

Dr. Charles Rocca
Higgins 102B
roccac@wcsu.edu
<http://sites.wcsu.edu/roccac/>

MAT 599: Applications in Number Theory
Meeting Times TBA

Office Hours:
TBA

Course Materials:

Textbook: *Elementary Number Theory & Applications* by Kenneth Rosen

Course Description:

This is a continuation of MAT 528: Number Theory. This course will focus on applications of Number Theory to factorization, primality testing, and cryptology. We will emphasize both theoretical understanding and basic implementation. Students will need to complete text exercises, programing exercises, and will be expected to present some content themselves as a demonstration of their ability to learn independently.

Course Objectives:

After successful completion of this course a student will be able to demonstrate:

- familiarity with factorization algorithms and knowledge of their theoretical underpinnings;
 - familiarity with methods for primality testing and knowledge of their theoretical underpinnings;
 - familiarity with encryption algorithms and knowledge of their theoretical underpinnings;
 - an ability to implement the above algorithms using a CAS or the PYTHON.
-

Course Content:

Unit	Chapter(s)
Review Critical Theorems	4, 6 & 7
Primality Testing, Primes, and Pseudoprimes	3.6, 4.6, 6.2, 7.4, 9, 11, & 12
Cryptographic Algorithms:	8 & 10

Grading:

Assignments	50%
Presentations	25%
Implementations	25%

Assignments: Complete some subset of selected problems from the text including some programming exercises.

Presentations: Present key theorems and algorithms in detail and with examples.

Implementations: Demonstrate an ability to implement algorithms using a CAS such as Maple, Mathematica, or SAGE, or using a programming language such as PYTHON.

Classroom Policies:

Assignment Guidelines: Out of class assignments should always look *neat, legible, and professional; they must be written on loose leaf college ruled paper or be typed*. Messy work, work on crumpled papers, or on paper torn from a notebook with “frillies” will be rejected and counted as late. Whenever appropriate answers on all assignments should be given in *complete sentences*. I will almost always accept late work. An assignment is considered late after I have handed it back or gone over it in class. Late assignments will receive at most 75% credit.

Exam Makeup Policy: To qualify for a makeup exam you must present evidence of a valid reason for missing the exam and, if at all possible, contact me ahead of time to make arrangements for the makeup. If you do not present a valid reason, do not give prior notice when possible, or simply do not show up for an exam, you are not entitled to a makeup and will not be given one. Finally, if you fail to show up for your makeup exam at the agreed upon time you will not be given a second opportunity under any circumstances.

Time on Task: Please note that for all your classes you should be spending at least 2 hours working outside of the class for every 1 hour in the class. Note that this is an average, if you are weak in the subject or under prepared you will need to spend more time on the class.

Attendance: There is no specific policy for attendance in this course. However please keep the following in mind:

- if you have three consecutive unexcused absences I am required to report to the University that you have stopped attending,
- while most of the dates and assignments for the course will be posted on the website occasionally small assignments or quizzes will only be announced in class.

Therefore, you should try to make every effort to attend all the classes.

Academic Honesty: If on any assignment, quiz, or exam you turn in someone else's work as if it were your own you will receive a zero on that assignment, quiz, or exam. If you are caught doing this three times you will receive an F in the course and the Dean will be informed of your academic dishonesty.

(WCSU Honesty Policy: <http://www.wcsu.edu/facultystaff/handbook/forms/honesty-policy.pdf>)

Accommodations: If you have need of an accommodation for testing or note taking, please visit AccessAbility Services, located in Higgins Annex 017 (<http://www.wcsu.edu/accessability>). They will give you an accommodation letter which you must bring to me as soon as possible.