

Katherine E. Stange

Curriculum Vitae as of February 21st, 2012

PERSONAL Stanford University *Voice:* (650) 283-4655
 Department of Mathematics *Fax:* (650) 725-4066
 450 Serra Mall, Building 380 *E-mail:* stange@math.stanford.edu
 Stanford, CA, USA, 94305 *Webpage:* math.stanford.edu/~stange

Citizenships: Canadian, American
Languages: English (native), French, basic German, basic Russian

RESEARCH AREAS Number theory, arithmetic geometry, elliptic curves, integer sequences, cryptography, arithmetic dynamics, game theory

HISTORY

EDUCATION **Brown University**, Providence, Rhode Island, USA

Ph.D., Mathematics, May 2008
 Dissertation: *Elliptic nets and elliptic curves*
 Advisor: Joseph H. Silverman

M.S., Mathematics, May 2003

University of Waterloo, Waterloo, Ontario, Canada

B.Math., Honours Pure Mathematics, June 2001
 With Distinction, Dean's Honours List

CURRENT **Stanford University**, Stanford, California, USA

POSITION NSF Postdoctoral Fellow, April 2011–June 2012
 Advisor: Brian Conrad

EMPLOYMENT **Simon Fraser University & Pacific Institute for the Mathematical**
2008-2011 **Sciences, University of British Columbia**, Vancouver, BC, Canada

 NSERC/PIMS/NSF Postdoctoral Fellow, 2009–2011
 Advisor: Nils Bruin

Harvard University, Cambridge, MA, USA

 NSF Postdoctoral Fellow and Junior Lecturer, 2008–2009
 Advisor: Noam Elkies

GRADUATE **Microsoft Research**, Seattle, WA, USA

EXPERIENCE Research Intern, Cryptography Group, September–December 2007
 Advisor: Kristin Lauter

Volunteer Work, Europe and Asia

 Personal Leave from Studies, June–December 2005
 Volunteer, English Teacher, School #27, Izhevsk, Russia
 Volunteer, Community Projects, Tibetan Village Project, Rural Tibet

AWARDS

- POSTDOCTORAL AWARDS
- NSERC Postdoctoral Fellowship** (Government of Canada)
“**Most outstanding candidate at the Postdoctoral level, Mathematics**”
Two years full support (postdoctoral)
Awarded March 2009, held September 2009–March 2011
previously awarded March 2008, declined
- National Science Foundation Postdoctoral Fellowship** (Government of USA)
Two years full support (postdoctoral)
Awarded February 2008, held September 2008–July 2009, April 2011–May 2012
- Pacific Institute of the Mathematical Sciences Postdoctoral Fellowship**
Two years full support (postdoctoral)
Awarded January 2008, held September 2009–March 2011
- GRADUATE AWARDS
- NSERC Postgraduate Scholarship** (Government of Canada)
Two years full support (graduate)
Awarded May 2006, held June 2006–May 2008
Awarded May 2002, unable to accept due to foreign tenure restrictions
Awarded May 2001, unable to accept due to foreign tenure restrictions
- VIGRE Fellowship** (Brown University)
One semester full support (graduate)
January–May 2005
January–May 2004
- Dean’s Fellowship** (Brown University)
One year full support (graduate)
September 2001–May 2002
- UNDERGRADUATE AWARDS
- NSERC Undergraduate Research Fellowship** (Government of Canada)
Summers of 1999, 2000
- Sybase Scholarship** (University of Waterloo)
Full scholarship 1997–2001

PUBLICATIONS

- REFEREED PUBLICATIONS
- “A duality principle for selection games.” with Lionel Levine and Scott Sheffield (2012) To appear in *Proceedings of the American Mathematical Society*, 8 pages. [arXiv:1110.2712](https://arxiv.org/abs/1110.2712)
- “Algebraic divisibility sequences over function fields.” with Patrick Ingram, Valéry Mahé, Joseph H. Silverman and Marco Streng (2012) To appear in *Journal of the Australian Mathematical Society* (special issue dedicated to Alf van der Poorten), 28 pages. [arXiv:1105.5633](https://arxiv.org/abs/1105.5633)
- “How to make the most of a shared meal: plan the last bite first.” with Lionel Levine (2011) To appear in *American Mathematical Monthly*, 20 pages. [arXiv:1104.0961](https://arxiv.org/abs/1104.0961)

“Character sums with division polynomials.” with Igor E. Shparlinski (2011) To appear in *Canadian Mathematical Bulletin*, 8 pages. [doi:10.4153/CMB-2011-126-x](https://doi.org/10.4153/CMB-2011-126-x)

“Elliptic nets and elliptic curves.” (2011) *Algebra & Number Theory* 5.2, pp. 197-229. [doi:10.2140/ant.2011.5.197](https://doi.org/10.2140/ant.2011.5.197)

“Amicable pairs and aliquot cycles for elliptic curves.” with Joseph H. Silverman (2011) *Experimental Mathematics* 20.3, pp. 329-357. [doi:10.1080/10586458.2011.565253](https://doi.org/10.1080/10586458.2011.565253)

“Terms in elliptic divisibility sequences divisible by their indices.” with Joseph H. Silverman (2011) *Acta Arithmetica* 146.4, pp. 355-378. [doi:10.4064/aa146-4-4](https://doi.org/10.4064/aa146-4-4)

“Pairings on hyperelliptic curves.” with Jennifer Balakrishnan, Juliana Belding, Sarah Chisholm, Kirsten Eisenträger and Edlyn Teske (2011) *WIN – Women in Numbers: Research Directions in Number Theory*, Fields Institute Communications 60, pp. 87-120.

“The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences.” with Kristin Lauter (2008) *Selected Areas in Cryptography 2008*, vol. 5381 of *Springer Lecture Notes in Computer Science*, pp. 309-327. [doi:10.1007/978-3-642-04159-4_20](https://doi.org/10.1007/978-3-642-04159-4_20)

“The Tate pairing via elliptic nets.” (2007) *Pairing-Based Cryptography – PAIRING 2007*, vol. 4575 of *Springer Lecture Notes in Computer Science*, pp. 329-348. [doi:10.1007/978-3-540-73489-5_19](https://doi.org/10.1007/978-3-540-73489-5_19)

SUBMITTED

“Integral points on elliptic curves and explicit valuations of division polynomials.” 37 pages. [arXiv:1108.3051](https://arxiv.org/abs/1108.3051)

PRESENTATIONS

INVITED &
REFEREED
CONFERENCE
PRESENTATIONS

Canadian Number Theory Association XII, Lethbridge, Alberta, Canada, June 2012 (upcoming).

Algebraic Dynamics, Berkeley, California, USA, May 2012 (upcoming).

Arithmetic Geometry, Special Session, AMS Western Sectional Meeting, Honolulu, Hawaii, USA, March 2012 (upcoming).

“Integral points on elliptic curves and explicit valuations of division polynomials.” **Rational Points on Varieties**, AMS Special Session, Joint Mathematics Meetings, Boston, Massachusetts, USA, January 2012.

“A dynamical system for elliptic divisibility sequences.” **Dynamical Systems in Algebraic and Arithmetic Geometry**, AMS Special Session, Joint Mathematics Meetings, Boston, Massachusetts, USA, January 2012.

“Integral points on elliptic curves and explicit valuations of division polynomials.” **Analytic Number Theory and Diophantine Approximation**, Special Session, CMS Winter Meeting, Toronto, Ontario, December 2011.

“I was messing with elliptic divisibility sequences and Sage didn’t do what I wanted.” **Sage Days 33: Women in Sage**, Seattle, Washington, USA, September 2011.

“Dynamical Units.” **Arithmetic Dynamics**, Special Session, AMS Spring Western Sectional Meeting, Las Vegas, Nevada, USA, May 2011.

“Amicable pairs for elliptic curves.” **Sage Days 26: Women in Sage**, Seattle, Washington, USA, December 2010.

“Elliptic divisibility sequences and elliptic nets in computation.” **Computational Number Theory**, Special Session, CMS Winter Meeting, Vancouver, British Columbia, Canada, December 2010.

“Amicable pairs for elliptic curves.” **Diophantine Approximation and Analytic Number Theory: A Tribute to Cam Stewart** Banff International Research Station, Banff, Alberta, Canada, June 2010.

“Amicable pairs for elliptic curves.” **Pacific Northwest Number Theory Conference**, Simon Fraser University, Vancouver, British Columbia, May 2010.

“Amicable pairs for elliptic curves.” **Number Theory**, Special Session, CMS Winter Meeting, Windsor, Ontario, December 2009.

“The elliptic curve discrete logarithm problem...,” **Fields Cryptography Retrospective Meeting**, Fields Institute, Toronto, Canada, May 2009.

“The elliptic curve discrete logarithm problem...,” **Arithmétique, géométrie, cryptographie and théorie des codes 2009**, Centre International de Rencontres Mathématiques, Marseille, France, March 2009.

“The elliptic curve discrete logarithm problem...,” (Accepted paper) **Selected Areas in Cryptography 2008**, Sackville, New Brunswick, August 2008.

“The elliptic curve discrete logarithm problem...,” **Computational Number Theory**, Session, Foundation of Computational Mathematics 2008, Hong Kong, China, June 2008.

“Elliptic nets and elliptic curves,” **Arithmetic and Geometry Summer School**, Alpbach, Tirol, Austria, June 2008.

“Elliptic nets,” **Low Genus Curves and Applications**, AMS Special Session, Joint Mathematics Meetings 2008, San Diego, CA, USA, January 2008.

“Elliptic nets in cryptography,” **Elliptic Curve Cryptography 2007**, Dublin, Ireland, September 2007.

“The Tate pairing via elliptic nets,” (Accepted Paper) **Pairing 2007**, Tokyo, Japan, July 2007.

“Elliptic nets,” **Workshop in Number Theory and Computability**, Edinburgh, Scotland, June 2007.

SELECTED OTHER PRESENTATIONS

Boise State REU, June 2011.
Stanford University Number Theory Seminar, March 2011.
McMaster Algebra Seminar, November 2009.
U. of Waterloo Pure Mathematics Colloquium, November 2009.
UBC/SFU Number Theory Seminar, November 2009, January 2008.
Five Colleges Number Theory Seminar, April 2009.
Harvard University Number Theory Seminar, December 2008.
MIT Combinatorics Seminar, September 2008.
Special Seminar ETH Zurich, Switzerland, June 2008.
U. of Connecticut Algebra Seminar, April 2008.
U. of California Los Angeles Number Theory Seminar, December 2007.
U. of California San Diego Number Theory Seminar, November 2007.
Boston U. Algebra Seminar, November 2007.
U. of Southern California Women in Science Seminar, November 2007.
Microsoft Research Seminar, February 2007.
Algorithmic Number Theory, Finland, May 2007.
Canadian Number Theory Association IX, Canada, July 2006.
Vilnius U. Visiting Seminar, Visiting Seminar, Lithuania, January 2004.
Nipissing U. Special Undergraduate Seminar, Canada, November 2002.
Brown U. Graduate Student Seminar, numerous.

SELECTED INVITATIONAL WORKSHOPS

Women in Numbers 2, Banff International Research Station, Banff, Alberta, Canada, November 2011.
Curves, Coding Theory and Cryptography, Marseille, France, March 2009.
Women in Numbers, Banff International Research Station, Banff, Alberta, Canada, November 2008.
Zeta Functions All the Way, Institute for Advanced Study, Princeton, NJ, USA, May 2006.
Intensive Research Period in Diophantine Geometry, Centro Ricerca Matematica Ennio De Giorgi, Pisa, Italy, June 2005.

TEACHING

COURSES TAUGHT

Postdoctoral Teaching Fellow, University of British Columbia
 Vector Calculus, Fall 2010
 Was entirely responsible for a lecture course of 88 students.

Junior Lecturer, Harvard University
 Advanced Algebraic Number Theory, Spring 2009
 The Mathematics of Symmetry, Fall 2008
 Was entirely responsible for courses. *The Mathematics of Symmetry* was seminar-format (student-taught), incorporating writing, programming and group projects as well as homework and tests.

Teaching Fellow, Brown University

Linear Algebra, Spring 2006
Multivariable Calculus, Fall 2004
Introductory Calculus, Part I, Fall 2003

Under the supervision of a faculty course head; was responsible for giving lectures, assigning homework, holding office hours and review sessions, maintaining a course web page, and aiding in the writing and grading of exams.

Teaching Assistant, Brown University

Introductory Calculus, Part I, Spring 2003
Introductory Calculus, Part I, Fall 2002

Two weekly recitation sections; was responsible for reviewing concepts, designing practice problems, discussing homework, holding office hours and review sessions, and creating and grading weekly quizzes.

TEACHING
AWARDS

Postdoctoral Teaching Award, University of British Columbia Mathematics, March 2011.

Outstanding Teaching Award, Brown University Mathematics, awarded to a graduating Ph.D. student, May 2008.

Departmental Nominee for Brown University Presidential Award for Excellence in Teaching, 2005 and 2007.

OTHER TEACHING
EXPERIENCE

Developer, Multivariable Calculus Collection for MathDL, Mathematical Association of America

January 2011 – present

Collecting, organizing and deploying a catalog of multivariable calculus resources as part of the Course Communities for Undergraduate Mathematics, within MathDL.

Invited Speaker, A Taste of Pi

October 16, 2010

Led a lecture and workshop for 88 high school students on modular arithmetic and elliptic curve cryptography.

Sheridan Center Teaching Certificate, Brown University

Completed May 2005

One year lecture/workshop course with assignments, a critiqued practice teaching session, and a video evaluation of lecture skills.

Tutorial Section Leader, University of Waterloo

Fall 1998

Led once weekly evening tutorial sections for introductory calculus; prepared and worked example problems and answered questions.

Tutoring

1995 – present

Volunteer tutor in mathematics help centres at Waterloo and Brown. Private tutor in topics including calculus, linear algebra, discrete mathematics, and mathematics for education. Volunteer tutor for Ask Dr. Math (www.mathforum.org/dr.math).

OTHER

- SOFTWARE** **Developer**, Sage Mathematics Software (sagemath.org).
Project leader and speaker at Sage Days 26 and 33.
Contributions in versions 4.7.2 onwards.
Author, Scripts and classes for use with Pari/GP and Sage
(math.stanford.edu/~stange/scripts.html)
Elliptic divisibility sequences tools (Pari/GP script and Sage class).
Elliptic nets tools (Pari/GP script).
Tate pairings via elliptic nets (Pari/GP script).
Ethiopian dinner (Sage class and notebook).
- SERVICE** **Co-organiser**, Women in Numbers 3 (upcoming conference).
Reviewer, Mathematical Reviews.
Referee, Algebra & Number Theory, Journal of Cryptology, numerous others.
Panelist, Careers in Mathematics and Science, WISE, Brown University, 2007.
Critiquing, graduate practice teaching sessions, Spring 2007.
Co-organiser, Graduate Student Seminar, Brown University, 2005.
Co-organiser, various reading courses and informal seminars, Brown University.
- TECHNICAL SKILLS** LaTeX, Python, PARI/gp, Sage, HTML, Photoshop/photography
- BEYOND MATH** **President**, Brown Cycling Club, 2002-2005.
Eastern Conference Champion and **National Silver Medalist**, USA Collegiate Cycling, 2005.
Amateur Photographer (pixel.katestange.net).