Dr. Charles Rocca
Higgins 101D
roccac@wcsu.edu
http://sites.wcsu.edu/roccac

MAT 428/528 : Number Theory
MW: 5:30 am - 9:15 pm,
Higgins 124

Office Hours:

- TWR: 1 pm - 2 pm
- or by appointment

Text:

Textbook: *Elementary Number Theory & its Applications, 6th edition* by Kenneth Rosen

Course Description and Objectives:

This course will give a broad overview of the fundamental ideas in number theory and examine a handful of applications.

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

- Demonstrate knowledge and understanding of definitions which are fundamental to number theory,
- Construct an outline showing how ideas build throughout the subject with advanced topics and applications depending on solid foundational understanding,
- Prove or outline the proofs of theorems central to the study of number theory such as the Division Algorithm, the Fundamental Theorem of Arithmetic, and the Chinese remainder Theorem, and
- Illustrate how number theory may be applied to solving algorithmic problems.

Course Content:

"Unit"	**Chapter(s)**
Integers, Primes, Congruences	3 & 4
Basic Applicaitons	4 & 5
Number Theoretic Functions:	6 & 7
Cryptology:	8
Primitive Roots & their Applications:	Selections from 9, & 10

Grading:

Assignments	60%
Quizzes	20%
Fundamentals Exam	20%

Assignments: You will be given four or five problems from the text for each chapter. Four of these problems will focus on basic understanding an algorithmic knowledge the other(s) will require you to demonstrate deeper understanding and 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.

Quizzes: Each day you will have a quiz with four or five questions to check your understanding from the previous class. Quizzes will focus exclusively on algorithms and definitions.

Fundamentals Exam: The purpose of this exam is to ensure you have mastered foundational material. You will need to state (and for graduate students prove) some theorems and demonstrate proficiency with basic algorithms we have studied. Below is a listing of the content on the exam.

Definition and Theorem Statements:

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

Computations:

- Euclidian Algorithm
- Write the 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 $n \in \mathbb{N}$

Theorem Proofs:

- Bezout's Theorem
- 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

Course Calendar:

Monday	Wednesday
6/20 **1** Syl. & Intro. Divisibility, Well Ordering Principle, Division Algorithm, Greatest Common Divisor, Bezout's Theorem, Euclidean Algorithm, Fundamental Theorem of Arithmetic	6/22 **2** Modular Equivalence and Arithmetic, Zero Divisors, Invertible Elements, Bezout Again, Basic Linear Equations, Chinese Remainder Theorem
6/27 **3** Linear Diophantine Equations, Polynomial Equations, and Linear Systems	6/29 **4** Fermat's Factorization, Pollard's ρ-Factorization, Divisibility Tests, and Hash Functions
7/4 July Fourth - No Class	7/6 **5** Theorems of Wilson, Fermat, and Euler, Euler's ϕ-Function and Other Number Theoretic Functions ($\sigma,\ \tau,\ \&\ \mu$), and Möbius Inversion
7/11 **6** Applications of Number Theory to Cryptology	7/13 **7** Primitive Roots and Primality Testing
7/18 **8** Pseudorandom numbers, ElGamal Cryptosystem, and Review	7/20 **9** Fundamentals Exam

Course Outline:

MAT 467/528: Number Theory

1. Divisibility and Prime Factors
   (a) Definition of Divisibility
   (b) Well Ordering Principle
   (c) Division Algorithm
   (d) Greatest Common Divisor
      i. Definition
      ii. Bezout's Theorem
      iii. Euclidean Algorithm
      iv. Relation to the Least Common Multiple
   (e) Fundamental Theorem of Arithmetic
2. Modular Arithmetic
   (a) Definition of Modular Equivalence
   (b) Equivalence Relations and Classes
   (c) Modular Arithmetic
      i. Consistency of Modular Arithmetic
      ii. Units and Zero Divisors
      iii. Quadratic Residues
   (d) Solving Modular Equations
   (e) Chinese Remainder Theorem
3. Number Theoretic Functions
   (a) Euler's ϕ-Function (the totient function)
   (b) Wilson's, Fermat's Little, and Euler's Theorems
   (c) Multiplicative Functions (in the number theoretic sense)
      i. Euler's ϕ-Function (the totient function)
      ii. Sum of divisors function
      iii. Number of divisors function
      iv. Möbius Function and the Möbius Inversion Formula
4. Applications (suggested possible topics)
   (a) Divisibility Tests:
      i. Divisibility by Powers of 2
      ii. Divisibility by 3 and 9
      iii. Divisibility by 7 or 11
      iv. Divisibility in Base b
   (b) Factorization Algorithms:
      i. Fermat Factorization
      ii. Pollard Rho Factorization
   (c) Primality Testing:
      i. Fermat
      ii. Miller
      iii. Lucas
      iv. Proth
   (d) Applications to Computer Science
      i. Hash Functions
      ii. Check Sums
      iii. Pseudo Random Number Generation
      iv. Cryptographic Protocols

You and Your Grades:

- "A" (Exceptional) range 90% to 100%:
  The student has demonstrated significant mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve standard formulaic exercises and most nonstandard problems which require deeper insight.
  - "A" $\iff 92.5\% \leq Grade \leq 100\%$
  - "A-" $\iff 90\% \leq Grade < 92.5\%$
- "B" (Good) range 80% to 90%:
  The student has demonstrated mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve standard formulaic exercises and some nonstandard problems which require deeper insight.
  - "B+"$\iff 87.5\% \leq Grade < 90\%$
  - "B" $\iff 82.5\% \leq Grade < 87.5\%$
  - "B-"$\iff 80\% \leq Grade < 82.5\%$
- "C" (Adequate) range 70% to 80%:
  The student has demonstrated adequate mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve most standard formulaic exercises but struggles with nonstandard problems which require deeper insight.
  - "C+"$\iff 77.5\% \leq Grade < 80\%$
  - "C"$\iff 72.5\% \leq Grade < 77.5\%$
  - "C-"$\iff 70\% \leq Grade < 72.5\%$
- "D" (Inadequate) range 60% to 70%:
  The student has demonstrated inadequate or incomplete mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve some standard formulaic exercises but few if any nonstandard problems which require deeper insight.
  - "D+"$\iff 67.5\% \leq Grade < 70\%$
  - "D" $\iff 62.5\% \leq Grade < 67.5\%$
  - "D-" $\iff 60\% \leq Grade < 62.5\%$
- "F" (Unacceptable) below 60%:
  The student has demonstrated essentially no mastery of the appropriate knowledge and skills relevant to the course. The student is unable to solve most standard formulaic exercises and essentially no nonstandard problems which require deeper insight.

End User Agreement:

General Expectations: As a student in this class you are expected to:

- attend class and take notes,
- actively read material in each section, taking notes,
- review your notes on a regular basis,
- check your university email every day,
- check the class site ***at least*** every other day,
- begin studying for exams in a timely fashion,
- ask questions early and often,
- attend office hours,
- seek help in the math clinic or tutoring center, and
- complete assignments and readings on time.

Assignment Guidelines: (These apply to ***all out of class work***.)

- Work handed in must always look neat, legible, and professional. Work must be very neatly written or preferably typed. The quality of your work will be factored into your grade, up to 10%, in extreme cases work may be rejected and then counted as late.
- Answers on all assignments should be given in complete sentences. I should be able to tell what your answer means without re-reading the problem. This does not mean you simply rewrite the question.
- An assignment is considered late after I have handed it back or gone over it in class. Late assignments are accepted but may receive at most 75% credit. Late assignments go to the absolute bottom of the stack of papers to be graded; ***all on time work is graded before any late work.***
- If you work on an assignment as part of a group, then there may be no more than three individuals in the group and all your names must be on the assignment. You should hand in only one copy of the work.
- All work must be submitted in the manner directed.

Email Etiquette Guidelines: When sending an email you must include the course number and semester in the subject line. For example, if you are taking MAT 314 in Fall 1592 then the the subject line should begin with "[MAT 314 Fall 1592]." Also, you should always begin with a salutation such as "Dear Dr. Rocca" and end with a closing such as "Sincerely, I. Newton."

Exam Makeup Policy: To qualify for a makeup exam you must have a valid reason for missing the exam and, if at all possible, let me know ahead of time that you are missing the exam. You will need to meet with me in order to arrange a time for the make up exam. If you do not have 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. If you fail to show up for your makeup exam, you will not be given a second opportunity.

The 2% Exception: Any quiz or class work which is ultimately worth no more then 2% of your final grade can not be made up.

Time on Task: As a 3 credit class you should expect to average 14 to 21 hours of work a week including class time. Some weeks you may get away with less and some may require more.

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 within the first half of the semester I am required to report to the University that you have stopped attending.

Academic Honesty: If on any assignment, quiz, or exam you turn in someone else's work, regardless of the source, 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. (https://www.wcsu.edu/faculty-handbook/2019-2020/policies-pertaining-to-students/academic-honesty-policy/)

Accommodations: If you have need of an accommodation for testing or note taking, please visit AccessAbility Services, located in White Hall 005 (http://www.wcsu.edu/accessability).