CS/Math 240: Introduction to Discrete Math
Homework 2
Due: October 23rd - in Lecture.

Change to the Quiz Schedule:
Quiz 2: Oct 29 and 31

Problem 1. Suppose that d is an integer greater than 0. Prove that the numbers 2d+1 and 9d+4 are relatively prime for every integer d. Hint: Find the greatest common divisor of 2d+1 and 9d+4 as a function of d.

Problem 2. Section 2.4, Problem 16 from the textbook.

> A digital signature is a way to securely sign a document. That is, it is a way to put your "signature" on a document so that anyone reading it knows that it is you who have signed it, but no one else can "forge" your signature. The document itself may be public; it is your signature that we are trying to protect. Digital signatures are, in a way, the opposite of encryption, as if Bob wants to sign a message, he first applies his signature to it (think of this as encryption) and then the rest of the world can easily read it (think of this as decryption). Explain, in detail, how to achieve digital signatures, using ideas similar to those used for RSA. In particular, anyone who has the document and has your signature of the document (and knows your public key) should be able to determine that you signed it.

Problem 3. Suppose n and k are two positive integers, and they are relatively prime. Prove that n divides C(n,k) evenly. Then, give an example to show that this fact is not always true if n and k are not relatively prime.
Hint: Recall from the last homework assignment that you proved k * C(n,k) = n * C(n-1,k-1).

Problem 4. Show that we can easily factor n (and thus break the RSA cryptosystem) when we know that n is the product of two primes, p and q, and we know the value of (p-1)(q-1).

Problem 5. Show that if m is not prime, then at least square root of m elements of Z_m do not have multiplicative inverses.