Math 55: Discrete Mathematics, Fall 2008
First Midterm Exam Solutions

1. Prove that a composite positive integer n must have a factor less than or equal to $\sqrt{n}$.

Since n is composite, let $n = pq$ where p and q are positive integers less than n. Without loss of generality we can let p be the smaller of p and q, so $p \leq q$. Multiplying both sides of this inequality by p, we get $p^2 \leq pq = n$, and therefore $p \leq \sqrt{n}$.

2. Identify the flaw(s) in the following reasoning:

> "Theorem:" If a function $f\colon S \to T$ is one-to-one, and the set T is non-empty, then T has more than one element.
>
> "Proof:" Using contraposition, we will show that if T has only one element, then f is not one-to-one. So assume that $T = \{t\}$. Then for all $x, y \in S$ we have $f(x) = f(y) = t$. If f were one-to-one we would have to have $f(x) \neq f(y)$, so f is not one-to-one.

We have not given a correct argument to show that f is not one-to-one. For this we should establish that there exist *distinct* elements $x, y \in S$ such that $x \neq y$ but $f(x) = f(y)$. But we have not shown that S has two distinct elements, or even that it has any elements at all. In fact, there are counterexamples to the the supposed theorem when S is empty or has only one element.

3. Three pirates stole a bag of gold coins. When they tried to divide the coins equally, one pirate ended up with one more coin than the other two. The two pirates who got less killed the third and took his coins. When the two surviving pirates tried to divide the coins equally, again one of them ended up with one extra coin. The other pirate killed him and ran off with all the loot. If there were between 95 and 100 coins in the bag, what was the exact number?

Let n denote the number of coins. The first division of the coins was into amounts k, k and $k+1$ for some k, so $n = 3k + 1$, that is, $n \equiv 1 \pmod 3$. Similarly, the second division into amounts l and $l+1$ shows that $n \equiv 1 \pmod 2$. By the Chinese Remainder Theorem, these two conditions together imply that $n \equiv 1 \pmod 6$. Therefore $n = 97$.

4. Compute $3^{1001} \bmod 11$

Since 11 is prime, we have $3^{10} \equiv 1 \pmod{11}$ by Fermat's theorem. Then $3^{1001} = (3^{10})^{100} \cdot 3 \equiv 3 \pmod{11}$, which shows that $3^{1001} \bmod 11 = 3$.

5. Suppose I am using the RSA cipher with modulus $n = 55$ and encryption exponent $e = 3$, so my public encryption function is $E(x) = x^3 \bmod 55$. Find my (supposedly secret) decryption function.

The prime factorization $n = pq$ is $55 = 5 \cdot 11$. The decryption function is $D(x) = x^d \bmod 55$, where the decryption exponent is inverse to 3 modulo $(p-1)(q-1) = 40$. Solving $3d \equiv 1 \pmod{40}$ we find that $d = 27$ (any $d \equiv 27 \pmod{40}$ will work, but $d = 27$ is the simplest solution).