MA/CSSE 473 Day 08 Announcements and Summary

Announcements:

1. HW 4 due Thursday night at 11:55PM. HW 5 due Monday, Sept 22 at 11:55 PM.
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!
4. Link to late days balance spreadsheet is near the top of the schedule page.

Main ideas from today (and some review from yesterday):

1. r is an *inverse* of m (mod N) iff r*m ≡ 1 (mod N). If m has an inverse it is unique.
2. We can find the inverse by using the extended Euclidean algorithm. If GCD is not 1, no inverse.
   Show that a number m cannot have two different inverses q and r (mod N) that are both in range 1… N-1.
3. Fermat's Little Theorem: If p is prime, and a is not 0 (mod p), then $a^{p-1} \equiv 1$ (mod p).
4. What does Fermat's Little Theorem say about a^{N-1}(mod N)
   a. if N is prime?

   b. if N is not prime?

5. **Note that the inverse of Fermat's little theorem is not true!**

6. **Prove:** If a is a number that is relatively prime to N such that a^{N-1} is not congruent to 1 mod N, then that same condition must be true for at least half of the numbers in the range 1…N-1.

7. What is a Carmichael number, and why are such numbers troublesome for primality testing?

8. Outline our (Carmichael-free) primality testing algorithm

9. Give a simple and efficient algorithm for finding the t and u such that $N-1 = 2^t u$ (where u is odd) .

10. How does the Miller-Rabin test work?