MA/CSSE 473 Day 07 Announcements and Summary

Announcements:

1. HW 3 Due Tonight (really!) 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!
4. Link to late days balance spreadsheet is near the top of the schedule page.
5. Will I assign a few homework problems for which neither I nor the textbook have told you all that you need to solve them? Of course. This is a 400-level course, and it's partly about being resourceful and clever. The world doesn't only need people who can do only the things they have been explicitly taught! And Rose-Hulman is supposed to produce graduates who are better than that. SE majors have to go out and find and learn software tools that no one ever taught them. CS majors should be able to do the same with Math tools.

Main ideas from today:

1. Use the extended Euclid algorithm to find integers x and y such that x*25 + y*11 = 1.
   (forward + substitution approach)

2. `r` is an *inverse* of `m` (mod `N`) iff `r*m` ≡ 1 (mod `N`).
   Show that a number `m` cannot have two different inverses `q` and `r` (mod `N`) that are both in range 1… `N-1`

3. What is the inverse of 11 (mod 25)?

4. What is 4/11 (mod 25)? (a/b = a*$^{b-1}$)

5. Use the algorithm from the Primailty Testing slide to show that 1953 (my birth year) is divisible by 7.

6. What does Fermat's Little Theorem say about a^{N-1}(mod N)
   a. if N is prime?

   b. if N is not prime?

7. Prove: Let $S = \{1, 2, \ldots, p-1\}$. For all a in S:
Lemma: Multiplying all of the numbers in S by a (mod p) permutes S. I.e. $\{a \cdot n \pmod{p} : n \in S\} = S$

8. Use the lemma to prove Fermat's little theorem.

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

10. **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.