EULER SYSTEMS AND MODULAR ELLIPTIC CURVES

KARL RUBIN

Introduction

This paper consists of two parts. In the first we present a general theory of Euler systems. The main results (see §§3 and 4) show that an Euler system for a p-adic representation T gives a bound on the Selmer group associated to the dual module $\mathrm{Hom}(T, \boldsymbol{\mu}_{p^\infty})$. These theorems, which generalize work of Kolyvagin [Ko], have been obtained independently by Kato [Ka1], Perrin-Riou [PR2], and the author [Ru3]. We will not prove these theorems here, or even attempt to state them in the greatest possible generality.

In the second part of the paper we show how to apply the results of Part I and an Euler system recently constructed by Kato [Ka2] (see the article of Scholl [Scho] in this volume) to obtain Kato's theorem in the direction of the Birch and Swinnerton-Dyer conjecture for modular elliptic curves (Theorem 8.1).

Part 1. Generalities

1. Selmer groups attached to p-adic representations

A *p-adic representation* of $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ is a free $\mathbf{Z}_p$-module T of finite rank with a continuous, $\mathbf{Z}_p$-linear action of $G_{\mathbf{Q}}$. We will assume in addition throughout this paper that T is unramified outside of a finite set of primes.

Given a p-adic representation T, we also define

$$V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p,$$
$$W = V/T = T \otimes \mathbf{Q}_p/\mathbf{Z}_p.$$

(Note that T determines V and W, and W determines T and V, but in general there may be non-isomorphic $\mathbf{Z}_p$-lattices T giving rise to the same vector space V.)

The following are basic examples of p-adic representations to keep in mind.

Example. If $\rho : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ is a continuous character we can take T to be a free, rank-one $\mathbf{Z}_p$-module with $G_{\mathbf{Q}}$ acting via ρ (clearly every one-dimensional representation arises in this way). For example, when ρ is the cyclotomic character we get

$$T = \mathbf{Z}_p(1) = \varprojlim_n \boldsymbol{\mu}_{p^n}.$$

Example. If A is an abelian variety we can take the p-adic Tate module of A

$$T = T_p(A) = \varprojlim_n A_{p^n}.$$

This is the situation we will concentrate on in this paper, when A is an elliptic curve.

---

partially supported by NSF grant DMS-9306287.

Example. If T is a p-adic representation, then we define the dual representation

$$T^* = \mathrm{Hom}(T, \mathbf{Z}_p(1))$$

and we denote the corresponding vector space and divisible group by

$$V^* = T^* \otimes \mathbf{Q}_p = \mathrm{Hom}(V, \mathbf{Q}_p(1)), \quad W^* = V^*/T^* = \mathrm{Hom}(T, \boldsymbol{\mu}_{p^\infty}).$$

If E is an elliptic curve then the Weil pairing gives an isomorphism $T_p(E)^* \cong T_p(E)$.

Let $\mathbf{Q}_\infty \subset \mathbf{Q}(\boldsymbol{\mu}_{p^\infty})$ denote the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. For every n let $\mathbf{Q}_n \subset \mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}})$ be the extension of $\mathbf{Q}$ of degree p^n in $\mathbf{Q}_\infty$, and let $\mathbf{Q}_{n,p}$ denote the completion of $\mathbf{Q}_n$ at the unique prime above p.

Fix a p-adic representation T as above. We wish to define a Selmer group $\mathcal{S}(\mathbf{Q}_n, W) \subset H^1(\mathbf{Q}_n, W)$ for every n. If v is a place of $\mathbf{Q}_n$ not dividing p, let I_v denote an inertia group of v in $G_{\mathbf{Q}_n}$, let $\mathbf{Q}_{n,v}^{\mathrm{ur}}$ denote the maximal unramified extension of $\mathbf{Q}_{n,v}$, and define

$$\begin{aligned} H^1_{\mathcal{S}}(\mathbf{Q}_{n,v}, V) = H^1_{\mathrm{ur}}(\mathbf{Q}_{n,v}, V) &= \ker(H^1(\mathbf{Q}_{n,v}, V) \to H^1(\mathbf{Q}_{n,v}^{\mathrm{ur}}, V)) \\ &= H^1(\mathbf{Q}_{n,v}^{\mathrm{ur}}/\mathbf{Q}_{n,v}, V^{I_v}). \end{aligned}$$

For the unique prime of $\mathbf{Q}_n$ above p, we will ignore all questions about what is the "correct" definition, and we just fix some choice of subspace $H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V) \subset H^1(\mathbf{Q}_{n,p}, V)$. (For example, one could choose $H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V) = H^1(\mathbf{Q}_{n,p}, V)$ or $H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V) = 0$.)

For every place v of $\mathbf{Q}_n$ we now define

$$H^1_{\mathcal{S}}(\mathbf{Q}_{n,v}, W) \subset H^1(\mathbf{Q}_{n,v}, W) \quad \text{and} \quad H^1_{\mathcal{S}}(\mathbf{Q}_{n,v}, T) \subset H^1(\mathbf{Q}_{n,v}, T)$$

to be the image and inverse image, respectively, of $H^1_{\mathcal{S}}(\mathbf{Q}_{n,v}, V)$ under the maps on cohomology induced by the exact sequence

$$0 \to T \to V \to W \to 0.$$

Finally, we define

$$\mathcal{S}(\mathbf{Q}_n, W) = \ker\left(H^1(\mathbf{Q}_n, W) \to \bigoplus_{v \text{ of } \mathbf{Q}_n} H^1(\mathbf{Q}_{n,v}, W)/H^1_{\mathcal{S}}(\mathbf{Q}_{n,v}, W)\right).$$

Of course, this definition depends on the choice we made for $H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V)$.

2. Euler systems

Fix a p-adic representation T of $G_{\mathbf{Q}}$ as in §1, and fix a positive integer N divisible by p and by all primes where T is ramified. Define

$$\mathcal{R} = \mathcal{R}(N) = \{\text{squarefree integers } r : (r, N) = 1\}$$

For every prime q which is unramified in T, let Fr_q denote a Frobenius of q in $G_{\mathbf{Q}}$ and define the characteristic polynomial

$$P_q(x) = \det(1 - \mathrm{Fr}_q x | T) \in \mathbf{Z}_p[x].$$

Since q is unramified in T, P_q is independent of the choice of Frobenius element Fr_q.

Definition. An *Euler system* $\mathbf{c}$ for T is a collection of cohomology classes

$$\mathbf{c}_{\mathbf{Q}_n(\boldsymbol{\mu}_r)} \in H^1(\mathbf{Q}_n(\boldsymbol{\mu}_r), T)$$

for every $r \in \mathcal{R}$ and every $n \geq 0$, such that if $m \geq n$, q is prime, and $rq \in \mathcal{R}$, then

$$\mathrm{Cor}_{\mathbf{Q}_n(\boldsymbol{\mu}_{rq})/\mathbf{Q}_n(\boldsymbol{\mu}_r)} \mathbf{c}_{\mathbf{Q}_n(\boldsymbol{\mu}_{rq})} = P_q(q^{-1}\mathrm{Fr}_q^{-1}) \mathbf{c}_{\mathbf{Q}_n(\boldsymbol{\mu}_r)},$$
$$\mathrm{Cor}_{\mathbf{Q}_m(\boldsymbol{\mu}_r)/\mathbf{Q}_n(\boldsymbol{\mu}_r)} \mathbf{c}_{\mathbf{Q}_m(\boldsymbol{\mu}_r)} = \mathbf{c}_{\mathbf{Q}_n(\boldsymbol{\mu}_r)}.$$

Note that this definition depends on N (since $\mathcal{R}$ does), but not in an important way so we will suppress it from the notation.

Remarks. Kolyvagin's original method (see [Ko] or [Ru1]) required the Euler system to satisfy an additional "congruence" condition. The fact that our Euler system "extends in the $\mathbf{Q}_\infty$ direction" (i.e., consists of classes defined over the fields $\mathbf{Q}_n(\boldsymbol{\mu}_r)$ for every n, and not just over $\mathbf{Q}(\boldsymbol{\mu}_r)$) eliminates the need for the congruence condition.

There is some freedom in the exact form of the distribution relation in the definition of an Euler system. It is easy to modify an Euler system satisfying one distribution relation to obtain a new Euler system satisfying a slightly different one.

3. Results over $\mathbf{Q}$

We now come to the fundamental applications of an Euler system. For the proofs of Theorems 3.1, 3.2, and 4.1 see [Ka1], [PR2], or [Ru3]. In fact, once the setting is properly generalized the proofs are similar to the original method of Kolyvagin [Ko]; see also [Ru1] and [Ru2].

For this section and the next fix a p-adic representation T as in §1. Fix also a choice of subspaces $H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V)$ and $H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V^*)$ for every n, so that we have Selmer groups as defined in §1. We assume only that these choices satisfy the following conditions:

- $H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V)$ and $H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V^*)$ are orthogonal complements under the cup product pairing
$$H^1(\mathbf{Q}_{n,p}, V) \times H^1(\mathbf{Q}_{n,p}, V^*) \to H^2(\mathbf{Q}_{n,p}, \mathbf{Q}_p(1)) = \mathbf{Q}_p,$$
- if $m \geq n$ then
$$\mathrm{Cor}_{\mathbf{Q}_{m,p}/\mathbf{Q}_{n,p}} H^1_{\mathcal{S}}(\mathbf{Q}_{m,p}, V) \subset H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V),$$
$$\mathrm{Res}_{\mathbf{Q}_{m,p}} H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V) \subset H^1_{\mathcal{S}}(\mathbf{Q}_{m,p}, V)$$
and similarly for V^*.

We will write $H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, T) = H^1(\mathbf{Q}_{n,p}, T)/H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, T)$ (and similarly with T replaced by V or W), and we write $\mathrm{loc}_p^{\mathrm{ram}}$ for the localization map

$$\mathrm{loc}_p^{\mathrm{ram}} : H^1(\mathbf{Q}_n, T) \to H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, T).$$

We will make use of two different sets of hypotheses on the Galois representation T. Hypotheses $\mathrm{Hyp}(\mathbf{Q}_\infty, T)$ are stronger than $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$, and will allow us to prove a stronger conclusion.

Hypotheses $\mathrm{Hyp}(\mathbf{Q}_\infty, T)$. (i) There is a $\tau \in G_{\mathbf{Q}_\infty}$ such that

- τ acts trivially on $\boldsymbol{\mu}_{p^\infty}$,
- $T/(\tau - 1)T$ is free of rank one over $\mathbf{Z}_p$.

(ii) T/pT is an irreducible $\mathbf{F}_p[G_{\mathbf{Q}_\infty}]$-module.

Hypotheses $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$. (i) There is a $\tau \in G_{\mathbf{Q}_\infty}$ such that
- τ acts trivially on $\boldsymbol{\mu}_{p^\infty}$,
- $\dim_{\mathbf{Q}_p}(V/(\tau-1)V) = 1$.

(ii) V is an irreducible $\mathbf{Q}_p[G_{\mathbf{Q}_\infty}]$-module.

Theorem 3.1. *Suppose* $\mathbf{c}$ *is an Euler system for* T*, and* V *satisfies* $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$. *If* $\mathbf{c}_\mathbf{Q} \notin H^1(\mathbf{Q},T)_{\mathrm{tors}}$ *and* $[H^1_{/\mathcal{S}}(\mathbf{Q}_p,T) : \mathrm{loc}_p^{\mathrm{ram}}(H^1(\mathbf{Q},T))]$ *is finite, then* $\mathcal{S}(\mathbf{Q},W^*)$ *is finite. In particular if* $\mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}_\mathbf{Q}) \neq 0$ *and* $\mathrm{rank}_{\mathbf{Z}_p} H^1_{/\mathcal{S}}(\mathbf{Q}_p,T) = 1$*, then* $\mathcal{S}(\mathbf{Q},W^*)$ *is finite.*

Define $\Omega = \mathbf{Q}(W)\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})$, where $\mathbf{Q}(W)$ denotes the minimal extension of $\mathbf{Q}$ such that $G_{\mathbf{Q}(W)}$ acts trivially on W.

Theorem 3.2. *Suppose* $\mathbf{c}$ *is an Euler system for* T*, and* T *satisfies* $\mathrm{Hyp}(\mathbf{Q}_\infty, T)$. *If* $p > 2$ *and* $\mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}_\mathbf{Q}) \neq 0$ *then*

$$|\mathcal{S}(\mathbf{Q},W^*)| \le |H^1(\Omega/\mathbf{Q},W)||H^1(\Omega/\mathbf{Q},W^*)|[H^1_{/\mathcal{S}}(\mathbf{Q}_p,T) : \mathbf{Z}_p \mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}_\mathbf{Q})].$$

Remark. Hypotheses $\mathrm{Hyp}(\mathbf{Q}_\infty,T)$ are satisfied if the image of the Galois representation on T is "sufficiently large." They often hold in practice; see for example the discussion in connection with elliptic curves below. If $\mathrm{rank}_{\mathbf{Z}_p} T = 1$ then $\mathrm{Hyp}(\mathbf{Q}_\infty,T)$ holds with $\tau = 1$.

4. Results over $\mathbf{Q}_\infty$

Essentially by proving analogues of Theorem 3.2 for each field $\mathbf{Q}_n$, we can pass to the limit and prove an Iwasawa-theoretic version of Theorem 3.2.

Let Λ denote the Iwasawa algebra

$$\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]] = \varprojlim_n \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]],$$

so Λ is (noncanonically) isomorphic to a power series ring in one variable over $\mathbf{Z}_p$. If B is a finitely generated torsion Λ-module then there is a pseudo-isomorphism (a Λ-module homomorphism with finite kernel and cokernel)

$$B \to \bigoplus_i \Lambda/f_i\Lambda$$

with nonzero $f_i \in \Lambda$, and we define the characteristic ideal of B

$$\mathrm{char}(B) = \prod_i f_i\Lambda.$$

The characteristic ideal is well-defined, although the individual f_i are not. If B is not a finitely-generated torsion Λ-module we define $\mathrm{char}(B) = 0$.

Define Λ-modules

$$X_\infty = \mathrm{Hom}(\varinjlim_n \mathcal{S}(\mathbf{Q}_n,W^*), \mathbf{Q}_p/\mathbf{Z}_p).$$

and

$$H^1_{\infty,/\mathcal{S}}(\mathbf{Q}_p,T) = \varprojlim_n H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p},T).$$

(Our requirements on the choices of $H^1_\mathcal{S}(\mathbf{Q}_{n,p},V)$ and $H^1_\mathcal{S}(\mathbf{Q}_{n,p},V^*)$ ensure that if $m \ge n$, the restriction and corestriction maps induce maps

$$\mathcal{S}(\mathbf{Q}_n,W^*) \to \mathcal{S}(\mathbf{Q}_m,W^*) \quad \text{and} \quad H^1_{/\mathcal{S}}(\mathbf{Q}_{m,p},T) \to H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p},T)$$

so these limits are well-defined.) If $\mathbf{c}$ is an Euler system let $[\mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}_{\mathbf{Q}_n})]$ denote the corresponding element of $H^1_{\infty,/\mathcal{S}}(\mathbf{Q}_p, T)$.

Theorem 4.1. *Suppose that V satisfies* $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$, $\mathbf{c}$ *is an Euler system for T,* $[\mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}_{\mathbf{Q}_n})] \notin H^1_{\infty,/\mathcal{S}}(\mathbf{Q}_p, T)_{\mathrm{tors}}$*, and* $H^1_{\infty,/\mathcal{S}}(\mathbf{Q}_p, T)/\Lambda[\mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}_{\mathbf{Q}_n})]$ *is a torsion Λ-module. Define*

$$\mathcal{L} = \mathrm{char}(H^1_{\infty,/\mathcal{S}}(\mathbf{Q}_p, T)/\Lambda[\mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}_{\mathbf{Q}_n})]).$$

Then

(i) X_∞ *is a torsion Λ-module,*
(ii) *there is a nonnegative integer t such that* $\mathrm{char}(X_\infty)$ *divides $p^t\mathcal{L}$,*
(iii) *if T satisfies* $\mathrm{Hyp}(\mathbf{Q}_\infty, T)$ *then* $\mathrm{char}(X_\infty)$ *divides $\mathcal{L}$.*

Part 2. Elliptic curves

The 'Heegner point Euler system' for modular elliptic curves used by Kolyvagin in [Ko] does not fit into the framework of §2, because the cohomology classes are not defined over abelian extensions of $\mathbf{Q}$. However, Kato [Ka2] has constructed an Euler system for the Tate module of a modular elliptic curve, using Beilinson elements in the K-theory of modular curves. We now describe how, given Kato's Euler system and its essential properties, one can use the general results above to study the arithmetic of elliptic curves. The main result is Theorem 8.1 below.

5. Local cohomology groups

Suppose E is an elliptic curve defined over $\mathbf{Q}$, and take $T = T_p(E)$, the p-adic Tate module of E. Then $V = V_p(E) = T_p(E) \otimes \mathbf{Q}_p$ and $W = E_{p^\infty}$. The Weil pairing gives isomorphisms $V \cong V^*$, $T \cong T^*$, and $W \cong W^*$.

If B is an abelian group, we will abbreviate $B \otimes \mathbf{Z}_p = \varprojlim B/p^nB$, the p-adic completion of B, and

$$B \otimes \mathbf{Q}_p = (\varprojlim_n B/p^nB) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p, \quad B \otimes \mathbf{Q}_p/\mathbf{Z}_p = (\varprojlim_n B/p^nB) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p.$$

For every n define

$$H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V) = \mathrm{image}(E(\mathbf{Q}_{n,p}) \otimes \mathbf{Q}_p \hookrightarrow H^1(\mathbf{Q}_{n,p}, V)),$$

image under the natural Kummer map. Since $V = V^*$, this also fixes a choice of $H^1_{\mathcal{S}}(\mathbf{Q}_p, V^*)$, and this subgroup is its own orthogonal complement as required.

Let $\text{Ш}(E_{/\mathbf{Q}_n})$ denote the Tate-Shafarevich group of E over $\mathbf{Q}_n$.

Proposition 5.1. *With $H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V)$ as defined above, $\mathcal{S}(\mathbf{Q}_n, E_{p^\infty})$ is the classical p-power Selmer group of E over $\mathbf{Q}_n$, so there is an exact sequence*

$$0 \to E(\mathbf{Q}_n) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to \mathcal{S}(\mathbf{Q}_n, E_{p^\infty}) \to \text{Ш}(E_{/\mathbf{Q}_n})_{p^\infty} \to 0$$

Proof. If $v \nmid p$ then the p-part of $E(\mathbf{Q}_{n,v})$ is finite, and one can check easily that $H^1_{\mathcal{S}}(\mathbf{Q}_{n,v}, V_p(E)) = 0$. Therefore for every v, $H^1_{\mathcal{S}}(\mathbf{Q}_{n,v}, V_p(E))$ is the image of $E(\mathbf{Q}_{n,v}) \otimes \mathbf{Q}_p$ under the Kummer map. It follows that for every v, $H^1_{\mathcal{S}}(\mathbf{Q}_{n,v}, E_{p^\infty})$ is the image of $E(\mathbf{Q}_{n,v}) \otimes \mathbf{Q}_p/\mathbf{Z}_p$ under the corresponding Kummer map, and so the definition of $\mathcal{S}(\mathbf{Q}_n, E_{p^\infty})$ coincides with the classical definition of the Selmer group of E. □

For every n let $\tan(E_{/\mathbf{Q}_{n,p}})$ denote the tangent space of $E_{/\mathbf{Q}_{n,p}}$ at the origin and consider the Lie group exponential map

$$\exp_E : \tan(E_{/\mathbf{Q}_{n,p}}) \xrightarrow{\sim} E(\mathbf{Q}_{n,p}) \otimes \mathbf{Q}_p.$$

Fix a minimal Weierstrass model of E and let ω_E denote the corresponding holomorphic differential. Then the cotangent space $\mathrm{cotan}(E)$ is $\mathbf{Q}_{n,p}\omega_E$, and we let ω_E^* be the corresponding dual basis of $\tan(E)$. We have a commutative diagram

$$\begin{tikzcd}
\tan(E_{/\mathbf{Q}_{n,p}}) \arrow[rr, "\exp_E"] & & E(\mathbf{Q}_{n,p}) \otimes \mathbf{Q}_p \\
\lambda_E(\mathfrak{p}_n) \arrow[u, "\cdot\omega_E^*"] \arrow[r, "\sim"] & \hat{E}(\mathfrak{p}_n) \arrow[r, "\sim"] & E_1(\mathbf{Q}_{n,p}) \arrow[u]
\end{tikzcd}$$

where $\hat{E}$ is the formal group of E, λ_E is its logarithm map, $\mathfrak{p}_n$ is the maximal ideal of $\mathbf{Q}_{n,p}$, $E_1(\mathbf{Q}_{n,p})$ is the kernel of reduction in $E(\mathbf{Q}_p)$, and the bottom maps are the formal group exponential followed by the isomorphism of [T] Theorem 4.2. (Note that $\hat{E}(\mathfrak{p}_n)_{\mathrm{tors}} = 0$ because $\mathbf{Q}_p(\hat{E}_p)/\mathbf{Q}_p$ is totally ramified of degree $p-1$, so λ_E is injective.) Extending λ_E linearly we will view it as a homomorphism defined on all of $E(\mathbf{Q}_{n,p}) \otimes \mathbf{Q}_p$.

Since $V \cong V^*$,

$$\mathrm{Hom}(E(\mathbf{Q}_{n,p}), \mathbf{Q}_p) \cong \mathrm{Hom}(H^1_{\mathcal{S}}(\mathbf{Q}_{n,p}, V), \mathbf{Q}_p) \cong H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, V).$$

Thus there is a dual exponential map

$$\exp_E^* : H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, V) \xrightarrow{\sim} \mathrm{cotan}(E_{/\mathbf{Q}_{n,p}}) = \mathbf{Q}_{n,p}\omega_E.$$

We write $\exp^*_{\omega_E} : H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, V) \xrightarrow{\sim} \mathbf{Q}_{n,p}$ for the composition $\omega_E^* \circ \exp_E^*$ Since $H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, T)$ injects into $H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, V)$, $\exp^*_{\omega_E}$ is injective on $H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, T)$. The local pairing allows us to identify

$$\begin{tikzcd}
H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, V) \arrow[r, "\sim"] & \mathrm{Hom}(E(\mathbf{Q}_{n,p}), \mathbf{Q}_p) \\
H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, T) \arrow[u] \arrow[r, "\sim"] & \mathrm{Hom}(E(\mathbf{Q}_{n,p}), \mathbf{Z}_p).
\end{tikzcd} \tag{1}$$

Explicitly, $z \in H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, V)$ corresponds to the map

$$x \mapsto \mathrm{Tr}_{\mathbf{Q}_{n,p}/\mathbf{Q}_p} \lambda_E(x) \exp^*_{\omega_E}(z). \tag{2}$$

Proposition 5.2. $\exp^*_{\omega_E}(H^1_{/\mathcal{S}}(\mathbf{Q}_p, T)) = [E(\mathbf{Q}_p) : E_1(\mathbf{Q}_p) + E(\mathbf{Q}_p)_{\mathrm{tors}}]p^{-1}\mathbf{Z}_p$.

Proof. By (2),

$$\exp^*_{\omega_E}(H^1_{/\mathcal{S}}(\mathbf{Q}_p, T)) = p^a\mathbf{Z}_p$$

where

$$\lambda_E(E(\mathbf{Q}_p)) = p^{-a}\mathbf{Z}_p.$$

We have $\lambda_E(E_1(\mathbf{Q}_p)) = p\mathbf{Z}_p$ and, since $\mathrm{rank}_{\mathbf{Z}_p} E(\mathbf{Q}_p) = 1$,

$$[\lambda_E(E(\mathbf{Q}_p)) : \lambda_E(E_1(\mathbf{Q}_p)] = [E(\mathbf{Q}_p) : E_1(\mathbf{Q}_p) + E(\mathbf{Q}_p)_{\mathrm{tors}}].$$

Thus the proposition follows. $\square$

6. The p-adic L-function

Let

$$L(E,s)=\sum_{n\geq 1} a_n n^{-s}=\prod_q \ell_q(q^{-s})^{-1}$$

denote the Hasse-Weil L-function of E, where $\ell_q(q^{-s})$ is the usual Euler factor at q. If $N\in\mathbf{Z}^+$ we will also write

$$L_N(E,s)=\sum_{(n,N)=1} a_n n^{-s}=\prod_{q\nmid N}\ell_q(q^{-s})^{-1}$$

for the L-function with the Euler factors dividing N removed. If F is an abelian extension of $\mathbf{Q}$ of conductor f and $\gamma\in\mathrm{Gal}(F/\mathbf{Q})$, define the partial L-function

$$L_N(E,\gamma,F/\mathbf{Q},s)=\sum_{n\mapsto\gamma} a_n n^{-s}$$

where the sum is over n prime to fN which map to γ under

$$(\mathbf{Z}/f\mathbf{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_f)/\mathbf{Q})\twoheadrightarrow \mathrm{Gal}(F/\mathbf{Q}).$$

If χ is a character of $G_{\mathbf{Q}}$ of conductor f_χ, and $\ker(\chi)=\mathrm{Gal}(\bar{\mathbf{Q}}/F_\chi)$, let

$$\begin{aligned}L_N(E,\chi,s)&=\sum_{(n,f_\chi N)=1}\chi(n)a_n n^{-s}=\prod_{q\nmid f_\chi N}\ell_q(q^{-s}\chi(q))^{-1}\\ &=\sum_{\gamma\in\mathrm{Gal}(F_\chi/\mathbf{Q})}\chi(\gamma)L_N(E,\gamma,F_\chi/\mathbf{Q},s).\end{aligned}$$

When $N=1$ we write simply $L(E,\chi,s)$, and then we have

$$L_N(E,\chi,s)=\prod_{q\mid N}\ell_q(q^{-s}\chi(q))L(E,\chi,s). \tag{3}$$

If E is modular then these functions all have analytic continuations to $\mathbf{C}$.

Fix a generator $[\zeta_{p^n}]_n$ of $\varprojlim \boldsymbol{\mu}_{p^n}$. Write $G_n=\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})=\mathrm{Gal}(\mathbf{Q}_{n,p}/\mathbf{Q}_p)$. If χ is a character of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$ of conductor p^n define the Gauss sum

$$\tau(\chi)=\sum_{\gamma\in\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{p^n})/\mathbf{Q})}\chi(\gamma)\zeta_{p^n}^\gamma.$$

Fix also an embedding of $\bar{\mathbf{Q}}_p$ into $\mathbf{C}$ so that we can identify complex and p-adic characters of $G_{\mathbf{Q}}$.

The following theorem is proved in [MSD] in the case of good ordinary reduction. See [MTT] for the (even more) general statement.

Theorem 6.1. *Suppose E is modular and E has good ordinary reduction or multiplicative reduction at p. Let $\alpha\in\mathbf{Z}_p^\times$ and $\beta\in p\mathbf{Z}_p$ be the eigenvalues of Frobenius if E has good ordinary reduction at p, and let $(\alpha,\beta)=(1,p)$ (resp. $(-1,-p)$) if E has split (resp. nonsplit) multiplicative reduction. Then there is a nonzero integer c_E independent of p, and a p-adic L-function $\mathcal{L}_E\in c_E^{-1}\Lambda$ such that for every character χ of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$ of finite order,*

$$\chi(\mathcal{L}_E)=\begin{cases}(1-\alpha^{-1})^2L(E,1)/\Omega_E & \text{if } \chi=1 \text{ and } E \text{ has good reduction at } p\\ (1-\alpha^{-1})L(E,1)/\Omega_E & \text{if } \chi=1 \text{ and } E \text{ is multiplicative at } p\\ \alpha^{-n}\tau(\chi)L(E,\chi^{-1},1)/\Omega_E & \text{if } \chi \text{ has conductor } p^n>1\end{cases}$$

where Ω_E is the fundamental real period of E.

If $N \in \mathbf{Z}^+$, define

$$\mathcal{L}_{E,N} = \prod_{q|N, q\neq p} \ell_q(q^{-1}\mathrm{Fr}_q^{-1})\mathcal{L}_E \in \Lambda.$$

Using (3) and Theorem 6.1 one obtains analogous expressions for $\chi(\mathcal{L}_{E,N})$ in terms of $L_N(E,\chi^{-1},1)$

7. Kato's Euler system

The following theorem of Kato is crucial for everything that follows.

Theorem 7.1 (Kato [Ka1], see also [Scho]). *Suppose that E is modular, and let N be the conductor of E. There are a positive integer r_E independent of p, positive integers $D \not\equiv 1$, $D' \not\equiv 1 \pmod{p}$, and an Euler system $\bar{\mathbf{c}} = \bar{\mathbf{c}}(D,D')$ for $T_p(E)$,*

$$\{\bar{\mathbf{c}}_{\mathbf{Q}_n(\boldsymbol{\mu}_r)} \in H^1(\mathbf{Q}_n(\boldsymbol{\mu}_r), T_p(E)) : r \text{ squarefree}, (r, NpDD') = 1, n \geq 0\}$$

such that for every such $n \geq 0$ and every character $\chi : \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}) \to \mathbf{C}^\times$,

$$\sum_{\gamma \in \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})} \chi(\gamma) \exp^*_{\omega_E}(\mathrm{loc}_p^{\mathrm{ram}}(\bar{\mathbf{c}}^\gamma_{\mathbf{Q}_n}))$$
$$= r_E DD'(D - \chi^{-1}(D))(D' - \chi^{-1}(D'))L_{Np}(E,\chi,1)/\Omega_E.$$

Proof. See the paper of Scholl [Scho] in this volume (especially Theorem 5.2.7) for the proof of this theorem when $p > 2$ and E has good reduction at p. □

Using the Coleman map $\mathrm{Col}_\infty : H^1_{\infty,/\mathcal{S}}(\mathbf{Q}_{n,p}, T) \to \Lambda$ described in the Appendix, we can relate Kato's Euler system to the p-adic L-function.

Corollary 7.2. *With hypotheses and notation as in Theorems 7.1 and 6.1, there is an Euler system $\mathbf{c}$ for $T_p(E)$ such that*
(i) $\exp^*_{\omega_E}(\mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}_{\mathbf{Q}})) = r_E L_{Np}(E,1)/\Omega_E$,
(ii) $\mathrm{Col}_\infty([\mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}_{\mathbf{Q}_n})]) = r_E \mathcal{L}_{E,N}$.

Proof. Let $\bar{\mathbf{c}}$ be the Euler system of Theorem 7.1 for some $D, D' \not\equiv 1 \pmod{p}$. Let $\sigma_D \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})/\mathbf{Q})$ denote the automorphism $\zeta \mapsto \zeta^D$ for $\zeta \in \boldsymbol{\mu}_{p^\infty}$, and similarly for $\sigma_{D'}$.

Since $D, D' \not\equiv 1 \pmod{p}$, $(D - \sigma_D)(D' - \sigma_{D'})$ is invertible in Λ. Let $\rho_{D,D'} \in \mathbf{Z}_p[[G_{\mathbf{Q}}]]$ be any element which restricts to $(D - \sigma_D)^{-1}(D' - \sigma_{D'})^{-1}$ in Λ, and define

$$\mathbf{c}_{\mathbf{Q}_n(\boldsymbol{\mu}_r)} = D^{-1}{D'}^{-1}\rho_{D,D'}\bar{\mathbf{c}}_{\mathbf{Q}_n(\boldsymbol{\mu}_r)}.$$

It is clear that $\{\mathbf{c}_{\mathbf{Q}_n(\boldsymbol{\mu}_r)}\}$ is still an Euler system, and for every $n \geq 0$ and every character $\chi : \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}) \to \mathbf{C}^\times$

$$\chi(\rho_{D,D'}) = \chi((D - \sigma_D)(D' - \sigma_{D'}))^{-1} = (D - \chi(D))^{-1}(D' - \chi(D'))^{-1},$$

so by Theorem 7.1

$$\sum_{\gamma \in \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})} \chi(\gamma) \exp^*_{\omega_E}(\mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}^\gamma_{\mathbf{Q}_n})) = r_E L_{Np}(E,\chi,1)/\Omega_E.$$

When χ is the trivial character this is (i), and as χ varies (ii) follows from Proposition A.2 of the Appendix along with the definition (Theorem 6.1) of $\mathcal{L}_E$ and (3). □

8. Consequences of Kato's Euler system

Following Kato, we will apply the results of §§3 and 4 to bound the Selmer group of E.

8.1. The main theorem.

Theorem 8.1 (Kato [Ka2]). *Suppose E is modular and E does not have complex multiplication.*

(i) *If $L(E,1) \neq 0$ then $E(\mathbf{Q})$ and $Ш(E)$ are finite.*
(ii) *If L is a finite abelian extension of $\mathbf{Q}$, χ is a character of $\mathrm{Gal}(L/\mathbf{Q})$, and $L(E,\chi,1) \neq 0$ then $E(L)^{\chi}$ and $Ш(E_{/L})^{\chi}$ are finite.*

Remarks. We will prove below a more precise version of Theorem 8.1(i).

Kato's construction produces an Euler system for $T_p(E) \otimes \chi$ for every character χ of $G_{\mathbf{Q}}$ of finite order, with properties analogous to those of Theorem 7.1. This more general construction is needed to prove Theorem 8.1(ii). For simplicity we will not treat this more general setting here, so we will only prove Theorem 8.1(i) below. But the method for (ii) is the same.

Theorem 8.1(i) was first proved by Kolyvagin in [Ko], using a system of Heegner points, along with work of Gross and Zagier [GZ], Bump, Friedberg, and Hoffstein [BFH], and Murty and Murty [MM]. The Euler system proof given here, due to Kato, is 'self-contained' in the sense that it replaces all of those other analytic results with the calculation of Theorem 7.1.

Corollary 8.2. *Suppose E is modular and E does not have complex multiplication. Then $E(\mathbf{Q}_\infty)$ is finitely generated.*

Proof. A theorem of Rohrlich [Ro] shows that $L(E,\chi,1) \neq 0$ for almost all characters χ of finite order of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$. Serre's [Se] Théorème 3 shows that $E(\mathbf{Q}_\infty)_{\mathrm{tors}}$ is finite, and the corollary follows without difficulty from Theorem 8.1(ii). $\square$

Remark. When E has complex multiplication, the representation $T_p(E)$ does not satisfy Hypothesis $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$(i) (see Remark 8.5 below), so we cannot apply the results of §§3 and 4 with Kato's Euler system. However, Theorem 8.1 and Corollary 8.2 are known in that case, as Theorem 8.1 for CM curves can be proved using the Euler system of elliptic units. See [CW], [Ru2] §11, and [RW].

8.2. Verification of the hypotheses.

Fix a $\mathbf{Z}_p$-basis of T and let

$$\rho_{E,p} : G_{\mathbf{Q}} \to \mathrm{Aut}(T) \xrightarrow{\sim} \mathrm{GL}_2(\mathbf{Z}_p)$$

be the p-adic representation of $G_{\mathbf{Q}}$ attached to E with this basis.

Proposition 8.3. (i) *If E has no complex multiplication, then $T_p(E)$ satisfies hypotheses $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$ and $H^1(\mathbf{Q}(E_{p^\infty})/\mathbf{Q}, E_{p^\infty})$ is finite.*
(ii) *If the p-adic representation $\rho_{E,p}$ is surjective, then $T_p(E)$ satisfies hypotheses $\mathrm{Hyp}(\mathbf{Q}_\infty, T)$ and $H^1(\mathbf{Q}(E_{p^\infty})/\mathbf{Q}, E_{p^\infty}) = 0$.*

Proof. The Weil pairing shows that

$$\rho_{E,p}(G_{\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})}) = \rho_{E,p}(G_{\mathbf{Q}}) \cap \mathrm{SL}_2(\mathbf{Z}_p).$$

If E has no complex multiplication then a theorem of Serre ([Se] Théorème 3) says that the image of $\rho_{E,p}$ is open in $\mathrm{GL}_2(\mathbf{Z}_p)$. It follows that $V_p(E)$ is an irreducible

$G_{\mathbf{Q}_\infty}$-representation, and if $\rho_{E,p}$ is surjective then E_p is an irreducible $\mathbf{F}_p[G_{\mathbf{Q}_\infty}]$-representation.

It also follows that we can find $\tau \in G_{\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})}$ such that

$$\rho_{E,p}(\tau) = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$$

with $x \neq 0$, and such a τ satisfies Hypothesis $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$(i). If $\rho_{E,p}$ is surjective we can take $x = 1$, and then τ satisfies Hypothesis $\mathrm{Hyp}(\mathbf{Q}_\infty, T)$(i).

We have

$$H^1(\mathbf{Q}(E_{p^\infty})/\mathbf{Q}, E_{p^\infty}) = H^1(\rho_{E,p}(G_\mathbf{Q}), (\mathbf{Q}_p/\mathbf{Z}_p)^2)$$

and the rest of the proposition follows. □

Remark 8.4. Serre's theorem (see [Se] Corollaire 1 of Théorème 3) also shows that if E has no complex multiplication then $\rho_{E,p}$ is surjective for all but finitely many p.

Remark 8.5. The conditions on τ in hypotheses $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$(i) force $\rho_{E,p}(\tau)$ to be nontrivial and unipotent. Thus if E has complex multiplication then there is no τ satisfying $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$(i).

8.3. **Bounding $\mathcal{S}(\mathbf{Q}, E_{p^\infty})$.**

Theorem 8.6. *Suppose E is modular, E does not have complex multiplication, and $L(E,1) \neq 0$.*

(i) *$E(\mathbf{Q})$ and $\text{Ш}(E)_{p^\infty}$ are finite.*

(ii) *Suppose in addition that $p \nmid 2r_E$ and $\rho_{E,p}$ is surjective. If E has good reduction at p and $p \nmid |\tilde{E}(\mathbf{F}_p)|$ (where $\tilde{E}$ is the reduction of E modulo p), then*

$$|\text{Ш}(E)_{p^\infty}| \text{ divides } \frac{L_N(E,1)}{\Omega_E}$$

where N is the conductor of E.

Proof. Recall that $\ell_q(q^{-s})$ is the Euler factor of $L(E,s)$ at q, and that by Proposition 5.1, $\mathcal{S}(\mathbf{Q}, E_{p^\infty})$ is the usual p-power Selmer group of E.

Since $\ell_q(q^{-1})$ is nonzero for every q, Corollary 7.2(i) shows that $\mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}_\mathbf{Q}) \neq 0$. By Proposition 8.3(i) and Proposition 5.2 we can apply Theorem 3.1 to conclude that $\mathcal{S}(\mathbf{Q}, E_{p^\infty})$ is finite, which gives (i).

If E has good reduction at p then $p\ell_p(p^{-1}) = |\tilde{E}(\mathbf{F}_p)|$ and

$$[E(\mathbf{Q}_p) : E_1(\mathbf{Q}_p) + E(\mathbf{Q}_p)_{\mathrm{tors}}] \quad \text{divides} \quad |\tilde{E}(\mathbf{F}_p)|.$$

Therefore if $p \nmid r_E|\tilde{E}(\mathbf{F}_p)|$ then

$$\exp^*_{\omega_E}(H^1_{/\mathcal{S}}(\mathbf{Q}_p, T_p(E))) = p^{-1}\mathbf{Z}_p$$
$$\exp^*_{\omega_E}(\mathbf{Z}_p \mathrm{loc}_p^{\mathrm{ram}}(\mathbf{c}_\mathbf{Q})]) = p^{-1}(L_N(E,1)/\Omega_E)\mathbf{Z}_p$$

by Proposition 5.2 and Corollary 7.2(i). By Proposition 8.3(ii), if $p \neq 2$ we can apply Theorem 3.2, and (ii) follows. □

Remarks. In Corollary 8.9 below, using Iwasawa theory, we will prove that Theorem 8.6(ii) holds for almost all p, even when p divides $|\tilde{E}(\mathbf{F}_p)|$. This is needed to prove Theorem 8.1(i), since $|\tilde{E}(\mathbf{F}_p)|$ could be divisible by p for infinitely many p. However, since $|\tilde{E}(\mathbf{F}_p)| < 2p$ for all primes $p > 5$, we see that if $E(\mathbf{Q})_{\mathrm{tors}} \neq 0$ then $|\tilde{E}(\mathbf{F}_p)|$ is prime to p for almost all p. Thus Theorem 8.1(i) for such a curve follows directly from Theorem 8.6.

The Euler system techniques we are using give an upper bound for the order of the Selmer group, but no lower bound.

8.4. **Bounding $\mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty})$.** Define

$$\mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty}) = \varinjlim \mathcal{S}(\mathbf{Q}_n, E_{p^\infty}) \subset H^1(\mathbf{Q}_\infty, E_{p^\infty}),$$

and recall that $X_\infty = \mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty}), \mathbf{Q}_p/\mathbf{Z}_p)$. Let r_E be the positive integer of Theorem 7.1 and let N be the conductor of E.

Theorem 8.7. *Suppose E is modular, E does not have complex multiplication, and E has good ordinary reduction or nonsplit multiplicative reduction at p. Then X_∞ is a finitely-generated torsion Λ-module and there is an integer t such that*

$$\mathrm{char}(X_\infty) \quad \textit{divides} \quad p^t \mathcal{L}_{E,N}\Lambda.$$

If $\rho_{E,p}$ is surjective and $p \nmid r_E \prod_{q \mid N, q \neq p} \ell_q(q^{-1})$ then $\mathrm{char}(X_\infty)$ divides $\mathcal{L}_E\Lambda$.

If E has split multiplicative reduction at p, the same results hold with $\mathrm{char}(X_\infty)$ replaced by $\mathcal{J}\mathrm{char}(X_\infty)$ where $\mathcal{J}$ is the augmentation ideal of Λ.

Proof. Rohrlich [Ro] proved that $\mathcal{L}_E \neq 0$. Thus the theorem is immediate from Propositions 8.3 and A.2, Corollary 7.2, and Theorem 4.1. □

Corollary 8.8. *Let E be as in Theorem 8.7. There is a nonzero integer M_E such that if p is a prime where E has good ordinary reduction and $p \nmid M_E$, then X_∞ has no nonzero finite submodules.*

Proof. This corollary is due to Greenberg [Gr1], [Gr2]; we sketch a proof here. Let Σ be a finite set of primes containing p, ∞, and all primes where E has bad reduction, and let $\mathbf{Q}_\Sigma$ be the maximal extension of $\mathbf{Q}$ unramified outside of Σ. Then there is an exact sequence

$$0 \to \mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty}) \to H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, E_{p^\infty}) \to \oplus_{q\in\Sigma} \oplus_{v\mid q} H^1_{/\mathcal{S}}(\mathbf{Q}_{\infty,v}, E_{p^\infty}). \tag{4}$$

Suppose $q \in \Sigma$, $q \neq p$, and $v \mid q$. If $p \nmid |E(\mathbf{Q}_q)_{\mathrm{tors}}|$ then it is not hard to show that $E(\mathbf{Q}_{\infty,v})$ has no p-torsion, and so by [Gr1] Proposition 2, $H^1(\mathbf{Q}_{\infty,v}, E_{p^\infty}) = 0$. Thus for sufficiently large p the Pontryagin dual of (4) is

$$\varprojlim_n E(\mathbf{Q}_{n,p}) \otimes \mathbf{Z}_p \to \mathrm{Hom}(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, E_{p^\infty}), \mathbf{Q}_p/\mathbf{Z}_p) \to X_\infty \to 0.$$

Since $\mathbf{Q}_\infty/\mathbf{Q}$ is totally ramified at p,

$$\varprojlim_n E(\mathbf{Q}_{n,p}) \otimes \mathbf{Z}_p = \varprojlim_n E_1(\mathbf{Q}_{n,p}) = \varprojlim_n \hat{E}(\mathfrak{p}_n)$$

and this is free of rank one over Λ (see for example [PR1] Théorème 3.1 or [Schn] Lemma 6, §A.1). It now follows, using the fact that X_∞ is a torsion Λ-module (Theorem 8.7) and [Gr1] Propositions 3, 4, and 5 that $\mathrm{Hom}(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, E_{p^\infty}), \mathbf{Q}_p/\mathbf{Z}_p)$ has no nonzero finite submodules, and by the Lemma on p. 123 of [Gr1] the same is true of X_∞. □

Corollary 8.9. *Suppose E is modular, E does not have complex multiplication, E has good reduction at p, $p \nmid 2r_E M_E \prod_{q\mid N} \ell_q(q^{-1})$ (where r_E is as in Theorem 7.1 and M_E is as in Corollary 8.8), and $\rho_{E,p}$ is surjective. Then*

$$|\text{Ш}(E)_{p^\infty}| \quad \textit{divides} \quad \frac{L(E,1)}{\Omega_E}.$$

Proof. First, if E has supersingular reduction at p then $|\tilde{E}(\mathbf{F}_p)|$ is prime to p, so the corollary follows from Theorem 8.6(ii).

Thus we may assume that E has good ordinary reduction at p. In this case the corollary is a well-known consequence of Theorem 8.7 and Corollary 8.8; see for example [PR1] §6 or [Schn] §2 for details. The idea is that if X_∞ has no nonzero finite submodules and $\mathrm{char}(X_\infty)$ divides $\mathcal{L}_E\Lambda$, then

$$|\mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty})^{\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})}| \quad \text{divides} \quad \chi_0(\mathcal{L}_{E,N}),$$

where χ_0 denotes the trivial character, and with α as in Theorem 6.1

$$\chi_0(\mathcal{L}_{E,N}) = (1-\alpha^{-1})^2 \prod_{q|N} \ell_q(q^{-1})(L(E,1)/\Omega_E).$$

On the other hand, one can show that the restriction map

$$\mathcal{S}(\mathbf{Q}, E_{p^\infty}) \to \mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty})^{\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})}$$

is injective with cokernel of order divisible by $(1-\alpha^{-1})^2$, and the corollary follows. $\square$

Proof of Theorem 8.1(i). Suppose E is modular, E does not have complex multiplication, and $L(E,1) \neq 0$. By Theorem 8.6, $E(\mathbf{Q})$ is finite and $Ш(E)_{p^\infty}$ is finite for every p. By Corollary 8.9 (and using Serre's theorem, see Remark 8.4) $Ш(E)_{p^\infty} = 0$ for almost all p. This proves Theorem 8.1(i). $\square$

We can also now prove part of Theorem 8.1(ii) in the case where E has good ordinary or multiplicative reduction at p and $L \subset \mathbf{Q}_\infty$. For in that case, by Theorem 8.7, $\chi(\mathrm{char}(\mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty}), \mathbf{Q}_p/\mathbf{Z}_p)))$ is a nonzero multiple of $L(E,\chi,1)/\Omega_E$. If $L(E,\chi,1) \neq 0$ it follows that $\mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty})^\chi$ is finite. The kernel of the restriction map $\mathcal{S}(L, E_{p^\infty}) \to \mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty})$ is contained in the finite group $H^1(\mathbf{Q}_\infty/L, E_{p^\infty}^{G_{\mathbf{Q}_\infty}})$, and so we conclude that both $E(L)^\chi$ and $Ш(E_{/L})^\chi_{p^\infty}$ are finite.

Appendix. Explicit description of the Coleman map

In this appendix we give an explicit description of the Coleman map from $H^1_{\infty,/\mathcal{S}}(\mathbf{Q}_{n,p}, T)$ to Λ. This map allows us to relate Kato's Euler system with the p-adic L-function $\mathcal{L}_E$.

Suppose for this appendix that E has good ordinary reduction or multiplicative reduction at p. As in Theorem 6.1, let $\alpha \in \mathbf{Z}_p^\times$ and $\beta \in p\mathbf{Z}_p$ be the eigenvalues of Frobenius if E has good ordinary reduction, let $\alpha = 1, \beta = p$ if E has split multiplicative reduction and let $\alpha = -1, \beta = -p$ if E has nonsplit multiplicative reduction.

Recall we fixed before Theorem 6.1 a generator $[\zeta_{p^n}]_n$ of $\varprojlim \boldsymbol{\mu}_{p^n}$. For every $n \geq 0$ define

$$x_n = \alpha^{-n-1}\mathrm{Tr}_{\mathbf{Q}_p(\boldsymbol{\mu}_{p^{n+1}})/\mathbf{Q}_{n,p}} \left(\sum_{k=0}^{n} \frac{\zeta_{p^{n+1-k}} - 1}{\beta^k} + \frac{\beta}{\beta - 1} \right) \in \mathbf{Q}_{n,p}.$$

Lemma A.1. (i) *If $n \geq m$ then* $\mathrm{Tr}_{\mathbf{Q}_{n,p}/\mathbf{Q}_{m,p}} x_n = x_m$.

(ii) *If χ is a character of G_n then*

$$\chi(\sum_{\gamma\in G_n} x_n^\gamma \gamma) = \begin{cases} \alpha^{-m}\tau(\chi) & \text{if } \chi \text{ has conductor } p^m > 1 \\ (1-\alpha^{-1})(1-\beta^{-1})^{-1} & \text{if } \chi = 1. \end{cases}$$

Proof. Exercise. □

Proposition A.2. (i) *For every $n \geq 0$ there is a $\mathbf{Z}_p[G_n]$-module map*

$$\mathrm{Col}_n : H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, T) \to \mathbf{Z}_p[G_n]$$

such that for every $z \in H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p}, T)$ and every nontrivial character χ of G_n of conductor p^m,

$$\chi(\mathrm{Col}_n(z)) = \alpha^{-m}\tau(\chi) \sum_{\gamma \in G_n} \chi^{-1}(\gamma) \exp^*_{\omega_E}(z^\gamma).$$

If χ_0 is the trivial character then

$$\chi_0(\mathrm{Col}_n(z)) = (1-\alpha^{-1})(1-\beta^{-1})^{-1} \sum_{\gamma \in G_n} \exp^*_{\omega_E}(z^\gamma).$$

(ii) *The maps Col_n are compatible as n varies, and in the limit they induce a map of Λ-modules*

$$\mathrm{Col}_\infty : H^1_{\infty,/\mathcal{S}}(\mathbf{Q}_p, T) \to \Lambda.$$

(iii) *The map Col_∞ is injective. If E has split multiplicative reduction at p then the image of Col_∞ is contained in the augmentation ideal of Λ.*

Proof. The proof is based on work of Coleman [Co].

For the curves E which we are considering, $\hat{E}$ is a height-one Lubin-Tate formal group over $\mathbf{Z}_p$ for the uniformizing parameter β. It follows that, writing R for the ring of integers of the completion of the maximal unramified extension of $\mathbf{Q}_p$, $\hat{E}$ is isomorphic over R to the multiplicative group $\mathbf{G}_m$. Fix an isomorphism $\eta : \mathbf{G}_m \xrightarrow{\sim} \hat{E}$, $\eta \in R[[X]]$. We define the p-adic period Ω_p of E

$$\Omega_p = \eta'(0) \in R^\times.$$

This period is unique up to $\mathbf{Z}_p^\times$, and is also characterized by the identity

$$\lambda_E(\eta(X)) = \Omega_p \log(1+X). \tag{5}$$

By [dS] §I.3.2 (4), if ϕ is the Frobenius automorphism of $R/\mathbf{Z}_p$ then

$$\Omega_p^\phi = \alpha^{-1}\Omega_p.$$

By [Co] Theorem 24 (applied to the multiplicative group) there is a power series g in the maximal ideal $(p, X)R[[X]]$ of $R[[X]]$ such that

$$\log(1+g(X)) = \Omega_p^{-1}\left((p-1)\frac{\beta}{\beta-1} + \sum_{k=0}^{\infty} \sum_{\delta \in \boldsymbol{\mu}_{p-1} \subset \mathbf{Z}_p^\times} \frac{(1+X)^{\delta p^k} - 1}{\beta^k}\right).$$

In particular if we set $X = \zeta_{p^{n+1}} - 1$ and use (5),

$$\lambda_E(\eta(g(\zeta_{p^{n+1}} - 1))) = \Omega_p \log(1 + g(\zeta_{p^{n+1}} - 1)) = \alpha^{n+1}x_n.$$

Observe that $\hat{E}(\mathfrak{p}_n R)_{\mathrm{tors}} = 0$ because $\mathbf{Q}_p(\hat{E}_p)/\mathbf{Q}_p$ is totally ramified of degree $p-1$. Therefore λ_E is injective on $\hat{E}(\mathfrak{p}_n R)$ and so

$$x_n \in \lambda_E(\mathfrak{p}_n R)^{\mathrm{Gal}(\mathbf{Q}_{n,p}R/\mathbf{Q}_{n,p})} = \lambda_E(\mathfrak{p}_n) \subset \lambda_E(E(\mathbf{Q}_{n,p})).$$

Define Col_n on $H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p},T)$ by

$$\begin{aligned}\mathrm{Col}_n(z) &= \left(\sum_{\gamma\in G_n} x_n^\gamma\gamma\right)\left(\sum_{\gamma\in G_n}\exp^*_{\omega_E}(z^\gamma)\gamma^{-1}\right)\\ &= \sum_{\gamma\in G_n}(\mathrm{Tr}_{\mathbf{Q}_{n,p}/\mathbf{Q}_p} x_n^\gamma \exp^*_{\omega_E}(z))\gamma\end{aligned}$$

Clearly this gives a Galois-equivariant map $H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p},T)\to\mathbf{Q}_p[G_n]$. Since $x_n^\gamma\in\lambda_E(E(\mathbf{Q}_{n,p}))$, (1) and (2) show that $\mathrm{Col}_n(z)\in\mathbf{Z}_p[G_n]$. The equalities of (i) follow from Lemma A.1(ii), and (ii) follows easily.

For (iii), suppose first that E has good ordinary reduction or nonsplit multiplicative reduction at p, so that $\alpha\neq 1$. Then the injectivity of Col_n (and of Col_∞) follows from (i), the nonvanishing of the Gauss sums, and the injectivity of $\exp^*_{\omega_E}$.

If E has split multiplicative reduction at p, then $\alpha=1$. In this case it follows from (i) that $\ker(\mathrm{Col}_n)=H^1_{/\mathcal{S}}(\mathbf{Q}_{n,p},T)^{G_n}$, which is free of rank one over $\mathbf{Z}_p$, for every n. But one can show using (1) that $H^1_{\infty,/\mathcal{S}}(\mathbf{Q}_p,T)$ has no Λ-torsion, so Col_∞ must be injective in this case as well. The assertion about the cokernel is clear from (i), since $\alpha=1$. □

References

[BFH] Bump, D., Friedberg, S., Hoffstein, J.: Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives, *Annals of Math.* **131** (1990) 53–127.

[CW] Coates, J., Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer, *Inventiones math.* **39** (1977) 223–251.

[Co] Coleman, R.: Division values in local fields. *Invent math.* **53** (1979) 91-116

[dS] de Shalit, E.: The Iwasawa theory of elliptic curves with complex multiplication, (*Perspec. in Math.* **3**) Orlando: Academic Press (1987)

[Gr1] Greenberg, R.: Iwasawa theory for p-adic representations, *Adv. Stud. in Pure Math.* **17** (1989) 97–137.

[Gr2] Greenberg, R.: Iwasawa theory for p-adic representations II, to appear.

[GZ] Gross, B., Zagier, D.: Heegner points and derivatives of L-series, *Inventiones math.* **84** (1986) 225–320

[Ka1] Kato, K.: Euler systems, Iwasawa theory, and Selmer groups, to appear

[Ka2] ———: to appear

[Ko] Kolyvagin, V. A.: Euler systems. In: The Grothendieck Festschrift (Vol. II), P. Cartier, et al., eds., *Prog. in Math* **87**, Boston: Birkhäuser (1990) 435–483.

[MSD] Mazur, B., Swinnerton-Dyer, H.P.F.: Arithmetic of Weil curves, *Inventiones math.* **25** (1974) 1–61

[MTT] Mazur, B., Tate, J., Teitelbaum, J.: On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. math.* **84** (1986) 1–48.

[MM] Murty, K., Murty, R.: Mean values of derivatives of modular L-series, *Annals of Math.* **133** (1991) 447–475.

[PR1] Perrin-Riou, B.: Théorie d'Iwasawa p-adique locale et globale, *Invent. math.* **99** (1990) 247–292.

[PR2] ———: Systèmes d'Euler p-adiques et théorie d'Iwasawa, to appear.

[Ro] Rohrlich, D.: On L-functions of elliptic curves and cyclotomic towers, *Invent. math.* **75** (1984) 409–423.

[Ru1] Rubin, K.: The main conjecture. Appendix to: Cyclotomic fields I and II, S. Lang, *Graduate Texts in Math.* **121**, New York: Springer-Verlag (1990) 397–419.

[Ru2] ———: The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. math.* **103** (1991) 25–68.

[Ru3] ———: Euler systems, to appear.

[RW] Rubin, K., Wiles, A.: Mordell-Weil groups of elliptic curves over cyclotomic fields. In: Number Theory related to Fermat's last theorem, *Progress in Math.* **26**, Boston: Birkhauser (1982) 237–254.

[Schn] Schneider, P.: p-adic height pairings, II, *Inventiones math.* **79** (1985) 329–374.

[Scho] Scholl, A.: this volume

[Se] Serre, J-P.: Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. math.* **15** (1972) 259–331.

[T] Tate, J.: Algorithm for determining the type of a singular fiber in an elliptic pencil. In: Modular functions of one variable (IV), *Lecture Notes in Math.* **476**, New York: Springer-Verlag (1975) 33–52.

Department of Mathematics, Ohio State University, Columbus, OH 43210 USA
E-mail address: rubin@math.ohio-state.edu