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?
   Integers x and y such that ax + by = gcd(a, b)

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
```

Solution: First, the number d it produces really is t
of a and b. We can just ignore the x and y values,
and we have the same algorithm as before.

– We must show that the x and y it returns are such that ax + by =d.
– We do that by induction on b.
  - **Base case:** b=0
    Then gcd(a,b) = a,
    and the algorithm
    produces x = 1,
    y = 0. ☑
  - **Induction step:** b > 0.
    – It finds gcd(a, b) by calling euclidExtended(b, a%b)
    – Since a%b is smaller than b, by induction the x' and y' returned by the recursive call are such that
      gcd(b, a %b) = bx'+ (a%b)y'
    – We can write a % b as a – ⌊a/b⌋ * b
    – d = gcd(a, b) = gcd(b, a%b) = bx' + (a%b)y'
      = bx' +(a – ⌊a/b⌋ * b)y' = ay' +b(x' - ⌊a/b⌋ y')
    – Thus x = y' and y = x' - ⌊a/b⌋ y' are the numbers that make ax + by = d

This x and y are the numbers returned by the algorithm

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

37 = 2*15 + 7
15 = 2 * 7 + 1
7 = 7 * 1 + 0, so gcd(37, 15) = 1

Now work backwards
1 = 1 – 0. **Substitute 0 = 7 – 7*1**
1 = 1 – (7 – 7*1) = 1*7 – 6*1. **Substitute 1 = 15 – 2*7**
1 = 1*7 – 6(15 – 2*7) = 13*7 – 6*15 **Substitute 7 = 37 – 2*15**
1 = 13*(37 – 2*15) – 6*15 = 13*37 – 32*15.
X = 13, y=-32 (other answers are possible).

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

   gcd(a, N) = 1

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

   From #4, -32*15 + 13*37 = 1, so -32*15 ≡ 1 (mod 37). -32 mod 37 is 5, so 5 is the inverse of 15 (mod 37).

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

   $18/15 = 18*15^{-1} = 18*5 = 90 \equiv 16 \pmod{37}$.

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

   $\Theta(n^3)$

9. What does Fermat's Little Theorem say?

   Must have an answer. Any answer is OK.

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

    Must have an answer. Any answer is OK.

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)