KATHERINE E. STANGE

UNIVERSITY OF COLORADO, BOULDER
math.colorado.edu/~kstange

RESEARCH AREAS

Algebraic number theory and arithmetic geometry, including Kleinian groups, elliptic curves and abelian varieties, integer sequences, cryptography.

EDUCATION

Ph.D. 2008	Brown University, under Joseph H. Silverman
M.Sc. 2003	Brown University
B.Math. 2001	University of Waterloo

ACADEMIC POSITIONS

Faculty

2012– The University of Colorado, Boulder
Assistant 2012-2018; Associate 2018-2024; Full Professor since 2024

Visiting

Fall 2019 The Institute for Computational and Experimental Research in Mathematics (ICERM)
Research Fellow, Semester program on Illustrating Mathematics

Postdoctoral

2011-2012 Stanford University (NSF Fellow)

2009-2011 Simon Fraser University, Pacific Institute for the Mathematical Sciences, and the University of British Columbia (NSERC/PINS/NSF Fellow)

2008-2009 Harvard University (NSF Fellow, Lecturer)

RESEARCH AWARDS

Prizes

2024 2020 Ribenboim Prize
"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)

2025 2025 Boulder Faculty Assembly Excellence Award in Research, Scholarly and Creative Work
Awarded by the Boulder Faculty Assembly at the University of Colorado Boulder, for "faculty contributions of the highest quality."

Fellowships

2025-2026 AMS Joan and Joseph Birman Fellowship, $50,000

2021-2022 Simons Fellowship, Simons Foundation, $94,489

Selected Research Grants

2024-2027 PI, NSF, DMS 2401580, $350,000

2018-2019 Co-PI, CU Boulder RIO QuEST, $50,000

2017-2024 PI, NSF CAREER, CNS-1652238, $539,975

2016-2018 PI, NSF EAGER, DMS-1643552, $200,000

2016-2017 PI, NSA, Young Investigators, $40,000

2014-2015 PI, NSA, Young Investigators, $40,000

Postdoctoral Awards

2008-2012 NSF Postdoctoral Fellowship, $108,000

2009-2011 NSERC (Canada) Postdoctoral Fellowship, $80,000
"Most outstanding candidate at the Postdoctoral level, Mathematics"

2009-2011 PIMS Postdoctoral Fellowship

PUBLICATIONS

ASIACRYPT 2024

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.

Annals of Mathematics

The Local-Global Conjecture for Apollonian circle packings is false
Summer Haag, Clyde Kertzer, James Rickards, Katherine E. Stange *Annals of Mathematics*, 200 (2) (2024), 749–770.

The Computer Journal (CFAIL 2022)

Failing to hash into supersingular graphs
Jeremy Booher, Ross Bowden, Javad Doliskani, Tako Boris Fouotsa, Steven D. Galbraith, Sabrina Kunzweiler, Simon-Philipp 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.

Research Directions in Number Theory

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 (2024), 25-86.

Mathematical Cryptology (Mathcrypt 2023)

Factoring using multiplicative relations modulo n: a subexponential algorithm inspired by the index calculus
Katherine E. Stange
Mathematical Cryptology, 3(2) (2023), 2-10. (Mathcrypt 2023 special issue)

La Matematica

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.

Experimental Mathematics

Algebraic Number Starscapes
Edmund Harriss, Katherine E. Stange, Steve Trettel
Experimental Mathematics, 31:4 (2022) 1098–1149.

Involve

Monogenic fields arising from trinomials
Ryan Ibarra, Henry Lembeck, Mohammad Ozaslan, Hanson Smith, Katherine E. Stange
Experimental Mathematics, 15:2 (2022) 299–317.

CRYPTO 2021

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.

SIAM Journal on Applied Algebra and Geometry

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.

Journal of Number Theory

A family of monogenic S_4 quartic fields arising from elliptic curves
T. Alden Gassert, Hanson Smith and Katherine E. Stange
Journal of Number Theory, 197 (2019), 361-382.

Compositio Mathematica

Local-Global Principles in Circle Packings
Elena Fuchs, Katherine E. Stange, and Xin Zhang
Compositio Mathematica, 155:6 (2019), 1118-1170.

SIAM Journal of Applied Algebra and Geometry

Attacks on the Search-RLWE problem with small errors
Hao Chen, Kristin Lauter and Katherine E. Stange
SIAM Journal of Applied Algebra and Geometry, 1-1 (2019), 665–682.

Transactions of the AMS

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.

Transactions of the AMS

The Apollonian structure of Bianchi groups
Katherine E. Stange
Transactions of the American Mathematical Society, 370 (2018), 6169–6219.

International Mathematics Research Notices

Visualising the arithmetic of imaginary quadratic fields
Katherine E. Stange
International Mathematics Research Notices, 2018:12 (2018), 3908–3938.

SAC 2016

Security Considerations for Galois Non-dual RLWE Families
Hao Chen, Kristin Lauter and Katherine E. Stange
Selected Areas in Cryptography 2016 – SAC 2016, LNCS vol 10532 (2017), 443–462.

New York Journal of Mathematics

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.

International Mathematics Research Notices

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.

Expositiones Mathematicae

The sensual Apollonian circle packing
Katherine E. Stange
Expositiones Mathematicae, 34.4 (2016), 364-395.

Research Directions in Number Theory

RLWE 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.

Canadian Journal of Mathematics

Integral points on ellitic curves and explicit valuations of division polynomials
Katherine E. Stange
Canadian Journal of Mathematics, 68.5 (2016), 1120–1158.

CRYPTO 2015

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.

Proceedings of the AMS

A duality principle for selection games
Lionel Levine, Scott Sheffield and Katherine E. Stange
Proceedings of the American Mathematical Society, 141 (2013), 4349-4356.

American Mathematical Monthly

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.

Journal of the Australian Mathematical Society

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.

Canadian Mathematical Bulletin

Character sums with division polynomials
Igor E. Shparlinski and Katherine E. Stange
Canadian Mathematical Bulletin, 55 (2012), 850-857.

Algebra & Number Theory

Elliptic nets and elliptic curves
Katherine E. Stange
Algebra & Number Theory 5.2 (2011), 197-229.

Experimental Mathematics

Amicable pairs and aliquot cycles for elliptic curves
Joseph H. Silverman and Katherine E. Stange
Experimental Mathematics 20.3 (2011), 329-357.

Acta Arithmetica

Terms in elliptic divisibility sequences divisible by their indices
Joseph H. Silverman and Katherine E. Stange
Acta Arithmetica 146.4 (2011), 355-378.

Women in Numbers

Pairings on hyperelliptic curves
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

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.

PAIRING 2007

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.

TO APPEAR

Duke Mathematical Journal

Reciprocity Obstructions for Thin Semigroup Orbits in $\mathrm{SL}(2,\mathbb{Z})$
James Rickards and Katherine E. Stange

STOC 2025

On the complexity of isomorphism problems for tensors, groups, and polynomials V: over commutative rings
Joshua Grochow, Youming Qiao, Katherine E. Stange, Xiaorui Sun

Research Directions in Number Theory

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

SCHOLARSHIP OF TEACHING AND LEARNING

PRIMUS

Standards Based Grading in an Introduction to Abstract Mathematics
Katherine E. Stange
PRIMUS: Problems, Resources and Issues in Mathematics Undergraduate Studies 28.9 (2018), 797–820.

OTHER HONORS

Association for Women in Mathematics Fellow

Class of 2021, "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."

Writing Award

2013 Paul R. Halmos - Lester R. Ford Award for outstanding paper 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*

Exposition Award

2023 Winner (one of five), Summer of Mathematics Exposition 3 https://some.3b1b.co/, sponsored by 3blue1brown, for YouTube video *Rethinking the real line*.

OTHER ACTIVITIES

Expositional Writing

On the importance of illustration for mathematical research, with Rémi Coulon, Gabriel Dorfsman-Hopkins, Edmund Harriss, Martin Skrodzki, and Glen Whitney; *Notices of the American Mathematical Society* 71:01 (2024), 105-115, https://www.ams.org/notices/202401/rnoti-p105.pdf.
April Fools Break Math Rules, with Julia Barnes, Marc Chamberland, James Grime, Bath Schaubroeck and Robert W. Vallin, *Math Horizons* 31:4 (2024), 5–9., doi:10.1080/10724117.2024.2313428.
The Ingenious Physical Factoring Devices of D.N. Lehmer, *Math Horizons* 30:2 (2022), 8–11., doi:10.1080/10724117.2022.2112892.
Untitled two-page spread including computer graphics in chapter *Graphics* of *Illustrating Mathematics*, Diana Davis, ed., American Mathematical Society, 2020.https://bookstore.ams.org/mbk-135.
An illustration in number theory (2019 Lecture Sampler), *Notices of the American Mathematical Society* 66:03 (2019), 411–413, https://www.ams.org/journals/notices/201903/rnoti-p411.pdf.
Visualizing Imaginary Quadratic Fields, *CMS Notes* 48:4 (2016), 16–17.
The Farey Structure of the Gaussian Integers, *Asia Pacific Math Newsletter*, 2 (2016), 10–13. http://www.asiapacific-mathnews.com/toc/0602.html.

Supervision

Postdoctoral: James Rickards (2021-2024), T. Alden Gassert (2014-2016)
Ph.D.: Sarah Arpin (2022), Daniel Martin (2020), Hanson Smith (2020); Robert Hines (2019), Amy Feaver (2014)
M.A.: Elizabeth Parsons (2016)

Pedagogy

University of British Columbia Postdoctoral Teaching Award, 2011
Brown University Mathematics Outstanding Teaching Award, 2008
Proof of Concept, Educational YouTube Channel (6K+ subscribers, 230K+ views)
TRESTLE Scholar, CU Boulder, Spring 2017
Faculty Teaching Excellence Program Summer Insitute, Summer 2014
Selected professional development Be The Change: Practicing Inclusive Excellence in the Classroom (2019), Graduating Advising Workshop (2017), Inquiry Based Learning Workshop (2016)
Sheridan Center Teaching Certificate, Brown University, 2005
Standards Based Grading in a First Proofs Course, presentation at JMM 2017
Course materials incl. online videos via University of Colorado Boulder ASSETT grant

Courses Taught

Undergraduate, CU Boulder: Calculus II, Introduction to Discrete Mathematics (x8), Linear Algebra, Coding and Cryptography (x6), Combinatorics, Introduction to the Theory of Numbers
Graduate, CU Boulder: Introduction to Number Theory (x3), Introduction to Modern Algebra I, Algebraic Number Theory (x4), Topics: Arithmetic in Kleinian Groups, Topics: Elliptic Curves, Topics: Mathematical Cryptography
University of British Columbia: Vector Calculus
Harvard University: Algebraic Number Theory, Mathematics of Symmetry
Brown University: Introductory Calculus, Multivariable Calculus, Linear Algebra

Graduate Schools Given

2024/06 · Computational Aspects of Thin Groups (Integral packings and number theory), IMS Singapore
2023/07 · Renormalization and visualization for packing, billiard and surfaces (Number theory through geometry, dynamics and visualization), CIRM Luminy

Selected Research Talks

upcoming · Plenary, Canadian Mathematical Society Summer Meeting 2025
2024/07 · Plenary, Algorithmic Number Theory XVI
2024/06 · 2020 Ribenboim Prize Lecture, Canadian Number Theory Association XVI
2024/03 · Plenary, Southern Regional Number Theory Conference
2023/08 · Semi-Plenary, The VIth Interdisciplinary International Conference on Applied Mathematics, Modeling and Computational Science
2022/02 · Plenary, Florida Women in Mathematics Day
2021/06 · Plenary, Arithmetic Geo., Crypt., and Coding Theory 2021 (CIRM)
2020/07 · Lucas Lecturer, The Nineteenth International Conference on Fibonacci Numbers and Their Applications
2019/03 · Invited Address, AMS Spring Joint Central and Western Sectional
2016/03 · Plenary, Alberta Number Theory Days
2016/04 · Plenary, SouthEast Regional Meeting on Numbers
2015/09 · Invited, ECC 2015
2007/09 · Invited, ECC 2007

Selected Art	Exhibit, joint work with Edmund Harriss and Steve Trettel, *Algebraic Number Starscapes*, Iceland, 2020 Contributed piece *The Secret Life of Gaussian Integers*, Seattle Universal Math Museum, *Intersections: Math, Art, Truth, Humanity*, March 2025.
Selected Press & Exposure	Featured in *Current Events Bulletin*, American Mathematical Society, 2025, work on Apollonian packings Featured in *Quanta Magazine*, 2023, work on Apollonian packings Featured in *What's Happening in the Mathematical Sciences*, Volume 12, 2022, work on Apollonian packings and Schmidt arrangements Featured in *New Scientist* Magazine, 2011, work in game theory
Women in Mathematics	Co-organizer and refereed proceedings editor, Women in Numbers 3 Project Leader at Women in Numbers 4, Women in Numbers 5 Chair, Women in Number Theory Steering Committee, 2019-onwards Webmaster, Women in Number Theory Steering Committee, 2016-onwards Member, Women in Number Theory Steering Committee, 2014-onwards AWM Advance NSF Grant, AWM Research Networks Committee, 2017-2021 Mentor, AWM Mentor Network, 2016-onwards Invited mentor, AWM Graduate Student Poster Session, JMM 2016, 2017
Software and Illustration	Co-Organizer, Illustrating Mathematics, Special Trimester Spring 2026, IHP Co-Organizer, Illustrating Mathematics, Special Semester Fall 2019, ICERM Steering Committee, Illustrating Mathematics Director of Development, Numberscope Contributer to Sage Mathematics Software
Conference Grants	Co-PI, NSA, $15,000 (CTNA XVI) (2020) Co-PI, NSF, DMS 1936672, $12,735 (FRNTD) (2019-2022) Co-PI, CU Boulder RIO $1,625 (FRNTD) (2019)
Editorial	Proceedings Volume Editor, with Ellen Eischen and Ling Long, *Directions in Number Theory: Proceedings of the 2014 WIN4 Workshop*, Association for Women in Mathematics Series. Editorial Board, Mathematische Zeitschrift, 2025 onwards Editorial Board, Advances in Mathematics of Communications, 2023 onwards Editorial Board, Math Horizons, 2020 onwards Program Co-Chair, MathCrypt 2022 Program Committee, ANTS 2020, 2022; MathCrypt 2018, 2021
Early Research Experiences	Director, CU Experimental Mathematics Lab, 2017-onwards Mathematics Lab Project Leader, 2017-onwards Summer REU/G group leader, 2015, 2016, 2017, 2018, 2023 Advisor of high school student research, 2015-16 Honors Thesis advising, 2015-16, 2018-19, 2023-24
Selected Outreach	YouTube channel *Proof of Concept*, 324K+ views, 9K+ subscribers Numberscope (web tool for the general public) CU Science Ambassador, 2016 Speaker (with Jordan Ellenberg, moderated by Terry Tao), The National Academies Webinar *Illustrating Mathematics: Abstract Geometry, Concrete Impact* (2020) Public Web Seminar, Bay Area Mathematical Adventures, 2024 Public Web Seminar, Gathering4Gardner Celebration of Mind, 2022 Public Lecture, The Pacific Rim Mathematical Association Congress, 2022 Julia Robinson Math Festival, 2012 Workshop Leader, A Taste of Pi, 2010
Prize Committees	Alice T. Schafer Prize Committee, AWM, 2025-2028 Microsoft Research Prize Committee, AWM, 2024-2028 David P. Robbins Prize Selection Committee, AMS, 2024-2027
Selected Other Service	Advisory Boards, Scientific and DEI, Banff IRS, 2022-2023

March 5, 2025