week9_lec1

Main Topics

- Primality Testing
  - Randomized Algorithms
  - Fermat's Theorem
  - Miler Rabin Primality Test

Primality Testing

Prime numbers are of great importance especially in key generation during cryptography and RSA.

Users must create a private key made up of two huge prime integers and a public key made up of their product, when using the RSA public-key crypto-system, . To do so, one must be able to quickly determine whether a number is prime.

Randomized Algorithms

- Naive Method would take 2^{125} operations
- Can be optimized using Miler Rabin

Fermat's Theorem

If p is a prime number and 'a' belongs to (1,p-1)
$a^p \equiv a \ mod \ p$
$a^p \ \% \ p = a$

Dividing LHS and RHS with 'a'
$a^{p-1} \ \% \ p = 1$

> Some composite numbers might even satisfy this criteria. Thos numbers are called pseudo-primes or Miler-Rabin Pseudo Primes.

Miller-Rabin Randomized Test

Algorithm Working

- If number is even, then return except when it is 2, since 2 is the only even prime number
- n is prime iff solutions of x^2 = 1 (mod n) are x = (+-) (1).
  - Continue halving the exponent as long as it is possible until we reach a value other than 1. anything else ⇒ it is composite.
  - so given n, we need to find s such that : $n - 1 = 2^s q$,
  where 2^s = largest power of 2 dividing n-1
  q is any odd number
  - We get a sequence a^{n-1} which is as follows:
  $a^{n-1} = a^{2^s q}, a^{2^{s-1} q}, ..., a^q$

  a is a random integer between 0 and n - 1.
  - The number n is prime if:
    - the sequence starts with 1 and all following members are 1
    - if the sequence doesn't isn't all 1 then the first non one member should be -1

Code

```
Loop: for each i (repeat k times):
        pick a random integer a in the range [1, n − 1]
        compute x = a_i ^ (2^s q)
        if x != 1 reject
        compute a^{2^s q}, a^{2^{s-1} q},...,a^q
            if some element isn't all 1 then the first non one member should be -1
            if all passed => return “probably prime”
```

A composite number is 1/4 times likely to pass the above algorithm. Due to comparatively low error, it is widely used nowadays.