Name: _____

Math 4150 – Introduction to Number Theory Spring 2010

Test # 2

Solve the first four problems in class and bring the solution to the remaining two to the class on Monday, April 5th.
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. Define the *order* of an integer a mod n?

   b. Let a and n be relatively prime to each other. Let a^{-1} be the inverse of a mod n. What is the order of a^{-1} mod n in terms of the order of a mod n? Prove your answer for full credit.

2. (6+4 points)

   a. Is 3 a primitive root mod 17? (Prove or disprove.) How many primitive roots does 17 have?

   b. Is 25 a *pseudoprime* to base 3? (Prove or disprove.)

3. (5+5=10 points) Let μ be the Möbius function defined on the positive integers.

   a. Show that μ is multiplicative.

   b. For $n \geq 1$, what is $\sum_{d|n} \mu(d)$? Prove your answer.

4. (4+4+4=12 points) Explain your answers briefly.

   a. How many (incongruent) integer solutions does $x^{11} \equiv 1 \pmod{23}$ have?
   How many (incongruent) integer solutions does $x^2 + x - 2 \equiv 0 \pmod{10}$ have?

   b. What is the least significant digit in the decimal expansion of $(13)^{4446}$?

   c. How would you check if a composite number n is a *strong pseudoprime* to base b?

Extra Space

Take-home Problems

5. (10 points) Show that if $n = (a^{2p} - 1)/(a^2 - 1)$, where a is an integer, $a > 1$, and p is an odd prime not dividing $a(a^2 - 1)$, then n is a pseudoprime to base a. Conclude that there are infinitely many pseudoprimes to any base a.

(*Hint*: To establish that $a^{n-1} \equiv 1 \pmod{n}$, show that $2p \mid (n-1)$, and demonstrate that $a^{2p} \equiv 1 \pmod{n}$.)

6. (10 points) Use the Möbius inversion formula and the identity $n = \sum_{d|n} \phi(n/d)$ to show the following:

(a) $\phi(p^k) = p^k - p^{k-1}$, whenever p is prime and k is a positive integer.

(b) $\phi(n)$ is multiplicative.