CS 812
Spring 2024
Topics List

Topics for lectures will be chosen from the list below. Exact coverage will reflect student interest and/or resistance.

1. **Computations in Elementary Number Theory.** (3 weeks)
   - Computation models, cost of arithmetic
   - Euclid's algorithm, inverses mod n
   - Exponentiation
   - Chinese remainder theorem, residue arithmetic
   - Linear equations and linear systems
   - Generators, power residues, residue symbols
   - Solving equations in finite fields
2. **Primes.** (2 weeks)
   - Prime number theorem, density results
   - Pratt's certificates
   - Randomized tests
   - Algorithmic applications of the ERH
   - AKS test
3. **Factorization.** (2 weeks)
   - Motivation: RSA and digital signatures
   - Reductions to factoring
   - Smooth numbers, random splitting model, factored random numbers
   - Exponential algorithms (Pollard rho etc.)
   - Quadratic sieve
   - Number field sieve
4. **Discrete Logarithms.** (2 weeks)
   - Motivation: Diffie-Hellman key exchange
   - Square-root algorithms: Shanks, Pollard, etc.
   - Lower bounds for generic algorithms
   - Index calculus methods
5. **Pseudo-Random Numbers.** (2 weeks)
   - Classic methods: iterated affine maps, shift registers
   - Boyar's algorithm (prediction of Lehmer sequences)
   - Berlekamp-Massey algorithm (prediction of shift register sequences)
   - Lattice reduction and applications
   - "Unpredictable" generators
6. **Geometry-Based Algorithms.** (3 weeks)
   - Projective space and secret sharing
   - Algebraic curves
   - Elliptic curve cryptography
   - Factoring using elliptic curves
   - Limited-randomness algorithms
   - Analysis of iterated quadratic maps