Math 4400/Number Theory/Fall 2012
Stuff to Know for the Second Midterm

Definitions you need to know.

(1) What is a ring?
(2) What is field?
(3) What is the characteristic of a field?
(4) What is a quadratic integer?
(5) What is a perfect number?
(6) What is a Mersenne prime?
(7) What is the function $\sigma(n)$?
(8) What is a primitive dth root of 1 in a field F?
(9) What is the discrete logarithm I_a in $(\mathbb{Z}/p\mathbb{Z})^\times$?
(10) What is the cyclotomic polynomial $\Phi_d(x)$?

How to's.

(1) How to solve linear equations mod p.
(2) How to find mth roots (mod p) when $\gcd(m, p-1) = 1$.
(3) How to find multiplicative inverses in $\mathbb{Q}[\sqrt{d}]$
(4) How to find multiplicative inverses in $\mathbb{Z}[\sqrt{d}]$ (mod p).
(5) How to compute $\sigma(n)$.
(6) How to find high powers a^u (mod p) by successive squaring.

Theorems you should be able to state precisely.

(1) Wilson's Theorem
(2) The Lucas-Lehmer Test
(3) Dirichlet's Theorem on Primes in Arithmetic Progressions

Stuff you should be able to prove.

(1) Wilson's Theorem.
(2) Every even perfect number is of the form $2^{l-1}(2^l - 1)$ where $2^l - 1$ is a Mersenne prime.
(3) $\mathbb{Q}[\sqrt{d}]$ is a field whenever $d \in \mathbb{Z}$ and $\sqrt{d}$ is irrational.
(4) $\sum_{d|n} \phi(d) = n$.