Math 487, Final Exam Study Guide

General information

(1) The exam will be cumulative. Books, calculators, and notes will not be allowed.
(2) WARNING: this study guide is not meant to be exhaustive. Just because something is not on the study guide does not mean it will not be on the exam.

Basics

(1) Concepts from the first and second midterm exams: rings, groups, fields, integral domains, divisibility, prime, gcd, division algorithm, Euclidean algorithm, LCM, fundamental theorem of arithmetic, congruences, $\mathbb{Z}_n$, Euler φ-function, units, Fermat's little theorem, order of elements, primitive roots, Chinese remainder theorem, quadratic residues, Legendre and Jacobi symbols, quadratic reciprocity, $\zeta(s)$, Fermat and Mersenne numbers, perfect numbers, Fibonacci numbers, golden section, quadratic forms, Pythagorean triples, Dirichlet characters, Dirichlet L-series, $\mu(n)$, $\Lambda(n)$, twin primes, $\tau(n)$, $\sigma_k(n)$, multiplicative functions, binomial coefficients, big O and little o notation, $\pi(x)$
(2) Definitions:
   - Pseudoprime, Euler pseudoprime, strong pseudoprime
   - Carmichael numbers
   - Plaintext, ciphertext
   - Shift, affine, substitution ciphers
   - Vigenére code
   - Public key cryptography
   - Elliptic curve

Theorems you should know and be able to use

- Division algorithm, Euclidean algorithm, fundamental theorem of arithmetic
- Wilson's theorem
- Euler's theorem (Theorem 2.4.4.3)
- Chinese remainder theorem
- Theorems 2.5.2.1 and 2.5.2.2
- Properties of Legendre and Jacobi symbols, quadratic reciprocity
- There are infinitely many primes.
- Euler product expansion of zeta function
- Continued fraction expansion of real numbers
- Binet's formula for Fibonacci numbers
- Dirichlet's theorem on primes in arithmetic progressions
- Fermat's two-square theorem, Lagrange's four-square theorem
- Properties of Dirichlet characters: Theorem 3.3.1, Lemma 3.3.1, Lemma 3.3.3, Lemma 3.3.4, Corollary 3.3.1, Theorem 3.3.2
- Euler product representation of L-series
- Theorem 3.6.1, Theorem 3.6.3
- Möbius inversion formula
- Prime number theorem, Chebychev's estimate
- Theorem 4.1.2
- Binomial theorem
- Combinatorial proofs for binomial coefficients and Fibonacci numbers
- Legendre's formula for the sieve of Eratosthenes
- Fermat probable prime test
- Lucas' extension of Fermat's theorem
- Idea of AKS algorithm
- Korselt criterion
- Solovay-Strassen primality test
- Miller-Rabin primality test
- Lucas-Lehmer test
- RSA cryptosystem
- Formulas for adding points on an elliptic curve
- Pollard's $p-1$ method of factorization
- Elliptic curve factorization
- Diffie-Hellman key exchange (standard and elliptic curve)
- ElGamal cryptosystem on elliptic curves