

Curriculum Vitae

Personal Information

Name: Matthew William Darnall

Address: Department of Mathematics
University of Wisconsin
Madison, WI 53706

Phone: (608) 332-8998

Email: darnall@math.wisc.edu

Education

Bachelor of Arts in Mathematics, Humboldt State University, Spring - 2004

Currently pursuing PhD in Mathematics at the University of Wisconsin - Madison

Employment

Research Assistant, University of Wisconsin - Madison *Fall 2005 to Present*
Study Information Theory and Cryptography under Professor Nigel Boston as it relates to face recognition.

Intern, Motorola Labs - Schaumburg, IL *Summer 2005*
NSF VIGRE sponsored internship studying cryptography with the information security specialists at Motorola Labs.

Instructor of Mathematics, University of Wisconsin - Madison *Fall 2004*
Preparation and presentation of lectures, creating and grading quizzes, grading the final exam for the course, leading review sections.

Tutor - Humboldt State University *Fall 2002 to Spring 2004*
Worked up to 15 hours a week assisting various students from disadvantaged backgrounds master mathematics courses.

Awards and Honors

NSF VIGRE Fellowship *Spring 2005*
Awarded to promising incoming math graduate students at the University of Wisconsin - Madison.

NSF Graduate Fellowship - Honorable Mention *Fall 2004*

Humboldt State University Commencement Honor *Spring 2004*
Recognized at Humboldt State University Commencement as first student to graduate with a bachelor's degree after only two years of attending college.

Kieval Scholarship *Fall 2003*
Awarded to most distinguished mathematics major at Humboldt State University.

Research Experience

Research Assistant - University of Wisconsin - Madison *Fall 2005*
Work inside the Face Recognition group under Professor Nigel Boston.

Motorola Internship *Summer 2005*
Studied implementations of the Advanced Encryption Standard on embedded systems.

Research Assistant - Humboldt State University *Spring 2004*
Studied the combinatorial identities in Pascal's triangle under Professor Tyler Evans.

REU, Temple University *Summer 2003*
Studied the growth of noncommutative algebras with D. Constantine under Professor Edward Letzter.

Publications

(With D. Constantine) "Lengths of Finite Dimensional Representations of PBW Algebras." *Linear Algebra and its Applications* 377, 175-181 (2005)

(With D. Kuhlman) "AES Software Implementations on ARM7TDMI", to appear in *Proceedings of Indocrypt 2006*

Conferences and Workshops Attended

Indocrypt 2006, December 11- 13, Kolkata, India

Midwest Number Theory Conference for Graduate Students IV, October 28-29, 2006, Urbana-Champaign, Illinois

MSRI Summer Graduate Workshop in Computational Number Theory, July 31-August 11, 2006, Berkeley, CA

Canadian Number Theory Association Meeting IX, July 9-14, 2006, Vancouver, BC, Canada

Sequences and Codes, July 17-21, 2006, Vancouver, BC, Canada

Arizona Winter School on Computational Aspects of Algebra and Arithmetic, March 11-15, 2006, Tucson, Arizona

Midwest Number Theory Conference for Graduate Students III, November 5-6, Madison, Wisconsin

Midwest Number Theory Day, November 4, 2005, Madison, Wisconsin

AMS Sectional Meeting, October 21-23, 2005, Lincoln, Nebraska

Courses Related to Number Theory

Algebraic Number Theory, Analytic Number Theory, Modular Forms, Elliptic Curves and Modular Forms, Fermat's Last Theorem, Rational Points on Varieties, Class Field Theory, Algebraic Geometry, Arithmetic Algorithms. GPA: 4.0