John Voight

Department of Mathematics
Dartmouth College
6188 Kemeny Hall
Hanover, NH 03755, USA

jvoight@gmail.com
http://www.math.dartmouth.edu/~jvoight/

Born in Savannah, Georgia, USA

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 Sydney**
  Professor of Mathematics, starting August 2024
- **Dartmouth College**
  Research Professor of Mathematics, July 2024–June 2026
  Professor of Mathematics, July 2020–June 2024
  Associate Professor of Mathematics, July 2013–June 2020
- **University of Vermont**
  Assistant Professor of Mathematics, September 2007–June 2013
  Assistant Professor of Computer Science, November 2011–June 2013
- **McGill University** and **Centre de Recherches Mathématiques (CRM)**
  Visiting Researcher, January–April 2010
- **University of Minnesota**
  Postdoctoral Fellow, Institute for Mathematics and its Applications (IMA),
  September 2006–August 2007
- **University of Sydney**
  Visiting Scholar, Magma Computational Algebra Group, August 2005–June 2006

Research Interests

- **Arithmetic algebraic geometry**
  Modular curves, Shimura varieties, moduli spaces, elliptic curves and abelian varieties, modular and automorphic forms, zeta functions of varieties over finite fields, computational and algorithmic aspects
- **Algebra and number theory**
  Algebraic number theory, quaternion algebras, quadratic forms, finite-dimensional algebras, elementary number theory, cryptography, coding theory

Date: March 10, 2024

Honors, Awards, and Grants

- ◇ Simons Collaborations in the Mathematics and the Physical Sciences Award, *Arithmetic geometry, number theory, and computation* (550029), PI (with Brendan Hassett, director, and Jennifer Balakrishnan, Noam Elkies, Bjorn Poonen, and Andrew Sutherland, PIs), \$949 378 (total collaboration award \$8 million), September 2017–August 2021; renewal, \$1 015 903 (total collaboration award \$6 million), September 2021–August 2024
- ◇ 2019–2020 John M. Manley Huntington Award for Newly Promoted Faculty, Dartmouth College, July 2020
- ◇ NSF Division of Mathematical Sciences Award, Algebra, Number Theory, and Combinatorics, *Arithmetic, Algebra, and Algorithms* (DMS-1954475, conference award), PI, \$33 000, April 2020–March 2021
- ◇ NSF Division of Mathematical Sciences Award, Algebra, Number Theory, and Combinatorics, *ANTS XIV: Algorithmic Number Theory Symposium 2020* (DMS-1946311, conference award), PI (with Drew Sutherland and Kiran Kedlaya, co-PIs), \$34 800, June 2020–May 2021
- ◇ Selfridge Prize (with Michael Musty, Sam Schiavone, and Jeroen Sijsling), awarded by the Number Theory Foundation, Algorithmic Number Theory Symposium (ANTS) XIII, University of Wisconsin, Madison, July 2018

  Best paper accepted for presentation at ANTS
- ◇ Neukom Institute CompX Faculty Grant, *L-Functions and Modular Forms Database (LMFDB)*, PI (with Edgar Costa, co-PI), \$27 000, April 2016–May 2018
- ◇ NSF Division of Mathematical Sciences Award, Algebra, Number Theory, and Combinatorics, *Number theory: from arithmetic statistics to zeta elements II* (DMS-1519977, conference award), PI (with Carl Pomerance, co-PI), \$27 250, March 2015–February 2017
- ◇ NSF Division of Mathematical Sciences Award, Algebra, Number Theory, and Combinatorics, *Number theory: from arithmetic statistics to zeta elements* (DMS-1430032, conference award), PI (with Carl Pomerance, co-PI), \$49 999, August 2014–April 2015
- ◇ NSF Division of Mathematical Sciences Award, Algebra, Number Theory, and Combinatorics, *Impact of Computation on Number Theory* (DMS-1414219, conference award), co-PI (with Wen-Ching Li, PI), \$35 360, July 2014–July 2015
- ◇ NSF Division of Mathematical Sciences Award, Algebra, Number Theory, and Combinatorics, *CAREER: Explicit methods in arithmetic geometry* (DMS-1151047), \$400 000, July 2012–July 2018
- ◇ Milt Silveira Award, College of Engineering and Mathematical Sciences, University of Vermont, May 2011

  Junior faculty member that "best embodies a 'pioneering spirit', drive and potential to succeed at the highest levels of his or her profession"
- ◇ Selfridge Prize, awarded by the Number Theory Foundation, Algorithmic Number Theory Symposium (ANTS) IX, INRIA, Nancy, July 2010
- ◇ NSF Division of Mathematical Sciences Award, Algebra, Number Theory, and Combinatorics, *Quaternion algebras, Shimura curves, and modular forms: Algorithms and arithmetic* (DMS-0901971), \$74 775, July 2009–August 2011
- ◇ NSA Young Investigator's Grant, *Topics in number theory: Geometry, cohomology and algorithms* (H98230-09-1-0037), \$30 000, January 2009–December 2010
- ◇ NSF Graduate Research Fellowship, Fall 2000–Spring 2003
- ◇ NSF International Travel Award, Summer 2002
- ◇ NSF VIGRE Award, Fall 1999–Spring 2000

- ◇ William A. Garrigan, S.J. Award, Gonzaga University, May 1999
  Top academic achievement of a graduating senior
- ◇ Rank 107 in William Lowell Putnam Competition, December 1998
- ◇ Rhodes Scholarship Finalist, 1998
- ◇ National Merit Presidental Scholarship, Gonzaga University, 1995–1999

Publications

(80) *Kneser's method of neighbors*, Arch. Math. **121** (2023), 537–557.

> In a landmark paper published in 1957, Kneser introduced a method for enumerating classes in the genus of a definite, integral quadratic form. This method has been deeply influential, on account of its theoretical importance as well as its practicality. In this survey, we exhibit Kneser's method of neighbors and indicate some of its applications in number theory.

(78) *The value of mathematical storytelling: our perspective on giving talks* (with Bianca Viray), Notices Amer. Math. Soc. **70** (2023), no. 6, 928–931.

> We develop the perspective of mathematical storytelling in giving talks.

(77) *Counting elliptic curves over the rationals with a 7-isogeny* (with Grant Molnar), Res. Number Theory **9**:75 (2023), 31 pages.

> We count by height the number of elliptic curves over the rationals, both up to isomorphism over the rationals and over an algebraic closure, that admit a cyclic isogeny of degree 7.

(75) *Appendix A: Computing invertible ideals*, appendix to Stefano Marseglia and Harry Smit, *Ideal classes of orders in quaternion algebras*, J. Pure Appl. Algebra. **228** (July 2024), no. 7, 107649.

> We exhibit an algorithm to compute a set of representatives for the right class set of a quaternion order over a number ring.

(70) *Stickelberger's discriminant theorem for algebras* (with Asher Auel and Owen Biesel), Amer. Math. Monthly. **130** (2023), no. 7, 656–670.

> Stickelberger proved that the discriminant of a number field is congruent to 0 or 1 modulo 4. We generalize this to an arbitrary (not necessarily commutative) ring of finite rank over $\mathbb{Z}$ using techniques from linear algebra. Our proof relies on elementary matrix identities.

(66) *Triangular modular curves of small genus* (with Juanita Duque-Rosero), Res. Number Theory **9**:3 (2023), 26 pages.

> Triangular modular curves are a generalization of modular curves that arise from quotients of the upper half-plane by congruence subgroups of hyperbolic triangle groups. These curves also arise naturally as Belyi maps with monodromy $\mathrm{PGL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$. We present a computational approach to enumerate triangular modular curves of low genus, and we carry out this enumeration up to genus 2.

(65) *Definite orthogonal modular forms: computations, excursions, and discoveries* (with Eran Assaf, Dan Fretwell, Colin Ingalls, Adam Logan, and Spencer Secord), Res. Number Theory. **8**:70 (2022), 32 pages.

> We consider spaces of modular forms attached to definite orthogonal groups of low even rank and nontrivial level, equipped with Hecke operators defined by Kneser neighbours. After reviewing algorithms to compute with these spaces, we investigate endoscopy using theta series and a theorem of Rallis. Along the way, we exhibit many examples and pose several conjectures. As a first application, we express counts of Kneser neighbours in terms of coefficients of classical or Siegel modular forms, complementing work of Chenevier–Lannes. As a second application, we prove new instances of Eisenstein congruences of Ramanujan and Kurokawa–Mizumoto type.

(64) *Computing Euclidean Belyi maps* (with Matthew Radosevich), J. Théorie Nombres Bordeaux **35** (2023), no. 2, 543–565.

We exhibit an explicit algorithm to compute three-point branched covers of the complex projective line when the uniformizing triangle group is Euclidean.

(63) *Appendix A: Jacobians of arbitrary modular curves* (with Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown), appendix to Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$*, Forum Math. Sigma. **10** (2022), e62.

We generalize Ribet's observation that the simple abelian varieties attached to newforms on $\Gamma_1(N)$ are of GL_2-type to the curves X_H; this extends Kolyvagin's theorem that analytic rank zero implies algebraic rank zero to isogeny factors of J_H.

(62) *The L-Functions and Modular Forms Database* (with John Cremona, John Jones, and Andrew V. Sutherland), Notices Amer. Math. Soc. **68** (2021), no. 9, 1520–1522.

We describe the *L-Functions and Modular Forms Database* (LMFDB), a resource for researchers in number theory and related areas.

(61) *A canonical form for positive definite matrices* (with Mathieu Dutour Sikirić, Anna Haensch, and Wessel P.J. van Woerden, Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV), ed. Steven Galbraith, Open Book Series 4, Mathematical Sciences Publishers, Berkeley, 2020, 179–195.

We exhibit an algorithm for finding a canonical form for a positive definite matrix under unimodular integral transformations. The method uses characteristic sets of short vectors and partition-backtracking graph software, and it is much more efficient than canonical forms based on Minkowski reduction. We present an extension of this formalism to the symplectic group as well as finite index subgroups. We then present applications to a database of lattices, genus enumeration, algebraic modular forms, and perfect form enumeration.

(60) *A Prym variety with everywhere good reduction over $\mathbb{Q}(\sqrt{61})$* (with Nicolas Mascot and Jeroen Sijsling), Arithmetic Geometry, Number Theory, and Computation, eds. Jennifer S. Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, Andrew V. Sutherland, and John Voight, Simons Symp., Springer, Cham, 2021, 559–581.

We compute an equation for a modular abelian surface A that has everywhere good reduction over the quadratic field $K = \mathbb{Q}(\sqrt{61})$ and that does not admit a principal polarization over K.

(59) *Counting elliptic curves with an isogeny of degree three* (with Maggie Pizzo and Carl Pomerance), Proc. Amer. Math. Soc. Ser. B **7** (2020), 28–42.

We count by height the number of elliptic curves over $\mathbb{Q}$ that possess an isogeny of degree 3.

(58) *Computing classical modular forms* (with Alex J. Best, Jonathan Bober, Andrew R. Booker, Edgar Costa, John Cremona, Maarten Derickx, David Lowry-Duda, Min Lee, David Roe, and Andrew V. Sutherland), Arithmetic Geometry, Number Theory, and Computation, eds. Jennifer S. Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, Andrew V. Sutherland, and John Voight, Simons Symp., Springer, Cham, 2021, 131–213.

We discuss practical and some theoretical aspects of computing a database of classical modular forms in the L-functions and Modular Forms Database (LMFDB).

(57) *On a probabilistic local-global principle for torsion on elliptic curves* (with John Cullinan and Meagan Kenney), J. Théorie Nombres Bordeaux, **34** (2022), no. 1, 41–90.

Let m be a positive integer and let E be an elliptic curve over $\mathbb{Q}$ with the property that $m \mid \#E(\mathbb{F}_p)$ for a density 1 set of primes p. Building upon work of Katz and Harron–Snowden, we study the probability that $m \mid \#E(\mathbb{Q})_{\mathrm{tors}}$: we find it is nonzero for all $m \in \{1, 2, \ldots, 10\} \cup \{12, 16\}$ and we compute it exactly when $m \in \{1, 2, 3, 4, 5, 7\}$. As a supplement, we give an asymptotic count of elliptic curves with extra level structure when the parametrizing modular curve arises from the quotient by a torsion-free group of genus zero.

(56) *On rational Bianchi newforms and abelian surfaces with quaternionic multiplication* (with John Cremona, Lassina Dembélé, Ariel Pacetti, and Ciaran Schembri), Arithmetic Geometry, Number Theory, and Computation, eds. Jennifer S. Balakrishnan, Noam Elkies,

Brendan Hassett, Bjorn Poonen, Andrew V. Sutherland, and John Voight, Simons Symp., Springer, Cham, 2021, 343–363.

> We study the rational Bianchi newforms (weight 2, trivial character, with rational Hecke eigenvalues) in the LMFDB that are not associated to elliptic curves, but instead to abelian surfaces with quaternionic multiplication. Two of these examples exhibit a rather special kind of behaviour: we show they arise from twisted base change of a classical newform with nebentypus character of order 4 and many inner twists.

(55) *Special hypergeometric motives and their L-functions: Asai recognition* (with Lassina Dembélé, Alexei Panchishkin, and Wadim Zudilin), Exp. Math. **31** (2022), no. 4, 1278–1290.

> We recognize certain special hypergeometric motives, related to and inspired by the discoveries of Ramanujan more than a century ago, as arising from Asai L-functions of Hilbert modular forms.

(51) *The Belyi degree of a curve is computable* (with Ariyan Javanpeykar), Arithmetic geometry: computation and applications, Contemp. Math., vol. 722, 2019, Amer. Math. Soc., Providence, RI, 43–57.

> We exhibit an algorithm that, given input a curve X over a number field, computes as output the minimal degree of a Belyi map $X \to \mathbb{P}^1$.

(50) *On unit signatures and narrow class groups of odd degree abelian number fields* (with Benjamin Breen and Ila Varma; appendix with Benjamin Breen, Noam Elkies, and Ila Varma), Trans. Amer. Math. Soc. Ser. B **10** (2023), 86–128.

> For an abelian number field of odd degree, we study the structure of its 2-Selmer group as a bilinear space and as a Galois module. We prove structural results and make predictions for the distribution of unit signature ranks and narrow class groups in families where the degree and Galois group are fixed.

(49) *Identifying central endomorphisms of an abelian variety via Frobenius endomorphisms* (with Edgar Costa and Davide Lombardo), Res. Number Theory **7**:46 (2021), 14 pages.

> Assuming the Mumford–Tate conjecture, we show that the center of the endomorphism ring of an abelian variety defined over a number field can be recovered from an appropriate intersection of the fields obtained from its Frobenius endomorphisms. We then apply this result to exhibit a practical algorithm to compute this center.

(48) *On basic and Bass quaternion orders* (with Sara Chari and Daniel Smertnig), Proc. Amer. Math. Soc. Ser. B **8** (2021), 11–26.

> A quaternion order $\mathcal{O}$ over a Dedekind domain R is Bass if every R-superorder is Gorenstein, and $\mathcal{O}$ is basic if it contains an integrally closed quadratic R-order. In this article, we show that these conditions are equivalent in local and global settings: a quaternion order is Bass if and only if it is basic. In particular, we show that the property of being basic is a local property of a quaternion order.

(47) *Sylvester's problem and mock Heegner points* (with Samit Dasgupta), Proc. Amer. Math. Soc. **146** (2018), no. 8, 3257–3273.

> We prove that if $p \equiv 4, 7 \pmod 9$ is prime and 3 is not a cube modulo p, then both of the equations $x^3 + y^3 = p$ and $x^3 + y^3 = p^2$ have a solution with $x, y \in \mathbb{Q}$.

(46) *Definite orders with locally free cancellation* (with Daniel Smertnig), Trans. Lond. Math. Soc. **6** (2019), vol. 1, 53–86.

> We enumerate all orders in definite quaternion algebras over number fields with the Hermite property; this includes all orders with the cancellation property for locally free modules.

(45) *Rigorous computation of the endomorphism ring of a Jacobian* (with Edgar Costa, Nicolas Mascot, and Jeroen Sijsling), Math. Comp. **88** (2019), 1303–1339.

> We describe several improvements to algorithms for the rigorous computation of the endomorphism ring of the Jacobian of a curve defined over a number field.

(44) *A database of Belyi maps* (with Michael Musty, Sam Schiavone, and Jeroen Sijsling), Proceedings of the Thirteenth Algorithmic Number Theory Symposium (ANTS-XIII), eds.

Renate Scheidler and Jonathan Sorenson, Open Book Series 2, Mathematical Sciences Publishers, Berkeley, 2019, 375–392.

> We use a numerical method to compute a database of three-point branched covers of the complex projective line of small degree. We report on some interesting features of this data set, including issues of descent.

(43) *Hypergeometric decomposition of symmetric K3 quartic pencils* (with Charles F. Doran, Tyler L. Kelly, Adriana Salerno, Steven Sperber, and Ursula Whitcher), Res. Math. Sci. **7**:7 (2020), 81 pages.

> We study the hypergeometric functions associated to five one-parameter deformations of Delsarte K3 quartic hypersurfaces in projective space. We compute all of their Picard–Fuchs differential equations; we count points using Gauss sums and rewrite this in terms of finite field hypergeometric sums; then we match up each differential equation to a factor of the zeta function, and we write this in terms of global L-functions. This computation gives a complete, explicit description of the motives for these pencils in terms of hypergeometric motives.

(42) *A database of Hilbert modular forms* (with Steve Donnelly), Arithmetic Geometry, Number Theory, and Computation, eds. Jennifer S. Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, Andrew V. Sutherland, and John Voight, Simons Symp., Springer, Cham, 2021, 365–373.

> We describe the computation of tables of Hilbert modular forms of parallel weight 2 over totally real fields.

(41) *Zeta functions of alternate mirror Calabi–Yau families* (with Charles F. Doran, Tyler L. Kelly, Adriana Salerno, Steven Sperber, and Ursula Whitcher), Israel J. Math. **228** (2018), 665–705.

> We prove that if two Calabi-Yau invertible pencils have the same dual weights, then they share a common factor in their zeta functions. By using Dwork cohomology, we demonstrate that this common factor is related to a hypergeometric Picard–Fuchs differential equation. The factor in the zeta function is defined over the rationals and has degree at least the order of the Picard–Fuchs equation. As an application, we relate several pencils of K3 surfaces to the Dwork pencil, obtaining new cases of arithmetic mirror symmetry.

(39) *The* 2*-Selmer group of a number field and heuristics for narrow class groups and signature ranks of units* (with David S. Dummit; appendix with David S. Dummit and Richard Foote), Proc. London Math. Soc. **117** (2018), 682–726.

> We investigate in detail a homomorphism which we call the 2-Selmer signature map from the 2-Selmer group of a number field K to a nondegenerate symmetric space, in particular proving the image is a maximal totally isotropic subspace. Applications include precise predictions on the density of fields K with given narrow class group 2-rank and with given unit group signature rank. In addition to theoretical evidence, extensive computations for totally real cubic and quintic fields are presented that match the predictions extremely well. In an appendix with Richard Foote, we classify the maximal totally isotropic subspaces of orthogonal direct sums of two nondegenerate symmetric spaces over perfect fields of characteristic 2 and derive some consequences, including a mass formula for such subspaces.

(38) *On the paramodularity of typical abelian surfaces* (with Armand Brumer, Ariel Pacetti, Cris Poor, Gonzalo Tornaría, and David S. Yuen), Algebra & Number Theory **13** (2019), no. 5, 1145–1195.

> Generalizing the method of Faltings–Serre, we rigorously verify that certain abelian surfaces without extra endomorphisms are paramodular. To compute the required Hecke eigenvalues, we develop a method of specialization of Siegel paramodular forms to modular curves.

(37) *A database of genus* 2 *curves over the rational numbers* (with Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, and Dan Yasaki), LMS. J. Comput. Math. **19** (Special Issue A) (2016), 235–254.

We describe the construction of a database of genus 2 curves of small discriminant that includes geometric and arithmetic invariants of each curve, its Jacobian, and the associated L-function. This data has been incorporated into the L-Functions and Modular Forms Database (LMFDB).

(36) *A heuristic for boundedness of ranks of elliptic curves* (with Jennifer Park, Bjorn Poonen, and Melanie Matchett Wood), J. European Math. Soc. **21** (2019), no. 9, 2859–2903.

We present a heuristic that suggests that ranks of elliptic curves E over $\mathbb{Q}$ are bounded. In fact, it suggests that there are only finitely many E of rank greater than 21. Our heuristic is based on modeling the ranks and Shafarevich–Tate groups of elliptic curves simultaneously, and relies on a theorem counting alternating integer matrices of specified rank. We also discuss analogues for elliptic curves over other global fields.

(35) *On the arithmetic dimension of triangle groups* (with Steve Nugent), Math. Comp. **86** (2017), no. 306, 1979–2004.

Let $\Delta = \Delta(a, b, c)$ be a hyperbolic triangle group, a Fuchsian group obtained from reflections in the sides of a triangle with angles $\pi/a, \pi/b, \pi/c$ drawn on the hyperbolic plane. We define the arithmetic dimension of Δ to be the number of split real places of the quaternion algebra generated by Δ over its (totally real) invariant trace field. Takeuchi has determined explicitly all triples (a, b, c) with arithmetic dimension 1, corresponding to the arithmetic triangle groups. We show more generally that the number of triples with fixed arithmetic dimension is finite, and we present an efficient algorithm to completely enumerate the list of triples of bounded arithmetic dimension.

(34) *Nonvanishing of twists of L-functions attached to Hilbert modular forms* (with Nathan C. Ryan and Gonzalo Tornaría), LMS J. Comput. Math. **17** (Issue A) (2014), 330–348.

We describe algorithms for computing central values of twists of L-functions associated to Hilbert modular forms, carry out such computations for a number of examples, and compare the results of these computations to some heuristics and predictions from random matrix theory.

(33) *Commensurability classes of fake quadrics* (with Benjamin Linowitz and Matthew Stover), Selecta Math. (New. Ser.) **25**:48 (2019), 39 pages.

A fake quadric is a smooth projective surface that has the same rational cohomology as a smooth quadric surface but is not biholomorphic to one. We provide an explicit classification of all irreducible fake quadrics according to the commensurability class of their fundamental group. To accomplish this task, we develop a number of new techniques which allow one to explicitly bound the arithmetic invariants of a fake quadric and more generally of an arithmetic manifold of bounded volume arising from a form of SL_2 over a number field.

(32) *On explicit descent of marked curves and maps* (with Jeroen Sijsling), Res. Number Theory **2**:27 (2016), 35 pages.

We revisit a statement of Birch that the field of moduli for a marked three-point ramified cover is a field of definition. Classical criteria due to Dèbes and Emsalem can be used to prove this statement in the presence of a smooth point, and in fact these results imply more generally that a marked curve descends to its field of moduli. We give a constructive version of their results, based on an algebraic version of the notion of branches of a morphism and allowing us to extend the aforementioned results to the wildly ramified case. Moreover, we give explicit counterexamples for singular curves.

(31) *Lattice methods for algebraic modular forms on classical groups* (with Matthew Greenberg), Computations with modular forms, eds. Gebhard Böckle and Gabor Wiese, Contrib. Math. Comput. Sci., vol. 6, Springer, Berlin, 2014, 147–179.

We use Kneser's neighbor method and isometry testing for lattices due to Plesken and Souveigner to compute systems of Hecke eigenvalues associated to definite forms of classical reductive algebraic groups.

(30) *Small isospectral and nonisometric orbifolds of dimension* 2 *and* 3 (with Benjamin Linowitz), Math. Z. **281** (2015), no. 1, 523–569.

Revisiting a construction due to Vignéras, we exhibit small pairs of orbifolds and manifolds of dimension 2 and 3 arising from arithmetic Fuchsian and Kleinian groups that are Laplace isospectral (in fact, representation equivalent) but nonisometric.

(29) *Computing power series expansions of modular forms* (with John Willis), Computations with modular forms, eds. Gebhard Böckle and Gabor Wiese, Contrib. Math. Comput. Sci., vol. 6, Springer, Berlin, 2014, 331–361.

We exhibit a method to numerically compute power series expansions of modular forms on a cocompact Fuchsian group Γ, using the explicit computation a fundamental domain and linear algebra.

(28) *On computing Belyi maps* (with Jeroen Sijsling), Publ. Math. Besançon: Algèbre Théorie Nr. 2014/1, Presses Univ. Franche-Comté, Besançon, 73–131.

We survey methods to compute Belyĭ maps, three-point branched covers of the projective line. These methods include a direct approach, solving a system of polynomial equations, as well as complex analytic methods, modular forms methods, and p-adic methods. Along the way, we pose several questions and provide numerous examples.

(27) *Discriminants and the monoid of quadratic rings*, Pacific J. Math. **283** (2016), no. 2, 483–510.

We consider the natural monoid structure on the set of quadratic rings over an arbitrary base scheme and characterize this monoid in terms of discriminants.

(26) *Explicit methods for Hilbert modular forms* (with Lassina Dembélé), Elliptic curves, Hilbert modular forms and Galois deformations, Birkhauser, Basel, 2013, 135–198.

We exhibit algorithms to compute systems of Hecke eigenvalues for spaces of Hilbert modular forms over a totally real field. We provide many explicit examples as well as applications to modularity and Galois representations.

(25) *Rings of low rank with a standard involution*, Illinois J. Math. **55** (2011), no. 3, 1135–1154.

We consider the problem of classifying (possibly noncommutative) R-algebras of low rank over an arbitrary base ring R. We first classify algebras by their degree, and we relate the class of algebras of degree 2 to algebras with a standard involution. We then investigate a class of exceptional rings of degree 2 which occur in every rank $n \geq 1$ and show that they essentially characterize all algebras of degree 2 and rank 3.

(24) *The canonical ring of a stacky curve* (with David Zureick-Brown), Mem. Amer. Math. Soc. **277** (2022), no. 1362.

Generalizing the classical theorems of Max Noether and Petri, we describe generators and relations for the canonical ring of a stacky curve, including an explicit Gröbner basis. We work in a general algebro-geometric context and treat log canonical and spin canonical rings as well. As an application, we give an explicit presentation for graded rings of modular forms arising from finite-area quotients of the upper half-plane by Fuchsian groups.

(23) *Numerical calculation of three-point branched covers of the projective line* (with Michael Klug, Michael Musty, and Sam Schiavone), LMS J. Comput. Math. **17** (2014), no. 1, 379–430.

We exhibit a numerical method to compute three-point branched covers of the complex projective line. We develop algorithms for working explicitly with Fuchsian triangle groups and their finite index subgroups, and we use these algorithms to compute power series expansions of modular forms on these groups.

(22) *Computing automorphic forms on Shimura curves over fields with arbitrary class number*, Algorithmic number theory (ANTS IX, Nancy, France, 2010), eds. Guillaume Hanrot, Francois Morain, and Emmanuel Thomé, Lecture Notes in Comp. Sci., vol. 6197, Springer, Berlin, 2010, 357–371.

We extend methods of Greenberg and the author to compute effectively with the cohomology of a Shimura curve over a totally real field with arbitrary class number. Via the Jacquet-Langlands correspondence, we thereby compute systems of Hecke eigenvalues associated to Hilbert modular

forms of arbitrary level over a totally real field of odd degree. We conclude with two examples which illustrate the effectiveness of our algorithms.

(21) *Nondegenerate curves of low genus over small finite fields* (with Wouter Castryck), Arithmetic, Geometry, Cryptography and Coding Theory 2009, Contemp. Math., vol. 521, Amer. Math. Soc., Providence, RI, 2010, 21–28.

In a previous paper, we proved that over a finite field k of sufficiently large cardinality, all curves of genus at most 3 over k can be modeled by a bivariate Laurent polynomial that is nondegenerate with respect to its Newton polytope. In this paper, we prove that there are exactly two curves of genus at most 3 over a finite field that are *not* nondegenerate, one over $\mathbb{F}_2$ and one over $\mathbb{F}_3$. Both of these curves have remarkable extremal properties concerning the number of rational points over various extension fields.

(20) *Nonsolvable number fields ramified only at* 3 *and* 5 (with Lassina Dembélé and Matthew Greenberg), Compositio Math. **147** (2011), no. 3, 716–734.

For $p = 3$ and $p = 5$, we exhibit a finite nonsolvable extension of $\mathbb{Q}$ which is ramified only at p via explicit computations with Hilbert modular forms.

(19) *Characterizing quaternion rings over an arbitrary base*, J. Reine Angew. Math. **657** (2011), 113–134.

We consider the class of algebras of rank 4 equipped with a standard involution over an arbitrary base ring. In particular, we characterize quaternion rings, those algebras defined by the construction of the even Clifford algebra.

(18) *Computing systems of Hecke eigenvalues associated to Hilbert modular forms* (with Matthew Greenberg), Math. Comp. **80** (2011), 1071–1092.

We utilize effective algorithms for computing in the cohomology of a Shimura curve together with the Jacquet-Langlands correspondence to compute systems of Hecke eigenvalues associated to Hilbert modular forms over a totally real field F.

(17) *Algebraic curves uniformized by congruence subgroups of triangle groups* (with Pete L. Clark), Trans. Amer. Math. Soc. **371** (2019), no. 1, 33–82.

We construct certain subgroups of hyperbolic triangle groups which we call "congruence" subgroups. These groups include the classical congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, Hecke triangle groups, and 19 families of Shimura curves associated to arithmetic triangle groups. We determine the field of moduli of the curves associated to these groups and thereby realize the Galois groups $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ regularly.

(16) *Computing zeta functions of nondegenerate hypersurfaces with few monomials* (with Steven Sperber), LMS J. Comput. Math. **16** (2013), 9–44.

Using the cohomology theory of Dwork, as developed by Adolphson and the first author, we exhibit a deterministic algorithm to compute the zeta function of a nondegenerate hypersurface defined over a finite field. This algorithm is particularly well-suited to work with polynomials in small characteristic that have few monomials (relative to their dimension). Our method covers toric, affine, and projective hypersurfaces and also computes the L-function of an exponential sum.

(15) *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, Quadratic and higher degree forms, eds. K. Alladi, M. Bhargava, D. Savitt, and P.H. Tiep, Developments in Math., vol. 31, Springer, New York, 2013, 255–298.

We discuss the relationship between quaternion algebras and quadratic forms with a focus on computational aspects. Our basic motivating problem is to determine if a given algebra of rank 4 over a commutative ring R embeds in the 2×2-matrix ring $\mathrm{M}_2(R)$ and, if so, to compute such an embedding. We discuss many variants of this problem, including algorithmic recognition of quaternion algebras among algebras of rank 4, computation of the Hilbert symbol, and computation of maximal orders.

(14) *Algorithmic enumeration of ideal classes for quaternion orders* (with Markus Kirschmer), SIAM J. Comput. (SICOMP) **39** (2010), no. 5, 1714–1747; *Corrigendum: Algorithmic*

enumeration of ideal classes for quaternion orders, SIAM J. Comput. (SICOMP) **41** (2012), no. 3, 714.

We provide algorithms to count and enumerate representatives of the (right) ideal classes of an Eichler order in a quaternion algebra defined over a number field. We analyze the run time of these algorithms and consider several related problems, including the computation of two-sided ideal classes, isomorphism classes of orders, connecting ideals for orders, and ideal principalization. We conclude by giving the complete list of definite Eichler orders with class number at most 2.

(13) *The Gauss higher relative class number problem*, Ann. Sci. Math. Québec **32** (2008), no. 2, 221–232.

Assuming the 2-adic Iwasawa main conjecture, we find all CM fields with higher relative class number at most 16: there are at least 31 and at most 34 such fields, and exactly one is not abelian.

(12) *Shimura curves of genus at most two*, Math. Comp. **78** (2009), 1155–1172.

We enumerate all Shimura curves $X_0^{\mathfrak{D}}(\mathfrak{N})$ of genus at most two: there are exactly 858 such curves, up to equivalence.

(11) *Computing fundamental domains for Fuchsian groups*, J. Théorie de Nombres de Bordeaux **21** (2009), no. 2, 467–489.

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

(10) *On nondegeneracy of curves* (with Wouter Castryck), Algebra & Number Theory **3** (2009), no. 3, 255–281.

We study the conditions under which an algebraic curve can be modelled by a Laurent polynomial that is nondegenerate with respect to its Newton polytope. We prove that every curve of genus $g \leq 4$ over an algebraically closed field is nondegenerate in the above sense. More generally, let $\mathcal{M}_g^{\mathrm{nd}}$ be the locus of nondegenerate curves inside the moduli space of curves of genus $g \geq 2$. Then we show that $\dim \mathcal{M}_g^{\mathrm{nd}} = \min(2g+1, 3g-3)$, except for $g = 7$ where $\dim \mathcal{M}_7^{\mathrm{nd}} = 16$; thus, a generic curve of genus g is nondegenerate if and only if $g \leq 4$.

(9) *Enumeration of totally real number fields of bounded root discriminant*, Algorithmic number theory (ANTS VIII, Banff, 2008), eds. Alfred van der Poorten and Andreas Stein, Lecture Notes in Comp. Sci., vol. 5011, Springer, Berlin, 2008, 268–281.

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

(8) *Shimura curve computations*, Arithmetic Geometry, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, RI, 2009, 103–113.

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), Arithmetic Geometry, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, RI, 2009, 91–102.

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.

(6) *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.

(5) *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 Comp. Sci., vol. 4076, Springer, Berlin, 2006, 406–420.

Let $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ 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.

(3) *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.

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

In the first part, we prove a result concerning representation of primes by quadratic forms. 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. We confirm their conjecture, and in fact find all pairs of such forms that represent the same primes outside of a finite set.

In the second part, we investigate a constellation of results concerning algorithms for quaternion algebras and their application to Shimura curves. Let A be a quaternion algebra over a number field F. We discuss the computational complexity and, in many cases, give effective algorithms to solve the following problems:

- Determine if $A \cong M_2(F)$, and if so, exhibit an isomorphism;
- Find a maximal order $\mathcal{O} \subset A$; and
- Determine if a right ideal $I \subset \mathcal{O}$ is principal, and if so, exhibit a generator ξ.

We then present fast methods for computing the value of hypergeometric series to large precision. Putting these together, we are able to compute special values of the map $j : \Gamma \setminus \mathfrak{H} \to \mathbb{P}^1_{\mathbb{C}}$ for Γ a compact triangle group, which we may recognize as putative algebraic numbers by also computing their Galois conjugates. We apply this to construct the canonical polynomial $\Phi_{\mathfrak{N}}(x, y)$ for the curve $X_0(\mathfrak{N})$ and to find nontorsion points on some elliptic curves over number fields.

Publications: Books

(B2) *Arithmetic geometry, number theory, and computation* (editor with Jennifer S. Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, and Andrew V. Sutherland), Simons Symp., Springer, Cham, 2021. 587 pages.

This volume contains articles related to the work of the Simons Collaboration "Arithmetic Geometry, Number Theory, and Computation." The papers present mathematical results and algorithms necessary for the development of large-scale databases like the L-functions and Modular Forms Database (LMFDB). The authors aim to develop systematic tools for analyzing Diophantine properties of curves, surfaces, and abelian varieties over number fields and finite fields. The articles also explore examples important for future research.

(B1) *Quaternion algebras*, Grad. Texts in Math., vol. 288, Springer, Cham, 2021. 885 pages.

Quaternion algebras sit prominently at the intersection of many mathematical subjects. They capture essential features of noncommutative ring theory, number theory, K-theory, group theory, geometric topology, Lie theory, functions of a complex variable, spectral theory of Riemannian manifolds, arithmetic geometry, representation theory, the Langlands program—and the list goes on. Quaternion algebras are especially fruitful to study because they often reflect some of the

general aspects of these subjects, while at the same time they remain amenable to concrete argumentation. In this text, we introduce the topics above to graduate students interested in algebra, geometry, and number theory.

Publications: Accepted

(79) *A database of paramodular forms from quinary orthogonal modular forms* (with Eran Assaf, Watson Ladd, Gustavo Rama, and Gonzalo Tornaría), accepted to Contemp. Math.

We compute tables of paramodular forms of degree two and cohomological weight via a correspondence with orthogonal modular forms on quinary lattices.

(69) *A database of basic numerical invariants of Hilbert modular surfaces* (with Eran Assaf, Angelica Babei, Ben Breen, Edgar Costa, Juanita Duque-Rosero, Aleksander Horawa, Jean Kieffer, Avinash Kulkarni, Grant Molnar, and Sam Schiavone), accepted to Contemp. Math.

We describe algorithms for computing geometric invariants for Hilbert modular surfaces, and we report on their implementation.

Publications: Submitted

(72) *Appendix A: Polarized class sets of quaternion orders*, appendix to Jiangwei Xue and Chia-Fu Yu, *Trace formulas for the norm one group of totally definite quaternion algebras*, submitted.

We give an alternate, conceptual proof of the spinor class number formula using the notion of a polarization.

(68) *Rational torsion points on abelian surfaces with quaternionic multiplication* (with Jef Laga, Ari Shnidman, and Ciaran Schembri), submitted.

Let A be an abelian surface over $\mathbb{Q}$ whose geometric endomorphism ring is a maximal order in a non-split quaternion algebra. Inspired by Mazur's theorem for elliptic curves, we show that the torsion subgroup of $A(\mathbb{Q})$ is 12-torsion and has order at most 18. Under the additional assumption that A is of GL_2-type, we give a complete classification of the possible torsion subgroups of $A(\mathbb{Q})$.

(67) *Monodromy groups of Jacobians with definite quaternionic multiplication* (with Victoria Cantoral-Farfán and Davide Lombardo), submitted.

Let A be an abelian variety over a number field. The connected monodromy field of A is the minimal field over which the images of all the ℓ-adic torsion representations have connected Zariski closure. We show that for all even $g \geq 4$, there exist infinitely many geometrically nonisogenous abelian varieties A over $\mathbb{Q}$ of dimension g where the connected monodromy field is strictly larger than the field of definition of the endomorphisms of A. Our construction arises from explicit families of hyperelliptic Jacobians with definite quaternionic multiplication.

Publications: Preprints

(71) *On abelian varieties whose torsion is not self-dual* (with Sarah Frei and Katrina Honigs), preprint.

We construct infinitely many abelian surfaces A defined over the rational numbers such that, for $\ell \leqslant 7$ prime, the ℓ-torsion subgroup of A is not isomorphic as a Galois module to the ℓ-torsion subgroup of the dual $A^\vee$. We do this by analyzing the action of the Galois group on the ℓ-adic Tate module and its reduction modulo ℓ.

(54) *On Galois inertial types of elliptic curves over* $\mathbb{Q}_\ell$ (with Lassina Dembélé and Nuno Freitas), preprint.

We provide a complete, explicit description of the inertial Weil–Deligne types arising from elliptic curves over $\mathbb{Q}_\ell$ for ℓ prime.

Publications: Non peer-reviewed

(53) *Alternate mirror families and hypergeometric motives* (with Charles F. Doran, Tyler L. Kelly, Adriana Salerno, Steven Sperber, and Ursula Whitcher), 2017 MATRIX Annals, eds. David R. Wood, Jan de Gier, Cheryl E. Praeger, and Terence Tao, MATRIX Book Series, vol. 2, Springer Nature, Switzerland, 2019, 441–448.

> Mirror symmetry predicts surprising geometric correspondences between distinct families of algebraic varieties. In some cases, these correspondences have arithmetic consequences. Among the arithmetic correspondences predicted by mirror symmetry are correspondences between point counts over finite fields, and more generally between factors of their Zeta functions. In particular, we will discuss our results on a common factor for Zeta functions of alternate families of invertible polynomials. We will also explore closed formulas for the point counts for our alternate mirror families of K3 surfaces and their relation to their Picard–Fuchs equations. Finally, we will discuss how all of this relates to hypergeometric motives. This report summarizes work from two papers.

(52) *Triangular modular curves*, 2017 MATRIX Annals, eds. David R. Wood, Jan de Gier, Cheryl E. Praeger, and Terence Tao, MATRIX Book Series, vol. 2, Springer Nature, Switzerland, 2019, 481–483.

> We consider certain generalizations of modular curves arising from congruence subgroups of triangle groups.

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

(1) *On the nonexistence of odd perfect numbers*, MASS Selecta: Teaching and learning advanced undergraduate mathematics, eds. Svetlana Katok, Alexei Sossinsky, and Serge Tabachnikov, 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

- **Associate Professor/Professor**, Dartmouth College
  - MATH 75: Mathematical Cryptography, Spring 2016, Spring 2024
  - MATH 101: Linear and Multilinear Algebra, Fall 2021, Fall 2022, Fall 2023
  - MATH 25: Number Theory, Fall 2018, Fall 2020, Fall 2023
  - MATH 71: Algebra, Fall 2022
  - MATH 31: Topics in Algebra, Summer 2021, Summer 2022
  - MATH 11: Accelerated Multivariable Calculus, Fall 2014, Fall 2016, Fall 2017, Fall 2021
  - MATH 105: Introduction to Linear Algebraic Groups, Winter 2021
  - MATH 81/111: Rings and Fields, Winter 2015, Winter 2019, Winter 2021
  - MATH 17: An Introduction to Mathematics Beyond Calculus, Spring 2019
  - MATH 125: Explicit Methods for Hilbert Modular Surfaces, Winter 2018
  - MATH 101: Topics in Algebra, Fall 2016, Fall 2017
  - MATH 24: Linear Algebra, Spring 2017
  - MATH 115: Elliptic Curves, Spring 2016
  - MATH 125: Geometry of Discrete Groups, Summer 2015
  - MATH 105: Algebraic Number Theory, Fall 2014
  - MATH 125: Quaternion Algebras, Spring 2014
- **Assistant Professor**, University of Vermont
  - MATH 351: Riemann Surfaces and Dessins d'Enfants, Spring 2013

- MATH/CS 295: Mathematical Cryptography, Fall 2012
- MATH 052: Fundamentals of Mathematics, Fall 2011, Fall 2012
- MATH 252: Abstract Algebra II, Spring 2012, Spring 2008
- MATH 251: Abstract Algebra I, Fall 2011, Fall 2007
- MATH 295: Lie Theory, Summer 2011
- MATH 295/395: Cryptography, Fall 2010, Fall 2008
- MATH 241: Analysis in Several Real Variables I, Fall 2010, Fall 2009
- HONS 195: Enigma: A Social and Mathematical History of Cryptography, Fall 2009
- MATH 255: Elementary Number Theory, Spring 2009
- MATH 020: Calculus II, Fall 2008

▶ **Visiting Lecturer**, McGill University

- MATH 727: Quaternion Algebras: Algorithms and Arithmetic, Winter 2010

▶ **Graduate Student Instructor (GSI)**, University of California, Berkeley

- MATH 110: Linear Algebra, Spring 2005
- MATH 115: Elementary Number Theory, Summer 2004
- MATH 1A: Calculus, Spring 2004
- MATH 250B: Multilinear Algebra, Spring 2003
- MATH 195: Cryptography, Spring 2002
- MATH 1B: Calculus, Fall 2001

Advising

▶ **Ph.D. thesis advisor**

- Haochen Wu, Dartmouth College, expected May 2026
- Santiago Arango (co-advisor with David Zureick-Brown), Emory University, expected May 2025
- Juanita Duque-Rosero, *Triangular modular curves of low genus and geometric quadratic Chabauty*, Dartmouth College, May 2023
- Grant Molnar, *Counting elliptic curves with a cyclic m-isogeny over $\mathbb{Q}$*, Dartmouth College, May 2023
- Benjamin Breen, *The 2-Selmer group of number fields*, Dartmouth College, May 2020
- Michael Musty, *2-group Belyi maps*, Dartmouth College, July 2019
- Sam Schiavone, *On algebras of low rank and on Belyi maps*, Dartmouth College, July 2019
- Sara Chari, *Orders in quaternion and central simple algebras*, Dartmouth College, May 2019
- Jeffery Hein, *Orthogonal modular forms: an application to a conjecture of Birch, algorithms and computations*, Dartmouth College, May 2016

▶ **Postdoctoral mentor**

- Andrew Hanlon (JWY), September 2023–Spring 2024
- Shiang Tang, Fall 2023–Spring 2024
- Tristan Phillips (NSF MSPRF), Fall 2023–Spring 2024
- Angelica Babei (Simons Collaboration), March 2021–August 2021
- Avinash Kulkarni (Simons Collaboration), Winter 2020–Spring 2023
- Eran Assaf (Simons Collaboration), Fall 2019–Spring 2024
- Ciaran Schembri (Simons Collaboration), Fall 2019–Spring 2024

· Lassina Dembélé (Simons Collaboration), April 2018–March 2019
· Daniel Smertnig (Erwin Schrödinger Fellowship, FWF), October 2017–January 2018
· Edgar Costa (IACM), Winter 2016–Spring 2018
· Naomi Tanabe, Fall 2015–Spring 2017
· Jeroen Sijsling, Fall 2014–Winter 2016

▶ **Master's thesis advisor**

· Michael Klug, *Computing rings of modular forms via power series expansions*, University of Vermont, May 2013
· Alex Levin, *On the classification of algebras*, University of Vermont, May 2013
· Aurel Page, *Computing fundamental domains for arithmetic Kleinian groups*, École Normale Supérieure, August 2010

▶ **Undergraduate honors thesis advisor**

· Zachary Couvillion, *On specializations of Belyi maps and inverse Galois theory*, Dartmouth College, May 2022, winner of the Byrne Prize
· Jacob Swenberg, *Fields of moduli for QM abelian surfaces with CM*, James O. Freedman Presidential Scholar, Dartmouth College, May 2021, winner of the Byrne Prize and the Gazzaniga Award
· Matthew Radosevich, *Euclidean triangle groups and Belyi maps*, Dartmouth College, May 2020, winner of the Byrne Prize
· Prajeet Bajpai, *On class numbers as determinants of random matrices*, Dartmouth College, May 2016
· Steve Nugent, *A computational investigation of arithmetic triangle groups*, Dartmouth College, May 2015
· Barbara Abbott, *Investigating binary cubic forms*, University of Vermont, May 2009

▶ **Other graduate research projects**

· John Willis, *Power series expansions of modular forms*, University of Vermont, Summer 2010, Summer 2011
· Leona Sparaco, *Hauptman's continued fractions and units in pure cubic fields*, University of Vermont, Fall 2011

▶ **Other undergraduate research projects**

· Colin Glew, *Estimates for the mass of Belyi map passport*, Dartmouth College, Fall 2023
· Zachary Couvillion and Mitchell Jubeir, *On specialization of Belyi maps*, Dartmouth College, Spring 2021
· Ahmed Naveed, *Algorithmic enumeration of reduced ternary quadratic forms*, Dartmouth College, Spring 2021
· Eliza Crocker, *Reducibility of Belyi maps and resulting specializations of Galois groups*, Dartmouth College, Winter 2021
· Joshua Perlmutter, *Verifying monodromy groups of Belyi maps*, Dartmouth College, Spring–Summer 2018, Spring 2019, Summer 2020
· Maggie Pizzo, *Counting elliptic curves with a* 3*-isogeny*, Dartmouth College, Winter 2018
· Mauricio Esquivel Rogel, *Explicit methods in number theory: numerical linear algebra applied to computation of modular forms*, James O. Freedman Presidential Scholar, Dartmouth College, Fall 2016, Spring 2017

· Adenrele Adewusi, *Contributions of women to mathematics*, Poster art installation, Dartmouth College, Spring 2015
· Michael Novick, *Signature ranks of cubic fields*, University of Vermont, Winter–Summer 2013
· Kayla LeBlanc, *Arithmetic dimension of triangle groups*, University of Vermont, Summer 2012
· Suma Desu, *Computer algebra in systems biology*, University of Vermont, Fall 2009

Invited Lectures

◇ *Sato–Tate groups and automorphy for atypical abelian surfaces*
· Southern Regional Number Theory Conference 2024, Baton Rouge, March 10, 2024
· Session: Arithmetic Geometry, 2021 CMS 75th +1 Anniversary Summer Meeting, Ottawa (virtual), June 8, 2021
◇ *Two theorems on discriminants*, Colloquium, Wake Forest University, March 7, 2024
◇ *Computing with Hilbert modular surfaces*, Number Theory Seminar, Duke University, March 6, 2024
◇ *Hypergeometric identities for* $1/\pi^2$, AAG Colloquium, Washington University of St. Louis, February 29, 2024
◇ *Counting elliptic curves with level structure*
· Number Theory Seminar, University of Illinois, Chicago, February 28, 2024
· Number Theory Web Seminar, virtual, June 16, 2022
◇ *Abelian varieties whose torsion is not self-dual*, Number Theory Seminar, Ohio State University, Columbus, February 26, 2024
◇ *A norm refinement of Bézout's Lemma, quaternion orders, and generalized Kummer surfaces*, Algebra Seminar, Brown University, Providence, January 29, 2024
◇ *Polarized class sets of quaternion orders*, Joint Mathematics Meetings, San Francisco, January 4, 2024
◇ *On explicit moduli problems for Shimura curves*, Computational Algebra and Magma, University of Sydney, December 1, 2023
◇ *Lattice methods for modular forms*
· Colloquium, Rice University, Houston, August 24, 2023
· University of Sydney, June 13, 2023
◇ *Effective methods in inverse Galois theory*, Graduate Student Conference in Algebra, Geometry, and Topology (GTA), Temple University, Philadelphia, May 28, 2023
◇ *Zeta functions of cyclic branched covers from hypergeometric functions, and their degeneration*
· Dwork Seminar, virtual, May 3, 2023
· Conference on Algebraic Varieties over Finite Fields and Algebraic Geometry Codes (COGNAC), CIRM, Luminy, February 15, 2023
◇ *A norm refinement of Bézout's Lemma, and quaternion orders*, Lethbridge Number Theory and Combinatorics Seminar, Lethbridge, Alberta, March 6, 2023
◇ *On some families of Jacobians with definite quaternionic multiplication*, Symposium on Arithmetic Geometry and its Applications (SAGA), CIRM, Luminy, February 9, 2023
◇ *Identities for* $1/\pi^2$ *and special hypergeometric motives*
· No Boundaries, University of Chicago, February 2, 2023
· Southern California Number Theory Day, University of California, San Diego, February 22, 2020
· Number Theory Seminar, Vanderbilt University, Nashville, Tennessee, February 4, 2020

· Colloquium, Rutgers University, New Brunswick, November 13, 2019
· Colloquium, University of California, Berkeley, September 26, 2019
◇ *Ternary and quaternary quadratic forms, quaternions and quaternion ideal classes*, Special Session: Quadratic Forms, Modular Forms, and Applications, Joint Mathematics Meetings, Boston, January 7, 2023
◇ *A refinement of Bézout's Lemma and elements of order* 3 *in some rational quaternion algebras*, Special Session: Quaternions, Joint Mathematics Meetings, Boston, January 7, 2023
◇ *On the connected monodromy field of some families of Jacobians with definite quaternionic multiplication*, Special Session: Arithmetic Geometry Informed by Computation, Joint Mathematics Meetings, Boston, January 4, 2023
◇ *Canonical models for triangular modular curves*, Special Session: Modular Forms, Hypergeometric Functions, Character Sums, and Galois Representations, Joint Mathematics Meetings, Boston, January 4, 2023
◇ *Counting elliptic curves with a* 7*-isogeny*, Special Session: Algebraic and Analytic Theory of Elliptic Curves, AMS Fall Eastern Sectional Meeting, University of Massachusetts, Amherst, October 1, 2022
◇ *Orthogonal modular forms and their L-functions*, Research Seminar: Number Theory and Arithmetic Geometry, Leibniz Universität Hannover, Germany, April 22, 2022
◇ *Canonical models for triangular modular curves*
· Number Theory Lunch Seminar, Max Planck Institute of Mathematics (MPIM), Bonn, April 20, 2022
· Number Theory Seminar, MIT, Cambridge, May 9, 2017
◇ *A family of Jacobians with definite quaternionic multiplication*
· Joint Columbia–CUNY–NYU Number Theory Seminar, New York University (virtual), April 14, 2022
· Number Theory Seminar, Boston University, March 21, 2022
◇ *Computing classical modular forms as orthogonal modular forms*
· Special Session: Quadratic Forms, Theta Functions and Modularity, Joint Mathematics Meetings, Seattle (virtual), April 7, 2022
· Arithmetic, Geometry, Cryptography and Coding Theory (AGC^{2}T-16), CIRM, Luminy, June 21, 2017
◇ *Triangular modular curves*
· Colloquium, University of Michigan, Ann Arbor, March 8, 2022
· Hypergeometric Motives and Calabi–Yau Differential Equations, MATRIX, Creswick, Australia, January 19, 2017
◇ *Stickelberger's discriminant theorem for algebras*, Algebra and Number Theory Seminar, Universität Graz (virtual), January 20, 2022
◇ *Quaternions*
· Math Club, Carnegie Mellon University (virtual), January 19, 2022
· Undergraduate Mathematics Symposium, University of Illinois at Chicago (virtual), November 13, 2021
· Colloquium, Dartmouth College, September 30, 2021
◇ *Counting elliptic curves with torsion (and heights on stacky curves)*, Number Theory and Algebraic Geometry Seminar, Boston College, December 2, 2021
◇ *Some problems and questions*, Trimester Program on Triangle Groups, Belyi Uniformization, and Modularity, Bhaskaracharya Pratishthana, Pune, India (virtual), November 30, 2021

◇ *Definite quaternion orders with stable cancellation*

· Special Session: Algebraic Number Theory, 2021 CMS 75th +1 Anniversary Summer Meeting, Ottawa (virtual), June 8, 2021

· Pure Colloquium, University of Manchester (virtual), March 26, 2021

· Oregon Number Theory Days, Oregon State University, February 16, 2019

· Eighth Annual Upstate Number Theory Conference, University at Buffalo, April 28, 2018

◇ *Computing Belyi maps: a survey*, Seminar on Graphs on Surfaces and Curves over Number Fields, Lomonosov Moscow State University, May 19, 2021

◇ *Heuristics for boundedness of ranks of elliptic curves*

· Colloquium, McMaster University (virtual), April 9, 2021

· Colloquium, Penn State University, February 1, 2018

· Number Theory Seminar, Brigham Young University, December 6, 2016

· Special Session: Elliptic curves, AMS Spring Southeastern Sectional Meeting, University of Georgia, Athens, March 5, 2016

· Number Theory Seminar, University of Connecticut, Storrs, November 18, 2015

· Explicit Methods in Number Theory, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, July 9, 2015

· Five College Number Theory Seminar, University of Massachusetts, Amherst, February 24, 2015

· Number Theory Seminar, University of Rochester, February 4, 2015

◇ *Counting elliptic curves with torsion, and a probabilistic local-global principle*, Heilbronn Number Theory Seminar, University of Bristol (virtual), March 17, 2021

◇ *Toward rigorous monodromy and 1-parameter enumerative problems*, Monodromy and Galois Groups in Enumerative Geometry and Applications, ICERM, Brown University (virtual), September 2, 2020

◇ *Archimedean aspects of the Cohen–Lenstra heuristics*, Chicago Number Theory Day, University of Chicago, Illinois (virtual), June 20, 2020

◇ *The Belyi degree of a curve is computable*, Commutative Algebra and Algebraic Geometry: The Fellowship of the Ring, University of California, Berkeley, March 3, 2020

◇ *Zeta functions of alternate mirror Calabi–Yau families*, Special Session: Explicit Methods in Arithmetic Geometry in Characteristic p, Joint Mathematics Meetings, Denver, January 16, 2020

◇ *Two theorems counting elliptic curves*, Front Range Number Theory Day, Colorado State University, Fort Collins, November 16, 2019

◇ *Heuristics for units in number rings*, Colloquium, Louisiana State University, November 14, 2019

◇ *A Prym variety with everywhere good reduction over* $\mathbb{Q}(\sqrt{61})$, Arithmetic Geometry Seminar, Ohio State University, Columbus, November 12, 2019

◇ *Lecture series: Computing modular forms by automorphic and inertial type* (3 lectures), p-adic Langlands Correspondence: a Constructive and Algorithmic Approach, Centre Henri Lebesgue, Université de Rennes 1, September 2, 3, 5, 2019

◇ *The Faltings–Serre method, with applications*, International Workshop on Arithmetic Geometry and Quantum Field Theory, KIAS, Seoul, August 13, 2019

◇ *Lecture series: Computing endomorphism rings of Jacobians* (4 lectures), CMI-HIMR Summer School in Computational Number Theory, Heilbronn Institute for Mathematical Research, University of Bristol, June 24–28, 2019

◇ *Computing Belyi maps*

· Oregon Number Theory Days, Oregon State University, February 16, 2019

· Colloquium, Temple University, February 6, 2018

◇ *The L-functions and Modular Forms DataBase (LMFDB)*, Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation Annual Meeting, Simons Foundation, New York City, January 10, 2019

◇ *Rigorous computation of the endomorphism ring of a Jacobian*

· Explicit Methods in Number Theory, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, July 26, 2018

· Algebraic Geometry Seminar, NYU–Courant, May 1, 2018

· Arithmetic of Algebraic Curves, University of Wisconsin, Madison, April 7, 2018

· Number Theory Seminar, Brown University, March 5, 2018

◇ *Lecture series: Computational aspects of Shimura curves* (2 lectures, with Drew Sutherland), Building Bridges: 4th EU/US Summer School on Automorphic Forms and Related Topics, Alfréd Rényi Institute of Mathematics, Budapest, July 9–10, 2018

◇ *Mock Heegner points and Sylvester's conjecture*

· Algebra, Geometry and Number Theory Seminar, Tufts University, April 26, 2018

· Number Theory Seminar, Penn State University, February 1, 2018

· Heilbronn Number Theory Seminar, University of Bristol, June 14, 2017

◇ *Heuristics for units in number fields*

· PAlmetto Number Theory Series (PANTS) XXVIII, University of Tennessee, Knoxville, September 16, 2017

· Colloquium, Wesleyan University, Middletown, Connecticut, April 20, 2017

◇ *Lattice methods for algebraic modular forms on orthogonal groups*, Computational Challenges in the Theory of Lattices, ICERM, Brown University, April 24, 2018

◇ *The* 2*-Selmer group of a number field and heuristics for narrow class groups and signature ranks of units*, Special Session: Algebraic Number Theory, AMS Spring Eastern Sectional Meeting, Northeastern University, April 21, 2018

◇ *On the paramodularity of typical abelian surfaces*, Number Theory Seminar, Harvard University, April 18, 2018

◇ *Explicit modularity in genus* 2

· Number Theory Seminar, University of Washington, April 17, 2018

· Automorphic Forms: Theory and Computation, King's College, London, September 6, 2016

· Group Theory/Lie Theory/Number Theory Seminar, University of Michigan, Ann Arbor, February 15, 2016

◇ *On the hypergeometric decomposition of symmetric K3 quartic pencils*, Picard-Fuchs Equations and Hypergeometric Motives, HIM, Bonn, March 29, 2018

◇ *Modularity of K3 surfaces*, Simons Collaboration Lecture, MIT, February 2, 2018

◇ *On explicit modularity for atypical genus* 2 *curves*, Workshop on Arithmetic of Hyperelliptic Curves, ICTP, Trieste, Italy, September 6, 2017

◇ *Belyi maps and effective computation*, Seminar, Telecom ParisTech, Paris, September 1, 2017

◇ *Semi-arithmetic points*

· Workshop Arithmetic Geometry and Computer Algebra, Universität Oldenburg, June 29, 2017

· Elliptic Curves, L-functions, and Torsors, University of Virginia, Charlottesville, March 25, 2017

· Number Theory Seminar, University of California, Berkeley, September 4, 2013

· Rational Points on Curves: A p-adic and Computational Perspective, Mathematical Institute, University of Oxford, September 24, 2012

· Arithmetic Geometry of Orthogonal and Unitary Shimura Varieties, BIRS, Banff, Alberta, June 8, 2012

◇ *Heuristics for narrow class groups and signature ranks of units in number fields*

· Algebra and Number Theory Seminar, Yale University, New Haven, April 4, 2017

· Arithmetic Statistics and the Cohen-Lenstra Heuristics, University of Warwick, Coventry, July 1, 2016

◇ *Rigorous computation of the endomorphism algebra of a Jacobian*, New Trends in Arithmetic and Geometry of Algebraic Surfaces, BIRS, Banff, Alberta, March 15, 2017

◇ *Lecture series: Computational methods for modular and Shimura curves* (4 lectures), Connecticut Summer School in Number Theory, University of Connecticut, Storrs, August 8–11, 2016

◇ *Quadratic forms and orthogonal modular forms*, Southern New England Conference on Quadratic Forms and Modular Forms, Wesleyan University, Middletown, Connecticut, June 4, 2016

◇ *Cryptography for everyone*

· Mount Wachusett Community College, Gardner, Massachusetts, February 22, 2016

· TEDxUVM: Big scale, big fail?, University of Vermont, October 19, 2012

◇ *Can you hear the shape of a pinched sphere?*

· Helen Barton Lecture in Computational Mathematics, University of North Carolina, Greensboro, February 17, 2016

· Frank Battles Lecture, Northeastern Section MAA Meeting, Keene State College, Keene, New Hampshire, May 29, 2015

· 2014 NCTS Special Lectures in Number Theory III, NCTS, National Tsing Hua University, Hsinchu, Taiwan, August 5, 2014

· Distinguished Visiting Professor Lecture, Bucknell University, Lewisburgh, April 16, 2013

◇ *Discriminants and the monoid of quadratic rings*

· Lattices and Applications in Number Theory, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, January 22, 2016

· Special Session: Arithmetic Theory of Quadratic Forms and Lattices, Joint Mathematics Meetings, San Diego, January 10, 2013

◇ *Course: Quaternion algebras* (13 lectures), Computational Aspects of the Langlands Program, ICERM, Brown University, September 14–November 6, 2015

◇ *Petri's theorem for log (stacky) curves*, Algebraic and Tropical Geometry Seminar, Yale University, New Haven, October 29, 2015

◇ *Presentations for rings of modular forms*

· Boston University/Keio University Workshop 2015, Number Theory, Boston University, September 11–12, 2015

· Number Theory Seminar, Duke University, April 15, 2015

· BAANTAG, University of California, Santa Cruz, December 7, 2013

◇ *Triangles, permutations, and (covers of) surfaces*, UNC–Duke Students Math Colloquium, Duke University, Durham, April 14, 2015

◇ *Numerical methods and equations for surfaces obtained by gluing together triangles*, Colloquium, University of Vermont, April 2, 2015

◇ *Numerical computation of Belyi maps*, Constructive Methods in Number Theory, Bethe Forum, Universität Bonn, March 2, 2015

◇ *Experiments with Arakelov class groups and ranks of elliptic curves*, Counting Arithmetic Objects (Ranks of Elliptic Curves), Centre de Recherche Mathémetics (CRM), Montréal, November 11, 2014

◇ *On computing Hilbert modular forms by type and generalized Fermat curves of degree* 19, Special Session: Automorphic Forms and Related Topics, AMS Fall Southeastern Sectional Meeting, University of North Carolina, Greensboro, November 8, 2014

◇ *Computing Belyi maps, with arithmetic applications*, Joint Columbia–CUNY–NYU Number Theory Seminar, New York University, October 23, 2014

◇ *Abstract Brandt modules*, Sage Days 61: Quaternion Orders and Brandt Modules, University of Copenhagen, Denmark, August 27–28, 2014

◇ *Computing power series expansions of modular forms*, Algorithmic Number Theory Symposium (ANTS) XI, Hotel Hyundai, Gyeongju, Korea, August 11, 2014

◇ *Nonvanishing of twists of L-functions attached to Hilbert modular forms*, Algorithmic Number Theory Symposium (ANTS) XI, Hyundai Hotel, Gyeongju, Korea, August 10, 2014

◇ *Quaternary quadratic forms and quaternion ideals*, ICM 2014 Satellite Conference on Integral Quadratic Forms and Related Topics, Hotel Hyundai, Gyeongju, Korea, August 8, 2014

◇ *Computational methods for Belyi maps and dessins*, 2014 NCTS International Conference on the Impact of Computation on Number Theory, NCTS, National Tsing Hua University, Hsinchu, Taiwan, August 2, 2014

◇ *Computing three-point branched covers of the projective line*, Fourth Upstate New York Number Theory Conference, University of Buffalo, April 26, 2014

◇ *Power series expansions of modular forms*, Algebra and Number Theory Seminar, Yale University, New Haven, April 29, 2014

◇ *Computing Hilbert modular forms*, Curves and Automorphic Forms, Arizona State University, Tempe, March 10, 2014

◇ *The canonical rings of curves and log stacky curves*, Commutative Algebra and Algebraic Geometry Seminar, University of California, Berkeley, February 25, 2014

◇ *Numerical calculation of three-point branched covers of the projective line*

· Number Theory and Representation Theory Seminar, University of Wisconsin, Madison, February 13, 2014

· Number Theory Seminar, University of California, San Diego, November 14, 2013

◇ *Presentations for rings of modular forms*, BAANTAG, University of California, Santa Cruz, December 7, 2013.

◇ *Semi-arithmetic points*

· Number Theory Seminar, University of California, Berkeley, September 4, 2013

· Rational Points on Curves: A p-adic and Computational Perspective, Mathematical Institute, University of Oxford, September 24, 2012

· Arithmetic Geometry of Orthogonal and Unitary Shimura Varieties, BIRS, Banff, Alberta, June 8, 2012

◇ *Computing zeta functions of toric hypersurfaces with few monomials*, Computational Number Theory, Geometry and Physics, Clay Mathematics Institute, University of Oxford, September 23–29, 2013

◇ *Mini-course: Brandt modules* (3 lectures), Méthodes Algébriques et Explicites en Théorie des Nombres, Salins-les-Bains, September 16–20, 2013

◇ *Lattice methods for algebraic modular forms on classical groups*

· Distinguished Visiting Professor Lecture, Bucknell University, Lewisburgh, April 18, 2013

· Number Theory Seminar, University of South Carolina, Columbia, March 5, 2013

· Number Theory Seminar, Wesleyan University, Middletown, Connecticut, February 1, 2013

· Colloquium, Dartmouth College, January 31, 2013

· Number Theory Seminar, MIT, Cambridge, November 6, 2012

◇ *The canonical ring of a stacky curve*, Algebraic Geometry Seminar, NYU–Courant, April 9, 2013

◇ *Computing power series expansions of modular forms*

· Explicit Methods for Modular Forms, University of Warwick, Coventry, March 18, 2013

· Number Theory Seminar, Emory University, Atlanta, February 13, 2013

· Atkin Memorial Lecture and Workshop, University of Illinois at Chicago, April 29, 2012

◇ *Minimal isospectral, nonisometric orbifolds*

· Colloquium, University of Georgia, Athens, March 7, 2013

· Torsion in the Homology of Arithmetic Groups, BIRS, Banff, Alberta, July 2, 2012

◇ *The Brauer monoid of quaternion rings*, Special Session: Brauer Group in Algebra and Geometry, Joint Mathematics Meetings, San Diego, January 11, 2013

◇ *Kronecker's Jugendtraum and power series expansions of modular forms*, Regular Session on Algebraic Number Theory, Canadian Mathematical Society Winter Meeting, Montréal, December 8, 2012

◇ *Computing Belyi maps, and congruence subgroups of triangle groups*, FRAGMENT, Colorado State University, Fort Collins, May 3, 2012

◇ *Can one hear the shape of a (pinched) drum?*, Colloquium, University of Vermont, March 16, 2012

◇ *Expander graphs from Hilbert modular forms*, Number Theory Seminar, Dartmouth College, February 23, 2012

◇ *Arithmetic aspects of triangle groups*, Number Theory Seminar, University of California, San Diego, February 21, 2012

◇ *On the computation of Galois Belyĭ maps*, Special Session: Mathematics of Computation: Algebra and Number Theory, Joint Mathematics Meetings, Boston, January 7, 2012

◇ *Congruence subgroups of triangle groups*, 2011 NCTS International Conference on Galois Representations, Automorphic Forms and Shimura Varieties, NCTS, National Tsing Hua University, Hsinchu, Taiwan, June 17, 2011

◇ *Quaternion rings and ternary quadratic forms*

· Ramification in Algebra and Geometry at Emory, Emory University, Atlanta, May 19, 2011

· Upstate New York Number Theory Conference, Cornell University, Ithaca, New York, April 30, 2011

◇ *Computing Hilbert modular forms*

· 2011 NCTS Seminar on Number Theory, NCTS, National Tsing Hua University, Hsinchu, Taiwan, June 17, 2011

· Second Montreal-Toronto Workshop in Number Theory, Fields Institute, University of Toronto, Ontario, Canada, April 9, 2011

◇ *Nonsolvable number fields ramified only at small primes*

· Algebra Seminar, Wesleyan University, Middletown, Connecticut, February 18, 2011

· Number Theory Seminar, State University of New York (SUNY) Buffalo, April 26, 2010

· Dartmouth Number Theory Seminar, October 1, 2009

◇ *Rings of low rank with a standard involution and quaternion rings*

· Algebra and Number Theory Seminar, University of California, Santa Cruz, March 31, 2011

· Algebra Seminar, Brown University, February 28, 2011

· Number Theory Seminar, Stanford University, May 14, 2010

· Dartmouth Colloquium, October 1, 2009

◇ *Explicit methods for Hilbert modular forms*

· Algebra/Number Theory Seminar, Boston University, April 25, 2011

· Group Theory/Lie Theory/Number Theory Seminar, University of Michigan, Ann Arbor, February 14, 2011

· Arithmetic Statistics: Introductory Workshop, MSRI, Berkeley, February 2, 2011

· Workshop on Computer Methods for L-functions and Automorphic Forms, Centre de Récherche Mathématiques (CRM), Montréal, March 22, 2010

◇ *Algebraic curves uniformized by congruence subgroups of triangle groups*

· Computational Algebra Seminar, University of Sydney, January 13, 2011

· Canadian Number Theory Association (CNTA) XI, Acadia University, Wolfville, Nova Scotia, July 15, 2010

· Number Theory Seminar, Harvard University, November 25, 2009

◇ *Computing automorphic forms on Shimura curves over fields with arbitrary class number*, Algorithmic Number Theory Symposium (ANTS) IX, INRIA, Nancy, July 21, 2010

◇ *Lecture series: Computing Hilbert modular forms* (3 lectures), Centre de Recerca Matemàtica (CRM), Bellaterra (Barcelona), Spain, June 28, 30, and July 2, 2010

◇ *Algorithms for automorphic forms on Shimura curves*

· Number Theory Seminar, University of Washington, Seattle, May 6, 2010

· Noncongruence modular forms and modularity, American Institute of Mathematics (AIM), August 19, 2009

◇ *Computing automorphic forms on Shimura curves*, Number Theory Seminar, UCLA, May 3, 2010

◇ *Computing zeta functions for sparse nondegenerate hypersurfaces using Dwork cohomology*, Counting Points: Theory, Algorithms and Practice, Centre de Récherche Mathématiques (CRM), Montréal, April 21, 2010

◇ *The Gauss higher relative class number problem*, Joint Mathematics Meetings, Arithmetic Geometry session, San Francisco, January 14, 2010

◇ *On nondegeneracy of curves*, CMS Winter Meeting, Windsor, Ontario, December 4, 2009

◇ *Tables of Hilbert modular forms*, AMS 2009 Fall Southeastern Meeting, Boca Raton, Florida, October 31, 2009

◇ *Algorithms for automorphic forms on Shimura curves*

· Noncongruence Modular Forms and Modularity, American Institute of Mathematics (AIM), August 19, 2009

· Explicit Methods in Number Theory, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, July 14, 2009

◇ *Lecture series: Algorithmic theory of quaternion algebras* (4 lectures), 2009 Summer School Automorphic Forms and L-Functions: Computational Aspects, Centre de Recherches Mathématiques (CRM), Montréal, June 25–26, July 2–3, 2009

◇ *Constructing modular Galois representations ramified only at small primes*

· Computational Algebra Seminar, University of Sydney, Australia, May 21, 2009

· Arithmetic Geometry Seminar, McMaster University, Hamilton, Ontario, April 2, 2009

◇ *Quaternions*, Mathematics Seminar, Middlebury College, Middlebury, March 31, 2009

◇ *Characterizing quaternion rings*, Quadratic Forms, Sums of Squares, Theta Functions, and Integral Lattices, University of Florida, Gainesville, March 11, 2009

◇ *Algorithms for enumerating ideal classes in quaternion orders*, Sage Days 13, University of Georgia, Athens, February 28, 2009

◇ *Computing automorphic forms on Shimura curves*

· Five College Number Theory Seminar, Amherst College, Massachusetts, February 10, 2009

· Québec-Vermont Number Theory Seminar, Concordia University, Montréal, December 11, 2008

◇ *A database of totally real quintic fields*, Sage Days 11, University of Texas, Austin, Texas, November 9, 2008

◇ *Computing fundamental domains for Fuchsian groups*, Computations with Modular Forms, University of Bristol, August 21, 2008

◇ *Enumeration of totally real fields of bounded root discriminant*, Algorithmic Number Theory Symposium (ANTS) VIII, BIRS, Banff, Alberta, May 17, 2008

◇ *Moduli of nondegenerate curves*, Algebraic Geometry Seminar, Duke University, Durham, May 1, 2008

◇ *Escher and the Droste effect*

· Mathematics Seminar, Middlebury College, Middlebury, April 15, 2008

· 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

◇ *Shimura curves of genus at most two*, Number Theory Seminar, University of Washington, Seattle, February 20, 2008

◇ *Shimura curves of low genus and totally real fields of small root discriminant*, Québec-Vermont Number Theory Seminar, McGill University, Montréal, December 6, 2007

◇ *Heegner points and Sylvester's conjecture*, Five College Number Theory Seminar, Amherst College, Massachusetts, November 27, 2007

◇ *Enumeration of totally real number fields*

· Colloquium, University of Washington, Seattle, February 20, 2008

· MIT Number Theory Seminar, Cambridge, Massachusetts, October 25, 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* and *Some Diophantine applications of Heegner points*, Clay Summer School in Arithmetic Geometry, George-August Universität, Göttingen, August 1–2, 2006

◇ *Computational aspects of Shimura curves*, Magma 2006 Conference, Technische Universität, Berlin, July 30, 2006

◇ *Computing CM points on Shimura curves arising from cocompact arithmetic triangle groups*, Algorithmic Number Theory Symposium (ANTS) VII, Technische Universität, Berlin, July 27, 2006

◇ *Special lecture series: Shimura curves* (3 lectures), University of Sydney, Australia, April 4, 7, 11, 2006

◇ *Curves over finite fields with many points: an introduction*, Computational aspects of algebraic curves, University of Idaho, Moscow, Idaho, May 27, 2005

◇ *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*

· Number Theory Seminar, University of Georgia, Athens, April 10, 2008

· Colloquium, Wake Forest University, Winston-Salem, 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

◇ *Computing maximal orders for quaternion algebras*, Explicit Methods in Number Theory, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, July 18, 2005

◇ *Introduction to stacks*, Basic Notions Seminar, Harvard University, April 19, 2004

Contributed Talks

◇ *Polarized class sets of quaternion orders*, Algebra/Number Theory Seminar, Dartmouth College, September 12, 2023

◇ *A norm refinement of Bezout's lemma*, Algebra/Number Theory Seminar, Dartmouth College, September 13, 2022

◇ *A family of Jacobians with definite quaternionic multiplication*, Algebra/Number Theory Seminar, Dartmouth College, March 29, 2022

◇ *Stickelberger's discriminant theorem for algebras*

· Maine–Québec Number Theory Conference, University of Maine, Orono (virtual), October 2, 2021

· Algebra/Number Theory Seminar, Dartmouth College, September 20, 2021

◇ *On Galois inertial types for elliptic curves over $\mathbb{Q}_p$*, Algebra/Number Theory Seminar, Dartmouth College, February 2, 2021

◇ *Arithmetic and geometric aspects of hypergeometric functions* (3 lectures), First Year Graduate Seminar, Dartmouth College, July 6–10, 2020

◇ *Counting elliptic curves with an isogeny of degree three*

· West Coast Number Theory, Asilomar Center, Monterey, California, December 17, 2019

· Québec–Maine Number Theory Conference, University of Maine, Orono, October 5, 2019

◇ *Identities for $1/\pi^2$ and special hypergeometric motives*, Colloquium, Dartmouth College, September 19, 2019

◇ *Quaternions and the sum of four squares* (2 lectures), First Year Graduate Seminar, Dartmouth College, July 8, 2019

◇ *Definite Hermite quaternion orders*, Algebra/Number Theory Seminar, Dartmouth College, May 2, 2019

- ◇ *Ranks of elliptic curves*, Dartmouth Math Society, Dartmouth College, April 10, 2019
- ◇ *Elliptic curves with locally a subgroup of order m*, Maine–Québec Number Theory Conference, Université Laval, Québec City, October 6, 2018
- ◇ *Strong approximation* (3 lectures), Algebra/Number Theory Seminar, Dartmouth College, January 4, 14, and 18, 2018
- ◇ *Adelic integration and the Riemann zeta function*, Algebra/Number Theory Seminar, Dartmouth College, September 14 and 21, 2017
- ◇ *Fake quadrics*, Geometry/Topology Seminar, Dartmouth College, February 28, 2017
- ◇ *Explicit modularity in genus* 2, Maine–Québec Number Theory Conference, Université Laval, Québec City, October 9, 2016
- ◇ *Adeles and ideles* (2 lectures), Algebra/Number Theory Seminar, Dartmouth College, September 20, October 18, 2016
- ◇ *Quaternions and the sum of four squares* (2 lectures), First Year Graduate Seminar, Dartmouth College, July 8, 2019
- ◇ *Clifford algebras* (3 lectures), First Year Graduate Seminar, Dartmouth College, July 25–29, 2016
- ◇ *Discriminants and the monoid of quadratic rings*, Algebra/Number Theory Seminar, Dartmouth College, October 25, 2012 and January 14, 2016
- ◇ *Belyi polynomials and the marvels of factoring*, Math Club, University of Connecticut, Storrs, November 18, 2015
- ◇ *Heuristics for boundedness of ranks of elliptic curves*, Algebra/Number Theory Seminar, Dartmouth College, April 23, 2015
- ◇ *Presentations for rings of modular forms*, Maine–Québec Number Theory Conference, Université Laval, Québec City, September 28, 2014
- ◇ *Modular forms on triangle groups*, Building Bridges: Workshop on Automorphic Forms, University of Bristol, July 11, 2014
- ◇ *Generators for rings of modular forms*, Third Upstate New York Number Theory Conference, Binghamton, April 27, 2013
- ◇ *Tables of Hilbert modular forms*, Québec–Maine Conference on Number Theory, University of Maine, Orono, October 4, 2009
- ◇ *On moduli of nondegenerate curves*, GeoCrypt 2009, Point-à-Pitre, Guadeloupe, May 1, 2009
- ◇ *Probability distributions on abelian groups*, Vermont Number Theory Seminar, University of Vermont, Burlington, February 26, 2009
- ◇ *Quadratic symbols over commutative rings*, Workshop Norm Residue Symbols, Universiteit Leiden, February 3–4, 2009
- ◇ *The analogy between number fields and function fields*, Vermont Number Theory Seminar, University of Vermont, Burlington, January 22, 2009
- ◇ *Computing the tame kernel of a number field*, Vermont Number Theory Seminar, University of Vermont, Burlington, October 9, 2008
- ◇ *The Gauss higher relative class number problem*, Maine–Québec Conference on Number Theory and Related Topics, Université Laval, Québec City, October 4, 2008
- ◇ *On lattice polygons*, Joint University of Vermont/St. Michael's College Combinatorics Seminar, University of Vermont, Burlington, September 18, 2008
- ◇ *The Gauss higher relative class number problem*, Vermont Number Theory Seminar, University of Vermont, Burlington, April 11, 2008

◇ *How many times should you shuffle a deck of cards?*, UVM Math Club, University of Vermont, Burlington, March 18, 2008

◇ *Introduction to quaternion orders*, Vermont Number Theory Seminar, University of Vermont, Burlington, February 28, 2008

◇ *Enumeration of totally real number fields*, Vermont Number Theory Seminar, University of Vermont, Burlington, October 11, 2007

◇ *Fundamental domains for finitely generated Fuchsian groups*, Québec–Maine Conference on Number Theory and Related Topics, University of Maine, Orono, September 29–30, 2007

◇ *Zeta functions of varieties over finite fields*, 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

◇ *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

◇ *Computing zeta functions of Δ-regular hypersurfaces*, Zeta Functions Seminar, University of California, Berkeley, February 27 and March 5, 2004

◇ *Modular curves as coarse moduli spaces*, Graduate Student Number Theory Seminar, University of California, Berkeley, Spring 2003

◇ *Representation of primes by quadratic forms*, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, November 16, 2002

◇ *Error-correcting codes using algebraic geometry*, Undergraduate Applied Mathematics Seminar, University of California, Berkeley, March 1, 2002

◇ *Explicit resolution of plane curve singularities*, Graduate Student Number Theory Seminar, University of California, Berkeley, February 13, 2002

◇ *Height functions defined by line bundles*, Arithmetic Geometry Seminar, University of California, Berkeley, February 5 and 12, 2002

◇ *Curves over finite fields with many points*, Function Fields Seminar, University of California, Berkeley, October 6, 2000

◇ *On the nonexistence of odd perfect numbers*

· Graduate Student Number Theory Conference, University of Illinois, Urbana-Champaign, Illinois, March 25, 2000

· West Coast Number Theory, Asilomar Center, Monterey, California, December 16, 1999

◇ *On perfect numbers*, MASS Colloqium, Penn State University, State College, Pennsylvania, November 3, 1998

Expository Work

◇ *The genus of a quadratic form*, Arizona Winter School: Quadratic Forms, University of Arizona, Tucson, course notes from John Conway, March 14–17, 2009

◇ *Introduction to stacks*, notes from lecture at Harvard, April 2004

◇ *Integral and rational points on higher dimensional varieties*, American Institute of Mathematics (AIM), Palo Alto, December 11–20, 2002

◇ Notes from *Explicit algebraic number theory*, Oberwolfach Seminar, November 10–16, 2002
◇ *Complex multiplication and group schemes*, course notes from Don Zagier and René Schoof, Spring 2001
◇ *Toric surfaces and continued fractions*, manuscript, May 2000

Service and Professional Experience

▶ **Refereeing and editorial work**

· Referee for 75 journals and book series (168 referee reports/written opinions)
· Associate editor, Essential Number Theory, May 2021–present
· Managing editor, LMFDB (L-Functions and Modular Forms Database, `http://lmfdb.org`), September 2018–present
· Associate editor, Research in Number Theory, September 2017–December 2022
· Associate editor, Experimental Mathematics, November 2019–December 2022
· Reviewer, Math. Reviews, Spring 2006–Spring 2022
· NSF review panelist, 2010, 2013, 2014, 2019, 2021
· External referee, NSERC Discovery Grant proposal, Summer 2010, Winter 2019
· Editorial board member, Hilbert Modular Forms, LMFDB, April 2012–September 2018
· NSA referee, 2013, 2015
· NSF external reviewer, 2011, 2014

▶ **Professional memberships and service**

· Member, American Mathematical Society (AMS), 1999–2004, 2007–present
· Member, National Organization of Gay and Lesbian Scientists and Technical Professionals (NOGLSTP), 2012–2014, 2016–2024
· Member, National Association of Mathematicians (NAM), 2020–present
· Member, Association for Women in Mathematics (AWM), 2021–present
· Treasurer, Number Theory Foundation, October 2019–present
· Member at large, AMS Council, February 2024–January 2027
· Council representative, AMS Committee on Equity, Diversity, and Inclusion, February 2024–January 2027
· Member at large, AMS Committee on the Profession, February 2021–January 2024
· Member, AMS Eastern Section Program Committee, February 2019–January 2020; and chair, February 2020–January 2021
· Member, Sigma Xi, 2015–2018
· Mentor, Association for Women Mathematicians (AWM), Fall 2007–Spring 2017
· Member, Mathematical Association of America (MAA), 1994–1995, 2001–2002

▶ **Thesis committees**

· Ph.D. defense committee member, Kai (Steve) Fan, *Rough numbers and variations on the Erdös–Kac theorem*, student of Carl Pomerance, Dartmouth College, September 2023
· Ph.D. defense committee member, Richard Haburcak, *Brill–Noether theory via K3 surfaces*, student of Asher Auel, Dartmouth College, May 2023
· Ph.D. jury member, Antonin Leroux, *Quaternion algebras and isogeny-based cryptography*, student of François Morain, École Polytechnique, September 2022

- Ph.D. thesis committee, Sebastiano Tronto, *Kummer theory for commutative algebraic groups*, student of Antonella Perucca, Peter Bruin, and Peter Stevenhagen, Universiteit Leiden, June 2022
- HDR rapporteur, Damien Robert, *Efficient algorithms for abelian varieties and their moduli spaces*, Université de Bordeaux, June 2021
- Ph.D. thesis committee, Jan Bouw, *On the computation of norm residue symbols*, student of Ronald van Luijk (co-advised by Hendrik Lenstra and Michiel Kosters), Universiteit Leiden, November 2020
- Ph.D. external reviewer, James Rickards, *Intersections of closed geodesics on Shimura curves*, student of Henri Darmon, McGill University, May 2020
- Undergraduate honors thesis outside examiner, Deveena R. Banerjee, *Classifying Euclidean origami constructions in hyperbolic space*, Bates College, April 2020
- Ph.D. defense committee member, Angelica Babei, *On the arithmetic of tiled orders*, student of Thomas Shemanske, Dartmouth College, May 2019
- Ph.D. jury member, Matthieu Rambaud, *Courbes de Shimura et algorithmes bilinéaires de multiplication dans les corps finis*, student of Hugues Randriam, Telecom ParisTech, September 2017
- Ph.D. defense committee member, Joseph Quinn, *Quaternion algebras and hyperbolic* 3*-manifolds*, student of Abhijit Champanerkar, The Graduate Center of CUNY, April 2016
- Ph.D. defense committee member, Nathan McNew, *Multiplicative problems in combinatorial number theory*, student of Carl Pomerance, Dartmouth College, May 2015
- Ph.D. defense committee member, Michael Wijaya, *A function-field analogue of Conway's topograph*, student of Thomas Shemanske, Dartmouth College, April 2015
- Ph.D. opponent, Nadim Rustom, *Algebra and arithmetic of modular forms*, student of Ian Kiming, University of Copenhagen, December 2014
- Ph.D. jury member, Nicolas Mascot, *Calcul de représentations galoisiennes modulaires*, student of Jean-Marc Couveignes, Université de Bordeaux, July 2014
- Ph.D. rapporteur and jury member, Aurel Page, *Méthodes explicites pour les groupes arithmétiques*, student of Karim Belabas, Université de Bordeaux, July 2014
- Ph.D. defense committee member, Zebediah Engberg, *The arithmetic of cyclic subgroups*, student of Carl Pomerance, Dartmouth College, May 2014
- Ph.D. rapporteur and jury member, Virgile Ducet, *Construction of algebraic curves with many rational points over finite fields*, student of David R. Kohel, Aix-Marseille Université, September 2013
- Undergraduate honors thesis committee member, Emily Hoogesteger, *An exploration of the modulo* 5 *and* 5^n *Ramanujan congruences for the partition function*, University of Vermont, April 2013
- Ph.D. defense committee member, Matt Welz, *Fusion systems with standard components of small rank*, student of Richard Foote, University of Vermont, August 2012
- Ph.D. defense committee member, Benjamin Linowitz, *Selectivity in central simple algebras and isospectrality*, student of Thomas Shemanske, Dartmouth College, May 2012
- Undergraduate honors thesis committee member, Allison Morse, *Combinatorial game theory*, University of Vermont, April 2012
- Ph.D. defense (reading) committee member, Jeroen Sijsling, *Equations for arithmetic pointed tori*, student of Frits Beukers, Universiteit Utrecht, Netherlands, August 2010

· Ph.D. defense committee member, Xavier Guitart, *Arithmetic properties of abelian varieties under Galois conjugation*, student of Jordi Quer, Universitat Politècnica de Catalunya, Barcelona, Spain, July 2010

· Ph.D. defense committee member, Jason Price, *Popescu's conjecture in multiquadratic extensions*, student of Jonathan Sands, University of Vermont, June 2009

· Ph.D. referee, David Gruenewald, *Explicit algorithms for Humbert surfaces*, student of David Kohel, University of Sydney, August 2009

▶ **Conference organization**

· Organizer (with Jennifer Balakrishnan, Kiran Kedlaya, and Andrew V. Sutherland), Algorithmic Number Theory Symposium (ANTS) XVI, MIT, July 15–19, 2024

· Organizer (with Jennifer Balakrishnan, Edgar Costa, Noam Elkies, David Roe, and Andrew Sutherland), Modular Curves Workshop 3, MIT, March 11–15, 2024

· Organizer (with Noam Elkies and Adam Logan), Families of K3 Surfaces in the LMFDB, ICERM, Brown University, February 14–17, 2024

· Organizer, Dartmouth–UVM Math Day, Dartmouth College, February 10, 2024

· Organizer (with Eran Assaf and Ciaran Schembri), Shimura Curves in the LMFDB, Dartmouth College, February 5–9, 2024

· Organizer (with Eran Assaf and Edgar Costa), Hilbert Modular Forms Infrastructure Week 5, MIT, December 11–15, 2023

· Organizer (with John Cremona, John Jones, Jennifer Paulhus, and Andrew Sutherland), LMFDB, Computation, and Number Theory (LuCaNT), ICERM, Brown University, July 10–14, 2023

· Organizer (with Andrew Kobin, Soumya Sankar, Libby Taylor, and David Zureick-Brown), AMS Mathematics Research Community (MRC), Explicit Computations with Stacks, June 5–9, 2023

· Organizer (with Eran Assaf and Edgar Costa), Hilbert Modular Forms Infrastructure Week 4, Dartmouth College, May 8–12, 2023

· Organizer (with Alex Bartel), Arithmetic, Algebra, and Algorithms: Celebrating the Mathematics of Hendrik Lenstra, ICMS, Edinburgh, April 10–14, 2023

· Scientific committee member, COmputations and their Uses in Number Theory (COUNT), CIRM, Luminy, February 27–March 3, 2023

· Organizer (with Eran Assaf and Edgar Costa), Hilbert Modular Forms Infrastructure Week 3, Dartmouth College, December 12–16, 2022

· Organizer (with Jennifer Balakrishnan, Edgar Costa, Noam Elkies, David Roe, and Andrew V. Sutherland), Modular Curves Workshop 2, MIT, November 5–9, 2022

· Organizer (with Juliette Bruce, Renzo Cavalieri, and Tyler Kelly), Spec($\overline{Q}$), Fields Institute, University of Toronto, Ontario, Canada, July 6–8, 2022

· Organizer (with Jennifer Balakrishnan, Edgar Costa, Noam Elkies, David Roe, and Andrew V. Sutherland), Modular Curves Workshop, MIT, March 21–25, 2022

· Organizer, Hilbert Modular Forms Infrastructure Week 2, Dartmouth College, February 21–25, 2022

· Advisory board member, A Series of Trimester Programs on Triangle Groups, Belyi Uniformization, and Modularity, Bhaskaracharya Pratishthan, Pune, India (virtual), September 1, 2021–August 31, 2022

· Organizer (with Angie Babei), Hilbert Modular Forms Infrastructure Week, Dartmouth College, July 26–30, 2021

- Organizer (with Haluk Şengün), Computations with Arithmetic Groups, Canadian Mathematical Society (CMS) Winter Meeting, Ottawa (virtual), December 3, 8, 2020
- Organizer (with Sam Schiavone), Belyi LMFDB Mini-Meeting, MIT (virtual), June 11–12, 2020
- Organizer (with Jennifer Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, and Andrew Sutherland), Workshop on Arithmetic Geometry, Number Theory, and Computation, ICERM, Brown University (virtual), June 1–5, 2020
- Organizer (with Jennifer Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, and Andrew Sutherland), Arithmetic of Low-Dimensional Abelian Varieties, ICERM, Brown University, June 3–7, 2019
- Organizer (with Drew Sutherland), Abelian Varieties over Finite Fields, ICERM, Brown University, January 31–February 3, 2019
- Organizer (with Brendan Hassett and Drew Sutherland), Special Session: Number Theory, Arithmetic Geometry, and Computation, Joint Mathematics Meetings, Baltimore, January 19, 2019
- Organizer (with Jennifer Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, and Andrew Sutherland), Arithmetic Geometry, Number Theory, and Computation, MIT, August 20–24, 2018
- Organizer (with Bianca Viray), Communicating Mathematics Effectively, University of Washington, June 18–22, 2018
- Organizer (with John Cremona, Nicolas Mascot, Aurel Page, and Haluk Şengün), LMFDB Workshop: Hilbert and Bianchi Modular Forms, University of Warwick, June 12–16, 2017
- Organizer (with Nils Bruin, Kiran Kedlaya, and Samir Siksek), Arithmetic Aspects of Explicit Moduli Problems, BIRS, Banff, Alberta, May 28–June 2, 2017
- Organizer (with Taylor Dupuy, Carl Pomerance, and Christelle Vincent), QVNTS Topics: Kummer Classes and Anabelian Geometry, September 10–11, 2016
- Scientific committee member, Algorithmic Number Theory Symposium (ANTS) XII, University of Kaiserslautern, August 29–September 2, 2016
- Organizer (with Srinath Baba), Power Series Expansions of Modular Forms on Shimura Curves, SQuaRE, American Institute of Mathematics, Palo Alto, February 17–21, 2014, June 15–19, 2015, June 20–24, 2016
- Organizer, LMFDB 1.0 Release Party, Dartmouth College, May 10, 2016
- Organizer, Explicit Methods for Modularity of K3 Surfaces and Other Higher Weight Motives (with Fernando Rodriguez-Villegas, Matthias Schütt, Holly Swisher, Yuri Tschinkel, and Bianca Viray), ICERM, Brown University, October 19–23, 2015
- Organizer, Semester Program: Computational Aspects of the Langlands Program (with Alina Bucur, Brian Conrey, David Farmer, John Jones, Kiran Kedlaya, Michael Rubinstein, and Holly Swisher), ICERM, Brown University, Fall 2015
- Scientific committee member, 29th Journées Arithmetiques (JA 2015), University of Debrecen, Hungary, July 6–10, 2015
- Organizer, 2014 NCTS Conference on the Impact of Computation on Number Theory (with Wen-Ching Li and Yifan Yang), National Center for Theoretical Sciences, Hsinchu, Taiwan, July 30–August 3, 2014
- Organizer, Algorithms for Lattices and Algebraic Automorphic Forms (with Matthew Greenberg and Markus Kirschmer), American Institute of Mathematics (AIM), Palo Alto, May 6–10, 2013

· Organizer, Computations with Modular Forms 2011, Summer School and Conference, Universität Heidelberg, Interdisciplinary Center for Scientific Computing, August 29–September 8, 2011

· Organizer (with Chantal David and Jayce Getz, 2010–2011; with Henri Darmon and Xander Faber, 2009–2010), Québec-Vermont Number Theory Seminar (QVNTS), Fall 2009–Fall 2011

▶ **Outreach**

· Plenary lecturer, Johns Hopkins Center for Talented Youth, Family Academic Programs, Science and Technology Series: Mathematics, Dartmouth College, May 12, 2018, October 4, 2014

· Lecturer, Governor's Institute of Vermont, Mathematical Sciences, University of Vermont, June 18–22, 2012, June 18, 2013

Fun, accelerated learning residencies on college campuses for Vermont teenagers

· Visiting faculty, MathPath, Summer 2008

Taught breakout course and gave three plenary lectures at an "advanced summer camp for students age 11–14 who show high promise and love mathematics"

· 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 pedagogy and implementation

· Volunteer, Math Nerds, Summer 2000–Summer 2002

▶ **Panels**

· The Future of Graduate Mathematics Textbooks, Joint Mathematics Meetings, San Francisco, January 4, 2024

· The Future of Extensive Computation in Sciences (moderator), ICTP, Trieste, Italy, September 14, 2023

· Professional Development, Symposium on Arithmetic Geometry and its Applications (SAGA), CIRM, Luminy, February 7, 2023

· How To Give Good Talks, Midwest Arithmetic Geometry and Number Theory Series 2021 (miniMAGNTS), Ohio State University (virtual), August 11, 2021

· Panel Discussion, PAlmetto Joint Arithmetic, Modularity, and Analysis Series (PAJAMAS), University of South Carolina (virtual), December 6, 2020

· How to Give a Good Math Talk, Lunch in the Time of Covid (virtual), December 3, 2020

· My Process: Thoughts from Funded Recipients, NSF CAREER workshop series, Dartmouth College, May 30, 2019

· Early-career Panel, Ramification in Algebra and Geometry at Emory (RAGE), Emory University, Atlanta, May 16, 2011

· Teaching Critical Reading Across the Disciplines, Berkeley, March 14, 2005

· Spring GSI Teaching & Orientation Workshop, Berkeley, January 17, 2002

· Fall meeting of the Faculty Advisers for GSI Affairs, Berkeley, October 15, 2001

▶ **Other professional experience**

· Visitor, MPIM, Bonn, April 2022

· Participant, Trimester Program: Periods in Number Theory, Algebraic Geometry and Physics, HIM, Bonn, March–April 2018

· Visiting scholar, University of California, Berkeley, Fall 2013–Spring 2014

· Distinguished visiting professor, Bucknell University, April 15–19, 2013

· Part B examiner, Luiz Takei, student of Henri Darmon, McGill University, May 25, 2011
· Visiting Scholar, Magma Computational Algebra Group, July 2007, May 2009, January 2011
· Visitor, Research Programme on Arithmetic Geometry, Centre de Recerca Matemàtica, Bellaterra (Barcelona), Spain, June–July 2010
· Course assistant, Arizona Winter School 2009: Quadratic Forms, University of Arizona, Tucson, March 14–18, 2009
· Special Session Leader, Spring GSI Teaching & Orientation Workshop, January 14, 2005
· 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
· Workshop leader, Fall GSI Teaching & Orientation Workshop, August 27, 2004
· Web liaison, Future Directions in Algorithmic Number Theory, American Institute of Mathematics (AIM), Palo Alto, March 24–28, 2003
· Web coordinator, Lenstra Treurfeest, University of California, Berkeley, March 21–23, 2003
· Visitor, Universiteit Leiden, Fall 2002
· Representative, Mathematical Graduate Student Association (MGSA), 2000–2002
· Participant, Mathematics Advanced Study Semester (MASS), Penn State University, State College, Pennsylvania, Fall 1998
· Participating student researcher, Summer 1997–Summer 1998
Center for the Design of Analog-Digital Integrated Circuits (CDADIC); supervised by Massimo Capobianchi, Gonzaga University
· Computer analyst, Docent Inc., Summer 1996

Service: Dartmouth College

◇ Departmental committee member:
· Webpage committee, Fall 2018–Spring 2019, Fall 2020–Spring 2021, Fall 2021, Spring 2022, Fall 2022, Spring 2023
· Graduate program committee (GPC), Spring 2014–Spring 2015, Winter 2016–Spring 2016, Fall 2020–Spring 2021 (chair), Fall 2021, Spring 2022, Fall 2022, Spring 2023, Fall 2023–Spring 2024
· Prize committee, Fall 2021, Spring 2022, Fall 2022, Spring 2023
· Self-study and planning committee, Fall 2022, Spring 2023, Fall 2023–Spring 2024
· Equipment committee, Fall 2021, Spring 2022
· Ad hoc prelim exam committee, Fall 2020–Spring 2021
· TA discussion group, Fall 2020
· Hiring committee, Fall 2019–Spring 2020 (chair)
· Graduate admissions committee (GAC), Fall 2014–Spring 2016
· Undergraduate program committee (UPC), Spring 2014
◇ Hannah Croasdale Award selection committee, Spring 2020, Spring 2022, Spring 2023
◇ Office space task force, Spring 2021
◇ Group advising (for first-year students), Fall 2020
◇ Faculty co-advisor, Green Lambda, Fall 2018–Spring 2019, Spring 2021–Spring 2022
◇ Vice chair of the Department of Mathematics, Fall 2016–Spring 2019

- ◇ Graduate representative, Winter 2016, Fall 2016–Spring 2018
- ◇ Committee on Standards member, Winter 2017–Spring 2017, Winter 2018–Spring 2018
- ◇ Mock Marshall and Rhodes scholarship interviews, Winter 2017, Fall 2017
- ◇ Judge for Association for Women in Mathematics (AWM) Upper Valley Essay Contest, 2016
- ◇ Graduate advisor, Fall 2014–Spring 2015

Service: University of Vermont

- ◇ Departmental committee member:
  - · Graduate committee, Fall 2011–Spring 2013
  - · Putnam committee, Fall 2007–Spring 2013
  - · High school contest committee, Fall 2007–Spring 2013
  - · Math Club committee, Fall 2010–Spring 2011, Fall 2012–2013
  - · Reappointment committee for Helen Read, Fall 2011
  - · Committee to review and update Faculty Evaluation Guidelines, Fall 2009–Spring 2010
  - · Curriculum committee: the first two years, Fall 2009–Spring 2010
  - · Colloquium committee, Fall 2007–Spring 2008
- ◇ Volunteer, Vermont Northwest Regional MATHCOUNTS, February 2010, 2011, 2012, 2013
- ◇ Graduate faculty appointment, Fall 2007–Spring 2013
- ◇ Mock Rhodes interview, Fall 2009, Fall 2010;
  Mock Marshall interview, Fall 2012
- ◇ Academic Integrity Council member, Center for Student Ethics and Standards, Fall 2007–Fall 2008
- ◇ Volunteer coach, Lawrence Debate Union, Fall 2007–Spring 2013
- ◇ Member, President's Commission on Lesbian, Gay, Bisexual, and Transgender (LGBT) Equity, Fall 2008–Spring 2010

Other Conferences Attended

- ◇ Monodromy and Its Applications, Princeton University (virtual), December 7–10, 2023
- ◇ Siegel Modular Forms in the LMFDB, ICERM, Brown University, November 16–19, 2023
- ◇ Artificial Intelligence to Assist Mathematical Reasoning, National Academies, Washington, DC, September 19, 2023
- ◇ Shimura Varieties and L-Functions, MSRI, Berkeley, March 13–17, 2023
- ◇ ALCOCRYPT 2023: Algebraic and Combinatorial Methods for Coding and Cryptography, CIRM, Luminy, France, February 20–24, 2023
- ◇ International Congress of Mathematicians (ICM) 2022, virtual, July 5–14, 2022
- ◇ Modern Breakthroughs in Diophantine Problems, BIRS, Banff, Alberta, June 20–24, 2022
- ◇ Computational Aspects of Discrete Subgroups of Lie Groups, ICERM, Brown University (virtual), June 14–18, 2021
- ◇ Arithmetic, Geometry, Cryptography and Coding Theory (AGC^{2}T-18), CIRM, Luminy (virtual), May 31–June 4, 2021
- ◇ Curves over Finite Fields: Past, Present, and Future, Université de Rennes (virtual), May 24–28, 2021
- ◇ Online workshop on Rational Points and Galois Representations, University of Pittsburgh (virtual), May 10–12, 2021

- ◇ Joint Mathematics Meetings, Washington, D.C. (virtual), January 6–9, 2021
- ◇ A Database of Siegel Modular Forms, Bucknell University (virtual), November 7–8, 2020
- ◇ Algebraic Geometry Northeastern Series (AGNES), Stony Brook (virtual), October 23–25, 2020
- ◇ Arithmetic Quotients of Locally Symmetric Spaces and their Cohomology, Centre de Récherche Mathématiques (CRM) (virtual), Montréal, October 19–23, 2020
- ◇ Québec–Maine Number Theory Conference, Université Laval (virtual), Québec City, September 26–27, 2020
- ◇ Modern Breakthroughs in Diophantine Problems, BIRS, Banff, Alberta (virtual), August 31–September 4, 2020
- ◇ Mod ℓ and ℓ-adic Galois Representations, SQuaRE, American Institute of Mathematics (AIM), San Jose (virtual), August 17–21, 2020
- ◇ Algorithmic Number Theory Symposium (ANTS) XIV, University of Auckland, New Zealand (virtual), June 29–July 4, 2020
- ◇ Lattices: Geometry, Algorithms and Hardness, Simons Institute for the Theory of Computing, Berkeley, February 18–21, 2020
- ◇ Symposium in Honor of Julia Robinson's 100th Birthday, MSRI, Berkeley, December 9, 2019
- ◇ Hypergeometric Motives, American Institute of Mathematics (AIM), San Jose, August 19–23, 2019
- ◇ Abelian Varieties over Finite Fields, University of Vermont, Burlington, May 7–10, 2019
- ◇ Connections in the LMFDB, IAS, Princeton, March 18–22, 2019
- ◇ Birational Geometry and Arithmetic, ICERM, Brown University, Providence, May 14–18, 2018
- ◇ Conference on Arithmetic and Automorphic Forms on the occasion of Günter Harder's 80th birthday, Max Planck Institute of Mathematics (MPIM), Bonn, March 12–14, 2018
- ◇ Symmetries of Surfaces, Maps and Dessins, BIRS, Banff, Alberta, September 25–September 29, 2017
- ◇ Effective Computations in Arithmetic Mirror Symmetry, SQuaRE, American Institute of Mathematics (AIM), Palo Alto/San Jose, June 16–20, 2014, August 10–14, 2015, November 28–December 2, 2016
- ◇ Algorithmic Number Theory Symposium (ANTS) XII, University of Kaiserslautern, August 29–September 2, 2016
- ◇ AGNES, Brown University, Providence, October 2–4, 2015
- ◇ Modular Forms and Curves of Low Genus: Computational Aspects, ICERM, Brown University, Providence, September 28–October 2, 2015
- ◇ LMFDB Mini-Workshop on Genus 2 Curves, University College, Dublin, March 22–27, 2015
- ◇ New Geometric Methods in Number Theory and Automorphic Forms, MSRI, Berkeley, December 1–5, 2014
- ◇ International Congress of Mathematicians (ICM) 2014, Seoul, Korea, August 13–21, 2014
- ◇ LMFDB Workshop, University of Warwick, Coventry, June 2–6, 2014
- ◇ Arizona Winter School 2014: Arithmetic Statistics, University of Arizona, Tucson, March 15–19, 2014
- ◇ Arithmetic Statistics over Finite Fields and Function Fields, American Institute of Mathematics (AIM), Palo Alto, January 27–31, 2014
- ◇ Workshop on Lattices with Symmetry, University of California, Irvine, August 12–16, 2013

- ◇ Explicit Methods in Number Theory, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, July 15–19, 2013
- ◇ Special Functions and Special Numbers, at the occasion of the 60th birthday of Frits Beukers, Universiteit Utrecht, July 10–12, 2013
- ◇ Conference on Algebraic Geometry, Amsterdam, July 8–12, 2013
- ◇ AGNES, Yale University, New Haven, April 19–21, 2013
- ◇ Arizona Winter School 2013: Modular Forms, University of Arizona, Tucson, March 9–13, 2013
- ◇ Pro-unipotent Fundamental Groups: Arithmetic and Diophantine Aspects, Bellairs Research Institute, Barbados, May 6–12, 2012
- ◇ Sage Days 36: p-adics in Sage, University of California, San Diego, February 19–23, 2012
- ◇ Cycles on Modular Varieties, BIRS, Banff, Alberta, October 31–November 4, 2011
- ◇ Bay Area Algebraic Number Theory and Arithmetic Geometry Day II, University of California, Berkeley, April 2, 2011
- ◇ Arizona Winter School 2011: Stark–Heegner Points, University of Arizona, Tucson, March 12–16, 2011
- ◇ Modular Conference: Arithmetic of Modular Forms and Modularity Results, Centre de Recerca Matemàtica (CRM), Bellaterra (Barcelona), Spain, July 5–9, 2010
- ◇ Number Theory and Representation Theory: in honor of Dick Gross's 60th birthday, Harvard University, Cambridge, June 2–5, 2010
- ◇ Computer Security and Cryptography, Centre de Récherche Mathématiques (CRM), Montréal, April 12–16, 2010
- ◇ Magma 2010 Conference on p-adic L-functions, Centre de Récherche Mathématiques (CRM), Montréal, February 22–26, 2010
- ◇ Borcherds Products and their Applications to Arithmetic Geometry, Bellairs Workshop in Number Theory, Bellairs Research Institute, Holetown, Barbados, May 3–10, 2009
- ◇ Modular Forms and Arithmetic, MSRI, Berkeley, June 28–July 2, 2008
- ◇ Elliptic Curves, Annual Workshop on Computational Complexity, Bellairs Research Institute, Holetown, Barbados, March 2–9, 2008
- ◇ Conference in honour of John Labute, McGill University and Centre de Récherche Mathématiques (CRM), Montréal, November 15–16, 2007
- ◇ L-functions and Modular Forms, American Institute of Mathematics (AIM), Palo Alto, 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, March 10–14, 2007
- ◇ Explicit Methods for Rational Points on Curves, BIRS, Banff, Alberta, February 4–9, 2007
- ◇ Recent Developments in the Arithmetic of Shimura Varieties and Arakelov Geometry, Centre de Recerca Matemàtica (CRM), Bellaterra (Barcelona), Spain, July 10–15, 2006
- ◇ Intersection of Arithmetic Cycles and Automorphic Forms, Centre de Recherches Mathématiques (CRM), Montréal, 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, July 17–23, 2005
- ◇ Explicit Arithmetic Geometry, Institut Henri Poincaré, Paris, December 6–10, 2004
- ◇ Explicit Algebraic Number Theory, Institut Henri Poincaré, Paris, October 11–15, 2004

- ◇ Number theory and Algebraic Geometry in Magma, Institut Henri Poincaré, Paris, October 4–8, 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
- ◇ Arithmetic Degeneration of Moduli, University of California, Irvine, May 7–10, 2003
- ◇ Future Directions in Algorithmic Number Theory, American Institute of Mathematics (AIM), Palo Alto, March 24–28, 2003
- ◇ Lenstra Treurfeest, University of California, Berkeley, March 21–23, 2003
- ◇ Arizona Winter School: Logic and Number Theory, University of Arizona, Tucson, Arizona, March 15–19, 2003
- ◇ Joint Mathematics Meetings, Baltimore, Maryland, January 15–18, 2003
- ◇ Rational and Integral Points on Higher Dimensional Varieties, American Institute of Mathematics (AIM), Palo Alto, December 11–20, 2002
- ◇ Explicit Algebraic Number Theory, Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach, 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
- ◇ Elliptic Curves and Higher Dimensional Analogoues (ECHIDNA), University of Sydney, Sydney, Australia, July 15–19, 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
- ◇ Arizona Winter School: Periods, University of Arizona, Tucson, Arizona, March 9–13, 2002
- ◇ Special Values of Rankin L-series, MSRI, Berkeley, December 10–14, 2001
- ◇ Arizona Winter School: Modular Forms, University of Arizona, Tucson, March 10–14, 2001
- ◇ Joint Mathematics Meetings, New Orleans, Louisiana, January 10–13, 2001
- ◇ Western Number Theory Conference, University of San Diego, December 16–20, 2000
- ◇ Arithmetic Geometry: Algorithmic Number Theory Program, MSRI, Berkeley, December 11–15, 2000
- ◇ Midwest Arithmetic Geometry in Cryptography (MAGC) Workshop, University of Illinois, Urbana-Champaign, Illinois, November 17–19, 2000
- ◇ Clay Mathematics Institute Introductory Workshop in Algorithmic Number Theory, MSRI, Berkeley, August 14–23, 2000
- ◇ Mathematical Challenges of the 21st Century, University of California, Los Angeles, August 8–10, 2000
- ◇ Millennial Number Theory Conference, University of Illinois, Urbana-Champaign, Illinois, May 21–27, 2000
- ◇ Advances in Algebraic Geometry and Commutative Algebra (AAGCA), Texas A&M University, College Station, Texas, May 18–20, 2000

- ◇ Graduate Student Number Theory Conference, University of Illinois, Urbana-Champaign, Illinois, March 25–26, 2000
- ◇ Arizona Winter School: Arithmetic of Function Fields, University of Arizona, Tucson, Arizona, March 10–15, 2000

Skills

- ▶ **Computer skills**: Programming in C, C++, Python, Java; HTML, Unix, LaTeX; Magma, SageMath, Mathematica, Pari-GP, Maple; Macaulay, Singular
- ▶ **All-American college debater**: Analytic communication at a nationally competitive level