Math 255 - Spring 2017
Final Exam Information

The Final Exan will be in our usual classroom (Votey 254) on Thursday May 11 between 10:30am and 1:15pm. It is cumulative, with some emphasis on the material of Chapter 9.

Please note this important Final Exam University policy:

> Students who are absent from a final exam for any reason must report that fact and the reason, in writing[1], to their instructor within 24 hours. If the absence is due to any situation beyond the reasonable control of the student (e.g., illness or family tragedy), the instructor must provide the student with the opportunity to complete the course requirements. At the instructors discretion, this may be an exam or some other suitable project. The instructor may require evidence in support of the student's reason for absence.

Please read these instructions carefully, as not heeding them will constitute a breach of the UVM Code of Academic Integrity:

- You may not use a calculator or any notes or book during the exam.
- You may not access your cell phone during the exam for any reason; if you think that you will want to check the time please wear a watch.
- The work you present must be your own.
- Finally, you will more generally be bound by the UVM Code of Academic Integrity, with which you should familiarize yourself if you haven't already.

You will be asked to acknowledge that you have read these instructions on the first page of the exam.

For each problem, you should write down all of your work carefully and legibly to receive full credit. For each question, you should use theorems and/or mathematical reasoning to support your answer, as appropriate.

To help you study for this exam:

- Solutions to the Review Homework will be posted online on Monday May 8 around the end of the day (please feel free to email me if I forget).
- Office hours will be held on Friday May 5 from 10:30 to 11:30am and 4 to 5pm, as well as Monday, Tuesday and Wednesday May 8, 9 and 10, from 1 to 3pm. I will also be available on Piazza during the week.
- Conceptually it might help you to think of the exam as having "two parts." The first part is a review of the material covered by Exams 1 and 2. This will cover the main ideas of this part of the class. To prepare for this part of the exam you should
  - Work the Review Homework
  - Review Exams 1 and 2 from this semester

  The second part is comprehensive coverage of the material of Chapter 9, which is what we have been doing since Exam 2. This material will be covered in greater depth. To prepare for this part of the exam you should
  - Work the problems suggested between April 14 and May 5, as well as the quizzes administered during those dates. Answers to selected suggested problems have been posted on our course website. **Solutions to other problems will not be posted,** although I will answer any question you have on Piazza.

[1] Email is fine.

- Review Homework 10 and 11
- Work the Review Homework

Please note that I might not answer questions after 11pm on Wednesday May 10, at my discretion.

Things that could be on the Final Exam:

- As usual you may be asked to state theorems or definitions, or to decide if a conclusion follows from a theorem. More precisely:
  - Given any theorem (even one we have not studied!), state the hypotheses and the conclusion of the theorem and determine if the theorem can be applied to reach a certain conclusion.
  - You may be asked to state (and use!) an important theorem from class. Those are: the Division Algorithm (Theorem 2.1), the Fundamental Theorem of Arithmetic (Theorem 3.2), the Chinese Remainder Theorem (Theorem 4.8), Fermat's Little Theorem (Theorem 5.1) and its Corollary on page 88, Wilson's Theorem (Theorem 5.4), The Big Theorem (Theorem 6.4), the Möbius Inversion Formula (Theorem 6.7), Euler's Theorem (Theorem 7.5), Euler's Criterion (Theorem 9.1) and its Corollary on page 172, and Quadratic Reciprocity (Theorem 9.9).
  - Even though you might not have to state them, you might need to use one of the following theorems: Theorem 2.9, the primality test from Section 3.2, Theorem 4.7 and its Corollary on page 77, Theorem 6.1, Theorem 8.1, Theorem 8.2 and its Corollary on page 149, Theorem 8.11, Theorem 9.2, the Corollary on page 177, Theorem 9.6, Theorem 9.11 and its expanded version from class, Theorem 9.12 and its expanded version from class, and Theorem 9.13.
  - You may be asked to give (and use!) the definition of: divisibility, the greatest common divisor (either the book definition or Theorem 2.6), relatively prime, prime number (either the book definition or Theorem 3.1), unit, zero divisor, inverse of a number, congruence modulo n, multiplicative function (Definition 6.2), Möbius's μ-function (Definition 6.3), Euler's φ-function (Definition 7.1), the (multiplicative) order of an integer modulo n (Definition 8.1), primitive root of an integer n (Definition 8.2), the discrete logarithm in base r of an integer a modulo n ($\log_r a$, Definition 8.3, although the book uses the notation $\operatorname{ind}_r a$ for the same quantity), quadratic residue and nonresidue (Definition 9.1), and Legendre symbol (Definition 9.2).
  - You may be asked to explain or use the Euclidean Algorithm.
- You should be able to compute the inverse of a number modulo n, if it exists, be able to solve a linear congruence (as in the proof of Theorem 4.7, say), compute the order of an integer a modulo n if $\gcd(a, n) = 1$, and compute $\log_r(a)$ in $\mathbb{Z}/n\mathbb{Z}$ if r is a primitive root of n and $\gcd(a, n) = 1$.
- The rest of the exam will consist of various computations, problems and proofs. To solve those you should:
  - Carefully review our Exams 1 and 2, as well as Homework 10 and 11. Blank copies of the exams and complete solutions for all problems can be found online.
  - Solve all of the suggested problems as well of the quizzes assigned between April 14 and May 5.
  - Solve the Review Homework.

  Several questions will be substantially similar or identical to questions coming from these sources.
- As far as last year's final exam is concerned, note that Problem 13 was assigned this year as a homework problem, but it was not assigned last year. You should expect our last exam problem to be a problem you have not seen before, but one you have all of the tools to solve.

You will not be given any formulae for the exam.