

Math 595 Algorithmic Number Theory

Fall 2009, MWF 1-2

Instructor: Iwan Duursma

In this course we discuss topics of current interest in the areas of algorithmic number theory and algebraic curves over finite fields.

Possible topics include the theory of function fields in one variable and their applications (including results analogous to those taught in Math 530 for number fields, as well as the Riemann-Roch theorem, a proof of the Riemann hypothesis analogue for function fields, etc), theory of elliptic curves and their applications, point counting and zeta functions for varieties over finite fields, quadratic sieve and number field sieve methods for factoring integers, primality testing algorithms, others. Final choice of topics and emphasis to be decided together with the audience.

Possible references for core material, and some standard references:

Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography
by J.P. Buhler and P. Stevenhagen (2008)

Algebraic curves over a finite field.
by Hirschfeld, J. W. P.; Korchmáros, G.; Torres, F. (2008)

Algebraic function fields and codes.
by Henning Stichtenoth (2009)

Number Theory: Volume I: Tools and Diophantine Equations
by Henri Cohen (2007)

Algorithmic Number Theory, Vol. 1: Efficient Algorithms
by Eric Bach and Jeffrey Shallit (1996)

Algorithmic Algebraic Number Theory
by M. Pohst and H. Zassenhaus (1997)

A Course in Computational Algebraic Number Theory
by Henri Cohen (200)

Prime Numbers: A Computational Perspective
by Richard Crandall and Carl Pomerance (2005)

Number-Theoretic Algorithms in Cryptography
by O. N. Vasilenko (2006)