Extending Kato's result to elliptic curves with p-isogenies

Christian Wuthrich

13th January 2006

Abstract

Let E be an elliptic curve without complex multiplication defined over $\mathbb{Q}$ and let p be an odd prime number at which E has good and ordinary reduction. Kato has proved in [Kat04] the first half of the main conjecture for E under the condition that the representation $\rho_p\colon G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(T_pE)$ of the absolute Galois group of $\mathbb{Q}$ attached to the Tate module T_pE is surjective. We prove here that the result still holds if the E admits an isogeny of degree p. As a by-product, we show that the p-adic L-functions attached to an elliptic curve with good ordinary reduction at p is always an integral series.11G05, 11G40, 11R23, 11F67

1 Introduction

Let E be an elliptic curve without complex multiplication defined over $\mathbb{Q}$ and let $p > 2$ be a prime number. Suppose that E has good ordinary reduction at p. We denote by $\rho_p\colon G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(T_pE)$ the representation of the absolute Galois group of $\mathbb{Q}$ attached to the Tate module T_pE.

Let E_{p^∞} be the group of all points on E whose order is a power of p. Let ${}_\infty\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension and ${}_n\mathbb{Q}$ its n-th layer. The Selmer group of E is defined as the kernel of the map

$$\mathcal{S}(E/{}_n\mathbb{Q}) = \ker\bigl(\mathrm{H}^1({}_n\mathbb{Q}, E_{p^\infty}) \longrightarrow \prod_v \mathrm{H}^1({}_n\mathbb{Q}_v, E)\bigr),$$

where the product runs over all places v in ${}_n\mathbb{Q}$. The Pontryagin dual of the direct limit of these groups under the restriction maps

$$X(E/{}_\infty\mathbb{Q}) = \mathrm{Hom}\bigl(\varinjlim \mathcal{S}(E/{}_n\mathbb{Q}), {}^{\mathbb{Q}_p}\!/\!_{\mathbb{Z}_p}\bigr)$$

has naturally the structure of a finitely generated Λ-module, if Λ denotes the Iwasawa algebra of the $\mathbb{Z}_p$-extension ${}_\infty\mathbb{Q}/\mathbb{Q}$. By Theorem 17.4 of [Kat04], we know that $X(E/{}_\infty\mathbb{Q})$ is Λ-torsion. The characteristic ideal $\mathrm{char}_\Lambda(X(E/{}_\infty\mathbb{Q}))$ in Λ is an important algebraic object attached to E and p.

On the analytic side, Mazur and Swinnerton-Dyer have constructed in [MSD74] a p-adic L-function $\mathcal{L}_p(E/\mathbb{Q}, T)$ in $\Lambda \otimes \mathbb{Q}_p$. See section 3 for more details. It was conjectured that this series has integral coefficients. We will prove the following extension of Proposition 3.7 in [GV00].

Theorem 5.
The analytic p-adic L-function $\mathcal{L}_p(E/\mathbb{Q}, T)$ belongs to Λ for all elliptic curves $E/\mathbb{Q}$ with good ordinary reduction at $p > 2$.

The conclusion can certainly not be extended to the supersingular case since the p-adic L-functions in this case will never be integral. The supersingular case is well explained in [Pol03] where it is shown how one can extract integral power series.

The main conjecture asserts that the element $\mathcal{L}_p(E/\mathbb{Q},T)$ generates the characteristic ideal $\mathrm{char}_\Lambda(X(E/_\infty\mathbb{Q}))$. Kato has proved in [Kat04] the first half of the main conjecture under the assumption that the representation ρ_p is surjective. Our aim is to extend his result to curves where the $G_\mathbb{Q}$-module $E[p]$ is reducible.

Theorem 4.
Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let $p > 2$ be a prime. Suppose that E has good ordinary reduction at p and that the representation ρ_p is either surjective or that $E[p]$ is reducible. Then $\mathrm{char}_\Lambda(X(E/_\infty\mathbb{Q}))$ divides the ideal generated by $\mathcal{L}_p(E/\mathbb{Q},T)$.

The same argument does not extend to the remaining cases; for them we only obtain a conditional result. See Proposition 7.

In special cases, Greenberg and Vatsal have proved in [GV00] the full main conjecture. Namely if the E admits an isogeny of degree p whose kernel is either ramified at p and odd or unramified at p and even.

The paper consists of two parts. The first part concerns tha so-called fine Selmer group. The existence of Kato's Euler system gives directly a bound on this group. We use a result of Coates and Sujatha in [CS05] to strengthen the usual bound.

The second part transfers the bound from the fine Selmer group to the Selmer group using global duality. The proof of theorem 4 is first done on the so-called optimal curve where one knows already that the p-adic L-function is integral.

The author wishes to thank John Coates, Robert Pollack, and Karl Rubin for helpful discussions.

2 The fine Selmer group

Let E be an elliptic curve defined over $\mathbb{Q}$ and let p be any odd prime. We define the fine[1] Selmer group to be the subgroup of $\mathcal{S}(E/_n\mathbb{Q})$ defined by imposing stronger conditions at the completion $_n\mathbb{Q}_\mathfrak{p}$ of $_n\mathbb{Q}$ at the unique prime $\mathfrak{p}$ above p :

$$0 \longrightarrow \mathcal{R}(E/_n\mathbb{Q}) \longrightarrow \mathcal{S}(E/_n\mathbb{Q}) \longrightarrow \mathrm{H}^1(_n\mathbb{Q}_\mathfrak{p}, E_{p^\infty})$$

The dual of the direct limit of the groups $\mathcal{R}(E/_n\mathbb{Q})$ will be denoted by $Y(E/_\infty\mathbb{Q})$; it is again a finitely generated Λ-module. Theorem 12.4.1 in [Kat04] proves that $Y(E/_\infty\mathbb{Q})$ is Λ-torsion. Denote by $\mathrm{char}_\Lambda(Y(E/_\infty\mathbb{Q}))$ the characteristic ideal of $Y(E/_\infty\mathbb{Q})$ in Λ.

Kato constructs an Euler system $\mathbf{c}$ attached to E and p. This is a collection of cohomology classes $\mathbf{c}_K \in H^1(K, T_pE)$ for sufficiently many abelian extensions K of $\mathbb{Q}$, including $K = \mathbb{Q}(\mu[p^k])$ for all $k \geqslant 0$. The norm compatibility imposed on an Euler system, provides us with an element $_\infty\mathbf{c}$ in the projective limit

$$_\infty\mathbf{c} \in \varprojlim_n \mathrm{H}^1(_n\mathbb{Q}, T_pE) = {}_\infty\mathrm{H}^1(\mathbb{Q}, T_pE)$$

where the limit follows the corestriction map. We also recall that $_\infty\mathrm{H}^1(\mathbb{Q}, T_pE)$ is a Λ-module of rank 1. The ideal

$$\mathrm{ind}_\Lambda(_\infty\mathbf{c}) = \{\phi(_\infty\mathbf{c}) \mid \phi \in \mathrm{Hom}_\Lambda(_\infty\mathrm{H}^1(\mathbb{Q}, T_pE), \Lambda)\}$$

in Λ measures the Λ-divisibility of $_\infty\mathbf{c}$ in $_\infty\mathrm{H}^1(\mathbb{Q}, T_pE)$.

Lemma 1. *Let E be an elliptic curve and p an odd prime such that E admits an isogeny of degree p. Then the fine Selmer group $Y(E/_\infty\mathbb{Q})$ is a finitely generated $\mathbb{Z}_p$-module, i.e. its μ-invariant vanishes.*

[1] This group is sometimes called the "strict" or "restricted" Selmer group.

Proof. The extension K of $\mathbb{Q}$ fixed by the kernel of $\rho_\phi \colon G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[\phi])$ is a cyclic extension of degree dividing $p-1$. Let Δ be the Galois group of $K/\mathbb{Q}$. Over the abelian field K, the curve admits a p-torsion point. We can therefore apply Corollary 3.6 in [CS05] (a consequence of the theorem of Ferrero-Washington) to $Y(E/{}_\infty K)$ where ${}_\infty K$ is the cyclotomic $\mathbb{Z}_p$-extension of K. This proves that $Y(E/{}_\infty K)$ is a finitely generated $\mathbb{Z}_p$-module. Write $\mathcal{R}(E/{}_\infty\mathbb{Q})$ and $\mathcal{R}(E/{}_\infty K)$ for the dual of $Y(E/{}_\infty\mathbb{Q})$ and $Y(E/{}_\infty K)$ respectively. Then we have the following diagram

$$\begin{array}{ccccc}
0 & \longrightarrow & \mathcal{R}(E/{}_\infty K)^\Delta & \longrightarrow & \mathrm{H}^1({}_\infty K, E_{p^\infty})^\Delta \\
 & & \uparrow & & \uparrow \\
0 & \longrightarrow & \mathcal{R}(E/{}_\infty\mathbb{Q}) & \longrightarrow & \mathrm{H}^1({}_\infty\mathbb{Q}, E_{p^\infty}) \\
 & & & & \uparrow \\
 & & & & \mathrm{H}^1(\Delta, E({}_\infty K)_{p^\infty})
\end{array}$$

and since the group Δ is of order prime to p, the kernel on the right is trivial. We deduce that the left hand side is injective, too, and hence that the dual map $Y(E/{}_\infty K) \longrightarrow Y(E/{}_\infty\mathbb{Q})$ is surjective. Therefore $Y(E/{}_\infty\mathbb{Q})$ is a finitely generated $\mathbb{Z}_p$-module. ☐

Theorem 2.
If $E/\mathbb{Q}$ is an elliptic curve without complex multiplication and $p > 2$ a prime such that the presentation $\rho_p \colon G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(T_pE)$ is either surjective or that $E[p]$ is reducible then $\mathrm{char}_\Lambda(Y(E/{}_\infty\mathbb{Q}))$ divides $\mathrm{ind}_\Lambda({}_\infty\mathbf{c})$.

Proof. If we are in the surjective case, then the theorem is a known consequence of Kato's Euler system. See Theorem 2.3.3 and Proposition 3.5.8 in [Rub00]. In the latter case when ρ_p is not surjective, we know that there exists an isogeny $\phi \colon E \longrightarrow E'$ of degree p defined over $\mathbb{Q}$. The Euler system argument gives us only a divisibility of the form

$$\mathrm{char}_\Lambda(Y(E/{}_\infty\mathbb{Q})) \bigm| p^t \cdot \mathrm{ind}_\Lambda({}_\infty\mathbf{c})$$

for some integer $t \geqslant 0$, see Theorem 2.3.4 in [Rub00]. The previous lemma shows now that $\mathrm{char}_\Lambda(Y(E/{}_\infty\mathbb{Q}))$ is not divisible by p and hence we can take t to be equal to 0. ☐

3 The Selmer group

Suppose now that the curve E has good and ordinary reduction at the odd prime p. It is known that there exists an element $\mathcal{L}_p(E/\mathbb{Q}, T) \in \Lambda \otimes \mathbb{Q}_p$, called the analytic p-adic L-function, which interpolates in a certain precise way the Hasse-Weil L-function associated to E which we are going to recall now. Let γ be a topological generator of $\Gamma = \mathrm{Gal}({}_\infty\mathbb{Q}/\mathbb{Q})$. Let $\chi \colon \Gamma \longrightarrow \mu_{p^\infty}$ be a Dirichlet character of conductor p^{k+1}. It is determined by its image $\chi(\gamma) = \zeta$ which is a primitive root of unity of order p^k. Then $\mathcal{L}_p(E/\mathbb{Q}, T)$ is characterised by

$$\mathcal{L}_p(E/\mathbb{Q}, \zeta - 1) = \frac{1}{\alpha^{k+1}} \cdot \frac{p^{k+1}}{\tau(\chi^{-1})} \cdot \cdot \frac{L_E(\chi^{-1}, 1)}{\Omega_E}. \tag{1}$$

Here $\tau(\chi^{-1})$ is the usual Gauss sum and α is the unit root of the characteristic polynomial of Frobenius acting on T_pE. The real Néron period of E is denoted by Ω_E and $L_E(\chi^{-1}, s)$ is the Hasse-Weil L-function attached to E twisted by the character χ^{-1}.

We recall from [Ste89] that an elliptic curve $E/\mathbb{Q}$ is called *optimal* among the curves in the isogeny class of E if the map $\varphi^* \colon \mathrm{Pic}^0(E) \longrightarrow \mathrm{Pic}^0(X_1(N))$ induced by the modular parametrisation $\varphi \colon X_1(N) \longrightarrow E$ is injective. It is conjectured that the optimal curve is a curve with minimal analytic μ-invariant. It is also conjectured that the μ-invariant of the optimal curve is zero. Greenberg and Vatsal have shown in Proposition 3.7 of [GV00] that the p-adic L-series of an optimal curve is integral, i.e. $\mathcal{L}_p(E/\mathbb{Q},T) \in \Lambda$.

Lemma 3. *Let $p > 2$ be a prime. Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication with good ordinary reduction at p and such that $E[p]$ is reducible. Suppose E is the optimal curve in the isogeny class. Then $\mathrm{char}_\Lambda(X(E/{}_\infty\mathbb{Q}))$ divides the ideal $\mathcal{L}_p(E/\mathbb{Q},T)\cdot\Lambda$.*

Proof. We follow the proof of Theorem 2.3.8 in [Rub00].

Let ${}_\infty\mathbb{Q}_\mathfrak{p}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$. Define the singular local cohomology group $Z(E/{}_\infty\mathbb{Q}) = {}_\infty\mathrm{H}^1_s(\mathbb{Q}_p, T_pE)$ to be the dual of $E({}_\infty\mathbb{Q}_\mathfrak{p})\otimes\mathbb{Q}_p/\mathbb{Z}_p$. It is a Λ-module of rank 1. By global duality (see Proposition 1.3.2 in [PR95]), we have the following exact sequence

$$0 \longleftarrow Y(E/{}_\infty\mathbb{Q}) \longleftarrow X(E/{}_\infty\mathbb{Q}) \longleftarrow Z(E/{}_\infty\mathbb{Q}) \longleftarrow {}_\infty\mathrm{H}^1(\mathbb{Q},T_pE) \longleftarrow 0. \quad (2)$$

Write ${}_\infty\mathbf{c}_s$ for the image of ${}_\infty\mathbf{c}$ in $Z(E/{}_\infty\mathbb{Q})$. Theorem 16.6.2 in [Kat04] states that the image of ${}_\infty\mathbf{c}_s$ via the Perrin-Riou–Coleman map $\mathrm{Col}\colon Z(E/{}_\infty\mathbb{Q}) \rightarrowtail \Lambda$ is up to a p-adic unit the analytic p-adic L-function $\mathcal{L}_p(E/\mathbb{Q},T)$. Here we use that Greenberg and Vatsal [GV00, Theorem 3.1] have shown that the canonical period associated to the newform corresponding to E differs from Ω_E by a p-adic unit, if E is the optimal curve.

Rohrlich [Roh84] has shown that $\mathcal{L}_p(E/\mathbb{Q},T)$ is non-zero. Hence ${}_\infty\mathbf{c}_s$ is not torsion and the characteristic ideal of the Λ-torsion module $Z(E/{}_\infty\mathbb{Q})/{}_\infty\mathbf{c}_s\Lambda$, which is equal to $\mathrm{Col}(Z(E/{}_\infty\mathbb{Q}))/\mathcal{L}_p(E/\mathbb{Q},T)\,\Lambda$ contains $\mathcal{L}_p(E/\mathbb{Q},T)\,\Lambda$.

The sequence (2) induces an exact sequence of Λ-modules

$$0 \longleftarrow Y(E/{}_\infty\mathbb{Q}) \longleftarrow X(E/{}_\infty\mathbb{Q}) \longleftarrow \frac{Z(E/{}_\infty\mathbb{Q})}{{}_\infty\mathbf{c}_s\Lambda} \longleftarrow \frac{{}_\infty\mathrm{H}^1(\mathbb{Q},T_pE)}{{}_\infty\mathbf{c}\,\Lambda}$$

in which all terms are known to be torsion Λ-modules. We know that ${}_\infty\mathrm{H}^1(\mathbb{Q},T_pE)$ is a Λ-module of rank 1 and hence there is a Λ-morphism ψ from ${}_\infty\mathrm{H}^1(\mathbb{Q},T_pE)$ to Λ whose kernel is Λ-torsion and whose cokernel is pseudo-null. Since ${}_\infty\mathbf{c}$ cannot be torsion, the quotient on the right hand side of the above sequence is Λ-torsion and its characteristic ideal is contained in $\psi({}_\infty\mathbf{c})\,\Lambda$. The latter is contained in $\mathrm{ind}_\Lambda({}_\infty\mathbf{c})$.

So, using theorem 2, we conclude that

$$\begin{aligned}\mathrm{char}_\Lambda(X(E/{}_\infty\mathbb{Q})) &\supset \mathrm{char}_\Lambda(Y(E/{}_\infty\mathbb{Q}))\cdot\mathrm{char}_\Lambda\Big(\frac{Z(E/{}_\infty\mathbb{Q})}{{}_\infty\mathbf{c}_s\Lambda}\Big)\cdot\mathrm{char}_\Lambda\Big(\frac{{}_\infty\mathrm{H}^1(\mathbb{Q},T_pE)}{{}_\infty\mathbf{c}\,\Lambda}\Big)^{-1}\\ &\supset \mathrm{ind}_\Lambda({}_\infty\mathbf{c})\cdot\mathcal{L}_p(E/\mathbb{Q},T)\,\Lambda\cdot\big(\mathrm{ind}_\Lambda({}_\infty\mathbf{c})\big)^{-1}\\ &\supset \mathcal{L}_p(E/\mathbb{Q},T)\,\Lambda\end{aligned}$$

□

Theorem 4.
Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let $p > 2$ be a prime. Suppose that E has good ordinary reduction at p and that the representation ρ_p is either surjective or that $E[p]$ is reducible. Then $\mathrm{char}_\Lambda(X(E/{}_\infty\mathbb{Q}))$ divides the ideal generated by $\mathcal{L}_p(E/\mathbb{Q},T)$.

Proof. If the representation ρ_p is surjective, then this is Theorem 17.4. of Kato [Kat04].

Suppose now that $E[p]$ is reducible. Then there is an isogeny ϕ from E to the optimal curve E^{opt} in the isogeny class of E. Note that (1) and the formula for the change of the μ-invariant by Perrin-Riou [PR87, Appendice] show that the statement that $\mathrm{char}_\Lambda(X(E/{}_\infty\mathbb{Q}))$ contains $\mathcal{L}_p(E/\mathbb{Q},T)\,\Lambda$ is invariant under isogeny. So the conclusion drawn for E^{opt} in the previous lemma applies also to E. □

Theorem 5.
The analytic p-adic L-function $\mathcal{L}_p(E/\mathbb{Q}, T)$ *belongs to* Λ *for all elliptic curves* $E/\mathbb{Q}$ *with good ordinary reduction at* $p > 2$.

Proof. If the elliptic curve E admits no isogenies of degree dividing p this is well-known by [GV00, Proposition 3.7]. If this is not the case, then $E[p]$ is reducible and we have seen in the previous theorem 4 that the ideal generated by $\mathcal{L}_p(E/\mathbb{Q}, T)$ is divisible by an integral ideal $\mathrm{char}_\Lambda(X(E/_\infty\mathbb{Q}))$. □

Corollary 6. *If* $E/\mathbb{Q}$ *is a semi-stable elliptic curve and* $p > 3$ *a prime of good ordinary reduction, then* $\mathrm{char}_\Lambda(X(E/_\infty\mathbb{Q}))$ *divides the ideal generated by* $\mathcal{L}_p(E/\mathbb{Q}, T)$.

Proof. By a theorem of Serre ([Ser96, Proposition 1] and [Ser72, Proposition 21]), we know that the image of the representation $\bar{\rho}_p\colon G_\mathbb{Q} \longrightarrow \mathrm{Aut}(E[p])$ is either the whole of $\mathrm{GL}_2(\mathbb{F}_p)$ or it is contained in a Borel subgroup. In the latter case the representation ρ_p is reducible and in the first case the representation $\rho_p\colon G_\mathbb{Q} \longrightarrow \mathrm{Aut}(T_pE)$ is surjective by another result of Serre [Ser81, Lemme 15]. □

Unfortunately, the hypothesis that E is semi-stable can not be dropped. There are curves $E/\mathbb{Q}$ such that $\bar{\rho}_p$ has its image in the normaliser of a Cartan subgroup. In this case there are no p-torsion points defined over an abelian extension of $\mathbb{Q}$. Similar there are also curves without complex multiplications for $p = 5$ such that the image of ρ_5 maps to the exceptional subgroup S_4 in $\mathrm{PGL}(\mathbb{F}_5)$.

The methods in this article are not sufficient to extend the main theorem 4 to these cases. The best we can do is the following

Proposition 7. *Let* $E/\mathbb{Q}$ *be an elliptic curve without complex multiplication, with good and ordinary reduction at* $p > 13$ *or* $p = 7$. *If the conjecture of Iwasawa on the vanishing of the classical* μ*-invariant in cyclotomic* $\mathbb{Z}_p$*-extensions is valid for abelian extensions of imaginary quadratic fields, then* $\mathrm{char}_\Lambda(X(E/_\infty\mathbb{Q}))$ *divides the ideal generated by* $\mathcal{L}_p(E/\mathbb{Q}, T)$.

Proof. By theorem 4, we may assume that the image of $\bar{\rho}_p$ is contained in the normaliser of a Cartan subgroup. The case of the exceptional subgroups is excluded by the hypothesis on p by Lemme 18 in [Ser81].

The idea of the proof is the same as for the proofs of Theorem 2 and Theorem 4, but we replace the Corollary 3.6 in [CS05] by the previous Corollary 3.5 with L being the field $\mathbb{Q}(E[p])$. In our case L is an abelian extension of an imaginary quadratic field. □

References

[CS05] John Coates and Ramdorai Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. **331** (2005), no. 4, 809 – 839.

[GV00] Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63.

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et application arithmétiques. III, Astérisque, vol. 295, Société Mathématique de France, Paris, 2004.

[MSD74] Barry Mazur and Peter Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

[Pol03] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558.

[PR87] Bernadette Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456.

[PR95] ———, *Fonctions L p-adiques des représentations p-adiques*, Astérisque (1995), no. 229, 198.

[Roh84] David E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), no. 3, 409–423.

[Rub00] Karl Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study.

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401.

[Ser96] ———, *Travaux de Wiles (et Taylor, ...). I*, Astérisque (1996), no. 237, Exp. No. 803, 5, 319–332, Séminaire Bourbaki, Vol. 1994/95.

[Ste89] Glenn Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. **98** (1989), no. 1, 75–106.