MATH 4400/6400 – Final Exam Study Guide
Exam time/location: Wednesday, May 11, 12:00 PM – 3 PM, usual classroom

The exam is **cumulative**. You should expect ≤ 10 questions, with a format similar to that used in the three midterms.

Course summary

Part I: Unique factorization in $\mathbb{Z}$ (review from 4000)

- Basic properties of divisibility in $\mathbb{Z}$
- Division algorithm in $\mathbb{Z}$
- Ideals in $\mathbb{Z}$ are principal
- Existence of gcds, computing gcds by Euclidean algorithm, the gcd is a linear combination of the starting numbers
- Fundamental Lemma, Euclid's lemma
- Unique factorization theorem for $\mathbb{Z}$

Part II: Arithmetic in $\mathbb{Z}[i]$, primes as sums of two squares, and allied concepts

- Definition of $\mathbb{Z}[i]$; verification that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$
- the norm map on $\mathbb{Z}[i]$ and its multiplicativity
- Basic properties of divisibility in $\mathbb{Z}[i]$ (echoing those of $\mathbb{Z}$)
- Units in $\mathbb{Z}[i]$ as elements of norm 1
- Gaussian primes
  - π is prime in $\mathbb{Z}[i]$ if $N\pi$ is prime in $\mathbb{Z}$
  - π is prime $\iff$ $\bar{\pi}$ is prime
  - π is prime $\iff$ all of its associates are prime
  - if p is prime in $\mathbb{Z}$, then p fails to be prime in $\mathbb{Z}[i]$ if and only if $p = \square + \square$
  - if p is prime in $\mathbb{Z}$ and $p \equiv 3 \pmod 4$, then p is prime in $\mathbb{Z}[i]$
  - if p is prime in $\mathbb{Z}$ and $p \mid n^2 + 1$ for some integer n, then p is not prime in $\mathbb{Z}[i]$
- Unique factorization theorem in $\mathbb{Z}[i]$
  - careful formulation (we factor nonzero nonunits into irreducibles, and the uniqueness is up to order and associates)
  - existence of factorizations

  - theory of gcds in $\mathbb{Z}[i]$ (echoing that of $\mathbb{Z}$)
  - Fundamental Lemma and Euclid's Lemma in $\mathbb{Z}[i]$
  - completion of proof of UFT in $\mathbb{Z}[i]$

- Wilson's theorem and Euler's criterion for squares mod p; determination of when -1 is a square mod p
- if p is prime in $\mathbb{Z}$ and $p \equiv 1 \pmod 4$, then p is not prime in $\mathbb{Z}[i]$; consequently, $p = \square + \square$
- analogues of these results for $\mathbb{Z}[\sqrt{-2}]$
- arithmetic in $\mathbb{Z}[\sqrt{2}]$
  - $\mathbb{Z}[\sqrt{2}]$ is dense in $\mathbb{R}$
  - units of $\mathbb{Z}[\sqrt{2}]$ as solutions to norm $= \pm 1$
  - complete description of the unit group $U(\mathbb{Z}[\sqrt{2}])$

Part III: Pell's equation $(x^2 - dy^2 = 1)$

- explanation of why this is only interesting when $d > 0$ and d is not a square !
- description of all solutions to $x^2 - 2y^2 = 1$, in terms of units in $\mathbb{Z}[\sqrt{-2}]$
- application: classification of all square triangular numbers
- a nontraditional proof that $\sqrt{d}$ is irrational when $d \neq \square$
- description of solutions to Pell's equation in terms of powers of smallest unit > 1
- infinitely many elements of bounded norm in $\mathbb{Z}[\sqrt{d}]$; deduction of the existence of a unit of norm > 1
- magic with continued fractions

Part IV: Squares modulo p

- Legendre's symbol
- Euler's criterion (proved in HW by a pairing up argument)
- basic properties of the Legendre symbol
  - if $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
  - $\left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right)$
- Gauss's criterion and rules for $\left(\frac{a}{p}\right)$ for small values of a
- Gauss's criterion v2.0, using floor functions
- Statement of the Law of Quadratic Reciprocity (QR)

- use of QR to determine specific Legendre symbols, as well as rules for $\left(\frac{a}{p}\right)$ for given values of a
- Floor function sums as lattice point counts
- Proof of Quadratic Reciprocity
- Jacobi symbol
  - definition and basic properties
  - QR and supplementary laws for the Jacobi symbol
  - computing with the Jacobi symbol and interpreting the results

Part V: Distribution of prime numbers

- there are infinitely many primes (Euclid)
- Legendre's formula for $\mathrm{ord}_p(n!)$
- $\sum_p 1/p$ diverges, via analysis of $\mathrm{ord}_p(n!)$
- Chebyshev's theorems on $\pi(x)$: There are $c_0, c_1 > 0$, as well as a real number x_0, such that $c_1 x/\log x \leq \pi(x) \leq c_2 x/\log x$ for all $x > x_0$.
- discussion of Gauss's approximation $\mathrm{Li}(x)$ to $\pi(x)$ and Riemann's zeta function; Euler's proof that $\sum_p 1/p$ diverges (non-examinable)

Part VI: Arithmetic functions

- Set-up: Definitions of arithmetic functions and multiplicative functions
- "Theorem A": if $f(n)$ is multiplicative, so is $g(n) := \sum_{d|n} f(d)$; deduction of multiplicativity of $d_k(n)$ and $\sigma(n)$
- the formula $n = \sum_{d|n} \phi(d)$
- "Theorem A′": if f, f' are multiplicative, so is $g(n) = \sum_{d|n} f(d)f'(n/d)$
- definition of the Möbius function; the fundamental relation $\sum_{d|n} \mu(d) = 1$ if $n = 1$ and 0 if $n > 1$
- Möbius inversion formula
- "Theorem B": if $\sum_{d|n} f(d)$ is multiplicative, then f is; consequently, ϕ is multiplicative
- discussion of the ring of arithmetic functions (with multiplication given by Dirichlet convolution); non-examinable

Part VII: Sums of squares

- Euler's theorem: for positive integers n, we have $n = \square + \square \iff \mathrm{ord}_p(n)$ is even for all primes $p \equiv 3 \pmod 4$
- $\mathbb{H}$ (the Hamiltonians) as an analogue of $\mathbb{C}$
  - definition; computing in $\mathbb{H}$
  - the norm map on $\mathbb{H}$
  - $\mathbb{H}$ is a noncommutative field ("division ring")
- the ring $\mathcal{L}$ of Lipschitz integers as a first analogue of $\mathbb{Z}[i]$; failure of the division algorithm in $\mathcal{L}$
- the ring $\mathcal{I}$ of Hurwitz integers; existence of the division algorithm in $\mathcal{I}$
- right ideals of $\mathcal{I}$ are principal
- units in $\mathcal{I}$ as elements of norm 1; description of all units in $\mathcal{I}$ (on HW)
- every rational prime p divides $x^2 + y^2 + 1$ for some $x, y \in \mathbb{Z}$
- Lagrange's four square theorem: Every $n = \square + \square + \square + \square$.
- brief discussion of sums of three squares
  - If $n \equiv 7 \pmod 8$, then $n \neq \square + \square + \square$. If $4 \mid n$, then $n = \square + \square + \square \iff \frac{1}{4}n = \square + \square + \square$. Hence: If $n = 4^k(8\ell + 7)$ for nonnegative integers k, ℓ, then $n \neq \square + \square + \square$.
  - Gauss's three square theorem: Unless $n = 4^k(8\ell+7)$ for nonnegative integers k, ℓ, we have $n = \square + \square + \square$. (No proof!)
  - Consequence of Gauss's theorem: Every $n = \Delta + \Delta + \Delta$.
- Dirichlet series, the Dedekind zeta function of $\mathbb{Z}[i]$, and Jacobi's two square theorem (non-examinable)

Practice problems

1. (a) State Gauss's theorem characterizing which positive integers n are sums of three squares.

   (b) Assume Gauss's theorem. Show that if n is any positive integer, we can write $n = x^2 + y^2 + z^2 + w^2$ for some integers x, y, z, w where $x \in \{0\} \cup \{2^k : k = 0, 1, 2, 3, \dots\}$.

2. Prove that for every $\alpha \in \mathbb{H}$, there is a $\gamma \in \mathcal{I}$ with $N(\alpha - \gamma) \leq \frac{13}{16}$.

3. For $\alpha, \beta \in \mathcal{I}$, say α is a **left divisor** of β if $\beta = \alpha\gamma$ for some $\gamma \in \mathcal{I}$.

   For $\alpha, \beta \in \mathcal{I}$, say that $\delta \in \mathcal{I}$ is an **LGCD** of α, β if (a) δ is a left divisor of α, β, (b) if γ is any left divisor of α, β, then δ is a left-divisor of γ.

   (a) Prove that every pair of $\alpha, \beta \in \mathcal{I}$ has some LGCD in $\mathcal{I}$.

   (b) Suppose δ, δ' are two LGCDs of the same pair α, β. Show that there is a unit ϵ of $\mathcal{I}$ with $\alpha = \beta\epsilon$.

   (c) Show that every LGCD of α, β can be written in the form $\alpha\nu + \beta\mu$ for some $\nu, \mu \in \mathcal{I}$.

4. Prove the following version of the "Fundamental Lemma" in $\mathcal{I}$: Let $\alpha, \beta, \gamma \in \mathcal{I}$. Suppose α left divides $\gamma\beta$ and that 1 is an LGCD of α and β. Suppose also that α, γ commute. Prove that α left divides γ.