MATH 4400 – Learning objectives to meet for Exam #1

The exam will cover all material that was covered since the previous exam through the lecture on Friday, March 29, concluding with the proof of Lagrange's four square theorem.

What to be able to state

Basic definitions

You should be able to give complete and precise definitions of each of the following items:

- "a is a square modulo p"
- Legende symbol $\left(\frac{a}{p}\right)$
- half-set modulo an odd prime p
- greatest integer function $\lfloor x \rfloor$
- Jacobi symbol $\left(\frac{a}{m}\right)$
- "substantial set" of positive integers
- the functions $\pi(x)$ and $\theta(x)$
- $\mathbf{Z}[i]$ and associated concepts, including the norm and the concept of a prime in $\mathbf{Z}[i]$

Big theorems

Give full statements of each of the following results, making sure to indicate all necessary hypotheses. For results proved in class or on homework, describe the components and main ideas of the proof.

- for every odd prime p, there are $\frac{p-1}{2}$ nonzero squares mod p
- Euler's criterion for squares modulo p
- Gauss's lemma
- Generalized Gauss's lemma
- Explicit Gauss's lemma for $\left(\frac{a}{p}\right)$, with a odd
- Kronecker's version of the Explicit Gauss Lemma
- Quadratic Reciprocity Law
- the Quadratic Reciprocity Law for the Jacobi symbol
- rules for computing the Legendre symbols $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$, as well as the Jacobi symbols $\left(\frac{-1}{m}\right)$ and $\left(\frac{2}{m}\right)$
- the set of primes is a substantial set
- Chebyshev's upper and lower bounds on $\pi(x)$
- Prime number theorem (statement only)
- Bertrand's postulate

- Unique factorization theorem in $\mathbf{Z}[i]$
- Fermat's two square theorem
- Thue's lemma
- Fermat's two square theorem via Thue's lemma
- Lagrange's four square theorem
- for each nonzero $\mu \in \mathbf{Z}[i]$, the number of elements in $\mathbf{Z}[i]/\langle\mu\rangle$ is $N\mu$ (statement only)
- Thue's lemma in $\mathbf{Z}[i]$
- for every odd prime p, there is an $\alpha \in \mathbf{Z}[i]$ with $N\alpha \equiv -1 \pmod{p}$
- if $2m$ is a sum of four squares, then m is a sum of four squares

What to be able to do

You can expect 5 problems on the exam. At least one will be purely computation-focused; you should know how to use the methods from class for all of the following.

- Compute the highest power of a prime dividing a factorial, as well as the highest power of a prime dividing a binomial coefficient $\binom{n}{k}$
- Use Euler's criterion to determine if a given integer a is a square modulo a given prime p
- Use Gauss's lemma (or its extended version) to determine if a given integer a is a square modulo a given prime p
- Use the quadratic reciprocity law to classify all primes p for which a given integer a is a square mod p. (For example, find all p with -7 a square mod p.)

I will not ask you to reproduce any very long proofs — for instance, I will not ask for a full proof of Chebyshev's bounds, or of the quadratic reciprocity law, or of Lagrange's four square theorem. But I may ask you questions related to the lemmas we used to prove these big results. For example, for Chebyshev's theorems, you should have a good idea how our lemmas on binomial coefficients were proven.