Lecture 1:
Course Introduction

Lecture 5:
Primality and factoring

Primes

Theorem

The function $\pi(X)$ counts the number of primes less than X, where we have the approximation

$$\pi(X) \approx \frac{X}{\log X}$$

- Trial Division
- FermatŠs Test
- Miller-Rabin Test

Factoring Algorithms

- Trial division
- $p-1$ method
- $p+1$ method
- Pollard rho method
- Modern methods: Quadratic Sieve (QS), Elliptic Curve Method (ECM), Number Field Sieve (NFS).

Modern methods: complexity

- Modern factoring algorithms lie somewhere between polynomial and exponential time, in an area called sub-exponential time. These algorithms have complexity measured by the function

$$L_N(\alpha, \beta)e(\beta + o(1))(\log N)^{\alpha}(\log \log N)^{(1-\alpha)}).$$

- Trial division, has complexity $L_N(1, 1/2)$.
- Quadratic Sieve has complexity $L_N(1/2, c)$.
- The current fastest algorithm is the Number Field Sieve which has complexity $L_N(1/3, c)$.

- Methods known for solving the discrete logarithm problem,

$$h = g^x$$

  in various groups G.
- Two categories, either the algorithms are generic and apply to any finite abelian group or the algorithms are specific to the special group under consideration.

Pohlig-Hellman

- Pohlig-Hellman observation: the discrete logarithm problem in a group G is only as hard as the discrete logarithm problem in the largest subgroup of prime order in G.