Material to Study for Math 788M
Comprehensive Exam

- Be able to do problems related to any of the homework. This includes homework problems not directly related to computational aspects of number theory such as topics in Elementary Number Theory and problems on notation. It also includes material not covered below (for example, public-key encryption).
- Be able to prove Lamé's Theorem concerning greatest common divisors.
- Be able to prove that $\gcd(u, v)$ is $\asymp \log N$ and that usually it's much smaller.
- Be able to define a strong pseudoprime to the base b and be able to prove that no n is a strong pseudoprime to every base b with $1 \leq b \leq n$ and $\gcd(b, n) = 1$.
- Be able to check if a number is prime by using Maple's version of the Lucas-Lehmer test. (This is not a sure prime test.)
- Be able to state and prove the Proth, Pocklington, Lehmer Test for primality.
- Be able to prove that most numbers n have a prime factor $> \sqrt{n}$.
- Be able to explain Pollard's ρ-Algorithm including Floyd's cycle-finding algorithm.
- Be able to factor n using Dixon's Algorithm (see homework). (You will be given some information and you will need to make use of it and give the remaining details.)
- Be able to factor n using the Quadratic Sieve Algorithm. (You will be given some information and you will need to make use of it and give the remaining details.)
- Be able to prove Mignotte's inequality for the size of the factors of a polynomial.