MA/CSSE 473 – Design and Analysis of Algorithms **In-class Quiz Day 09**

Name:_____ Score:____/ 7 circle your Section # 01(3rd) 02 (4th)

1 = 13*37 – 32*15.

1. What is the inverse of 15 (mod 37)?

2. What is 18/15 (mod 37)?

3. What does Fermat's Little Theorem say about a^{N-1}(mod N)
   a. if N is prime?

   b. if N is not prime?

4. Prove: If a is a number that is relatively prime to N such that a^{N-1} is not congruent to 1 mod N, then that same condition must be true for at least half of the numbers in the range 1…N-1.

5. What is a Carmichael number, and why are such numbers troublesome for primality testing?

6. What became clear to you as a result of today's discussion? (or write N/A)

7. Is there anything from today's discussion that was unclear, do you have questions, or is there anything else you want to tell me? (or write N/A)