

MA 350 NUMBER THEORY SYLLABUS

Class time: Monday, Wednesday, Friday 1-2 PM

Instructor: Joshua Zelinsky

Office Hours Monday – Friday, 2:10 PM to 3:30 PM or by appointment

Contact: joshuaz1@iastate.edu

Textbook: Kenneth H. Rosen, *Elementary Number Theory*, Pearson (6th Ed.) 2011.

Course Objectives: Math 350 is the first course in Number Theory for the mathematics majors. It covers common topics such as congruences and modular arithmetic, multiplicative functions, primitive roots, quadratic residues, and continued fractions from an elementary number theory perspective. The course will focus on algebraic rather than analytic number theory. As you will see in the lecture schedule below, you will learn selected topics from Chapters 1-4, 6, 7, 9, 11, and 12 of the text as well as a small number of topics from outside the text. You are encouraged to read the remaining chapters, especially Chapters 5 and to use computers to do number theory;. The text contains important basics of numbers, both classical and modern, and at the same time, both pure and applied.

Prerequisites and Expectations: As it is an introductory course, there are no particular requirements other than some level of mathematical maturity and an ability to write and understand proofs. However, this course does require considerable work as you will learn material which is new to you. You should be devoting at least 6 to 8 hours a week outside of class—reading the textbook, comprehending the new concepts and notions, thinking about the proofs, ideas and techniques, discussion with classmates, and completing all the assigned homework problems. It is expected that you will read the book as not everything you should learn and know will be discussed in class. Regular attendance and participation in class activities are the prerequisites for success.

Course Grade Course Grading will be determined out of a total of 400 points. There will be ten homeworks, each worth ten points (for a total of 100 points, 25% of the grade), three in class exams, each worth 50 points (for a total of 150 points, 37.5 % of the grade), a final worth 100 points (25 % of the grade), a project worth 40 points (10 % of the grade), and in class participation and attendance being 10 points (worth 2.5 % of the grade). The percent grades will translate into final grades as follows: At least 325 will guarantee an A-, at least 275 points will guarantee at east a B-, 225 points will guarantee at least a C- and 200 points will guarantee at least a D+. Plus or minus break downs will be made further based on the final end of semester curve. The above are only minimums: it is possible that the these minimums will be curved downwards. Additionally, if one is on the border between grades, other considerations such as apparent effort may be taken into account.

Exams There will be three in-class exams during the semester, each worth 50 points, and a final exam, worth 100 points (see the accompanying schedule). A make-up exam for missing exam due to an extenuating circumstance must be arranged with the instructor according to the departmental and school-wide policies on excusable absences. Please see <https://dept.math.iastate.edu/syllabus-and-class-policies/>

University mandated makeups are given for the following reasons (official documentation must be given upon request and when possible requests must be made at least 10 days in advance):

- (1) Extra curricular activities as a representative of Iowa State University (e.g., sponsored sports, band, etc.).
- (2) Armed forces deployment (e.g., ROTC, military duty).
- (3) Officially mandated court appearances (e.g., jury duty).

In addition, makeups are possible for additional reasons where the accommodations are reasonable and sufficient advance notice is given (at least 10 days when possible). Such makeup exams usually fall into one of the following categories:

- (1) Medical situation for the student or medical emergency of family members.
- (2) Conflict with religious practices and/or observances.

Homework: Mathematics is not a spectator sport; the best way to learn math is to do math. Accordingly, there will be ten homework sets and they will be assigned mostly weekly. Each set of homework problems will be assigned in advance, and collected about a week later according to the schedule (refer to the calendar below). Each set will be worth 10 points. Assignments may be submitted early but they will not be accepted if more than four days are passed from the due date. Each day late will result in 2 points subtracted from the grade. Homework will generally be returned 1-2 weeks after it has been collected. Your work on any assignments or solutions on homework should be well-presented in good English. It is acceptable and encouraged to work with your fellow students on homework, however any final write-up must be your own, and you must clearly indicate what ideas are yours.

Projects: Number theory is a topic which has many famous problems which are easy to state but are hard to solve or are still unsolved. Number theory also has some fascinating applications in modern technological contexts. The project will consist of a three to six page report on a topic of your choice. Possible topics include (but certainly are not limited to): Collatz's Conjecture, the Erdos-Strauss Conjecture, Fermat's Last Theorem, Hilbert's Tenth Problem, Goldbach's Conjecture, odd perfect numbers, primality testing, primes in arithmetic progression, quantum computing and Shor's Algorithm, the Riemann Hypothesis, twin primes and Polignac's Conjecture, and Schanuel's Conjecture. We will discuss projects before spring break and it is expected that project topics will be chosen by the end of the first week after break.

Classroom Expectations: It is expected that students will show up to class every class day. Being late is not in general acceptable. However, if one is running late, I would strongly prefer that you show up late rather than not show up. Electronics must be off during class time. This includes cell phones and laptops. Electronic pads are acceptable for taking notes with permission. It is important that you be involved in class, do any assigned reading before hand, and do any relevant homework assignments. Also, on occasion, a proof or example may not be finished in class and I will ask you to finish it on your own time; it is expected that such problems even when they are not assigned as homework will be completed.

Office Hours: Despite the elementary nature of the material covered in this class, there are many subtleties involved. In that context, showing up to office hours may be helpful. Additionally, I will generally have tea and cookies available in my office.

Class Schedule: The tentative course schedule is as follows:

Week 1: Divisibility (1.5), Representations of Integers (2.1), Prime numbers (3.1), Greatest common divisors (3.3).

Week 2: Euclidean algorithms (3.4), Fundamental Theorem of Arithmetic (3.5).

Week 3: Factorization (3.6), Linear Diophantine equations (3.7), Congruences (4.1).

Week 4: Linear congruences (4.2), The Chinese remainder theorem (4.3), Systems of linear congruences (4.5).

Week 5: Review for Exam 1. Exam 1 February 9

Week 6: Wilson's Theorem, Fermat's Little Theorem (6.1), Pseudoprimes (6.2).

Week 7: Euler's Theorem (6.3), Euler Phi-function (7.1). The sum and number of divisors (7.2), Average values of multiplicative functions*

Week 8: Perfect numbers and Mersenne primes (7.3), Mobius inversion (7.4), Partitions (7.5)

Week 9: Review for Exam 2. Exam 2 Friday March 9

Week 10: Primitive roots (9.1, 9.2), The existence of primitive roots (9.3), Index arithmetic (9.4), Project topics

Week 11: Public key cryptography and RSA (8.4) Diffie-Hellman key exchange and other cryptographic applications (8.6)

Week 12: Quadratic residues and nonresidues (11.1), Law of quadratic reciprocity (11.2).

Week 13: Jacobi symbols (11.3), Review for Exam 3. Exam 3 Friday April 13. Project drafts due.

Week 14: Decimal fractions (12.1), Finite continued fractions (12.2), Infinite, periodic continued fractions and infinite non-periodic continued fractions(12.3, 12.4),

Week 15: Gaussian integers (14.1, 14.2), Quadratic extensions*, Review for final. Projects due.

Final Exam Week

Topics marked with an asterisk above are topics which we will cover which are outside the textbook.

Academic Honesty: Any occurrence of cheating will be reported to the appropriate school authorities as per <https://www.studentconduct.dso.iastate.edu/academic-misconduct/armfacultystaff>. Cheating can result in a failing grade on a homework, exam, and or class. If you have concerns over what constitutes plagiarism or academic dishonesty, please speak to me.

Accommodations: This course complies with the Americans with Disabilities Act and Sect 504 of the Rehabilitation Act. If you have a disability and anticipate needing accommodations in this course, please read the Math Student Disability Accommodation Policy available at <https://iastate.app.box.com/s/c17d3ljul83lujr2j1mdeqoqcdqiva1t> and contact me as soon as you become aware of your need (even if you have not yet obtained all the documentation). Requests for accommodations that are retroactive to discussion with me may not be honored. You will need to obtain a SAN form with recommendations for accommodations from the Disability Resources Office, located in Room 1076 on the main floor of the Student Services Building. Please call them at 515-294-7220 or email disabilityresources@iastate.edu.

Discrimination and Harassment: Harassment and Discrimination: Iowa State University strives to maintain our campus as a place of work and study for faculty, staff, and students that is free of all forms of prohibited discrimination and harassment based upon race, ethnicity, sex (including sexual assault), pregnancy, color, religion, national origin, physical or mental disability, age, marital status, sexual orientation, gender identity, genetic information, or status as a U.S. veteran. Any student who has concerns about such behavior should contact his/her instructor, Student Assistance at 515-294-1020 or email dso-sas@iastate.edu, or the Office of Equal Opportunity and Compliance at 515-294-7612.