Andrew V. Sutherland

Curriculum Vitae

(Last updated May 2026)

Department of Mathematics (2-341)
Massachusetts Institute of Technology
77 Massachusetts Avenue, Cambridge, MA 02139

(617) 253-4381
drew@math.mit.edu
math.mit.edu/~drew

Education

Ph.D. in Mathematics, Massachusetts Institute of Technology, 2007.

S.B. in Mathematics, Massachusetts Institute of Technology, 1990.

Employment

Massachusetts Institute of Technology (2024–) Senior Research Scientist
(2012–2024) Principal Research Scientist
(2009–2011) Research Scientist
(2007–2009) Research Affiliate

Editorial and Board Positions

Advisory Board Member, Zulip Foundation, 2026–present.

Scientific Advisory Board Member, Institute for Computational and Experimental Research in Mathematics, 2024–present.

Board Member, Sagemath Inc., 2023–present.

President, The Number Theory Foundation, 2019–present.

Steering Committee, Algorithmic Number Theory Symposia, 2019–present.

Editor in Chief, Research in Number Theory (Springer Nature), 2017–present.

Managing Editor, The L-Functions and Modular Forms Database, 2016–present.

Associate Editor, Mathematics of Computation (AMS), 2014–present.

Grants and Fellowships

New AI Based Methods to Prove and Verify Mathematics, DARPA, 2026-2029, Award HR0011684748 ($3.2 million)

Scalable Theorem Proving via Mathematical Databases, Renaissance Philanthropy, 2025-2027 ($266 thousand)

Computational Mathematics in Magma, Simons Foundation, 2024-2029, SFI-MPS-Infrastructure-00008651 ($2.2 million at MIT of $4.8 million total).

Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation, Simons Foundation, 2017-2025, Grant 550033 ($6.7 million at MIT of $14 million total).

ANTS XVI: Algorithmic Number Theory Symposium, NSF, 2024 [DMS-2401305].

ANTS XIV: Algorithmic Number Theory Symposium, NSF, 2020 [DMS-1946311].

Computational Methods in Arithmetic Geometry, NSF, 2015-2019 [DMS-1522526].

Computational Methods in Arithmetic Geometry, NSF, 2011-2014 [DMS-1115455].

Graduate Research Fellowship, NSF, 1990-1993.

Honors and Awards

Fellow of the American Mathematical Society, class of 2021.

Selfridge Prize, Number Theory Foundation, 2012.

Infinite Kilometer Award, MIT, 2011.

George M. Sprowls Award for Outstanding Ph.D. Thesis, MIT, 2007.

Grand Prize, MIT LCS Programming Contest, 1991.

Phi Beta Kappa, MIT, 1990.

Conferences Organized

LMFDB, Computation, and Number Theory (LuCaNT 2025), ICERM, July 2025, with J.W. Jones, J. Paulhus, and J. Voight.

Sixteenth Algorithmic Number Theory Symposium (ANTS XVI), MIT, July 2024, with J. Balakrishnan, K.S. Kedlaya, and J. Voight.

The Mordell Conjecture 100 Years Later, MIT, July 2024, with J. Balakrishnan, P. Habegger, B. Poonen, A. Sutherland, and W. Zhang.

LMFDB, Computation, and Number Theory (LuCaNT), ICERM, July 2023, with J.E. Cremona, J.W. Jones, J. Paulhus, and J. Voight.

AMS Special Session on Arithmetic Geometry Informed by Computation, Joint Mathematics Meetings, Boston, January 2023, with J. Balakrishnan and B. Poonen.

Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation Annual Meeting 2022, Simons Foundation, January 2022, with J. Balakrishnan, N. Elkies, B. Hassett, B. Poonen, and J. Voight.

Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation Annual Meeting 2021, Simons Foundation (online), January 2021, with J. Balakrishnan, N. Elkies, B. Hassett, B. Poonen, and J. Voight.

Fourteenth Algorithmic Number Theory Symposium (ANTS XIV), University of Auckland (online), July 2020, with S. Galbraith.

Workshop on Arithmetic Geometry, Number Theory, and Computation, ICERM (online), June 2020, with J. Balakrishnan, N. Elkies, B. Hassett, B. Poonen, and J. Voight.

AMS Special Session on Rational Points on Algebraic Varieties: Theory and Computation, Joint Mathematics Meetings, Denver, January 2020, with B. Hassett and A. Varilly-Alvarado.

Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation Annual Meeting 2020, January 2020, with J. Balakrishnan, N. Elkies, B. Hassett, B. Poonen, and J. Voight.

AMS Special Session on Number Theory, Arithmetic Geometry, and Computation, Joint Mathematics Meetings, Baltimore, January 2019, with B. Hassett and J. Voight.

Arithmetic of Low-Dimension Abelian Varieties, ICERM, Providence, June 2019, with J. Balakrishnan, N. Elkies, B. Hassett, B. Poonen, and J. Voight.

Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation Annual Meeting, January 2019, with J. Balakrishnan, N. Elkies, B. Hassett, B. Poonen, and J. Voight.

Arithmetic Geometry, Number Theory, and Computation, MIT, August 2018, with J. Balakrishnan, N. Elkies, B. Hassett, B. Poonen, and J. Voight.

Postdoctoral Researchers Supervised (at MIT)	Nina Zubrilina, C.L.E. Moore Instructor, NSF Postdoctoral Fellow, 2024–present.
	Eran Assaf, Research Scientist, 2024–present.
	Edgar Costa, Research Scientist, 2024–present.
	Shiva Chidambaram, Research Scientist, 2021–2024 (co-supervised by B. Poonen).
	Wanlin Li, Research Scientist, 2019–2022 (co-supervised by B. Poonen).
	Sam Schiavone, Research Scientist, 2019–present (co-supervised by B. Poonen).
	Raymond van Bommel, Research Scientist, 2019–2024 (co-supervised by B. Poonen).
	Francesc Fité, Research Scientist, 2019–2021 (co-supervised by B. Poonen).
	Dohyeong Kim, Research Scientist, 2018–2019 (co-supervised by B. Poonen).
	Maarten Derickx, Research Scientist, 2018–2019 (co-supervised by B. Poonen).
	Edgar Costa, Research Scientist, 2018–2024 (co-supervised by B. Poonen).
	David Roe, Research Scientist, 2018–present (co-supervised by B. Poonen).
Graduate Students Supervised (at MIT)	Jia (Jane) Shi, Ph.D. 2028 (expected).
	Xunjing Wei, Ph.D. 2027 (expected).
	Pratyush Venkatakrishnan. M.Eng. 2027 (expected).
	Krit Boonisreth, M.Eng. 2024.
Service (at MIT)	Mathematics Department IT Oversight Committee, chair, 2021–present
	Pset Partners, administrator, 2020–present.
	Number Theory Seminar, co-organizer, 2020–present.
	Mathematics Department Diversity and Community Building Committee, 2020–present.
	Mathematics Major Advisor, 2019–present.
	BC-MIT Number Theory Seminar, co-organizer, 2018–present.
	OpenCourseWare contributor, 2012, 2013, 2015, 2017, 2019, 2021.
	Undergraduate Research Opportunity Supervisor (UROP), 2010–present.
	First-Year Advisor, 2009–2011.
	Educational Studies Program (Splash and HSSP), 2003–2008
Service (other)	Arizona Winter School, advisory board member, 2024–present.
	AMS David P. Robbins Prize Committee, chair, 2021–2024.
	Research Seminars, administrator, 2020–present.
	VaNTAGe Seminar, co-organizer, 2020–present.

Invited Lectures (selected)

L-functions from nothing, Plenary Lecture, 33èmes Journées Arithmétique, Luxembourg, 2025 (plenary lecture).

The fine art of point counting, The Beeger Lecture, Nederlands Mathematisch Congres, De Werelt, 2024.

Lattices in computational number theory and arithmetic geometry, Simons Symposium on the Math of Computing According to Lattices, 2023.

Murmurations of arithmetic L-functions, Institute for Advanced Study, 2023.

A database of modular curves, Arithmetic, Algebra, and Algorithms, ICMS Edinburgh, 2023.

Counting points on modular curves, Foundations of Computational Mathematics (FoCM), Sorbonne University, 2023.

Diophantine computations, The Arf Lecture, Ankara, 2022.

On a question of Mordell, Mordell 2022, Cambridge University, 2022.

Computational tools for number theorists, IAS/PCMI summer program, Park City, 2022 (five part lecture series).

Number theory and the LMFDB, Harvard Center of Mathematical Sciences and Applications, Harvard University, 2022.

ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$, Upstate Number Theory Conference, Union College, 2021 (plenary lecture).

The L-functions and modular forms database, International Congress on Mathematical Software, online, 2020.

Sato-Tate groups of abelian threefolds, Front Range Number Theory Day, online, 2020.

Arithmetic L-functions and their Sato–Tate distributions, VaNTAGe Seminar, online, 2020.

Sums of three cubes, Computational Mathematics Colloquium, University of Waterloo, Canada, 2019.

Computing zeta functions and L-functions of curves, Clay Mathematics Institute and Heilbronn Institute for Mathematical Research Summer School in Computational Number Theory, University of Bristol, UK, 2019 (four part lecture series).

Counting points on modular curves, Arithmetic Geometry, Coding Theory, and Cryptography, 2019, CIRM Luminy, France, June 2019.

Building telescopes for mathematicians, Simons Foundation Lectures, New York City, 2019 (public lecture).

Stronger arithmetic equivalence, Princeton/IAS Number Theory Seminar, Princeton University, 2019.

A database of genus 3 *curves*, Birational Geometry and Arithmetic, ICERM, Providence, 2018.

Computing zeta functions in average polynomial time, International Conference on Applied Mathematics, Modeling and Computational Science (AMMCS IV), Waterloo, Canada, 2017 (plenary lecture).

Computing L-series of hyperelliptic curves, Workshop on the Arithmetic of Hyperelliptic Curves, International Centre for Theoretical Physics, Trieste, 2017.

Sato–Tate in dimension 3, Harvard Number Theory Seminar, Harvard University, 2016.

Torsion subgroups of rational elliptic curves over the compositum of all cubic fields, Explicit Methods in Number Theory, Warwick University, UK, 2016.

Sato–Tate distributions, 2016 Arizona Winter School on Analytic Methods in Arithmetic Geometry, University of Arizona, Tucson, 2016 (four part lecture series).

Sieve theory and small gaps between primes (joint with Andrew Granville), Explicit Methods in Number Theory, Oberwolfach, Germany, 2015 (five part lecture series).

Computing the image of Galois, Dartmouth Mathematics Colloquium, 2014.

Telescopes for mathematicians, Conference on the Impact of Computation in Number Theory, NCTS, Taiwan, 2014.

The refined Sato–Tate conjecture, 13th Conference of the Canadian Number Theory Association (CNTA XIII), Ottawa, Canada, 2014 (plenary lecture).

The Sato–Tate conjecture for abelian varieties, Heilbronn Seminar, Bristol University, United Kingdom, 2014.

Sato–Tate distributions of curves (joint with Francesc Fité), 2014 CIRM Winter School on Frobenius Distributions of Curves, Luminy, France, 2014 (six part lecture series).

New bounds on gaps between primes, Brandeis–Harvard–MIT–Northeastern Joint Colloquium, MIT, 2013.

Sato–Tate distributions in genus 2, Princeton/IAS Number Theory Seminar, Institute for Advanced Study, Princeton, 2012.

Computing the modular equation, Barcelona-Boston-Tokyo Number Theory Seminar in Memory of Fumiyuki Momose, Universitat Politècnica de Catalunya, Barcelona, 2012.

Isogeny volcanoes, Algorithmic Number Theory Tenth International Symposium (ANTS X), San Diego, 2012 (plenary lecture).

On the evaluation of modular polynomials, 16th Workshop on Elliptic Curve Cryptography (ECC 2012), Querétaro, Mexico, 2012 (plenary lecture).

Genus 1 point counting in quadratic space and essentially quartic time, Foundations of Computational Mathematics (FoCM 2011), Budapest, Hungary, 2011.

Hyperelliptic curves, L-polynomials, and random matrices, Workshop on Arithmetic Statistics, MSRI, Berkeley, 2011.

A local-global principle for rational isogenies of prime degree, 11th Conference of the Canadian Number Theory Association (CNTA XI), Acadia, Canada, 2010.

L-polynomial distributions of genus 2 *curves*, Rational Points: Theory and Experiment, ETH Zurich, Switzerland, 2010.

Computing modular polynomials with the Chinese remainder theorem, 13th Workshop on Elliptic Curve Cryptography (ECC 2009), Calgary, 2009 (plenary lecture).

Powered by volcanoes: three new algorithms, Cryptography Retrospective Meeting, Fields Institute, Toronto, Canada, 2009 (plenary lecture).

Computing Hilbert class polynomials with the CRT method, 12th Workshop on Elliptic Curve Cryptography (ECC 2008), Utrecht, Netherlands, 2008 (plenary lecture).

Research Publications

B. Alexeev, E. Conway, M. Rosenfeld, A.V. Sutherland, T. Tao, M. Uhr, and K. Ventullo, *Decomposing a factorial into large factors*, to appear in Math. Comp.

J.S. Ellenberg, C.S. Fraser-Taliente, T.R. Harvey, K. Srivastava, and A.V. Sutherland, *Generative modeling for mathematical discovery*, to appear in Adv. Theor. Math. Phys.

J. Paulhus and A.V. Sutherland, *Completely decomposable modular Jacobians*, LuCaNT: Databases, Algorithms, and Computational Number Theory , 271–276, Contemp. Math. **840**, Amer. Math. Soc., 2026.

Edited by J. Jones, J. Paulhus, A.V. Sutherland, and J. Voight, *LuCaNT: Databases, Algorithms, and Computational Number Theory*, Contemp. Math. **840**, Amer. Math. Soc., 2026.

[MR5037238] J. Booher, E.W. Howe, A.V. Sutherland, and J.F. Voloch, *Doubly isogenous curves of genus two with a rational action of D_6*, Res. Math. Sci. **13** (2026), no. 1, Paper No. 23, 43 pp.

[MR4959388] F. Fité, K.S. Kedlaya, and A.V. Sutherland, *Sato–Tate groups of abelian threefolds*, Mem. Amer. Math. Soc. **312** (2025), no. 1582, v+104 pp.

[MR4868102] C. Maistret, *Computing Euler factors of genus 2 curves at odd primes of almost good reduction*, Proceedings of the Sixteenth Algorithmic Number Theory Symposium (ANTS XVI), Res. Number Theory **11** (2025), 21 pages.

[MR4732684] J.E. Cremona and A.V. Sutherland, *Computing the endomorphism ring of an elliptic curve over a number field*, LuCaNT: LMFDB, Computation, and Number Theory, 75–102, Contemp. Math. **796**, Amer. Math. Soc., 2024.

[MR4732680] Edited by J.E. Cremona, J. Jones, J. Paulhus, A.V. Sutherland, and J. Voight, *LuCaNT: LMFDB, Computation and Number Theory*, Contemp. Math. **796**, Amer. Math. Soc., 2024.

[MR4514545] E. Costa, D. Harvey, and A.V. Sutherland, *Counting points on smooth plane quartics*, Proceedings of the Fifteenth Algorithmic Number Theory Symposium (ANTS XV), Res. Number Theory **9** (2023), 32 pages.

[MR4496969] Appendix to S. Kim and M.R. Murty, *From the Birch and Swinnerton-Dyer conjecture to Nagao's conjecture*, Math. Comp. **92** (2023), 385–408.

[MR4468989] J. Rouse, A.V. Sutherland, and D. Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$*, with an appendix by J. Voight, Forum of Math., Sigma **10** (2022), 62 pages.

[MR4379983] Appendix to S. Asif, F. Fité, D. Pentland, *Computing L-Polynomials of Picard curves from Cartier-Manin matrices*, Math. Comp. **91** (2022), 943–971.

[MR4427962] A.J. Best, J. Bober, A.R. Booker, E. Costa, J. Cremona, M. Derickx, M. Lee, D. Lowry-Duda, D. Roe, A.V. Sutherland, and J. Voight, *Computing classical modular forms*, Arithmetic Geometry, Number Theory, and Computation, Simons Symposia, Springer, 2021, 123–213.

[MR4427958] Edited by J. Balakrishnan, N. Elkies, B. Hassett, A.V. Sutherland, J. Voight, *Arithmetic Geometry, Number Theory, and Computation*, Simons Symposia, Springer, 2021.

[MR4341956] A.V. Sutherland, *Stronger arithmetic equivalence*, Discrete Anal. (2021), no. 23.

[MR4279690] A.R. Booker and A.V. Sutherland, *On a question of Mordell*, Proc. Natl. Acad. Sci. **118** (2021), paper no. 2022377118, 11 pages.

[MR4280389] F. Fité, K.S. Kedlaya, and A.V. Sutherland, *Sato–Tate groups of abelian threefolds: a preview of the classification*, Arithmetic, Geometry, Cryptography, and Coding Theory, 103–129, Contemp. Math. **770** Amer. Math Soc., 2021.

[MR4235126] A.V. Sutherland, *Counting points on superelliptic curves in average polynomial time*, Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS XIV), 403–422, Open Book Ser. **4**, Math. Sci. Publ., 2020.

[MR4038255] E. Costa, F. Fité, and A.V. Sutherland, *Arithmetic invariants from Sato–Tate moments*, C. R. Math. Acad. Sci. Paris **357** (2019), 823–826.

[MR4033732] A.V. Sutherland, *Sato–Tate distributions*, Analytic methods in arithmetic geometry, 197–248, Contemp. Math. **740**, Amer. Math. Soc., 2019.

[MR3952027] A.V. Sutherland, *A database of nonhyperelliptic genus 3 curves over* $\mathbb{Q}$, Proceedings of the Thirteenth Algorithmic Number Theory Symposium (ANTS XIII), 443–459, Open Book Ser. **2**, Math. Sci. Publ., 2019.

[MR3952026] A.V. Sutherland, *Fast Jacobian arithmetic for hyperelliptic curves of genus 3*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium (ANTS XIII), 425–442, Open Book Ser. **2**, Math. Sci. Publ., 2019.

[MR3896855] J.F. Voloch and A.V. Sutherland, *Maps between curves and arithmetic obstructions*, Arithmetic geometry: computations and applications, 167–175, Contemp. Math. **722**, Amer. Math. Soc., 2019.

[MR3864839] F. Fité, E. Lorenzo García, and A.V. Sutherland, *Sato–Tate distributions of twists of the Fermat and the Klein quartics*, Res. Math. Sci. **5** (2018), 41:1–40.

[MR3716201] H.B. Daniels, A. Lozano-Robledo, F. Najman, and A.V. Sutherland, *Torsion subgroups of rational elliptic curves over the compositum of all cubic fields*, Math. Comp. **87** (2018), 425–458.

[MR3690609] M. Derickx and A.V. Sutherland, *Torsion subgroups of elliptic curves over quintic and sextic number fields*, Proc. Amer. Math. Soc. **145** (2017), 4233–4245.

[MR3671434] A.V. Sutherland and D. Zywina, *Modular curves of prime-power level with infinitely many rational points*, Algebra Number Theory **11** (2017), 1199–1299.

[MR3573417] I.E. Shparlinski and A.V. Sutherland, *Finding elliptic curves with a subgroup of prescribed size*, Int. J. Number Theory **13** (2017), 133–152.

[MR3540958] A.R. Booker, J. Sijsling, A.V. Sutherland, J. Voight, and D. Yasaki, *A database of genus 2 curves over the rational numbers*, LMS J. Comp. Math. **19A** (2016), 235–254.

[MR3540957] D. Harvey, M. Massierer, and A.V. Sutherland, *Computing L-series of geometrically hyperelliptic curves of genus three*, LMS J. Comp. Math. **19A** (2016), 220–234.

[MR3540942] K.S. Kedlaya and A.V. Sutherland, *A census of zeta functions of quartic K3 surfaces over* $\mathbb{F}_2$, LMS J. Comp. Math. **19A** (2016), 1–11.

[MR3502941] D. Harvey and A.V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions, Lang–Trotter and Sato–Tate conjectures, 127–147, Contemp. Math. **663**, Amer. Math. Soc., 2016.

[MR3502940] F. Fité and A.V. Sutherland, *Sato–Tate groups of $y^2=x^8+c$ and $y^2=x^7-cx$*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures, 103–126, Contemp. Math. **663**, Amer. Math. Soc., 2016.

[MR3502939] F. Fité, K.S. Kedlaya, and A.V. Sutherland, *Sato–Tate groups of some weight 3 motives*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures, 57–101, Contemp. Math. **663**, Amer. Math. Soc., 2016.

[MR3482279] A.V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), 4:1-79.

[MR3454371] A. Abatzoglou, A. Silverberg, A.V. Sutherland, and A. Wong, *A framework for deterministic primality proving using elliptic curves with complex multiplication*, Math. Comp. **85** (2016), 1461–1483.

[MR3435725] J.H. Bruinier, K. Ono, and A.V. Sutherland, *Class polynomials for nonholomorphic modular functions*, J. Number Theory **161** (2016), 204–229.

[MR3373710] D.H.J. Polymath, *Variants of the Selberg sieve and bounded intervals containing many primes*, Res. Math. Sci. **1** (2014), 12:1–83.

[MR3349320] I.E. Shparlinski and A.V. Sutherland, *On the distribution of Atkin and Elkies primes for reductions of elliptic curves on average*, LMS J. Comp. Math. **18** (2015), 308–322.

[MR3294387] W. Castryck, E. Fouvry, G. Harcos, E. Kowalski, P. Michel, P. Nelson, E. Paldi, J. Pintz, A.V. Sutherland, T. Tao, and X.-F. Xie, *New equidistribution estimates of Zhang type*, Algebra Number Theory **8** (2014), 2067–2199.

[MR3240808] D. Harvey and A.V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comp. Math. **17A** (2014), 257–273.

[MR3218802] F. Fité and A.V. Sutherland, *Sato–Tate distributions of twists of $y^2 = x^5 - x$ and $y^2 = x^6 + 1$*, Algebra Number Theory **8** (2014), 543–585.

[MR3179585] I.E. Shparlinski and A.V. Sutherland, *On the distribution of Atkin and Elkies primes*, Found. Comp. Math. **14** (2014), 285–297.

[MR3207430] A.V. Sutherland, *On the evaluation of modular polynomials*, Proceedings of the Tenth Algorithmic Number Theory Symposium (ANTS X), Open Book Ser. **1**, Math. Sci. Publ., 2013, 531–555.[1]

[MR3207429] A.V. Sutherland, *Isogeny volcanoes*, Proceedings of the Tenth Algorithmic Number Theory International Symposium (ANTS X), Open Book Ser. **1**, Math. Sci. Publ., 2013, 507–530.

[MR3207405] A. Abatzoglou, A. Silverberg, A.V. Sutherland, and A. Wong, *Deterministic elliptic curve primality proving for a special sequence of numbers*, Proceedings of the Tenth Algorithmic Number Theory Symposium (ANTS X), 1–20, Open Book Ser. **1**, Math. Sci. Publ., 2013.

[MR2988819] A.V. Sutherland, *Identifying supersingular elliptic curves*, LMS J. Comp. Math. **15** (2012), 317–325.

[MR2982436] F. Fité, K.S. Kedlaya, V. Rotger, and A.V. Sutherland, *Sato–Tate distributions and Galois endomorphism modules in genus 2*, Compos. Math. **148** (2012), 1390–1442.

[MR2970725] A.V. Sutherland, *Accelerating the CM method*, LMS J. Comp. Math. **15** (2012) 172–204.

[1] Awarded the Selfridge Prize.

[MR2946086] W. Castryck, A. Folsom, H. Hubrechts, and A.V. Sutherland, *The probability that the number of points on the Jacobian of a genus 2 curve is prime*, Proc. Lond. Math. Soc. **104** (2012), 1235–1270.

[MR2950703] A.V. Sutherland, *A local–global principle for rational isogenies of prime degree*, J. Théor. Nombres Bordeaux **24** (2012), 474–485.

[MR2890318] G. Bisson and A.V. Sutherland, *A low-memory algorithm for finding short product representations in finite groups*, Des. Codes Crypt. **63** (2012), 1–13.

[MR2869057] R. Bröker, K. Lauter, and A.V. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. **81** (2012), 1202–1231.

[MR2869053] A.V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), 1131–1147.

[MR2772473] G. Bisson and A.V. Sutherland, *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, J. Number Theory **113** (2011), 815–831.

[MR2728992] A.V. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. **80** (2011), 501–538.

[MR2728991] A.V. Sutherland, *Structure computation and discrete logarithms in finite abelian p-groups*, Math. Comp. **80** (2011), 477–500.

[MR2721418] A. Enge and A.V. Sutherland, *Class invariants by the CRT method*, Algorithmic Number Theory 9th International Symposium (ANTS IX), 142–156, Lecture Notes in Comput. Sci. **6197**, Springer, 2010.

[MR2670978] R. Bröker and A.V. Sutherland, *An explicit height bound for the classical modular polynomial*, Ramanujan J. **22** (2010), 293–313.

[MR2769066] J.E. Cremona and A.V. Sutherland, *On a theorem of Mestre and Schoof*, J. Théor. Nombres Bordeaux **22** (2010), 353–358.

[MR2555991] K.S. Kedlaya and A.V. Sutherland, *Hyperelliptic curves, L-polynomials, and random matrices*, Arithmetic, Geometry, Cryptography, and Coding Theory, 119–162, Contemp. Math. **487**, Amer. Math. Soc., 2009.

[MR2448717] A.V. Sutherland, *A generic approach to searching for Jacobians*, Math. Comp. **78** (2009), 485–507.

[MR2467855] K.S. Kedlaya and A.V. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic Number Theory 8th International Symposium (ANTS VIII), 312–326, Lecture Notes in Comput. Sci. **5011**, Springer, 2008.

[MR2717420] A.V. Sutherland, *Order computations in generic groups*, Ph.D. thesis, Massachusetts Institute of Technology, 2007.[2]

Research articles in preparation

W. Sawin and A.V. Sutherland, *Murmurations for elliptic curves ordered by height*, arXiv: 2504.12295.

A.R. Booker, J. Sijsling, A.V. Sutherland, J. Voight, and D. Yasaki, *Sato–Tate groups and automorphy for atypical abelian surfaces*, in preparation.

Y-H He, K-H Lee, T. Oliver, A. Pozdnyakov, and A.V. Sutherland, *Murmurations of L-functions*, in preparation.

[2] Awarded the George M. Sprowls Prize.

A.R. Booker and A.V. Sutherland, *L-functions from nothing*, in preparation.

A.R. Booker and A.V. Sutherland, *Genus* 2 *curves of small conductor*, in preparation.

A.V. Sutherland, *Counting points on modular curves*, in preparation.

A.V. Sutherland, *A database of modular curves*, in preparation.

Letters and Expository Publications

A.V. Sutherland, *Letter to Michael Rubinstein and Peter Sarnak*, August, 2022.

A.V. Sutherland, *Pset Partners*, Notices Amer. Math. Soc. **68** (2021), 1919–1923.

J.E. Cremona, J.W. Jones, A.V. Sutherland, and J. Voight, *The L-functions and modular forms database*, Notices Amer. Math. Soc. **68** (2021), 1520–1522.

[MR4436914] E. Costa, D. Roe, and A. Sutherland, *Research seminars: A new hope*, Math in the time of Corona, Mathematics Online First Collections, Springer, 2021.

Educational Publications

Number Theory I (18.785), MIT OpenCourseWare, 2013, 2015, 2017, 2019, 2021.

Elliptic Curves (18.783), MIT OpenCourseWare, 2013, 2015, 2017, 2019, 2021, 2023, 2025.

Introduction to Arithmetic Geometry (18.782), MIT OpenCourseWare, 2013.

Online Databases

Modular curves (with D. Roe), `www.lmfdb.org`, 2022.

Classical modular forms (with A. Best, J. Bober, A.R. Booker, E. Costa, J.E. Cremona, M. Derickx, D. Lowry-Duda, M. Lee, D. Roe, and J. Voight), `www.lmfdb.org`, 2019.

Genus 3 curves over $\mathbb{Q}$, `genus3curves`, 2017.

Elliptic curves to conductor 500,000 (with J.E. Cremona), `www.lmfdb.org`, 2019.

Galois representations of elliptic curves over $\mathbb{Q}$, `www.lmfdb.org`, 2016.

Galois representations of elliptic curves over number fields, `www.lmfdb.org`, 2016.

Genus 2 curves over $\mathbb{Q}$ (with A.R. Booker, J. Sijsling, J. Voight, and D. Yasaki), `www.lmfdb.org`, 2016.

Sato–Tate groups, `www.lmfdb.org` (with F. Fité, K.S. Kedlaya, and V. Rotger and also with F. Fité, K.S. Kedlaya) 2015, 2020.

Narrow admissible tuples (with D.H.J. Polymath), `primegaps`, 2013.

Partition class polynomials (with J. Bruinier and K. Ono), `PartitionPolys`, 2013.

Classical modular polynomials (with R. Bröker and K. Lauter, and also with J. Bruinier and K. Ono), `ClassicalModPolys`, 2010, 2013.

Elliptic curve point counting records, `SEArecords`, 2010.

CM elliptic curve records, `CMrecords`, 2010.

Weber modular polynomials (with W. Bröker and K. Lauter), `WeberModPolys`, 2010.

Optimized equations for $X_1(N)$, `X1_optcurves`, 2008.

Trace zero varieties, `TraceZeroVarieties`, 2008.

Pairing friendly curves, `EdwardsE6`, 2008.

Software

`lmfdb-mcp`, LMFDB MCP server, 2026.

`erdos-guy-selfridge`, software to prove upper and lower bounds on decompositions of factorials into large factors (with B. Alexeev, E. Conway, A.V. Sutherland, M. Rosenfeld, T. Tao, M. Uhr, and K. Ventullo), 2025.

`funsearch`, high performance program search using LLMs (with J.S. Ellenberg, C.S. Fraser-Taliente, T.R. Harvey, K. Srivastava), 2025.

`CompletelyDecomposableModularJacobians`, Magma package to search for completely decomposable modular Jacobians (with J. Paulhus), 2025.

`Genus2Euler`, Magma package to compute Euler factors of genus 2 curves over $\mathbb{Q}$ at primes of almost good reduction (with C. Maistret), 2024.

`EndECNF`, program to compute the endomorphism ring of an elliptic curve over a number field (with J.E. Cremona). 2023. Incorporated into Pari/GP and SageMath, 2023.

`ell-adic-galois-images`, Magma package to compute ℓ-adic Galois images of elliptic curves over $\mathbb{Q}$ (with J. Rouse and D. Zureick-Brown), 2021.

`zcubes`, program to efficiently search for integer solutions to $x^3 + y^3 + z^3 = k$ (with A.R. Booker), 2019.

`galrep`, Magma package to compute mod-ℓ images of Galois representations of elliptic curves over number fields, 2015.

`classpoly`, program to compute defining polynomials for ring class fields; portions of this code have now been incorporated into Pari/GP, 2008–2015.

`smoothrelation`, program to compute endomorphism rings of elliptic curves over finite fields (with G. Bisson), 2010–2011.

`smalljac`, library for computing zeta functions and L-functions of low genus curves over finite fields and number fields (with K.S. Kedlaya), 2008–present.

`ffpoly`, library for fast arithmetic over finite fields, 2008–present.

Patents

United States Patent US-8874451-B2, "Personal mail piece and electronic mail tracking system," J.R. Smith, P.M. Yarin, M.J. Murphy, A.V. Sutherland, E. Metois, 2014.

United States Patent US-7069295-B2, "Peer-to-peer enterprise storage," A. Sutherland, M.R. Klugerman, D. O'Neill, S. Ludmann, E. Zukovsky, 2006.

United States Patents US-6609117-B2 and US-6349292-B1, "System and method for distributing postage over a public network, enabling efficient printing of postal indicia on items to be mailed and authenticating the printed indicia," A.V. Sutherland, M.R. Klugerman, F.M. D'Ippolito, 2002 and 2003.

United States Patents US-8527284-B2, US-10304026-B2, US-11475392-B2, "System for personal mail piece tracking and tracing from multiple sources by user identifier," Joshua R. Smith, Michael J. Murphy, Andrew V. Sutherland, Eric Metois, 2002, 2019, 2022.

United States Patent US-D450759-S, "Postal indicia for an envelope," William Crosby, Michael J. Murphy, Joshua R. Smith, Andrew Sutherland, 2001.

United States Patent US-D401920-S, "Computer video display terminal screen with wallpaper and icon," Michael J. Murphy, Andrew V. Sutherland, 1998.