KATHERINE E. STANGE

PERSONAL INFORMATION

email	kstange@math.colorado.edu
website	math.colorado.edu/~kstange
office	Math. Bldg. 308 · +1 (303) 492 3346
address	University of Colorado Boulder Department of Mathematics Campus Box 395 Boulder, CO, USA 80309-0395

RESEARCH AREAS

Algebraic and algorithmic number theory and arithmetic geometry, including Apollonian circle packings, Kleinian groups, Diophantine approximation, elliptic curves and abelian varieties, integer sequences, and cryptography, including elliptic curve, lattice-based, isogeny-based and post-quantum cryptography.

EDUCATION

Doctor and Master of Mathematics

2001-2008 Brown University

Ph.D. Dissertation: *Elliptic nets and elliptic curves*
Advisor: Joseph H. Silverman

Bachelor of Mathematics

1997-2001 University of Waterloo

Pure Mathematics
With Distinction, Dean's Honours List

HISTORY

Current Position

2024-present The University of Colorado, Boulder

Professor

2018-2024 The University of Colorado, Boulder

Associate Professor

2012-2018 The University of Colorado, Boulder

Assistant Professor

Visiting Position

Fall 2019 Institute for Computational and Experimental Research in Mathematics (Brown University)

Research Fellow, Special Semester on Illustrating Mathematics

Postdoctoral Experience

2011-2012 Stanford University

NSF Postdoctoral Fellow
Advisor: Brian Conrad

2009-2011 Simon Fraser University, Pacific Institute for the Mathematical Sciences, and the University of British Columbia

NSERC/PIMS/NSF Postdoctoral Fellow
Advisor: Nils Bruin

2008-2009 Harvard University

NSF Postdoctoral Fellow and Junior Lecturer
Advisor: Noam Elkies

Graduate Experience

Fall 2007 Microsoft Research

Research Intern, *Cryptograph Group*
Advisor: Kristin Lauter

Summer/Fall 2005 Volunteer Work

Volunteer, English Teacher, School #27, Izhevsk, Russia
Volunteer, Community Projects, Tibetan Village Project, Rural Tibet

RESEARCH PRIZE

Canadian Number Theory Association

2024 Ribenboim Prize for 2020

"The Ribenboim Prize, named in honour of Paulo Ribenboim, is awarded by the Canadian Number Theory Association for distinguished research in number theory by a mathematician who is Canadian or has close connections to Canadian mathematics." Awarded in 2024 (pandemic delay)

RESEARCH AWARDS

Fellowships

2025-2026 Americal Mathematical Association Joan and Joseph Birman Fellowship for Women Scholars

$50,000

2021 Simons Fellow

Sabbatical support for 2021-2022, Award 822143

NSF Research Grants

2024–present Standard Grant

Arithmetic of Thin Groups and Isogeny-Based Cryptography, DMS-2401580
Mathematical Sciences Program
$350 000, three years

2017-2024 CAREER Grant

Research and Education: Number Theory, Geometry and Cryptography, CNS-1652238
Secure and Trustworthy Cyberspace/Mathematical Sciences Program
$450 000, five years (extended), plus $177,922 in supplements

2016-2018 EAGER Grant

Number Theory and Cryptography, DMS-1643552
Secure and Trustworthy Cyberspace/Mathematical Sciences Program
$200 000, two years

NSA Research Grants

2016-2017 Young Investigators Grant

The Geometry of Recurrence Structures
$40 000, two years (held for only 7 months due to overlap with NSF)

2014-2015 Young Investigators Grant

The Geometry of Recurrence Structures
$40 000, two years

Other Research Grants

2024 Association for Women in Mathematics Travel Grant

$3 500

2023-2024 CU Office of Faculty Affairs LEAP Individual Growth Grant

Secure Post-Quantum Cryptography
$8 721.56 for course release

2019-2020 CU Boulder RIO QuEST

A Quantum Randomness Beacon
$50 000
Co-PI with PI Krister Shalm and Co-PI Paul Beale

Postdoctoral Awards

2008-2012 National Science Foundation

Mathematical Sciences Postdoctoral Research Fellowship
$108 000

2009-2011 National Sciences and Engineering Research Council of Canada

Postdoctoral Fellowship
"Most outstanding candidate at the Postdoctoral level, Mathematics"
$80 000
also awarded in 2008, declined due to foreign tenure restrictions

2009-2011 Pacific Institute of the Mathematical Sciences

Postdoctoral Fellowship
accepted in name only (declined funding due to NSERC award)

Graduate Awards

2006-2008 National Sciences and Engineering Research Council of Canada

Postgraduate Scholarship
Two years full support
Also awarded 2001, 2002, declined due to foreign tenure restrictions

2004, 2005 Brown University

VIGRE Fellowship (×2)
One semester full support

2001-2002 Brown University

Dean's Fellowship
One year full support

Undergraduate Awards

1999, 2000 National Sciences and Engineering Research Council of Canada

Undergraduate Research Fellowship (×2)
Summer research support

1997-2001 University of Waterloo

Sybase Scholarship
Full scholarship, four years

OTHER HONORS

Service Awards

2021 Association for Women in Mathematics

Class of 2021 Fellow
Awarded to individuals for their exceptional dedication to increasing the

success and visibility of women in mathematics.
Citation: "For leadership in the Women in Numbers Network by creating its website (the first of its kind), mentoring early-career researchers, organizing conferences, editing its proceedings volumes, and chairing its steering committee; and for service on AWM committees, including support of other research networks."

Outreach/Exposition Awards

2013 Mathematical Association of America

Paul R. Halmos - Lester R. Ford Award
Awarded annually for outstanding papers in *The American Mathematical Monthly*
Awarded for joint paper with Lionel Levine, *How to make the most of a shared meal: plan the last bite first*

2021, 2023 3blue1brown Summer of Math Exposition

Annual competition for mathematical exposition run by YouTube Channel 3blue1brown
2023 Winner (one of five): YouTube video *Rethinking the real line*
https://www.youtube.com/watch?v=uFWJuZQLKJs
2023 results announcement:
https://www.youtube.com/watch?v=6a1fLEToyvU
2021 Honorable Mention: YouTube video *Lehmer Factor Stencils: A paper factoring machine before computers* https://www.youtube.com/watch?v=QzohwKT6TNA
2021 results announcement: https://www.youtube.com/watch?v=F3Qixy-r˙rQ

REFEREED RESEARCH PUBLICATIONS

Articles resulting from supervision are marked as follows:

$*$	high school student
†	undergraduate student
‡	graduate student
††	postdoctoral scholar under my supervision

ASIACRYPT 2024

1 Extending Class Group Action Attacks via Sesquilinear Pairings

Joseph Macula‡ and Katherine E. Stange
Advances in Cryptology – ASIACRYPT 2024, Part 3, vol. 15486 of *Springer Lecture Notes in Computer Science* (2024), 371–395.
https://doi.org/10.1007/978-981-96-0891-1˙12

Annals of Mathematics

2 The local-global conjecture for Apollonian circle packings is false

Summer Haag‡, Clyde Kertzer†, James Rickards†† and Katherine E. Stange
Annals of Mathematics, 200 (2) (2024), 749–770.
https://doi.org/10.4007/annals.2024.200.2.6

The Computer Journal

3 Failing to Hash Into Supersingular Isogeny Graphs

Jeremy Booher, Ross Bowden, Jake Doliskani, Tako Boris Fouotsa, Steven D. Galbraith, Sabrina Kunzweiler, Simon-Philip Merz, Christophe Petit, Benjamin Smith, Katherine E. Stange, Yan-Bo Ti, Christelle Vincent, José Felipe Voloch, Charlotte Weitkämper, Lukas Zobernig
The Computer Journal, 67(8) (2024), 2702–2719.
https://doi.org/10.1093/comjnl/bxae038

Research Directions in Number Theory

4 Orientations and Cycles in Supersingular Isogeny Graphs

Sarah Arpin‡, Mingjie Chen‡, Kristin E. Lauter, Renate Scheidler, Katherine E. Stange, Ha T. N. Tran
Research Directions in Number Theory: Women in Numbers V, vol. 33 of *Association for Women in Mathematics Series* (2024), 25–86.
https://doi.org/10.1007/978-3-031-51677-1˙2

Mathematical Cryptology

5 Factoring using multiplicative relations modulo n: a subexponential algorithm inspired by the index calculus

Katherine E. Stange
Mathematical Cryptology, 3(2) (2023), 2-10.
https://journals.flvc.org/mathcryptology/article/view/134295

La Matematica

6 Orienteering with one endomorphism

Sarah Arpin‡, Mingjie Chen‡, Kristin E. Lauter, Renate Scheidler, Katherine E. Stange and Ha T. N. Tran
La Matematica, 2 (2023), 523-582. doi:10.1007/s44007-023-00053-2

Experimental Mathematics

7 Algebraic Number Starscapes

Edmund Harriss, Katherine E. Stange and Steve Trettel
Experimental Mathematics, 31:4 (2022), 1098–1149.
doi:10.1080/10586458.2022.2102094

Involve

8 Monogenic fields arising from trinomials

Ryan Ibarra†, Henry Lembeck†, Mohammad Ozaslan†, Hanson Smith‡ and Katherine E. Stange
Involve – A Journal of Mathematics, Vol. 15 (2022), No. 2, 299–317.
doi:10.2140/involve.2022.15.299

CRYPTO 2021

9 Improved torsion point attacks on SIDH variants

Victoria de Quehen, Péter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, Katherine E. Stange
Advances in Cryptology – CRYPTO 2021, Part 3, vol. 12827 of *Springer Lecture Notes in Computer Science* (2021), 432–470. doi:10.1007/978-3-030-84252-9˙15

SIAM Journal on Applied Algebra and Geometry

10 Algebraic aspects of solving Ring-LWE, including ring-based improvements in the Blum-Kalai-Wasserman algorithm

Katherine E. Stange
SIAM Journal on Applied Algebra and Geometry, 5:2 (2021), 366–387.
doi:10.1137/19M1280442

Compositio Mathematica

11 Local-global principles in circle packings

Elena Fuchs, Katherine E. Stange and Xin Zhang
Compositio Mathematica, 155:6 (2019), 1118–1170.
doi:10.1112/S0010437X19007139

Journal of Number Theory

12 A family of S_4 quartic monogenic fields arising from elliptic curves

T. Alden Gassert††, Hanson Smith‡ and Katherine E. Stange
Journal of Number Theory, 197 (2019), 361–382. doi:10.1016/j.jnt.2018.09.026

Transactions of the American Mathematical Society

13 The dynamics of super-Apollonian continued fractions

Sneha Chaubey‡, Elena Fuchs, Robert Hines‡ and Katherine E. Stange
Transactions of the American Mathematical Society, 372 (2019), 2287–2334.
doi:10.1090/tran/7372

SIAM Journal on Applied Algebra and Geometry

14 Attacks on the Search RLWE Problem with Small Errors

Hao Chen‡, Kristin Lauter and Katherine E. Stange
SIAM Journal on Applied Algebra and Geometry, 1:1 (2019), 665–682.
doi:10.1137/16M1096566

International Mathematics Research Notices

15 Visualising the arithmetic of imaginary quadratic fields

Katherine E. Stange
International Mathematics Research Notices, 2018:12 (2018), 3908–3938.
doi:10.1093/imrn/rnx006

Transactions of the American Mathematical Society

16 The Apollonian structure of Bianchi groups

Katherine E. Stange
Transactions of the American Mathematical Society, 370 (2018), 6169–6219.
doi:10.1090/tran/7111

SAC 2016

17 Security Considerations for Galois Non-dual RLWE Families

Hao Chen‡, Kristin Lauter and Katherine E. Stange
Selected Areas in Cryptography – SAC 2016, vol. 10532 of *Springer Lecture Notes in Computer Science* (2017), 443–462. doi:10.1007/978-3-319-69453-5˙24

New York Journal of Mathematics

18 Index divisibility in dynamical sequences and cyclic orbits modulo p

Annie S. Chen*, T. Alden Gassert†† and Katherine E. Stange
New York Journal of Mathematics, 2017:23 (2017), 1045–1063.
http://nyjm.albany.edu/j/2017/23-45.html

International Mathematics Research Notices

19 Arithmetic properties of the Frobenius traces defined by a rational abelian variety

Alina Cojocaru, Rachel Davis‡ and Alice Silverberg and Katherine E. Stange
with two appendices by J-P. Serre
International Mathematics Research Notices, 2017:12 (2017), 3557–3602.
doi:10.1093/imrn/rnw058

Expositiones Mathematicae

20 The sensual Apollonian circle packing

Katherine E. Stange
Expositiones Mathematicae, 34.4 (2016), 364-395.
doi:10.1016/j.exmath.2016.01.001

Research Directions in Number Theory

21 Ring-LWE Cryptography for the Number Theorist

Yara Elias‡, Kristin E. Lauter, Ekin Ozman and Katherine E. Stange
Research Directions in Number Theory: Proceedings of the 2014 WIN3 Workshop, vol. 3 of *Association for Women in Mathematics Series* (2016), 271–290.
https://doi.org/10.1007/978-3-319-30976-7˙9

Canadian Journal of Mathematics

22 Integral points on ellitic curves and explicit valuations of division polynomials

Katherine E. Stange
Canadian Journal of Mathematics, 68:5 (2016), 1120–1158.
doi:10.4153/CJM-2015-005-0

CRYPTO 2015

23 Provably weak instances of Ring-LWE

Yara Elias‡, Kristin E. Lauter, Ekin Ozman and Katherine E. Stange
Advances in Cryptology – CRYPTO 2015, Part I, vol. 9215 of *Springer Lecture Notes in Computer Science* (2015), 63–92. doi:10.1007/978-3-662-47989-6˙4

Proceedings of the American Mathematical Society

24 A duality principle for selection games

Lionel Levine, Scott Sheffield and Katherine E. Stange
Proceedings of the American Mathematical Society, 141 (2013), 4349–4356. doi:10.1090/S0002-9939-2013-11707-7

American Mathematical Monthly

25 How to make the most of a shared meal: plan the last bite first

Lionel Levine and Katherine E. Stange
American Mathematical Monthly, 119:7 (2012), 550–565. doi:10.4169/amer.math.monthly.119.07.550

Journal of the Australian Mathematical Society

26 Algebraic divisibility sequences over function fields

Patrick Ingram, Valéry Mahé, Joseph H. Silverman, Katherine E. Stange and Marco Streng
Journal of the Australian Mathematical Society (special issue dedicated to Alf van der Poorten) 92:1 (2012), 99–126. doi:10.1017/S1446788712000092

Canadian Mathematical Bulletin

27 Character sums with division polynomials

Igor E. Shparlinski and Katherine E. Stange
Canadian Mathematical Bulletin, 55 (2012), 850–857. doi:10.4153/CMB-2011-126-x

Algebra & Number Theory

28 Elliptic nets and elliptic curves

Katherine E. Stange
Algebra & Number Theory 5:2 (2011), 197–229. doi:10.2140/ant.2011.5.197

Experimental Mathematics

29 Amicable pairs and aliquot cycles for elliptic curves

Joseph H. Silverman and Katherine E. Stange
Experimental Mathematics 20:3 (2011), 329–357. doi:10.1080/10586458.2011.565253

Acta Arithmetica

30 Terms in elliptic divisibility sequences divisible by their indices

Joseph H. Silverman and Katherine E. Stange
Acta Arithmetica 146:4 (2011), 355–378. doi:10.4064/aa146-4-4

Women in Numbers

31 Pairings on hyperelliptic curves

with Jennifer Balakrishnan, Juliana Belding, Sarah Chisholm‡, Kirsten Eisenträger, Katherine E. Stange and Edlyn Teske
WIN – Women in Numbers: Research Directions in Number Theory, Fields Institute Communications 60 (2011), 87–120.

SAC 2008

32 The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences

Kristin Lauter and Katherine E. Stange‡
Selected Areas in Cryptography 2008, vol. 5381 of *Springer Lecture Notes in Computer Science* (2009), 309–327. doi:10.1007/978-3-642-04159-4 ˙20

PAIRING 2007

33 The Tate pairing via elliptic nets

Katherine E. Stange
Pairing-Based Cryptography – PAIRING 2007, vol. 4575 of *Springer Lecture Notes in Computer Science* (2007), 329–348. doi:10.1007/978-3-540-73489-5˙19

RESEARCH PREPRINTS ACCEPTED

Research Directions in Number Theory

34 Prime and thickened prime components in Apollonian circle packings

Holley Friedlander, Elena Fuchs, Piper Harris, Catherine Hsu, James Rickards, Katherine Sanden, Damaris Schindler and Katherine E. Stange
In press with *Proceedings of Women in Number Theory 6*, 41 pages.
arXiv:2410.00177

RESEARCH PREPRINTS

35 Reciprocity obstructions in semigroup orbits in $SL(2, \mathbb{Z})$

James Rickards[††], Katherine E. Stange
27 pages. arXiv:2401.01860

35 Sesquilinear Pairings on Elliptic Curves

Katherine E. Stange
20 pages. arxiv:2405.14167

SCHOLARSHIP OF TEACHING AND LEARNING

PRIMUS: Problems, Resources and Issues in Math. Underg. Studies

37 Standards Based Grading in an Introduction to Abstract Mathematics

Katherine E. Stange
PRIMUS, 28:9 (2018), 797–820. doi:10.1080/10511970.2017.1408044

EXPOSITIONAL WRITING

Notices of the American Mathematical Society

38 On the importance of illustration for mathematical research

Rémi Coulon, Gabriel Dorfsman-Hopkins, Edmund Harriss, Martin Skrodzki, Katherine E. Stange, and Glen Whitney
Notices of the AMS 71(01) (2024), 105-115. https://doi.org/10.1090/noti2839.

Math Horizons

39 April Fools Break Math Rules

Julie Barnes, Marc Chamberland, James Grime, Beth Schaubroeck, Katherine E. Stange and Robert W. Vallin
Math Horizons 31:4 (2024), 5–9. doi:10.1080/10724117.2024.2313428.

Math Horizons

40 The Ingenious Physical Factoring Devices of D.N. Lehmer

Katherine E. Stange
Math Horizons 30:2 (2022), 8–11. doi:10.1080/10724117.2022.2112892.

Illustrating Mathematics

41 Untitled

Katherine E. Stange
Two-page spread including computer graphic in chapter *Graphics* of *Illustrating Mathematics*, Diana Davis, Ed., American Mathematical Society, 2020.
https://bookstore.ams.org/mbk-135.

Notices of the American Mathematical Society

42 An illustration in number theory (2019 Lecture Sampler)

Katherine E. Stange
Notices of the American Mathematical Society 66:03 (2019), 411–413.
https://doi.org/10.1090/noti1826.

CMS Notes

43 Visualizing imaginary quadratic fields

Katherine E. Stange
CMS Notes 48:4 (2016), 16–17.

Asia Pacific Math Newsletter

44 The Farey structure of the Gaussian integers

Katherine E. Stange
Asia Pacific Math Newsletter, 2 (2016), pp. 10-13.
http://www.asiapacific-mathnews.com/toc/0602.html.

VOLUME EDITING

Springer

2016 Directions in Number Theory: Proceedings of the 2014 WIN3 Workshop

with Ellen Eischen, Ling Long and Rachel Pries, vol. 3 of *Association for Women in Mathematics Series*, 339+xv pages. doi:10.1007/978-3-319-30976-7
Refereed conference proceedings.

OTHER WRITING

AWM Newsletter

2012 Women in Numbers II

Association for Women in Mathematics Newsletter, March-April 2012 issue.

EXPOSITIONS OF MY WORK BY OTHERS

Current Events Bulletin

2025/01 Elena Fuchs: Apollonian Packings: The Rise and Fall of the Local-to-Global Conjecture

My joint work (with Haag, Kertzer and Rickards) was featured in the Current Events Bulletin, 2025.

INVITED LECTURE SERIES

Graduate Summer Schools

2024/06 Computational aspects of thin groups

Minicourse: Integral packings and number theory (3 lectures) June 2024
IMS Singapore

2023/07 Renormalization and Visualization for packing, billiard and surfaces

Minicourse: Number theory as a door to geometry, dynamics and illustration (4 lectures) July 2023
CIRM, Marseille, France

CONFERENCE PRESENTATIONS

Plenary/Keynote

upcoming Integers Conference 2025

Plenary Speaker May 2025
Athens, GA

2024/07 Algorithm Number Theory Symposium XVI

Plenary Speaker: Sesquilinear pairings on elliptic curves
Boston, MA

2024/06 Canadian Number Theory Association XVI Meeting

Prize Speaker: Reciprocity obstructions in Apollonian circle packings and continued fractions
Toronto, ON

2024/03 2024 Southern Regional Number Theory Conference

Plenary Speaker: Reciprocity obstructions in Apollonian circle packings and continued fractions
Baton Rouge, LA

2023/08 The VIth Interdisciplinary International Conference on Applied Mathematics, Modeling and Computational Science

Semi-Plenary Speaker: Supersingular isogeny graphs and orientations
Waterloo, Canada

2022/02 Florida Women in Mathematics Day 2022

Keynote Speaker: Preparing cryptography for the arrival of quantum computers
February 2022
Virtual / Boca Raton, FL

2021/06 Arithmetic Geometry, Cryptography and Coding Theory

Plenary Speaker: Ring learning with errors and rounding June 2021
Virtual / CIRM, Luminy, France

2020/08 Canadian Undergraduate Mathematics Conference

Keynote Address: The integer shadows of curves, August 2020
Online

2020/07 The Nineteenth International Conference on Fibonacci Numbers and Their Applications

Lucas Speaker: A visual tour of Fibonacci numbers and their eccentric cousins, elliptic divisibility sequences, July 2020
Online

2019/03 AMS Spring 2019 Joint Central and Western Sectional Meeting

Invited Address: An Illustration in Number Theory
Honolulu, HI

2017/03 Alberta Number Theory Days

Plenary Speaker: Circle packings, thin orbits and the arithmetic of imaginary quadratic fields
Banff, Alberta

2016/04 SouthEast Regional Meeting on Numbers

Plenary Speaker: Visualizing the arithmetic of imaginary quadratic fields
Harrisonburg, VA

Invited

upcoming Rational Points 2025

Invited Speaker July 2025
Schney, Germany

2024/10 Southern California Number Theory Day

Reciprocity obstructions in Apollonian circle packings and continued fractions
Irvine, CA

2024/09 Isogeny Days 5

Sesquilinear pairings on elliptic curves
Leuven, Belgium

2024/04 Pittsburgh Number Theory Day

Reciprocity obstructions in Apollonian circle packings and continued fractions
Pittsburgh, PA

2023/09 ICMAM Latin America Satellite Conference on Algebra, Combinatorics, and Number Theory

The local-global conjecture for Apollonian circle packings is false
International Virtual

2023/08 Isogeny Graphs in Cryptography

The local-global conjecture for Apollonian circle packings is false
Banff, Alberta

2022/08 Park City Mathematics Institute Summer Program on Computation in Number Theory

Orienteering on Isogeny Volcanoes
Research Program

2021/11 Number Theory Web Seminar

Algebraic Number Starscapes
International Virtual

2021/04 Geometry Labs United Seminar

The geometry of number theory, through Möbius transformations
International Virtual

2019/10 Midwest Arithmetic Geometry and Number Theory Series

Apollonia
Columbus, OH

2018/09 Front Range Number Theory Day

A visual tour in arithmetic: from Farey fractions to Apollonian circles
Fort Collins, CO

2017/04 Bay Area Algebraic Number Theory and Arithmetic Geometry Day

Circle packings, thin orbits and the arithmetic of imaginary quadratic fields
Santa Cruz, CA

2016/06 Illustrating Mathematics

Two lecture series: *Visualizing Kleinian Groups* and *Number theory and visualizing Kleinian groups*
ICERM Workshop, Providence, RI

2016/06 Canadian Number Theory Association XIV

Visualizing the arithmetic of imaginary quadratic fields
Calgary, Alberta

2016/06 Secure and Trustworthy Cyberspace

Ring Learning with Errors from a number theorist's perspective
ICERM Workshop, Madison, WI

2015/09 19th Workshop on Elliptic Curve Cryptography

Weaknesses in Ring Learning with Errors
Bordeaux, France

2015/08 Silvermania 2015

Visualising the arithmetic of imaginary quadratic fields
Providence, RI

2014/04 Alberta Number Theory Days

Here a circle, there a circle
Banff, Alberta

2013/06 Pacific Northwest Number Theory Conference

The sensual Apollonian circle packing
Seattle, WA

2012/10 Workshop on Sandpiles and Number Theory

The sensual Apollonian circle packing
Ithaca, NY

2012/06 Canadian Number Theory Association XII

The sensual Apollonian circle packing
Lethbridge, Alberta

2012/05 Algebraic Dynamics

Elliptic divisibility sequences
Berkeley, CA

2011/09 Sage Days 33: Women in Sage

I was messing with elliptic divisibility sequences and Sage didn't do what I wanted
Seattle, WA

2010/12 Sage Days 26: Women in Sage

Amicable pairs for elliptic curves
Seattle, WA

2010/06 Diophantine Approximation and Analytic Number Theory: A Tribute to Cam Stewart

Amicable pairs for elliptic curves
Banff, Alberta

2010/05 Pacific Northwest Number Theory Conference

Amicable pairs for elliptic curves
Vancouver, British Columbia

2009/05 Fields Cryptography Retrospective Meeting

The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences
Toronto, Ontario

2009/03 Arithmétique, géométrie, cryptographie and théorie des codes 2009

The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences
Marseille, France

2008/06 Arithmetic and Geometry Summer School

Elliptic nets and elliptic curves
Tirol, Austria

2007/09 Elliptic Curve Cryptography 2007

Elliptic nets in cryptography
Dublin, Ireland

2007/06 Workshop in Number Theory and Computability

Elliptic nets
Edinburgh, Scotland

2007/05 Algorithmic Number Theory

Elliptic nets
Turku, Finland

Refereed (publications listed above)

2023/08 MathCrypt 2023

Factoring using multiplicative relations modulo n: a subexponential algorithm inspired by the index calculus
Santa Barbara, CA

2022/08 CFAIL 2022

Failing to hash into supersingular isogeny graphs (extended abstract)
Santa Barbara, CA

2015/08 CRYPTO 2015

Provably Weak Instances of Ring-LWE
Santa Barbara, CA

2008/08 Selected Areas in Cryptography 2008

The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences
Sackville, NB, Canada

2007/07 PAIRING 2007

The Tate pairing via elliptic nets
Tokyo, Japan

Special Sessions

upcoming · Topics in Number Theory and Arithmetic Geometry · AMS Western
2025/01 · Methods of Compassionate Math · JMM
2025/01 · Dynamics of Continued Fractions and Related Systems · JMM
2024/12 · Comp. Number Theory and Appl. · Joint AMS-NZMS-AustMS
2020/01 · Experimental and Computer-Assisted Mathematics · JMM
2020/01 · Rational Points on Algebraic Var.: Theory and Comput. · JMM

2020/01 · Algorithms, Experimentation, and Applic. in Number Th. · JMM
2019/03 · The Mathematics of Cryptography · AMS Joint Western-Central
2019/07 · Coding Theory and Cryptography · SIAM AG19
2017/01 · Mathematics of Cryptography · JMM
2017/01 · AWM Workshop on Number Theory · JMM
2016/06 · Analytic Number Theory and Diophantine Equations · CMS
2016/06 · Computational Number Theory · CMS
2016/03 · Elliptic Curves · AMS Southeastern
2016/01 · Arithmetic Dynamics · JMM
2016/01 · Number Theory and Cryptography · JMM
2015/11 · Number Th., Spectral Th., and Homog. Dynamics · AMS Eastern
2015/08 · The Arithmetic of Spheres and Applications · MAA Mathfest
2015/06 · Computational Number Theory · AMMCS-CAIMS
2015/04 · Somos Sequences and Nonlinear Recurrences · AMS Eastern
2015/01 · Recent Developments in Algebraic Number Theory · JMM
2012/03 · Arithmetic Geometry · AMS Western
2012/01 · Rational Points on Varieties · JMM
2012/01 · Dynamical Systems in Algebraic and Arithmetic Geo. · JMM
2011/12 · Analytic Number Theory and Diophantine Approx. · CMS
2011/05 · Arithmetic Dynamics · AMS Western
2010/12 · Computational Number Theory · CMS
2009/12 · Number Theory · CMS
2008/06 · Computational Number Theory · FoCM Hong Kong
2008/01 · Low Genus Curves and Applications · JMM

Contributed

2007/05 · Algorithmic Number Theory · Turku, Finland
2006/07 · Canadian Number Theory Association IX · Vancouver, BC

VISITING PRESENTATIONS

Colloquia

2024/10 · Colorado College Colloquium
2024/02 · Quebec Mathematical Sciences Colloquium
2023/12 · University of Washington
2022/09 · Virginia Tech
2019/11 · Montana State University
2019/11 · DePaul University
2019/10 · Boise State University
2018/09 · University of Colorado, Colorado Springs
2016/03 · University of Washington
2012/02 · University of Denver
2012/02 · University of Iowa
2012/01 · Smith College
2012/01 · University of Colorado, Boulder
2011/12 · Northeastern University
2009/11 · University of Waterloo

Visiting Seminars

upcoming · Number Theory Web Seminar (virtual)
2024/03 · Oregon State University (virtual)
2024/02-03 · Illustrating Mathematics Seminar (virtual) x2
2024/01 · Quebec-Vermont Number Theory Seminar
2023/10 · University of Chicago
2023/10 · Boise State (virtual)
2021/12 · Heidelberg University (virtual)
2019/12 · Princeton University
2019/10 · Harvard University
2019/09 · Brown University
2019/06 · Johann Wolfgang Goethe-Universität, Germany
2019/06 · University of Bristol, UK
2016/11 · University of Madison, Wisconsin
2016/03 · Duke University
2016/03 · University of Oregon

2015/08 · Microsoft Research
2015/05 · University of Illinois, Urbana-Champaign
2014/12 · Rutgers University
2013/07 · Boise State University
2012/10 · University of California, Berkeley
2012/08 · Colorado State University
2012/01 · Smith College
2011/06 · Boise State University
2011/04 · Stanford University
2011/09 · McMaster University
2009/09 · University of British Columbia / Simon Fraser University
2009/04 · Five Colleges
2008/12 · Harvard University
2008/09 · Massachussetts Institute of Technology
2008/06 · ETH Zurich
2008/04 · University of Connecticut
2008/01 · University of British Columbia / Simon Fraser University
2007/12 · University of California Los Angeles
2007/11 · University of California San Diego
2007/11 · Boston University
2007/11 · University of Southern California
2007/02 · Microsoft Research
2004/01 · Vilnius University
2002/11 · Nipissing University

SELECTED INVITATIONAL WORKSHOPS

2023/08 · Isogeny Graphs in Cryptography · BIRS
2022/07 · Park City Mathematics Institute Research Program (3 weeks) Number Theory Informed by Computation · PCMI, Park City, UT
2021/08 · Supersingular Isogeny Graphs in Cryptography (project leader) · BIRS (online)
2021/07 · Park City Mathematics Institute Virtual Program (1 week) Number Theory Informed by Computation · virtual
2020/07 · Women in Numbers 5 (project leader) · BIRS (virtual)
2019/09 · Isogeny-Based Cryptography Workshop · Birmingham, UK
2017/08 · Women in Numbers 4 (project leader, virtual) · BIRS
2017/04 · Arithmetic Golden Gates · AIM
2016/03 · re:boot Number Theory · Duke University
2014/06 · Apollonian Circle Packings (EWM) · Institute Mittag-Leffler
2014/04 · Women in Numbers 3 (project leader) · BIRS
2012/12 · Sandpiles and Number Theory · Cornell University
2011/11 · Women in Numbers 2 · BIRS
2009/03 · Curves, Coding Theory and Cryptography · Luminy
2008/11 · Women in Numbers · BIRS
2006/05 · Zeta Functions All the Way · Institute for Advanced Study
2005/06 · Diophantine Geometry · CRM Ennio De Giorgi

RESEARCH SOFTWARE

Research Scripts

2022 · *Orientation-based algorithms for isogeny graphs* (github github.com/SarahArpin/WIN5)
2021 · *Torsion attacks* (github github.com/torsion-attacks-SIDH/6party)
2019 · *Ring-BKW* (Sage notebook)
2017 · *Schmidt Arrangements: Visual Exploration* (Sage notebook and online interactive)
2015 · *Ring-LWE and Poly-LWE attack* (Sage notebook) with Yara Elias, Kristin E. Lauter and Ekin Ozman
2012 · *Ethiopian Dinner Game* (Sage notebook) with Lionel Levine
2008 · *Tate pairing computation via elliptic nets* (Pari/GP script)
2008 · *Elliptic Divisibility Sequences Tools* (Pari/GP script)

2008 · *Elliptic Nets Tools* (Pari/GP script)
math.katestange.net/code/

Contributor

2010 Sage Mathematics Software (sagemath.org)

Project leader and speaker, Sage Days 26 and 33
Contributions to versions 4.7.2 onwards

INTERDISCIPLINARY ACTIVITIES

Preprint

2024 Traceable random numbers from a nonlocal quantum advantage

Gautam A. Kavuri, Jasper Palfree, Dileep V. Reddy, Yanbao Zhang, Joshua C. Bienfang, Michael D. Mazurek, Mohammad A. Alhejji, Aliza U. Siddiqui, Joseph M. Cavanagh, Aagam Dalal, Carlos Abellán, Waldimar Amaya, Morgan W. Mitchell, Katherine E. Stange, Paul D. Beale, Luís T.A.N. Brandão, Harold Booth, René Peralta, Sae Woo Nam, Richard P. Mirin, Martin J. Stevens, Emanuel Knill, Lynden K. Shalm. https://arxiv.org/abs/2411.05247

Conference Presentation

2023 Responsible AI In the Natural Sciences: a mini workshop

Contributed Talk: *Can large language models prove theorems?*, Virtual / Carnegie Mellon University, May 2023.

POPULAR PRESS & PUBLICITY

Quanta Magazine

2023 The Hidden Connection that Changed Number Theory

Quanta Magazine. Interviewed and quoted in the article, which described quadratic reciprocity. https://www.quantamagazine.org/the-hidden-connection-that-changed-number-theory-20231101/

2023 Two Students Unravel a Widely Believed Math Conjecture

Quanta Magazine. Topic of the article is my work (joint with Haag, Kertzer, Rickards) showing that the local-global conjecture for Apollonian circle packings is false, which grew out of a CU Boulder REU project. https://www.quantamagazine.org/two-students-unravel-a-widely-believed-math-conjecture-20230810/

American Scientist, Pour la Science

2023 The Princess and the Philosopher

American Scientist, Vol. 111, Iss. 2 (Mar/Apr 2023): 80-84. Translated in *Pour la Science*. My images of the Gaussian Schmidt arrangement and laser-cut Apollonian gasket were featured.

Quanta Magazine

2022 Cryptography's future will be quantum-safe. Here's how it will work.

Quanta Magazine. Interviewed and quoted in the article, which described lattice-based cryptography. https://www.quantamagazine.org/cryptographys-future-will-be-quantum-safe-heres-how-it-will-work-20221109/

What's Happening in the Mathematical Sciences

2022 Descartes' Homework

Work featured as part of chapter *Descartes' Homework* of Volume 12. https://bookstore.ams.org/view?ProductCode=HAPPENING/12

Visions of the Universe

2016 Schmidt arrangement visualizations

Schmidt arrangement visualizations featured in *Visions of the Universe: A Coloring Journey Through Math's Greatest Mysteries* (Alex Bellos and Edmund Harris)

AMS Blog

2015 Schmidt arrangement

Featured in the Blog *Visual Insight* of the American Mathematical Society (AMS)
blog.ams.org/visualinsight/2015/03/01/
Also briefly used as AMS branding on Twitter/YouTube/Annual Report etc.

Caltech Radio

2012 Altruists vs. Louts

The Loh-Down on Science, Caltech Radio, November 7, 2012, by Sandra Tsing Loh. Popular account of my game theory work. www.scpr.org/programs/loh-down-on-science/2012/11/07/29100/altruists-vs-louts/

Stanford Magazine

2012 Game Theory Goes to Dinner

Farm Report: Research Notebook, Stanford Magazine, May/June 2012. Popular account of my game theory work, among others.
stanfordmag.org/contents/research-notebook-4061

New Scientist

2011 Step up to the plate

New Scientist, 24/31 December 2011, by Jamie Condliffe. Popular account of my game theory work, among others.

Frankfurter Allgemeine Zeitung

2011 Die Kunst des allseits gerechten Teilens

Frankfurter Allgemeine Zeitung, April 27, 2011, by Heinrich Hemme. Popular account of my game theory work.

The Times and The Sunday Times

2011 The secret of the 3ft-tall salad bowl

The Times and The Sunday Times, January 8, 2011, by James Gillespie. Popular account of my game theory work, among others.

OUTREACH

Public Lectures

2024/04 Bay Area Mathematical Adventures

Public Webinar: The Rational Numbers are Not What They Seem April 2024
Virtual

2023/03 Gathering 4 Gardner Celebration of Mind

Public Webinar: The illustrated field diary of a mathematical naturalist March 2023
Virtual

2022/12 4th Pacific Rim Mathematical Association Congress

Public Lecture: The illustrated field diary of a mathematical naturalist December 2022
Vancouver, Canada

2020/03 National Academies Webinar

Public Webinar: Illustrating Mathematics: Abstract Geometry, Concrete Impact with Jordan Ellenberg, moderated by Terry Tao, March 2020
https://vimeo.com/399320822

General Public

2018 onwards Numberscope

Numberscope is an online tool for visualizing integer sequences from the OEIS, for researchers, artists and interested public. It is being developed via the Experimental Mathematics Lab at CU Boulder under my direction.
math.katestange.net/numberscope github.com/numberscope

2015 onwards YouTube Channel: Proof of Concept

Videos on topics of general interest to all levels, from general public to students and mathematicians (324K+ views, 9K+ subscribers). Featured on channel 3blue1brown. https://www.youtube.com/c/ProofofConceptMath

Fall 2016 CU Science Ambassadors

Training for public outreach through a seminar series that culminates in the creation of an interactive exhibit event at the Boulder and Broomfield Public Libraries

Mathematical Art

upcoming Intersections: Math, Art, Truth, Humanity

contributed digital print at Seattle Universal Math Museum, Spring 2025, Seattle, WA

2020 Art Exhibit: Algebraic Number Starscapes

with Edmund Harriss, Pierre Arnoux, and Steve Trettel. *Algebraic starscapes*. Art Exhibit at Gaukurinn, Reykjavik, Iceland, February 2020.

K-12

2024/07 Program in Mathematics for Young Scientists

Summer Camp Lecture: The Rise and Fall of the Local-to-Global Conjecture July 2024 Boston, MA

2018 Colorado Academy

Math Club Talk: *A Whirlwind tour of cryptography*

2015 onwards Logan School Contact

Meet with grade school students from the Logan School for Creative Learning in Denver who are interested in cryptography or mathematics, approximately yearly.

2012/06 Volunteer, Julia Robinson Math Festival

Staffed an activity table for students in grades 6-12 in Palo Alto, CA.

2010/10 Speaker and Workshop Leader, A Taste of Pi

Led a lecture and workshop for 88 high school students in the greater Vancouver area, on modular arithmetic and elliptic curve cryptography.

SUPERVISION

Postdoctoral

2021-2024 James Rickards

2014-2016 T. Alden Gassert

Doctoral

Ph.D. 2014 Amy Feaver

Thesis: *Euclid's Algorithm in Multiquadratic Fields*

Ph.D. 2019 Robert Hines

Thesis: *Applications of hyperbolic geometry to continued fractions and Diophantine approximation*

Ph.D. 2020 Hanson Smith

Thesis: *Monogeneity and Torsion*

Ph.D. 2020 Daniel Martin

Thesis: *The Geometry of Imaginary Quadratic Fields*

Ph.D. 2022 Sarah Arpin

Thesis: *Supersingular elliptic curve isogeny graphs*

candidate Rebecca DeLand

candidate Joseph Macula

candidate Eli Orvis

candidate Colin Jackson

candidate Summer Haag

Masters

M.A. 2016 Elizabeth Parsons

Thesis: *Simulation of Quantum Prime Factoring Algorithm: Limitations of Random Variables*

Undergraduate

Honours 2024 Clyde Kertzer

Thesis: *Parametrizations of Descartes Quadruples*

Honours 2016 Evan Oliver

Thesis: *Tangency and Structure in Congruence Subarrangements of the Schmidt Arrangement of the Eisenstein Integers*

Honours 2019 Ryan Ibarra

Thesis: *Factorization of Ideals in Algebraic Number Theory and the Montes Algorithm*

Mathematics Lab Director

2017 onwards Experimental Mathematics Lab of CU Boulder

Director, supported by NSF CAREER.
Supports faculty–student project teams synthesizing research, computation, visualization, pedagogy and outreach.

Research Mentoring of Women

2020 Women in Numbers 5 Group Research Co-Leader

Co-leader with Kristin Lauter, leading Sarah Arpin, Mingjie Chen, Renate Scheidler, and Ha Tran.
Topic: *Isogeny graphs in cryptography*

2017 Women in Numbers 4 Group Research Co-Leader

Co-leader with Elena Fuchs and Damaris Schindler, leading Holley Friedlander, Piper Harron and Catherine Hsu.
Topic: *Primes in Apollonian circle packings*

2015 Women in Numbers 3 Group Research Co-Leader

Co-leader with Kristin Lauter, leading Ekin Ozman and Yara Elias.
Topic: *Ring-Learning-with-Errors*
Paper published in CRYPTO 2015: *Weak instances of Ring-LWE*

Student Research Experience

Spring 2024 TU Delft Software Project

Matej Bavec, Ziggy Beijer, Max Derbenwick Kaldis Bērziņš, Gido Vitner
Topic: *New User Interface for Numberscope*
Co-leaders: Glen Whitney, Aaron Fenyes github.com/numberscope

Summer 2023 CU Boulder Internal Research Experience for Undergraduates and First-Year Graduates

Summer Haag (graduate), Clyde Kertzer (undergraduate), James Rickards (postdoc co-leader)
Topic: *Curvatures in Apollonian circle packings*
Preprint: The local-global conjecture for Apollonian circle packings is false.

Fall 2022 Experimental Mathematics Lab

Olivia Brobin, Devlin Costello, Clyde Kertzer, Jenny Leong
Topic: *Numberscope*
Co-leaders: Liam Mulhall, Glen Whitney github.com/numberscope

Fall 2021 Experimental Mathematics Lab

Brendan Heaney, Steven Hristopoulos, Liam Mulhall
Topic: *Numberscope*
Co-leader: Glen Whitney github.com/numberscope

Spring 2020 Experimental Mathematics Lab

Khaled Allen, Isabel Anaya, Theo Lincke, Josiah Martinez, Willem Mirkovich
Topic: *Numberscope*
Co-leader: Sebastian Bozlee (graduate student) github.com/numberscope

Spring 2019 Experimental Mathematics Lab

Abdullatif Khalid Alabduljaleel, Josiah Martinez, Tobias Aldape
Topic: *Visualizing integer sequences*
Co-leader: Sebastian Bozlee (graduate student)

Spring 2019 Experimental Mathematics Lab

Guofeng Deng, Ezzeddine El Sai, Aaron Li
Topic: *Randomness in number theory*
Co-leader: Paul Beale (faculty)

Fall 2018 Experimental Mathematics Lab

Abdullatif Khalid Alabduljaleel, Ang Li, Josiah Martinez, Daniel H. Taylor
Topic: *Visualizing integer sequences*
Co-leader: Sebastian Bozlee (graduate student)

Summer 2018 CU Boulder Internal Research Experience for Undergraduates and First-Year Graduates

Ryan Ibarra (undergraduate), Henry Lembeck (undergraduate), Mohammad Ozaslan (undergraduate), Hanson Smith (graduate co-leader)
Topic: *Monogenic fields arising from trinomials*
Preprint accepted to *Involve – A journal of mathematics*.

Summer 2017 CU Boulder Internal Research Experience for Undergraduates and First-Year Graduates

Sarah Arpin (graduate), Maya Orenstein (graduate), Michael Wheeler (graduate)
Topic: *Geometry of number fields and Ring-LWE*
Presentation at JMM 2018.

Spring 2017 Experimental Mathematics Lab

Sharon Huh, Paul-Robert Laliberte, Chloe Pradeau, John Werner
Topic: *Abelian sandpiles and Gaussian prime tori*
Exhibit with poster, Gemmill Engineering, Mathematics and Physics Library
Software: *Schmidt Arrangement Sandpile Explorer*
Co-advised with Eric Stade

Summer 2016 CU Boulder Internal Research Experience for Undergraduates and First-Year Graduates

Cady Gebhart (undergraduate), Ruofan Li (graduate), Daniel Martin (graduate), Peter Rock (undergraduate)

Topic: *Complex continued fractions*
Poster, *Undergraduate Research Poster Session*, CU Boulder. Presenter: Peter Rock.
Presentation, *Pikes Peak Regional Undergraduate Mathematics Conference.* Presenter: Peter Rock.

Summer 2015 CU Boulder Internal Research Experience for Undergraduates and First-Year Graduates

Andrew Jensen (undergraduate), Cherry Ng (graduate), Evan Oliver (undergraduate), Tyler Schrock (graduate)
Topic: *The Schmidt arrangement of the Eisenstein integers*
Poster, *Undergraduate Research Opportunities Program Poster Session*, CU Boulder. Presenter: Cherry Ng.
Poster, *MAA Undergraduate Student Poster Session*, Joint Mathematics Meetings 2016, Seattle. Presenter: Evan Oliver.

2015-2016 Boulder Valley School District Research Seminar

Annie Chen (Boulder High)
Topic: *Index divisibility in dynamical sequences*
co-advised with T. Alden Gassert
Poster, *Regional Science Fair*, Boulder, CO. Presenter: Annie Chen.
Presentation, *Science Research Symposium*, Boulder, CO. Presenter: Annie Chen.
Presentation, *Joint Mathematics Meetings 2017*, Atlanta. Presenter: Annie Chen.
Paper: *Index divisibility in dynamical sequences and cyclic orbits modulo p.*

Recognition

2023 Invited panelist (as experienced mentor)

Workshop on graduate and postdoc mentoring, Rice University, November 2023

TEACHING AWARDS

University of Colorado, Boulder

2014 ASSETT Development Award

Grant to support teaching with technology, specifically technology for the production of mathematics videos

University of British Columbia

2011 Postdoctoral Teaching Award

Awarded to a teaching postdoctoral fellow

Brown University Mathematics

2008 Outstanding Teaching Award

Awarded to a graduating Ph.D. student

Brown University Mathematics

2005, 2007 Departmental Nominee

Departmental nominee for the Brown University Presidential Award for Excellence in Teaching

COURSES TAUGHT

University of Colorado, Boulder

2024–present Professor

Introduction to Coding Theory and Cryptography, Fall 2024
Graduate *Introduction to the Theory of numbers)*, Fall 2024
Solely responsible for lecture courses of 5 to 35 students. Undergraduate courses are frequently taught in a 50/50 active-learning/lecture format.

University of Colorado, Boulder

2018–2024 Associate Professor

Introduction to Coding Theory and Cryptography, Fall 2020, Fall 2022, Fall 2023
Introduction to Discrete Mathematics, Spring 2020, Fall 2020, Spring 2023

Introduction to the Theory of Numbers, Spring 2019
Graduate *Topics in Number Theory (Elliptic Curves)*, Spring 2020
Graduate *Algebraic Number Theory*, Spring 2019, Spring 2021, Spring 2023
Graduate *Topics in Algebra (Cryptography)*, Spring 2024
Solely responsible for lecture courses of 5 to 35 students. Undergraduate courses are frequently taught in a 50/50 active-learning/lecture format.

University of Colorado, Boulder

2012–2018 Assistant Professor

Calculus II, Fall 2012
Introduction to Discrete Mathematics, Spring 2015, Fall 2015, Fall 2016, Spring 2018 (x2)
Linear Algebra, Fall 2013
Coding and Cryptography, Spring 2014, Fall 2016
Combinatorics, Fall 2015
Graduate *Introduction to Number Theory*, Fall 2012, Fall 2013
Graduate *Introduction to Modern Algebra I*, Fall 2014
Graduate *Topics in Number Theory (Arithmetic of Kleinian Groups)*, Spring 2016
Graduate *Algebraic Number Theory*, Spring 2017
Solely responsible for lecture courses of 5 to 35 students. Undergraduate courses are frequently taught in a 50/50 active-learning/lecture format.
Student independent study (non-thesis): Dalton Jones (Spring 2014), John Willis (Spring 2015), Jenna Allen (Fall 2016), Maya Ornstein (Spring 2018), Sarah Arpin (Spring 2018)

University of British Columbia

2010 Postdoctoral Teaching Fellow

Vector Calculus, Fall 2010
Solely responsible for a standard lecture course of 88 students.

Harvard University

2008–2009 Junior Lecturer

Advanced Algebraic Number Theory, Spring 2009
The Mathematics of Symmetry, Fall 2008
Solely responsible. *The Mathematics of Symmetry* was a seminar-format (student-taught), incorporating writing, programming and group projects as well as homework and tests.

Brown University

2003–2008 Graduate Teaching Fellow

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.

Brown University

2002–2003 Graduate Teaching Assistant

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

OTHER TEACHING EXPERIENCE

Professional Development

Spring 2019 Be The Change: Practicing Inclusive Excellence in the Classroom

1-Day workshop

Spring 2017 CU TRESTLE Scholars Program

Semester-long program on student metacognition

Summer 2016 Inquiry-Based Learning Workshop

3-day workshop, mathematics specific, held at CU Mathematics

2012 onwards Faculty Teaching and Excellence Program

Summer Institute: Digital Learning Communities, May 12–16, 2014
Workshops: *Inverting the Classroom* (2013), *Teaching Portfolio* (2013), *Early Career Faculty: Graduate Advising and Mentoring* (2015), *Getting around student pushback & passiveness in active learning classrooms* (2018)

2012 onwards University of Colorado Workshops

2023 · CHAT+: Disabilities in Academia
2020 · Bystander Training
2018 · Diversity and Inclusion Summit
2016 · Graduate Student Mentoring and Advising Workshop with Jan Morse
2014 · LEAP: Lunch for Women Faculty on Mentoring
2013 · Course Goals and Objectives (2 sessions)
2012 · LGBTQ Issues in the Classroom

2004–2005 Sheridan Center Teaching Certificate, Brown University

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

Guest Lecturing

2021/05 · Swarthmore College · Analytic Number Theory of Circle Packings
2016/03 · University of Oregon · Cryptography

Other Experience

Fall 1998 Tutorial Section Leader, University of Waterloo

As an undergraduate, led once weekly evening tutorial sections for introductory calculus; prepared and worked example problems and answered questions.

1995–2008 Tutoring and math help

Volunteer tutor in mathematics help centres at Waterloo and Brown.
Private tutor for high school and undergraduate students.
Volunteer tutor for Ask Dr. Math (www.mathforum.org/dr.math).

PRESENTATIONS ON TEACHING

Special Sessions

2017 MAA Session on Proofs and Mathematical Reasoning in the First Two Years of College

Standards-based grading in a first proofs course

PEDAGOGICAL SOFTWARE

Sole Author

2018 onwards Online Demos for Elementary Number Theory and Cryptography

8 interactive javascript demonstrations of concepts for elementary number theory math.katestange.net/illustration/elementary-number-theory/

2016 onwards Sage Interactives for Cryptography

20+ online interactive Sage demonstrations of concepts for cryptography crypto.katestange.net

TEACHING RESOURCE DEVELOPMENT

Collaborative

2011 **Mutivariable Calculus Collection, MathDL**

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

Sole Author

2005 onwards **Other Teaching Resources Made Available**

All available at math.colorado.edu/~kstange
YouTube Channel: Proof of Concept, videos on undergraduate mathematics (see also Outreach)
proofofconcept.katestange.net, blog for mathematics majors
Course Notes in the *Arithmetic of Kleinian Groups* (121 pages)
Course Notes for an *Introduction to Number Theory* (153 pages)
Worksheets, combinatorics (13 worksheets)
Worksheets, discrete mathematics and proof (18 worksheets)
Tutorial projects, calculus (7 worksheets)
Advice on Studying in Early Graduate School (3 pages)
many others

MENTORING

Graduate

2012 onwards **Mentoring of Graduate Students**

Graduate Advising Workshop, University of Michigan, 2017.
Mentor, AWM Mentor Network, 2016–onwards.
Invited Mentor, Association for Women in Mathematics Graduate Student Poster Session, JMM 2016, JMM 2017.
Panelist, Applying to Graduate School, Boise State University REU, 2013.
Mentor to incoming graduate students, 1-2 per year, University of Colorado, Boulder.

High School

2023 onwards **Mentoring of High School Student**

Regular meetings with one student.

SERVICE AND LEADERSHIP

Conference Grants

2020 **National Security Agency**

CNTA-XVI
$15 000, one year
with Jeff Achter

2019-2022 **National Science Foundation**

Collaborative Research: Front Range Number Theory Days DMS 1936672,
$12 735, three years
with Hanson Smith, Jeff Achter, Ozlem Ejder

2019 **RIO Faculty Conference Support**

Front Range Number Theory Days
$1 625, one year
with Hanson Smith

Editorial Board

Mathematische Zeitschrift 2025 onwards
Advances in Mathematics of Communications 2023 onwards
Math Horizons 2020 onwards

Program Co-Chair

MathCrypt 2022

Program Committee

Algorithmic Number Theory Symposium (ANTS) 2020, 2022
MathCrypt 2018, 2021

Advisory Boards

Scientific, *Banff International Research Station*, 2022-2023

Equity, Diversity and Inclusion, *Banff International Research Station*, 2022-2023

Prize Committees

David P. Robbins Prize Selection Committee, American Mathematical Society, 2024-2027
Microsoft Research Prize Committee, Association for Women in Mathematics, 2024-2028
Alice T. Schafer Prize Committee, Association for Women in Mathematics, 2025-2028

Women in Mathematics

AWM ADVANCE NSF Grant, Research Networks Committee, member 2017-2019
Women in Numbers Steering Committee, member since 2014, chair 2019–present
Women in Numbers website (www.womeninnumbertheory.org), webmaster
co-developer of a document on making conferences accessible to mathematicians with family responsibilities

Semester co-organizing

upcoming · *IHP trimester in Illustrating Mathematics (January-March 2026)*
Fall 2019 · *ICERM Semester in Illustrating Mathematics in Fall 2019*

Major conference co-organizing

2023/09 · *Renormalization, computation and visualization in Geometry, Number Theory and Dynamics (5 days, 45 participants)*
2019/10 · *Illustrating Number Theory and Algebra (5 days, 94 participants)*
2018 onwards · *Front Range Number Theory Days (1 day, 30-40 participants, twice yearly)*
2015/08 · *Silvermania (5 days, 168 participants)*
2014/04 · *Women in Numbers 3 (5 days, 42 participant research collaboration conference)*

Special session co-organizing

2025/01 · *Local-to-Global in Apollonian Circle Packings and Beyond* · JMM
2019/03 · *Emerging Connections with Number Theory* · AMS Western-Central
2017/04 · *Number Theory* · AWM Symposium
2015/04 · *Arithmetic Geometry* · AMS Western
2013/04 · *Num. Th. with a focus on Dioph. Eq. and Rec. Seq.* · AMS Western

Professional Development

LEAP Workshop Spring 2017

Journal Refereeing

Algebra & Number Theory, American Mathematical Monthly, Annals of Mathematics, Annali della Scuola Normale Superiore, Classe di Scienze, Bulletin of the American Mathematical Society, Canadian Mathematical Bulletin, Communications in Algebra, Electronic Journal of Combinatorics, European Mathematical Society Surveys, Essential Number Theory, Expositiones Mathematicae, Finite Fields and their Applications, Geometriae Dedicata, Hacettepe Journal of Mathematics and Statistics, Houston Journal of Mathematics, IEEE Trans. Comp., International Journal of Number Theory, Involve – a journal of Mathematics, Journal de Théorie des Nombres de Bordeaux, Journal of Algebra and its Applications, Journal of Cryptology, Journal of INTEGERS, Journal of Mathematics and the Arts, Journal of Mathematical Cryptology, Journal of Number Theory, Journal of Operator Theory, Journal of Physics A, Journal of Symbolic Computation, Journal of the Australian Mathematical Society, Linear Algebra and its Applications, New York Journal of Mathematics, Notices of the American Mathematical Society, PRIMUS, Research in Number Theory, Rocky Mountain Mathematics Journal, SIAM Journal on Applied Algebra and Geometry, Transactions of the American Mathematical Society

Proceedings Refereeing

AfricaCrypt, Algorithmic Number Theory Symposium (ANTS), AMMCS-CAIMS, Foundations of Computer Science, PAIRING

Book Refereeing

CRC Press, Princeton University Press

Grant Refereeing

National Science Foundation, frequent panelist, reviewer, including GRFP
National Science and Engineering Research Council of Canada, reviewer
Banff International Research Station, proposal reviewer
American Institute of Mathematics, proposal reviewer

Reviewing

Mathematical Reviews (7 published)

Other Professional Committees

Illustrating Mathematics Steering Commitee, member 2019–present

2025 Mathematical Congress of the Americas Travel Grants Selection Committee, 2024–2025

Other Mathematical Service

panelist for *How to Give a Good Math Talk*, part of ”Lunch in the Time of Covid” professional development series, December 2020.

Professional memberships

American Mathematical Society

Association for Women in Mathematics

Mathematical Association of America

Canadian Mathematical Society

University Service

RIO Week Poster Session Judge Fall 2018

3 Minute Thesis Judge Fall 2018

organizer, CU undergraduate research poster session Fall 2016, 2017

reviewer, UROP Grants Spring 2017, 2020

Departmental Service

director, Experimental Mathematics Lab 2017–present

interim graduate chair fall 2018

executive committee, 2023

graduate committee 2015–2021, 2022–2023

outreach committee 2013–2016

ad-hoc committee for major requirement revision 2015

learning assistant committee 2013, chair 2014

ad-hoc committee for undergraduate research 2014

ad-hoc committee on mentoring 2014

computing committee 2012

website committee 2023–2024

computer scheduler for teaching assignments, including writing software, 2016–present

co-director of graduate student mentoring program, 2018–present

co-organizer of number theory seminar 2012–2020

faculty advisor, COSMOS, 2023–present

presentations visiting prospective student weekend 2015, Undergraduate Math Club 2016, 2020; Math Research Demystified 2021, 2022, COSMOS 2023

department representative Admitted Student Day 2016, UROP Symposium 2018

co-author and grader of algebra preliminary exam (regularly)

grader of algebra diagnostic exam (regularly)

perform teaching observations (regularly)

Examination Committees

doctoral defense chair Amy Feaver, Robert Hines, Daniel Martin, Hanson Smith, Sarah Arpin

doctoral defense thesis reader Nathan Wakefield, Jonathan Kish, Caroline Matson, Ivan Rasskin (Université de Montpellier), Carminda Mennen (University of the Witwatersrand)

doctoral defense committee member Justin Keller, Jared Nishikawa, Ryan Rosenbaum, Cliff Blakestad, Athreya Shankar (physics), Ruofan Li

masters defense chair Elizabeth Parsons

masters defense committee member Jim Maxwell, Laken Top, Lauren Farquhar

honours thesis chair Evan Oliver, Ryan Ibarra, Clyde Kertzer

honours thesis committee member Kaye Sitterley (economics), Andrew Loeliger (physics), Carlos Lopez-Abadia (physics)

comprehensive exam chair Robert Hines, Hanson Smith, Daniel Martin, Sarah Arpin, Eli Orvis, Joseph Macula, Rebecca DeLand, Colin Jackson, Summer Haag

comprehensive exam committee member Cliff Blakestad, Jared Nishikawa, John Willis, Jon Lamar, Megan Ly, Leo Herr, Sarah Salmon, Ruofan Li, Carly Matson, Tyler Schrock, Maya Ornstein, Jun Hong, Jon Kim, Cinea Jenkins, Ben Kitchen

OTHER SKILLS

Languages

English · Mothertongue

French · Intermediate (conversationally fluent)

Technical Skills LaTeX · Python · Pari/GP · Sage Mathematics Software · HTML/css/javascript · photo/video editing

Extracurricular Cycling (past president of Brown Cycling Club as well as Eastern Conference Champion and National Silver Medalist, 2005)

January 19, 2025