

BIBLIOGRAPHY

Karl Rubin

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.
- [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] (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.
- [28] Modularity of mod 5 representations. In: *Modular forms and Fermat’s Last Theorem*, Cornell, Silverman, and Stevens, eds. New York: Springer (1997) 463–474.
- [29] 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.
- [30] (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.
- [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 (2002) 349–365.

Preprints (available at <http://math.stanford.edu/~rubin/preprints>)

- [40] (with B. Mazur) Kolyvagin systems. To appear in *Memoirs of the AMS*.
- [41] (with R. Pollack) The main conjecture for CM elliptic curves at supersingular primes. To appear in *Annals of Mathematics*.
- [42] (with B. Mazur) Studying the growth of Mordell-Weil. To appear in *Documenta math.* volume dedicated to K. Kato.
- [43] (with B. Mazur) Introduction to Kolyvagin systems. Submitted.
- [44] (with A. Silverberg) Algebraic tori in cryptography. To appear in *High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Institute Communications Series, American Mathematical Society (2003).
- [45] (with B. Mazur) Pairings in the arithmetic of elliptic curves. To appear in the proceedings of the 2002 Barcelona conference.