TOPICS FOR FINAL EXAM, MATH 55 SPRING 2016

You must know all definitions and proofs presented in class, as well as proofs that I told you to read in the book. You must write all answers in complete English sentences.

Chapter 1. Main topics:

- Propositional logic
- Propositional equivalences
- Predicates and quantifiers
- Nested quantifiers and negation of quantifiers
- Rules of inference (dont need to memorize names)
- Basic proof techniques: direct, contrapositive, contradiction, cases.

Types of problems

- Write truth tables for propositions
- Determine when two propositions are equivalent
- Determine when proposition is a tautology
- Turn English statements into propositions and vice-versa
- Determine truth values of propositional functions
- Use rules of inference to build valid arguments
- To identify logical fallacies in arguments

Chapter 2. Main topics:

- Elements, sets, subsets; know difference between elements and sets
- Set operations (power set, Cartesian product, union, difference, complement)
- Functions (injective, surjective, bijective; inverses and compositions)
- Cardinality, countable and uncountable sets

Types of problems:

- Prove set identities
- Determine (with proof) whether a function is injective, surjective, bijective
- Determine (with proof) whether a set is countable or uncountable

Chapter 4. Main topics:

- Basic properties of divisibility, primes and composites
- Existence of infinitely many primes
- The Well-Ordering Principle
- Division algorithm
- Euclidean algorithm and GCD
- Bezout's theorem and strong version
- Euclid's lemma
- Fundamental theorem of arithmetic
- Basic properties of arithmetic modulo m
- Existence of inverses when a, m are relatively prime
- Fermat's little theorem
- Chinese remainder theorem
- RSA (proof that decryption undoes encryption)

Types of problems:

- Prove simple statements about divisibility
- Prove more sophisticated statements, possibly using the named theorems listed above
- Convert numbers into binary and back again

- Use the Euclidean algorithm to find the gcd and Bezout coefficients $sa + tb = 1$
- Find the inverse of a mod m
- Solve systems of linear congruences using the Chinese Remainder Theorem
- Use Fermats Little Theorem to compute large powers modulo m
- Use repeated squaring to compute large powers modulo m
- Encrypt and decrypt messages using RSA

Chapter 5. Main topics:

- Induction (key examples: proofs of inequalities and identities, divisibility, statements about sequences defined recursively, statements about unions and intersections of n sets).
- Strong induction (key examples: tiling with dominos, making monetary amounts, outcomes of games such as the one we played in class, induction with graphs)
- Well-ordering principle (and why it implies that induction works)
- Recursive definitions (key examples: Fibonacci, Euclidean Algorithm)

Types of problems:

- Proofs using induction and its variants, including proofs of statements about topics in other chapters.

Chapter 6. Main topics

- Cardinality, product and sum rules
- Bijections, many to one maps, division rule
- Permutations and combinations, with and without repetitions (stars and bars)
- Combinatorial proofs
- Pigeonhole Principle (including Generalized Pigeonhole Principle, and more sophisticated applications such as: must have 3 friends or 3 strangers in a group of 6).
- Binomial coefficients, Binomial Theorem, Pascals identity

Types of problems

- Basic counting using product and sum rule (by defining a process for constructing the objects you want to count)
- Proofs using the pigeonhole principle
- Counting permutations and combinations with and without repeated objects
- Distributing indistinguishable objects into distinguishable boxes.
- Proofs involving binomial coefficients, including combinatorial proofs (i.e., counting the same thing in two different ways)

Chapter 7. Main topics

- Probability (experiment, sample space, event, outcome, probability distribution)
- Conditional probability, independent events, law of total probability (key examples: Monty Hall)
- Bayes Theorem
- Coin flips (Bernoulli Trials), the binomial distribution, the geometric distribution
- Random variables, expected value, linearity of expectation
- Independent random variables
- Variance and Chebyshev's inequality
- Inclusion-Exclusion for probabilities of unions of events (see chapter 8)

Types of problems

- Be able to clearly specify the experiment, sample space, probabilities, and events given a word problem
- Compute probabilities and conditional probabilities using basic definitions and counting (e.g. for poker hands or coin flips)
- Compute probabilities using the law of total probabiity and Bayes' theorem.
- Determine whether events and random variables are independent
- Compute the expectation and variance of random variables
- Apply linearity of expectation
- Apply Chebyshev's inequality

- Proofs of basic properties of expected value and variance, including Bienayme's theorem.

Chapter 8. Main topics:

- Recurrence relations
- Generating functions and formal power series (key example: Fibonacci)
- Inclusion-exclusion, its proof and applications (key examples: derangements, counting onto functions)

Types of problems:

- Find the recurrence to describe a word problem (such as Towers of Hanoi or a counting problem).
- Find the closed form of the generating function of a sequence satisfying a recurrence
- Going from a generating function to an explicit formula for a sequence (using partial fractions)
- Be able to multiply, add, and divide generating functions (Theorem 1 from 8.4).
- Recognize basic generating functions (e.g. $\frac{1}{1-x}$ and $\frac{1}{1-x^2}$)
- Find a (polynomial) generating function which solves a fixed, finite counting problem (such as giving bars of chocolate to three kids)
- Applications of inclusion-exclusion

Chapter 9. Main topics:

- Relations (including notions of reflexive, symmetric, antisymmetric, transitive)
- Representing relations by matrices and diagrams (informal, for intuition)
- Equivalence relations; equivalence classes
- If R is an equivalence relation on a set S, its equivalence classes partition S
- Modular arithmetic as arithmetic on congruence classes modulo m.

Types of problems:

- Recognize and prove when a relation has certain properties
- Determine (with proof) whether a relation is an equivalence relation
- Identify equivalence classes of relations; and determine how many there are

Chapter 10. Main topics

- Basic definitions: edge, vertex, (simple) graph, multigraph, adjacent, incident, endpoint, neighborhood, degree, path, circuit, simple path/circuit, Euler circuit, bipartite, connected, subgraph, union, connected component, coloring, chromatic number, cut edge, cut vertex
- Special types of graphs (complete, bipartite, cycle, etc)
- Connected components as equivalence classes of an equivalence relation
- Handshaking theorem
- Bipartite iff no odd circuit
- Chromatic number at most one plus maximum degree
- Euler circuit iff connected and even degrees

Types of problems:

- Determine whether a given graph is bipartite, has an Euler circuit, is connected; find a coloring of a given graph or show that none exists
- Draw a particular graph.
- Determine whether a degree sequence can be realized by a simple graph
- Proofs relating notions such as degree, partitions, connectivity, bipartiteness, chromatic number, and Euler circuits, possibly requiring application of the above theorems
- Proofs using induction (where $P(n)$ will depend on either the number of vertices or the number of edges, and a smaller graph is obtained by deleting an edge or vertex)

Directed graphs and graphs with loops are not covered in this course.