MR2270567 (2008c:11146) 11R23 (11G05)
Iovita, Adrian (3-CONC-MS); **Pollack, Robert [Pollack, Robert[2]]** (1-BOST-MS)
Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields. (English summary)
J. Reine Angew. Math. **598** (2006), 71–103.

An elliptic curve E over a number field K is said to be supersingular at a prime p of K if the coefficient $a_p(E)$ is not a unit modulo the residue characteristic of p. Frequently, for instance when the rational prime p splits completely in K and $p > 3$, this means that $a_p(E) = 0$, by the Hasse bound. The present article studies the Iwasawa theory of an elliptic curve at a supersingular prime p along an arbitrary $\mathbf{Z}_p$-extension K_∞ of a number field K in the case where p splits completely in K. The main conjecture of Iwasawa theory relates a p-adic L-function attached to E/K_∞ (defined, typically, by interpolating classical special values of the Hasse-Weil L-series of E/K twisted by various characters of K_∞/K) to the characteristic power series of the (Pontryagin dual of a) Selmer group attached to E/K_∞. In contrast to the ordinary case, in the supersingular setting the p-adic L-function does not belong to the Iwasawa algebra; for instance, when $a_p = 0$, it has infinitely many "trivial zeros" occurring at p-power roots of unity. On the algebraic side, this difficulty is mirrored by the fact that the Selmer group, naively defined as in the ordinary case, is too large to be cotorsion over the Iwasawa algebra. One of the earlier insights of the second author was that one could, in the special case where the coefficient $a_p = 0$, remove the simple factors accounting for these trivial zeroes, and thereby obtain *two distinct* p-adic L-functions called $L_p^+(E/K_\infty)$ and $L_p^-(E/K_\infty)$. On the algebraic side, Kobayashi was able to define corresponding Selmer groups in the case where K_∞ is the cyclotomic $\mathbf{Z}_p$-extension of K, and hence to formulate a main conjecture relating the structure of these Selmer groups to the p-adic L-functions. These modified Selmer groups are defined by imposing more stringent local conditions on the behaviour of the cohomology classes at p. (The so-called "plus and minus conditions".) The resulting Selmer groups can frequently be shown to be cotorsion over the Iwasawa algebra and one thus obtains "algebraic" λ and μ-invariants μ^+, μ^-, λ^+ and λ^- whose behaviour can be related, at least conjecturally, to the analytically defined invariants $L_p^+(E/K_\infty)$ and $L_p^-(E/K_\infty)$. In the case where K_∞ is the cyclotomic $\mathbf{Z}_p$-extension, much of the foundational material needed to flesh out this program was carried out by R. Pollack in [Duke Math. J. **118** (2003), no. 3, 523–558; MR1983040 (2004e:11050)] (on the analytic side) and S. Kobayashi in [Invent. Math. **152** (2003), no. 1, 1–36; MR1965358 (2004b:11153)] (on the algebraic side). To be able to work with arbitrary, not necessarily cyclotomic, $\mathbf{Z}_p$-extensions, the authors prove a new local result that gives a complete description of the formal group of an elliptic curve at a supersingular prime along any ramified $\mathbf{Z}_p$-extension of $\mathbf{Q}_p$. This result represents an important contribution to the general program of studying the Iwasawa theory of elliptic curves in the supersingular setting.

Reviewed by *Henri Darmon*

References

1. *A. Agboola* and *B. Howard*, Anticyclotomic Iwasawa theory of CM elliptic curves II, preprint. cf. MR 2006i:11127
2. *C. Cornut*, Mazur's conjecture on higher Heegner points, Invent. Math. **148** (2002), no. 3, 495–523. MR1908058 (2004e:11069a)
3. *R. Greenberg*, Introduction to Iwasawa theory for elliptic curves, in: Arithmetic algebraic geometry (Park City, UT, 1999), Amer. Math. Soc., Providence, RI (2001), 407–464. MR1860044 (2003a:11067)
4. *R. Greenberg*, Iwasawa theory for elliptic curves, in: Arithmetic theory of elliptic curves (Cetraro 1997), Lect. Notes Math. **1716**, Springer, Berlin (1999), 51–144. MR1754686 (2002a:11056)
5. *R. Greenberg*, Iwasawa theory for p-adic representations, in: Algebraic number theory, Adv. Stud. Pure Math. **17**, Academic Press, Boston, MA, 1989. MR1097613 (92c:11116)
6. *R. Greenberg*, Iwasawa theory for p-adic representations II, preprint. cf. MR 92c:11116
7. *R. Greenberg*, On the Birch and Swinnerton-Dyer conjecture, Invent. Math. **72** (1983), 241–265. MR0700770 (85c:11052)
8. *M. Hazewinkel*, On norm maps for one dimensional formal groups. III, Duke Math. J. **44** (1977), no. 2, 305–314. MR0439851 (55 #12733)
9. *K. Kato*, p-adic Hodge theory and values of zeta functions of modular forms, preprint. cf. MR 2006b:11051
10. *S. Kobayashi*, Iwasawa theory for elliptic curves at supersingular primes, Invent. Math. **152** (2003), no. 1, 1–36. MR1965358 (2004b:11153)
11. *M. Kurihara*, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, Invent. Math. **149** (2002), 195–224. MR1914621 (2003f:11078)
12. *B. Mazur*, Rational points of abelian varieties with values in towers of number fields, Invent. Math. **18** (1972), 183–266. MR0444670 (56 #3020)
13. *B. Mazur*, *J. Tate* and *J. Teitelbaum*, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. Math. **84** (1986), no. 1, 1–48. MR0830037 (87e:11076)
14. *B. Perrin-Riou*, Théorie d'Iwasawa p-adique locale et globale, Invent. Math. **99** (1990), no. 2, 247–292. MR1031902 (91b:11116)
15. *B. Perrin-Riou*, Fonctions Lp-adiques d'une courbe elliptique et points rationnels, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 945–995. MR1252935 (95d:11081)
16. *B. Perrin-Riou*, Théorie d'Iwasawa des représentations p-adiques sur un corps local, Invent. Math. **115** (1994), no. 1, 81–161. MR1248080 (95c:11082)
17. *B. Perrin-Riou*, Arithmétique des courbes elliptiques á réduction supersingulière en p, Experiment. Math. **12** (2003), no. 2, 155–186. MR2016704 (2005h:11138)
18. *R. Pollack*, On the p-adic L-function of a modular form at a supersingular prime, Duke Math. J. **118** (2003), no. 3, 523–558. MR1983040 (2004e:11050)
19. *R. Pollack*, An algebraic version of a theorem of Kurihara, J. Number Th. **110** (2005), no. 1, 164–177. MR2114679 (2005m:11105)
20. *K. Rubin*, Euler systems, Ann. Math. Stud. **147**, Princeton Univ. Press, Princeton, NJ, 2000.
21. *P. Schneider*, p-adic height pairings. II, Invent. Math. **79** (1985), no. 2, 329–374. MR0778132

(86j:11063)
22. *J. H. Silverman*, The arithmetic of elliptic curves, Corrected reprint of the 1986 original, Springer, New York 1992. MR1329092 (95m:11054)
23. *J. Tate*, Duality theorems in Galois cohomology over number fields, Proc. Internat. Congr. Mathematicians (Stockholm 1962), Inst. Mittag-Leffler, Djursholm (1963), 288–295. MR0175892 (31 #168)
24. *V. Vatsal*, Uniform distribution of Heegner points, Invent. Math. **148** (2002), no. 1, 1–46. MR1892842 (2003j:11070)
25. *V. Vatsal*, Special values of anticyclotomic L-functions, Duke Math. J. **116** (2003), no. 2, 219–261. MR1953292 (2004e:11069b)
26. *K. Wingberg*, Duality theorems for abelian varieties over $\mathbb{Z}_p$-extensions, in: Algebraic number theory, Adv. Stud. Pure Math. **17**, Academic Press, Boston, MA (1989), 471–492. MR1097629 (92h:11052)

Note: This list reflects references listed in the original paper as accurately as possible with no attempt to correct errors.