MA/CSSE 473 Day 07

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` $\equiv 1$ (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 Primality 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, …, 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.