Midterm 1 Detailed Topic List

* This topic list is based on the list from the Math 55, Spring 2016 offering

Important You must know all definitions and proofs of theorems presented in **lecture**. Rather than memorizing the proof, understanding the main idea is more helpful. None of the challenge problems from the worksheet/homework will be on the midterm. There will be no questions on tiling checkerboards and you will not be asked to prove Wilson's theorem.

Chapter outline (all the page numbers and sections refer to the 7-th edition)

Chapter 1

Sections covered 1.1, 1.2 (skip Logic Circuits), 1.3 (skip Propositional satisfiability), 1.4 – 1.8

Main topics:

- Propositional logic
- Propositional equivalences
- Predicates and quantifiers
- Nested quantifiers and negation of quantifiers
- Rules of inference (don't need to memorize terms)
- Basic proof techniques: direct, contrapositive, contradiction, cases

You should be to write truth tables for propositions, determine when two propositions are equivalent, turn English statements into propositions and vice-versa, determine truth values of propositional functions, use rules of inference to build valid arguments and identify logical fallacies in arguments.

Chapter 2

Sections covered 2.1 – 2.4, 2.5 (up to the end of Theorem 1 on page 174)

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

You should be able to prove set identities, determine (with proof) whether a function is injective, surjective, bijective and determine (with proof) whether a set is countable or uncountable.

Chapter 4

Sections covered 4.1 (skip Arithmetic modulo m), 4.2 (up to the end of page 249), $4.3 - 4.4$

* To ease the workload, Monday's lecture will **not** be on the midterm, but it might be back for the final exam.

Main topics:

- Basic properties of divisibility, primes and composites
- Existence of infinitely many primes
- Converting between bases
- Division algorithm
- Euclidean algorithm and GCD
- Bezout's theorem
- Fundamental theorem of arithmetic
- Existence of inverses when a, m are relatively prime
- Fermat's little theorem
- Chinese remainder theorem
- Statement of Wilson's theorem

You should be able to prove simple statements about divisibility, sometimes 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 and use Fermat's Little Theorem to compute large powers modulo m.