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

MAT 467/528 - 41: Number Theory
MW: 5:30-9:15 in HA 213

Office Hours:

MW: 4pm to 5pm

Course Materials:

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

---

Course Objectives:

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

- demonstrate familiarity with the principle definitions and theorems of elementary number theory.
- prove foundational theorems such as (though not limited to) *The Division Algorithm*, *Fundamental Theorem of Arithmetic*, *Euler's Theorem*, *Wilson's Theorem*, *Chinese Remainder Theorem*, etc.
- solve basic problems involving modular arithmetic and systems of linear equations.
- exhibit knowledge of some applications of number theory.

Course Content:

Unit	**Chapter(s)**
Integers, Primes, Congruences	3 & 4
Basic Applicaitons	5
Number Theoretic Functions:	6 & 7
Cryptology, Primality Testing, and Pseudo-Random Numbers:	Selections from 8, 9, & 10

Course Calendar:

Monday	Wednesday
5/22 **1** Syl., Intro., & Primes, GCD's, Fundamental Theorem of Arithmetic	5/24 **2** Euclidean Algorithm and Modular Arithmetic
5/29 Memorial Day - No Class	5/31 **3** Solving Modular Equations
6/5 **4** Basic Applications	6/7 **5** Theorems of Wilson, Fermat, & Euler and Number Theoretic Functions
6/12 **6** More Number Theoretic Functions and Möbius Inversion	6/14 **7** Primitive Roots & Primality Testing
6/19 **8** Pseudorandom Numbers & Cryptosystems	6/21 **9** Fundamentals Exam

Grading:

Assignments	60%
Fundamentals Exam	40%

Assignments: You will be given about ten problems from the text for each chapter. Some of these will be practice of algorithms covered in class, but others will be problem solving exercises which require more creativity. You will want to start these problems early. You may work in pairs or in groups of up to three. If you work with someone on the assignment then only hand in one copy of the work.

Fundamentals Exam: The purpose of this exam is to ensure you have mastered foundational material. You will need to state and prove some theorems and demonstrate proficiency with basic algorithms as follows:

Definition and Theorem Statements:

- Well Ordering Principle
- Principle of Mathematical Induction
- Divisibility
- Division Algorithm
- Modular Equivalence
- Fundamental Theorem of Arithmetic
- Chinese Remainder Theorem
- Wilson's Theorem
- Fermat's Little Theorem
- Euler's Theorem
- Euler's ϕ-function

Theorem Proofs:

- Fundamental Theorem of Arithmetic
- Chinese Remainder Theorem
- Wilson's Theorem
- Fermat's Little Theorem or Euler's Theorem
- Basic properties of divisibility and/or modular arithmetic
- Basic example of proof by induction

Computations:

- Euclidian Algorithm
- Writing G.C.D. as a linear combination
- Linear Diophantine equations
- G.C.D. and L.C.M. using the Fundamental Theorem of Arithmetic
- Multiplicative inverses modulo an integer m
- Solve a linear congruence equation
- Solve a system of equations using the Chinese Remainder Theorem
- $\phi(n)$ for various $n \in \mathbb{N}$

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. In particular ***for this class you should be doing 15 hours of work a week not including class time***. 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.