John Voight

Department of Mathematics and Statistics
16 Colchester Ave
University of Vermont
Burlington, VT 05401 USA
(802) 656-2271

jvoight@gmail.com
http://www.cems.uvm.edu/~voight/
Born in Georgia, USA, November 25, 1977

Education

- **University of California, Berkeley**
  Ph.D. in Mathematics, May 2005
  Thesis title: *Quadratic forms and quaternion algebras: algorithms and arithmetic*
  Thesis advisor: Hendrik W. Lenstra, Jr.
- **Gonzaga University**, Spokane, Washington
  B.S. (*Summa cum laude*, 4.0 GPA), May 1999
  Major: Pure mathematics, Minor: Computer science

Employment

- **University of Vermont**
  Assistant Professor, September 2007–present
- **University of Minnesota**
  Postdoctoral Fellow, Institute for Mathematics and its Applications (IMA),
  September 2006–August 2007
- **University of Sydney**, Australia
  Visiting Scholar, Magma Computational Algebra Group, August 2005–June 2006

Research Interests

- **Arithmetic algebraic geometry**:
  Modular curves, Shimura curves, moduli spaces, elliptic curves, computational and algorithmic aspects
- **Number theory**:
  Algebraic number theory, quaternion algebras, quadratic forms, p-adic cohomology, zeta functions of varieties over finite fields, cryptography and coding theory

Honors and Awards

· NSF Graduate Research Fellowship, 2000–2003
· NSF International Travel Award, Summer 2002
· NSF VIGRE Award, 1999-2000
· Ranked 107 in William Lowell Putnam Competition, 1999
· William A. Garrigan, S.J. Award, Gonzaga University, May 1999
  Best academic achievement of a graduating senior
· Rhodes Scholarship finalist, Washington state, 1998
· National Merit Presidental Scholarship, Gonzaga University, 1995–1999

Publications

(1) *Algorithms for quaternion algebras*, in preparation.

We discuss basic algorithmic problems for quaternion algebras, organizing many of the known results and providing several new algorithms. We treat five main topics: identifying if an algebra is a quaternion algebras, determining if a quaternion algebra is isomorphic to a matrix ring, computing a maximal order, calculating the group of units, and calculating a representative set of ideal classes.

(2) *Shimura curves of genus at most two*, to be submitted to Math. Comp.

In this article, we enumerate all Shimura curves $X_0^{\mathfrak{D}}(\mathfrak{N})$ of genus at most two.

(3) *Computing fundamental domains for Fuchsian groups*, submitted to J. Théorie de Nombres de Bordeaux (XXVth Journées Arithmetiques).

We exhibit an algorithm to compute a Dirichlet domain for a cofinite Fuchsian group Γ. As a consequence, we compute the invariants of Γ, including an explicit finite presentation for Γ.

(4) *On moduli of nondegenerate curves* (with Wouter Castryck), submitted to J. Alg. Geom.

Let $\mathcal{M}_g$ be the moduli space of curves of genus $g \geq 2$, and let $\mathcal{M}_g^{\mathrm{nd}}$ be the locus of curves which are birational to a curve defined by a nondegenerate bivariate Laurent polynomial. We show that $\dim \mathcal{M}_g^{\mathrm{nd}} = \min(2g+1, 3g-3)$ except for $g = 7$ where $\dim \mathcal{M}_7^{\mathrm{nd}} = 16$. In particular, a generic curve of genus g is nondegenerate if and only if $g \leq 4$.

(5) *Enumeration of totally real number fields of bounded root discriminant*, accepted to Lecture Notes in Comp. Sci. (ANTS VIII).

We enumerate all totally real number fields F with root discriminant $\delta_F \leq 14$. There are 1229 such fields, each with degree $[F : \mathbb{Q}] \leq 9$.

(6) *Shimura curve computations*, to appear in proceedings from the 2006 Clay Mathematics Institute summer school, Arithmetic Geometry.

We introduce Shimura curves first as Riemann surfaces and then as moduli spaces for certain abelian varieties. We give concrete examples of these curves and do some explicit computations with them.

(7) *Heegner points and Sylvester's conjecture* (with Samit Dasgupta), to appear in proceedings from the 2006 Clay Mathematics Institute summer school, Arithmetic Geometry.

We consider the classical Diophantine problem of writing positive integers n as the sum of two rational cubes, i.e. $n = x^3 + y^3$ for $x, y \in \mathbb{Q}$. A conjecture attributed to Sylvester asserts that a rational prime $p > 3$ can be so expressed if $p \equiv 4, 7, 8 \pmod 9$. The theory of mock Heegner points gives a method for exhibiting such a pair (x, y) in certain cases. In this article, we give an expository treatment of this theory, focusing on two main examples: a theorem of Satgé, which asserts that $x^3 + y^3 = 2p$ has a solution if $p \equiv 2 \pmod 9$, and a proof sketch that Sylvester's conjecture is true if $p \equiv 4, 7 \pmod 9$ and 3 is not a cube modulo p.

(8) *Quadratic forms that represent almost the same primes*, Math. Comp. **76** (2007), 1589–1617.

Jagy and Kaplansky exhibited a table of 68 pairs of positive definite binary quadratic forms that represent the same odd primes and conjectured that their list is complete outside of "trivial" pairs. In this article, we confirm their conjecture, and in fact find all pairs of such forms that represent the same primes outside of a finite set.

(9) *Computing CM points on Shimura curves arising from cocompact arithmetic triangle groups*, Algorithmic number theory (ANTS VII, Berlin, 2006), eds. Florian Hess, Sebastian Pauli,

Michael Pohst, Lecture notes in computer science, vol. 4076, Springer, Berlin, 2006, 406–420.

Let $\Gamma \subset PSL_2(\mathbb{R})$ be a cocompact arithmetic triangle group, i.e. a Fuchsian triangle group that arises from the unit group of a quaternion algebra over a totally real number field. The group Γ acts on the upper half-plane $\mathfrak{H}$; the quotient $X_{\mathbb{C}} = \Gamma\backslash\mathfrak{H}$ is a Shimura curve, and there is a map $j : X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. We algorithmically apply the Shimura reciprocity law to compute CM points $j(z_D) \in \mathbb{P}^1_{\mathbb{C}}$ and their Galois conjugates so as to recognize them as purported algebraic numbers. We conclude by giving some examples of how this method works in practice.

(10) *Quaternion algebras* (with David Kohel), *Associative orders* (with Nicole Sutherland), *Arithmetic Fuchsian groups and Shimura curves*, Handbook of Magma functions, eds. John Cannon and Wieb Bosma, Sydney, July 2007.

(11) *Curves over finite fields with many points: an introduction*, Computational aspects of algebraic curves, ed. Tanush Shaska, Lecture notes series on computing, vol. 13, World Scientific, Hackensack, NJ, 2005, 124–144.

The number of points on a curve defined over a finite field is bounded as a function of its genus g. In this introductory article, we survey what is known about the maximum number of points on a curve of genus g defined over $\mathbb{F}_q$, including an exposition of upper bounds, lower bounds, known values of this maximum, and briefly indicate some methods of constructing curves with many points, providing many references to the literature.

(12) *Quadratic forms and quaternion algebras: Algorithms and arithmetic*, Ph.D. thesis, University of California, Berkeley, 2005.

(13) *On the nonexistence of odd perfect numbers*, MASS Selecta: Teaching and learning advanced undergraduate mathematics, Svetlana Katok, Alexei Sossinsky, and Serge Tabachnikov, eds., Amer. Math. Soc., Providence, RI, 2003, 293–300.

In this article, we show how to prove that an odd perfect number with eight distinct prime factors is divisible by 5.

Teaching

- **Assistant Professor**, University of Vermont
  Math 252: Abstract Algebra II, Spring 2008
  Math 251: Abstract Algebra I, Fall 2007
- **Graduate Student Instructor (GSI)**, University of California, Berkeley
  Math 110: Linear Algebra, Spring 2005
  Math 115: Elementary Number Theory, Summer 2004 (full teaching responsibilities)
  Math 1A: Calculus, Spring 2004
  Math 250B: Multilinear Algebra, Spring 2003
  Math 195: Cryptography, Spring 2002
  Math 1B: Calculus, Fall 2001
  Consistently rated very highly in department teaching evaluations
- **Research in Mathematics Education**
  Panelist, Teaching Critical Reading Across the Disciplines, March 14, 2005
  Special Session Leader, Spring GSI Teaching & Orientation Workshop, January 14, 2005
  Workshop Leader, Fall GSI Teaching & Orientation Workshop, August 27, 2004
  Plenary panelist, Spring GSI Teaching & Orientation Workshop, January 17, 2002
  Panelist, Fall meeting of the Faculty Advisers for GSI Affairs, October 15, 2001

Expository Work

- *Integral and rational points on higher dimensional varieties*, American Institute of Mathematics, December 11–20, 2002, available at `http://www.aimath.org/WWN/qptsurface2/`
- Notes from *Explicit algebraic number theory*, Oberwolfach Seminar, November 10–16, 2002
- *Introduction to stacks*, notes from lecture at Harvard, April 2004
- *Complex multiplication and group schemes*, course notes from Don Zagier and Rene Schoof, Spring 2001
- *Toric surfaces and continued fractions*, manuscript, May 2000

Articles and notes available at `http://www.cems.uvm.edu/~voight/`.

Invited Lectures

- *Shimura curves of low genus and totally real fields of small root discriminant*, Québec-Vermont Number Theory Seminar, McGill University, Montreal, Québec, December 6, 2007
- *Heegner points and Sylvester's conjecture*, Five College Number Theory Seminar, University of Massachusetts, Amherst, November 27, 2007
- *Enumeration of totally real number fields*, MIT Number Theory Seminar, Cambridge, Massachusetts, October 25, 2007
- *Fundamental domains for finitely generated Fuchsian groups*, Maine/Québec Conference on Number Theory and Related Topics, University of Maine, Orono, September 29–30, 2007
- *Computing zeta functions using p-adic cohomology*
  Number Theory Seminar, University of Georgia, Athens, December 6, 2006
  Computational Algebra Seminar, University of Sydney, June 7, 2007
- *Shimura curve computations*
  Some Diophantine applications of Heegner points
  Clay Summer School in Arithmetic Geometry, George-August Universität, Göttingen, Germany, August 1–2, 2006
- *Computational aspects of Shimura curves*, Magma 2006 conference, Technische Universität, Berlin, Germany, July 30, 2006
- *Special lecture series: Shimura curves (3 lectures)*
  University of Sydney, Australia, April 4, 7, 11, 2006
- *Computing zeta functions of Δ-regular hypersurfaces*, Number Theory Seminar, University of California, Irvine, April 22, 2005
- *Quadratic forms that represent almost the same primes*
  Colloquium, Wake Forest University, Winston-Salem, North Carolina, May 2, 2005
  Explicit algebraic number theory, Institut Henri Poincaré, Paris, October 12, 2004
  Colloquium, Santa Clara University, September 28, 2004
  Modular Seminar, Harvard University, April 20, 2004
- *Introduction to stacks*, Basic Notions Seminar, Harvard University, April 19, 2004

Selected Contributed Talks

- *Enumeration of totally real number fields*
  Vermont Number Theory Seminar, University of Vermont, Burlington, October 11, 2007
- *Escher and the Droste effect*
  Math Day (Vermont High School Mathematics Contest), University of Vermont, Burlington, May 15, 2007
  Undergraduate Math Club Lecture, University of Minnesota, Minneapolis, March 29, 2007

- *Zeta functions of varieties over finite fields* (2 lectures), Institute for Mathematics and its Applications (IMA), University of Minnesota, Minneapolis, November 14, December 12, 2006
- *Algorithms for quaternion algebras*, SAGE Days 2, University of Washington, Seattle, October 8, 2006
- *Computing CM points on Shimura curves arising from cocompact arithmetic triangle groups*, Algorithmic Number Theory Symposium (ANTS) VII, Technische Universität, Berlin, Germany, July 27, 2006
- *Computing maximal orders for quaternion algebras*, Explicit methods in number theory, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, Germany, July 18, 2005
- *Quadratic forms that represent almost the same primes*
  Number Theory Seminar, Universiteit Leiden, Netherlands, December 11, 2003
  Number Theory Seminar, University of California, Berkeley, April 30, 2003
- *Computing the reciprocity law for CM points on Shimura curves*
  Number theory and algebraic geometry in Magma, Institut Henri Poincaré, October 5, 2004
  Number Theory Seminar, University of California, Berkeley, September 1, 2004
- *Modular curves as coarse moduli spaces*, Semester Course, University of California, Berkeley, Spring 2003
- *Representation of primes by quadratic forms*, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, Germany, November 16, 2002
- *Error-correcting codes using algebraic geometry*, Undergraduate Applied Mathematics Seminar, University of California, Berkeley, March 1, 2002
- *Height functions defined by line bundles*, Arithmetic Geometry Seminar, University of California, Berkeley, February 5 and 12, 2002
- *On the nonexistence of odd perfect numbers*, West Coast Number Theory Conference, Asilomar Center, Monterey, California, December 16, 1999

Mathematical Activities and Professional Experience

- Referree, Lect. Notes in Comp. Sci., J. of Comb. Theory (Ser. A)
- Mentor, Association for Women Mathematicians (AWM), Fall 2007–present
- Reviewer, Math. Reviews, Spring 2006–present
- Berichterstatter, Explicit methods in number theory, Mathematisches Forschungsinstitut Oberwolfach, July 17–23, 2005, published in *Oberwolfach reports*, European Mathematical Society, vol. 2, no. 3, 2005, 1799–1866.
- Visitor, Institut Henri Poincaré, Fall 2004
- Web Liaison, Future directions in algorithmic number theory, American Institute of Mathematics, `http://www.aimath.org/WWN/primesinp/`, March 24–28, 2003
- Web Coordinator, Lenstra Treurfeest, University of California, Berkeley, March 21–23, 2003
- Visitor, Universiteit Leiden, Fall 2002
- Analyst, Education Program for Gifted Youth (EPGY), Summer 2000
  Analyzed the question-and-answer session of computerized mathematics courses (through calculus) for gifted students. Categorized problem types by content and input and made recommendations to improve pedadogy and implementation.
- Volunteer, Math Nerds (`http://www.mathnerds.com`), Summer 2000–Summer 2002
- Representative, Mathematical Graduate Student Association (MGSA), 2000–2002

- Participating Student Researcher, Summer 1997–Summer 1998
  Center for the Design of Analog-Digital Integrated Circuits (CDADIC)
  Supervised by Massimo Capobianchi, Gonzaga University
- Member, American Mathematical Society (AMS), 1999–2004, 2007–present
- Member, Mathematical Association of America (MAA), 1994–1995, 2001–2002
- Participant, Mathematics Advanced Study Semester (MASS), Penn State University, State College, Pennsylvania, Fall 1998
- Computer analyst, Docent Inc., Summer 1996

University Service

- **Departmental committee member**
  Putnam committee (2007–2008)
  Colloquium committee (2007–2008)
  High school contest committee (2007–2008)
- Graduate faculty appointment, Fall 2007–present
- Academic Integrity Council member, Center for Student Ethics and Standards, Fall 2007–present
- Volunteer, Lawrence Debate Union, University of Vermont, Fall 2007–present

Skills

- **Computer skills**: Programming in C, C++, Java, Visual Basic, Lisp; HTML, Unix, LaTeX; Magma, Maple, Mathematica, Pari-GP, Macaulay, Singular, CoCoA
- **All-American college debater**: Analytic communication at a nationally competitive level
- **Background**: A meticulous outlook in all pursuits as a result of training in engineering, mathematics, computer science, and debate tempered with an artistic and creative outlook grounded in a liberal arts tradition

Selected Conferences Attended

- Conference in honour of John Labute, McGill University and Centre de Recherche Mathématiques (CRM), Montréal, Québec, November 15–16, 2007
- L-functions and Modular Forms, American Institute of Mathematics, Palo Alto, California, July 30–August 3, 2007
- Journées Arithmétiques, University of Edinburgh, Scotland, July 2–6, 2007
- Arizona Winter School: p-adic Geometry, University of Arizona, Tucson, Arizona, March 10–14, 2007
- Explicit Methods for Rational Points on Curves, BIRS, Banff, Alberta, February 4–9, 2007
- Clay Summer School in Arithmetic Geometry, Georg-August Universität, Göttingen, Germany, July 17–August 11, 2006
- Algorithmic Number Theory Symposium (ANTS) VII, Technische Universität, Berlin, Germany, July 23–29, 2006
- Recent Developments in the Arithmetic of Shimura Varieties and Arakelov Geometry, Centre de Recerca Matemàtica (CRM), Universitat Autònoma de Barcelona, Bellaterra, Spain, July 10–15, 2006
- Intersection of Arithmetic Cycles and Automorphic Forms, Centre de Recherches Mathématiques (CRM), Montréal, Québec, December 12–16, 2005
- Summer Institute in Algebraic Geometry, AMS, Seattle, Washington, August 1–12, 2005

- Explicit Methods in Number Theory, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, Germany, July 17–23, 2005
- Explicit Arithmetic Geometry, Institut Henri Poincaré, Paris, France, December 6–10, 2004
- Algorithmic Number Theory Symposium (ANTS) VI, University of Vermont, Burlington, Vermont, June 13–16, 2004
- Special Points on Shimura Varieties, Lorentz Center, Leiden, the Netherlands, December 15–19, 2003
- Progress on the Birch and Swinnerton-Dyer Conjecture, Princeton University, New Jersey, November 5–7, 2003
- Future Directions in Algorithmic Number Theory, American Institute of Mathematics, Palo Alto, California, March 24–28, 2003
- Lenstra Treurfeest, University of California, Berkeley, March 21–23, 2003
- AMS-MAA Joint Mathematics Meeting, Baltimore, Maryland, January 15–18, 2003
- Rational and Integral Points on Higher Dimensional Varieties, American Institute of Mathematics, Palo Alto, California, December 11–20, 2002
- Explicit Algebraic Number Theory, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, Germany, November 10–16, 2002
- Perspectives in Classification and Moduli Spaces, Il Palazzone, Cortona, Italy, October 14–19, 2002
- Explicit Algebraic Number Theory (Stieltjes Onderwijsweek, NWO-OTKA Workshop), Lorentz Center, Leiden, the Netherlands, September 23–October 2, 2002
- Algorithmic Number Theory Symposium (ANTS) V, University of Sydney, Sydney, Australia, July 7–12, 2002
- Learning Stacks and Computational Methods through Problem-Solving, University of Illinois, Urbana-Champaign, Illinois, June 12–15, 2002