

Andrew V. Sutherland

Curriculum Vitae

(Last updated January 2022)

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 (2012–) Principal Research Scientist. (2009–2011) Research Scientist. (2007–2009) Research Affiliate. Escher Group Ltd. (1993–2003) Founder and Chief Technology Officer.
EDITORIAL AND BOARD POSITIONS	President, The Number Theory Foundation, 2019–present. Steering Committee, Algorithmic Number Theory Symposia, 2019–present. Advisory Board, Sagemath Inc., 2018–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	Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation, Simons Foundation grant 550033, 2017-2024. 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	Fourteenth Algorithmic Number Theory Symposium (ANTS XIV), University of Auckland, New Zealand, July 2020 (program committee).
	Arithmetic Geometry, Number Theory, and Computation, ICERM, June 2020.
	AMS Special Session on Rational Points on Algebraic Varieties: Theory and Computation, Joint Mathematics Meetings, Denver, January 2020.
	AMS Special Session on Number Theory, Arithmetic Geometry, and Computation, Joint Mathematics Meetings, Baltimore, January 2019.
	Arithmetic of Low-Dimension Abelian Varieties, ICERM, Providence, June 2019.
	Arithmetic Geometry, Number Theory, and Computation, MIT, August 2018.
	Fifteenth Workshop on Elliptic Curve Cryptography (ECC 2011), Loria, France, September 2011 (program committee).
POSTDOCTORAL RESEARCHERS SUPERVISED (AT MIT)	Shiva Chidambaram, Research Scientist, 2021–present.
	Wanlin Li, Research Scientist, 2019–2022.
	Sam Schiavone, Research Scientist, 2019–present.
	Raymond van Bommel, Research Scientist, 2019–present.
	Francesc Fité, Research Scientist, 2019–2021.
	Dohyeong Kim, Research Scientist, 2018–2019.
	Maarten Derickx, Research Scientist, 2018–2019.
	Edgar Costa, Research Scientist, 2018–present.
	David Roe, Research Scientist, 2018–present.
SERVICE (AT MIT)	AMS David P. Robbins Prize Committee, chair, 2021–present.
	IT Oversight Committee, chair, 2021–present
	Pset Partners, administrator, 2020–present.
	Research Seminars, administrator, 2020–present.
	VaNTAGe Seminar, co-organizer, 2020–present.
	Number Theory Seminar, co-organizer, 2020–present.
	Diversity and Community Building Committee, 2020–present.
	Mathematics Major Advisor, 2019–present.
	BC-MIT Number Theory Seminar Co-organizer, 2018–present.
	Undergraduate Research Opportunity Supervisor (UROP), 2010–present.
	OpenCourseWare Contributor, 2013–present.
	Independent Activities Period Lecture Series, 2014–2017.
	Freshman Advisor, 2009–2011.
	Educational Studies Program (Splash and HSSP), 2006–2008

Abelian surfaces and their L-functions, Simons Foundation (online), 2022.

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

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

Sato-Tate groups of abelian threefolds, Joint Mathematics Meetings, online, 2020.

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

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.

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

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

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).

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, Boston, 2013 (colloquium).

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.

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

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.

[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.

[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), no. 11.

[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, Contemp. Math. **770** (2021), 103–129.

[MR4235126] A.V. Sutherland, *Counting points on superelliptic curves in average polynomial time*, Proceedings of the Fourteenth Algorithmic Number Theory Symposium, 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, 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, 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. Shparlinksi 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. One, and A.V. Sutherland, *Class polynomials for nonholomorphic modular functions*, J. Number Theory **161** (2016), 204–229.
- [MR3349320] I.E. Shparlinksi 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.
- [MR3373710] D.H.J. Polymath, *Variants of the Selberg sieve and bounded intervals containing many primes*, Res. Math. Sci. **1** (2014), 12:1–83.
- [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, 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, 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, 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.
- [MR2950703] A.V. Sutherland, *A local–global principle for rational isogenies of prime degree*, J. Théor. Nombres Bordeaux **24** (2012), 474–485.
- [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.
- [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.
- [MR2769066] J.E. Cremona and A.V. Sutherland, *On a theorem of Mestre and Schoof*, J. Théor. Nombres Bordeaux **22** (2010), 353–358.
- [MR2721418] A. Enge and A.V. Sutherland, *Class invariants by the CRT method*, Algorithmic Number Theory 9th International Symposium, 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.

¹Awarded the Selfridge Prize.

[MR2555991]	K.S. Kedlaya and A.V. Sutherland, <i>Hyperelliptic curves, L-polynomials, and random matrices</i> , Arithmetic, Geometry, Cryptography, and Coding Theory, 119–162, Contemp. Math. 487 , Amer. Math. Soc., 2009.
[MR2448717]	A.V. Sutherland, <i>A generic approach to searching for Jacobians</i> , Math. Comp. 78 (2009), 485–507.
[MR2467855]	K.S. Kedlaya and A.V. Sutherland, <i>Computing L-series of hyperelliptic curves</i> , Algorithmic Number Theory 8th International Symposium, 312–326, Lecture Notes in Comput. Sci. 5011 , Springer, 2008.
[MR2717420]	A.V. Sutherland, <i>Order computations in generic groups</i> , Ph.D. thesis, Massachusetts Institute of Technology, 2007. ²
SUBMITTED RESEARCH ARTICLES	J. Rouse, D. Zureick-Brown, and A.V. Sutherland, <i>ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$</i> , with an appendix by J. Voight, arXiv:2106.11141. F. Fité, K.S. Kedlaya, and A.V. Sutherland, <i>Sato–Tate groups of abelian threefolds</i> , arXiv:2106.13759.
EDUCATIONAL PUBLICATIONS	Elliptic Curves (18.783), MIT OpenCourseWare, 2013, 2015, 2017, 2019, 2021. Number Theory I (18.785), MIT OpenCourseWare, 2013, 2015, 2017, 2019. Introduction to Arithmetic Geometry (18.782), MIT OpenCourseWare, 2013.
ONLINE DATABASES (CLICK URL TO ACCESS)	Classical Modular Forms (with Best, Bober, Booker, Costa, Cremona, Derickx, Lowry-Duda, Lee, Roe, Voight), www.lmfdb.org , 2019. Genus 3 curves over $\mathbb{Q}$, math.mit.edu , 2017. Elliptic curves to conductor 500,000 (with Cremona), www.lmfdb.org , 2019. Galois representations of elliptic curves, www.lmfdb.org , 2016. Genus 2 curves over $\mathbb{Q}$ (with Booker, Sijsling, Voight, Yasaki), www.lmfdb.org , 2016. Sato–Tate groups, www.lmfdb.org (with Fité, Kedlaya, Rotger), 2015, 2020. Narrow admissible tuples (with D.H.J. Polymath), math.mit.edu , 2013. Partition class polynomials (with Bruiner and Ono), math.mit.edu , 2013. Classical modular polynomials (with Bröker, Lauter, and also with Bruinier, Ono), math.mit.edu , 2010, 2013. Weber modular polynomials (with Bröker and Lauter), math.mit.edu , 2010. Optimized equations for $X_1(N)$, math.mit.edu , 2008. Pairing friendly curves, math.mit.edu , 2008.
SOFTWARE	ell-adic-galois-images , magma package to compute ell-adic Galois images of elliptic curves (with Rouse and Zureick-Brown), 2021. classpoly , program to compute defining polynomials for ring class fields (portions of this code have now been incorporated into PARI/GP), 2008–2015.

²Awarded the George M. Sprowls prize.

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

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

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

PATENTS

United States Patent **7069295**, “Peer-to-peer enterprise storage,” Andrew Sutherland, Michael Klugerman, Donal O’Neill, Sandor Ludmann, Eli Zukovsky, 2006.

United States Patents **6609117** and **6349292**, “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,” Andrew V. Sutherland, Michael R. Klugerman, Frank M. D’Ippolito, 2002 and 2003.

United States Patent **8527284**, “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

United States Patent **D450759**, “Postal indicia for an envelope,” William Crosby, Michael J. Murphy, Joshua R. Smith, Andrew Sutherland, 2001.

United States Patent **D401920**, “Computer video display terminal screen with wallpaper and icon,” Michael J. Murphy, Andrew V. Sutherland, 1998.