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: Pierce Hall 206
Class Time: T,Th 1:00-2:15 PM

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

Required Texts/Resources: *The Code Book* by Simon Singh; a scientific calculator that adheres to the order of operations (it need not be a graphing calculator, but these are welcome); and access to Mathematica 7. [*Note: Oxford computers available for student use should already have Mathematica installed, although students may wish to purchase it for their own machines. Students can buy a semester license from http://www.wolfram.com for $44.95. They also sell an annual edition for $69.95.*]

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, well-ordering principle, induction); Pythagorean triples; the Fundamental Theorem of Arithmetic; congruences and modular arithmetic; the Euclidean Algorithm; perfect numbers; fast exponentiation; primes and pseudoprimes; Euler's Theorem; the Chinese Remainder Theorem; $\varphi(n)$; shift, affine, substitution, and Vigenere's ciphers; the Enigma Machine; Diffie-Hellman Key Exchange and RSA Public Key methods.

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) Using tools, like Mathematica, to aid them in their mathematical investigations. (c) Identifying patterns; making and testing conjectures; and (e) Proving (and possibly generalizing) their results.

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
Final Exam	200 points
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.

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 the fruitful "fundamental questions" that led them to the solution.

These problems may initially appear unrelated to class content – but one can be assured that there are some deep connections between them that will be explored "post mortem". The novelty of many of these problems serves a second purpose as well – 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 will be asked to look for generalizations of their arguments, as well as limitations on their argument's validity. 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 as well.

Some of the investigations will be identified as requiring a non-written explanation. Students will be given a great deal of creative license in how to address these investigations. Possibilities include: a narrated Camtasia video or PowerPoint, an in-class presentation, a podcast, etc…

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 many cases, students will need to discover what encryption scheme is being used from the properties of the encrypted text itself, the "intelligence" 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.

Quizzes: The instructor reserves the right to give students a quiz, 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.

The Math Center Online: The math center's website, http://mathcenter.oxford.emory.edu/ , will be an essential resource for students in this class. It will contain the calendar for the course, as well as notes and assignments. Students are responsible for all content related to Math 125 posted on this site.

Calculators, Mathematica, and "Good Style": Students will be allowed to use calculators on any quizzes or exams. Mathematica can be used in investigations and code-breaking activities unless otherwise prohibited. 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".