MA/CSSE 473 – Design and Analysis of Algorithms **In-class Quiz Day 10**

Name:_____ Score:____/ 11 circle your Section # 01(3rd) 02 (4th)

1. What does Fermat's Little Theorem say about $a^{N-1} \pmod N$
   a. if N is prime?

   b. if N is not prime?

2. Outline our (Carmichael-free) primality testing algorithm

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

4. Is expressing N-1 as $2^t u$ (where u is odd) an expensive operation? Explain.

5. How does the Miller-Rabin test work?

6. Example: N = 105.

   a = 8

   a = 29

7. If there is a nontrivial square root of 1 (mod N), how do we know that N is composite?

8. What does Lagrange's Theorem say about $\pi(N)$, the number of primes smaller than N (for large N)?

9. What does this imply about the probability of randomly finding an n-bit prime?

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

11. 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)