MA/CSSE 473 Quiz Day 9 20 points Name _____ **Section** 01 (9:00) 02 (9:55) 03 (10:50)

Due 10 minutes after class starts (9:10, 10:05, 11:00)

1. (4) Show how to use the extended Euclid algorithm to find 5^{-1} (mod 29). You will receive 1 point for the correct answer, and the other 4 for using extended Euclid correctly to get it.

   29 = 5*5 + 4
   5 = 1*4 + 1. GO gcd(29,5) =1. Thus 5 has an inverse (mod 29)
   Now work backwards:
   1 = 5 – 4 = 5 – (29 – 5*5) = 6*5 – 29. Summary: 1 = 6*5 – 29.

   Thus 6 is the inverse of 5 (mod 29).

   Check it: Not required. 6*5 = 30, which is one more than 29.

2. (4) A *permutation* of a set **S** is a function from **S** to **S** that is **one-to-one and onto.**

3. (4) Fermat's little theorem says that if p is prime, then for all numbers **a** in {1, 2, 3, …, p-1}

   $a^{p-1} \equiv 1 \pmod p$. Equivalently, $a^p \equiv p \pmod p$. Either answer counts as correct.

4. (4) Circle the correct answer. Fermat's little theorem can be used to show that a number **N**

   (a) is definitely prime
   (b) is definitely not prime
   (c) whichever of those is true for N
   (d) neither

5. (4) What is a Fermat liar? A number **a** such that **$a^{N-1} \equiv 1 \pmod N$** even though **N** is composite.