Review - Number Theory

- Modular arithmetic
  - Notation x in Z_i
- Greatest common divisor
  - if gcd(x,y) = 1 we say that x and y are relatively prime
- Modular Inversion
  - The inverse of x in Z_n is an element y in Z_n
  - s.t.
    - x * y = 1 in Z_n
  - x in Z_n has an inverse iff gcd(x,n) = 1
- More notation
  - Z_n* = the set of invertible elements in Z_n
- Solving modular linear equations
  - a*x + b = 0 in Z_n
  - x = -b * a^-1 in Z_n
  - Find a^-1 in Z_n using extended Euclid
- Fermat's theorem
  - Let p be a prime for all x element (Z_p)*: x^p-1 = 1in Z_p
- Generating random primes
  - step1: choose a random integer p element {2 ^ 1024, 2 ^ 1025 - 1}
  - step2: test if 2 ^ p - 1 in Z_p
    - if so, output p and stop. If not, goto step 1
- Structure
  - (Z_p)* is a cyclic group, that is there is a g element (Z_p)* such that {1, g, g^2, ..} = (Z_p)* g is called a generator of (Z_p)*
    - Note: note every element is a generator
- Order
  - For g element (Z_p)* the set {1, g, ..} is called the group generate by g, denoted <g>
  - Def: the order of g element (Z_p)* is the size of <g>
    - ord_p(g) = l<g>l
- Euler's generalization of Fermat
  - Def: For an integer N define sigma(N) = l(Z_n)*l
  - Thm (Euler): For all x element (Z_n)*: x ^ sigma(N) = 1 in Z_n
- Modular e'th roots
  - Let p be a prime and c element of Z_p
  - Def: x element of Z_p s.t.
    - x^e = c in Z_p is called an e'ht root of c
- Euler's theorem
- Computing square roots mod p
- Solving quadratic equations mod p
- Repeated squaring algorithm
- DLOG