

The exam will be designed to take 50 minutes to do 6 problems, each worth 10 pts. The exam will be graded out of 50 pts, so that there is the option to do only 5 out of 6 problems. If you do 6 out of 6, you will get extra credit.

Below is an outline of what you need to know from the sections that we covered. Unless otherwise stated, you do not need to know the proofs of theorems, just understand their statements and be able to use them to solve problems. You should be able to state that you are using a theorem and what the theorem says when you use it.

- Sec 3.3 – Euclidean Algorithm to find $gcd(a, b)$ and to express it as a linear combination of a and b .
 – No proofs of theorems from the section.
 – Homework problems like 1-4.
- Sec 3.4 – Fundamental Theorem. Lemmas 3.4, 3.5. Least common multiple. Lemma 3.6, Theorem 3.15. Dirichlets Theorem (Statement on page 72) Theorem 3.16. Lemma 3.8.
 – No proofs of theorems from the section. Be able to prove that $\sqrt{2}$ is irrational.
 – Homework problems like 1-5, 6.
- Sec 3.5 – Factorization. Trial division. Lemma 3.9, Fermat factorization. State Fermat's Last Theorem. Defn - Fermat numbers.
 – No proofs of theorems from the section.
 – Homework problems like 1-4.
- Sec 3.6 – Linear Diophantine Equations. Theorem 3.21
 – Be able to prove Theorem 3.21.
 – Homework problems like 1-6.
- Sec 4.1 – Definitions: congruent, system of complete residues mod m . Theorems 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8. Corollaries 4.4.1, 4.8.1. Lemma 4.1. Be able to do modular exponentiation.
 – Proofs of Theorems 4.4, and 4.5. Corollary 4.4.1
 – Homework problems like 1-3, 6-7, 8-11, **26(I added this one)**, 28.
- Sec 4.2 – Linear Congruences. Theorem 4.10. Modular inverses. Theorem 4.11
 – No proofs of Theorems from the section.
 – Homework problems like 1-3, 5-9.