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

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

1 = 13*37 – 32*15.

1. What is the inverse of 15 (mod 37)?
   -32*15 ≡ 1, and -32 ≡ 5 (mod 37), so 5 is the inverse.

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

   18/15 = 15*5 = 90 ≡ 16 (mod 37), so the answer is 16.

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

   b. if N is not prime? **The theorem tells us nothing**

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.

   See today's powerpoint slides.

   http://www.rose-hulman.edu/class/csse/csse473/201110/Slides/Day09_Fermat_Primality.pdf

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

   A composite number N for which every number a that is relatively prime to N, $a^{N-1} \equiv 1 \pmod N$.
   So everything passes the Fermat test, but still N is not prime.

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

   Must have an answer; any answer is OK

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)

   Must have an answer; any answer is OK