

## MA/CSSE 473 Day 06 Announcements and Summary

### Announcements:

1. HW 3 Due Tonight at 11:55PM.
2. Exam dates: Tuesday Sept 30, Tuesday, November 4. In-class. Not in schedule page yet.
  - If you are allowed extra time for the exam and plan to use that time, please talk with me soon about timing.
3. Don't use a pirated copy of the textbook!

### Main ideas from today:

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

2. What problem does Euclid's Algorithm solve?

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

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

a.

b.

5. Use the extended Euclid algorithm to find integers  $x$  and  $y$  such that  $x \cdot 25 + y \cdot 11 = 1$ .

6.  $r$  is an *inverse* of  $m \pmod{N}$  iff  $r \cdot m \equiv 1 \pmod{N}$ .

Show that a number  $m$  cannot have two different inverses  $q$  and  $r \pmod{N}$  that are both in range  $1 \dots N-1$

7. What is the inverse of  $11 \pmod{25}$ ?