Final Exam Study Guide

The final exam is on **Sunday, November 24 3pm-6pm** in **Location: Kemeny 007**. The final exam is worth 35% of your final grade. The exam will be cumulative, but new material will be worth about 40% of the points.

My office hours for the final week are listed below. Also, feel free to email me at samantha.g.allen@dartmouth.edu or message me via Canvas.

- Tuesday (11/19) 1:30-3:30pm,
- Friday (11/22) 1:30-2:30pm.

Below is a list of topics that will be covered on the final exam. Please refer to the Syllabus on the webpage for "Suggested Practice" problems. I have listed a few additional (and occasionally more challenging) practice problems with each chapter below.

- Chapter 1:Divisibility, GCDs and LCMs, the Euclidean algorithm Bezout's Identity, solving linear Diophantine equations
  Practice: Prove Corollary 1.11. Exercise 1.12, 1.13, 1.14, 1.15.
- Chapter 2: Facts about prime numbers, GCD, and prime factorization. There are infinitely many primes. An integer $n > 1$ is composite iff it is divisible by some prime $p \leq \sqrt{n}$. Divisibility tests (i.e. when is a number divisible by 3?)
  (We did not cover the material on p. 21. You will not be tested on the material from Corollary 2.7 through Exercise 2.5. We did not cover Section 2.3)
  Practice: Prove Corollary 2.2. Exercise 2.1, 2.2, 2.3, 2.11, 2.12.
- Chapter 3: Modular arithmetic, least nonnegative/absolute value residues, solving linear congruences, Chinese Remainder Theorem.
  (We did not cover p.44-46 or Sections 3.4 and 3.5.)
  Practice: Exercise 3.2, 3.7, 3.8, 3.9

- Chapter 4: Lagrange's Theorem, Fermat's Little Theorem, Wilson's Theorem. The base a test and successive squaring. The existence of pseudoprimes and Carmichael numbers and what they are counterexamples to. (You do not need to be able to prove anything about them.)
  (We did not cover Section 4.3.)
  Practice: Prove Corollary 4.5. Exercise 4.2, 4.3, 4.7, 4.10.
- Chapter 5: Units, multiplicative inverses, and the group U_n. Euler's $\phi(n)$ function and its many properties. Euler's Theorem.
  (We did not cover Section 5.3.)
  Practice: Prove Lemma 5.1. Exercise 5.6, 5.8, 5.9, 5.22.

- RSA Encryption Algorithm: Not covered on the exam.
- Chapter 6: Orders of elements in U_n, primitive roots, which U_n are cyclic. Solving congruences using primitive roots.
  (We did not cover Sections 6.7 and 6.8.)
  Practice: Prove Lemma 6.4. Exercise 6.1, 6.4, 6.5, 6.25, 6.26.

- Chapter 7 (through Exercise 7.12 on p. 132): The set of quadratic residues Q_n. Given an element of Q_n, how many values in U_n square to it? What is $|Q_n|$? Varius other facts about Q_n. The Legendre symbol: definition, computation, and varius theorems. Euler criterion. Gauss's Lemma. The law of quadratic reciprocity.
  (We did not cover the proof of quadratic reciprocity or Sections 7.5 and 7.6.)
  Practice: Show that Q_n is closed under multiplication. Prove Lemma 7.3. Prove Theorem 7.5. Exercise 7.4, 7.5, 7.6, 7.9, 7.11, 7.12.
- Chapter 8: Arithmetic and multiplicative functions. Examples $\phi, \tau, \sigma, \sigma_k$. Lemma 8.1. What is a perfect number? What is a Mersenne prime? Theorem 8.4. The Mobius function (inductive definition and later theorem based on prime factorization). The Mobius inversion formula theorem.
  (We did not cover Section 8.4, we covered some of Section 8.6, but you will not be tested on it.)
  Practice: Prove Lemma 8.1. Exercise 8.1, 8.3, 8.4, 8.5, 8.7, 8.12. Compute $\mu(n)$ using the inductive definition for some (moderately-sized) values, then verify them using Theorem 8.8.
- Chapter 9: You will not be tested on this material.
- Chapter 10: Identifying values as sums of 2, 3, or 4 squares (or 5 squares or 6 squares or ...). S_2 and S_4 are closed under multiplication.
  (We only covered 10.1, 3, 4)
  Practice: Choose some random values and decide if they are sums of 2, 3, or 4 squares. Carefully read the proof of Theroem 10.2. Exercise 10.3, 10.12.
- Chapter 11: Fermat's Last Theorem. Facts and proofs about Pythagorean triples, primitive pythagorean triples, and Fermat's method of descent. Identifying primitive pythagorean triples.
  (We covered 11.1-5 through the end of the proof on p. 224).
  Practice: Exercise 11.2, 11.3, 11.4, 11.5, 1.6, 11.8.