MA/CSSE 473 Day 06

1. Modular exponentiation x^Y (mod N) . Why not just compute the power and then find the remainder mod N?

   Alternative 1: Compute the remainder after ever multiplication:

   Alternative 2: Cut down on the number of multiplications.

2. Prove by induction that in an Odd Pie Fight, at least one participant does not get hit by a pie.

3. What problem does Euclid's Algorithm solve?

   How do we know that gcd(x, y) = gcd (y, x-y)?

4. Show the recursive calls for Euclid's Algorithm applied to a=188 and b=144.

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

   a.

   b.

6. What is an upper bound on the number of recursive calls needed to compute gcd(a, b) if a > b?

7. Use the extended Euclid algorithm to find integers x and y such that x*25 + y * 11 = 1.