NUMBER THEORY
Math 522

Michael E. O'Sullivan

Preparing for the Second Exam

Things you should be able to do.

I. Chapter 3

- The unique factorization theorem is one of the most fundamental results in number theory. Be able to state it precisely and use it in a variety of contexts.
- Solve a linear diophantine equation.

II. Chapter 4

- Solve linear congruences modulo n.
- Identify units (invertible elements), zero divisors, and quadratic residues modulo n (§11.1).
- Compute the inverse of a modulo n when a is coprime to n.
- Solve problems with the Chinese remainder theorem
  - with two coprime moduli;
  - with three coprime moduli;
  - with two moduli that are not coprime.
- Solve a system of linear equations modulo n
- Invert a matrix modulo n.
- Solve a quadratic equation modulo a prime (§11.1 ex.12).

III. Chapter 5

- Test for divisibility by 2, 3, 5, 11.
- Develop similar test for divisibility in other bases.
- Use a check digit scheme for detecting errors and analyze error events that the scheme will fail to detect.

No calculators can be used on the exam.