DISCRETE MATH (MATH 2100)
HANDOUT 3 (October 27, 2008)

SUMMARY OF TOPICS FROM 9/29/08-10/31/08

I. Relations (Section 3.1)
- (i) Equivalence relations.
  - (a) Definition and examples.
  - (b) Partitions.
  - (c) Kernels of functions.
  - (d) Bell numbers.
- (ii) Applications of equivalence relations.
  - (a) Construction of $\langle \mathbb{Z}; \cdot, + \rangle$.
  - (b) Construction of $\langle \mathbb{Q}; \cdot, + \rangle$.
- (ii) Order relations.
  - (a) Definition and examples.
  - (b) Linear orders, Law of Trichotomy.
  - (c) Well orders.
  - (d) Lattices.

II. Arithmetic of $\mathbb{Z}$ related to divisibility (Chapter 2)
- (i) GCD
  - (a) Definition.
  - (b) Well ordering principle.
  - (c) Division algorithm.
  - (d) Euclidean algorithm.
  - (e) $\gcd(m, n)$ is an integral combination of m and n.
  - (f) LCM.
- (ii) Factorization of integers.
  - (a) Euclid's Lemma.
  - (b) Fundamental Theorem of Arithmetic.
  - (c) gcd and lcm via prime factorization.
  - (c) Mersenne primes.

III. Modular arithmetic (Chapter 2)
- (i) $\mathbb{Z}_n$.
  - (a) Congruence modulo n is an equivalence relation.
  - (b) Construction of $\langle \mathbb{Z}_n; \cdot, + \rangle$.
  - (c) Laws of arithmetic.
  - (d) Units and zero divisors.

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.)
(vi) Know how to correct mistakes made on old HW.

Sample Problems.

(1) What is the *kernel* of a function?

(2) Under what circumstances can an equivalence relation be a partition?

(3) Define $L(n)$ to be the number of linear orderings of the set $\{1, \ldots, n\}$.
   (i) Use counting arguments to show that $L(0) = L(1) = 1$ and
$$L(n+1) = \sum_{k=0}^{n} \binom{n}{k} L(k)L(n-k).$$
   (ii) Use (i) to provide another proof that $L(n) = n!$.
   (iii) Use (i) and (ii) to provide another proof that the Bell numbers are dominated by the factorials (i.e., $B_n \leq n!$.)

(4) Is the Well Ordering Principle a definition, an axiom, a theorem, a philosophy, or a constitutional amendment? Justify your answer!

(5) (i) Use the Euclidean Algorithm to compute $\gcd(132, 150)$ and $\mathrm{lcm}(132, 150)$.
   (ii) Find a and b so that $150a + 132b = \gcd(132, 150)$.

(6) State the Fundamental Theorem of Arithmetic.

(7) Find the units in $\mathbb{Z}_{36}$. For each unit, what is its inverse?