

Jonathan E. Webster

Department of Mathematics
Bates College
3 Andrews Rd
Lewiston, ME 04240

Phone (Office): (207) 786-6403
Fax: (207) 786-8331
jwebster@bates.edu
<http://bates.edu/~jwebster/>
Citizenship: United States

Education

Ph.D. in Mathematics, University of Calgary, Canada, 2010
Thesis title: *Cubic Function Fields in Characteristic Three*.
Thesis Supervisor: Mark Bauer

M.S. Mathematics, University of Illinois at Urbana-Champaign, 2004

B.S. Mathematics and B.S. Computer Engineering, Rose-Hulman Institute of Technology, 2001

Awards and Fellowships

Project NExT Fellow 2011.

Summer Research Apprenticeship Grant. A Bates College grant to work with an undergraduate student to translate original works by Dedekind, Hensel, and Bauer from German to English.

Positions Held

Visiting Assistant Professor, Bates College, August 2010 to Present.

Visiting Instructor, Bates College, August 2009 to July 2010.

Visiting Researcher and Teaching Assistant, University of Calgary, August 2004 to April 2009.

Research Assistant and Teaching Assistant, University of Illinois, August 2001 to December 2007.

Publications

P. Rozenhart and J. Webster, *Simple cubic function fields and class number computations*, submitted, available at <http://arxiv.org/abs/1108.6048>.

M. Bauer and J. Webster, *Computations in Cubic Function Fields of Characteristic Three*, submitted, available at <http://arxiv.org/abs/1009.0737>.

E. Landquist, P. Rozenhart, R. Scheidler, J. Webster and Q. Wu, *An explicit treatment of cubic function fields with applications*, Canadian Journal of Mathematics **62** (2010), no. 4, 787-807.

N. Boston, T. Clancy, Y. Liow and J. Webster, *Genus Two Hyperelliptic Curve Coprocessor*. Workshop on Cryptographic Hardware and Embedded Systems. Lecture Notes in Computer Science vol 2523. August 2002.

Teaching Experience

Bates College

Undergraduate Thesis Advising

- Fall 2011: Joseph Ekpenyong, “Square-free Factorization and Unbalanced RSA.”

- Fall 2010 - Winter 2011: Joseph Kibe, “Query Expansion and Truncation in the Comparison of Short Text Documents.”

Fall 2011

Sole instructor for two sections of Calculus I. In all courses where I was the sole instructor the responsibilities include preparing classroom lessons, creating and grading exams, and assigning all grades.

Winter 2011

Sole instructor for Numerical Analysis.

Fall 2010

Sole instructor for two sections of Linear Algebra.

Spring 2010

Sole instructor for Number Theory and an Independent Studies with two students in function fields.

Winter 2010

Sole instructor for a section of Calculus II.

Fall 2009

Sole instructor for two sections of Calculus I and Probability.

University of Calgary

January 2005 - April 2009

Taught various calculus and linear algebra tutorials for first year students. Duties included leading tutorial sections by answering student questions and presenting extra examples, along with administering and grading quizzes.

University of Illinois

Spring 2006

Sole instructor for Calculus II. This section was also taught using a small group active learning philosophy.

Fall 2004, Fall 2005

Administered an active learning Calculus I section. I was responsible for creating the environment to foster group participation and active learning.

Fall 2003, Spring 2004, Fall 2006

Conducted Calculus I tutorials for first year students. Duties include presenting example problems, administering and writing quizzes, and grading exams.

Fall 2002

Sole instructor for College Algebra.

Talks

Simple Cubic Function fields. Maine-Quebec Number Theory Conference; University of Maine, Orono, ME October 2, 2011.

Cubic Function Fields in Characteristic Three. AMS Special Session, Joint Mathematics Meetings; New Orleans, LA; January 6-9, 2011.

Cubic Function Fields in Characteristic Three. Quebec-Maine Number Theory Conference; Université Laval, October 2-4, 2010.

Cubic Function Fields in Characteristic Three. Canadian Number Theory Association XI; Acadia University, July 11-16, 2010.

Cryptography, Finite Groups, and the Discrete Log Problem. Rose-Hulman Mathematics Seminar, April 21, 2010.

Cryptography, Finite Groups, and the Discrete Log Problem. Colby College Math and Stats Colloquium, March 8, 2010.

Arithmetic Aspects of Cubic Function Fields in Characteristic Three. AMS Special Session, Joint Mathematics Meetings; Washington, D.C. January 5-8, 2009.

Cubic Function Fields in Characteristic Three. West Coast Number Theory conference; Pacific Grove, CA; December 19, 2007.

Splitting primes in $\mathbb{F}_q(x)[y]/(y^3 - Ay + B)$. Midwest Number Theory Conference for Graduate Students; Urbana, IL; October 28, 2006.

Splitting primes in $\mathbb{F}_q(x)[y]/(y^3 - Ay + B)$. Introduction, University of Wyoming Summer School on computational number theory and applications to cryptography, University of Wyoming; July 6, 2006.

The Multiple Polynomial Number Field Sieve, IMA PI Summer Program for Graduate Students: Coding and Cryptography, University of Notre Dame; June 25, 2004

Conferences Attended

Maine-Quebec Number Theory Conference, University of Maine, Orono, ME; October 1-2, 2011.

AWM's 40 Years and Counting, Brown University; September 17-18, 2011.

MathFest; Lexington, KY; August 2-4, 2011.

Joint Mathematics Meetings, New Orleans, LA; January 6-9, 2011.

Quebec-Maine Number Theory Conference, Université Laval, Quebec City, QC; October 2-4, 2010.

MAA Prep in Algebraic Number Theory, Williams College, Williamstown, MA; June 28-July 2, 2010.

Maine-Quebec Number Theory Conference, University of Maine, Orono, ME; October 3-4, 2009.

Joint Mathematics Meetings, Washington, D.C.; January 5-8, 2009.

Eighth Algorithmic Number Theory Symposium, Banff Centre, Banff, Alberta; May 17-22, 2008.

West Coast Number Theory Conference 2007, Asilomar Conference Grounds, Pacific Grove, CA; December 16-20, 2007.

Rocky Mountain Mathematics Consortium Summer School on "Computational Number Theory and Applications to Cryptography", University of Wyoming; June 19-July 7, 2006.

Pacific North West Number Theory Conference 9, Simon Fraser University; April 23, 2005.

IMA PI Summer Program for Graduate Students on "Coding and Cryptography." University of Notre Dame; June 8-26, 2004.

CRYPTO 2002, Santa Barbara, CA; August 18-22, 2002.

Service and Membership

Member MAA, 2010-present.

Reviewer for Pairing 2007 proceedings, an international conference on pairing-based cryptography.

Student co-leader for the discrete logarithms group, University of Wyoming Summer School on computational number theory and applications to cryptography.