

**Contact Information**

Address: University of Waterloo  
David R. Cheriton School of Computer Science  
Ontario, Canada, N2L 3G1  
E-mail: andy@novocin.com  
URL: <http://andy.novocin.com/pro>

**Personal Data**

Date of Birth: June 12, 1983  
Place of Birth: Jacksonville, Florida  
Nationality: USA  
Marital status: Married

**Education**

2001–2003 BS Mathematics Florida State University  
2003–2006 MS Mathematics Florida State University  
2006–2008 PhD Mathematics Florida State University

**Dissertation Adviser:** Mark van Hoeij

**Dissertation Title:**

Factoring Univariate Polynomials over the Rationals

**Academic Employment History**

- ANR post-doctorate with the LAREDA group at Montpellier, France. September 2008 through August 2009.
- Post-doctorate with the Arénaire project at ENS Lyon, France. September 2009 through August 2011, on the topic of lattice reduction algorithms.
- Post-doctorate with Symbolic Computation Group at University of Waterloo, Canada. September 2011 to present.

## Peer-Reviewed Papers

- (with M. van Hoeij) *Gradual sub-lattice reduction and a new complexity for factoring polynomials* (extended abstract) proceedings LATIN 2010 and (journal version) accepted to ALGORITHMICA
- (with D. Stehlé and G. Villard) *An LLL-reduction algorithm with quasi-linear time complexity*, proceedings Symposium on Theory of Computing 2011.
- (with B. Hart and M. van Hoeij) *Practical Polynomial Factoring in Polynomial Time*, proceedings International Symposium on Symbolic and Algebraic Computation 2011.
- (with J. Klüners and M. van Hoeij) *Generating subfields*, proceedings International Symposium on Symbolic and Algebraic Computation 2011.
- (with B. Hart) *Practical divide-and-conquer algorithms for polynomial arithmetic*, proceedings Computer Algebra in Scientific Computing 2011.

## Pre-Prints/Submissions

- (with M. van Hoeij and J. Klüners) *Generating subfields*, submitted JSC.
- (with B. Hart and M. van Hoeij) *Complexity Analysis of Practical Polynomial Factoring*, pre-print.
- (with M. van Hoeij) *Reparametrizing Curves*, unpublished.
- (with M. van Hoeij) *A Reduction Algorithm for Algebraic Function Fields*, unpublished.

## Conference Posters

- *Simplifying Algebraic Extensions*, poster presented at the International Symposium on Symbolic and Algebraic Computation, 2004, University of Cantabria
- *Early Termination Factorization*, poster presented at the International Symposium on Symbolic and Algebraic Computation, 2007, University of Waterloo
- *Factorization of Univariate Polynomials over the Rationals*, International Symposium on Symbolic and Algebraic Computation, 2008, Research Institute for Symbolic Computation

## Software

- Co-Author of FLINT a highly optimized C-library for number theory
- (with Bill Hart) Developed and implemented fast polynomial factoring algorithm over the integers.
- Developed and implemented efficient new lattice reduction package.
- (with Mark van Hoeij and Juergen Klueeners) Developed and implemented a new algorithm for finding all subfields of a given field extension.
- Contributor to SAGE Computer Algebra System
- Some MAPLE snippets for simplifying number field representatives and parametrizations of algebraic curves

**Invitations/projects**

- University of Delaware, Newark, Delaware, December 2nd, 2011
- IDACCR, Princeton, New Jersey, November 30th, 2011
- University of Western Ontario, ORCCA JLM, November 4th, 2011
- Université de Rennes, France, May 13th, 2011
- Institut de Mathématiques de Bordeaux, France, May 5th, 2011
- Codage et Cryptographie, St. Pierre d'Oléron, April 3-8, 2011
- Computer Algebra Group, Limoges, France, March 10th, 2011
- EPFL, Lausanne, Switzerland, February 18th, 2011
- LaReDa Group, Lyon, France, February 1st, 2011
- Computer Algebra Group, Paderborn Germany, December 2nd, 2010
- SIAM/MSRI Workshop on Hybrid Methodologies for Symbolic Numeric Computation, Berkeley California, November 18th, 2010
- TaMaDi Project, September 8th, 2010
- SAGE days 23, Leiden, the Netherlands, July 2010
- 21st Rencontres Arithmétiques de Caen 2010, June 23-25, Caen France
- Chair of the poster committee for ISSAC 2009, July 28-31, Seoul, South Korea
- CACAO group, INRIA Nancy, June 23, 2009

- Algorithms group, INRIA Paris-Rocquencourt, June 22 2009
- LIX at École Polytechnique, Mar. 24-25 2009, Paris France
- 2nd SCIENCE workshop, Jan. 19-21 2009, École Polytechnique, Paris, France
- Warwick Mathematics Institute, Dec. 11-26th, 2008, Coventry, UK
- Computational Mathematics Work Group, August 16th, 2008, Kassel, Germany
- Mathematics Department, August 6th, 2008, Dusseldorf, Germany
- American Institute of Mathematics, The computational complexity of polynomial factorization, Workshop, May 2006, Palo Alto, California
- ACA 2003, North Carolina State University

### Teaching Honors

- *Dwight Goodner Teaching Fellowship* from the Department of Mathematics, Florida State University, 2006.
- *PIE Excellence in Teaching Nominee* from Florida State University, 2007.

### Teaching Experience

- Taught Calculus II, spring 2008.
- Taught Modern Algebra, spring 2007.
- Taught Linear Algebra, fall 2006.

- Taught Calculus I, summer 2006.
- Taught Calculus I, spring 2006.
- Taught two sections of Trigonometry, fall 2005.
- Conducted recitations Pre-Calculus course, summer 2005.
- Taught Pre-Calculus, spring 2005.

### **Other Professional Experiences & Skills**

- Organized Graduate Student Seminar 2004-2006.
- Organized a series of lectures on *Class Field Theory*.
- Gave several series of talks in the department Algebra Seminar.
- Developed expertise in Python, C, C++, HTML, CSS, Javascript, and many computer algebra systems.
- Primary operator of the Pat Thomas Planetarium from 2002-2006.
- Heavily involved with a US FIRST Robotics team from 1999-2001.

### **Major areas of research interest**

- Algorithmic analysis including computational complexity
- Computer Algebra including Computational Algebraic Number Theory
- Lattice Reduction algorithms and applications
- Asymptotically fast algorithms for arithmetic on integers, matrices, and polynomials