

Syllabus for Math 125

Codes and Connections: An Introduction to Number Theory

A "Ways of Inquiry" Course

Instructor: Oser

Office: Pierce Hall, 122A

Email: poser3@emory.edu

Phone: 4-4655

Location: Seney Hall 209

Class Time: MWF 1:15 – 2:20 PM

Office Hours: Math Center (in Pierce-Hall) 3-6PM; "Open door" policy at other times, and by appointment.

Required Texts/Resources: The majority of the required material for this course will be available at www.oxfordmathcenter.com under the tab labeled "Cryptography / Number Theory". In addition to this, students should have at their disposal a copy of *The Code Book* by Simon Singh and a scientific calculator that adheres to the order of operations (it need not be a graphing calculator, but these are welcome).

Course Description: Using secret codes, puzzles, and curious mathematical oddities as motivation, this course explores the elementary concepts behind the theory of numbers and their unexpected connections with other major branches of mathematics. Being a "ways of inquiry course", a strong emphasis is placed on developing the skills of mathematical inquiry. The student will have multiple chances to practice these skills in and outside of class.

Content: Divisibility; methods of proof (direct, indirect, existence, pigeonhole principle, well-ordering principle, induction) and mathematical inquiry; the Fibonacci sequence; Pythagorean triples; the Fundamental Theorem of Arithmetic; congruences and modular arithmetic; the Euclidean Algorithm; perfect numbers; fast exponentiation; primes and pseudoprimes; Euler's Theorem; Wilson's Theorem; the Chinese Remainder Theorem; $\phi(n)$; roots; quadratic reciprocity; historically significant ciphers and techniques, including (but not limited to) the shift, affine, substitution, and Vigenere's ciphers; the Enigma Machine; Diffie-Hellman Key Exchange and RSA Public Key codes.

Course Goals: Upon successful completion of Math 125, students will:

1. Understand the basic elements of number theory and some of its more interesting applications and connections to other disciplines, especially with regard to cryptography.
2. Have developed some of the fundamental skills needed to investigate something mathematically. That is to say, they will have learned the basics of "mathematical inquiry". Specifically, students should start to become proficient at: (a) Asking good mathematical questions; (b) Identifying patterns; making and testing conjectures; and (c) Proving (and possibly generalizing) their results when appropriate.

The "Ways of Inquiry" at Oxford:

"Ways of Inquiry" courses are designed to introduce students to the specific ways knowledge is pursued in each discipline through active engagement in the discipline's methods of analysis. INQ courses start with questions, are student-centered and often collaborative, and they place increasing responsibility on students for their own learning. Students not only experience each discipline's distinctiveness but also move beyond its boundaries to understand connections with other disciplines and fields.

The “Ways of Inquiry” Used in this Course: The questions and motivations mathematicians use to investigate problems will be emphasized and modeled by the instructor during an exploration of the classic results of number theory, and some additional connected topics in mathematics. As in most introductory courses on number theory, students will be required to demonstrate competence in the standard number theoretic techniques. However, in this class – where a heavy emphasis is given to the active practice of mathematical inquiry -- students will also be asked to collaboratively investigate novel mathematical problems and try their hand at code-breaking, journaling for both how the aforementioned modeled questions and motivations prove valuable to these ends. These activities are more fully described below:

Investigations: “Investigation” problems will be given over the course of the semester. Different students will have different collections of problems for which they are responsible (with some overlap).

Collaboration is encouraged, as all students ultimately responsible for a problem will need to be able to explain its solution. One of the aims of these investigations is to make students conscious of the usefulness of certain questions that might be asked during the course of mathematical inquiry. As such, for each investigation, students will need to identify and contextualize the fruitful “fundamental questions” that either led them – or could have led them -- to the solution.

Some of these problems may initially appear only tangentially related to the rest of the class content. The novelty of these problems serves a purpose – it forces students to abandon the ever too limiting *“If I see this type of problem, I use this memorized formula or blindly-applied mechanical manipulations to solve it”* approach to problem solving – a critical hurdle that must be overcome if the art of mathematical inquiry is to be mastered. Many of the problems will require data be accumulated at some level, so that a search for patterns can begin, and conjectures can be contemplated, investigated, and ultimately proven or disproven.

Students are encouraged to consult with the instructor over the course of their investigatory work so that:

- a) They can see how the “fundamental” questions of mathematical inquiry can be pursued in the context of the investigation at hand,
- b) They don't get stuck in a mathematical quagmire of un-resolvable conjectures; and
- c) They don't just skim the surface of what can be a rich mathematical area of exploration.

Students should consider generalizations of their arguments, as well as limitations on their argument's validity, as appropriate. Some portion of class time will be reserved for these investigations, although students should be prepared to spend a significant time outside of class working on these problems.

For some of these investigations, the instructor may opt to require the work done be explained by the students in a non-written way (possibly through student-recorded video).

Code-Breaking Activities: There will be multiple opportunities to demonstrate one's ability to “break secret codes” using ideas discussed in class, in the reader, and in supplementary material provided by the instructor.

Each student will have unique messages to decrypt, although all of the messages released at a given time will be encrypted in a similar manner (just with different “keys”), thus encouraging collaboration. In some cases, students will need to discover what encryption scheme is being used from the properties of the encrypted text itself, the “clues” they are provided, and from actual history.

The intent of these activities is to get students “down in the trenches” to cultivate an understanding of the “arms-race evolution” of secret codes – where each new encryption and decryption scheme mathematically addresses the weaknesses of the last one.

Tests: Three tests will be given (in class, at dates to be announced later). Students are expected to be present for all scheduled tests. Any conflicts should be brought to the instructor's attention as soon as possible. If a legitimate reason exists for missing a test – as determined by the instructor – then the test must be taken prior to the regularly scheduled date. In the unusual circumstance where taking the test early is not possible, students should be aware that any make-up tests given will likely be designed to be more difficult to offset the additional time given for study. Students must provide written documentation in advance of any special accommodations required for testing. This includes additional time or other needs.

Grading: Students' grades are determined by performance on investigations, code-breaking activities, tests/quizzes, and a *comprehensive* final exam according to the table below. All tests will be administered during class.

Investigations	200 points
Code-Breaking Activities	200 points
3 Tests/Quizzes	400 points
<u>Final Exam</u>	<u>200 points</u>
Total	1000 points

Grade cut-offs are as follows: 90% - A, 80% - B, 70% - C, 60% - D. Plus/minus grades may be assigned for percentages near the grade cut-offs.

Homework: The intent of the homework exercises is to practice necessary skills and techniques found in number theory, cryptography, and the other topics found in this course. Timely completion of these assignments is expected and will serve as an excellent preparation for the tests.

Quizzes: The instructor reserves the right to give students quizzes, announced or unannounced, at any time. The points awarded for the "Tests/Quizzes" portion of the student's grade will be calculated according to the formula $300 \cdot T_{avg} + 100 \cdot Q_{avg}$, where T_{avg} is the percent average of the student's three test scores and Q_{avg} is the percent average of all of the student's equally-weighted quiz scores. In the event that no quizzes are given over the course of the semester, the points awarded to the student will be calculated according to the formula $400 \cdot T_{avg}$.

Class Attendance: Students are responsible for all material covered in class and any changes to the syllabus that may be announced. Any conflicts between the course schedule and religious holy days are to be negotiated in advance with one's instructor.

Online Resources: The math center's website, <http://www.oxfordmathcenter.com> will be an essential resource for students in this class. It will contain all of the course notes and exercises. Additionally, there is a blackboard site for this course, where the calendar, assignments, and other pertinent information will be posted. Students are responsible for checking both of these resources DAILY for updates.

Calculators and "Good Style": Students will be allowed to use calculators on any quizzes or exams. When asked for, all necessary work must be correctly shown in a clear and organized fashion for full credit. Organization and clarity of thought are essential to mathematical thinking. Therefore, points may be deducted for a lack of organization, illegible or sloppy work, and/or the inappropriate use of mathematical symbols, even if answers found are correct. Students will be provided examples of what is considered "acceptably clear and organized work".