

## I. Be able to state:

1. Well Ordering Principle
2. Binomial Theorem
3. Division Algorithm (2.1)
4. GCD Theorem (2.3)
5. Relatively Prime Theorem (2.4)
6. Fundamental Theorem of Arithmetic & canonical form corollary (3.2 & corollary)
7. Dirichlet's Theorem (3.7)
8. Definition of multiplicative inverse
9. Chinese Remainder Theorem (4.8)
10. Result from Theorem 5.5 (quadratic congruence)

## II. Be able to state and prove:

1. Euclid's Lemma (2.5)
2. There exists an infinite number of primes of the form  $4k + 3$ . (3.6)
3. If  $ca \equiv cb \pmod{n}$ , then  $a \equiv b \pmod{n/d}$ , where  $d = \gcd(c, n)$ . (4.3)
4. Fermat's Little Theorem & Corollary (5.1)
5. Wilson's Theorem (5.4)

## III. Know:

1. Definitions
2. Conditions under which linear diophantine equations can be solved, how to find them and how many solutions exist.
3. Divisibility conditions (section 4.3)
4. Euclidean Algorithm
5. Techniques from homework problems.