Mathematics 297R, Fall 2009
Computational Number Theory

Instructor: Michael Rogers
Office: 115 Seney Hall
Phone: x4-8419
E-mail: LearnLink "Michael Rogers"
Hours: MWThF 2:15–3:30. Available at other times, too.

Textbooks:

Crandall and Pomerance, *Prime Numbers: A Computational Perspective*.

Course Content: This is a one semester-hour course in computational number theory, with emphases on primes and factoring. Primes, modular arithmetic, primality testing algorithms, and factoring algorithms will be covered. Programming will be done in *Mathematica.* In particular,

a survey of what is known about primes: fundamental theorem of arithmetic, computational records, the distribution of primes, the Prime Number Theorem, Mersenne primes, Fermat's conjecture, the Riemann zeta function, the Riemann hypothesis, twin primes, the Goldbach Conjecture;

computational tools in elementary number theory: Euclid's algorithm, modular equations, quadratic residues, quadratic reciprocity, square roots, finite fields;

primality testing: sieving and its applications, smooth numbers, pseudoprimes, probable primes, Lucas test, Frobenius test, Lucas-Lehmer test;

basic factoring: Fermat method, Pollard rho method, Pollard $p-1$ method, quadratic seive method;

elliptic curve method: elliptic curves, their arithmetic, elliptic curves over finite fields, the elliptic curve method (ECM) algorithm;

other related topics if time allows.

Course Goals: The goal is to develop the background in number theory and writing computer programs to implement and analyze the Elliptic Curve Method for factoring. To able to do this, the student will have to understand methods for testing whether an integer is a prime, how to perform arithmetic in finite fields, other methods for factoring, and how to perform elliptic curve arithmetic.

Coursework: Problems will be assigned; these will be discussed, students will present their solution and/or students will write solutions that will be collected for credit.

Grading: Grades will be based primarily on the students presentations and problems collected for credit (80%) as well as on class participation (20%). Each student's work will be judged in relation to the goals set for the course.

The Honor Code of Oxford College applies to all work submitted for credit in this course. By placing your name on such work, you pledge that the work has been done in accordance with the given instructions and that you have witnessed no Honor Code violations in the conduct of the assignment.