = pq$, $e = 3$ be the public key. Feel free to use a computer to assist with the computations, but show all your work.

a) What is the result of encrypting the message $m = 86$ with these keys?

b) What is d?

c) How would the encrypted message be decrypted?

5. a) We saw in class that the RSA scheme can also be used for digital signatures. What happens if you sign an encrypted message which was encrypted using your public key?

b) Indeed, it is not safe to sign any random message given to you. Suppose someone gets a message $x' = x^e$ sent to you. He can pick another random message y, encrypt it using your public key e, and get y^e. Explain how the hacker can recover x if he can ask you to sign $y^e x'$.

6. We saw a secret sharing scheme that worked as long as k members all agree that they want to see the secret. Suppose that Bush wants to construct a variant so that the secret (launch code) can be recovered if **any 10** members of his n person cabinet agree to launch the missile *or* if **he and any 3** other cabinet members agree to launch the missile. Explain how to adapt the secret sharing scheme we saw in class to this case. (Hint: No fancy math is needed – just think about how to modify the scheme so that Bush has more "weight" than the other cabinet members.)