Lecture: (Sec 01) Monday-Wednesday-Thursday, 1:35pm–2:40pm, 119 Dodge.
(Sec 02) Monday-Wednesday-Thursday, 10:30am–11:35am, 130 Hurtig.

Instructor: Evan Dummit (he/him/his), 571 Lake Hall, edummit@northeastern.edu.

Instructor Office Hours: Monday noon–1:00pm and Monday/Thursday 3:00pm-4:00pm, or by appointment.

Course Webpage: https://dummit.cos.northeastern.edu/teaching_sp26_3527.html.

Course Textbook: The instructor will provide lecture notes for the course in lieu of an official textbook. For additional reference, Silverman's "A Friendly Introduction to Number Theory" covers topics at a similar level.

Course Philosophy: This course covers the fundamentals of elementary number theory from both the computational and the theoretical perspectives. Classically, number theory involved studying the integers $\mathbb{Z}$ and solving equations in integers, while the modern perspective on number theory generalizes and extends these ideas to other settings such as $\mathbb{Z}[i]$ (the Gaussian integers) and $F[x]$ (polynomials with coefficients from a field F). The primary theme of Math 3571 is to develop arithmetic inside $\mathbb{Z}$, and then explore the similarities and differences between $\mathbb{Z}$, $\mathbb{Z}[i]$, and $F[x]$. Due to the abstract nature of the material, Math 3571 is a proof-based course with an emphasis on problem-solving; correspondingly, many of the problems on the homework assignments and exams will ask for you to write proofs or explore examples.

At the end of the course, you will have a solid grasp of the arithmetic of the integers and how these properties extend to other number systems like the Gaussian integers and polynomials, along with some of their applications in other areas like cryptography. Success in this course thereby demands facility with the basic concepts, with the underlying theory, and with its applications.

Grades: Your course grade consists of **20% homework** and **80% exams**.

The homework score is the average of the written assignment scores, with the lowest score dropped.
The exam score is the maximum of [20% each midterm and 35% final] and [30% best midterm, 45% final].

An overall raw score of 92% will be **at least** an A, 90% will be **at least** an A-, 88% will be **at least** a B+, 82% will be **at least** a B, 80% will be **at least** a B-, 78% will be **at least** a C+, 72% will be **at least** a C, and 70% will be **at least** a C-.

If you feel that an assignment or exam has been misgraded, please talk to the instructor directly. Requests for regrading will not be considered more than two days past the date the assignment or exam was returned.

Exams: There will be two 1-hour midterm exams, along with a 2-hour final exam. If you miss an examination for any reason, you will receive a 0; make-up exams will not be given other than in exceptional circumstances.

The midterms are in class and scheduled for Thursday, February 19th and Monday, March 30th.

The final exam will occur during the final exam week, date and time TBA.

Homework: Written assignments will be assigned weekly and due via Gradescope by 11:59pm on the due date. **It is highly recommended to start work on the assignments early**: many problems will require substantial thought and effort to solve, even if the solution is ultimately fairly short. There is a **30-hour late period** during which assignments may still be submitted, possibly with a late penalty assessment. The lowest assignment grade is dropped, to provide you a cushion if an emergency arises and you cannot complete an assignment.

Problem sessions will be held weekly on Tuesdays and Fridays. The problem sessions provide you a place to work collaboratively on the homework assignments with help from the TAs. **It is highly recommended to start the assignments early**: many problems will require substantial thought and effort to solve, even if the solution is ultimately fairly short. **Do not fall into the trap of only starting the assignment the evening before it is due!**

Written assignments should be organized carefully, neatly, and in complete sentences, with concise well-reasoned logical arguments. Cite any external resources used, and clearly label all problems. If you collaborated with any other students, write the names of all collaborators on the top of your assignment. **Failure to adhere to any of these guidelines may result in point deductions, at the grader's discretion.**

Collaboration Policy: Mathematics is fundamentally a collaborative endeavor, and discussing the course material with others is an excellent way to solidify your own understanding. However, it is critical not to outsource your learning! You cannot expect to retain knowledge if you do not solve your homework problems yourself (e.g., if you relied on other people or on technology to explain how to do the problems). **On written assignments, you may work together with other people, but you must write up your work independently**.

Course Schedule: The course and lecture notes are organized into five chapters, as follows:

Weeks 1-2: Chapter 1 $\sim$ The Integers: The integers, induction, properties of arithmetic, greatest common divisors, the Euclidean algorithm, primes and prime factorization, rings and units

Weeks 3-5: Chapter 2 $\sim$ Modular Arithmetic: Modular congruences, modular arithmetic, Fermat's and Euler's theorems, the Chinese remainder theorem, repeating decimals

Weeks 6-8: Chapter 3 $\sim$ Cryptography: History of cryptography, Rabin and RSA cryptosystems, zero-knowledge protocols, primality testing and factorization algorithms

Weeks 9-13: Chapter 4 $\sim$ Unique Factorization and Applications: Integral domains, Euclidean domains, modular arithmetic in Euclidean domains, arithmetic in $F[x]$ and $\mathbb{Z}[i]$, finite fields, sums of two squares

Weeks 13-14: Chapter 5 $\sim$ Squares and Quadratic Reciprocity: Polynomial congruences and Hensel's lemma, quadratic residues and nonresidues, Legendre and Jacobi symbols, quadratic reciprocity and its applications

Resources and AI Policy: If you use **any** external resources (e.g., wikipedia, stackexchange, other books beyond the course text or notes, other people, etc.) you must say what results you are citing and where they are from. **If you happen to find a solution to an assigned problem online or elsewhere, it is plagiarism to present it as your own work without attribution of its source.**

Use of generative AI / large language models (e.g., ChatGPT, Copilot) or similar technology, is expressly prohibited in this course. This includes asking for hints or solutions to assigned problems, checking solutions, searching or summarizing course-related content, and outlining drafts of submitted work.

Although the course lectures and notes provide a basic introduction to the course material, you will not actually understand the ideas until you have used them to solve new problems yourself. **Using generative AI to assist with solving the homework problems thus short-circuits your learning**, because you will not have worked through the problems as fully as you should have. Additionally, while generative AI technology produces confident and authoritative answers, it in fact often makes mistakes both small and large.

The instructor reserves the right to require any student to explain any submitted work in person; failure or inability to do so satisfactorily will be considered evidence that the work is not your own. **If plagiarism or AI use is detected on an assignment, you will receive a warning and an automatic zero on the assignment. Another violation after the warning will result in an automatic F in the course.**

Attendance Policy: It is expected that you will attend every class. This course moves very fast, and it is quite possible to fall behind even if you only miss one day. If you miss class for any reason, it is highly advisable to consult the course lecture notes to catch up, and you may also wish to obtain notes from another student. It is your responsibility to be aware of all information announced in class, including modifications to the course syllabus or schedule, even if you are absent.

If you will be absent from a class activity due to a religious observance or practice, or for participation in a university-sanctioned event (e.g., university athletics), it is your responsibility to inform the instructor during the first week of class and provide appropriate documentation if required. Your instructor will work with you on alternative and reasonable arrangements for any time missed.

Statement on Academic Integrity: A commitment to the principles of academic integrity is essential to the mission of Northeastern University. Academic dishonesty violates the most fundamental values of an intellectual community and undermines the achievements of the entire University. Violations of academic integrity include (but are not limited to) cheating on assignments or exams, fabrication or misrepresentation of data or other work, plagiarism, unauthorized collaboration, and facilitation of others' dishonesty. Possible sanctions include (but are not limited to) warnings, grade penalties, course failure, suspension, and expulsion.

Statement on Accommodations: Any student with a disability is encouraged to meet with the instructor during the first week of classes to discuss accommodations. The student must bring a current Memorandum of Accommodations from the Office of Student Disability Services.

Statement on Inclusivity: Faculty are encouraged to address students by their preferred name and gender pronoun. If you would like to be addressed using a specific name or pronoun, please let your instructor know.

Statement on Evaluations: Students are requested to complete the TRACE evaluations at the end of the course.

Miscellaneous Disclaimer: The instructor reserves the right to change course policies, including the evaluation scheme of the course. Notice will be given in the event of any substantial changes.