MA 335, Spring 2014

List of Topics for the Final Exam

Final will be, with one exception, Closed book: no textbook, no notes, no cooperation. Electronic means of communication (cell phones, smartphones, tablet pc, laptops, etc) will be forbidden. The exception is as follows: you are **allowed to bring** and use during entire exam **one sheet** of A4/lettersize paper filled on one side with your handwriting (contingent on the handwriting not being too small in my personal view).

For the final, you need to know notions, methods, statements and their proofs in the list below. In particular, you need to able to reproduce (of course, not necessarily word by word, but correctly) definitions, statements and proofs; know basic examples of definitions and theorems; be able to apply theorems, ideas in their proofs, and methods in the list below to solve problems.

There may be changes to this list, but no later than April 29.

(1) *Preliminaries.*
- Mathematical induction.
- Binomial coefficients, Pascal's triangle.

(2) *Early number theory.*
- Polygonal numbers (triangular, oblong, square): definition, basic properties, simple "picture proofs".
- Theorem about a sum of values of a polynomial at integer points $0, 1, 2, \ldots, n$.
- Method of finite differences for finding a sum of values of a polynomial at points $0, 1, 2, \ldots, n$. Connection to Pascal's triangle.
- Method of indeterminate coefficients for finding a sum of values of a polynomial at points $0, 1, 2, \ldots, n$.

(3) *Divisibility of integers: basic facts.*
- Division algorithm.
- Base b place-value (positional) number notation system. Converting to and from arbitrary base. Multiplication table, long addition and long multiplication in arbitrary base.
- Definition and basic properties of divisibility.
- Greatest common divisor: definition, basic properties, Bezout's theorem (linear expression of gcd), Euclid's lemma.

(4) *Primes.*
- Definition of prime and composite numbers.
- Fundamental theorem of arithmetic (Unique prime factorization for integers).
- Canonical (prime power) form of integers, deciding divisibility and finding gcd and lcm using canonical form.
- Infinitude of primes: Euclid's proof, Euler's proof. Infinitude of primes of the form $4k + 3$.
- Sieve or Eratosthenes.

(5) *Linear Diophantine equations.*
- Finding gcd via Euclidean algorithm.
- Finding linear expression of gcd via reverse Euclidean algorithm.
- Notion of a Diophantine equation.

- Solving linear Diophantine equation in two variables.

(6) *Congruences.*
- Definition of congruence modulo n. Basic properties of congruence.
- Canceling out a factor in a congruence. Coprime and not coprime cases.
- Tests for divisibility by 2, 3, 5, 9, 10, 11.
- Tests for divisibility by 7, 11, 13.
- Solving a single linear congruence. Number of solutions of a single linear congruence.
- Chinese remainder theorem, relation to solving multiple linear congruences with coprime bases.

(7) *Fermat's theorem and related questions.*
- Fermat's little theorem.
- Converse statement to Fermat's theorem: notion of an absolute pseudoprime, existence of (at least one) absolute pseudoprime.
- Wilson's theorem.

(8) *Number-theoretic functions.*
- Notion of a number-theoretic function. Number of divisors τ and sum of divisors σ. Formula for τ and σ using canonical form of an integer.
- Multiplicative number-theoretic functions. Examples. Multiplicativity of τ and σ.
- Multiplicativity of sum of values of a multiplicative function f at divisors of n.
- Representing τ, σ as a sum. Multiplicativity of τ, σ via this representation. Formula for τ and σ via multiplicativity.

(9) *Möbius function and inversion formula.*
- Möbius function μ: definition, multiplicativity. Main property: sum of values of μ at divisors of n.
- Möbius inversion formula. Multiplicativity of f given multiplicativity of $F(n) = \sum_{d|n} f(d)$.

(10) *Euler's function. Euler's theorem.*
- Euler's function φ: definition, two proofs of multiplicativity.
- Expression of $\varphi(n)$ through prime decomposition of n. Expression of φ through Möbius function.
- Euler's theorem.

(11) *Primitive roots.*
- Order of a number modulo n. Order of a power and other properties of order.
- Primitive roots: definition, basic properties. Existence and quantity of primitive roots of a prime p.
- Primitive roots of p^k. Lifting primitive roots of p to primitive roots of p^k, $2p^k$.
- Criterion for $n \in \mathbb{N}$ to have a primitive root.
- Using primitive roots to solve congruences of the form $ax^k \equiv b \pmod{n}$ when $\gcd(a, n) = \gcd(b, n) = 1$, given a primitive root of n.

(12) *Quadratic congruences modulo prime p.*
- Reduction of a quadratic congruence mod odd prime p to a congruence of the form $x^2 \equiv a \pmod{p}$.

- Quadratic residues and nonresidues, Euler's criterion.
- Legendre symbol, basic properties of Legendre symbol. Finding $\left(\frac{-1}{p}\right)$. Infinitely many primes of the form $4k+1$.
- Reduction of computing $\left(\frac{n}{p}\right)$ to prime numerators $\left(\frac{q}{p}\right)$.
- Gauss's Lemma. Finding $\left(\frac{2}{p}\right)$.
- Reformulation of Gauss's Lemma using the integer part function (a.k.a. the greatest integer function, or the floor function).
- Quadratic Reciprocity Law. Using quadratic reciprocity law to compute arbitrary $\left(\frac{n}{p}\right)$ assuming availability of prime decompositions.

(13) *Quadratic congruences modulo composite n.*

- Lifting solutions of $x^2 \equiv a \pmod{p^k}$ to solutions of $x^2 \equiv a \pmod{p^{k+1}}$.
- Solving a congruence $x^2 \equiv a \pmod{2^k}$ for odd a and $k \geq 1$.
- Solving a congruence $x^2 \equiv a \pmod{n}$ for arbitrary $n > 1$ and $\gcd(a, n) = 1$. Number of solutions.
- Blum's remote coin flipping protocol, connection to the prime factorization problem.

(14) *Continued fractions.*

- Continued fractions: definition of infinite and finite continued fractions, simple fractions, periodic fractions. Convergents C_k of a continued fraction.
- Numerators p_k and denominators q_k of convergents, recursive formulas for p_k, q_k. Main technical lemma connecting $p_k, p_{k-1}, q_k, q_{k-1}$.
- Existence of value (limit of convergents) of an infinite continued fraction.
- A number is rational iff it is a value of a finite simple continued fraction.
- A number is irrational iff it is a value of an infinite continued fraction. Representing a given irrational number by an infinite continued fraction. Uniqueness of infinite continued fraction with a given value.
- Periodic infinite continued fractions represent quadratic irrationalities.
- Quadratic irrationalities are represented by infinite periodic continued fractions (no proof required).
- Convergents as approximations of value of a continued fraction. "Quadratic" error of approximation by convergents.
- Convergents as best rational approximations of a given irrational number (no proof required).

(15) *Application of number theory to cryptography.*

- Diffie–Hellman key exchange protocol, connection to the discrete log problem.
- RSA (Rivest–Shamir–Adleman) public key cryptosystem, connection to the prime factorization problem.