Noam D. Elkies

Department of Mathematics
Harvard University
Cambridge, MA 02138
(617)495-4625 (office), (617)495-5132 (fax)

BIOGRAPHICAL

Born Aug. 1966 in New York City
Moved Dec. 1970 to Ramat Gan, Israel
Returned Aug. 1978 to New York
In Cambridge, Mass. since September 1985

EDUCATION

Harvard University (GSAS), 9/1985–6/1987, M.A. in Mathematics 6/1986, Ph.D. in Mathematics 6/1987. Dissertation advised by Barry Mazur and Benedict Gross: *Supersingular primes of a given elliptic curve over a number field.*

Columbia College, 9/1982–5/1985, B.A. *summa cum laude* in Mathematics and Music

Stuyvesant High School, 9/1979–6/1982

EMPLOYMENT

Harvard University, 7/1993–present, Professor (Mathematics)
(Department head, 7/2012–6/2013)

Harvard University, 7/1990–6/1993, Associate Professor (Mathematics), John L. Loeb Professor of the Natural Sciences

Harvard University, 9/1987–6/1990, Junior Fellow (Mathematics)

Institute for Defense Analyses, intermittently from 7/1986 to present, consultant

Bell Laboratories, 7/1991, consultant

DOCTORAL THESES ADVISED

Henry L. Cohn (2000): *New Bounds on Sphere Packing*

David Y. Jao (2003): *Supersingular Primes for Rational Points on Modular Curves*

Nicholas F. Rogers (2004): *Elliptic Curves $x^3 + y^3 = k$ with High Rank*

Abhinav Kumar (2006): *K3 Surfaces of High Rank*

Sonal Jain (2007): *Minimal Heights and Regulators On Elliptic Surfaces*

Jeechul Woo (2011): *Arithmetic of Elliptic Curves and Surface: Descents and Quadratic Sections*

Yevgeny Zaytman (2010): *K3 surfaces of high Picard number and arithmetic applications*

Nathan Kaplan (2012): *Rational Point Counts for del Pezzo Surfaces over Finite Fields and Coding Theory*

SELECTED AWARDS AND HONORS

2011 - Louise and Richard Guy Lecture, University of Calgary

2006 - K. Ireland Memorial Lecture, Univ. of New Brunswick

2005 - Plenary address at British Mathematical Colloquium

2005 - R.E. Phillips Lecture Series, Michigan State Univ.

2004 - L.L. Conant Prize, American Mathematical Society

2004 - L.R. Ford Award, Mathematical Association of America

2004 - Plenary address at annual meeting of the Israel Mathematical Union
2003 - Invited address at the 2003 AMS-MAA Joint Mathematics Meetings
1995 - Columbia University Medal of Excellence
1992 - Prix Peccot (Collège de France)
1991 - Packard Fellowship for Science and Engineering
1991 - Presidential Young Investigator
1991 - W.O. Baker Award for Initiatives in Research (National Academy of Sciences)
1990 - John L. Loeb Professor of the Natural Sciences (Harvard University)
1987 - Junior Fellow (Harvard University)
1985 - NSF Graduate Fellowship in Mathematics
1983–85 - Top 5 in 42nd, 43rd and 44th Putnam competitions; Putnam Fellowship for graduate study at Harvard
1985 - Valedictorian, Columbia College
1984 - Phi Beta Kappa (while in Junior year)
1982 - 1st in USA Math Olympiad; Gold Medal at International Math Olympiad
1982 - 8th in Westinghouse Science Talent Search
1981 - Tied for 1st in USA Math Olympiad; Gold Medal with perfect score at International Math Olympiad

PUBLICATIONS

1. Integers expressible in the form $a^4 + b^4$, pages 22–28 in Vol. 3 of *Mathematical Buds* (H. Ruderman, ed.; Norman, Oklahoma: Mu Alpha Theta, 1984).
2. An improved lower bound on the greatest element of a sum-distinct set of fixed order, *J. Comb. Theory A* **41** (Jan. 1986), 89–94.
3. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$, *Invent. Math.* **89** (1987), 561–568.
4. On $A^4 + B^4 + C^4 = D^4$, *Math. of Comp.* **51** (Oct. 88), 825–835.
5. Supersingular primes for elliptic curves over real number fields, *Compositio Math.* **72** (1989), 165–172.
6. The automorphism group of the modular curve $X_0(63)$, *Compositio Math.* **74** (1990), 203–208.
7. On the Hurwitz scheme and its monodromy (with D. Eisenbud, J. Harris, and R. Speiser), *Compositio Math.* **77** (1991), 95–117.
8. Distribution of supersingular primes, *Astérisque* **198-199-200** (1991; proceedings of Journées Arithmétiques 1989), 127–132.
9. On the packing densities of superballs and other bodies (with A.M. Odlyzko and J.A. Rush), *Invent. Math.* **105** (1991), 613–639.
10. ABC implies Mordell, *International Math. Research Notices* **7** (1991), 99–109.
11. Alternating sign matrices and domino tilings I, II (with G. Kuperberg, M. Larsen, and J. Propp), *J. Alg. Combinatorics* **1** (1992), 111–132 and 219–234.
12. Mordell–Weil lattices in characteristic 2: I. Construction and first properties, International Math. Research Notices, 1994 #8, 343–361; II. The Leech lattice as a Mordell–Weil lattice, Inventiones Math. **128** (1997), 1–8; III. A Mordell–Weil lattice of rank 128, *Experimental Math.* **10** (2001) #3, 467–473.

13. Wiles minus epsilon implies Fermat, pages 38–40 in *Elliptic Curves, Modular Forms, and Fermat's Last Theorem* (J. Coates and S.-T. Yau, eds.; Boston: International Press, 1995; proceedings of the 12/93 conference on elliptic curves and modular forms at the Chinese University of Hong Kong).
14. Heegner point computations, *Lecture Notes in Computer Science* **877** (proceedings of ANTS-1, 1994; L.M. Adleman, M.-D. Huang, eds.), 122–133.
15. On numbers and endgames, pages 135–150 in *Games of No Chance* (R.J. Nowakowski, ed.; MSRI Publ. #29, 1996 via Cambridge Univ. Press; proceedings of the 7/94 MSRI conference on combinatorial games). math.CO/9905198 on the arXiv.
16. A characterization of the $\mathbf{Z}^n$ lattice, *Math. Research Letters* **2** (1995), 321–326.
17. Lattices and codes with long shadows, *Math. Research Letters* **2** (1995), 643–651.
18. Local statistics for random domino tilings of the Aztec diamond (with H. Cohn and J. Propp), *Duke Math. J.* **85** #1 (Oct. 1996), 117–166.
19. The exceptional cone and the Leech lattice (with B.H. Gross), *International Math. Research Notices* **1996** #14, 665–698.
20. Elliptic and modular curves over finite fields and related computational issues, pages 21–76 in *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin* (D.A. Buell and J.T. Teitelbaum, eds.; AMS/International Press, 1998).
21. Explicit modular towers, pages 23–32 in *Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing* (1997, T. Başar, A. Vardy, eds.), Univ. of Illinois at Urbana-Champaign 1998 (math.NT/0103107 on the arXiv).
22. Embeddings into the Integral Octonions (with B.H. Gross), *Pacific J. Math.*, Dec. 1997 (Olga Taussky-Todd Memorial Issue), 147–158.
23. Shimura curve computations, *Lecture Notes in Computer Science* **1423** (proceedings of ANTS-3, 1998; J.P. Buhler, ed.), 1–47 (math.NT/0005160 on the arXiv).
24. The still-Life density problem and its generalizations, pages 228–253 in *Voronoï's Impact on Modern Science, Book I* (P. Engel and H. Syta, eds.; Institute of Math., Kyiv 1998 = Vol.21 of *Proc. Inst. Math. Nat. Acad. Sci. Ukraine*). math.CO/9905194 on the arXiv.
25. Linearized algebra and finite groups of Lie type. I: Linear and symplectic groups, pages 77–107 in *Applications of curves over finite fields* (Seattle, 1997) = *Contemp. Math.* **245**, Providence: AMS, 1999.
26. The Klein quartic in number theory, pages 51–102 in *The Eightfold Way: The Beauty of Klein's Quartic Curve* (S. Levy, ed.; Cambridge Univ. Press, 1999; also online at the MSRI Publications site).
27. Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction, *Lecture Notes in Computer Science* **1838** (proceedings of ANTS-4, 2000; W. Bosma, ed.), 33–63 (on the arXiv at math.NT/0005139).
28. Explicit towers of Drinfeld modular curves, *Progress in Mathematics* **202** (2001), 189–198 (Proceedings of the 3rd European Congress of Mathematics, Barcelona, 7/2000: paper presented at the mini-symposium on "curves over finite fields and codes"; math.NT/0005140 on the arXiv).
29. Lattices, Linear Codes, and Invariants (2-part expository article), *Notices of the American Math. Society* **47** (2000), 1238–1245 and 1382–1391.

30. Cubic rings and the exceptional Jordan algebra (with B.H. Gross), *Duke Math. J.* **109** #2 (2001), 383–409.
31. Excellent nonlinear codes from modular curves, pages 200–208 in *STOC'01: Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, Hersonissos, Crete, Greece. Isomorphic with math.NT/0104115 on the arXiv.
32. On finite sequences satisfying linear recursions, *New York J. Math.* **8** (2002), 85–97 = http://nyjm.albany.edu:8000/j/2002/8-5.html (math.CO/0105007 on the arXiv).
33. Curves $Dy^2 = x^3 - x$ of Odd Analytic Rank, *Lecture Notes in Computer Science* **2369** (proceedings of ANTS-5, 2002; C. Fieker and D.R. Kohel, eds.), 244–251. math.NT/0208056 on the arXiv.
34. Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with Galois Groups of Order 168 and $8 \cdot 168$ (with N. Bruin), *Lecture Notes in Computer Science* **2369** (proceedings of ANTS-5, 2002; C. Fieker and D.R. Kohel, eds.), 172–188.
35. Appendix to "New Optimal Tame Towers of Function Fields over Small Finite Fields" by W.-C.W. Li, H. Maharaj, and H. Stichtenoth [identifying each of their four towers with a tower of classical modular curves], *Lecture Notes in Computer Science* **2369** (proceedings of ANTS-5, 2002; C. Fieker and D.R. Kohel, eds.), 384–389.
36. Higher Nimbers in pawn endgames on large chessboards, pages 61–78 in *More Games of No Chance* (R.J. Nowakowski, ed.; MSRI Publ. #42, 2002 via Cambridge Univ. Press; proceedings of the 7/00 MSRI workshop on combinatorial games). math.CO/0011253 on the arXiv.
37. The mathematical knight (with Richard Stanley), *Math. Intelligencer* **25** #1 (2003), 22–34.
38. New upper bounds on sphere packings I (with H. Cohn), *Annals of Math.* **157** (2003), 689–714 (math.MG/0110009 on the arXiv).
39. On the Sums $\sum_{k=-\infty}^{\infty}(4k+1)^{-n}$, *Amer. Math. Monthly* **110** #7 (Aug.-Sep. 2003), 561–573. Nearly isomorphic with math.CA/0101168 on the arXiv. Corrigenda: *Amer. Math. Monthly* **111** #5 (May 2004), 456.
40. On Elliptic K-curves, *Progress in Mathematics* **224** (2004), 81–91 (Proceedings of the 7/2002 Barcelona Euroconference on "Modular Curves and Abelian Varieties", ed. J. Cremona, J.-C. Lario, J. Quer, and K. Ribet).
41. Curves of every genus with many points, II: Asymptotically good families (with E.W. Howe, A. Kresch, B. Poonen, J.L. Wetherell, and M.E. Zieve), *Duke Math. J.* **122** #2 (2004), 399–422 (math.NT/0208060 on the arXiv).
42. Elliptic Curves of Large Rank and Small Conductor (with M. Watkins), *Lecture Notes in Computer Science* **3076** (proceedings of ANTS-6, 2004; D. Buell, ed.), 42–56 (on the arXiv at math.NT/0403374).
43. Elliptic Curves $x^3 + y^3 = k$ of High Rank (with N.F. Rogers), *Lecture Notes in Computer Science* **3076** (proceedings of ANTS-6, 2004; D. Buell, ed.), 184–193. math.NT/0403116 on the arXiv.
44. Gaps in $\sqrt{n}$ mod 1 and ergodic theory (with C.T. McMullen), *Duke Math. J.* **123** #1 (2004), 95–139.
45. The conjugate dimension of algebraic numbers (with N. Berry, A. Dubickas, B. Poonen, and C. Smyth), *Quart. J. Math.* **55** (2004), 237–252 (math.NT/0308069 on the arXiv).
46. New Directions in Enumerative Chess Problems, *Electronic J. of Combinatorics* **11(2)** (2004–2005) [Stanley-60 Festschrift], Article #4 (math.CO/0508645 on the arXiv).

47. Reduction of CM Elliptic Curves and Modular Function Congruences (with K. Ono and T. Yang), *International Math. Research Notices* **2005** #44, 2695–2707 (math.NT/0512350 on the arXiv).
48. Sylvester–Gallai Theorems for Complex Numbers and Quaternions (with L.M. Pretorius and K.J. Swanepoel), *Discrete and Computational Geometry* **35** #3 (3/2006), 361–373 (on the arXiv at math.MG/0403023).
49. The Mathieu group M_{12} and its pseudogroup extension M_{13} (with J.H. Conway and J.L. Martin), *Experimental Math.* **15** (2006) #2, 223–236 (math.GR/0508630 on the arXiv).
50. Points of Low Height on Elliptic Curves and Surfaces I: Elliptic surfaces over $\mathbf{P}^1$ with small d, *Lecture Notes in Computer Science* **4076** (proceedings of ANTS-7, 2006; F. Hess, S. Pauli, and M. Pohst, eds.), 287–301. math.AG/0608593 on the arXiv.
51. Shimura Curves for Level-3 Subgroups of the (2,3,7) Triangle Group, and Some Other Examples, *Lecture Notes in Computer Science* **4076** (proceedings of ANTS-7, 2006; F. Hess, S. Pauli, and M. Pohst, eds.), 302–316. math.AG/0409020 on the arXiv.
52. On some points-and-lines problems and configurations, *Periodica Mathematica Hungarica* **53** #1–2 (2006), 133–148. math.MG/0612749 on the arXiv.
53. The D_4 Root System Is Not Universally Optimal (with Henry Cohn, John H. Conway, and Abhinav Kumar), *Experimental Math.* **16** (2006) #3, 313–320. math.NT/0607447 on the arXiv.
54. Shimura Curve Computations Via K3 Surfaces of Néron-Severi Rank at Least 19, *Lecture Notes in Computer Science* **5011** (proceedings of ANTS-8, 2008; A.J. van der Poorten and A.Stein, eds.), 196–211. math.NT/0802.1301 on the arXiv.
55. About the cover: Rational curves on a K3 surface, pages 1–4 of Arithmetic Geometry: Proceedings of the Clay Mathematics Institute, Göttingen, 17 July – 11 August, 2006 (Henri Darmon, David Alexandre Ellwood, Brendan Hassett, and Yuri Tschinkel, eds.), *Clay Math. Proceedings* **8**, 2009. www.math.rice.edu/~hassett/conferences/Clay2006/Elkies/CMIPelkies.pdf
56. Refined Configuration Results for Extremal Type II Lattices of Ranks 40 and 80 (with Scott Duke Kominers), *Proceedings of the American Math. Society* **138** #1 (2010), 105–108. math.NT/0905.4306 on the arXiv.
57. On the Classification of Type II Codes of Length 24 (with Scott Duke Kominers), *SIAM J. Discrete Math.* **23** #4 (2010), 2173–2177. math.NT/0902.1942 on the arXiv.
58. Point configurations that are asymmetric yet balanced (with Henry Cohn, Abhinav Kumar, and Achill Schürmann), *Proceedings of the American Math. Society*, posted on March 23, 2010, PII S 0002-9939(10)10284-6; **138** #8 (August 2010), 2863–2872. math.MG/0812.2579 on the arXiv.
59. Weighted Generating Functions for Type II Lattices and Codes (with Scott Duke Kominers), pages 63–108 in *Quadratic and Higher Degree Forms* (Krishnaswami Alladi, Manjul Bhargava, David Savitt, and Pham Huu Tiep, eds.), *Developments in Mathematics* **31** 2013 (New York: Springer). math.NT/1111.2392 on the arXiv.

OTHER

Extensive training as composer and pianist; some performances broadcast on television or radio in Israel and the United States; several commissions including *Shema* Op.34 for the Campaign for Choral Music at Harvard-Radcliffe and *Brandenburg Concerto #7* Op.49 for the Metamorphosen ensemble; Opera *Yossele Solovey* (libretto by J.Dauber after the novel by Sholem Aleichem) fully

staged at Harvard, 1999; *Four of my First* Op. 3 for piano, and *A Meditation on Mortality* Op. 31 #3 for mixed chorus, published respectively by Israeli Music Publications and Broude Brothers, Inc.

U.S. Chess master since 1986; Solving World Champion in 1996, and Solving Grandmaster since 2001. Chess publications include "Chess Art in the computer age" (*American Chess Journal* **2** (1995)), an endgame column in *Chess Horizons* running from 1988 to 1990, and numerous original endgame studies and chess problems. See also items 15, 36, 46 in the publication list above.

REFERENCES

Prof. B. Mazur
Dept. of Mathematics
Harvard University
Cambridge, MA 02138

Prof. B.H. Gross
Dept. of Mathematics
Harvard Univ.
Cambridge, MA 02138