

Curriculum Vitae of Christopher Monico

Department of Mathematics and Statistics

Texas Tech University

Lubbock, TX 79409-1042

email: c.monico@ttu.edu

April 21, 2008

Positions held

- 2003–present Assistant Professor, Texas Tech University.
- 2002–2003 Postdoctoral Researcher, University of Notre Dame. Support received from NSF research grants through Joachim Rosenthal and Andrew Sommese, with partial support from the Department of Mathematics.
- 2001–2002 Fellowship from the Center of Applied Mathematics, University of Notre Dame.
- 1998–2001 Teaching Assistantship, University of Notre Dame.
- 1997–1998 Systems Analyst/Programmer, Ilex Systems / L^3 Communications, Shrewsbury, NJ.
- 1996–1997 Graduate Student Fellowship, University of Notre Dame.

Education

- 2002, May Ph.D in Mathematics, University of Notre Dame. Dissertation: “Semirings and semigroup actions in public-key cryptography”.
Advisor : Joachim Rosenthal
- 2000 M.S. in Mathematics, University of Notre Dame.
- 1996 B.S. in Mathematics, Computer Science minor, Monmouth University.

Research Interests

I have worked on computational problems in general, and specifically discrete computational problems, such as the discrete logarithm problem and zero-dimensional primary decomposition. This work has included trying to build efficient cryptosystems on the semigroup action problem, and using distributed computing to solve large problems (i.e., Certicom’s *ECCp-109 challenge*). I am also interested in integer factorization; my GGNFS number field sieve software (distributed with Jens Franke’s lattice siever) has been used by many people to factor large integers as part of various projects.

I am also interested in some general algebraic problems. In my dissertation, I classified finite, additively commutative simple semirings, except for the idempotent ones. There, I also gave an algorithm for computing the primary decomposition of zero-dimensional ideals. More recently, I have become interested in additive (combinatorial) structure on the fibers of characters on \mathbb{F}_p^* .

Publications

- (1) M. Peterson, C. Monico. \mathbb{F}_2 Lanczos Revisited. *Linear Algebra and Its Applications*, 428:4 (2008), 1135–1150.
- (2) M. Elia, C. Monico. On the representation of primes in $\mathbb{Q}(\sqrt{2})$ as sums of squares. *JP Journal of Algebra, Number Theory and Applications*, 8:1 (2007), 121–133.
- (3) G. Maze, C. Monico, J. Rosenthal. Public key cryptography based on semigroup actions. *Advances in Mathematics of Communications*, 1:4 (2007), 491–509.
- (4) C. Monico, M. Elia. Note on an additive characterization of quadratic residues modulo p . *Journal of Combinatorics, Information, and System Sciences*, v.31 (2006), 209–215.
- (5) C. Monico. On finite congruence-simple semirings. *J. of Algebra* 271 (2004), 846–854, doi:10.1006/jabr.2000.8483.
- (6) E. Byrne, C. Kelley, C. Monico, and Rosenthal J. Non-linear codes for belief propagation. In *Proceedings of the 2003 IEEE International Symposium on Information Theory*, page 43, Yokohama, JAPAN, 2003.
- (7) C. Monico. Computing the primary decomposition of zero-dimensional ideals. *J. of Symbolic Computation*, 34:5 (2002) 451–459.
- (8) G. Maze, C. Monico, J. Climent and J. Rosenthal. Public-key cryptography based on simple modules over simple rings. *Proceedings of MTNS 2002*.
- (9) G. Maze, C. Monico, J. Rosenthal. A public-key cryptosystem based on actions by semigroups. In *Proceedings of the 2002 IEEE International Symposium on Information Theory*, page 266, Lausanne, Switzerland, 2002.
- (10) C. Monico, J. Rosenthal and A. Shokrollahi. Using low density parity check codes in the McEliece cryptosystem. *Proceedings 2000 IEEE International Symposium on Information Theory*.

Selected Talks Given

“Primality testing/proving” and “GNFS factorization”, series of talks given at 2004 IMA Workshop on Coding Theory and Cryptography, University of Notre Dame, 6/2004.

“ECCp-109: An excursion in Internet-distributed computing”. Colloquium, Texas Tech University, 1/29/04.

“Public-key cryptography via algebra and number theory.” Texas Tech University, 19th Annual Fall SIAM Symposium, November 20, 2003.

“Factoring Polynomials by Numerical Methods.” AMS Meeting # 985, Indiana University, Bloomington, April 4, 2003.

“Public-Key Cryptography : Where are we and where do we go from here?”. Colloquium, Texas Tech University, 11/2002.

“Nonlinear Belief Propagation Decodable Codes” & “The Caveats of Generalizing Public-Key Cryptosystems”. Ohio State University, 10/2002.

“Computing the Primary Decomposition of Zero-Dimensional Ideals.” 966th Meeting of the American Mathematical Society, Stevens Institute of Technology, 4/2001.

“Using Low Density Parity Check Codes in the McEliece Cryptosystem.” 2000 IEEE International Symposium on Information Theory, Sorrento, Italy. 6/2000.

Teaching Experience

I have taught undergraduate courses including Discrete Mathematics, Calculus I & II (both business and for engineers), Linear Algebra, ODE’s for engineers, Fundamentals of Computing, Elementary Number Theory, Abstract Algebra and Introductory Analysis. At the graduate level I have taught courses including Number Theory, Cryptography, Fundamentals of Computing, Modern Algebra for teachers, and Real Analysis. Student evaluations of my courses are consistently above average.

Thesis directed

- Steven Lawless, “Super-Resolution by Local Function Approximation”, M.S. Thesis, December 2007.
- Michael Peterson, “Parallel block Lanczos for solving large binary systems”, M.S. Thesis, June 2006.
- Brian Miller, “A construction and analysis of arithmetic progression-free sequences”, M.S. Thesis, December 2004.
- Michael Peterson, “The general number field sieve”, Senior Honors Thesis, December 2004.

Grants, Honors and Memberships

- Member of the *Mathematical Association of America*.
- Awarded “Hemphill Wells New Professor Excellence in Teaching Award”, 2007.
- Awarded “Professor of the Year, 2007” by TTU Chapter of Kappa Mu Epsilon.

- Awarded “Graduate Professor of the Year, 2005-2006” by the TTU Chapter of SIAM.
- Awarded “Professor of the Year, 2005” by the TTU chapter of the MAA.
- Awarded TTU REF grant \$2500 for proposal: “The distribution of quadratic non-residues”, 4/2005.
- Awarded TTU REF grant \$2974 for proposal: “Factoring integers with the number field sieve”, 4/2004.
- Solved Certicom’s \$10,000 “ECC2-109” elliptic curve cryptography challenge, 4/2004.
- Solved Certicom’s \$10,000 “ECCp-109” challenge, representing the new world record in elliptic curve discrete logarithm computation. Press coverage by CNN.com, Reuters, Slashdot, The South Bend Tribune, NBC local news, and others.
- Awarded fellowship for 2001-2002 from the Center for Applied Mathematics at the University of Notre Dame.
- SGI Award for Visualization and Computational Sciences, 2001 (only recipient from the College of Science at Notre Dame).
- NSF Travel Award to attend MSRI Workshop on Computational Number Theory and Cryptography in Berkeley, CA. 10/2000.

Committees and Service

- Serving on the Department of Mathematics and Statistics Graduate Committee, Fall 2007–present.
- Serving on the Department of Mathematics and Statistics Noether Day Committee, Spring 2006– present.
- Served on the Department of Mathematics and Statistics Undergraduate Committee, Fall 2005– Spring 2007.
- Faculty advisor to Texas Tech chapter of the MAA, 2005–Present.
- Served on the Department of Mathematics and Statistics Information Technology Committee, 2003–2005.
- Organized “Cryptography and Number Theory” seminar, Fall 2003 at Texas Tech University.