MA/CSSE 473 – Design and Analysis of Algorithms **In-class Quiz Day 08**

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

1. The following two conditions imply that d = gcd(a,b):

   a.

   b.

2. Given positive integers a and b, what does the extended Euclid algorithm compute?

3. Prove the validity of the extended Euclid algorithm.

```
def euclidExtended(a, b):
    """ INPUT:  Two integers a and b with a >= b >= 0
        OUTPUT: Integers x, y, d such that d = gcd(a, b)
                and d = ax + by"""
    print ("    ", a, b) # so we can see the process.
    if b == 0:
        return 1, 0, a
    x, y, d =  euclidExtended(b, a % b)
    return y, x - a//b*y, d
```

4. Find integers x and y such that 37x + 15y = 1.

5. What is the necessary and sufficient condition for **a** to have an inverse modulo **N**?

6. What is the inverse of 15, mod 37?

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

8. What is the running time for modular division, as a function of the number of bits in the numbers?

9. What does Fermat's Little Theorem say?

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)