Review Sheet for Math 125 Test 2 Summer 2014

Chapter 3

There will be no specific questions from Chapter 3. However you are expected to read the chapter and understand the concepts of function, domain, target, range, one-to-one, onto, bijection, inverse function, composition of functions, floor and ceiling functions, cardinality of a set.

Section 4.1

Know the Well-Ordering Principle.
Know the Division Algorithm.
Be able to represent decimal numbers in any other base, especially binary, hexadecimal, and octal.
Convert a number from one base system to another.
[BB] exercises.

Section 4.2

Use the Euclidean algorithm to find the GCD of two numbers.
Find m and n where GCD(a,b) = am + bn.
Find the Least Common Multiple once the GCD is known.
Study Example 14 p. 111.
[BB] exercises.

Section 4.3

Know how to find prime numbers using the Sieve of Eratosthenes.
Understand the fundamental Theorem of Arithmetic (Prime decomposition is unique).
No [BB] exercises.

Section 4.4

Understand the equivalence relation "congruence mod n".
Solve a congruence or system of congruences for $0 \leq x < n$ (See Example 21).
Understand Proposition 4.4.9
Study Problem 25 on p. 131.
Know Fermat's Little Theorem.
[BB] exercises.

Section 4.5

Understand the Chinese Remainder theorem.
Know that RSA is possible due to the Fermat's little Theorem and the Chinese Remainder Theorem.
Encrypt and/or De-encrypt a message using the RSA Algorithm.
[BB] exercises.

Section 5.1

Use the Principle of Mathematical induction to prove a conjecture.
[BB] in Exercise 6.