MA/CSSE 473 Day 08

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 $a^{p-1} \equiv 1 \pmod{p}$.
4. What does Fermat's Little Theorem say about $a^{N-1} \pmod{N}$
   a. if N is prime?

   b. if N is not prime?

5. **N** 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. $\{a \cdot n \pmod{p} : n \in S\} = S$

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

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

8. **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.

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

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

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

12. How does the Miller-Rabin test work?