

## I. Be able to state:

1. Theorem 6.7: Möbius Inversion formula
2. How to calculate  $\sigma, \tau, \mu$  and  $\phi$ . In particular, Theorems 6.2 & 7.3
3. Theorem 7.5: Euler's Theorem
4. Theorem 8.3 (on the order of  $a^h \pmod{n}$ )
5. Corollary to 8.4 (If  $n$  has a primitive root, then it has exactly  $\phi(\phi(n))$  of them.)
6. Lagrange's Theorem (Theorem 8.5)
7. Theorem 8.6 (If  $p$  is a prime number and  $d \mid p - 1$ , then there are exactly  $\phi(d)$  incongruent integers having order  $d$  modulo  $p$ .) & corollary on the number of primitive roots of primes.
8. Theorem 8.10 (which integers have primitive roots.)
9. Theorem 9.2 on properties of the Legendre symbol.
10. Theorem 9.6 (on the calculation of  $(2/p)$ ) and the corollary (stating that for  $p$  an odd prime,  $(2/p) = (-1)^{(p^2-1)/8}$ ).

## II. Be able to state and prove:

1.  $\tau$  is a multiplicative function (Part of theorem 6.3)
2. Theorem 7.6 Gauss' Theorem
3. Theorem 8.1: If  $a^k \equiv 1 \pmod{n}$ , then the order of  $a \pmod{n}$  divides  $k$ .
4. Theorem 8.8: If  $\gcd(m, n) = 1$  where  $m > 2$  and  $n > 2$ , then  $mn$  has no primitive roots.
5. Theorem 9.1: Euler's Criterion

## III. Know:

1. Definitions of
  - (a) a multiplicative function,
  - (b) the number theoretic functions  $\sigma, \tau, \phi, \mu$ ,
  - (c) the *order* of an integer modulo  $n$ ,
  - (d) a *primitive* root of an integer  $n$ ,
  - (e) a quadratic residue and a quadratic non-residue of  $n$ ,
  - (f) the Legendre symbol  $(a/p)$  for  $p$  an odd prime,
2. Know how to calculate  $a^n \pmod{m}$  using Euler's Theorem for large  $n$ .
3. Know how to find all elements of a given order given a primitive root of  $n$ .
4. Know how to find all solutions (and when they exist) to  $x^d \equiv 1 \pmod{n}$ .
5. Practice manipulation of Legendre symbols using theorem 9.2 & corollaries.
6. Know how to find solutions to  $ax^2 + bx + c \equiv 0 \pmod{p}$  for  $p$  an odd prime.
7. Techniques from homework.