Math 2710 First Exam Study Guide

The exam will cover Chapters One and Two. This means that you are responsible for all of the material in those chapters, With the exception of the Extended Euclidean Algorithm, presented on pages 31, 32, and the top of page 33 in the book. I will, however, expect you to know that, given integers a and b, you can find x and y so that $ax + by = gcd(a, b)$ using the (regular) Euclidean algorithm via backsubstitution; and know how to calculate this in simple cases.
Strictly speaking this fact is buried in the discussion in the book immediately following Theorem 2.24 on page 30.

Key topics from Chapter One

In parentheses I indicate problems from the book that are related.

- Understand how to use truth tables to determine the truth or falsehood of compound propositions built up using AND, OR, NOT, IMPLIES, and EQUIVALENCE, based on the truth or falsehood of the component propositions (problems 7-16)
- Interpret logical propositions in conventional English, and vice versa (Problems 26-32)
- Be able to determine if two compound propositions are equivalent and to prove that using truth tables (22-25)
- Understand the relationship between an implication, its contrapositive, and its converse and, given a proposition, to state its contrapositive and its converse. (55-61, 64)
- Be able to explain how a proof of a compound proposition such as "If P, then Q OR R" and be converted to "If P and NOT Q, then R" and similar techniques labelled "Proof Methods" in Chapter 1. (77-79)
- Work with existential and universal quantifiers, and how they interact with negation. (41-44)
- Be able to interpret statements of the form "For all x, there exists y such that ...." or "There exists x such that for all y..." and to prove simple propositions that involve these constructions. (45-54,67,74)
- Understand the relationship between set operations (Union, Intersection, subset, equality) and logical constructions and be able to prove simple propositions about sets. (68-74)

Key Topics from Chapter Two

In Chapter Two, you should:

- Be able to reproduce, exactly, the crucial definitions:
  - Definition of what it means to say that an integer a divides an integer b

  - Definition of the quotient and remainder that arise from the statement of the division algorithm.

  - Definition of the greatest common divisor and the least common multiple of two integers
  - Definition of a prime number

- Be able to state the well-ordering principle.
- Be able to prove the key results of Chapter Two:
  - Proposition 2.11 on properties of divisibility
  - The Division Algorithm 2.12
  - The Euclidean Algorithm (2.21, 2.22, 2.24, 2.27, 2.28, 2.29)
  - The Main Theorem on Diophantine Equations (2.31)
  - Theorem 2.41 on representing integers in base b
  - The Theorems and propositions on primes and unique factorization, including the relationship to gcd and lcm (2.51-2.59)

Because of time, I will not ask you for a complete proof of, for example, the Euclidean algorithm. I could:

- ask you to prove one of the parts of Proposition 2.11 such as the claim that $a|b$ and $b|c$ means $a|c$.
- ask you to prove that the remainder constructed by the division algorithm is unique; in other words, to show that if $b = aq + r$ and $b = aq' + r'$ then $r = r'$.
- ask you to prove Proposition 2.29 without using prime factorization; for example, prove that if $a|bc$ and $gcd(a, b) = 1$ then $a|c$ using the fact that $gcd(a, b)$ is a linear combination of a and b
- ask you to prove that the only divisors of a prime power p^n are $1, p, \ldots, p^{n-1}, p^n$

or many other smaller results that are buried in the proofs of the bigger results.

Sample problems from Chapter 2: 9, 10, 11, 27, 28, 47-50, 67, 73, 74, 75, 83, 93, 99-102