Name: $\qquad$
Math 4150 - Introduction to Number Theory

## Test \# 1

You have 50 minutes to take this test. There are 52 total points possible. Simple calculators are fine, but no programmable calculators are allowed. Please write your answers neatly and show all of your work.

Feel free to write on both sides of each sheet.

1. $(4+6=10$ points $)$
a. State Fermat's Little Theorem.
b. Let $p$ and $q$ be distinct primes. Let $b$ be a positive integer so that $\operatorname{GCD}(b, p q)=1$. Then explain why the following is true.

$$
b^{(p-1)(q-1)} \equiv 1(\bmod \mathrm{pq}) .
$$

2. (10 points) Here is another way to prove that there are infinitely many primes. Suppose there are only finitely many, and $p_{1}, p_{2}, \ldots, p_{k}$ is all of them. Then consider the integer

$$
M=\frac{\prod_{i} p_{i}}{p_{1}}+\frac{\prod_{i} p_{i}}{p_{2}}+\cdots+\frac{\prod_{i} p_{i}}{p_{k}}
$$

where $\prod_{i} p_{i}$ is the product of all the $k$ primes.
... (Complete the proof).
3. $(5+10=15$ points $)$
a. Use the extended Euclidean algorithm to compute the multiplicative inverse of 11 modulo 97 .
b. Find the smallest positive integer $x$ such that $x \equiv 2(\bmod 11)$ and $x \equiv 3(\bmod 97)$.
4. $(4+4+4+5=17$ points) Answer each of the following with one or two sentences of explanation.
a. If $a, b, c$ are arbitrary positive integers with $a \mid b c$ then we may conclude that $a \mid c$. Prove or disprove.
b. How many integers from 1 to $p$ have an inverse modulo $p$, if $p$ is prime.
c. Find the GCD and LCM of the following three integers:

$$
7^{3} \times 5 \times 11^{2}, 3^{3} \times 5^{2} \times 11,3^{2} \times 5 \times 7^{2} \times 11^{3}
$$

d. If $p$ is prime and $1 \leq k<p$, show that the binomial coefficient $\binom{p}{k}$ is divisible by $p$.
Tip: First think without paying attention to the hint on the next page. If you are stuck, you may try the hint, at your own risk.

Hint : The binomial coefficient is always an integer!

## Extra Space

