



Karl Rubin  
Department of Mathematics  
UC Irvine  
Irvine, CA 92697-3875

phone: 949-824-1645  
fax: 508-374-0599  
krubin@math.uci.edu  
<http://www.math.uci.edu/~krubin>

## CV and Bibliography

### Karl Rubin

#### *Education*

1981 Ph.D., Mathematics, Harvard University  
1977 M.A., Mathematics, Harvard University  
1976 A.B. *summa cum laude*, Mathematics, Princeton University

#### *Employment*

2004– Thorp Professor of Mathematics, University of California Irvine  
1997–2006 Professor, Stanford University  
1996–1999 Distinguished University Professor, Ohio State University  
1987–1996 Professor, Ohio State University  
1988–1989 Professor, Columbia University  
1984–1987 Assistant Professor, Ohio State University  
1982–1983 Instructor, Princeton University

#### *Selected visiting positions*

Universität Erlangen-Nürnberg  
Harvard University  
Institute for Advanced Study (Princeton)  
Institut des Hautes Etudes Scientifiques (Paris)  
Mathematical Sciences Research Institute (Berkeley)  
Max-Planck-Institut für Mathematik (Bonn)

#### *Selected honors and awards*

1999 Humboldt-Forschungspreis (Humboldt Foundation Research Award)  
1994 Guggenheim Fellowship  
1992 AMS Cole Prize in Number Theory  
1988 NSF Presidential Young Investigator Award  
1987 Ohio State University Distinguished Scholar Award  
1985 Sloan Fellowship  
1981 NSF Postdoctoral Fellowship  
1979 Harvard University Graduate School of Arts and Sciences Fellow  
1976 NSF Graduate Fellowship  
1975 Putnam Fellow

*Selected invited lectures*

- 5/2008 MAA Distinguished Lecture, Washington DC
- 8/2002 ICM invited 45 minute lecture, Beijing
- 1/2000 AMS-MAA-SIAM Invited Address, Washington DC
- 5/1997 Ohio State University Distinguished Lecture
- 10/1995 Hermann Weyl Lectures (4 lectures), Institute for Advanced Study
- 12/1994 Briefing to Secretary of Defense William Perry, Pentagon
- 9/1994 Deutsche Mathematiker-Vereinigung plenary lecture, Duisburg
- 1/1994 AAAS Topical Lecture, San Francisco
- 10/1993 Adrian Albert Lectures (3 lectures), University of Chicago
- 7/1993 Fermat Fest, Palace of Fine Arts, San Francisco
- 4/1993 Arnold Ross Lecture, Ohio State University
- 6/1990 Arbeitstagung, Bonn
- 4/1989 AMS Hour Lecture, Worcester
- 6/1988 Arbeitstagung, Bonn
- 3/1988 AMS Hour Lecture, East Lansing

*Editorial positions*

- 2007– Journal of the AMS
- 2007– Algebra & Number Theory
- 1994–01 Journal für die reine und angewandte Mathematik
- 1993–98 Compositio Mathematica
- 1987–99 Journal of Number Theory

*Selected committee service*

- 2004–07 AMS Editorial Boards Committee
- 1998– IAS/Park City Mathematics Institute, steering committee and organizer
- 1998 NSF Division of Mathematical Sciences Committee of Visitors
- 1997–99 Board of Trustees, Assn. of Members of the Institute for Advanced Study
- 1996 AMS Cole Prize Committee (chair)
- 1996 Co-organizer, National Academy of Sciences conference *Elliptic Curves and Modular Forms*
- 1995–99 MSRI Scientific Advisory Council
- 1994–97 AMS Arnold Ross Lectures Committee
- 1993–95 Director, OSU International Mathematical Research Institute
- 1992–94 AMS Central Section Program Committee (chair 1993–94)
- 1989–91 AMS Centennial Fellowship Committee

## Publications

### *Thesis*

On the arithmetic of CM elliptic curves in  $\mathbf{Z}_p$ -extensions. Harvard University, 1981

### *Books*

Euler Systems, *Annals of Mathematics Studies* **147**, 227 + xi pp., Princeton: Princeton University Press (2000).

(edited with B. Conrad) Arithmetic Algebraic Geometry, *IAS/Park City Mathematics Series* **9**, 569 pp., Providence: American Mathematical Society (2001).

### *Papers*

- [1] Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer, *Inventiones math.* **64**, (1981) 455–470.
- [2] Iwasawa theory and elliptic curves: supersingular primes. In: *Journées Arithmétiques 1980*, London Math. Soc. Lect. Notes **56**, Cambridge: Cambridge University Press (1982) 379–383.
- [3] (with A. Wiles) Mordell-Weil groups of elliptic curves over cyclotomic fields. In: *Number Theory related to Fermat's last theorem*, Progress in Math. **26**, Boston: Birkhauser (1982) 237–254.
- [4] Congruences for special values of  $L$ -functions of elliptic curves with complex multiplication, *Inventiones math.* **71** (1983) 339–364.
- [5] Elliptic curves and  $\mathbf{Z}_p$ -extensions, *Compositio math.* **56** (1985) 237–250.
- [6]  $p$ -adic  $L$ -functions and descent on non-CM elliptic curves. In: *Number Theory (proceedings of a conference in Montreal, 1985)*, Canadian Math. Soc. Conf. Proc. **7**, Providence: American Math. Soc. (1987) 405–419.
- [7] Local units, elliptic units, Heegner points, and elliptic curves, *Inventiones math.* **88** (1987) 405–422.
- [8] Descents on elliptic curves with complex multiplication. In: *Séminaire de Théorie des Nombres, Paris 1985-86*, Progress in Math. **71**, Boston: Birkhauser (1988) 165–174.
- [9] Global units and ideal class groups, *Inventiones math.* **89** (1987) 511–526.
- [10] Tate-Shafarevich groups and  $L$ -functions of elliptic curves with complex multiplication, *Inventiones math.* **89** (1987) 527–560.
- [11] Tate-Shafarevich groups of elliptic curves with complex multiplication. In: *Algebraic number theory in honor of K. Iwasawa*, Advanced Studies in Pure Math. **17**, Academic Press (1989) 409–419.
- [12] On the main conjecture of Iwasawa theory for imaginary quadratic fields, . *Inventiones math.* **93** (1988) 701–713

## Publications (continued)

- [13] The work of Kolyvagin on the arithmetic of elliptic curves. In: *Arithmetic of Complex Manifolds*, Barth and Lange, eds. Lecture Notes in Math. **1399**, New York: Springer (1989) 128–136.
- [14] The main conjecture. Appendix to: *Cyclotomic Fields I and II* by S. Lang, Graduate Texts in Math. **121**, New York: Springer (1990) 397–419.
- [15] Kolyvagin’s system of Gauss sums. In: *Arithmetic Algebraic Geometry*, van der Geer, Oort and Steenbrink, eds. Progress in Math. **89**, Boston: Birkhauser (1991) 309–324.
- [16] The one-variable main conjecture for elliptic curves with complex multiplication. In: *L-functions in arithmetic*, London Math. Soc. Lect. Notes **153**, Cambridge University Press (1991) 353–371.
- [17] The “main conjectures” of Iwasawa theory for imaginary quadratic fields, *Inventiones math.* **103** (1991) 25–68.
- [18] Stark units and Kolyvagin’s “Euler systems”, *J. für die reine und angew. Math.* **425** (1992) 141–154.
- [19]  $p$ -adic  $L$ -functions and rational points on elliptic curves with complex multiplication, *Inventiones math.* **107** (1992) 323–350.
- [20]  $p$ -adic variants of the Birch and Swinnerton-Dyer conjecture. In:  $p$ -adic monodromy and the Birch and Swinnerton-Dyer Conjecture, Mazur and Stevens, eds. *Contemporary Mathematics* **165**, Providence: Amer. Math. Soc. (1994) 71–80.
- [21] More “main conjectures” for imaginary quadratic fields. In: *Elliptic curves and related topics*, Kisilevsky and Murty, eds. CRM Proceedings and Lecture Notes **4**, Providence: Amer. Math. Soc. (1994) 23–28.
- [22] Abelian varieties,  $p$ -adic heights and derivatives. In: *Algebra and Number Theory (Essen, December 1992)*, Frey and Ritter, eds. Berlin: de Gruyter (1994) 247–266.
- [23] (with A. Silverberg) A report on Wiles’ Cambridge lectures, *Bull. Amer. Math. Soc.* **31** (1994) 15–38.
- [24] (with A. Silverberg) Families of elliptic curves with constant mod  $p$  representations. In: *Elliptic curves, modular forms, and Fermat’s Last Theorem (Hong Kong, December 1994)*, Coates and Yau, eds. Cambridge: International Press (1995) 148–161.
- [25] A Stark conjecture “over  $\mathbf{Z}$ ” for abelian  $L$ -functions with multiple zeros, *Annales de l’Institut Fourier* **46** (1996) 33–62.
- [26] Euler systems and exact formulas in number theory, *Jahresbericht der Deutschen Math.-Verein.* **98** (1996) 30–39.
- [27] Modularity of mod 5 representations. In: *Modular forms and Fermat’s Last Theorem*, Cornell, Silverman, and Stevens, eds. New York: Springer (1997) 463–474.

## Publications (continued)

- [28] (with B. de Smit and R. Schoof) Criteria for complete intersections. In: *Modular forms and Fermat's Last Theorem*, Cornell, Silverman, and Stevens, eds. New York: Springer (1997) 343–355.
- [29] (with A. Silverberg) Mod 6 representations of elliptic curves. In: *Automorphic forms, automorphic representations, and arithmetic*, Doran, Dau, and Gilbert, eds. Proc. Symp. Pure Math. **66**, Providence: American Math. Soc. (1999) 213–220.
- [30] Euler systems and modular elliptic curves. In: *Galois representations in arithmetic algebraic geometry*, Scholl and Taylor, eds. London Math. Soc. Lect. Notes **254**, Cambridge: Cambridge University Press (1998) 351–367.
- [31] Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. In: *Arithmetic theory of elliptic curves (Cetraro, Italy 1997)*, C. Viola, ed. Lecture Notes in Math. **1716**, New York: Springer (1999) 167–234.
- [32] (with C. Greither, D. Replogle, and A. Srivastav) Swan modules and Hilbert-Speiser number fields, *Journal of Number Theory* **79** (1999) 164–173.
- [33] (with A. Silverberg) Ranks of elliptic curves in families of quadratic twists, *Experimental Mathematics* **9** (2000) 583–590.
- [34] (with A. Silverberg) Mod 2 representations of elliptic curves, *Proc. Amer. Math. Soc.* **129** (2001) 53–57
- [35] (with A. Silverberg) Rank frequencies for quadratic twists of elliptic curves, *Experimental Mathematics* **10** (2001) 559–569.
- [36] (with B. Mazur) Elliptic curves and class field theory. In: *Proceedings of the International Congress of Mathematicians, ICM 2002, Beijing*, Ta Tsien Li, ed., vol. II. Beijing: Higher Education Press (2002) 185–195.
- [37] (with A. Silverberg) Supersingular abelian varieties in cryptology. In: *Advances in Cryptology — CRYPTO 2002*, M. Yung, ed., Lect. Notes in Computer Science **2442**, New York: Springer (2002) 336–353.
- [38] (with A. Silverberg) Ranks of elliptic curves, *Bull. Amer. Math. Soc.* **39** (2002) 455–474.
- [39] (with A. Silverberg) Torus-based cryptography. In: *Advances in Cryptology — CRYPTO 2003*, D. Boneh, ed., Lect. Notes in Computer Science **2729**, New York: Springer (2003) 349–365.
- [40] (with B. Mazur) Studying the growth of Mordell-Weil. In: *Documenta math. Extra Volume: Kazuya Kato's Fiftieth Birthday* (2003) 585–607.
- [41] (with B. Mazur) Kolyvagin systems. *Memoirs of the AMS* **168**, number 799 (2004) 96pp.

## Publications (continued)

- [42] (with B. Mazur) Pairings in the arithmetic of elliptic curves. In: *Modular Curves and Abelian Varieties*, J. Cremona et al., eds., Progress in Math. **224**, Basel: Birkhäuser (2004) 151–163.
- [43] (with R. Pollack) The main conjecture for CM elliptic curves at supersingular primes. *Annals of Mathematics* **159** (2004) 447–464.
- [44] Right triangles and elliptic curves. In: *Mathematical Adventures for Students and Amateurs*, D. Hayes and T. Shubin, eds., Mathematical Assn. of America (2004) 73–80.
- [45] (with B. Mazur) Introduction to Kolyvagin systems. In: *Stark's Conjectures: Recent Work and New Directions*, Contemp. Math. **358**, Providence: Amer. Math. Soc. (2004) 207–221.
- [46] (with A. Silverberg) Algebraic tori in cryptography. In: *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Institute Communications Series **41**, Providence: Amer. Math. Soc. (2004) 317–326.
- [47] (with A. Silverberg) Using primitive subgroups to do more with fewer bits. In: *Algorithmic Number Theory (ANTS VI)*, Lect. Notes in Computer Science **3076**, New York: Springer (2004) 18–41.
- [48] (with M. van Dijk, R. Granger, D. Page, A. Silverberg, M. Stam, and D. Woodruff) Practical cryptography in high dimensional tori. In: *Advances in Cryptology — EUROCRYPT 2005*, R. Cramer, ed., Lect. Notes in Computer Science **3494**, New York: Springer (2005) 234–250.
- [49] (with B. Mazur) Organizing the arithmetic of elliptic curves. *Advances in Mathematics* **198** (2005) 504–546.
- [50] (with B. Mazur) Finding large Selmer groups. *Journal of Differential Geometry* **70** (2005) 1–22.
- [51] Appendix to: Anticyclotomic Iwasawa theory of CM elliptic curves, by A. Agboola and B. Howard. *Annales de l'Institut Fourier* **56** (2006) 1001–1048.
- [52] (with A. Silverberg) Twists of elliptic curves of rank at least four. In: *Ranks of elliptic curves and random matrix theory*, Conrey et al., eds., London Math. Soc. Lect. Notes **341**, Cambridge: Cambridge University Press (2007) 177–188.
- [53] Fudge factors in the Birch and Swinnerton-Dyer conjecture. In: *Ranks of elliptic curves and random matrix theory*, Conrey et al., eds., London Math. Soc. Lect. Notes **341**, Cambridge: Cambridge University Press (2007) 233–236.
- [54] (with B. Mazur and A. Silverberg) Twisting commutative algebraic groups. *Journal of Algebra* **314** (2007) 419–438.

## Publications (continued)

- [55] (with B. Mazur) Finding large Selmer rank via an arithmetic theory of local constants. *Annals of Mathematics* **166** (2007) 579–612.
- [56] (with A. Silverberg) Compression in finite fields and torus-based cryptography. *SIAM Journal on Computing* **37** (2008) 1401–1428.
- [58] (with B. Mazur) Growth of Selmer rank in nonabelian extensions of number fields. *Duke Math. Journal* **143** (2008) 437–461.

### *Preprints*

- [58] (with A. Silverberg) Using abelian varieties to improve pairing-based cryptography. To appear in *Journal of Cryptology*.
- [59] (with A. Silverberg) Point counting on reductions of CM elliptic curves. Submitted.
- [60] (with A. Silverberg) Choosing the correct elliptic curve in the CM method. Submitted.