MATH 540: STUDY GUIDE FOR THE FINAL EXAM

The following is a list of topics covered since Exam 2. The study guides for the previous exams together with this guide serve as a study guide for the final exam. The final exam will consist of true-false questions, short answer questions (including stating definitions and major theorems), calculations, and two proofs. One proof will be from the indicated proofs from the previous study guides and another from the list below.

1. Fermat's two square theorem: Know both statements, one given for prime numbers only, and the more general statement for integers that are not necessarily rime numbers.

2. Lagrange's four squate theorem: Be able to state it and know the statements of any relevant lemmas used in the proof.

3. Know the deifinition of Gaussian integers and properties of the norm of Gaussian integers.

4. Know how to use the division algorithm for Gaussian integers to calculate GCDs of Gaussian integers, and how to express GCDs via Bezout's Principle.

5. Know how to state and apply the Fundamental Theorem of Arithmetic for Gaussian integers. SImilarly for Fermat's Little Theorem for Gaussian integers.

6. Know the description of Gaussian primes and be able to factor Gaussian primes with small norm into a product of Gaussian primes.

7. Know the properties of Gassuian integers modulo a fixed Gaussian integer and how to find a complete set of residue classes.

8. Be able to solve linear congruences modulo a Gaussian integer.

8. Be able to reproduce the proof of any one of the following three theorems:

(i) The Fundamental Theorem of Arithmetic for Gaussian integers.

(ii) The theorem that provides a complete set of residue classes modulo a Gaussian integer. For this you may assume the lemma which states that if $z = a + bi \in G$, with $\text{GCD}(a, b) = 1$ and $n \in \mathbb{Z}$, then $z|n$ in G implies $N(z)|n$ in $\mathbb{Z}$.

(iii) Fermat's Little Theorem for Gaussian integers.