Math 255 - Spring 2017
Exam 2 Information

Exam 2 will be in class on Wednesday April 12. It will cover the material covered in class between March 3 and April 7, inclusively. By necessity, it will cover some material from earlier in the semester, but it is not a cumulative exam.

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.

Things that could be on Exam 2:

- Given any theorem (even one we have not studied!), state the hypotheses and the conclusion of the theorem, determine if the theorem can be applied to reach a certain conclusion.
- Any proof or problem that is identical or substantially similar (same but with different numbers say) to a problem that was assigned on Homework 6, 7, 8 or 9 or in the problems suggested between March 3 and April 7, inclusively. All homework solutions are posted on our course website. 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.
- State and use any one of these important theorems/algorithms we have seen: Fermat's Little Theorem (Theorem 5.1) and its Corollary on page 88, Wilson's Theorem (Theorem 5.4), Theorem 6.1, Theorem 6.2, Theorem 6.3, The Big Theorem (Theorem 6.4), Theorem 6.5, Theorem 6.6, Möbius Inversion Formula (Theorem 6.7), Theorem 7.2, Theorem 7.3, Euler's Theorem (Theorem 7.5), Theorem 8.1, Theorem 8.2 and its Corollary on page 149, Theorem 8.4, and Theorem 8.11.
- Give the definition of: the τ and σ functions (Definition 6.1), 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).
- Some past theorems that are likely to come up again are the Division Algorithm (Theorem 2.1), the Euclidean Algorithm, the Fundamental Theorem of Arithmetic (Theorem 3.2), Theorem 4.7 and the Chinese Remainder Theorem (Theorem 4.8). Some definitions that are likely to come up again are 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, and congruence modulo n. You should also be able to compute the inverse of a number modulo n, if it exists, and be able to solve a linear congruence (as in the proof of Theorem 4.7, say).
- As far as Exam 2 from Spring 2016 is concerned, there will be no question like problems 2 and 4, since we covered these on Exam 1 this year (although finding multiplicative inverses and using the Chinese Remainder Theorem could come up this year on Exam 2). In problem 5, don't mind the function λ; you should be able to solve the problem even without the hint.

You will not be given any formulae for the exam.