# MATH 314 Spring 2019 - Class Notes

04/11/2019

Scribe: Jeremy Keith

**Summary:** In this class we covered two better primality tests than the ones we had previously covered that do not have the problem of Carmichael numbers. The Solovay-Strassen Primality Test and the Miller Rabin Primality Test.

**Notes:**

- We need better primality tests with no Carmichael numbers.
- Solovay-Strassen Primality Test
  - Again more of a compositeness test than a primality test.
  - Either composite or probably prime.
  - Uses Jacobi Symbols
    * If p is prime then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}$ (mod p)
  - Steps of Solovay-Strassen Primality Test
    1. Pick an a, 2$\leq a < p-1$
    2. Compute $\left(\frac{a}{p}\right)$ (Jacobi Symbol)
    3. Compute $a^{(p-1)/2}$ (mod p)
    4. If they are not equal then return composite
    5. Repeat these steps multiple times, if you don't ever get composite the conclusion is probably prime.
  - Solovay-Strassen is better than Fermat
    * If $a^{n-1} \equiv 1$ (mod n) but n is composite, n is a pseudoprime base a.
    * If $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2}$ (mod n) but n is composite , n is a base a euler pseudoprime.
    * There are a lot more Fermat pseudoprimes than Solovay-Strassen pseudoprimes
- Miller Rabin Primality Test
  - Again more of a compositeness test than a primality test.
  - Either composite or probably prime.
  - Take $n-1 = 2^k \cdot m$ where m is odd

– Like Fermat's with extra steps.

– Pick an a, 2$\leq a < n-1$

– We're going to compute $a^{n-1}$ (mod n)

– Steps of Miller Rabin Primality Test

1. Compute $b_0 \equiv a^m$ (mod n)
   * If $b_0 = \pm 1$ (mod n), return probably prime
2. For i in 1 to $(k-1)$
   * Compute $b_i \equiv (b_{i-1})^2$ (mod n)
     · If $b_i = 1$ (mod n), return composite
     · If $b_i = -1$ (mod n), return probably prime
     · If we finish the for loop, $b_{k-1} \neq \pm 1$ (mod n), return composite
3. Repeat for multiple values of a. If you never return composite, the number is probably prime.