AMERICAN MATHEMATICAL SOCIETY
MathSciNet Mathematical Reviews on the Web

Previous | Up | Next Article

Citations
From References: 2
From Reviews: 1

MR2052361 (2005g:11097) 11G05 (11G15 11R23)

Pollack, Robert [Pollack, Robert^2] (1-CHI); **Rubin, Karl** (1-STF)

The main conjecture for CM elliptic curves at supersingular primes. (English summary)

Ann. of Math. (2) **159** (2004), *no. 1,* 447–464.

In this paper, the authors prove the main conjecture for a CM elliptic curve E defined over $\mathbb{Q}$ at any prime $p > 3$ of supersingular reduction. This result has important consequence for the Birch and Swinnerton-Dyer (BSD) conjecture for E. In particular, it follows from the authors' work that if the Hasse-Weil L-function of E vanishes at 1, then $E(\mathbb{Q})$ is finite and the Tate-Shafarevich group $\text{Ш}(E)(\mathbb{Q})$ is also finite, and of order as predicted by the BSD conjecture.

The main conjecture for an elliptic curve E at a prime p of ordinary reduction was formulated by Mazur in the 1970's. The conjecture relates an algebraic object to an analytic object, both associated with the curve. The algebraic object is the Selmer group $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$, which contains information about the arithmetic of E over subfields of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. The corresponding analytic object is a p-adic L-function $\mathcal{L}_E$ that interpolates the values of the L-function of E, and is an element of the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$. The main conjecture in the ordinary case states that the characteristic ideal of the torsion Λ-module $\mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$ is generated by the p-adic L-function $\mathcal{L}_E$. This was proved by the second author [Invent. Math. **103** (1991), no. 1, 25–68; MR1079839 (92f:11151)] when E has complex multiplication. In the case of ordinary reduction, Kato's work implies one-half of the main conjecture, namely that the characteristic ideal contains the p-adic L-function.

However, it was difficult even to formulate the main conjecture at a prime p of supersingular reduction in an analogous way. On the algebraic side, the Selmer group was too big, i.e., $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ was not co-torsion over Λ, and hence one could not talk about a characteristic ideal. On the analytic side, the p-adic L-function $\mathcal{L}_E$ was no longer an element of Λ. The first author [Duke Math. J. **118** (2003), no. 3, 523–558; MR1983040 (2004e:11050)] removed the obstacle on the analytic side by introducing two modified p-adic L-functions $\mathcal{L}_E^\pm$ which are elements of Λ, and which still retain nice interpolation properties. On the algebraic side, S. Kobayashi [Invent. Math. **152** (2003), no. 1, 1–36; MR1965358 (2004b:11153)] introduced two modified Selmer groups $\mathrm{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_\infty)$, which are co-torsion over Λ. Kobayashi conjectured that the characteristic ideal of the modified Selmer group $\mathrm{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_\infty)$ is generated by Pollack's p-adic L-function $\mathcal{L}_E^\pm$. Kobayashi showed that his formulation of the main conjecture is equivalent to that of Perrin-Riou and of Kato. He even showed that the characteristic ideal contains $\mathcal{L}_E^\pm$, exploiting Kato's work.

In order to prove Kobayashi's version of the conjecture in the CM case, the authors obtain an exact sequence

$$0 \to \mathcal{E}/\mathcal{C} \to \mathcal{U}/(\mathcal{C}+\mathcal{V}^\pm) \to \mathcal{X}/\mathrm{image}(\mathcal{V}^\pm) \to \mathcal{A} \to 0,$$

which originates from class field theory. Here, $\mathcal{U}$, $\mathcal{E}$, and $\mathcal{C}$ are respectively the inverse limits of the local units, global units, and elliptic units in the tower of abelian extensions $K(E[p^n])$ (K is the field of complex multiplication of E), and $\mathcal{X}$ (respectively $\mathcal{A}$) is the Galois group of the maximal abelian p-extension unramified outside p (resp. everywhere unramified) over $K(E[p^\infty])$. The module $\mathcal{V}^\pm$ above is closely related to Kobayashi's Selmer groups. By an argument of the second author [op. cit.] involving Euler systems, $\mathcal{E}/\mathcal{C}$ and $\mathcal{A}$ have the same characteristic ideal in the relevant Iwasawa algebra $\tilde{\Lambda}$. The authors prove that the two modules in the middle of the above exact sequence are torsion over $\tilde{\Lambda}$, hence they must have the same characteristic ideal in $\tilde{\Lambda}$. The authors then deduce a similar result by descending to $\mathbb{Q}_\infty$. Finally, results of A. Wiles [Ann. Math. (2) **107** (1978), no. 2, 235–254; MR0480442 (58 #605)], J. Coates and Wiles [Invent. Math. **39** (1977), no. 3, 223–251; MR0463176 (57 #3134)] and Kobayashi [op. cit.] are used as ingredients to relate the module $\mathcal{U}/(\mathcal{C}+\mathcal{V}^\pm)$ to the p-adic L-function $\mathcal{L}_E^\pm$.

Reviewed by *Anupam Saikia*

References

1. Y. Amice and J. V'elu, Distributions *p*-adiques associ'ees aux s'eries de Hecke, in *Journ' ees Arithm'etiques de Bordeaux* (*Univ. Bordeaux*, *Bordeaux*, 1974) 119–131, *Ast'erisque* **24-25**, Soc. Math. France, Paris, 1975. MR0376534 (51 #12709)
2. J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math*. **39** (1977) 223–251. MR0463176 (57 #3134)
3. R. Greenberg, On the structure of certain Galois groups, *Invent. Math*. **47** (1978) 85–99. MR0504453 (80b:12007)
4. K. Kato, *p*-adic Hodge theory and values of zeta functions of modular forms, preprint. cf. MR 2006b:11051
5. S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, *Invent. Math*. **152** (2003) 1–36. MR1965358 (2004b:11153)
6. B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Invent. Math*. **18** (1972) 183–266. MR0444670 (56 #3020)
7. B. Mazur and P. Swinnerton-Dyer, Arithmetic of Weil curves, *Invent. Math*. **25** (1974) 1–61. MR0354674 (50 #7152)
8. B. Mazur, J. Tate, and J. Teitelbaum, On *p*-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. Math*. **84** (1986) 1–48. MR0830037 (87e:11076)
9. B. Perrin-Riou, Arithm'etique des courbes elliptiques te th'eorie d'Iwasawa, *Bull. Soc. Math. France Suppl*. M'emoire **17** (1984).
10. , Th'eorie d'Iwasawa *p*-adique locale et globale, *Invent. Math*. **99** (1990), 247– 292. MR1031902 (91b:11116)
11. , Fonctions *L* *p*-adiques d'une courbe elliptique et points rationnels, *Ann. Inst. Fourier* **43** (1993) 945–995. MR1252935 (95d:11081)
12. R. Pollack, On the *p*-adic *L*-function of a modular form at a supersingular prime, *Duke Math. J*. **118** (2003), 523–558. MR1983040 (2004e:11050)
13. D. Rohrlich, On *L*-functions of elliptic curves and cyclotomic towers, *Invent. Math*. **75** (1984) 409–423. MR0735333 (86g:11038b)
14. K. Rubin, Elliptic curves and **Z***p*-extensions, *Compositio Math*. **56** (1985) 237–250. MR0809869 (87h:11059)
15. , Local units, ellitpic units, Heegner points, and elliptic curves, *Invent. Math*. **88** (1987) 405–

422. MR0880958 (89h:11069)

16. , The “main conjectures” of Iwasawa theory for imgainray quadratic fields, *Invent. Math.* **103** (1991) 25–68. MR1079839 (92f:11151)

17. A. Wiles, Higher explicit reciprocity laws, *Ann. of Math.* **107** (1978) 235–254.(Received November 14, 2002) MR0480442 (58 #605)

Note: This list, extracted from the PDF form of the original paper, may contain data conversion errors, almost all limited to the mathematical expressions.

© *Copyright American Mathematical Society 2005, 2006*