CURRICULUM VITAE

Joseph H. Silverman

Contact Information

Department of Mathematics
Brown University
Providence, RI 02912
Voice: [401] 863-1124, Fax: [401] 863-9471
Email: `jhs@math.brown.edu`
Home Page: `www.math.brown.edu/~jhs`

Fields of Interest: Number theory, arithmetic geometry, elliptic curves, dynamical systems, cryptography

Academic Employment History

Professor of Mathematics
Brown University, 1991–present [Chair 2001–04, 2008; Assoc. Chair 2019]
Royce Family Professor of Teaching Excellence, 2014–17

Associate Professor of Mathematics
Brown University, 1988–1991

Associate Professor of Mathematics
Boston University, 1986–1988

NSF Postdoctoral Fellow and C.L.E. Moore Instructor of Mathematics
Massachusetts Institute of Technology, 1982–86

Education

Harvard University Ph.D. 1982
Brown University Sc.B. 1977

Doctoral Thesis

The Néron-Tate Height on Elliptic Curves
Advisor: Professor John Tate

Fellowships, Grants, Awards

Simons Collaboration Grant for Mathematicians, 2012–2017
NSF Research Grants, 1986–1998, 1999–2003, 2006–2015, 2016-2018
Fellow of the American Mathematical Society, elected 2012
ECC Visionary Award, 2011
NES MAA Award for Distinguished Teaching, 2011
NSA Research Grant, 2003–2006
Guggenheim Foundation Fellowship, 1998–1999
AMS Steele Prize for Mathematical Exposition, 1998
Brown University Award for Excellence in Teaching, 1996
MAA Lester Ford Award, 1994
Sloan Foundation Fellowship, 1987–1991

Service

AMS Board of Trustees, 2015–2025
ICERM Scientific Advisory Board, 2018–2021
AMS Fellows Selection Committee, 2013
AMS Council, 2008–2013; AMS Executive Committee 2009–2013
AMS Graduate Working Group (chair), 2011-2013
Editorial Committee of AMS Pure and Applied Undergraduate Texts, 2009–2015
Editorial Board, *Algebra and Number Theory*, 2011–
Advisory Board, *Acta Arithmetica*, 2011–
Claude Shannon Institute, Dublin, Advisory Board, 2006–2012
Editorial Board, *New York Journal of Mathematics*, 2008–
Editorial Board, *Compositio Mathematica*, 1993–2005
Reviewer for *Mathematical Reviews*, 1983– (340+ reviews written)
NSF Institute for Pure and Applied Math. (IPAM UCLA)
Board of Trustees, 2003–2005
AMS Conant Prize Selection Committee, 2000–2003
Referee for many journals and for NSF, NSA, NSERC

Selected Recent Invited Addresses

MAGNTS: Midwest Arithmetic Geometry and Number Theory Series
Ohio State University, Oct 12-13, 2019
MRC on Explicit Methods in Arithmetic Geometry in Characteristic p
Warwick, RI, June 17-18, 2019
Arithmetic of Low-Dimensional Abelian Varieties
ICERM, Providence, June 3–7, 2019
Simons Symposium on Algebraic, Complex, and Arithmetic Dynamics
Kuln, Germany, May 19–25, 2019
Dynamical Systems Seminar
University of Rhode Island, April 5, 2019
Hawaii Number Theory Conference 2019 (HINT) (Mon-Thurs)
AMS Sectional Meeting in Hawaii (Fri-Sun)
University of Hawaii, March 18 - 24, 2019 (Mon-Sun)
Simons Collaboration Conference on Arithemtic Geometry
New York City, January 9–11, 2019.

Publications – Joseph H. Silverman

BOOKS

[1] *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer-Verlag, N.Y., 1986; 2nd edition 2009.

[2] with J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Math., Springer–Verlag, N.Y., 1992; 2nd expanded edition 2015.

[3] *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math. **151**, Springer-Verlag, N.Y., 1994.

[4] *A Friendly Introduction to Number Theory*, Prentice-Hall, N.J., 1997; 2nd edition 2001; 3rd edition 2006; 4th edition 2012.

[5] with M. Hindry, *Diophantine Geometry: An Introduction*, Graduate Texts in Math. **201**, Springer-Verlag, New York, 2000.

[6] *The Arithmetic of Dynamical Systems*, Graduate Texts in Math. **241**, Springer-Verlag, N.Y., 2007.

[7] with Jill Pipher and Jeffrey Hoffstein, *An Introduction to Mathematical Cryptography*, Undergraduate Texts in Mathematics, Springer–Verlag, 2008; 2nd edition 2014.

[8] *Moduli Spaces and Arithmetic Dynamics*, (CRM Monograph Series, Vol. 30) American Mathematical Society, 2012.

EDITOR OF CONFERENCE PROCEEDINGS

[1] co-editor with G. Cornell, *Arithmetic Geometry,* a conference held at Storrs, Connecticut, 1984, Springer-Verlag, N.Y., 1986.

[2] co-editor with G. Cornell and G. Stevens, *Modular Forms and Fermat's Last Theorem*, a conference held at Boston University, 1995, Springer-Verlag, N.Y., 1997.

[3] editor of *Cryptography and Lattices Conference* (CaLC 2001), Lecture Notes in Computer Science 2461, Springer-Verlag, 2001.

ARTICLES

[1] Mean and variance for covering sets of congruences, *Math. Mag.* **51** (1978), 120–122

[2] Lower bound for the canonical height on elliptic curves, *Duke Math. J.* **48** (1981), 633–648

[3] The cubic Thue equation, *Number Theory Related to Fermat's Last Theorem,* ed. by N. Koblitz, Prog. in Math., Birkhauser, 1981, 263–267

[4] The Catalan equation over function fields, *Trans. Amer. Math. Soc.* **273** (1982), 201–205

[5] Integer points and the rank of Thue elliptic curves, *Invent. Math.* **66** (1982), 395–404

[6] Heights and the specialization map for families of abelian varieties, *J. Reine Angew. Math.* **342** (1983), 197–211

[7] The Néron fiber of abelian varieties with potential good reduction, *Math. Ann.* **264** (1983), 1–3

[8] Integer points on curves of genus 1, *J. London Math. Soc.* **28** (1983), 1–7

[9] Representations of integers by binary forms and the rank of the Mordell-Weil group, *Invent. Math.* **74** (1983), 281–292

[10] The Thue equation and height functions, *Approx. Dioph. et Nomb. Transc.,* ed. by D. Bertrand et M. Waldschmidt, Prog. in Math., Birkhauser, 1983, 259–270

[11] The S-unit equation over function fields, *Proc. Camb. Philos. Soc.* **95** (1984), 3–4

[12] Lower bounds for height functions, *Duke Math. J.* **51** (1984), 395–403

[13] Divisibility of the specialization map for families of elliptic curves, *Amer. J. Math.* **107** (1985), 555–565

[14] An inequality relating the regulator and the discriminant of a number field, *J. Number Theory* **19** (1984), 437–442

[15] Weierstrass equations and the minimal discriminant of an elliptic curve, *Mathematika* **31** (1984), 245–251

[16] Integral points on abelian varieties, *Invent. Math.* **81** (1985), 341–346

[17] with J.-H. Evertse, Uniform bounds for the number of solutions to $Y^n = f(X)$, *Proc. Camb. Philos. Soc.* **100** (1986), 237-248

[18] Points of finite order on elliptic curves, *Amer. Math. Monthly* **93** (1986), 793–795

[19] The theory of height functions, *Arithmetic Geometry,* ed. by G. Cornell and J. Silverman, Springer-Verlag, N.Y., 1986, 151-166

[20] Heights and elliptic curves, *Arithmetic Geometry,* ed. by G. Cornell and J. Silverman, Springer-Verlag, N.Y., 1986, 253–266

[21] Arithmetic distance functions and height functions in Diophantine geometry, *Math. Ann.* **279** (1987), 193–216

[22] A survey of the theory of height functions, *Current Trends in Arithmetical Geometry,* ed. by K. Ribet, Contemp. Math. **67**, Amer. Math. Soc., 1987, 269–278

[23] Integral points on abelian varieties are widely spaced, *Compos. Math.* **61** (1987), 253-266

[24] A quantitative version of Siegel's theorem: Integral points on elliptic curves and Catalan curves, *J. Reine Angew. Math.* **378** (1987), 60–100

[25] Rational points on certain families of curves of genus at least two, *Proc. London Math. Soc.* **55** (1987), 465–481

[26] Integral points on curves and surfaces, Proc. 15th Journées Arithmétiques, Ulm, 1987, *Lect. Notes in Math.* **1380** (1989), 202–241

[27] Computing heights on elliptic curves, *Math. Comp.* **51** (1988), 339–358

[28] with M. Hindry, The canonical height and integral points on elliptic curves, *Invent. Math.* **93** (1988), 419–450

[29] Wieferich's criterion and the *abc*-conjecture, *J. Number Theory* **30** (1988), 226–237

[30] Recent (and not so recent) developments in the arithmetic theory of elliptic curves, *Nieuw Archief voor Wiskunde* **7** (1989), 53–70

[31] Elliptic curves of bounded degree and height, *Proc. Amer. Math. Soc.* **105** (1989), 540–545

[32] A review of *Introduction to Arakelov Theory* by Serge Lang, *Bul. Amer. Math. Soc.* **21** (1989), 171–176

[33] Hecke points on modular curves, *Duke Math. J.* **60** (1990), 401–423

[34] Rational points on symmetric products of a curve, *Am. J. Math.* **113** (1991), 471–508

[35] The Markoff equation $X^2+Y^2+Z^2=aXYZ$ over quadratic imaginary fields, *J. Number Theory* **35** (1990), 72–104

[36] The difference between the Weil height and the canonical height on elliptic curves, *Math. Comp.* **192** (1990), 723–743

[37] with M. Hindry, On Lehmer's conjecture for elliptic curves, Sém. Th. Nombres Paris 1988–1989, *Prog. in Math.* **91** (1990), 103–116

[38] with J. Harris, Bi-elliptic curves and symmetric products, *Proc. AMS* **112** (1991), 347–356

[39] Some arithmetic properties of Weierstrass points: Hyperelliptic curves, *Bol. Soc. Bras. Mat.* **21** (1990), 11–50

[40] with J.F. Voloch, Multiple Weierstrass points, *Compos. Math.* **79** (1991), 123–134

[41] Rational points on K3 surfaces: A new canonical height, *Invent. Math.* **105** (1991), 347–373

[42] A uniform bound for rational points on twists of a given curve, *J. Lond. Math. Soc.* **47** (1993), 385–394

[43] Variation of the canonical height on elliptic surfaces I: Three examples, *J. Reine Angew. Math.* **426** (1992), 151–178

[44] Variation of the canonical height on elliptic surfaces II: Local analyticity properties, *J. Number Theory* **48** (1994), 291–329

[45] Variation of the canonical height on elliptic surfaces III: Global boundedness properties, *J. Number Theory* **48** (1994), 330–352

[46] Variation of the canonical height in algebraic families, *Contemp. Math.* (B. Mazur and G. Stevens, eds.) **165** (1994), 123–133

[47] Taxicabs and sums of two cubes: An excursion in number theory, *Am. Math. Monthly* **100** (1993), 331–340 (MAA Ford award)

[48] with P. Lockhart and M. Rosen, An upper bound for the conductor of an abelian variety, *J. Algebraic Geometry* **2** (1993), 569–601

[49] Counting integral and rational points on varieties, Columbia University Number Theory Seminar, New York, 1992, *Asterisque* **228** (1995), 223–236

[50] with G. Call, Canonical heights on varieties with morphisms, *Compos. Math.* **89** (1993), 163–205

[51] Integer points, Diophantine approximation, and iteration of rational maps, *Duke Math. J.* **71** (1993), 793–829

[52] Geometric and arithemtic properties of the Hénon map, *Math. Zeit.* **215** (1994), 237–250

[53] with P. Morton, Periodic points, multiplicities, and dynamical units, *J. Reine Angew. Math.* **461** (1995), 81–122

[54] with P. Morton, Rational periodic points of rational functions, *Inter. Math. Research Notices* **2** (1994), 97–110

[55] On the field of definition for dynamical systems on $\mathbf{P}^1$, *Compos. Math.* **98** (1995), 269–304

[56] with G. Call, Computing the canonical height on K3 surfaces, *Math. Comp.* **65** (1996), 259–290

[57] with R. Gross, S-integer points on elliptic curves, *Pacific J. Math.* **167** (1995), 263–288

[58] with M. Rosen, R. Murty, Variations on a theme of Romanoff, *Inter. J. Math.* **7** (1996), 373–391

[59] Small Salem numbers, exceptional units, and Lehmer's conjecture, *Rocky Mountain J. Math.* **26** (1996), 1099–1114

[60] Exceptional units and small Salem numbers, *Experimental Mathematics* **4** (1995), 69–83

[61] Rational functions with a polynomial iterate, *J. Algebra* **180** (1996), 102–110

[62] Computing canonical heights with little (or no) factorization, *Math. Comp.* **66** (1997), 787–805

[63] with A. Brumer, The number of elliptic curves over $\mathbf{Q}$ with conductor N, *Manuscripta Math.* **91** (1996), 95–102

[64] Computing rational points on rank 1 elliptic curves via L-series and canonical heights, *Math Comp.* **68** (1999), 835–858

[65] Divisibility of the specialization map for twists of abelian varieties, *Topics in number theory (University Park, PA, 1997)*, Math. Appl., 467, Kluwer Acad. Publ., Dordrecht, 1999, 245–258.

[66] A survey of the arithmetic theory of elliptic curves, *Modular Forms and Fermat's Last Theorem*, ed. by G. Cornell, J. Silverman, and G. Stevens, Springer-Verlag, N.Y., 1997, 17–40

[67] The space of rational maps on $\mathbf{P}^1$, *Duke Math. J.* **94** (1998), 41–77

[68] with M. Rosen, On the rank of an elliptic surface, *Invent. Math.* **133** (1998), 43–67

[69] The average rank of an algebraic family of elliptic curves, *J. Reine Angew. Math.* **504** (1998), 227–236

[70] with A. Bremner and N. Tzanakis, Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$, *Journal of Number Theory* **80** (2000), 187–208

[71] A bound for the Mordell-Weil rank of an elliptic surface after a cyclic base extension, *Journal of Algebraic Geometry* **9** (2000), 301–308

[72] On the distribution of integer points on curves of genus zero, *Theoretical Computer Science* **235** (2000), 163–170

[73] with J. Suzuki, Elliptic curve discrete logarithms and the index calculus, *Advances in Cryptology—ASIACRYPT'98*, Beijing, October 1998, ed. by K. Ohta and D. Pei, Lecture Notes in Computer Science 1514, Springer-Verlag, Berlin, 1998, 110–125

[74] *with Jeffrey Hoffstein, Jill Pipher, NTRU: A Ring Based Public Key Cryptosystem, in Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998, 267–288.

[75] The xedni calculus and the elliptic curve discrete logarithm problem, *Design, Codes and Cryptography* **20** (2000), 5–40

[76] with M. Jacobson, N. Koblitz, A. Stein, and E. Teske, Analysis of the xedni calculus attack, *Design, Codes and Cryptography* **20** (2000), 41–64

[77] with M. Hindry, Sur le nombre de points de torsion rationnels sur une courbe elliptique, *C.R. Acad. Sci. Paris* **329** (1999), 97–100

[78] *with Jeffrey Hoffstein, Daniel Lieman, Polynomial Rings and Efficient Public Key Authentication, in Proceeding of the International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99), M. Blum and C.H. Lee, eds., City University of Hong Kong Press.

[79] *Fast Multiplication in Finite Fields GF(2^N), in Workshop on Cryptographic Hardware and Embedded Systems (CHES '99) C.K. Koc and C. Paar, eds., LNCS, Springer-Verlag, 1999.

[80] *with J. Hoffstein, Polynomial rings and efficient public key authentication II, in Proceedings of a Conference on Cryptography and Number Theory (CCNT '99), I. Shparlinski et.al., eds., Lecture Notes in Computer Science, Springer-Verlag, 269–286.

[81] Rings of low multiplicative complexity, *Finite Fields and Their Applications* **6** (2000), 175–191

[82] *with Jeffrey Hoffstein, MiniPASS: Authentication and digital signatures in a constrained environment, in Workshop on Cryptographic Hardware and Embedded Systems (CHES 2000) C.K. Koc and C. Paar, eds., LNCS, Springer-Verlag, 2000.

[83] with I.E. Shparlinski, Linear complexity of the Naor–Reingold pseudo-random function from elliptic curves, *Designs, Codes and Cryptography* **24** (2001), 279–289.

[84] with A. May, Dimension reduction methods for convolution modular lattices, *Cryptography and Lattices Conference* (CaLC 2001), Lecture Notes in Computer Science 2461, Springer-Verlag, 2001, 110–125.

[85] *with Jeffrey Hoffstein, Optimizations for NTRU, Public Key Cryptography

and Computational Number Theory (Warsaw, Sept. 11–15, 2000), Walter de Gruyter, Berlin–New York, 2001, 77–88.

[86] *with Jeffrey Hoffstein, Jill Pipher, NSS: An NTRU lattice-based signature scheme, Advances in Cryptology–Eurocrypt 2001, Lecture Notes in Computer Science, Springer-Verlag.

[87] The rank of elliptic surfaces in unramified abelian towers, *J. Reine Angew. Math.*, **577** (2004), 153–169.

[88] A lower bound for the canonical height on elliptic curves over abelian extensions, *Journal of Number Theory* **104** (2004), 353–372

[89] with Matthew Baker, A lower bound for the canonical height on abelian varieties over abelian extensions, *Mathematical Research Letters* **11** (2004), 377–396.

[90] *Lattices, cryptography, and the NTRU public key cryptosystem, *Unusual Applications of Number Theory*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **64** (2004), 183–198.

[91] *with N. Howgrave-Graham, P. Nguyen, D. Pointcheval, J. Proos, A. Singer, W. Whyte, The impact of decryption failure on the security of NTRU encryption, *Advances in Cryptology — CRYPTO 2003*, Lecture Notes in Computer Science 2729, Springer-Verlag, 2003.

[92] *with J. Hoffstein, Random small Hamming weight products with applications to cryptography, Com2MaC Workshop on Cryptography (Pohang, Korea, June 2000), Discrete Applied Mathematics 130 (2003), 37–49.

[93] *with J. Hoffstein, N. Howgrave-Graham, J. Pipher, W. Whyte, NTRUSign: Digital Signatures Using the NTRU Lattice, *Topics in Cryptology – CT-RSA 2003*, San Francisco, February 2003, ed. by M. Joye, Lecture Notes in Computer Science 2612, Springer-Verlag, Berlin, 2003, 122–140.

[94] Common divisors of $a^n - 1$ and $b^n - 1$ over function fields, *New York Journal of Math.* (electronic) **10** (2004), 37–43

[95] Common divisors of elliptic divisibility sequences over function fields, *Manuscripta Mathematica* **114** (2004), 432–446

[96] p-adic properties of division polynomials and elliptic divisibility sequences, *Mathematische Annalen* **332**(2) (2005), 443–471 (addendum 473–474).

[97] *with N. Smart and F. Vercauteren, An algebraic approach to NTRU via Witt vectors and overdetermined systems of nonlinear equations, Security in Communication Networks: 4th International Conference, SCN 2004, Amalfi, Italy, September 8–10, 2004, Lecture Notes in Computer Science 3352, 2005, Springer-Verlag, 278–293.

[98] *with N. Howgrave-Graham, W. Whyte, Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3, *Topics in Cryptology – CT-RSA 2005*, San Francisco, February 2005, ed. by A.J. Menezes, Lecture Notes in Computer Science 3376, Springer-Verlag, Berlin, 2005, 118–135.

[99] Generalized greatest common divisors, divisibility sequences, and Vojta's con-

jecture on blowups, *Monatsch. Math.* **145** (2005), 333–350

[100] Elliptic curves and cryptography, in *Public-Key Cryptography*, P. Garrett and D. Lieman, eds., Proceedings of Symposia in Applied Mathematics **62**, 2005, American Mathematical Society, 91–112.

[101] Height bounds and preperiodic points for families of jointly regular affine maps, *Quart. J. Pure Appl. Math.* **2** (2006), 135–145

[102] with K. Bentahar, D. Page, M.-J. O. Saarinen and N.P. Smart, LASH, presented and published online at NIST: The Second Cryptographic Hash Workshop, 2006.
`csrc.nist.gov/groups/ST/hash/documents/SAARINEN_lash4-1_ORIG.pdf`

[103] with N. Stephens, The sign of an elliptic divisibility sequence, *Journal of the Ramanujan Math. Soc.* **21** (2006), 1–17.

[104] Greatest common divisors and algebraic geometry, Proceedings of a Workshop on Diophantine Geometry, Centro di Ricerca Matematica Ennio De Giorgi, Pisa, Italy, June 2005.

[105] *with J. Hoffstein, N. Howgrave-Graham, J. Pipher, W. Whyte, Performance improvements and a baseline parameter generation algorithm for NTRUSign, presented at a Workshop on Mathematical Problems and Techniques in Cryptology, Barcelona, Spain, June 2005, and published online at
`http://eprint.iacr.org/2005/274`.

[106] Divisibility Sequences and Powers of Algebraic Integers, *Documenta Math.* (electronic) Extra Volume: John H. Coates' Sixtieth Birthday (2006), 711–727

[107] with M. Rosen, On the independence of Heegner points associated to distinct quadratic imaginary fields, *Journal of Number Theory* 127 (2007), 10–36.

[108] with S. Kawaguchi, Dynamics of projective morphisms having identical canonical heights, *Proc. London Math. Soc.* **95** (2007), 519–544.

[109] with S. Kawaguchi, Canonical heights and the arithmetic complexity of morphisms on projective space, *Pure and Applied Mathematics Quarterly* **5** (2009), 1201–1217.

[110] with S. Kawaguchi, Nonarchimedian Green functions and dynamics on projective space, *Math. Zeit.* **262** (2009), 173–197.

[111] *with W. Whyte, Timing attacks on NTRUEncrypt based on variation in number of hash calls, CT-RSA 2007, Lecture Notes in Computer Science, Springer-Verlag.

[112] with Patrick Ingram, Uniform estimates for primitive divisors in elliptic divisibility sequences, Number theory, Analysis and Geometry (In memory of Serge Lang), Springer–Verlag, 2010, 233–263.

[113] Variation of periods modulo p in arithmetic dynamics, *New York Journal of Math.* **14** (2008), 601–616 (electronic).

[114] Elliptic curves. A new chapter for the sixth edition of *An Introduction to the Theory of Numbers* by G.H. Hardy and E.M. Wright, Oxford University Press, 2008.

[115] with Patrick Ingram, Primitive divisors in arithmetic dynamics, *Proc. Camb. Philos. Soc.* (2009), 146, #2, 289–302.

[116] with Liang-Chung Hsia, On a dynamical Brauer–Manin obstruction, Proceedings of the Journees Arithmetiques 2007, J. Théor. Nombres Bordeaux **21** (2009), 235–250.

[117] with José Felipe Voloch, A Local-Global Criterion for Dynamics on $\mathbf{P}^1$, *Acta Arithmetica* 137.3 (2009), 285–294.

[118] Lifting and elliptic curve discrete logarithms, Selected Areas of Cryptography (SAC 2008), Lecture Notes in Computer Science 5381, Springer–Verlag, Berlin, 2009, 82–102.

[119] Taxicabs and sums of two cubes: An excursion in number theory, reprinted from the 1993 original, with additional material, in *Biscuits of Number Theory*, A. Benjamin and E. Brown, editors, Mathematical Association of America, 2008.

[120] Local–global aspects of (hyper)elliptic curves over (in)finite fields, Conference on Hyperelliptic Curve Cryptography (Frutillar, Chile, March 16–20, 2009), *Advances in Mathematics of Communications* 4 (2010), 101–114.

[121] Height estimates for equidimensional dominant rational maps, *J. Ramanujan Math. Soc.* **26** (2011), 145–163

[122] Lang's height conjecture and Szpiro's conjecture, *New York Journal of Math.* **16** (2010), 1–12

[123] The greatest common divisor of $a^n - 1$ and $b^n - 1$ and the Ailon–Rudnick conjecture, *Gems in experimental mathematics, Contemp. Math.* **517** (2010), 339–347

[124] A survey of local and global pairings on elliptic curves and abelian varieties, Pairing-Based Cryptography (PAIRING 2010), M. Joye, A. Miyaji, A. Otsuka, eds., LNCS 6487, Springer-Verlag, Berlin, 2010, 377–396.

[125] with Liang-Chung Hsia, A quantitative estimate for quasi-integral points in orbits, *Pacific Journal of Math.* **249** (2011), 321–342.

[126] with Katherine Stange, Amicable pairs and aliquot cycles for elliptic curves, *Exper. Math.*, **20(3)** (2011), 329–357.

[127] with Katherine Stange, Terms in elliptic divisibility sequences divisible by their indices, *Acta Arith.* **146.4** (2011), 355–378.

[128] Lehmer's conjecture for polynomials satisfying a congruence divisibility condition and an analogue for elliptic curves, *Journal Number Theory Bordeaux* **24** (2012), 751–772

[129] An algebraic approach to certain cases of Thurston rigidity, *Proc. AMS* **140** (2012), 3421–3434

[130] with Patrick Ingram, Valéry Mahé, Katherine E. Stange, and Marco Streng. Algebraic divisibility sequences over function fields, *J. Australian Math. Soc.* **92** (2012), 99–126.

[131] Elliptic Carmichael numbers and elliptic Korselt criteria, *Acta Arithmetica* **155** (2012), 233–246

[132] with Bianca Viray, On a uniform bound for the number of exceptional linear subvarieties in the dynamical Mordell-Lang conjecture, *Math. Research Letters* **20** no. 3 (2013), 547–566.

[133] Dynamical degree, arithmetic entropy, and canonical heights for dominant rational self-maps of projective space, *Ergodic Th. and Dyn. Sys.* **34** (2014), 633–664.

[134] Elliptic Curves, Section 12.2 in *Handbook of Finite Fields*, Gary L. Mullen and Daniel Panario, eds., Discrete Mathematics and Its Applications (Book 78), Chapman and Hall/CRC, 2013, 422–439.

[135] A review of *Some problems of unlikely intersections in arithmetic and geometry* by Umberto Zannier (with appendixes by David Masser), *Bul. Amer. Math. Soc.*, **50** (2013), 353–358.

[136] with Shu Kawaguchi, On the dynamical degree and the arithmetic degree of rational self-maps of algebraic varieties, *J. Reine Angew. Math.*, **713** (2016), 21–48.

[137] Primitive divisors, dynamical Zsigmondy sets, and Vojta's conjecture, *J. Number Theory* **133** (2013), 2948–2963

[138] with Shu Kawaguchi, Examples of dynamical degree equals arithmetic degree, *Michigan Math. Journal*, **63** (2014), 41–63.

[139] A Century of Elliptic Curves, in *A century of advancing mathematics*, the centennary of the MAA, Math. Assoc. America, Washington, DC, 2015, 117–131.

[140] with Shu Kawaguchi, Dynamical canonical heights for Jordan blocks, arithmetic degrees of orbits, and nef canonical heights on abelian varieties, *Trans. Amer. Math. Soc.* **368** (2016), 5009–5035.

[141] What is the p-adic Mandelbrot set, *Notices of the AMS* **60** (2013), 1048–1050

[142] with Shu Kawaguchi and Mike Joyce, Landen transforms as families of (commuting) rational self-maps of projective space, *Bull Inst. Math. Academia Sinica* **9** (2014), 547–584.

[143] *with J. Hoffstein, J. Pipher, J. Schanck, W. Whyte, PASS-RS: Practical signatures from the partial Fourier recovery problem, In: Boureanu I., Owesarski P., Vaudenay S. (eds), Applied Cryptography and Network Security. ACNS 2014. Lecture Notes in Computer Science, vol 8479, Springer.

[144] *with J. Hoffstein, J. Pipher, J. Schanck, W. Whyte, Transcript Secure Signatures Based On Modular Lattices, PQCrypto 2014, Lecture Notes in Comput. Sci. **8772**, Springer, 142–159.

[145] with J. Hoffstein, PASS-Encrypt: A Public Key Cryptosystem Based on Partial Evaluation of Polynomials, *Designs, Codes, and Cryptography* (Vanstone memorial issue), **77:2** (2015), 541–552.

[146] Arithmetic and Dynamical Degrees on Abelian Varieties, *J. Théor. Nombres*

Bordeaux **29** (2017), 151–167.

[147] with A. Bridy, P. Ingram, R. Jones, J. Juul, A. Levy, M. Manes, S. Rubinstein-Salzedo, Finite ramification for preimage fields of postcritically finite morphisms, *Math. Res. Lett.* **24:6** (2017), 1633–1647.

[148] *with J. Hoffstein, J. Pipher, J. Schanck, W. Whyte, Z. Zhang, Choosing Parameters for NTRUEncrypt, Topics in cryptologyCT-RSA 2017, 318, Lecture Notes in Comput. Sci., 10159, Springer, Cham, 2017.

[149] Divisor divisibility sequences on tori, *Acta Arith.* 177(4), 2017, 315–345.

[150] with M. Manes, A classification of degree 2 semi-stable rational maps $P^2 \to P^2$ with large finite dynamical automorphism group, *Annales de la Faculte des Sciences de Toulouse*, to appear. `<arXiv:1607.05772>`

[151] with G. Call, Degeneration of dynamical degrees in families of maps, *Acta Arithmetica* 184(2), 2018, 101–116.

[152] Good reduction and Shafarevich-type theorems for dynamical systems with portrait level structures, *Pacific J. Math.*, 295-1 (2018), 145–190.

[153] with A. Salerno, Integrality properties of Böttcher coordinates for one-dimensional superattracting germs, *Ergodic Theory and Dynamical Systems* 40(1), 2020, 248–271.

[154] *with Y. Doröz, J. Hoffstein, J. Pipher, B Sunar, W. Whyte, Z. Zhang, Fully homomorphic encryption from the finite field isomorphism problem, Public-Key Cryptography—PKC 2018 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25–29, 2018, Proceedings, LNCS 10769, 125–155.

[155] *with J. Hoffstein, W. Whyte, Z. Zhang, A signature scheme from the finite fields isomorphism problem, MathCrypt 2018, accepted for publication.

[156] with J. Doyle, A Uniform Field-of-Definition/Field-of-Moduli Bound for Dynamical Systems on $\mathbf{P^N}$, *J. Number Theory* **195**, (2019), 1–22.

[157] with R. Benedetto, P. Ingram, R. Jones, M. Manes, T. Tucker, Current Trends and Open Problems in Arithmetic Dynamics, Bulletin of the AMS **56**(4), (2019), 611–685.

[158] with A. Bérczes, A. Ostafe, I. Shparlinski, Multiplicative dependence among iterated values of rational functions modulo finitely generated groups, *IMRN*, published online 27 May 2019. `arXiv:1811.04971`.

[159] To Write or Not To Write . . . a Book, and When?, *Notices of the AMS* **66**(3) (2019), 357–358.

[160] with J. Doyle, Moduli Spaces for Dynamical Systems with Portraits, `arxiv.org/abs/1812.09936`.

[161] with Chong Gyu Lee, GIT Stability of Hénon Maps, `arxiv.org/abs/1907.13247`.

[162] with P. Ingram and R. Ramadas, Post-Critically Finite Maps on P^n for $n \geq 2$ are Sparse, `arxiv.org/abs/1910.11290`.

*Articles marked with an asterisk were written in collaboration with individuals from NTRU Cryptosystems, Inc. (Security Innovations, Inc.)

Doctoral Students

2019 Thomas Silverman, Brown University
Stability in Non-archimedean Dynamics

2019 Seoyoung Kim, Brown University
The distribution of the trace of Frobenius and its applications in number theory

2018 Laura Walton, Brown University
Forward and inverse image problems in arithmetic dynamics

2015 Wade Hindes, Brown University
Height Functions and Specialization Map for Families of Elliptic Curves

2015 Wei Pin Wong, Brown University
Galois Uniformity in Arithmetic Dynamics

2014 Jonah Leshin, Brown University
Class field towers, solvable Galois representations, and Noether's problem in Galois theory

2013 Florian Sprung, Brown University
Iwasawa Theory for Elliptic Curves

2013 Jacqueline Anderson, Brown University
On the p-adic Mandelbrot Set

2012 Hatice Sahinoglu, Brown University
On the Independence of Heegner Points

2011 Matthew Spencer, Brown University
Moduli Spaces of Power Series in Finite Characteristic

2010 ChongGyu (Joey) Lee, Brown University
Height Estimates For Rational Maps

2009 Daniel Katz, Brown University
Sumfree Subsets in Cubes of Arbitrary Dimension

2008 Katherine Stange, Brown University
Elliptic Nets and Elliptic Curves

2008 Yu Yasufuku, Brown University
Vojta's Conjecture and Blowups

2007 Michelle Manes, Brown University
Arithmetic Dynamics of Rational Maps

2007 Ben Hutz, Brown University
Arithmetic Dynamics on Varieties of Dimension Greater Than One

2004 Michael Joyce, Brown University
Counting Rational Points on the E_6 Cubic Surface

2004 Rafe Jones, Brown University
Galois Martingales and the p-adic Hyperbolic Mandelbrot Set

2002 Ebru Bekyel, Brown University
Density of elliptic curves with global minimal Weierstrass equations

2001 Rania Wazir, Brown University
Arithmetic on elliptic threefolds

2000 Selemon Getachew, Brown University
Ramification properties and Galois groups of iterates of prime-degree Kummer type polynomials

2000 Su-Ion Ih, Brown University
Uniform bounds for the heights of rational points in families

1998 Rob Benedetto, Brown University
Fatou components in p-adic dynamics

1998 Matt Papanikolas, Brown University
Canonical heights in characteristic p

1997 Ottavio Rizzo, Brown University
On the variation of root numbers in families of elliptic curves

1994 Liang-Chung Hsia, Brown University
A weak Néron model with applications to p-adic dynamical systems

1993 Christopher Towse, Brown University
Weierstrass points on cyclic covers of $\mathbf{P}^1$

1993 Seng-Kiat Chua, Brown University
The arithmetic of étale quotients of varieties

1993 Yen-mei Julia Chen, Brown University
Descent via 3-Isogenies on Elliptic Curves

1991 Arthur Baragar, Brown University
The Markoff equation and equations of Hurwitz

1990 Hwasin Park, Brown University
Idempotent relations and the conjecture of Birch and Swinnerton-Dyer

1989 Masato Kuwata, Brown University
Mordell-Weil groups and elliptic K3 surfaces

1988 Nicholas Strauss, Boston University
Symbolic algebra: Jordan forms and local analysis

1986 Robert Gross, Massachusetts Institute of Technology
A quantitative version of Schmidt's theorem on simultaneous Diophantine approximation

Total: 34 Ph.D. students supervised with completed theses

Service

Service to Brown University

Committee to select Brown's Goldwater Fellowship applicants, 2012
Provost's Advisory Committee on Resource Allocation, 2003-2004
University Lectureships Committee, 1997–2000
Chair, 1998–1999
University Teaching Awards Committee, 1997–98
Wriston Grant Committee, 1996

Service to Mathematics Department

Mathematics Department Chairman, 2001–04, 2009
Algebra Seminar (Co-Organizer), 1988–present (most years)
Math Department Committees (* indicates chair)
Senior Search Committee, 1990, 1995*, 1998, 2001, 2002*, 2003, 2004, 2005, 2006, 2008, 2014
Tamarkin Search Committee, 1989, 1994*, 1996*, 1999*, 2004, 2005, 2007, 2008*, 2016*
Graduate Student Admissions Committee, 2006, 2013
Mathematics Department Executive Officer, 1994–97, 1999–00, 2004–06, 2007–08
Mathematics Department Computer Committee (Chair), 1990–93, 1997–98

Service with the American Mathematical Society

AMS Board of Trustees 2015–2020 (chair 2018)
AMS Fellows Selection Committee, 2013
AMS Executive Committee 2009–2013
AMS Council, 2008–2013
AMS Committee on Publications, 2008–2011 (chair 2011)
AMS Subcommittee on Graduate Students (chair), 2011–2012
AMS Subcommittee to select an AMS Associate Secretary, 2012
Editorial Committee of AMS Pure and Applied Undergraduate Texts, 2009–2015
AMS Conant Prize Selection Committee, 2000–2003

Editorial Service to Mathematical Community

Editorial Board, *Algebra and Number Theory*, 2011–
Advisory Board, *Acta Arithmetica*, 2011–
Editorial Board, *New York Journal of Mathematics*, 2008–
Editorial Board, *International Journal of Modern Mathematics*, 2007–2010
Editorial Board, *Compositio Mathematica*, 1992–2005
Reviewer for *Mathematical Reviews*, 1983–present, 300+ reviews written
Reviewer for *Zentralblatt für Mathematik*, 1984–90

Other Service to Mathematical Community

ICERM Scientific Advisory Board 2018–2021

NSF Review Panel, December 2018
NSF SaTC Review Panel, August 2016
AIM Workshop on Arithmetic Dynamics, May 2016, co-organizer
Co-Organizer AMS Special Session, Seattle, January 2016
Co-Organizer ICERM Workshop on Modular Forms and Curves of Low Genus Sept 2015
ICERM Semester on Complex and Arithmetic Dynamics, spring 2012, lead scientific organizer
Co-Organizer AMS Special Session, San Francisco, January 2010
AIM Workshop on Arithmetic Dynamics, January 2008, co-organizer
Claude Shannon Institute, Dublin, Advisory Board, 2006–2011
ECRYPT Workshop on Post-Quantum Cryptography, May 2006, Organizing/Program Committee
IPAM Semester on Cryptography, Fall 2006, Organizing Committee
NSF Inst. for Pure and Appl. Math. (IPAM-UCLA), Board of Trustees, 2003–2006
Co-Organizer AMS Special Session, New Jersey, April 2004
Co-Organizer Cryptography and Lattices Conference, Brown, March 2001
Program Committee, CHES Conferences, 2000, 2001, 2002, 2004
Co-Organizer AMS Special Session, Providence, October 1999
Co-Organizer Conference on Fermat's Last Theorem, Boston, August 1995
Member of NSA Mathematical Sciences Advisory Panel, 1991–94
Referee for many journals
Referee for National Science Foundation, 1985–present
Referee for National Security Agency, 1988–present

Invited Talks

—— 2019 ——

MAGNTS: Midwest Arithmetic Geometry and Number Theory Series
Ohio State University, Oct 12-13, 2019
REU Summer@ICERM program in Arithmetic Dynamics
Providence, July 16, 2019
MRC on Explicit Methods in Arithmetic Geometry in Characteristic p
Warwick, RI, June 17-18, 2019
Arithmetic of Low-Dimensional Abelian Varieties
ICERM, Providence, June 3–7, 2019
Simons Symposium on Algebraic, Complex, and Arithmetic Dynamics
Kuln, Germany, May 19–25, 2019
Dynamical Systems Seminar
University of Rhode Island, April 5, 2019
Hawaii Number Theory Conference 2019 (HINT) (Mon-Thurs)
AMS Sectional Meeting in Hawaii (Fri-Sun)
University of Hawaii, March 18 - 24, 2019 (Mon-Sun)
Simons Collaboration Conference on Arithemtic Geometry
New York City, January 9–11, 2019.

—— 2018 ——

Workshop on Nonlinear Algebra in Applications
ICERM, November 12 - 16, 2018 (Mon-Fri)
Special Session on Arithmetic Dynamics
AMS Sectional Meeting, Boston (co-organizer), April 21–22, 2018
Arithmetic Dynamics Workshop
Northwestern, May 17-20, 2018
UConn Number Theory Day
University of Connecticutt - April 11, 2018
JHU Center for Talented Youth
Brown - April 8, 2018
Special Session on Arithmetic Dynamics
AMS/MAA Joint Meeting, San Diego, Jan 10–13, 2018

—— 2017 ——

Math Circle Talk
Brown University, November 8, 2017
Number Theory Seminar
Harvard, October 11, 2017
Special Session on Arithmetic Dynamics
Mathematical Congress of the Americas, Montreal, July 23–28, 2017
Clemson REU
Clemson, June 18 - 21 (Sun-Weds)

Complex and Arithmetic Dynamics Workshop
University of Michigan, May 15–17, 2017
Mentoring Workshop for Graduate Advisors in Mathematics
University of Michigan, May 13–14, 2017
Upstate New York Number Theory Conference
Binghamton University, May 6–7, 2017
Number Theory Seminar
CUNY, New York, March 30, 2017
Heights and Applications to Unlikely Intersections Workshop
Fields Institute, Toronto, Feb 13–17, 2017
AMS Special session on Mathematics of Cryptography
MAA Session on Cryptology for Undergraduates
AMS/MAA Joint Meeting, Atlanta, Jan 4–7 2017

2016

Computational Arithmetic Dynamics
Collaborate@ICERM (co-organizer), June 25–29, 2016
Plenary lecture
CNTA, Calgary, June 20–24, 2016
The Galois theory of orbits in arithmetic dynamics
AIM (co-organizer), May 16–20, 2016
Diophantine Approximation
Oberwolfach, April 10–16, 2016
Number Theory Seminar
University of Colorado, Mar 8, 2016
Colloquium and Seminar
Colorado State University, Mar 2 & 10, 2016
Number Theory Seminar and Undergraduate Seminar
Amherst College, Feb 23, 2016
Undergraduate Seminar
Scripps College, Jan 2016
Colloquium, Number Theory Seminar, and Undergraduate Seminar
University of Hawaii, Jan 2016
Special session on Arithmetic Dynamics (organizer)
Special session on Number Theory (speaker)
AMS/MAA Joint Meeting, Seattle, Jan 6–9 2016

2015

Workshop on Arithmetic Dynamics
Univ of Michigan, Dec 3-6, 2015
Panelist
Cryptography Workshop, WPI, Oct 19, 2015
Research Seminar
ICERM, Thur Sept 24, 2015

Seminar
UConn, Weds Sept 16, 2015
Colloquium
Providence College, April 22, 2015
Workshop on Mathematics of Lattices and Cybersecurity
ICERM, April 21–24, 2015
Colloquium
Wheaton College, Weds April 15, 2015
Undergraduate Seminar
WPI, Tues Mar 3, 2015
Algebraic Aspects of Dynamical Systems
UNSW Sydney, Australia, Feb 2015
DIMACS Workshop on the Mathematics of Post-Quantum Cryptography
Rutgers, Jan 2015
Secure and Trustworthy Cyberspace (NSF SaTCPI '15)
Arlington, VA, Jan 2015

2014

BC–MIT Number Theory Seminar
Boston College, Nov 2014
Workshop on Statistics in Number Theory
CRM University of Montreal, Sept 2014
Algebrac Structures Workshop
IPAM, May 2014
Colloquium and Dynamical Systems Seminar
Stony Brook, April 2014
Mathematics Across the Cannon (2 talks)
Carleton and St. Olaf Colleges, April 2014
Leonard C. Sulski Memorial Lecture
Holy Cross, March 2014
AMS Graduate Student Chapter Lecture
Boston University, March 2014
Mathematical Challenges in Cybersecurity Workshop
ICERM, Providence, March 2014
Workshop on Postcritically Finite Maps
AIM, March 2014
Number Theory Seminar
Harvard, February 2014
Colloquium
University of Pennsylvania, February 2014
Colloquium
Tulane, January 2014

Eight Lectures on Elliptic Curves and Lattices
Seoul National University, January 2014

2013

SCHOLAR Number Theory Conference
Centre Research Mathematique, Montreal, October 2013
SIAM Conference on Applied Algebrac Geoemtry
Colorado State University, August 2013
Colloquium and seminar talk
Microsoft Research, Redmond, July 2013
IdeaLab on Homomorphich Encryption
ICERM, July 2013 (co-organizer and speaker)
Workshop on Transcendence and Number Theory
NCTS, Taiwan, June 2013
Conference on Arithmetic Geometry and Arithmetic Dynamics
Academica Sinica, Taiwan, June 2013
Colloquium
Weslyan University, April 2013
AMS Sectional Meeting
Boston College, April 2013
Colloquium
University of Rochester, March 2013
Distinguished Undergraduate Lecture in Number Theory
Hunter College, March 2013
Colloquium
University of Michigan, February 2013
Joint Mathematics Meeting Special Session
San Diego, January 2013

2012

Undergraduate Colloquium
Amherst College, December 2012
CRM Research Period on "Diophantine Geometry"
Pisa, Italy, October 2012
Colloquium
Allegheny College, August 2012
Workshop on Nevanlinna Theory and Number Theory
University College London, June 2012
Workshop on Algebraic Dynamics
UC Berkeley, May 2012 (co-organizer)
Conference on Arithmetic Geometry
CUNY, May 2012
ICERM Workshop on Dynamical Moduli Spaces
Providence, April 2012 (co-organizer and speaker)

ICERM Semester Program on Complex and Arithmetic Dynamics
    Providence, January–May 2012 (lead scientific organizer)
Joint Mathematics Meeting
    Boston, January 2012
        MAA Invited Paper Session on the Beauty and Power of Number Theory
        AMS Special Session on Global Dynamics of Rational Difference Equations
        AMS-SIAM Special Session on Mathematics of Computation
        AMS Special Session on Dynamical Systems in Algebraic/Arithmetic Geometry

2011

Conference on Endomorphisms of Algebraic Varieties
    Japan, December 2011
Colloquium and Number Theory Seminar
    University of Georgia, November 2011
Colloquium
    West Chester University, October 2011
Maine/Quebec Number Theory Conference
    University of Maine, October 2011
Number Theory Seminar
    Waterloo, June 2011
Elliptic Curve Cryptography Conference
    Toronto, June 2011
MAA NES Spring Meeting
    Northfield, Vermont, June 2011
AMS Special Session on Arithmetic Dynamics
    University of Las Vegas, May 2011
Trends in Dynamics
    Northwestern University, April 2011
AMS Special Session on Number Theory, Topology, and Dynamics
    Holy Cross, Worcester, April 2011
CRM Colloquium
    Montreal, April 2011
Quebec/Vermont Number Theory Seminar
    Montreal, March 2011
Colloquium
    Vassar College, February 2011
Special Session
    AMS/MAA Joint Meeting, New Orleans, Janaury 2011

2010

Number Theory Seminar
    Osaka University, Japan, December 2010
Algebraic Geometry Seminar
    Kyoto University, Japan, December 2010

Pairing 2010
    Japan, December 2010 (plenary speaker)
Workshop on Arithmetic Dynamics
    CUNY Graduate Center, June 2010 (co-organizer, did not speak)
Workshop on Moduli for Dynamics
    Bellairs research station, Barbados, May 2010 (5 2-hour lectures)
Workshop on Cryptography
    CRM Montreal, April 2010 (co-organizer, did not attend)
Arizona Winter School
    Arithmetic Dynamics, March 2010 (4 lectures)
Palmetto Number Theory Symposium (PANTS)
    Clemson University, February 2010 (plenary speaker)
Special Session on Arithmetic Dynamics
    AMS Winter Meeting, San Francisco, January 2010 (co-organizer, did not speak)

2009

MSR Colloquium
    Microsoft Research, Cambridge, December 2009
Number Theory Seminar
    MIT, November 2009
MIT/MSR Cryptography Seminar
    Microsoft Research, Cambridge, October 2009
Journees Arithmetique
    St. Etienne, France, July 2009 (plenary speaker)
Number Theory Seminar
    MIT, April 2009
Conference on (Hyper)elliptic Curve Cryptography
    Frutillar, Chile, March 2009
Dynamics Seminar
    Santiago, Chile, March 2009
New York Joint Number Theory Seminar
    CUNY Graduate Center, NY, February 2009
Special Session on Experimenal Mathematics
    MAA/AMS Joint Meeting, Washington DC, January 2009

2008

Workshop on Rational Points on K3 Surfaces
    Banff International Research Station, December 2008
Workshop on p-adic Dynamics
    Fields Institute, Toronto, October 2008 (co-organizer and speaker)
Selected Areas of Cryptography (SAC) (Invited Address)
    Sackville, N.B., Canada, August 2008
Canadian Number Theory Association (CNTA)
    University of Waterloo, July 2008

TateFest
University of Texas, Austen, May 2008
34$^{\text{th}}$ Annual New York State Regional Graduate Mathematics Conference
Syracuse University, March 2008 (Opening Address)
Algebra/Topology Seminar
Bates College, March 2008
Colloquium and Seminar Talks
University of Colorado and Colorado State University, February 2008
Workshop on The Uniform Boundedness Conjecture in Arithmetic Dynamics (co-organizer)
American Institute of Mathmatics, January 2008

2007

Colloquium
University of Connecticut, November 2007
Number Theory Seminar
Boston University, October 2007
11th Workshop on Elliptic Curve Cryptography
and a public lecture on "The Ubiquity of Elliptic Curves"
University College Dublin, September 2007
25th Journées Arithmétique
University of Edinburgh, July 2007
Workshop on Computability and Number Theory
ICMS, Edinburgh, June 2007
Distinguished Lecture Series
Oberlin College, April 2007
Kuwait Lecture and Number Theory Seminar (2 talks)
Cambridge University, England, February 2007

2006

Special Lecture Series (3 talks)
NCTS National Tsing Hua University, Taiwan, October 2006
Colloquium
National Central University, Taiwan, October 2006
Number Theory Seminar
UCLA, October 2006
Workshop on Number Theory and Cryptography — Open Problems
IPAM, UCLA, October 2006
Semester on Cryptography (organizing committee)
IPAM, UCLA, Fall 2006
Colloquium
University of Udine, Italy, September 2006
Number Theory Seminar
SNS Pisa, Italy, September 2006

Number Theory Seminar
University of Paris VI, France, September 2006
Summer School on Computational Number Theory and Applications
to Cryptography, University of Wyoming, June 2006 (4 lectures)
AMS Special Session on Arithmetic Geometry and Modular Forms
University of New Hampshire, April 2006
Five Colleges Number Theory Seminar
Amherst College, March 2006
Workshop in Rational and Integral Points on Higher-Dimensional Varieties
MSRI, Berkeley, January 2006

2005

Program on Diophantine Geometry
Centro di Ricerca Matematica, Pisa, Italy, June 2005
Number Theory Seminar
University of Texas at Austin, April 2005
Frontier Lectures on Arithmetic Dynamics (series of 3 talks)
Texas A & M, April 2005
ArithmeTexas Conference
Texas A & M, April 2005
Undergraduate Math Awareness Month Lecture
Texas A & M, April 2005

2004

Conference in Honor of Dale Brownawell
University of Waterloo, Canada, June 2004
Conference on Algebraic Dynamics
CUNY Graduate Center, NY, May 2004
AMS Special Session on Elliptic Surfaces (co-organizer)
New Jersey, April 2004

2003

Colloquium
Williams College, September 2003
Graduate Student Algebra Seminar
Brown University, July 2003
MAA Invited Address
AMS/MAA Joint Annual Meeting, Baltimore, MD, January 2003
Colloquium
Dartmouth University, January 2003

2002

MAA Short Course on the Mathematics of Cryptology (2 talks)
MathFest 2002, Burlington, VT, July 2002
Arithmetic Geometry Colloquium
Rikkyo University, Tokyo, July 2002

Undergraduate Colloquium
University of Massachusetts, Boston, May 2002
Algebraic Geometry Seminar
Princeton University, April 2002
Number Theory Seminar
Boston University, March 2002
Conference on Cryptography (co-organizer)
IPAM, UCLA, Los Angeles, January 2002

2001

Special Session on Number Theory
AMS Meeting, Williams College, October 2001
Special Session on Arithmetic Dynamical Systems
AMS Meeting, Williams College, October 2001
Research Seminar on Elliptic Curves and Lattice-Based Cryptography
Microsoft Research, Redmond, June 2001

2000

Research Seminar on Elliptic Curves and Lattice-Based Cryptography
Microsoft Research, Redmond, November 2000
Algorithmic Number Theory and Number Theoretic Cryptography Workshop
MSRI, Berkeley, October 2000
UVM/Montreal Joint Number Theory Seminar
University of Vermont, October 2000
Workshop on Recent Trends in Analytic Number Theory
Institue for Advanced Study, April 2000
Colloquium and Dynamical Systems Seminar
SUNY Stony Brook, March 2000
Unusual Applications of Number Theory
DIMACS, Rutgers University, January 2000

1999

Midwest Arithmetic Geometry and Cryptography Conference (MAGC)
University of Illinois at Urbana/Champagne, November 1999
American Mathematical Society—Session on Arithmetic Dynamics
Providence College, October 1999 (session co-organizer and speaker)
Cryptographic Hardware and Embedded Systems (CHES)
Worcester Polytechnic Institute, July, 1999
Princeton/IAS/Rutgers Number Theory & Harmonic Analysis Seminar
Princeton University, April 1999
MAA Dinner Meeting
Providence, April 1999
Conference on Rational Points and Algebraic Points on Varieties
Institut Henri Poincaré, Paris, February 1999

1998

Number Theory Seminar
Boston University, October 1998

Elliptic Curve Cryptography Workshop
University of Waterloo, Waterloo, Canada, September 1998

Conference on Rational Points on Varieties
Newton Institute, Cambridge, UK, March 1998

1997

Connecticut Valley Mathematics Colloquium
Amherst College, November, 1997

Conference on Topics in Number Theory
Penn State University, July 1997

Algebra Seminar
Boston University, April 1997

Conference on Elliptic Curves and Applications
Johns Hopkins, March 1997

1996

American Mathematical Society Meeting
New Jersey, October 1996

Conference on Computations on Curves
Maxwell Institute, Edinburgh, March 1996

1995

Conference on Arithmetic Geometry
University of Toronto, October 1995

Conference on Fermat's Last Theorem
Boston University, August 1995

Paris Number Theory Seminar
Institut Henri Poincaré, Paris, June 1995

Problèmes Diophantiens
Universite P. et M. Curie, Paris, June 1995

Number Theory Seminar
University of Pennsylvania, March 1995

1994

Number Theory Seminar
Columbia University, September 1994

Conference on Diophantine Approximation
University of Colorado at Boulder, June 1994

Number Theory Seminar
Harvard University, April 1994

Number Theory Seminar
Amherst College, April 1994

1993

Colloquium
Colby College, October 1993
Number Theory Seminar
Boston University, September 1993
Conference on Diophantine Geometry
MSRI, March 1993
IAS/Princeton Number Theory Seminar
Institute for Advanced Study, March 1993
Number Theory Seminar
Harvard University, March 1993
Colloquium
Boston University, February 1993
Undergraduate Mathematics Colloquium
Wellesley College, February 1993
Fellowship of the Ring Seminar
Brandeis University, February 1993

1992

Colloquium
University of New Hampshire, September 1992
Journees Arithmetique
Paris, July 1992
Problèmes Diophantiens
Universite P. et M. Curie, Paris, July 1992
Union College Mathematics Conference
Union College, April 1992
Number Theory Seminar
Harvard University, February 1992

1991

Number Theory Seminar
Columbia University, December 1991
American Mathematical Society Meeting
Philadelphia, PA, October 1991
Conference on p-adic Monodromy and the Birch-Swinnerton-Dyer Conjecture
Boston, MA, August 1991
Number Theory Seminar
Boston University, March 1991
Algebra Seminar
Amherst College, January 1991

1990

Conference on Diophantine Approximation and Transcendence Theory
Oberwolfach, Germany, October 1990

Workshop on Algebraic Geometry
IMPA, Rio de Janeiro, April 1990
Algebra Seminar
University of Pennsylvania, Philadelphia, March 1990

1989

Number Theory Seminar
Columbia University, New York, October 1989
Séminare Delange-Pisot-Poiteau
Institut Henri Poincaré, Paris, June 1989
Séminaire sur les Pinceaux Arithmétiques
Ecole Normale Supérieure, Paris, June 1989
Number Theory Seminar
Institut Henri Poincaré, Paris, June 1989
Number Theory Seminar
Bordeaux, June 1989
American Mathematical Society Meeting
Worcester, MA, April 1989
Colloquium
Rutgers University, April 1989
Conference on Arithmetic Geometry
University of Arizona, Tuscon, January 1989

1988

Algebra Seminar and Colloquium
Yale University, March 1988
Conference on Diophantine Approximation and Transcendence Theory
Oberwolfach, Germany, March 1988
Two invited talks at the University of Leiden
Leiden, The Netherlands, March 1988

1987

Number Theory Seminar
Columbia University, December 1987
Colloquium
University of Michigan, November 1987
Journées Arithmétiques
Ulm, Germany, September 1987
Special Week on Galois Representations
MSRI, Berkeley, March 1987
(invited participant, did not speak)

1986

Bi-Annual Mathematics Conference
Union College, May 1986

Conference on Diophantine Approximation and Transcendence Theory
Oberwolfach, Germany, March 1986

Number Theory Seminar
Institute for Advanced Study, Princeton, February 1986

1985

Number Theory Seminar
Massachusetts Institute of Technology, November 1985

Number Theory Seminar
Brown University, October 1985

Conference on Arithmetic Algebraic Geometry
Arcata, CA, August 1985

Number Theory Seminar
Harvard University, May 1985

1984

Number Theory Seminar
Brown University, December 1984

Algebra Seminar
Princeton University, November 1984

Conference on Arithmetic Geometry
Storrs, CT, August 1984 (Organizing committee)

1983

Colloquium and Special Seminar
University of Colorado, October 1983

Applied Mathematics Seminar
Massachusetts Institute of Technology, September 1983

Colloquium
University of Connecticut, September 1983

American Mathematical Society Meeting
New York, NY, April 1983

Algebraic Geometry Seminar
Massachusetts Institute of Technology, March 1983

Number Theory Seminar
Massachusetts Institute of Technology, February 1983

1980–1982

Conference on Transcendence Theory
Luminy, France, July 1982

Algebra Seminar
Princeton University, December 1981

Conference on Modern Trends in Number Theory
Boston, MA, July 1981

American Mathematical Society Meeting
Providence, RI, October 1980

Courses Taught

Spring, 2020	
MA54	Linear Algebra
MA076	Introduction to Higher Mathematics
Fall, 2019	
MA153	Algebra (48 students)
Spring, 2019	
MA254	Algebraic Number Theory
MA197	Number Theory (Reading Course, 1 undergrad)
Fall, 2018	
MA075	Introduction to Higher Mathematics
MA253	Algebraic Number Theory
MA197	Sphere Packing (Reading Course, 1 undergrad)
Spring, 2018	
MA042	Number Theory
MA076	Introduction to Higher Mathematics
Fall, 2017	
MA158	Cryptography
Spring, 2017	
MA254	Number Theory
MA197	Algebraic Number Theory (Reading Course, 1 undergrad)
Fall, 2016	
MA253	Number Theory
MA271	Topics Course on Complex and p-adic Dynamics
Spring, 2016	
Sabbatical — Travel and research	
Fall, 2015	
Sabbatical — ICERM Program on Langland's Program	
MA197	Advanced Elliptic Curves (Reading Course, 1 undergrad)
Spring, 2015	
MA154	Algebra (17 students)
MA197	(& MA298) Elliptic Curves (Reading Course, 2 undergrads & 7 grads)
Fall, 2014	
MA35	Honors Multivariable Calculus (76 students)
MA251	Graduate Algebra (26 students)
Spring, 2014	
MA272	Arithmetic Dynamics (6 students, 10+ attending)
MA197	Elliptic Curves (Reading Course, 2 students)

Fall, 2013

MA126	Complex Analysis (16 students)
MA153	Algebra (26 students)

Spring, 2013

MA54	Linear Algebra (31 students)
MA254	Number Theory (7 students)

Fall, 2012

MA158	Cryptography (42 students)
MA197	Advanced Cryptography (Reading Course, 1 student)

Spring, 2012

Sabbatical — ICERM Program on Complex and Arithmetic Dynamics

Fall, 2011

MA253	Number Theory

Spring, 2011

MA254	Number Theory
MA197	Elliptic Curve Cryptography (Reading Course, 2 students)

Fall, 2010

MA10	Calculus (2 sections, approx 90 students total)

Spring, 2010

MA42	Number Theory
MA156	Number Theory

Fall, 2009

Leave of absence — Microsoft Research New England

Spring, 2009

MA154	Algebra
MA156	Number Theory

Fall, 2008

No teaching duties while interim department chair. Ran an informal reading course on the arithmetic of elliptic curves for 4 graduate students.

Spring, 2008

MA42	Number Theory
MA197	Diophantine Geometry (Reading Course, 1 student, David Hansen)

Fall, 2007

MA158	Cryptography

Spring, 2007

MA252	Algebra
MA272	Topics in the Arithmetic of Elliptic Curves

Fall, 2006

Sabbatical Leave

Spring, 2006		
	MA156	Number Theory
Fall, 2005		
	MA9	Calculus
Spring, 2005		
	MA272	Number Theory and Dynamics
Fall, 2004		
	MA158	Cryptography
Fall, 2003		
	MA001	First Year Seminar—Explorations in Mathematics
Fall, 2002		
	MA156	Number Theory
Spring, 2002		
	MA192	Data Compression (Reading Course, 2 students)
	MA272	Arithmetic of Elliptic Curves (Reading Course)
Fall, 2001		
	MA161	Probability
Spring, 2000		
	MA254	Number Theory (Arithmetic Dynamics)
Fall, 1999		
	MA35	Honors Calculus
Spring, 1998		
	MA156	Number Theory
	MA272	Arithmetic of Elliptic Curves (Reading Course)
Fall, 1997		
	MA9	Calculus
	MA54	Honors Linear Algebra
Spring, 1997		
	MA254	Number Theory (Arithmetic of Elliptic Curves)
Fall, 1996		
	MA18	Intermediate Calculus
	MA271	Arithmetic of Elliptic Curves (topics)
Spring, 1996		
	MA42	Number Theory
Fall, 1995		
	MA17	Advanced Placement Calculus
	MA251	Algebra

Spring, 1995

MA42	Number Theory
MA254	Number Theory (Diophantine Geometry)

Fall, 1994

MA9	Calculus

Spring, 1993

MA254	Number Theory

Fall, 1992

MA35	Honors Multivariable Calculus
MA181	Elliptic Curves

Spring, 1992

MA156	Number Theory
MA206	Algebraic Geometry

Fall, 1991

MA10	Calculus

Spring, 1991

MA272	Elliptic Curves and Complex Multiplication (topics)

Fall, 1990

MA17	Advanced Placement Calculus
MA251	Algebra

Spring, 1990

MA154	Algebra
MA292	Class Field Theory (reading course)

Fall, 1989

MA35	Honors Multivariable Calculus
MA153	Algebra
MA291	Class Field Theory (reading course)

Spring 1989

MA252	Algebra

Fall 1988

MA251	Algebra
MA271	Diophantine Geometry (topics)

Spring 1988

MA272	Arithmetic of Elliptic Curves (topics)

Visiting Positions

Fall 1993 — Boston University

MA803	Arithmetic of Elliptic Curves