Math V3020: Number Theory and Cryptography
Syllabus

Instructor: David Hansen
Dave's office: Room 516 in the math building
Dave's email: hansen@math.columbia.edu
Dave's office hours: M 4-6, T 2:30-4
TAs: TBA
Course website: www.math.columbia.edu/∼hansen/v3020.html

Material: This is a course in elementary number theory, with some excursions into cryptographic applications. Topics include primes and unique factorization of integers, congruences and arithmetic "mod n", quadratic residues and quadratic reciprocity, RSA encryption, Diffe-Hellmann key exchange, Miller-Rabin primality testing, Farey sequences, and Pell's equation.

Textbook: There is **no assigned textbook** for this class. Your primary resource will be the notes that you take in class. If you would like to supplement your notes with a text, I recommend "A Friendly Introduction to Number Theory" by Joseph Silverman (available on Amazon). The Wikipedia articles on elementary number theory are also very good.

Homework: Homework will be due on Wednesdays, and should be handed in via the appropriate box on the fourth floor of the math building. You should attempt every homework problem and eventually understand how to do every problem correctly. Collaboration and discussion with your classmates is encouraged, but you must write up assignments individually.

Exams: There will be two in-class midterms, as well as a final exam. Examinations will not be rescheduled because of travel arrangements – it is your responsibility to schedule travel appropriately. Makeup midterms will be given only under exceptional circumstances and you will need a note from a doctor or a dean. The final exam must be taken at the scheduled time.

Grading: 15% homework, 20% your worse midterm, 25% your better midterm, 40% final.

Help: My office hours are Mondays, 4-6 PM, and Tuesdays, 2:30-4 PM, but you should also feel free to make an appointment or just drop by. Help is also available without appointment in the Columbia Help Room (406 Math) whenever it is open.

Academic Dishonesty: The vast majority of students do not cheat. Anyone who does so devalues the hard work of the rest of the class and creates a bad atmosphere for all. Anyone found to have cheated on an exam will receive a failing grade for the course and be subject to administrative discipline. If you are struggling with the material or have a problem regarding an upcoming exam, **please** discuss it with me instead of resorting to cheating!