

## 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](mailto:jhs@math.brown.edu)  
Home Page: [www.math.brown.edu/~jhs](http://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]  
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 in Mathematics  
Massachusetts Institute of Technology, 1982–86

### Education

Harvard University Ph.D. 1982  
Harvard University M.A. 1979  
Brown University Sc.B. 1977

### Doctoral Thesis

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

### Fellowships, Grants, Awards

NSF Research Grants, 1986–1998, 1999–2003, 2006–present  
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 Council, 2008–2011; AMS Executive Committee 2009–2013  
 AMS Graduate Working Group (chair), 2011–2013  
 Editorial Committee of AMS Pure and Applied Undergraduate Texts, 2009–2013  
 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–  
 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

Joint Mathematics Meeting  
     Boston, January 2012 (4 talks)  
 Conference on Endomorphisms of Algebraic Varieties  
     Japan, December 2011  
 Colloquium and Number Theory Seminar  
     University of Georgia, November 2011  
 Maine/Quebec Number Theory Conference  
     University of Maine, October 2011  
 MAA NES Spring Meeting  
     Northfield, Vermont, June 2011 (award recipient)  
 Elliptic Curve Cryptography Conference  
     Toronto, June 2011 (award recipient)  
 Trends in Dynamics  
     Northwestern University, April 2011  
 Pairing 2010  
     Japan, December 2010 (plenary speaker)  
 Workshop on Moduli for Dynamics  
     Bellairs research station, Barbados, May 2010 (5 2-hour lectures)  
 Arizona Winter School  
     Arithmetic Dynamics, March 2010 (4 lectures)  
 Palmetto Number Theory Symposium (PANTS)  
     Clemson University, February 2010 (plenary speaker)  
 MSR Colloquium  
     Microsoft Research, Cambridge, December 2009  
 Number Theory Seminar  
     MIT, November 2009

## Publications – Joseph H. Silverman

### BOOKS

- [1] *Moduli Spaces and Arithmetic Dynamics*, CRM/AMS, 2012.
- [2] *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer-Verlag, N.Y., 1986; 2nd edition 2009.
- [3] with J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Math., Springer-Verlag, N.Y., 1992.
- [4] *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math. **151**, Springer-Verlag, N.Y., 1994.
- [5] *A Friendly Introduction to Number Theory*, Prentice-Hall, N.J., 1997; 2nd edition 2001; 3rd edition 2006; 4th edition 2012.
- [6] with M. Hindry, *Diophantine Geometry: An Introduction*, Graduate Texts in Math. **201**, Springer-Verlag, New York, 2000.
- [7] *The Arithmetic of Dynamical Systems*, Graduate Texts in Math. **241**, Springer-Verlag, N.Y., 2007.
- [8] with Jill Pipher and Jeffrey Hoffstein, *An Introduction to Mathematical Cryptography*, Undergraduate Texts in Mathematics, Springer-Verlag, 2008.

### 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. 15<sup>th</sup> 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, Sémin. 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 arithmetic 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  $\text{GF}(2^N)$ , 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 NTRU-Encrypt 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 conjecture 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.

- [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\\_1ash4-1\\_ORIG.pdf](http://csrc.nist.gov/groups/ST/hash/documents/SAARINEN_1ash4-1_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, Nonarchimedean 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 Journées Arithmétiques 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, *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, submitted for publication, September 2010. <arXiv:1008.3649>
- [129] An algebraic approach to certain cases of Thurston rigidity, *Proc. AMS*, to appear.
- [130] with Patrick Ingram, Valéry Mahé, Katherine E. Stange, and Marco Streng. Algebraic divisibility sequences over function fields, submitted for publication, May 2011.
- [131] Elliptic Carmichael numbers and elliptic Korselt criteria, *Acta Arithmetica*, to appear. <arXiv:1108.3830>
- [132] with Bianca Viray, On a uniform bound for the number of exceptional linear subvarieties in the dynamical Mordell–Lang conjecture, submitted for publication, September 2011. <arXiv:1109.0207>

- [133] Generalized Stereographic Projections, Arithmetic Dynamics, and Quasi-Real Rational Maps Relative to Arbitrary Quadratic Extensions, in preparation.
- [134] Dynamical Degree, Arithmetic Entropy, and Canonical Heights for Dominant Rational Self-Maps of Projective Space, submitted.

\*Articles marked with an asterisk were written in collaboration with individuals from NTRU Cryptosystems, Inc.

**Doctoral Students**

- 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*
- 1990 Kathryn Furio, Brown University (Master's thesis)  
*Distribution of Weierstrass points on nodal curves of arithmetic genus zero*
- 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*

**Invited Talks**

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

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, January 2011

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)
- 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 Experimental Mathematics  
MAA/AMS Joint Meeting, Washington DC, January 2009
- Workshop on Rational Points on K3 Surfaces  
Banff International Research Station, December 2008
- Workshop on  $p$ -adic Dynamics  
Fields Institute, Toronto, October 2008 (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<sup>th</sup> 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 Arithmetic Dynamics (co-organizer)  
American Institute of Mathematics, January 2008

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

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

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

Arithmetic Texas Conference  
Texas A & M, April 2005

Undergraduate Math Awareness Month Lecture  
Texas A & M, April 2005

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

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

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

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
- 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  
Institut 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
- 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 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
- 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
- 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

American Mathematical Society Meeting  
New Jersey, October 1996

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

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

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

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

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

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

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

Number Theory Seminar  
Columbia University, New York, October 1989

Séminaire 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

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

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)

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

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

Number Theory Seminar  
Brown University, December 1984

Algebra Seminar  
Princeton University, November 1984

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

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

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, 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)

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

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 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