Review Sheet for the Final Exam of MATH 1600 - Fall 2009

1. Sets and Proofs

All of Chapter 1.

Concepts.

- Elements and subsets of a set.
- The notion of implication and the way you can use it to build a proof.
- Logical reasoning in ordinary language.
- Universal and existential quantifiers.
- The negation of a logical statement.
- Proof by contradiction.
- Truth tables.

Foundational Results.

- Know the truth tables of the basic logical connectives $\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg$
- Use truth tables to determine whether two logical statements are equivalent, and whether a logical statement is a tautology or a contradiction.
- Know how to form the negation of a statement.
- Know how to prove an existential statement and a universal statement (and any combinations).

Typical Problems. Those from the assignments, but if you like to try something new, here are a couple more:

(1) Which of the following sets are subsets of each other:

$$\begin{aligned} U &= \{u \in \mathbb{Z} |\, u^3 \leq 8\}, \\ X &= \{x \in \mathbb{Z} |\, x^2 < 5\}, \\ Y &= \{y \in \mathbb{R} | |y| < 4\}, \\ Z &= \{z \in \mathbb{R} |\, z^2 = 1\}. \end{aligned}$$

Determine for each pair whether or not they are subsets.

(2) Give a careful proof of the fact that if n is an integer such that n^2 is a multiple of 5, then n is a multiple of 5.

(3) For the following statement, form its negation, and either prove that the statement is true or prove that its negation is true: $\exists x \in \mathbb{Z}$ such that $\forall n \in \mathbb{Z}, x \neq n^2 + 2$.

(4) We have been given a new logical connective $\square$ with the following truth table

p	q	$p \square q$
T	T	F
T	F	T
F	T	T
F	F	F

Give an expression for $p \square q$ in terms of existing logical connectives. Show that your new expression is logically equivalent to $p \square q$.

(5) A very special island is inhabited only by knights and knaves. Knights always tell the truth, and knaves always lie. You meet two inhabitants: Abe and Homer. Abe tells you that Homer is a knave. Homer says, 'Abe could say that I am a knave.'

So who is a knight and who is a knave? Give a logical argument or a deduction using truth tables.

2. Complex Numbers

Chapter 6, and the first half of Chapter 7 (but I won't ask you to solve a cubic equation). Concepts.

- complex numbers
- real parts and imaginary parts
- the complex conjugate
- modulus and argument of a complex number
- The geometric representation of complex numbers (Argand plane)
- roots of unity

Foundational Results.

- De Moivre's Theorem for the multiplication of complex numbers
- integer powers of complex numbers:
  - if $z = r(\cos\theta + i\sin\theta)$ then $z^n =$
  - if $z = r(\cos\theta + i\sin\theta)$ then $z^{-n} =$
- Use these formulas to be able to find expressions for $\cos(n\theta)$ and $\sin(n\theta)$ in terms of $\cos(\theta)$ and $\sin(\theta)$.
- the $e^{i\theta}$ notation
- Be able to find a root of an equation of the form $z^n = w$ where w is a given complex number.
- Be able to find all n roots of an equation of the form $z^n = w$ where w is a given complex number, from that first root together with the roots of unity.
- Use these techniques to find roots for selected other polynomial equations.

Typical Problems.

- Find the real and imaginary parts of powers of complex numbers such as $(1-i)^{21}$ or $(1-i\sqrt{3})^{-15}$
- For which values of n is $(\sqrt{3}-i)^n$ an imaginary number? And for which values of n is it a real number?
- Find a formula for $\sin(6\theta)$ in terms of $\sin(\theta)$.
- If you consider all the roots of the equation $z^8 = 1+i$, what shape do they make?
- Be able to find complex roots of quadratic equations (and of equations of degree $2n$ that are quadratic equations in x^n).
- If you want a challenge problem, solve Problem 11 on Page 45 of the book (it is easier than it looks).

3. Induction

All of Chapter 8.

Concepts.

- The principle of mathematical induction.
- The principle of strong mathematical induction.
- Sigma notation

Foundational Results. Be able to use strong induction to prove the prime factorization theorem (Proposition 8.1).

Typical Problems.

- Use induction to show results about sums of sequences of numbers. See the assignment problems.
- Some induction problems need a bit more work for the induction basis. Here is an example:
  - Prove by (strong) induction that it is possible to pay, without requiring change, any whole number of roubles greater than 7, with banknotes of value 3 roubles and 5 roubles.
- Use induction to prove results about divisibility:
  (1) For all integers $n \geq 0$, the number $5^{2n} - 3^n$ is a multiple of 11.
  (2) For any integer $n \geq 1$, the integer 2^{4n-1} ends with an 8.
- Induction can also be very helpful in proving inequalities. For the induction step in this type of situation, you want to start with the left hand side of the equation and rewrite it until the left hand side of the induction hypothesis is part of it - then you can apply the induction hypothesis to get the first inequality; after that you may need to do a bit of rewriting with the remaining terms to show that they keep you on the correct side of the inequality. Here are some practice problems:
  (1) If $n \geq 3$ is an integer, then $5^n > 4^n + 3^n + 2^n$.
  (2) For every integer $n \geq 2$,
$$\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \geq \frac{7}{12}.$$
- Use induction to show results about geometric problems, such as the number of areas formed by n lines in the plane (see the assignment problems). If you want more practice, here two related problems:
  (1) Given n circles in the plane, suppose that you want to colour the finite regions formed by those circles, in such a way that if two regions share a circle segment (not just a point), then they have distinct colours. How many colours would you need? Prove your result.
  (2) Problem 15 of Chapter 8.
- Use strong induction to show results about recurrence relations. For example, let $u_0 = 1$, $u_1 = 0$, and $u_{n+1} = 2u_n - u_{n-1}$. Guess a formula for u_n as a function of n and prove it using strong induction.

4. Euler's Formula and Platonic Solids

All of Chapter 9.

Concepts.

- Euler's formula for convex polyhedra.
- Euler's formula for planar graphs.
- The five Platonic solids.

Foundational Results.

- For convex polyhedra, $V - E + F = 2$.
- For planar graphs, $v - e + f = 1$.

Typical Problems.

- Be able to do the kind of calculations as in Exercises 1, 4, and 7. Here is one more for practice:
  - Ivor Smallbrain has been hired by Sears to create polyhedral softballs for small children. Sears only provides Ivor with matching equilateral triangles and squares and stipulates that the softballs need to have four edges come together at every vertex. Greta Picture is there with Ivor to help him and she says immediately, that he will need exactly 8 triangular pieces for every softball. Show that Greta is right, and provide Igor and Greta with the design for such a softball.
- Prove related results for planar graphs or draw graphs with a particular property, such as every vertex being connected to three other vertices.

5. Infinity

All of Chapter 22, together with the Definitions on Pages 163 and 164, and Proposition 20.1 on Page 165.

Concepts.

- 1-1, onto and bijective (for functions)
- Countability and uncountability for sets.

Foundational Results.

- The diagonal argument.
- The integers and the rational numbers are countable (know a proof!).
- Every infinite subset of $\mathbb{N}$ is countable.
- If there is a 1-1 function $f\colon S \to \mathbb{N}$ and S is infinite, then S is countable.
- The powerset of $\mathbb{N}$ is uncountable.

Typical Problems.

- Determine for each of the following sets whether they are finite (give the size), countable or uncountable (give a proof):
  (1) the set of infinite 01-sequences;
  (2) the set of lines through the origin in the plane;
  (3) $\mathbb{N} \times \mathbb{Z}$;
  (4) the irrational numbers;
  (5) the set containing all prime numbers;
  (6) the set of points in the plane with coordinates (n^2, m^2), where n and m are integers;
  (7) the set of infinite sequences of digits;

(8) the set of finite sequences of digits;
(9) the set of finite sequences of digits of length less than or equal to 10 (if you find 10 hard, first try 4 or 5).

.

6. Number Theory

We have covered: Chapter 11 (all of it), Chapter 12 (only Theorem 12.1), Chapter 14 until and including page 116, Chapter 15 until the middle of page 126, but not the proof of Fermat's Little Theorem, Chapter 16.

Concepts.

- quotient and remainder
- congruence $a \equiv b \bmod m$
- the greatest common divisor
- the Euclidean algorithm
- RSA code
- the method of repeated squares

Foundational Results.

- The last non-zero remainder in Euclid's algorithm applied to positive integers a and b is the greatest common divisor of a and b. (**You need to know this result with its proof**)
- If $(a, c) = 1$ and $c|ab$ then $c|b$.
- If p is prime and $p|a_1a_2 \dots a_n$, then there is an $i \in \{1, 2, \dots, n\}$ such that $p|a_i$.
- The Fundamental Theorem of Arithmetic (know the statement)
- Proposition 14.6: When does the congruence equation $ax \equiv b \mod m$ have a solution?
- Fermat's Little Theorem (you need to know its statement, but not the proof).
- Proposition 15.2 and 15.3 (solutions for congruence equations of the form $x^k \equiv b \mod p$ and $x^k \equiv b \mod pq$).

Typical Problems.

(1) Problems as they were on your assignment (you are allowed to bring a calculator to this exam):
   - Apply Euclid's algorithm and find the greatest common divisor of two integers; also, if $d = (a, b)$, be able to find integers s,and t such that $d = sa + tb$ and with prescribed signage for s and t (either you may be requested that $s > 0$ and $t < 0$ or that $s < 0$ and $t > 0$).
   - Be able to solve equations of the form $ax \equiv b \mod m$ (or determine that they don't have a solution).
   - Be able to take powers modulo m (using repeated squares).
   - Be able to take roots modulo p and modulo pq.
   - Be able to encode RSA coding when you are given a public key.
   - Be able to decode an encoded message if you know the primes.