

CURRICULUM VITAE

Joseph H. Silverman

Address

(Office) 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]
Associate Professor of Mathematics
Brown University, 1988–1991
Associate Professor of Mathematics
Boston University, 1986–1988
NSF Postdoctoral Fellow
Massachusetts Institute of Technology, 1983–86
C.L.E. Moore Instructor in Mathematics
Massachusetts Institute of Technology, 1982–85

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, 2006–2008
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

AIM Workshop on Arithmetic Dynamics, January 2008, co-organizer
Claude Shannon Institute, Dublin, Advisory Board, 2006–
Editorial committee for the AMS University Lecture Series, 2006–
IPAM Semester on Cryptography, Fall 2006, Organizing Committee
Editorial Board, *International Journal of Modern Mathematics*, 2007–present
Editorial Board, *Compositio Mathematica*, 1993–2005
Reviewer for *Mathematical Reviews*, 1983–present
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

Recent Invited Addresses

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
NCTS National Tsing Hua University
Taiwan, October 2006 (3 lectures)
Number Theory Seminar
UCLA, October 2006
Workshop on Number Theory and Cryptography
IPAM, UCLA, October 2006

Publications – Joseph H. Silverman

- [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] *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer-Verlag, N.Y., 1986, 1–400
- [19] Points of finite order on elliptic curves, *Amer. Math. Monthly* **93** (1986), 793–795
- [20] co-editor with G. Cornell, *Arithmetic Geometry*, a conference held at Storrs, Connecticut, 1984, Springer-Verlag, N.Y., 1986, 1–353
- [21] The theory of height functions, *Arithmetic Geometry*, ed. by G. Cornell and J. Silverman, Springer-Verlag, N.Y., 1986, 151–166
- [22] Heights and elliptic curves, *Arithmetic Geometry*, ed. by G. Cornell and J. Silverman, Springer-Verlag, N.Y., 1986, 253–266

- [23] Arithmetic distance functions and height functions in Diophantine geometry, *Math. Ann.* **279** (1987), 193–216
- [24] 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
- [25] Integral points on abelian varieties are widely spaced, *Compos. Math.* **61** (1987), 253–266
- [26] A quantitative version of Siegel’s theorem: Integral points on elliptic curves and Catalan curves, *J. Reine Angew. Math.* **378** (1987), 60–100
- [27] Rational points on certain families of curves of genus at least two, *Proc. London Math. Soc.* **55** (1987), 465–481
- [28] Integral points on curves and surfaces, Proc. 15th Journées Arithmétiques, Ulm, 1987, *Lect. Notes in Math.* **1380** (1989), 202–241
- [29] Computing heights on elliptic curves, *Math. Comp.* **51** (1988), 339–358
- [30] with M. Hindry, The canonical height and integral points on elliptic curves, *Invent. Math.* **93** (1988), 419–450
- [31] Wieferich’s criterion and the *abc*-conjecture, *J. Number Theory* **30** (1988), 226–237
- [32] Recent (and not so recent) developments in the arithmetic theory of elliptic curves, *Nieuw Archief voor Wiskunde* **7** (1989), 53–70
- [33] Elliptic curves of bounded degree and height, *Proc. Amer. Math. Soc.* **105** (1989), 540–545
- [34] A review of *Introduction to Arakelov Theory* by Serge Lang, *Bul. Amer. Math. Soc.* **21** (1989), 171–176
- [35] Hecke points on modular curves, *Duke Math. J.* **60** (1990), 401–423
- [36] Rational points on symmetric products of a curve, *Am. J. Math.* **113** (1991), 471–508
- [37] The Markoff equation $X^2 + Y^2 + Z^2 = aXYZ$ over quadratic imaginary fields, *J. Number Theory* **35** (1990), 72–104
- [38] The difference between the Weil height and the canonical height on elliptic curves, *Math. Comp.* **192** (1990), 723–743
- [39] with M. Hindry, On Lehmer’s conjecture for elliptic curves, Sémin. Th. Nombres Paris 1988–1989, *Prog. in Math.* **91** (1990), 103–116
- [40] with J. Harris, Bi-elliptic curves and symmetric products, *Proc. AMS* **112** (1991), 347–356
- [41] Some arithmetic properties of Weierstrass points: Hyperelliptic curves, *Bol. Soc. Bras. Mat.* **21** (1990), 11–50
- [42] with J.F. Voloch, Multiple Weierstrass points, *Compos. Math.* **79** (1991), 123–134
- [43] Rational points on K3 surfaces: A new canonical height, *Invent. Math.* **105** (1991), 347–373

- [44] A uniform bound for rational points on twists of a given curve, *J. Lond. Math. Soc.* **47** (1993), 385–394
- [45] Variation of the canonical height on elliptic surfaces I: Three examples, *J. Reine Angew. Math.* **426** (1992), 151–178
- [46] Variation of the canonical height on elliptic surfaces II: Local analyticity properties, *J. Number Theory* **48** (1994), 291–329
- [47] Variation of the canonical height on elliptic surfaces III: Global boundedness properties, *J. Number Theory* **48** (1994), 330–352
- [48] Variation of the canonical height in algebraic families, *Contemp. Math.* (B. Mazur and G. Stevens, eds.) **165** (1994), 123–133
- [49] Taxicabs and sums of two cubes: An excursion in number theory, *Am. Math. Monthly* **100** (1993), 331–340 (MAA Ford award)
- [50] with P. Lockhart and M. Rosen, An upper bound for the conductor of an abelian variety, *J. Algebraic Geometry* **2** (1993), 569–601
- [51] Counting integral and rational points on varieties, Columbia University Number Theory Seminar, New York, 1992, *Asterisque* **228** (1995), 223–236
- [52] with J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Math., Springer–Verlag, N.Y., 1992, 1–281.
- [53] with G. Call, Canonical heights on varieties with morphisms, *Compos. Math.* **89** (1993), 163–205
- [54] Integer points, Diophantine approximation, and iteration of rational maps, *Duke Math. J.* **71** (1993), 793–829
- [55] Geometric and arithmetic properties of the Hénon map, *Math. Zeit.* **215** (1994), 237–250
- [56] with P. Morton, Periodic points, multiplicities, and dynamical units, *J. Reine Angew. Math.* **461** (1995), 81–122
- [57] with P. Morton, Rational periodic points of rational functions, *Inter. Math. Research Notices* **2** (1994), 97–110
- [58] On the field of definition for dynamical systems on \mathbf{P}^1 , *Compos. Math.* **98** (1995), 269–304
- [59] with G. Call, Computing the canonical height on K3 surfaces, *Math. Comp.* **65** (1996), 259–290
- [60] *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math. **151**, Springer-Verlag, N.Y., 1994, 1–525
- [61] with R. Gross, S -integer points on elliptic curves, *Pacific J. Math.* **167** (1995), 263–288
- [62] with M. Rosen, R. Murty, Variations on a theme of Romanoff, *Inter. J. Math.* **7** (1996), 373–391
- [63] Small Salem numbers, exceptional units, and Lehmer’s conjecture, *Rocky Mountain J. Math.* **26** (1996), 1099–1114
- [64] Exceptional units and small Salem numbers, *Experimental Mathematics* **4** (1995), 69–83

- [65] Rational functions with a polynomial iterate, *J. Algebra* **180** (1996), 102–110
- [66] Computing canonical heights with little (or no) factorization, *Math. Comp.* **66** (1997), 787–805
- [67] with A. Brumer, The number of elliptic curves over \mathbf{Q} with conductor N , *Manuscripta Math.* **91** (1996), 95–102
- [68] Computing rational points on rank 1 elliptic curves via L -series and canonical heights, *Math Comp.* **68** (1999), 835–858
- [69] 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.
- [70] 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, 1–569
- [71] 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
- [72] *A Friendly Introduction to Number Theory*, Prentice-Hall, N.J., 1997, 1–288
- [73] The space of rational maps on \mathbf{P}^1 , *Duke Math. J.* **94** (1998), 41–77
- [74] with M. Rosen, On the rank of an elliptic surface, *Invent. Math.* **133** (1998), 43–67
- [75] The average rank of an algebraic family of elliptic curves, *J. Reine Angew. Math.* **504** (1998), 227–236
- [76] 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
- [77] A bound for the Mordell-Weil rank of an elliptic surface after a cyclic base extension, *Journal of Algebraic Geometry* **9** (2000), 301–308
- [78] On the distribution of integer points on curves of genus zero, *Theoretical Computer Science* **235** (2000), 163–170
- [79] 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
- [80] *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.
- [81] The xendi calculus and the elliptic curve discrete logarithm problem, *Design, Codes and Cryptography* **20** (2000), 5–40
- [82] with M. Jacobson, N. Koblitz, A. Stein, and E. Teske, Analysis of the xedni calculus attack, *Design, Codes and Cryptography* **20** (2000), 41–64
- [83] with M. Hindry, Sur le nombre de points de torsion rationnels sur une courbe elliptique, *C.R. Acad. Sci. Paris* **329** (1999), 97–100

- [84] *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.
- [85] *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.
- [86] *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.
- [87] Rings of low multiplicative complexity, *Finite Fields and Their Applications* **6** (2000), 175–191
- [88] with M. Hindry, *Diophantine Geometry: An Introduction*, Graduate Texts in Math. **201**, Springer-Verlag, New York, 2000, 1–558
- [89] *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.
- [90] with I.E. Shparlinski, Linear complexity of the Naor–Reingold pseudo-random function from elliptic curves, *Designs, Codes and Cryptography* **24** (2001), 279–289.
- [91] *A Friendly Introduction to Number Theory*, Prentice-Hall, N.J., 2nd expanded edition, 2001, 1–390
- [92] editor of *Cryptography and Lattices Conference* (CaLC 2001), Lecture Notes in Computer Science 2461, Springer-Verlag, 2001, 1–215.
- [93] 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.
- [94] *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.
- [95] *with Jeffrey Hoffstein, Jill Pipher, NSS: An NTRU lattice-based signature scheme, Advances in Cryptology–Eurocrypt 2001, Lecture Notes in Computer Science, Springer-Verlag.
- [96] The rank of elliptic surfaces in unramified abelian towers, *J. Reine Angew. Math.*, **577** (2004), 153–169 <arXiv:mathNT/0305028>.
- [97] A lower bound for the canonical height on elliptic curves over abelian extensions, *Journal of Number Theory* **104** (2004), 353–372
- [98] with Matthew Baker, A lower bound for the canonical height on abelian varieties over abelian extensions, *Mathematical Research Letters* **11** (2004), 377–396 <arXiv:mathNT/0312393>.

- [99] 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.
- [100] *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.
- [101] *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.
- [102] *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.
- [103] Common divisors of $a^n - 1$ and $b^n - 1$ over function fields, *New York Journal of Math.* (electronic) **10** (2004), 37–43
- [104] Common divisors of elliptic divisibility sequences over function fields, *Manuscripta Mathematica* **114** (2004), 432–446
- [105] p -adic properties of division polynomials and elliptic divisibility sequences, *Mathematische Annalen* **332**(2) (2005), 443–471 (addendum 473–474).
- [106] 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.
- [107] *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.
- [108] Generalized greatest common divisors, divisibility sequences, and Vojta’s conjecture on blowups, *Monatsch. Math.* **145** (2005), 333–350
- [109] 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.
- [110] Height bounds and preperiodic points for families of jointly regular affine maps, *Quart. J. Pure Appl. Math.* **2** (2006), 135–145
- [111] *A Friendly Introduction to Number Theory*, Prentice-Hall, N.J., 3rd expanded edition, 2005, 1–434.
- [112] with N. Stephens, The sign of an elliptic divisibility sequence, *Journal of the Ramanujan Math. Soc.* **21** (2006), 1–17.
- [113] Greatest common divisors and algebraic geometry, Proceedings of a Workshop on Diophantine Geometry, Centro di Ricerca Matematica Ennio De Giorgi,

- Pisa, Italy, June 2005, to appear.
- [114] *with J. Hoffstein, N. Howgrave-Graham, J. Pipher, W. Whyte, Performance improvements and a baseline parameter generation algorithm for NTRUSign, preprint 2005 <http://eprint.iacr.org/2005/274>.
 - [115] Divisibility Sequences and Powers of Algebraic Integers, *Documenta Math.* (electronic) Extra Volume: John H. Coates' Sixtieth Birthday (2006), 711–727
 - [116] with M. Rosen, On the independence of Heegner points associated to distinct quadratic imaginary fields, *Journal of Number Theory* 127 (2007), 10–36.
 - [117] with S. Kawaguchi, Dynamics of projective morphisms having identical canonical heights, *Proc. London Math. Soc.* **95** (2007), 519–544.
 - [118] with S. Kawaguchi, The arithmetic complexity of morphisms on projective space, preprint June 2006.
 - [119] with S. Kawaguchi, Nonarchimedean Green functions and dynamics on projective space, preprint July 2006.
 - [120] *with W. Whyte, Timing attacks on NTRUEncrypt based on variation in number of hash calls, CT-RSA 2007, accepted for publication.
 - [121] with Patrick Ingram, Uniform estimates for primitive divisors in elliptic divisibility sequences, preprint December 2006.
 - [122] Variation of periods modulo p in arithmetic dynamics, preprint May 2007.
 - [123] *The Arithmetic of Dynamical Systems*, Graduate Texts in Math. **241**, Springer-Verlag, N.Y., 2007, 1–511.
 - [124] with Patrick Ingram, Primitive divisors in arithmetic dynamics, preprint July 2007.

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