Math 2513
Review for Second Exam
June 14, 2013

The second exam will be on material from sections 4.2, 4.3, 4.4, and 5.1 of the text. See Assignments 7 through 11 for homework problems on this material.

4.1. Divisibility and Modular Arithmetic. We've covered the entire section.

4.2. Integer representations and algorithms. We've also covered this entire section, except you can skip the algorithms in boxes. This section doesn't contain any examples of representations of integers to any bases besides 2, 8, and 16; but you should still be able to find representations to other bases, if asked. For example, what would the decimal number 3302 be when represented in base 3?

The last subsection describes how to compute exponents a^n modulo a number p. As mentioned in class, we've seen two ways to do this in class. The first way, described on pages 253–254, involves representing the exponent n as the sum of powers of 2, and is covered in this subsection. The second way uses the fact that, when you compute the value of $a^n \pmod{p}$ for $n = 1, 2, 3 \ldots$, you will see that the values start to repeat themselves. In fact, you will get back to a when n reaches p. Example 9 on page 281 illustrates how to use this fact. Generally, when the modulus p is a large number, the first way is faster, but when the modulus p is fairly small and n is large, then the second way is faster. On the test, you would probably want to use the second method.

4.3. Primes and greatest common divisors. In class, we covered the material in this section from the beginning through page 259, and on pages 265 through 271. You won't need to know any of the material on pages 260 to 264 for the exam; it is there just to be interesting and informative and give you a little better feel for the prime numbers.

4.4. Solving congruences. We only covered two topics from this section: inverses modulo m (see Theorem 1 and Examples 1 and 2), and modular exponentiation (see Example 9). For modular exponentiation it's useful to know Fermat's little theorem, but it's not really necessary. You can skip the remainder of the material in this section.

5.1. Mathematical induction. This is covered on Assignment 11. Since you won't get Assignment 11 returned to you before the exam, I will only ask simple induction problems on the exam, similar to Examples 1, 5, or 6; or problems 4 or 31 at the end of this section.