

Math 4150: Introduction to Number Theory
Dr. Matthew Baker
mbaker@math.gatech.edu
Office: Skiles 212

Class Time and Location: 9:35 pm - 10:55 pm TuTh in Skiles 270

Course web page: www.math.gatech.edu/~mbaker/Math4150.html

Textbook: *A Friendly Introduction to Number Theory*, by J. Silverman (3rd edition)

General description: This course is an introduction to number theory and its applications to modern cryptography. Number theory, which is one of the oldest branches of mathematics, is the study of the many fascinating properties of integers. For example, we will look at prime numbers and their distribution, modular (“clock”) arithmetic, Diophantine equations (including Fermat’s Last Theorem), factoring and primality testing, and encryption/decryption techniques based on number theory.

Course outline: Topics to be covered will include Pythagorean triples, unique factorization, divisibility criteria, the Euclidean algorithm, congruences and modular arithmetic, linear Diophantine equations, the Chinese Remainder Theorem, Fermat’s Little Theorem and Euler’s Theorem, public-key cryptography (including RSA, ElGamal, and digital signatures), primality testing, factoring methods, primitive roots, discrete logarithms, quadratic residues, quadratic reciprocity, and an introduction to elliptic curves.

Homework: There will be regular homework assignments in the class.

Exams: There will be 2 in-class midterm exams during the course of the semester, plus a cumulative in-class final exam at the end of the course.

Grading: The two midterm exams will each count for 25% of your grade, the final will count 35%, and homework will count 15%.

Office hours: I will have regular office hours which you are strongly encouraged to attend. My office hours are tentatively set to be on Tuesdays from 11:00am-12:00pm and 3:30pm-4:30pm, or by appointment. Please let me know if neither of these times is good for you. I will also be happy to answer questions by email any time at mbaker@math.gatech.edu.

Further thoughts: If at any point during the semester you feel unsatisfied with some aspect of the course, please come talk to me about it. I have no problem making adjustments mid-stream if necessary!