MA/CSSE 473 Day 9 Announcements and Summary

Announcements:

1. HW 4 Due Tonight at 11:55PM. HW 5 Monday night.
2. Exam dates: Tuesday Sept 30, Tuesday November 4. In-class. Not in the 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. I'll be in my office hours 6-8 today.
4. Tomorrow we will discuss the Donald Knuth interview.

Main ideas from today:

1. Summary of where we are so far with randomized primality testing (for a large number N):
   a. Fermat's Little Theorem: If p is prime, and a is not 0 (mod p), then $a^{p-1} \equiv 1$ (mod p).
      i. So if we find an **a** in range $1 < a < N$ for which $a^{N-1} \not\equiv 1$ (mod N), the number is not prime.
      ii. But it is possible that N is composite but there is an **a** with $a^{N-1} \equiv 1$ (mod N).
      iii. Such an **a** is called a *Fermat liar*.
   b. If there is at least one **a** that is relatively prime to N, for which $a^{N-1} \not\equiv 1$ (mod N), then that is true for at least half of the possible values of **a**.
   c. So if there is such an **a**, we have a good chance of finding one after a reasonable number of tries.
   d. A Carmichael number is a composite integer for which $a^{N-1} \equiv 1$ (mod N) for all **a** range $1 < a < N$. Example: 561 is the smallest Carmichael number.
2. Miller-Rabin test:
   a. Note that for some **t** and **u** (**u** is odd), $N-1 = 2^t u$. The **t** and **u** are unique.
   b. Consider the sequence a^u (mod N), a^{2u} (mod N), …, $a^{(2\wedge t0u}$ (mod N) $\equiv a^{N-1}$ (mod N)
   c. Suppose that at some point, $a^{(2\wedge i)u} \equiv 1$ (mod N), but $a^{(2\wedge(i-1))u}$ is not congruent to 1 or to N-1 (mod N)
      i. Then $a^{(2\wedge(i-1))u}$ is a non-trivial square root of 1 (mod N), and N cannot be prime (see below)

3. Example: N=561.

4. Important prof in the slides: If there is an s which is neither 1 or -1 (mod N), but $s^2 \equiv 1$ (mod N), then N is not prime

5. Rabin showed that if N is composite, this test will demonstrate its non-primality for at least ¾ of the numbers **a** that are in the range 1…N-1, even if **a** is a Carmichael number.

6. Efficiency of the test (for an individual a and N):

7. To generate a random prime that is less than M, repeatedly randomly choose numbers less than M until we find one that is prime.

8. **RSA cryptography intro.** We focus on how to encode a single integer message m with $0 \leq m < N$.
   e is the encoding key, and d is the decoding key. In *public-key* cryptography, I give you (e, N) so you can send me a message, but I keep d private.
9. Choose two large primes p and q, and let N = pq.
10. Choose e to be a number that is relatively prime to N' = (p-1)(q-1). Then
    a. the mapping $x \rightarrow x^e$ mod N is a bijection on {0, 1, …, N-1}, and
    b. If d is the inverse of e mod (p-1)(q-1), then for all x in {0, 1, …, N-1}, $(x^e)^d \equiv x \pmod{N}$.

11. Example: p=63, q=53 (so N=3233):