On the Integrality of Modular Symbols and Kato's Euler System for Elliptic Curves

Christian Wuthrich[1]

Received: April 29, 2013
Revised: February 17, 2014

Communicated by Otmar Venjakob

Abstract. Let $E/\mathbb{Q}$ be an elliptic curve. We investigate the denominator of the modular symbols attached to E. We show that one can change the curve in its isogeny class to make these denominators coprime to any given odd prime of semi-stable reduction. This has applications to the integrality of Kato's Euler system and the main conjecture in Iwasawa theory for elliptic curves.

2000 Mathematics Subject Classification: 11G05, 11F67, 11G40, 11R23, 11G16.
Keywords and Phrases: Elliptic Curves, modular symbols, Kato's Euler system

1 Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. Integrating a Néron differential ω_E against all elements in $H_1\bigl(E(\mathbb{C}),\mathbb{Z}\bigr)$, we obtain the Néron lattice $\mathscr{L}_E$ of E in $\mathbb{C}$. For any $r\in\mathbb{Q}$, define $\lambda(r)=2\pi i\int_{\infty}^{r} f(\tau)d\tau$ where f is the newform associated to the isogeny class of E. A theorem by Manin [12] and Drinfeld [7] shows that the values $\lambda(r)$ are commensurable with $\mathscr{L}_E$. In other words, if Ω_E^+ and Ω_E^- are the minimal absolute values of non-zero elements in $\mathscr{L}_E$ on the real and the imaginary axis respectively, then

$$\lambda(r)=2\pi i\int_{\infty}^{r} f(\tau)d\tau=[r]_E^+\cdot\Omega_E^+ + [r]_E^-\cdot\Omega_E^-\cdot i$$

for two rational numbers $[r]_E^\pm$, which we will call the modular symbols of E.

[1]The author was supported by the EPSRC grant EP/G022003/1

The first aim of this paper is to improve on the bound for the denominator of $[r]^{\pm}_{E}$ given by the Theorem of Manin and Drinfeld. It is not true in general that $[r]^{\pm}_{E}$ is an integer for all r. The only odd primes that can divide these denominators are those which divide the degree of an isogeny $E \to E'$ defined over $\mathbb{Q}$. Even by allowing to change the curve in the isogeny class, we can not always achieve that the modular symbols are integers; for instance 3 will be a denominator of $[r]^{\pm}_{E}$ for some $r \in \mathbb{Q}$ for all E of conductor 27. However the following theorem says that we may get rid of all odd primes p such that p^2 does not divides the conductor N of E.

Theorem 1. *Let $E/\mathbb{Q}$ be an elliptic curve. Then there exists an elliptic curve $E_\bullet$, which is isogenous to E over $\mathbb{Q}$, such that $[r]^{\pm}_{E_\bullet}$ is a p-integer for all $r \in \mathbb{Q}$ and for all odd primes p for which E has semi-stable reduction.*

As stated here one could take $E_\bullet$ to be one of the curves in the isogeny class with maximal Néron lattice. However it is a consequence of Theorem 4, which is more precise and says that there is a curve $E_\bullet$ whose Néron lattice is contained in the lattice of all values of $\lambda(r)$ with index not divisible by any odd prime of semi-stable reduction.

As a direct consequence of this Theorem 1, one deduces that the algebraic part of the special values of the twisted L-series $L(E_\bullet, \chi, s)$ at $s = 1$ are p-adic integers for all Dirichlet characters χ and all odd semi-stable primes p. See Corollary 7.

The second part of this paper is devoted to another application of this theorem. Let p be an odd prime of semi-stable reduction. Kato has constructed in [10] an Euler system for the isogeny class of E. See Section 3 for details of the definitions. There are two sets of p-adic "zeta-elements": First, a set of integral zeta elements denoted by ${}_{c,d}z_m(\alpha)$ in the Galois cohomology of a lattice T_f canonically associated to f which provides upper bounds for Selmer groups. Secondly, a set of zeta elements denoted by z_γ which are linked to the p-adic L-functions. The latter are not known to be integral with respect to T_f. We will show in Proposition 8 that T_f is equal to the Tate module $T_pE_\bullet$ of the curve $E_\bullet$ in Theorem 1.

Let K_n be the n-th layer in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Let $\mathbf{z} \in \varprojlim_n H^1(K_n, T_pE_\bullet) \otimes \mathbb{Q}_p$ be the zeta element that is sent to the p-adic L-function for $E_\bullet$ via the Coleman map.

Theorem 2. *If the reduction is good at p, then $\mathbf{z}$ belongs to the integral Iwasawa cohomology $\varprojlim_n H^1(K_n, T_pE_\bullet)$.*

This is Theorem 13 in the text. Actually, the proof gives a more precise result. The global Iwasawa cohomology group $\mathbf{H}^1(T_pE)$ with restricted ramification turns out to be very often, but not always, a free module of rank 1 over the Iwasawa algebra of the $\mathbb{Z}_p$-extension. If it is free for $E = E_\bullet$ then the integrality of $\mathbf{z}$ is easily deduced; otherwise one can show that $\mathbf{H}^1(T_pE_\bullet)$ is at worst equal to the maximal ideal in the Iwasawa algebra and the integrality above follows then from the interpolation property of the p-adic L-function $L_p(E)$.

Another consequence of Theorem 1 concerns the main conjecture in Iwasawa theory for elliptic curves. We formulate it here for the full cyclotomic $\mathbb{Z}_p^\times$-extension.

Theorem 3. *Let E be an elliptic curve and p an odd prime of semi-stable reduction. Assume that $E[p]$ is reducible as a Galois module over $\mathbb{Q}$. Then the characteristic series of the dual of the Selmer group over the cyclotomic extension $\mathbb{Q}(\zeta_{p^\infty})$ divides the ideal generated by the p-adic L-function $L_p(E)$ in the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})]]$.*

Note that our assumptions in the theorem imply that the reduction of E at p is ordinary in the sense that E has either good ordinary or multiplicative reduction, because $E[p]$ is irreducible when E has supersingular reduction, see Proposition 12 in [22]. In the case when E has split multiplicative reduction, we can strengthen our theorem, see Theorem 16.
This theorem was proven by Kato in [10] in the case that the reduction is ordinary and the representation on the Tate module was surjective. The method of proof follows and generalises the incomplete proof in [30], where unfortunately the integrality issue had been overlooked.
For most good ordinary primes p for which $E[p]$ is irreducible the full main conjecture, asserting the equality rather than the divisibility in the above theorem, is now known thanks to the work of Skinner and Urban [25]. However their proof of the converse divisibility does not seem to extend easily to the reducible case.
Nonetheless, the above theorem has applications to the conjecture of Birch and Swinnerton-Dyer and to the explicit computations of Tate-Shafarevich groups as in [26]. The theorem also implies that all p-adic L-functions for elliptic curves at odd primes p of semi-stable ordinary reductions are integral elements in the Iwasawa algebra. See Corollary 18.

Acknowledgements

It is my pleasure to thank Dino Lorenzini, Tony Scholl and David Loeffler.

2 The lattice of all modular symbols

Let E be an elliptic curve defined over $\mathbb{Q}$. In what follows p will always stand be an odd prime and we suppose that E does not have additive reduction at p. The only case for which the integrality of Kato's Euler system may not hold is when E admits an isogeny of degree p defined over $\mathbb{Q}$; so we may just as well assume that we are in this "reducible" case. All conclusions in this section and in the rest of the paper are still valid without this assumption, however they are not our original work but rather well-known results. Denote by N the conductor of E.
In the isogeny class of E there are two interesting elliptic curves. The first is the optimal curve E_0 with respect to the modular parametrisation from

the modular curve $X_0(N)$, which is also often called the strong Weil curve. The second is the optimal curve E_1 with respect to the parametrisation from $X_1(N)$. The definition of optimality is given in [28], for instance the map $H_1\bigl(X_0(N)(\mathbb{C}),\mathbb{Z}\bigr) \to H_1\bigl(E_0(\mathbb{C}),\mathbb{Z}\bigr)$ is surjective. Another interesting curve is the so-called minimal curve (see [28]), which is conjecturally equal to E_1, but we will not make use of it in this article. Recall that a cyclic isogeny $A \to A'$ defined over $\mathbb{Q}$ is étale (this is a slight abuse of notation, we should say more precisely that it extends to an étale isogeny on the Néron models over $\mathbb{Z}$) if the pull-back of a Néron differential of A' yields a Néron differential of A.
Let f be the newform of level N corresponding to the isogeny class of E. We write $\omega_f = 2\pi i f(\tau) d\tau = f(q) dq/q$ for the corresponding differential form on the modular curve $X_1(N)$. For any curve A in the isogeny class of E, we define the Néron lattice $\mathscr{L}_A$ to be the image of

$$\int \omega_A \colon H_1\bigl(A(\mathbb{C}),\mathbb{Z}\bigr) \to \mathbb{C}$$

where ω_A is a choice of a Néron differential. We denote by $\mathscr{L}_0$ and $\mathscr{L}_1$ the lattices $\mathscr{L}_{E_0}$ and $\mathscr{L}_{E_1}$ respectively. Then $\mathscr{L}_f$ is defined to be the lattice of all $\int_\gamma \omega_f$ where γ varies in $H_1\bigl(X_1(N),\mathbb{Z}\bigr)$. Finally, we define

$$\hat{\mathscr{L}_f} = \left\{ \int_\gamma \omega_f \;\middle|\; \gamma \in H_1\Bigl(X_1(N)(\mathbb{C}), \{\text{cusps}\}, \mathbb{Z}\Bigr) \right\}.$$

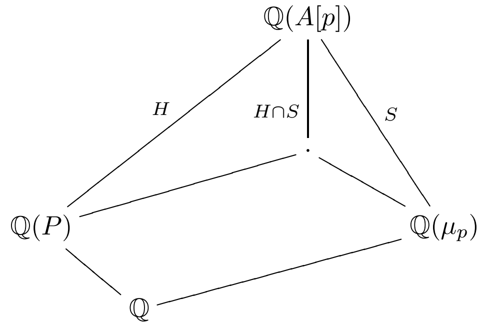
obtained by integrating ω_f along all paths between cusps in $X_1(N)$. This is the lattice of all modular symbols attached to f. By the Theorem of Manin–Drinfeld $\hat{\mathscr{L}_f}$ is a lattice with $\hat{\mathscr{L}_f} \subset \mathscr{L}_f\,\mathbb{Q}$. In fact, we know that all the lattices above are commensurable and we view them now as $\mathbb{Z}$-modules inside $V = \mathscr{L}_1 \otimes \mathbb{Q}$.

Theorem 4. *Let $E/\mathbb{Q}$ be an elliptic curve. Then there exists an elliptic curve $E_\bullet/\mathbb{Q}$ in the isogeny class of E whose lattice $\mathscr{L}_\bullet = \mathscr{L}_{E_\bullet}$ satisfies $\mathscr{L}_\bullet \otimes \mathbb{Z}_p = \hat{\mathscr{L}_f} \otimes \mathbb{Z}_p$ inside $V \otimes \mathbb{Q}_p$ for all odd primes p at which E has semi-stable reduction. Moreover the cyclic isogeny from E_1 to $E_\bullet$ is étale.*

Alternatively, we could also say that the index of $\mathscr{L}_\bullet \subset \hat{\mathscr{L}_f}$ is coprime to any odd prime of semi-stable reduction. We should also emphasise that the statement does not hold in general for primes p of additive reduction or for $p = 2$. Counter-examples for these will be provided later. The proof will require some intermediate lemmas.

Lemma 5. *Let $A/\mathbb{Q}$ be an elliptic curve and let p be an odd prime. Suppose P is a point of exact order p in A, defined over an abelian extension of $\mathbb{Q}$ which is unramified at p. Then the isogeny with kernel generated by P is defined over $\mathbb{Q}$.*

Proof. Let G be the Galois group of $\mathbb{Q}\bigl(A[p]\bigr)$ over $\mathbb{Q}$. Let H be the subgroup corresponding to the field of definition $\mathbb{Q}(P)$ of P. Then H is a normal subgroup



of G with abelian quotient. In any basis of $A[p]$ with P as the first element, the group H is contained in $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ when we view G as a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Let $S = G \cap \mathrm{SL}_2(\mathbb{F}_p)$ be the kernel of the determinant $G \to \mathbb{F}_p^\times$. Hence $H \cap S$ is contained in the subgroup of matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. So we have two cases to distinguish. Either $H \cap S$ is equal to the cyclic group of order p of all matrices of this form or it is trivial. But note first that the Weil pairing implies that $\mathbb{Q}(\mu_p)$ is contained in $\mathbb{Q}\bigl(A[p]\bigr)$. So G/S is isomorphic to $\mathbb{F}_p^\times$ via the determinant. Since $\mathbb{Q}(P)$ is unramified at p, it must be linearly disjoint from $\mathbb{Q}(\mu_p)$. For our groups, this means that $HS = G$. Hence $H/(H \cap S) = G/S = \mathbb{F}_p^\times$.
Case 1: $H \cap S$ is equal to the cyclic group of order p generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. The above then implies that H is equal to the subgroup of all matrices $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. Now G is contained in the normaliser of this group H inside $\mathrm{GL}_2(\mathbb{F}_p)$, which is easily seen to be equal to the Borel subgroup of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$. In particular, the subgroup generated by P is fixed by G.
Case 2: H intersects S trivially. Then $\mathbb{Q}\bigl(A[P]\bigr)$ is the composition of $\mathbb{Q}(\mu_p)$ and $\mathbb{Q}(P)$. Hence G is the abelian group $H \times S$. Note that H is now a cyclic group of order $p-1$. Let h be a non-trivial element of $H \subset \bigl\{\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)\bigr\}$. It has two eigenvalues, one equal to 1 and the other λ must be different than 1 as otherwise h would belong to S. Let $Q \in A[p]$ be an eigenvector for h with eigenvalue λ and use the basis $\{P, Q\}$ for $A[p]$. For H to be an abelian subgroup of $\bigl\{\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)\bigr\}$ containing the element $h = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \lambda \end{smallmatrix}\right)$, it is necessary that H is contained in the diagonal matrices. Therefore H is the group of all matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$.
We know that S has to commute with H. It is easy to see that this implies that S is contained in the group of matrices of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)$. It follows that G is contained in the diagonal matrices. Once again the isogeny defined by P is fixed by G. $\square$

If A is an elliptic curve defined over $\mathbb{Q}$, we know by [2] that there is a non-constant morphism of curves $\varphi_A \colon X_0(N) \to A$ defined over $\mathbb{Q}$. We normalise it by requiring that it is of minimal degree and that the cusp ∞ maps to $O \in A(\mathbb{Q})$. It is well-defined up to composition with an automorphism of A.

Lemma 6. *Let $A/\mathbb{Q}$ be an elliptic curve and let p be an odd prime such that A has semi-stable reduction at p. Let $r \in \mathbb{Q}$ represent a cusp on $X_0(N)$ such that the image $\varphi_A(r)$ in $A(\bar{\mathbb{Q}})$ has order divisible by p. Let $P \in A(\bar{\mathbb{Q}})$ be a multiple of $\varphi_A(r)$ which has exact order p. Then the isogeny with kernel generated by P is étale and defined over $\mathbb{Q}$.*

Proof. Let D be the greatest common divisor of the denominator of r and N. Next, let d be the greatest common divisor of D and $\frac{N}{D}$. So by definition d is only divisible by primes of additive reduction and hence it is coprime to p. By the description of the Galois-action on cusps of $X_0(N)$ given in Theorem 1.3.1. in [27],we see that the cusp r on $X_0(N)$, and hence its image in $A(\bar{\mathbb{Q}})$, are defined over the cyclotomic field $K = \mathbb{Q}(\zeta_d)$. The previous Lemma 5 proves that the isogeny generated by P is defined over $\mathbb{Q}$. Since the kernel acquires a point over an extension which is unramified at p, it has to be étale. $\square$

Proof of Theorem 4. The lattice $\hat{\mathscr{L}}_f$ is the set of all values of integrating $\omega_f = 2\pi i f(\tau) d\tau$ as τ runs along a geodesic from one cusp $r_1 \in \mathbb{Q}$ to another $r_2 \in \mathbb{Q}$ inside the upper half plane. So it is also the set of all $\int_\gamma \omega_f$ as γ varies in $H_1\bigl(X_0(N), \{\text{cusps}\}, \mathbb{Z}\bigr)$. We are allowed to switch here from $X_1(N)$ to $X_0(N)$ and to identify ω_f on both of them as the pullback of ω_f under $X_1(N) \to X_0(N)$ is again ω_f because it is determined by the q-expansion of f.
The Manin constant c_0 for the optimal curve E_0 is an integer such that $\varphi_0^*(\omega_0) = c_0 \cdot \omega_f$, where $\varphi_0 \colon X_0(N) \to E_0$ is the modular parametrisation of minimal degree and ω_0 is a Néron differential on E_0. One can choose φ_0 and ω_0 in such a way as to make $c_0 > 0$. It is known that c_0 is coprime to any odd prime for which E has semi-stable reduction. For this and more on the Manin constant we refer to [1]. From the description of optimality above, we can deduce that $c_0 \cdot \mathscr{L}_f = \mathscr{L}_0$ and hence that $c_0 \cdot \hat{\mathscr{L}}_f \supset \mathscr{L}_0$.
To start, we set A to be the optimal curve E_0. We shall successively replace A by one of its quotients by an étale kernel until we reach $E_\bullet$. Pick an odd semi-stable prime that divides the index i_A of $\mathscr{L}_A$ in $c_0 \cdot \hat{\mathscr{L}}_f$. The modular parametrisation $\varphi_A \colon X_0(N) \to A$ factors through E_0. The quotient $\bigl(c_0 \hat{\mathscr{L}}_f\bigr)/\mathscr{L}_A$ is generated by the images $\varphi_A(r) \in A(\mathbb{C}) \cong \mathbb{C}/\mathscr{L}_A$ of all cusps r in $X_0(N)$. So we find a cusp r whose image in $A(\bar{\mathbb{Q}})$ has order divisible by p. We can now apply Lemma 6, which gives us an étale isogeny $A \to A'$ such that the index of $\mathscr{L}_{A'}$ in $c_0 \hat{\mathscr{L}}_f$ is now $i_{A'} = i_A/p$. We replace now A by A' and repeat the procedure until the index i_A is coprime to all odd semi-stable primes. By the above mentioned property of c_0, we now have $\mathscr{L}_A \otimes \mathbb{Z}_p = \hat{\mathscr{L}}_f \otimes \mathbb{Z}_p$ for all odd semi-stable primes
By construction, A is now an étale quotient of E_0. We consider the isogeny $E_1 \to E_0 \to A$. The cyclic isogeny $E_1 \to E_0$ has a constant kernel and hence it is étale over $\mathbb{Z}[\frac{1}{2}]$, as explained in Remark 1.8 in [29]. If it is étale over $\mathbb{Z}$, we can set $E_\bullet = A$ and we are done. Otherwise, there is an isogeny $E_0 \to E_0'$ whose degree is a power of 2 such that the cyclic isogeny from E_1 to E_0' is étale. Since the degree of $E_0 \to A$ is odd by construction, there is an isogeny $A \to E_\bullet$

of the same degree as $E_0 \to E_0'$ such that $E_1 \to E_\bullet$ is étale. $\square$

For any A in the isogeny class of E, we write Ω_A^+ for the smallest positive real element of $\mathscr{L}_A$ and Ω_A^- for the smallest absolute value of a purely imaginary element in $\mathscr{L}_A$. For any $r \in \mathbb{Q}$, the modular symbols $[r]^\pm \in \mathbb{Q}$ attached to A are defined by

$$[r]^+ = \frac{1}{\Omega_A^+}\operatorname{Re}\left(\int_r^\infty \omega_f\right) \qquad \text{and} \qquad [r]^- = \frac{1}{\Omega_A^-}\operatorname{Im}\left(\int_r^\infty \omega_f\right).$$

Then our theorem tells us that $[r]^\pm$ will have denominator coprime to any odd semi-stable prime for the curve $E_\bullet$. In particular, it is obvious from the construction (see [14]) of the p-adic L-function by modular symbols that it will be an integral power series in $\mathbb{Z}_p[\![T]\!]$ for ordinary primes p. However this also follows from Proposition 3.7 in [9] and the fact that $E_1 \to E_\bullet$ is étale.
A reformulation of the theorem is the following integrality statement.

Corollary 7. *Let E be an elliptic curve over $\mathbb{Q}$ and p an odd prime for which E has semi-stable reduction. Then there is a curve $E_\bullet$ which is isogenous to E over $\mathbb{Q}$ such that for all Dirichlet characters χ we have*

$$\frac{G(\chi)\cdot L(E_\bullet,\chi,1)}{\Omega^+_{E_\bullet}} \in \mathbb{Z}_p[\chi] \qquad \text{if } \chi(-1) = 1 \text{ or}$$
$$\frac{G(\chi)\cdot L(E_\bullet,\chi,1)}{i\,\Omega^-_{E_\bullet}} \in \mathbb{Z}_p[\chi] \qquad \text{if } \chi(-1) = -1$$

where $\mathbb{Z}_p[\chi]$ is the ring of integers in the extension of $\mathbb{Q}_p$ generated by the values of χ and $G(\chi)$ stands for the Gauss sum.

Proof. This follows from the formula of Birch, see formula (8.6) in [14]:

$$L(E,\chi,1) = \frac{1}{G(\chi)} \sum_{a \bmod m} \chi(a)\left(\int_{a/m}^\infty \omega_f\right)$$

where m is the conductor of χ. $\square$

2.1 The semi-stable case

Let $E/\mathbb{Q}$ be an elliptic curve with semi-stable reduction at all primes. Hence N is square-free. So d in the proof of Lemma 6 is equal to 1 for all cusps and hence they are all defined over $\mathbb{Q}$. By Mazur's Theorem [13], we may obtain $E_\bullet$ satisfying $\hat{\mathscr{L}}_f \otimes \mathbb{Z}[\frac{1}{2}] = \mathscr{L}_\bullet \otimes \mathbb{Z}[\frac{1}{2}]$ by taking the quotient of E_0 only by at most a p-torsion point defined over $\mathbb{Q}$ for some $p = 3$, 5 or 7. In particular, if $E_0(\mathbb{Q})[3\cdot 5\cdot 7] = \{O\}$, then $E_\bullet = E_0$. If instead, there is a rational torsion point of odd order, then we might have to take the isogeny with kernel $E_0(\mathbb{Q})[p]$. Nonetheless the curve labelled 66c1 in [5] shows that in some examples we can have $E_\bullet = E_0$ even when E_0 has a rational 5-torsion point.

2.2 Examples

We can present here a few examples; in all of them we know that $c_0 = 1$. Throughout, we use the notations from Cremona's tables [5]. First, for the class 11a and $p = 5$, we find that E_1 =11a3, E_0 =11a1, and $E_\bullet$ =11a2 and the étale isogenies $E_1 \to E_0 \to E_\bullet$ are all of degree 5. To justify this, one has to note that $L(f,1) = \frac{1}{5}\Omega^+_{E_0}$ and so $[0]^+ = \frac{1}{5}$ for E_0. Hence the lattice $\hat{\mathscr{L}}_f$ has index at least 5 in $\mathscr{L}_0$.
For the class 17a, the curve E_0 =17a1 has Mordell-Weil group $E(\mathbb{Q}) = {}^{\mathbb{Z}}\!/_{4\mathbb{Z}}$. The optimal curve E_1 corresponds to a sublattice of index 4 in $\mathscr{L}_0$ and it is the minimal curve 17a4. It is easy to compute the modular symbols for f. Since $L(f,1) = \frac{1}{4}\Omega^+_0$, we find that $\hat{\mathscr{L}}_f$ has index at least 4 in $\mathscr{L}_0$. In fact, $\hat{\mathscr{L}}_f$ is the lattice $\frac{1}{2}\mathscr{L}_{17\mathrm{a}3}$. This shows that the above lemma is not valid for $p = 2$.
In the class 91b, we find that E_0 and E_1 are equal to 91b1, which has 3-torsion points over $\mathbb{Q}$. It turns out that $E_\bullet$, which is equal to 91b2, has a 3-torsion point as well. So it is not true in general that $E_\bullet(\mathbb{Q})$ has no p-torsion even when it is different from E_0.
Now to elliptic curves, which are not semi-stable. The class 98a is the twist of 14a by -7. This time the lattice $\hat{\mathscr{L}}_f$ is equal to the lattice of 98a5, which has the same real period as E_0, but the imaginary period is divided by 9. Both E_0 and $E_\bullet$ have only a 2-torsion point defined over $\mathbb{Q}$. The two cyclic isogenies of degree 3 acquire a rational point in the kernel only over $\mathbb{Q}(\sqrt{-7})$.
For the curves 27a, which admit complex multiplication, we find that $\hat{\mathscr{L}}_f = \frac{1}{3}\mathscr{L}_0$. The same happens for 54a. However in both cases E does not have semi-stable reduction at $p = 3$. This shows that the lemma and theorem can not be extended to primes p with additive reduction.

3 Kato's Euler system

Let $E/\mathbb{Q}$ be an elliptic curve and p an odd prime. Suppose E has semi-stable reduction at p. Since we are mainly interested in the case when $E[p]$ is reducible, we may assume that the reduction at E is ordinary.
We now follow the notations and definitions in [10]. As before f is the newform of weight 2 and level N associated to the isogeny class of E. Define the $\mathbb{Q}_p$-vector space $V_{\mathbb{Q}_p}(f)$ as the largest quotient of $H^1_{\text{ét}}\bigl(\overline{Y_1(N)}, \mathbb{Q}_p\bigr)$ on which the Hecke operators act by multiplication with the coefficients of f. Further the image of $H^1_{\text{ét}}\bigl(\overline{Y_1(N)}, \mathbb{Z}_p\bigr)$ in $V_{\mathbb{Q}_p}(f)$ is a $\operatorname{Gal}\bigl(\bar{\mathbb{Q}}/\mathbb{Q}\bigr)$-stable lattice, denoted by $V_{\mathbb{Z}_p}(f)$.

Proposition 8. *We have an equality of* $\operatorname{Gal}\bigl(\bar{\mathbb{Q}}/\mathbb{Q}\bigr)$*-stable lattices* $V_{\mathbb{Z}_p}(f)(1) = T_pE_\bullet$ *inside* $V_{\mathbb{Q}_p}(f)(1)$.

Proof. We consider first the version with coefficients in $\mathbb{Z}$ rather than in $\mathbb{Z}_p$ as in 6.3 of [10]. We define $V_{\mathbb{Q}}(f)$ as the maximal quotient of $H^1\bigl(Y_1(N)(\mathbb{C}), \mathbb{Q}\bigr)$ and $V_{\mathbb{Z}}(f)$ as the image of $H^1\bigl(Y_1(N)(\mathbb{C}), \mathbb{Z}\bigr)$ inside $V_{\mathbb{Q}}(f)$. By Poincaré duality, we have

$$H^1\big(Y_1(N)(\mathbb{C}),\mathbb{Z}\big) \cong H_1\big(X_1(N)(\mathbb{C}),\{\text{cusps}\},\mathbb{Z}\big)$$

as in 4.7 in [10]. Now let $\varphi_1\colon X_1(N) \to E_1$ be the optimal modular parametrisation. The optimality implies that φ_1 induces a surjective map from $H_1\big(X_1(\mathbb{C}),\mathbb{Z}\big)$ to $H_1\big(E_1(\mathbb{C}),\mathbb{Z}\big)$. Hence we may identify $V_{\mathbb{Q}}(f)$ via φ_1 with $H_1\big(E_1(\mathbb{C}),\mathbb{Q}\big)$. Under this identification, the lattice $V_{\mathbb{Z}}(f)$ is mapped to the image of the relative homology $H_1\big(X_1(N)(\mathbb{C}),\{\text{cusps}\},\mathbb{Z}\big)$. It contains the lattice $H_1\big(E_1(\mathbb{C}),\mathbb{Z}\big)$. Through the map integrating against the Néron differential ω_1 of E_1, the lattice $V_{\mathbb{Z}}(f)$ is brought to $c_1\hat{\mathcal{L}}_f$ containing $\mathcal{L}_1$ where c_1 is the Manin constant of φ_1, i.e. the integer such that $\varphi_1^*(\omega_1) = c_1\omega_f$. Since c_1 is a p-adic unit by Proposition 3.3 in [9], our Theorem 4 shows that

$$V_{\mathbb{Z}}(f)\otimes\mathbb{Z}_p = H_1\big(E_\bullet(\mathbb{C}),\mathbb{Z}\big)\otimes\mathbb{Z}_p \quad \text{inside} \quad V_{\mathbb{Q}}(f)\otimes\mathbb{Q}_p = H_1\big(E_1(\mathbb{C}),\mathbb{Q}\big)\otimes\mathbb{Q}_p.$$

Following 8.3 in [10], we can identify $V_{\mathbb{Z}_p}(f)$ with $V_{\mathbb{Z}}(f)\otimes\mathbb{Z}_p$ through the comparison of Betti and étale cohomology. We identify again $V_{\mathbb{Q}_p}(f)$ with $H^1_{\text{ét}}\big(\overline{E_1},\mathbb{Q}_p\big)$ through φ_1 and we obtain that

$$V_{\mathbb{Z}_p}(f) = H^1_{\text{ét}}\big(\overline{E_\bullet},\mathbb{Z}_p\big) \cong T_pE_\bullet(-1) \quad \text{containing} \quad H^1_{\text{ét}}\big(\overline{E_1},\mathbb{Z}_p\big) \cong T_pE_1(-1)$$

at least as $\mathbb{Z}_p$-lattices inside $V_{\mathbb{Q}_p}(f)$. But the Galois action is the same on both $V_{\mathbb{Z}_p}(f)$ and $T_p(E_\bullet)(-1)$. □

From now on we will denote this lattice in our Galois representation simply by $T = V_{\mathbb{Z}_p}(f)(1) = T_pE_\bullet$. Kato constructs in 8.1 in [10] two sets of p-adic zeta-elements in the Galois cohomology of T. First, let a and $A \geqslant 1$ be two integers. Then there is an element

$${}_{c,d}z_m\big(\tfrac{a}{A}\big) = {}_{c,d}z_m^{(p)}\big(f,1,1,a(A),\text{primes}(pA)\big) \in H^1_{\text{ét}}\big(\mathbb{Z}[\tfrac{1}{p},\zeta_m],T\big)$$

for all integers $m \geqslant 1$ and integers c,d coprime to $6pA$. They are linked to the modular symbol obtained from the path from $\frac{a}{A}$ to ∞ in the upper half plane. Also, ζ_m is a primitive m-th root of unity.

Secondly, for any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, there are elements

$${}_{c,d}z_m(\alpha) = {}_{c,d}z_m^{(p)}\big(f,1,1,\alpha,\text{primes}(pN)\big) \in H^1_{\text{ét}}\big(\mathbb{Z}[\tfrac{1}{p},\zeta_m],T\big)$$

for any integer $m \geqslant 1$ and integers $c \equiv d \equiv 1 \pmod N$ coprime to $6pN$. They are linked to the image under α of the path from 0 to ∞ in the upper half plane.

The advantage of these integral elements (with respect to our lattice T) is that they form an Euler system (13.3 in [10]). Namely by fixing α, c and d as above, the elements $\big({}_{c,d}z_m(\alpha)\big)_m$ form an Euler system.

Out of the above elements for m being a power of p, Kato builds the zeta-elements that are linked to the p-adic L-functions. We denote by

$$\Lambda = \mathbb{Z}_p\Big[\Big[\mathrm{Gal}\big(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}\big)\Big]\Big] = \varprojlim_n \mathbb{Z}_p\Big[\mathrm{Gal}\big(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\big)\Big]$$

the Iwasawa algebra of the cyclotomic $\mathbb{Z}_p^\times$-extension of $\mathbb{Q}$. Then we have the following finitely generated Λ-module

$$\mathbf{H}^1(T) := \varprojlim_n H^1_{\text{ét}}\bigl(\mathbb{Z}[\zeta_{p^n}, \tfrac{1}{p}], T\bigr) = \varprojlim_n H^1\bigl(G_\Sigma(\mathbb{Q}(\zeta_{p^n})), T\bigr),$$

where Σ is any set of primes containing the infinite places and those dividing pN and $G_\Sigma(K)$ is the Galois group of the maximal extension of K which is unramified outside Σ. See Section 3.4.1 in [17] for the independence on Σ. For each $\gamma \in T$, there is a

$$z_\gamma = z_\gamma^{(p)} \in \mathbf{H}^1(T) \otimes \mathbb{Q}_p = \varprojlim_n H^1_{\text{ét}}\bigl(\mathbb{Z}[\tfrac{1}{p}, \zeta_{p^n}], T\bigr) \otimes \mathbb{Q}_p\,.$$

In fact, they are defined in 13.9 in [10] as elements in the larger $\mathbf{H}^1(T) \otimes_\Lambda \operatorname{Frac}(\Lambda)$ as they are quotients of elements of the form ${}_{c,d}z_m(\alpha)$ by certain elements $\mu(c,d)$ in Λ. However Kato shows in 13.12 that they belong to the much smaller $\mathbf{H}^1(T) \otimes \mathbb{Q}_p$ by comparing them with elements of the form ${}_{c,d}z_{p^n}(\frac{a}{A})$. See also appendix A in [6] for more information about the division by $\mu(c,d)$.

3.1 Criteria for the Iwasawa cohomology to be free over the Iwasawa algebra

The Λ-module $\mathbf{H}^1(T)$ is torsion-free of rank 1 as shown in Theorem 12.4 in [10]. If $E[p]$ is irreducible, then Theorem 12.4.(3) shows that $\mathbf{H}^1(T)$ is free. In this section we gather further cases in which we can prove that $\mathbf{H}^1(T)$ is free or otherwise determine how far we are off from being free. When it is free one deduces that z_γ integral for all $\gamma \in T$. We will later turn back to this question in Section 3.3

Lemma 9. *Let p be an odd prime of semi-stable reduction. If the X_0-optimal curve E_0 has no rational p-torsion point, but the degree of the cyclic isogeny from E_0 to $E_\bullet$ is divisible by p, then $\mathbf{H}^1(T)$ is free of rank 1 over Λ.*

This lemma is essentially about curves that are not semi-stable. It applies to all twists of a semi-stable curve by a square-free $D \neq \pm p$. This follows from the fact that for semi-stable curves a result by Serre [24, Proposition 1] and [22, Proposition 21] shows that $E[p]$ is an extension of $\mathbb{Z}/p\mathbb{Z}$ by $\mu[p]$ or an extension of $\mu[p]$ by $\mathbb{Z}/p\mathbb{Z}$.
Conversely, if E_0 has a point of order $p > 2$ defined over $\mathbb{Q}$, then it has semi-stable reduction at all places, except for $p = 3$ when we could have fibres of type IV or IV*.

Proof. We claim that under our hypothesis, the Mordell-Weil group $E_\bullet\bigl(\mathbb{Q}(\zeta_p)\bigr)$ contains no p-torsion points. Let $\phi\colon A \to A'$ be a cyclic isogeny of degree p in the isogeny $E_0 \to E_\bullet$ and assume by induction that A has no torsion point defined over $\mathbb{Q}$. From the proof of Theorem 4, we know that $A[\phi]$ acquires rational points over $\mathbb{Q}(\zeta_d)$ with $d \mid N$ as in the proof of Lemma 6. In particular

p does not divide d and so $A[\phi]$ will not contain a rational point defined over $\mathbb{Q}(\zeta_p)$; neither will $A'[\hat{\phi}]$ as it is its Cartier dual. This means that the semi-simplification of $A[p]$ is the sum of two distinct characters with conductor divisible by a prime different from p. Hence A and A' both have no p-torsion point defined over $\mathbb{Q}(\zeta_p)$.

One way to prove the lemma is by adapting Kato's argument at the end of 13.8. The argument works as long as the twisted $\mathbb{F}_p(r)$ does not appear in $E[p]$ as a Galois sub-module. Instead we give a second proof here.

Let $\Gamma = \mathrm{Gal}\bigl(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)\bigr)$. Using the Tate spectral sequence [15, Theorem 2.1.11] we see that $\mathbf{H}^1(T)_\Gamma$ injects into $H^1\bigl(G_\Sigma(\mathbb{Q}(\zeta_p)), T\bigr)$ via the corestriction map. Now the torsion subgroup of the latter is equal to the torsion subgroup of $\varprojlim E\bigl(\mathbb{Q}(\zeta_p)\bigr)/p^n$, which is trivial if $E\bigl(\mathbb{Q}(\zeta_p)\bigr)$ has no p-torsion. Hence $\mathbf{H}^1(T)_\Gamma$ is a free $\mathbb{Z}_p$-module.

Choose an injection $\iota\colon \mathbf{H}^1(T) \to \Lambda$ with finite cokernel F. We deduce an exact sequence

$$0 \longrightarrow F^\Gamma \longrightarrow \mathbf{H}^1(T)_\Gamma \longrightarrow \Lambda_\Gamma \longrightarrow F_\Gamma \longrightarrow 0$$

Since $\mathbf{H}^1(T)_\Gamma$ is torsion-free, we obtain that $F^\Gamma = 0$. Since F is finite, F_Γ is of the same size. But by Nakayama's Lemma $F_\Gamma = 0$ implies that $F = 0$. Hence $\mathbf{H}^1(T)$ is Λ-free. $\square$

We refine our analysis of $\mathbf{H}^1(T)$ now a bit for the remaining cases. Any Λ-module M comes equipped with an action by the group $\Delta = \mathrm{Gal}\bigl(\mathbb{Q}(\zeta_p)/\mathbb{Q}\bigr)$ and we split M up into the eigenspaces $M = \bigoplus_{i=0}^{p-2} M_i$ where Δ acts on $M_i = M(-i)^\Delta$ by the i-th power of the Teichmüller character. Now M_i is a $\Lambda(\Gamma) = \mathbb{Z}_p[\![\Gamma]\!]$-module.

Lemma 10. *Let $\phi\colon E \to E'$ be an isogeny whose kernel has a point of order p defined over $\mathbb{Q}$. Then $\mathbf{H}^1(T_pE)_i$ and $\mathbf{H}^1(T_pE')_i$ are free of rank 1 over $\Lambda(\Gamma)$ for all $1 < i \leqslant p-2$. Furthermore $\mathbf{H}^1(T_pE)_1$ and $\mathbf{H}^1(T_pE')_0$ are also free of rank 1. The remaining $\mathbf{H}^1(T_pE)_0$ and $\mathbf{H}^1(T_pE')_1$ are either free of rank 1 or there is an injection into $\Lambda(\Gamma)$ with image equal to the maximal ideal.*

Proof. We have two short exact sequence

$$0 \longrightarrow T_pE \xrightarrow{\ \phi\ } T_pE' \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

$$0 \longleftarrow \mu_p \longleftarrow T_pE \xleftarrow[\ \hat{\phi}\ ]{} T_pE' \longleftarrow 0$$

which induces two exact sequences

$$0 \longrightarrow \mathbf{H}^1(T_pE) \xrightarrow{\ \phi\ } \mathbf{H}^1(T_pE') \longrightarrow \mathbf{H}^1\bigl(\mathbb{Z}/p\mathbb{Z}\bigr) \qquad (*)$$

$$\mathbf{H}^1(\mu_p) \longleftarrow \mathbf{H}^1(T_pE) \xleftarrow[\ \hat{\phi}\ ]{} \mathbf{H}^1(T_pE') \longleftarrow 0.$$

Here the last terms are the projective limits as n tends to infinity of the groups $H^1\bigl(G_\Sigma(\mathbb{Q}(\zeta_{p^n})),\mathbb{Z}/p\mathbb{Z}\bigr)$ and of $H^1\bigl(G_\Sigma(\mathbb{Q}(\zeta_{p^n})),\mu[p]\bigr)$ respectively. Since $p = 3$, 5 or 7, the class group of $\mathbb{Q}(\zeta_{p^n})$ has no p-torsion and hence $H^1(G_\Sigma(\mathbb{Q}(\zeta_{p^n})),\mu[p])$ is the quotient of the global Σ-units by its p-th powers. Lemma 4.3.4 and Proposition 4.5.3 in [4] show that $\mathbf{H}^1(\mu[p]) = \mathbb{F}_p(1)\oplus\Lambda^+/p$ as a $\Lambda = \mathbb{Z}_p[\Delta]\llbracket\Gamma\rrbracket$-module, where Λ^+ the part of Λ fixed by complex conjugation. Also we have $\mathbf{H}^1(\mathbb{Z}/p\mathbb{Z}) = \mathbf{H}^1(\mu[p])(-1) = \mathbb{F}_p\oplus\Lambda^-/p$. Because the composition of ϕ and $\hat\phi$ is the multiplication by p, the cokernels of the end maps of the two exact sequences (*) above have to be finite because $\mathbf{H}^1(T_pE)$ and $\mathbf{H}^1(T_pE')$ are known to be torsion-free Λ-modules of rank 1.
If i is not 0 or 1, then the argument in the proof of Lemma 9 applies to show that $\mathbf{H}^1(T_pE)_i$ and $\mathbf{H}^1(T_pE')_i$ are both free since the p-torsion subgroup of $E\bigl(\mathbb{Q}(\zeta_p)\bigr)$ and $E'\bigl(\mathbb{Q}(\zeta_p)\bigr)$ have trivial i-th eigenspace under the action of Δ.
Let now $i=0$ and set $A = \mathbf{H}^1(T_pE)_0$ and $B = \mathbf{H}^1(T_pE')_0$. In the case $i=1$, we would just swap the roles of A and B. The exact sequences (*) show that $\phi\colon A\to B$ has finite cokernel of size at most p and that $\hat\phi\colon B\to A$ has cokernel in $\Lambda(\Gamma)/p\cong\mathbb{F}_p\llbracket\Gamma\rrbracket$. Choose an injection $\iota\colon B\to\Lambda(\Gamma)$ with finite cokernel F. We now view B via ι and A via $\phi\circ\iota$ as ideals in $\Lambda(\Gamma)$ of finite index. The map $\hat\phi\colon B\to A$ becomes the multiplication by p.
Let I be the kernel of the map $\Lambda(\Gamma)\to\mathbb{Z}_p$ sending all elements of Γ to 1. Then we obtain the exact sequence

$$0\longrightarrow F^\Gamma\longrightarrow A/IA\longrightarrow\Lambda/I\longrightarrow F/IF\longrightarrow 0.$$

Again if $A/IA = A_\Gamma$ is $\mathbb{Z}_p$-free, then A is $\Lambda(\Gamma)$-free and since $A\to B$ has finite cokernel, then B has to be free, too. Assume therefore that A/IA is not free. We know that A/IA injects into $H^1\bigl(G_\Sigma(\mathbb{Q}),T_pE\bigr)$ whose torsion part is the p-primary part of $E(\mathbb{Q})$. Hence it is at most of order p. We conclude that F^Γ and F_Γ are both of order p under our assumption. Hence $A/IA\cong{}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\oplus\mathbb{Z}_p$ and we can take $p+IA$ to be the generator of the free part. Let $a\in A$ be such that $a+IA$ is a generator of the torsion part. It must lie in I but not in IA. By Nakayama's Lemma p and a generate the ideal A. Consider now the exact sequence

$$0\longrightarrow p\Lambda(\Gamma)/pB\longrightarrow A/pB\longrightarrow A/p\Lambda(\Gamma)\longrightarrow 0$$

where the middle term is a finite index sub-$\Lambda(\Gamma)$-module of $\Lambda(\Gamma)/p$. But a such does not have any finite non-zero sub-modules. Hence $p\Lambda(\Gamma) = pB$ shows that B is $\Lambda(\Gamma)$-free of rank 1. Since the smaller ideal A has index p it has no choice but to be the maximal ideal of $\Lambda(\Gamma)$. ☐

Here is an example for which $\mathbf{H}^1(T_pE)_0$ is not free. The semi-stable isogeny class 11a contains three curves

$$E_1 = 11\mathrm{a}3\xrightarrow{\ \phi\ }E_0 = 11\mathrm{a}1\xrightarrow{\ \psi\ }E_\bullet = 11\mathrm{a}2$$

where the direction of the arrow is the isogeny with kernel ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ with $p=5$. While E_1 and E_0 have rational 5-torsion points, the Mordell-Weil group of $E_\bullet$

over $\mathbb{Q}$ is trivial. Hence by the proof of Lemma 9, we see that $\mathbf{H}^1(T_pE_\bullet)_0$ is $\Lambda(\Gamma)$-free. This lemma does not apply to E_0, however Lemma 10 does and shows that $\mathbf{H}^1(T_pE_0)_0$ is also $\Lambda(\Gamma)$-free. We will now show that $\mathbf{H}^1(T_pE_1)_0$ is not free.

For this we continue the first exact sequence in (*) as follows

$$\mathbf{H}^1(T_pE_1)_0 \xrightarrow{\phi} \mathbf{H}^1(T_pE_0)_0 \longrightarrow \mathbb{F}_p \longrightarrow \mathbf{H}^2(T_pE_1)_0 \xrightarrow{\phi_2} \mathbf{H}^2(T_pE_0)_0$$

where $\mathbf{H}^2(\cdot)$ stands for the projective limit of $H^2\big(G_\Sigma(\mathbb{Q}(\zeta_{p^n})),\cdot\big)$. Our aim is to show that ϕ_2 is injective. Let $Z_{v,i}$ be the projective limit of $H^2\big(\mathbb{Q}_v(\zeta_{p^n}),T_pE_i\big)_0$ as $n\to\infty$ and consider the localisation maps

$$\begin{tikzcd}
0 \arrow[r] & Y_1 \arrow[r] \arrow[d] & \mathbf{H}^2(T_pE_1)_0 \arrow[r] \arrow[d, "\phi_2"] & \bigoplus_{v\in\Sigma} Z_{v,1} \arrow[r] \arrow[d] & {} \\
0 \arrow[r] & Y_0 \arrow[r] & \mathbf{H}^2(T_pE_0)_0 \arrow[r] & \bigoplus_{v\in\Sigma} Z_{v,0} \arrow[r] & {}
\end{tikzcd}$$

By global duality the kernels Y_1 and Y_0 are fine Selmer groups which we will properly define in Section 4; for our purpose here it is sufficient to say that they are both trivial in our example. To show that ϕ_2 is injective it is sufficient to show that $\phi\colon Z_{v,1}\to Z_{v,0}$ is injective for all $v\in\Sigma=\{5,11\}$. Local duality shows that $Z_{v,i}$ is dual to the p-primary part of the group of points of E_i over $\mathbb{Q}_v(\zeta_{p^\infty})^\Delta$. Hence we want to show that for all $v\in\ \{5,11\}$ the map

$$\hat{\phi}\colon E_0\big(\mathbb{Q}_v(\zeta_{p^\infty})^\Delta\big)[p^\infty]\to E_1\big(\mathbb{Q}_v(\zeta_{p^\infty})^\Delta\big)[p^\infty]$$

is surjective. First for $v=11$ where both curves have split multiplicative reduction; however the Tamagawa number for E_0 is 5 while it is 1 for E_1. We conclude that the p-primary part of $E\big(\mathbb{Q}_{11}(\zeta_{5^\infty})\big)$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ for $E=E_0$ and it is equal to $\mathbb{Q}_p/\mathbb{Z}_p\oplus\mathbb{Z}/p\mathbb{Z}$ for $E=E_1$. The map $\hat{\phi}$ is easily seen to be surjective by looking at the 5-torsion points over $\mathbb{Q}_{11}$.

Next for $v=5$, where the reduction is good ordinary. Here the p-primary parts of both groups of local points are equal to ${}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$. This follows from the fact that the formal group of these curves have torsion group isomorphic to μ_{p^∞} which has no Δ-fixed points and from the existence of the rational 5-torsion points over $\mathbb{Q}_5$.

This ends the proof that $\mathbf{H}^1(T_pE_1)_0$ is not free but equal to the maximal ideal as shown in Lemma 10. Note that the same argument won't work for ψ, because $\hat{\psi}$ is not surjective locally on the p-primary part neither at $v=5$ nor at $v=11$.

3.2 Link to the p-adic L-function

For any extension $K/\mathbb{Q}_p$, we write $H^1_f(K,T)$ for the Bloch-Kato group of local conditions. The quotient group $H^1_s(K,T)=H^1(K,T)/H^1_f(K,T)$ is in fact dual

to $E_\bullet(K)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ by local Tate duality. We set $\mathbf{H}^1_s(T)$ to be the projective limit of $H^1_s\bigl(\mathbb{Q}_p(\zeta_{p^n}),T\bigr)$, which is a Λ-module of rank 1.
Perrin-Riou has constructed a Coleman map $\mathrm{Col}\colon \mathbf{H}^1_s(T)\to\Lambda$. Proposition 17.11 in [10] shows that the Coleman map $\mathrm{Col}\colon \mathbf{H}^1_s(T)\to\Lambda$ is injective and has finite cokernel if the reduction of E at p is good. The same proof also applies when the reduction is non-split multiplicative. Instead in the case when E has split multiplicative reduction, then Theorem 4.1 in [11] proves that the Coleman map $\mathrm{Col}\colon \mathbf{H}^1_s(T)\to\Lambda$ is injective and has image with finite index inside $I=\ker\bigl(\mathbb{1}\colon\Lambda\to\mathbb{Z}_p\bigr)$ where the map $\mathbb{1}$ sends all elements of the Galois group $\mathrm{Gal}\bigl(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}\bigr)$ to 1. Extend Col to an injective map $\mathrm{Col}\colon \mathbf{H}^1_s(T)\otimes\mathbb{Q}_p\to\Lambda\otimes\mathbb{Q}_p$.
Choose $\gamma\in T$ such that $\gamma=\gamma^+ + \gamma^-$ with $\gamma^\pm$ being $\mathbb{Z}_p$-generators of the subspaces $T^\pm$ on which the complex conjugation acts by ±1. We now apply Theorem 16.6 in [10] with this "good choice" of γ and with the "good choice" of the Néron differential $\omega=\omega_{E_\bullet}$ in the terminology of 17.5. Consider the zeta element $\mathbf{z}=z_\gamma\in\mathbf{H}^1(T)\otimes\mathbb{Q}_p$. The theorem yields

$$\mathrm{Col}\bigl(\mathrm{loc}(\mathbf{z})\bigr)=L_p(E_\bullet)\in\Lambda,$$

where $\mathrm{loc}\colon \mathbf{H}^1(T)\otimes\mathbb{Q}_p\to\mathbf{H}^1_s(T)\otimes\mathbb{Q}_p$ is the localisation followed by the quotient map.
Let $Z_T=Z(f,T)$ be the Λ-module generated by z_γ in $\mathbf{H}^1(T)\otimes\mathbb{Q}_p$ and let Z be the Λ-submodule of $\mathbf{H}^1(T)$ generated by all $\bigl({}_{c,d}z_{p^n}(\alpha)\bigr)_n$ and $\bigl({}_{c,d}z_{p^n}(\tfrac{a}{A})\bigr)_n$ where c, d, a, A and α run over all permitted choices in the construction of these integral elements. Then Theorem 12.6 in [10] states that Z is contained in Z_T with finite index. Here it is crucial that we work with exactly the lattice $T=V_{\mathbb{Z}_p}(f)(1)$. Kato allows himself the flexibility of twists by the cyclotomic character and works with $V_{\mathbb{Z}_p}(f)(r)$; we only need $r=1$ here.
Since $\mathbf{H}^1(T)$ is Λ-torsion-free, there is an injective Λ-morphism $\iota\colon\mathbf{H}^1(T)\to\Lambda$ with finite cokernel. The linear extension $\iota_{\mathbb{Q}}\colon\mathbf{H}^1(T)\otimes\mathbb{Q}_p\to\Lambda\otimes\mathbb{Q}_p$ sends Z_T to a sub-Λ-module J. This J contains the integral ideal $\iota(Z)\subset\Lambda$ with finite index. Hence J itself is an integral ideal in Λ. Write $\lambda=\iota_{\mathbb{Q}}(\mathbf{z})\in J$.

Lemma 11. *For any $k\geqslant 0$ such that $p^kZ_T\subset Z$, the index of $p^k\mathbf{z}$ in $\mathbf{H}^1(T)$, defined as*

$$I=\mathrm{ind}_\Lambda(p^k\mathbf{z})=\Bigl\{\psi\bigl(p^k\mathbf{z}\bigr)\ \Big|\ \psi\in\mathrm{Hom}_\Lambda(\mathbf{H}^1(T),\Lambda)\Bigr\},$$

satisfies $I_{\mathfrak{p}}=\lambda\Lambda_{\mathfrak{p}}$ for all height one prime ideals $\mathfrak{p}$ of Λ that do not contain p.

Proof. Let $\mathfrak{p}\not\ni p$ be prime ideal of Λ of height 1. Because ι has finite cokernel, we have $\mathbf{H}^1(T)_{\mathfrak{p}}=\Lambda_{\mathfrak{p}}$ via ι. Hence

$$\begin{aligned}I_{\mathfrak{p}}&=\Bigl\{\psi\bigl(p^k\mathbf{z}\bigr)\ \Big|\ \psi\in\mathrm{Hom}_{\Lambda_{\mathfrak{p}}}(\mathbf{H}^1(T)_{\mathfrak{p}},\Lambda_{\mathfrak{p}})\Bigr\}\\&=\Bigl\{\tilde\psi\bigl(\iota(p^k\mathbf{z})\bigr)\ \Big|\ \tilde\psi\in\mathrm{Hom}_{\Lambda_{\mathfrak{p}}}(\Lambda_{\mathfrak{p}},\Lambda_{\mathfrak{p}})\Bigr\}\\&=\iota(p^k\mathbf{z})\Lambda_{\mathfrak{p}}=p^k\lambda\Lambda_{\mathfrak{p}}=\lambda\Lambda_{\mathfrak{p}}.\end{aligned}$$

because p does not belong to $\mathfrak{p}$. $\square$

3.3 Integrality of z_γ

Recall first how Kato deduces the integrality of his second set of zeta-elements in the case $E[p]$ is irreducible.

Lemma 12. *If $\mathbf{H}^1(T)$ is free over Λ then $z_\gamma \in \mathbf{H}^1(T)$ for all $\gamma \in T$.*

Proof. This is 13.14 in [10]: For every prime ideal $\mathfrak{p}$ of height 1 in Λ, we have $(Z_T)_{\mathfrak{p}} \subset \mathbf{H}^1(T)_{\mathfrak{p}}$ since Z has finite index in Z_T. Hence $Z_T \subset \mathbf{H}^1(T)$. $\square$

We will concentrate here on one case that interests us most. Let $\mathbf{z}_0$ be the corestriction of $\mathbf{z}$ from $\mathbf{H}^1(T)$ to $\mathbf{H}^1(T)_0$, which is the limit $\varprojlim_n H^1\bigl(G_\Sigma(K_n), T\bigr)$ as K_n increases in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Theorem 13. *Let $E/\mathbb{Q}$ be an elliptic curve and p an odd prime at which E has good reduction. Then $\mathbf{z}_0$ belongs to $\mathbf{H}^1(T)_0$.*

In other words $\mathbf{z}_0$ is integral with respect to the Tate module of $E_\bullet$.

Proof. First, we may apply the idea of the proof in Lemma 9, to conclude that $\mathbf{H} = \mathbf{H}^1(T)_0$ is free over $\Lambda(\Gamma)$ if $E_\bullet(\mathbb{Q})$ has no p-torsion point. If so the previous lemma shows that $\mathbf{z}_0$ lies in $\mathbf{H}$.
Assume now that $E_\bullet$ admits a rational p-torsion point. Let $\phi\colon E_\bullet \to E'$ be the isogeny whose kernel contains the rational p-torsion points. We apply Lemma 10 to see that either $\mathbf{H}$ is free or it injects into $\Lambda(\Gamma)$ with index p. As the former case is done with the previous lemma, we assume that we are in the latter. We know already that the Coleman map $\mathrm{Col}_0\colon \mathbf{H} \to \Lambda(\Gamma)$ is injective with finite cokernel. Now, since $\mathbf{H}$ is isomorphic to the maximal ideal, the image of Col_0 has to be equal to the maximal ideal of $\Lambda(\Gamma)$. Therefore if $\mathbf{z}_0$ is not integral, the image $\mathrm{Col}_0\bigl(\mathrm{loc}(\mathbf{z}_0)\bigr) = L_p(E_\bullet)_0 \in \Lambda_0 = \Lambda(\Gamma)$ must be a unit. However the interpolation property of the p-adic L-function tells us that

$$\mathbb{1}\bigl(L_p(E_\bullet)_0\bigr) = \bigl(1-\alpha^{-1}\bigr)^2 \cdot [0]^+_{E_\bullet}$$

where α is the unit root of the characteristic polynomial of Frobenius and the map $\mathbb{1}\colon \Lambda(\Gamma) \to \mathbb{Z}_p$ sends all elements of Γ to 1. Since we have a p-torsion point on the reduction of $E_\bullet$ to $\mathbb{F}_p$, the valuation of $1-\alpha^{-1}$ is 1. By construction of $E_\bullet$ the modular symbol $[0]^+_{E_\bullet}$ is a p-adic integer. Therefore the p-adic L-function cannot be a unit. Hence $\mathbf{z}_0$ is integral. $\square$

4 The fine Selmer group

Let E be an elliptic curve with a p-isogeny for an odd prime p. In this section, we do not need any condition on the type of reduction at p. We define the fine[2]

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

Selmer group $\mathcal{R}\big(E/\mathbb{Q}(\zeta_{p^n})\big)$ as the kernel of the localisation map

$$H^1\Big(G_\Sigma\big(\mathbb{Q}(\zeta_{p^n})\big), E[p^\infty]\Big) \longrightarrow \bigoplus_{v\in\Sigma} H^1\Big(\mathbb{Q}_v(\zeta_{p^n}), E[p^\infty]\Big)$$

where the sum runs over all places v in $\mathbb{Q}(\zeta_{p^n})$ above those in Σ. It is independent of the choice of the finite set Σ as long as it contains p and all the places of bad reduction. By global duality it is dual to the kernel

$$H^2\Big(G_\Sigma\big(\mathbb{Q}(\zeta_{p^n})\big), T_pE\Big) \longrightarrow \bigoplus\nolimits_{v\in\Sigma} H^2\Big(\mathbb{Q}_v(\zeta_{p^n}), T_pE\Big).$$

The Pontryagin dual of the direct limit of the groups $\mathcal{R}(E/\mathbb{Q}(\zeta_{p^n}))$ will be denoted by $Y(E)$; it is a finitely generated Λ-module. Theorem 13.4.1 in [10] proves that $Y(E)$ is Λ-torsion.

Lemma 14. *Let E be an elliptic curve and p an odd prime such that E admits an isogeny of degree p defined over $\mathbb{Q}$. Then the fine Selmer group $Y(E)$ is a finitely generated $\mathbb{Z}_p$-module.*

Proof. Let $\phi\colon E \to E'$ be an isogeny with cyclic kernel $E[\phi]$ of order p defined over $\mathbb{Q}$. The extension F of $\mathbb{Q}$ fixed by the kernel of $\rho_\phi\colon G_\Sigma\big(\mathbb{Q}\big) \to \mathrm{Aut}\big(E[\phi]\big)$ is a cyclic extension of degree dividing $p-1$. Let G be the Galois group of $K = F(\zeta_p)$ over $\mathbb{Q}(\zeta_p)$. Over the abelian field K, the curve admits a p-torsion point. We can therefore apply Corollary 3.6 in [3] (a consequence of the Theorem of Ferrero-Washington) to the dual $Y(E/K_\infty)$ of the Selmer group over the cyclotomic $\mathbb{Z}_p$-extension $K_\infty = K(\zeta_{p^\infty})$ of K. This proves that $Y(E/K_\infty)$ is a finitely generated $\mathbb{Z}_p$-module. Then we have the following diagram

$$\begin{tikzcd}
0 \arrow[r] & \widehat{Y(E/K_\infty)}^{\Delta} \arrow[r] & H^1\big(G_\Sigma(K_\infty), E[p^\infty]\big)^{\Delta} \\
0 \arrow[r] & \widehat{Y(E)} \arrow[r] \arrow[u] & H^1\big(G_\Sigma(\mathbb{Q}(\zeta_{p^\infty})), E[p^\infty]\big) \arrow[u] \\
& & H^1\big(G, E(K_\infty)[p^\infty]\big) \arrow[u]
\end{tikzcd}$$

and since the group G 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 $Y(E/K_\infty) \to Y(E)$ is surjective. Therefore $Y(E)$ is a finitely generated $\mathbb{Z}_p$-module. ☐

For any torsion Λ-module M, we define the characteristic series $\mathrm{char}_\Lambda(M)$ as the product of the ideals $\mathfrak{p}^{l_\mathfrak{p}}$ where $l_\mathfrak{p} = \mathrm{length}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p})$ as $\mathfrak{p}$ runs through all primes of height 1 in Λ.
Recall that we have defined $\lambda = \iota_{\mathbb{Q}}(\mathbf{z})$ as an element in $J \subset \Lambda$ just before Lemma 11.

PROPOSITION 15. *Suppose E does not have additive reduction at p. Then the characteristic series* $\mathrm{char}_\Lambda\bigl(Y(E)\bigr)$ *divides* $\lambda\,\Lambda$.

Proof. We will first prove this proposition in the case E is the curve $E_\bullet$ in Theorem 4. With a sufficiently large choice of k, the element $p^k\cdot\mathbf{z}\in Z\cap\mathbf{H}^1(T)$ extends to an Euler system for T as in [21]. Since the representation ρ_p is not surjective, the Euler system argument gives us only a divisibility of the form

$$\mathrm{char}_\Lambda\bigl(Y(E)\bigr)\qquad\text{divides}\qquad J\cdot\mathrm{ind}_\Lambda\bigl(p^k\mathbf{z}\bigr)$$

for some ideal J of Λ which is a product of primes containing p, see Theorem 2.3.4 in [21] or Theorem 13.4 in [10]. By Lemma 11, we know that $\mathrm{ind}_\Lambda\bigl(p^k\mathbf{z}\bigr)=J'\lambda\,\Lambda$ for some ideal J' which is a product of primes containing p. The previous lemma shows that $\mathrm{char}_\Lambda(Y(E))$ is not divisible by any prime ideal containing p, so the proposition follows for $E_\bullet$.
Now an isogeny $E\to E_\bullet$ can only change the μ-invariants of the dual of the fine Selmer groups, i.e. only by ideals containing p, but the previous lemma shows that they are zero for all curves in the isogeny class. ☐

5 THE FIRST DIVISIBILITY IN THE MAIN CONJECTURE

Let E be an elliptic curve defined $\mathbb{Q}$ such that $E[p]$ is reducible for some odd prime of semi-stable reduction. Recall that this implies that the reduction of E at p can not be good supersingular. The Selmer group E over $\mathbb{Q}(\zeta_{p^n})$ is defined as usual as the elements in $H^1\bigl(G_\Sigma(\mathbb{Q}(\zeta_{p^n})),E[p^\infty]\bigr)$ that are locally in the image of the points. It fits into the exact sequence

$$0\longrightarrow\mathcal{R}\bigl(E/\mathbb{Q}(\zeta_{p^n})\bigr)\longrightarrow\mathrm{Sel}\bigl(E/\mathbb{Q}(\zeta_{p^n})\bigr)\longrightarrow H^1\bigl(\mathbb{Q}_p(\zeta_{p^n}),E[p^\infty]\bigr).$$

We denote the dual of the limit of the Selmer group by $X(E)$; it is a finitely generated Λ-module. If the reduction is good ordinary, Theorem 17.4 in [10] shows that $X(E)$ is Λ-torsion. The same conclusion holds in general in our situation; see [11] for the split multiplicative case.

THEOREM 16. *Let $E/\mathbb{Q}$ be an elliptic curve and let $p>2$ be a prime. Suppose that E has semi-stable reduction at p and that $E[p]$ is reducible as a $G_\mathbb{Q}$-module. Then $\mathrm{char}_\Lambda\bigl(X(E)\bigr)$ divides the ideal generated by $L_p(E)$. If the reduction of E is split multiplicative at p, then $I\cdot\mathrm{char}_\Lambda\bigl(X(E)\bigr)$ divides the ideal generated by $L_p(E)$, where I is the kernel of the homomorphism $\Lambda\to\mathbb{Z}_p$ that sends all elements of $\mathrm{Gal}\bigl(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}\bigr)$ to 1.*

The main conjecture asserts that the element $L_p(E)$ generates the characteristic ideal $\mathrm{char}_\Lambda\bigl(X(E)\bigr)$.

LEMMA 17. *To prove Theorem 16 for E, it is sufficient to prove it for any one curve in the isogeny class of E.*

Proof. The fact that Theorem 16 is invariant under isogenies follows from the formula for the change of the μ-invariant under isogenies for the characteristic series by Perrin-Riou [16, Appendice] when compared to the change of the p-adic L-function. See in particular her Lemme on page 455. □

Proof of Theorem 16. By the previous Lemma 17, we may choose E to be the curve $E_\bullet$ in the isogeny class. Recall from Section 3.2 that the Coleman map $\mathrm{Col}\colon \mathbf{H}^1_s(T) \to \Lambda$ is injective and has image with finite index inside I in the multiplicative case and it has a finite cokernel in the other cases. In what follows we treat only the case when the reduction is not split multiplicative; otherwise one has to multiply with I where appropriate.
Rohrlich [20] has shown that $L_p(E)$ is non-zero and hence $\mathrm{loc}(\mathbf{z})$ is not torsion. Choose a k such that $p^k Z_T \subset Z$. Then the Λ-torsion module $\mathbf{H}^1_s(T)/p^k\,\mathrm{loc}(\mathbf{z})\Lambda$, which is equal to $\mathrm{Col}\bigl(\mathbf{H}^1_s(T)\bigr)/p^k L_p(E)\,\Lambda$, has characteristic series $p^k L_p(E)\Lambda$. The characteristic series of $\mathbf{H}^1(T)/p^k\mathbf{z}\Lambda$ is equal to the characteristic series of $\Lambda/\iota(p^k\mathbf{z})\Lambda$ and therefore equal to $p^k\lambda\Lambda$, where $\iota\mathbf{H}^1(T) \to \Lambda$ is an injective Λ-morphism with finite cokernel.
By global duality (see Proposition 1.3.2 in [18]), we have the following exact sequence

$$0 \longrightarrow \mathbf{H}^1(T) \longrightarrow \mathbf{H}^1_s(T) \longrightarrow X(E) \longrightarrow Y(E) \longrightarrow 0.$$

It induces an exact sequence of torsion Λ-modules

$$0 \longrightarrow \frac{\mathbf{H}^1(T)}{p^k\mathbf{z}\,\Lambda} \longrightarrow \frac{\mathbf{H}^1_s(T)}{p^k\mathbf{z}\Lambda} \longrightarrow X(E) \longrightarrow Y(E) \longrightarrow 0.$$

Using Proposition 15, we conclude that

$$\begin{aligned}\mathrm{char}_\Lambda\bigl(X(E)\bigr) &= \mathrm{char}_\Lambda\bigl(Y(E)\bigr)\cdot\bigl(p^k L_p(E)\Lambda\bigr)\cdot\bigl(p^k\lambda\,\Lambda\bigr)^{-1}\\ &\text{divides } \lambda\cdot p^k L_p(E)\cdot p^{-k}\lambda^{-1}\Lambda = L_p(E)\Lambda.\end{aligned}$$ □

6 Consequences

Corollary 18. *The analytic p-adic L-function $L_p(E)$ belongs to Λ for all elliptic curves $E/\mathbb{Q}$ with semi-stable 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 [19] where it is shown how one can extract integral power series.

Corollary 19. *If $E/\mathbb{Q}$ is a semi-stable elliptic curve and p an odd prime where E has ordinary reduction, then $\mathrm{char}_\Lambda\bigl(X(E)\bigr)$, or $I\,\mathrm{char}_\Lambda\bigl(X(E)\bigr)$ in the split multiplicative case, divides the ideal generated by $L_p(E)$.*

Proof. By a Theorem of Serre ([24, Proposition 1] and [22, Proposition 21]), we know that the image of the representation $\bar{\rho}_p \colon G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ 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 $\bar{\rho}_p$ is reducible and in the first case the representation $\rho_p \colon G_{\mathbb{Q}} \to \mathrm{Aut}(T_pE)$ is surjective by another result of Serre [23, Lemme 15] unless $p = 3$. Finally for $p = 3$ we use the following lemma to exclude that ρ_p is not surjective. ☐

Unfortunately, the hypothesis in Corollary 19 that E is semi-stable can not be dropped. For instance, there are curves $E/\mathbb{Q}$ such that $\bar{\rho}_p$ has its image in the normaliser of a non-split Cartan subgroup.

LEMMA 20. *Let $p = 3$ and suppose p^2 does not divide the conductor N. If the residual representation $\bar{\rho} \colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective then the p-adic representation $\rho \colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p)$ is surjective, too.*

Proof. We make use of the explicit parametrisation of all these exotic cases by Elkies in [8]. Let $E/\mathbb{Q}$ be an elliptic curve such that ρ is not surjective, but $\bar{\rho}$ is. Then its j-invariant satisfies

$$j(E) = 1728 - \frac{27\, A(n:m)^2\, B(n:m)^2\, C(n:m)}{D(n:m)^9} \qquad \text{with}$$
$$A(n:m) = n^6 + 6n^5m + 4n^3m^3 + 12n^2m^4 - 18nm^5 - 23m^6,$$
$$B(n:m) = 7n^6 + 24n^5m + 18n^4m^2 - 26n^3m^3 - 33n^2m^4 + 18nm^5 + 28m^6,$$
$$C(n:m) = 2n^3 - 3n^2m + 4m^3,$$
$$D(n:m) = n^3 - 3nm^3 - m^3.$$

for two coprime integers n and m. Note first that the denominator $D(n:m)$ in $j(E)$ is never divisible by 9, so $j(E)$ is a 3-adic integer.
With a bit more work one can see that $j(E) \equiv 2 \cdot 3^3 \pmod{3^4}$: If $n \not\equiv m \pmod 3$, then $A(n:m) \equiv (n-m)^6 \equiv B(n:m) \pmod 3$, $C(n:m) \equiv 2(n-m)^3$ and $D(n:m) \equiv (n-m)^3 \pmod 3$ gives the result. For $n = m + 3k$, we can use $A(n:m) \equiv B(n:m) \equiv 3^2 \pmod{3^3}$, $C(n:m) \equiv 3 \pmod{3^2}$, and $D(n:m) \equiv 2 \cdot 3 \pmod{3^2}$ to conclude.
Now suppose E is given by a Weierstrass equation minimal at 3. We may assume that it is of the form $y^2 = x^3 + a_2x^2 + a_4x + a_6$ with $a_2 \in \{-1, 0, +1\}$ and a_4, $a_6 \in \mathbb{Z}$. If $a_2 = \pm 1$, then

$$j(E) = 16 \frac{-27a_4^3 + 27a_4^2 - 9a_4 + 1}{\Delta}$$

where Δ is the discriminant. However this is a contradiction with $j(E) \in 3^3\mathbb{Z}_3$. Hence $a_2 = 0$ and so

$$j(E) = 3^3 \cdot 2^6 \cdot \frac{a_4^3}{a_4^3 + 27a_6^2/4}$$

and we see that it is impossible that $j(E) \equiv 2 \cdot 3^3 \pmod{3^4}$ unless 3 divides a_4 and the discriminant $\Delta = 4a_4^3 + 27a_6^2$. Therefore E has bad reduction at 3. The fact that $j(E)$ is a 3-adic integer shows that the reduction is additive. □

Finally, here is the usual application to the Birch and Swinnerton-Dyer conjecture.

Proposition 21. *Let E be an elliptic curve over $\mathbb{Q}$ such that $L(E,1) \neq 0$. Let c_v be the Tamagawa number of E at each finite place v and the number of components in $E(\mathbb{R})$ for $v = \infty$. Then*

$$\#Ш(E/\mathbb{Q}) \qquad \textit{divides} \qquad C \cdot \frac{L(E,1)}{\Omega_E^+} \cdot \frac{\bigl(\#E(\mathbb{Q})\bigr)^2}{\prod_v c_v}$$

where C is a rational number only divisible by 2, primes of additive reduction or primes for which the Galois representation on $E[p]$ is neither surjective nor contained in a Borel subgroup.

In particular, for semi-stable curve C is a power of 2. The methods in [26] can now be extended to the reducible case, too.

References

[1] Amod Agashe, Kenneth Ribet, and William A. Stein, *The Manin constant*, Pure Appl. Math. Q. 2 (2006), no. 2, part 2, 617–636.

[2] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), no. 4, 843–939.

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

[4] ———, *Cyclotomic fields and zeta values*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006.

[5] John E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, 1997.

[6] Daniel Delbourgo, *Elliptic curves and big Galois representations*, London Mathematical Society Lecture Note Series, vol. 356, Cambridge University Press, Cambridge, 2008.

[7] Vladimir G. Drinfeld, *Two theorems on modular curves*, Funkcional. Anal. i Priložen. 7 (1973), no. 2, 83–84.

[8] Noam Elkies, *Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9*, preprint available at `http://arxiv.org/abs/math/0612734`, 2006.

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

[10] 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.

[11] Shinichi Kobayashi, *An elementary proof of the Mazur-Tate-Teitelbaum conjecture for elliptic curves*, Doc. Math. (2006), no. Extra Vol., 567–575.

[12] Yuri I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), 19–66.

[13] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. 44 (1978), no. 2, 129–162.

[14] Barry Mazur, John Tate, and Jeremy Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. 84 (1986), no. 1, 1–48.

[15] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2000.

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

[17] ———, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble) 43 (1993), no. 4, 945–995.

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

[19] 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.

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

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

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

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

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

[25] Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for* GL_2, to be published in Invent. Math; preprint available `www.math.columbia.edu/~urban/eurp/MC.pdf`, 2013.

[26] William Stein and Christian Wuthrich, *Algorithms for the arithmetic of elliptic curves using Iwasawa theory*, Math. Comp. 82 (2013), no. 283, 1757–1792.

[27] Glenn Stevens, *Arithmetic on modular curves*, Progress in Mathematics, vol. 20, Birkhäuser Boston Inc., Boston, MA, 1982.

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

[29] Vinayak Vatsal, *Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves*, J. Inst. Math. Jussieu 4 (2005), no. 2, 281–316.

[30] Christian Wuthrich, *Extending Kato's result to elliptic curves with p-isogenies*, Math. Res. Lett. 13 (2006), no. 5, 713–718.

Christian Wuthrich
School of Mathematical Sciences
University of Nottingham
Nottingham NG7 2RD
United Kingdom