Math 3H03 Midterm 2 Info Sheet

The purpose of this handout is to help you study by listing the concepts, definitions, and results you will need to know for the midterm.

Midterm Information. The midterm will be on Wednesday, April 1, 2020. You will do your midterm via Crowdmark. Here is some specific information.

- I will send you a copy of the test and open up access to Crowdmark at 10:15AM, and closing off access at 11:45AM.
- Complete your midterm just as would complete your homework on Crowdmark, i.e., write out your solutions, take a picture, and post them to Crowdmark.
- The normal length of the midterm is 50 minutes (10:30-11:20). However, I am giving you 15 minutes before and 25 minutes after to deal with any technical problems.
- The test contains 5 questions, each worth five points. There is also one bonus question.
- The test is an open book test.

Material Covered. The midterm will cover the material we discussed in class about Sections 3.2, 3.3, 3.5, Chapter 4, Chapter 11, Chapter 5, Chapter 6, and Chapter 7 (this is the same material covered in homework assignments 5 through 8, and Lectures 13-32). Below is a breakdown of what you will need to know from each section. Note that when you are learning definitions, it is good to know an example of that definition, and an example of an object that does not satisfy the definition.

Section 3.2. Know how to solve linear congruences. In particular, know how to use Theorem 3.7 to determine if a linear congruence has a solution, and be able to use Lemma 3.9 to find solutions to linear congruences.

Section 3.3. Know Theorem 3.10 (The Chinese Remainder Theorem). In particular, you should be able to use the Chinese Remainder Theorem to solve systems of linear congruences. Also, although Theorem 3.4 appears in Section 3.1, we proved it as part of Theorem 3.10, so you should know Theorem 3.4.

Section 3.4. You are not responsible for this section.

Section 3.5. You should know how to use the generalized Chinese Remainder Theorem (Theorem 3.12).

Section 4.1. There are a number of extremely important results in this section: Theorem 4.1, Theorem 4.3, Corollary 4.4, and Corollary 4.5. In particular, you should know how to use these results to compute congruences like $a^m \pmod{p}$ for any prime p.

Section 4.2. Know the definitions of pseudo-primes and Carmichael numbers. Know Theorem 4.7 and Lemma 4.8.

Section 4.3. From this section, know how to solve equations of the form $f(x) \equiv 0 \pmod{p^e}$ with p a prime. In particular, know how to use Hensel's Lemma, and the procedure that was explicitly described in class.

Section 5.1. Know what we mean by a unit and and an inverse in $\mathbb{Z}_n$. Also, know how to find the group of units U_n.

Section 5.2. Know what Euler's function $\phi(-)$ is. Know what we mean by a reduced set of residues modulo n. Know Euler's Theorem (Theorem 5.3). Know how to compute $\phi(n)$ (see Lemma 5.4 and Corollary 5.7). Also know Theorems 5.6 and 5.8.

Section 5.3. There will be no questions based on this section since we spent an entire class working on RSA problems.

Section 6.1 Know what we mean by the order of an element in U_n, and how to determine the order of each element in a group U_n.

Section 6.2 Know what we mean by a primitive root mod (n). Know how to use Lemma 6.4 to determine if an element is a primitive root. Know Theorem 6.5 and 6.6.

Section 6.3-6.5 You will not be tested directly on this material. The only thing you should know is the statement of Theorem 6.11.

Section 7.1-7.2 Know what we mean by a quadratic residue mod (n). Be able to compute Q_n for small n by hand. Know Lemma 7.3.

Section 7.3 Know what we mean by the Legendre Symbol. Know Corollary 7.4, Theorem 7.5, and Euler's criterion (Theorem 7.6) in order to compute the Legendre Symbol. Also important are Corollary 7.7 and Gauss's Lemma (Theorem 7.9). Also useful to know is Corollary 7.10.

Section 7.4 Know the statement of the "Law of Quadratic Reciprocity" (Theorem 7.11) and how to use it (for example, see Example 7.9). You do not need to know the proof.

Sections 11.1, 11.2, 11.6. These are historical sections. You don't need to know them.

Section 11.3. Know what a Pythagorean triple and primitive Pythagorean triple are. Exercise 11.5 is also important (part of it was proved in class).

Section 11.4. Know Theorem 11.2.

Section 11.5. Know Theorem 11.3 which classifies all primitive Pythagorean triples. You do not need to know about the alternative approach which finds all rational solutions (i.e., you don't need to know the material after Corollary 11.4).

Section 11.7. Know the statement of Fermat's Last Theorem, and know Theorem 11.5 and Corollary 11.6.

Sections 11.8-11.10. Although I talked about the proof of Fermat's Last Theorem in class (Lecture 22), you will not be tested on this material.

If you have questions, please feel free to email me. I will also try to be online in case you have questions in the lead up to the test.