Lecture: (Sec 01) Monday-Wednesday-Thursday, 1:35pm–2:40pm, Ryder Hall 217.
(Sec 02) Monday-Wednesday-Thursday, 10:30am–11:35am, Snell Library 031.

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

Office Hours: (Instructor) Wednesday-Thursday 3:00pm–4:15pm or by appointment, online via Zoom.
(TA Problem Sessions) Friday, time and location TBA (one session via Zoom, another in person).

Course Webpage: https://web.northeastern.edu/dummit/teaching_sp22_3527.html.

Course Textbook: The instructor will write lecture notes for the course (in lieu of an official textbook) as the semester progresses. The course will roughly follow the presentation from Silverman's "A Friendly Introduction to Number Theory", but it is not necessary to purchase the textbook for this course.

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 similarities and differences among $\mathbb{Z}$, $\mathbb{Z}[i]$, and $F[x]$.

Due to the abstract nature of the material, Math 3571 is a proof-based course with an emphasis on problem-solving. The style of the lectures and assignments reflect this philosophy: some time will be spent discussing theorems and their proofs, along with examples and applications that extend our understanding of the underlying concepts. Correspondingly, many of the problems on the homework assignments and exams will ask for you to write proofs or explore unusual examples (or counterexamples).

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 **30% homework**, **40% midterms**, and **30% final exam**.

The homework score consists of the average of the written assignment scores, with the lowest score dropped.

There will be two 1-hour midterm exams (20% each) and a 2-hour final exam (30%). The final exam is divided into two parts: Part A covers the material from the two midterms, while Part B covers the material after the second midterm. If your score on Part A is higher than at least one midterm score, it will replace the lowest midterm score (however, it can only replace one midterm).

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 common final exam.

If you miss an examination for any reason, you will receive a 0; make-up exams will not be given. A missed midterm will automatically be replaced by the score on Part A of the final exam.

The midterms are in class and scheduled for Monday, March 2nd and Wednesday, April 6th. The final exam is during the final exam week, time to be determined.

Homework Assignments: Written assignments will be assigned weekly and due via Canvas on Fridays by 11pm.

Problem sessions will be held weekly on Fridays. The problem sessions provide you a place to work collaboratively on the homework assignments with help from the TA. **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. Do not fall into the trap of only starting the assignment the evening before it is due!

The lowest assignment grade is dropped, to provide you a cushion if an emergency arises and you cannot complete an assignment. Assignments may be submitted late, but late submissions may be penalized at the grader's discretion.

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. All electronic submissions are expected to be easily readable. **Failure to adhere to any of these guidelines may result in point deductions, at the grader's discretion.**

Course Schedule: The course and lecture notes are tentatively 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 3-4: Chapter 2 $\sim$ Modular Arithmetic: Modular congruences, modular arithmetic, Fermat's and Euler's theorems, the Chinese remainder theorem, repeating decimals

Weeks 5-6: Chapter 3 $\sim$ Applications to Cryptography: History of cryptography, Rabin and RSA cryptosystems, Diffie-Hellman key exchange, zero-knowledge protocols, primality testing and factorization algorithms

Week 7: Midterm 1, covers chapters 1-2 and portions of chapter 3.

Weeks 8-11: Chapter 4 $\sim$ Unique Factorization and Applications: Integral domains, arithmetic in $F[x]$ and $\mathbb{Z}[i]$, modular arithmetic in Euclidean domains, finite fields, Fermat's theorem on sums of two squares

Week 12: Midterm 2, covers portions of chapters 3 and 4.

Weeks 12-14: 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

Week 15: Final exam, covers chapters 1-5.

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, whether because you relied on other people to explain to you how to do the problems, or because you relied too heavily on technological assistance.

On written assignments, you may work together with other people, **but you must write up your work independently**. 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 academically dishonest to copy the solution and present it as your own work.

Please also note that 70% of your course grade is determined by the exams, on which collaboration is not allowed.

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 Classroom Behavior: Disruptive classroom behavior will not be tolerated.

In general, any behavior that impedes the ability of your fellow students to learn will be viewed as disruptive. Examples of disruptive behavior include, but are not limited to, ringing cell phones, listening to an audio player during class, constant talking, eating food noisily, or laptop usage (except for note-taking).

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.