E. Dummit's Math 3527 ∼ Number Theory 1, Spring 2020 ∼ Final Exam Topics List

- Integers, induction, divisibility, the Euclidean algorithm and GCDs, prime factorizations, rings
  - Suggested review: HW #1-#2, HW #3 problem 7.
  - Suggested reading: lecture notes 1.1-1.3.
- $\mathbb{Z}/m\mathbb{Z}$, units and zero divisors, Chinese remainder theorem, powers and orders, theorems of Fermat/Wilson/Euler, the Euler φ-function, computing orders, repeating decimals
  - Suggested review: HW #2-4, HW #5 problems 1, 2.
  - Suggested reading: lecture notes 2.1-2.4
- Cryptography, Rabin and RSA encryption, zero-knowledge proofs, Primality testing, factorization algorithms
  - Suggested review: HW #5 problems 4/5/7, HW #6, HW #7 problem 1
  - Suggested reading: lecture notes 3.1-3.6
- Integral domains and Euclidean domains, irreducible and prime elements, unique factorization
  - Suggested review: HW #7 problems 2, 3, 5, and 6, HW #8 problem 5.
  - Suggested reading: lecture notes 4.1.1-4.1.4
- Modular arithmetic and R/rR, units and zero divisors, Chinese remainder theorem + Euler's theorem + Fermat's theorem in R/rR
  - Suggested review: HW #8 problems 1-4, HW #10 problem 4d.
  - Suggested reading: lecture notes 4.2.1-4.2.2.
- Polynomial roots and factorization, Finite fields, counting irreducible polynomials in $\mathbb{F}_p[x]$, primitive roots
  - Suggested review: HW #5 problem 3, HW #9 problems 1-6
  - Suggested reading: lecture notes 4.3.1-4.3.3, Lectures 24-26.
- Modular arithmetic and factorization in $\mathbb{Z}[i]$, sums of two squares, Pythagorean triples
  - Suggested review: HW #10.
  - Suggested reading: lecture notes 4.4.1-4.4.2, Lectures 27-28.
- Polynomial congruences, Hensel's lemma
  - Suggested review: HW #11 problem 2, 6(b)
  - Suggested reading: lecture notes 5.1, Lecture 29.
- Quadratic residues, Legendre symbols, Euler's criterion
  - Suggested review: HW #11 problems 1, 3(a), 6(a), 9(a).
  - Suggested reading: lecture notes 5.2, Lecture 30.
- Quadratic reciprocity, Jacobi symbols, evaluating Legendre/Jacobi symbols with quadratic reciprocity
  - Suggested review: HW #11 problems 3(b), 4.
  - Suggested reading: lecture notes 5.3.1 + 5.4.1 + 5.4.3, Lecture 31.
- Characterizing quadratic residues, primes dividing quadratics, Berlekamp's algorithm, Solovay-Strassen
  - Suggested review: HW #11 problems 5, 7, 8, 9(bc).
  - Suggested reading: lecture notes 5.5.1-5.5.4, Lecture 32.