MATH 4400 – Learning objectives to meet for Exam #1

The exam covers everything up through the lecture on Friday, February 25. It is closed-book/notes. No calculators, formula sheets, or other aids are allowed.

What to be able to state

Basic definitions

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

- definition of divisibility in a commutative ring R
- prime number in $\mathbb{Z}$
- greatest common divisor in $\mathbb{Z}$
- definitions of "unit", "conjugation", "norm", "prime" and "gcd" in $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{-2}]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$
- Legendre symbol $\left(\frac{a}{p}\right)$

Big theorems

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

- $N(\alpha\beta) = N(\alpha)N(\beta)$, in $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{-2}]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$
- The units in $\mathbf{Z}$ are ± 1, those of $\mathbf{Z}[i]$ are $\pm 1, \pm i$, and those of $\mathbf{Z}[\sqrt{-2}]$ are ± 1
- Division Algorithm in $\mathbf{Z}$, $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{-2}]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$
- Every ideal of $\mathbf{Z}$, $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{-2}]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$ is generated by a single element.
- In each of $\mathbf{Z}$, $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{-2}]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$, every pair of elements has a gcd that is a linear combination of the two.
- Fundamental lemma in $\mathbf{Z}$, $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{-2}]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$
- Euclid's lemma in $\mathbf{Z}$, $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{-2}]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$
- Unique factorization theorem in $\mathbf{Z}$, $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{-2}]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$
- Description of all units in $\mathbf{Z}[\sqrt{2}]$
- a prime p of $\mathbb{Z}$ factors in $\mathbf{Z}[i]$ if if p divides $n^2 + 1$ for some n
- if p is an odd prime (in $\mathbb{Z}$), then $\sqrt{-1} \in \mathbf{Z}_p$ if and only if $p \equiv 1 \pmod 4$
- an odd prime p of $\mathbb{Z}$ factors in $\mathbb{Z}[i]$ if and only if $p \equiv 1 \pmod 4$.
- Let $d > 0$ be a nonsquare integer. There are infinitely many pairs of integers x, y, with $y > 0$, for which $|x^2 - dy^2| \le 2\sqrt{d} + 1$.
- Let $d > 0$ be a nonsquare integer. There is a smallest unit $\epsilon > 1$ in $\mathbf{Z}[\sqrt{d}]$. All units > 1 are powers of ϵ. Same statements with the added condition of "norm 1".

- Let $d > 0$ be a nonsquare integer, and let ϵ be the smallest unit > 1 of norm 1 in $\mathbb{Z}[\sqrt{d}]$. Then the solutions in positive integers x, y to $x^2 - dy^2 = 1$ can be read off from the positve powers of ϵ.
- Euler's criterion for $\left(\frac{a}{p}\right)$
- Gauss's criterion for $\left(\frac{a}{p}\right)$
- Gauss's criterion for $\left(\frac{a}{p}\right)$, v2.0
- Law of Quadratic Reciprocity (statement only!)

What to be able to compute

You should know how to use methods discussed in class to perform the following computations.

- Divide, with quotient and remainder, in any of $\mathbf{Z}$, $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{-2}]$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$
- Calculate greatest common divisors using the Euclidean algorithm ina any of the above systems. Express your greatest common divisor as a linear combination of the starting values, via backtracking.
- Compute values of Legendre symbols using Euler's criterion
- Compute values of Legendre symbols using Gauss's criterion
- Compute values of Legendre symbols symbols using quadratic reciprocity and the known rules for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$

Format

You can expect five (multi-part) questions on the exam. At least 40% of the exam will test you on definitions or computations. The rest of the exam is designed to test your comfort level manipulating the concepts and theorems from class. For the most part, I am not interested in having you regurgitate proofs of results from class/HW; I want to know if you have internalized the ideas enough to solve similar problems.

Practice problems

1. Let p be a prime in $\mathbf{Z}$.
   (a) Show that if 3 is a square mod p, then p does not stay prime in $\mathbf{Z}[\sqrt{3}]$.
   (b) Show that if 3 is a square mod p, then there are integers x, y with $x^2 - 3y^2 = p$ or integers x, y with $x^2 - 3y^2 = -p$.
   (c) As stated in class, 3 is a square mod p for every $p \equiv 1 \pmod{12}$. (You may assume this here.) Show that if $p \equiv 1 \pmod{12}$, then $-p = x^2 - 3y^2$ has no solution in integers x, y. Conclude that $p = x^2 - 3y^2$ for some integers x, y.
2. (a) Compute $\left(\frac{3}{11}\right)$ using Gauss's criterion.
   (b) Compute $\left(\frac{3}{11}\right)$ using Euler's criterion.
   (c) Compute $\left(\frac{21}{257}\right)$ using quadratic reciprocity. You may assume the rules from class for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$.
3. (a) State Euler's criterion for $\left(\frac{a}{p}\right)$.

(b) Let p be a prime that divides $2^{2021} - 1$. Show that $\left(\frac{2}{p}\right) = 1$.

4. (a) Find, by any method discussed in class (continued fractions are allowed), the smallest unit > 1 of norm 1 in $\mathbf{Z}[\sqrt{17}]$.

   (b) Prove or disprove: There is a solution to $x^2 - 17y^2 = 1$ for which $2021 \mid y$. (You do not need, or want, to use your solution to (a) for this.)

5. We work in the system $\mathbf{Z}[\sqrt{-2}]$.

   (a) Prove that if $\alpha \mid \beta$ in the system $\mathbf{Z}[\sqrt{-2}]$, then $N\alpha \mid N\beta$ in the system $\mathbf{Z}$.

   (b) Prove that $5 + \sqrt{-2}$ and $5 - \sqrt{-2}$ have a gcd of 1 in $\mathbf{Z}[\sqrt{-2}]$.