1. Overview

Test 3 will cover four topics.

1. Solving $ax \equiv b \mod m$ when $(a, m) > 1$. See Section 3.2 in the textbook, or the Various Topics handout.

2. Quadratic residues and quadratic reciprocity. Solving quadratic congruences. See the Quadratic Residues handout for this topic. For more practice work through Chapter 7 of the textbook. (My main objection to Chapters 6 and 7 is that they spend a lot of time working modulo $n$ where $n$ is not prime. That is interesting, but I want to focus on the simple case of modulo primes in order to leave more time for other topics.)

3. Cryptography, public key, RSA, digital signatures. See the Various Topics handout, class notes, or Section 5.3 from the textbook.

4. The first two pages of Counterexamples to the Hasse Principle: an elementary introduction. Learn Euler’s criteria, and the first two versions of the Hasse Principle. Also be able to work through some basic examples. You should know what homogeneous means, verify some steps, etc. (See the the Various Topics handout for some examples).

2. Practice Problems

1. Exercise 3.5. (I like the first solution in the back of the book).

2. Exercise 3.6. (I am not totally happy with the solution in the back of the book).

3. Exercise 3.7.


5. Exercise 5.15.

6. Exercise 5.16.

7. Exercise 5.17.

8. Exercise 5.19 (In real life, your $n$ would be so large that you couldn’t solve this problem).

9. Explain how to choose $p$, $q$, $n$, $e$, and $f$ in the RSA. (Hint: $e$ and $f$ are inverses modulo $\phi(n)$.)
10. Explain how to encrypt and decrypt messages using RSA.

11. Explain how to prove that you are you (digital signature) using RSA.

12. Explain why \( ef \equiv 1 \mod \phi(n) \) implies that \( E(x) = x^e \) and \( F(x) = x^f \) are inverse functions \( \mathbb{F}_n \to \mathbb{F}_n \). (See the Various Topics handout).


14. Exercise 7.10. (Hint: the answer is related to \( p \) modulo 8).

15. Exercise 7.11.


17. Give examples of homogeneous and non-homogeneous polynomials.

18. Does the Diophantine equation \( 2X^2 + 3Y^2 = 5Z^2 \) have a non-trivial integer solution? What about \( 3Y^2 + 5Z^2 = 2X^2 \)? What about \( 2X^2 + Y^2 + 5Z^2 = 0 \)? (Hint: Euler’s criterion) See the Other Topics handout for examples.

19. State the first two versions of Hasse’s Principle.

20. – 38. Do the nineteen exercises from the Quadratic Residue handout.

3. Proofs to Learn

Learn the proof of Theorem 1 of the Quadratic Residues handout and the proofs of all the Lemmas that lead up to it including Lemma 1, Lemma 2, and Lemma 3. Also be able to prove consequences of Theorem 1, including Property 3 and Property 4.

(Of course, you should know and be able to use the statements of all the results, even the ones that you do not need to know the proofs to.)

Dr. Wayne Aitken, Cal. State, San Marcos, CA 92096, USA

E-mail address: waitken@csusm.edu