Math 567: Modern Number Theory, Spring 2025

Course Details

Official Course Description: A course in number theory covering fundamentals and modern applications in topics of recent interest: modular arithmetic, quadratic reciprocity, arithmetic functions, zeta function, Diophantine equations, transcendental numbers, Roth's theorem, continued fractions, and the circle method. Optional material from probability including random matrix theory.

Instructional Modality: Classroom Instruction.

Meeting Time and Location: MoWeFr: 2:25pm–3:15pm, Van Vleck Hall, room B123.

Instructor: Mikhail Ivanov, Teaching Faculty, *Email:* mivanov@wisc.edu, *Office:* Van Vleck Hall B127.

Instructor Office hours: WF: 3:30pm–4:20pm in Van Vleck Hall, room B224 (please check Canvas page for updates), or by Appointment.

Grader and/or Course Assistant: We will have a grader that has yet to be determined. Canvas page will be updated once they are assigned.

Credits hours: 3.

How Credit Hours are Met by the Course. This course meets the Traditional Carnegie Definition for how credit hours are met by the course. Students in the course have 2.5 hours/week of direct faculty instruction during class time and are expected to work on course learning activities (reading, writing, problem sets, studying, etc) for a minimum of 2 hours outside of classroom per course credit (i.e. 6 hours/week). The syllabus includes more information about meeting times and expectations for student work.

Course Designations and Attributes:
Breadth – Natural Science
Level – Advanced
L&S Credit – Counts as Liberal Arts and Science credit in L&S
Grad 50% – Counts toward 50% graduate coursework requirement
Honors – Honors Optional (%)

Requisites: MATH 541 or graduate/professional standing or member of the Pre-Masters Mathematics (Visiting International) Program

Course Learning Outcomes

By the conclusion of this course, students should have a thorough understanding of:

1. Recall and state the formal definitions of the mathematical objects and their properties used in the field of Number Theory (e.g., congruence, quadratic residue, arithmetic function, elliptic curves, etc.). Audience: Both Grad & Undergrad
2. Use such definitions to argue that a mathematical object does or does not have the condition of being a particular type or having a particular property (e.g., a number is transcendental, a continued fraction is positive, etc.). Audience: Both Grad & Undergrad
3. Recall and state the standard theorems of number theory. (e.g., quadratic reciprocity, Roth's theorem, etc.). Moreover, the student will be able to recall the arguments for these theorems and the underlying logic of their proofs. Audience: Both Grad & Undergrad
4. Use such theorems in the context of longer arguments by examining their premises (e.g., Applying the euclidean algorithm to show that rational numbers have a finite continued fraction expansion , etc.) Audience: Both Grad & Undergrad
5. Prove or disprove statements related to the above definitions, properties, and theorems using techniques of mathematical argument (direct methods, indirect methods, constructing examples and counterexamples, induction, etc.). Audience: Both Grad & Undergrad
6. Convey arguments using English with appropriate mathematical terminology and notation. Audience: Both Grad & Undergrad
7. Identify applications of course content in areas of modern research. Audience: Graduate

Course Overview

Number theorists study prime numbers as well as the properties of mathematical objects made out of integers (for example, rational numbers) or defined as generalizations of the integers (for example, algebraic integers). Being one of the oldest branch of math, Number Theory can be dated back to ancient Greece where people studied integer solutions of the Pythagorean equation and proved there are infinitely many prime numbers. Despite its long history, Number Theory is still going through huge progress in the 20th centuries with important applications to computer science, especially to cryptography discovered. It is the mathematics that is hidden behind bitcoin.

The class will be a beginner's guide to number theory. We will go over the very basics trying to go more wide than deep. Background knowledge in Math 541 (Modern Algebra) will be helpful but will not be used extensively.

Tentative Course Schedule

We will cover Chapter 1, 2, 3, 4, 5 and 6 of the textbook, roughly 2 weeks per chapter, possibly supplemented by extra materials, for example Diophantine equations or more cryptography if time permits.

Chapter 1, Prime numbers: Definition of prime numbers, prime factorization (the fundamental theorem of arithmetic), counting primes.

Chapter 2, integers modulo n: Congruence modulo n, the Chinese Remainder Theorem, solving linear equations modulo n, the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$.

Chapter 3, Public key Cryptography: The Diffe–Hellman key exchange, the RSA algorithm, attacking RSA.

Chapter 4, Quadratic reciprocity: The statement of quadratic reciprocity, Euler's criterion, Gauss sums, finding square roots.

Chapter 5, Continues fractions: Finite and infinite continued fractions, continued fractions and diophantine approximation.

Chapter 6, Elliptic curves: the definition of elliptic curves, group law on elliptic curves, integer factorization using elliptic curves, elliptic curve cryptography.

Textbook, Course Website, Digital Tools and Other Course Materials

- Required textbook: William A. Stein, Elementary Number Theory: Primes, Congruences, and Secrets. This book is available for free from the author's website (https://wstein.org/books/ent/).
- Materials outside the textbook will be accompanied by notes and references.
- `Canvas` (`https://canvas.wisc.edu/courses/437769`) is our Learning Management System. All important course information will be relayed through Canvas. Make sure your Canvas notification setting for "Announcement" is "Notify immediately" so that you receive messages promptly. Notifications settings can be accessed here: `https://canvas.wisc.edu/profile/communication`.
- `Zoom`(`https://uwmadison.zoom.us`) will be used for remote office hours.
- `Gradescope`(`https://www.gradescope.com/`) will be used to grade homework and exams. Instructions will be shared later.
- `Piazza` (`https://piazza.com/class/m5x4f8wigls6o4`), the online discussion forum.

Class Components

Lectures. Lectures will be delivered in-person and synchronously three times a week during regular class hours. Lectures will involve some active learning components (e.g., problems and small group work). Attendance and active engagement is expected.

Piazza. The online discussion forum, known as `Piazza`, will be used to discuss ideas or questions outside of class. Piazza can be used to get hints on homework problems, but no one is allowed to post entire solutions to homework assignments. However, feel free to post entire solutions to practice problems. Logistic questions are usually better posted on Piazza rather than emailed to the instructor, so all students can benefit from the answer. (e.g., exam dates and locations). Please do not use email for math questions.

You can use private question in Piazza to communicate with Instructor about personal circumstances.

Any posts containing comments (either positive or negative) about the instructors, the class, the students, or anything else, will be deleted. Unprofessional conduct may result in disciplinary action.

Homework. Assignments will be posted on Canvas, and they will have to be submitted in Gradescope as a single pdf file. Written assignments will be several questions long and will be assigned weekly usually due roughly every Wednesday. Please make sure all pages are in the right orientation when you convert them. Do not hand in your rough draft or first attempt. Papers that are unreadable or disorganized cannot be graded. It is a good habit to download your submission every time and check everything is fine.

Collaborating with other students on the homework is encouraged, but you must write up all reasoning and solutions on your own (in other words, no copying). Failure to abide by this guideline could be construed as a form of academic dishonesty.

Each problem should be completed with neat, understandable, detailed solutions and explanations. Your explanations and proofs must be sound and rigorous, paying attention to detail and clarity. Computations without appropriate explanation will not receive credit, even if the final numerical answer is correct.

Late homework will generally not be accepted. Since it is quite likely that during the semester you will either experience a technical difficulty (e.g., missed the deadline, your computer shut down as you were submitting it, internet outage, etc) or a personal emergency (being sick, attending a funeral, etc), the two lowest HW scores will be dropped. You do not need to contact your instructor if such a situation does come up.

Usage of AI. You are welcome to use artificial intelligence (AI) tools and applications (such as Copilot, DALL-E, etc.) in this class as they support the learning objectives of this course. Please be aware you are responsible for the information you submit based on an AI query (i.e. ensure your professor has allowed you to publicly post course content such as assignment or assessment prompts and that the AI generated results do not contain misinformation or unethical content). Your use of AI tools must be documented and cited to conform to this course's expectations.

Mathematica. Mathematica and Wolfram—Alpha Pro are available at no charge to UW Madison students. They are useful for: (a) solving problems, (b) obtaining step-by-step solutions, and (c) writing programs with the assistance of Artificial Intelligence. (AI chat is built in.) To get access, go to www.wolfram.com/siteinfo and enter your University of Wisconsin email. (Here are click-by-click steps if you need them: wolfr.am/UWMadison) Learn how to use Mathematica at www.wolfram.com/wolfram-u/

Exams. The course will have three exams. We will have two evening Midterm Exams and a Final Exam, places to be scheduled by the University. Final Exam will be cumulative.

Midterm Exam 1	Wednesday, February 26	07:30PM–09:00PM
Midterm Exam 2	Wednesday, April 9	07:30PM–09:00PM
Final Exam	Friday, May 9	02:45PM–04:45PM

Students with academic or religious conflict with one of the exams should notify the instructor as soon as possible, and no later than the third week of the semester.

Calculator Policy. During an exam no books, notes, calculators, cell phones, pagers, or any electronic devices will be allowed.

Grading

In this course, you will be evaluated based on components described above with their corresponding percentages:

Homework	25%
Midterm Exam 1	25%
Midterm Exam 2	25%
Final Exam	25%

Grading Scale. The following grade lines are guaranteed in advance. A percentage score in the indicated range guarantees at least the letter grade next to it.

$$\text{A} \geq 90\% > \text{AB} \geq 88\% > \text{B} \geq 78\% > \text{BC} \geq 76\% > \text{C} \geq 66\% > \text{D} \geq 50\% > \text{F}$$

Final letter grades are not curved but the grade lines above may be lowered at the end. Class attendance is not part of the grading.

Graduate Level Course Attribute

This course have the Graduate Level Course Attribute. According to University Policy, such courses must hold graduate students to higher standards of learning than undergraduates in the same course. If you are graduate student you will have additional assignment which weight 10% of the overall course load.

Honors

Students pursuing an Honors degree may take this course for Honors Optional credit. Students should add or drop the Honors Option by following the steps outlined on the Honors Program website as soon as possible. To earn Honors credit in this course, students will be required to write an expository paper on a topic related to course material. More details on the requirements and rubric for this paper will be provided. Here are important policies for Honors Optional enrollment from the Registrar:

- The Honors project is not factored into your final letter grade. If you are enrolled for Honors and do not complete the Honors project in a satisfactory manner, however, your instructor will report a "Q" (Question) grade until the Honors designation is removed.
- Honors Optional is a way to earn general Honors credits and/or Honors breadth credits for Honors in the Liberal Arts. Honors Optional courses do not count toward Automatic Honors requirements.
- The deadline to add or drop Honors is the end of the twelfth week of the semester. Removing Honors after that deadline requires approval from the instructor and an L&S Academic Dean.
- You are responsible for removing the Honors Option from your enrollment if you decide to not complete the Honors Optional work.

How to Succeed in This Course

Here are a couple of suggestions for being successful in this class:

- The best way to learn math is by doing it. Try to work through the examples in the textbook before reading them, and try to solve as many practice problems as you can (on top of the homework problems). Let me know if you run out of problems to solve!
- Attend the lectures, and try to be active in class. Ask questions if something is not clear.
- Read the textbook.
- In general, try to keep up with the material. We cover several topics in the class that build on each other, and it will be hard to catch up if you get behind in the material.
- Use Piazza to ask questions related to the course material, and try to answer questions of other students if you can.
- Take advantage of the office hours! I am happy to help you, but I cannot do that if you do not ask for it.
- The Math Learning Center (in particular the Course Assistant and the Proof Table) could be a useful resource.

Campus Resources for Academic Success

- University Health Services
- Undergraduate Academic Advising and Career Services
- Office of the Registrar
- Office of Student Financial Aid
- Office of Student Assistance and Support
- Graduate Student Services

Academic Policies and Statements

- Academic Calendar and Religious Observances
- Academic Integrity Statement
- Accommodations for Students with Disabilities
- Course Evaluations
- Diversity and Inclusion Statement
- Mental Health and Well-Being Statement

- Privacy of Student Records and the Use of Audio Recorded Lectures Statement
- Students' Rules, Rights and Responsibilities
- Teaching and Learning Data Transparency Statement