DISCRETE MATH (MATH 2001)

SUMMARY OF TOPICS FROM 3/9/09-4/29/09

I. Modular arithmetic [arithmetic of $\mathbb{Z}_n$] (Chapter 2)
   (a) Congruence modulo n is an equivalence relation.
   (b) Construction of $\langle \mathbb{Z}_n; \cdot, + \rangle$.
   (c) Laws of arithmetic ($\mathbb{Z}_n$ satisfies all equational laws true in $\mathbb{Z}$, like commutativity and associativity of $+$ and $\cdot$, etc.)
   (d) Units and zero divisors in $\mathbb{Z}_n$. (Every element of $\mathbb{Z}_n$ is a unit or a zero divisor, but not both. There are $\phi(n)$ units in $\mathbb{Z}_n$.)
   (e) How to determine if $[a]$ divides $[b]$ in $\mathbb{Z}_n$. How to determine all solutions of $ax = b \pmod{n}$. How to find the inverse of a unit.
   (f) Fermat's Little Theorem. (If p is prime, then $a^p \equiv a \pmod{p}$ for any a.)
   (g) Chinese Remainder Theorem. Method for solving simultaneous linear congruences in one variable.

II. Counting methods (Section 3.3 and class notes)
   (a) Inclusion/Exclusion
      (i) Formula $|\bigcup A_i| = \sum |A_i| - \sum |A_i \cap A_j| + \sum |A_i \cap A_j \cap A_k| - \cdots$.
      (ii) Formula $N_=(S) = \sum_{S \subseteq T \subseteq P} (-1)^{|T|-|S|} N_\geq(T)$.
      (iii) Derangements. Probability that a permutation is a derangement is $\approx 1/e$.
      (iv) Formula $\phi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})$ for Euler's totient function.
      (v) Number of functions from an n-elements set to an m-element set, number of onto functions, number of 1-1 functions, number of bijections.
   (b) Number of ways to distribute k balls to n distinct boxes where balls may or may not be distinct, boxes may be required to get at least one ball or at most one ball. Number of k-element multisets chosen from an n-element set.
   (c) Discrete probability
      (i) Sample space.
      (ii) Discrete probability distribution.
      (iii) Probability of an event.
      (iv) Uniform distribution.
      (v) Probability of dealing certain card hands or rolling certain dice combinations.

III. Logic (Chapters 5 & 6, class notes)
   (a) Formulas
      (i) Alphabet of symbols: variables, equality, connectives, quantifiers, predicate symbols, punctuation symbols.
      (ii) Terms, atomic formulas, formulas and sentences.
      (iii) Formula trees, term trees.
   (b) Propositional logic
      (i) Truth tables.
      (ii) Tautologies, contradictions, logical equivalence.
      (iii) Contrapositive and converse.

(iv) Equivalence of $(H \to C)$, $((\neg C) \to (\neg H))$, and $((H \wedge (\neg C)) \to \text{False})$. Methods of proof.
(v) Disjunctive normal form.

(c) Structures (definition and examples).
(d) Truth of a sentence in a structure.
  (i) Converting a sentence to prenex form (including: scope of a quantifier, free and bound variables, rules for changing the order of quantifiers and connectives).
  (ii) Quantifier games to determine the truth of a sentence in prenex form in a given structure.
(e) Proof (definition, axioms, laws of deduction).
(f) The Completeness Theorem (statement only).

General advice on preparing for a math test.
Be prepared to demonstrate understanding in the following ways.

(i) Know the definitions of new concepts, and the meanings of the definitions.
(ii) Know the statements and meanings of the major theorems.
(iii) Know examples/counterexamples. (The purpose of an example is to illustrate the extent of a definition or theorem. The purpose of a counterexample is to indicate the limits of a definition or theorem.)
(iv) Know how to perform the different kinds of calculations discussed in class.
(v) Be prepared to prove elementary statements. (Understanding the proofs done in class is the best preparation for this.)

Sample Problems.

(1) Show that $[a] \in \mathbb{Z}_n$ is a unit iff $[a]^k = [1]$ for some k.
(2) Find all solutions to $45x \equiv 80 \pmod{100}$.
(3) Is there a natural number n such that $p = 1/12$ is the probability that a randomly chosen natural number $k \leq n$ is relatively prime to n?
(4) What is the probability that a 3-element multiset of elements from $\{1, 2, 3, 4, 5\}$ has no repeated elements? (Express your answer as a reduced fraction.)
(5) A theorem with two hypotheses has the form $((H_1 \wedge H_2) \to C)$. Which if the following would be a valid form of proof?
  (i) $(H_1 \wedge (\neg C)) \to (\neg H_2)$?
  (ii) $((\neg C) \to ((\neg H_1) \wedge (\neg H_2)))$?
  (iii) $(H_1 \to (H_2 \to C))$?
(6) Write a formal sentence expressing the axiom of union. Then draw a formula tree for your sentence.
(7) Describe a winning strategy for either $\exists$ or $\forall$, which determines the truth of

$$\forall x\, \forall y\, \exists z\, ((x < y) \to ((x < z) \wedge (z < y)))$$

in (i) $\langle \mathbb{R}; < \rangle$, (ii) $\langle Z; < \rangle$.