MATH 314 - Class Notes

4/25/2017

Scribe: Timothy Quartey

Summary: Today we did a review of Fermat's Primality Test, as well as specifically delving into Miller-Rabin's Test

Notes:

- Miller Rabin primality test is a primality test hence the name. It is an algorithm which determines whether a given number is prime.
- The following steps detail how to computer the Fermat primality test in relatively short order.
- Check if n is prime
- If n is prime, then we compute
- Pick a at random, $1 < a < p - 1$
- We then compute $a^n - 1(mod\ n)$
- If this is 1, then n is "probably prime!"
- If not then n is "composite"
- It is said that Carmichael numbers pass the Fermat Primality test for all numbers that are said to be not found composite.
- The smallest Carmichael number is 561.
- The following steps detail the steps needed to complete the Miller-Rabin Primality Test
- Step 1
- Check to see if n is prime/odd number
- $1 < a < n - 1$ Pick a random number for a
- Step 2
- Write $n - 1 = 2^k m$, where m is odd
- Example
- If n = 13, and a = 2
- $13 - 1 = 12$
- $12 = 2^k m$

- Proceed to break down a to its highest power, which would be 2^2
- $12 = 2^2 * 3$
- $b_0 = 2^3 (mod\ 13)$
- $b_1 = (b_1 \ - 1)^2 = (b_0)^2 = 64 = -1 (mod\ 13)$
- which means 13 is "probably prime".
- Step 3
- $b_0 = + - 1 (mod\ n)$ return "probably prime"
- Step 4
- $for(int\ i = 1;\ i < k - 1;\ i + +)$
- $b_i = (b_i \ - 1)^2 (mod\ n)$
- If $b_i = -1 (mod\ n)$ return "probably prime"
- If $b_i = -1 (mod\ n)$ return "composite"
- Step 5
- IF we never got $+ - 1$
- If $b_k - 1$ *not equal* $+ -1$ return "composite"
- Example 2, suppose $n = 121,\ and\ a = 3$
- $n - 1 = 120 = 2^3 * 15$
- Step 1 compute $3^1 5 mod\ n = 1 (mod 121)$

Nice things:

1. No Carmichael-like numbers for Miller Rabin
2. There exist n, a n composite, but it passes Miller-Rabin base a strong pseudo primes.
3. If n is composite then at least 3/4 of values of a prove n is composite for Miller-Rabin.

Important Tidbits:

1. If you try Miller-Rabin 10 times you probably get prime every time, then the probability that n is composite is at most $(1/4)^1 0 = (1/1,000,000)$
2. It helps if your m is odd. It allows for a seamless transition for the Miller-Rabin test.