End-of-Term Topic Lists

Math 25, Fall 2006

What follows is a list of topics that may be covered in the final exam. This is not an exhaustive list by any means, but aims to emphasize the important concepts covered during the term and to point out particular topics that will be excluded from the exam. In what follows below, you should assume that any topic not specifically excluded is fair game.

List of Topics

- Chapter 1
  - Fibonacci numbers: definition, relations
  - Mathematical induction: both types
- Chapter 3
  - Prime numbers: definition, infinitude, distribution
  - Classical theorems/conjectures: Prime number theorem, Goldbach conjecture, Twin prime conjecture, Bertrand's conjecture, etc.
  - Greatest common divisor (by definition and as a linear combination), least common multiple
  - Division algorithm, Euclidean algorithm
  - Fermat numbers, Fermat factorization
- Chapter 4
  - Definition of congruences, existence of solutions to linear congruences
  - Chinese Remainder Theorem
  - Polynomial congruences, Hensel's lemma
  - Systems of congruences: matrices, determinants (with respect to Hill Cipher only)
- Chapter 5
  - Divisibility tests
  - Julian and Gregorian calendars
  - Computing day of week with congruences
  - Check digit schemes
- Chapter 6
  - Wilson's theorem

  - Fermat's little theorem
  - Pseudoprimes, Carmichael numbers, strong pseudoprimes
  - Primality tests: Trial Division, Pollard $p-1$ Factorization, Miller's Test, Rabin's Test, Lucas-Lehmer
  - Euler's Theorem

- Chapter 7
  - Arithmetic functions: φ, σ, τ
  - Properties and formulae for arithmetic functions
  - Summatory functions
  - Perfect/abundant/deficient numbers, Mersenne numbers

- Chapter 8
  - Ciphers: Shift, Affine, Vigenère, Vernam, Hill, Exponentiation
  - Public key encryption, RSA, signatures
  - Knapsack problem: super-increasing sequences, knapsack cipher

- Chapter 11
  - Quadratic residues: Legendre symbol, formulae for -1 and 2, quadratic reciprocity
  - Pepin's Test, Jacobi Symbol*
  - Euler Pseudoprimes*

- Other Topics
  - ord, ind, basic properties [§9.1]
  - primitive root (definition only) [§9.1]
  - Diophantine equations* [§§3.7, 13.1]
  - Fermat's last theorem* [§13.2]

* You are only responsible for portions of these topics covered in class.

List of Non-Topics

- Möbius μ-function, Möbius inversion [§7.4]
- Big-O notation [§2.3]
- AKS algorithm
- Farey Series
- DEA, AES [pp. 296-297]
- Rabin cryptosystem [pp. 314-315]
- "Flipping Coins Electronically" [pp. 411-412]
- Algorithm for computing Jacobi symbols [pp. 434-436]
- "The Proof for $n = 4$" [pp. 520-522]