Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 110 (2005) 164–177

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

An algebraic version of a theorem of Kurihara

Robert Pollack[1]

Department of Mathematics, Boston University, 111 Cummington Street, Boston, MA 02215, USA

Received 1 March 2003; revised 17 October 2003

Communicated by D. Goss

Available online 29 September 2004

In memory of Professor Arnold Ross

Abstract

Let $E/\mathbf{Q}$ be an elliptic curve and let p be an odd supersingular prime for E. In this article, we study the simplest case of Iwasawa theory for elliptic curves, namely when $E(\mathbf{Q})$ is finite, $\text{Ш}(E/\mathbf{Q})$ has no p-torsion and the Tamagawa factors for E are all prime to p. Under these hypotheses, we prove that $E(\mathbf{Q}_n)$ is finite and make precise statements about the size and structure of the p-power part of $\text{Ш}(E/\mathbf{Q}_n)$. Here $\mathbf{Q}_n$ is the n-th step in the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$.

Keywords: Elliptic curves; Iwasawa theory; Supersingular primes

1. Introduction

Let $E/\mathbf{Q}$ be an elliptic curve with good supersingular reduction at an odd prime p. Let $\mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$ with subfields $\mathbf{Q}_n$ of degree p^n. In [8], Kurihara proved precise statements about the size and the structure of the p-part of the Tate–Shafarevich group $\text{Ш}(E/\mathbf{Q}_n)$ when $\text{ord}_p(L(E,1)/\Omega_E) = 0$ and when the Galois representation on the p-torsion is surjective. His proof made deep use of Kato's Euler system for the Tate module of E (and hence the need for an assumption on the Galois representation).

E-mail address: rpollack@math.bu.edu.

[1] The author was supported by an NSF Postdoctoral Fellowship.

0022-314X/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2003.10.008

In this paper, we offer a completely algebraic proof of a variant of a theorem of Kurihara (see [8, Theorem 0.1]) where his analytic assumptions are converted to algebraic ones (equivalent under the Birch and Swinnerton-Dyer conjecture). Before stating the result, we fix some notation. Set $\Gamma = \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$, $\Gamma_n = \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q}_n)$ and $G_n = \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})$. Let $\Lambda_n = \mathbf{Z}_p[G_n]$ be the group algebra at level n and $\Lambda = \mathbf{Z}_p[[\Gamma]]$ be the Iwasawa algebra. For a $\mathbf{Z}_p$-module M, denote by $M^\wedge$ its Pontrjagin dual.

Theorem 1.1. *Let $E/\mathbf{Q}$ be an elliptic curve with p an odd prime of good supersingular reduction. Assume that*

(1) *$E(\mathbf{Q})$ is finite.*
(2) $p \nmid \mathrm{Tam}(E/\mathbf{Q})$.
(3) $\text{Ш}(E/\mathbf{Q})[p] = 0$.

Then

(1) *$E(\mathbf{Q}_n)$ is finite for all $n \geqslant 0$.*
(2) $\mathrm{ord}_p(\#\text{Ш}(E/\mathbf{Q}_n)) = e_n$ *where* $e_0 = e_1 = 0$ *and*

$$e_n = \begin{cases} p^{n-1} + p^{n-3} + \cdots + p - \frac{n}{2} & \text{for even } n \geqslant 2, \\ p^{n-1} + p^{n-3} + \cdots + p^2 - \frac{n-1}{2} & \text{for odd } n \geqslant 3. \end{cases}$$

(3) *When $a_p = 0$, we have*

$$\text{Ш}(E/\mathbf{Q}_n)[p^\infty]^\wedge \cong \Lambda_n/(J_n^+ + J_n^-)$$

as $\mathbf{Z}_p[G_n]$-modules where

$$J_n^\pm := \{f \in \Lambda_n : \chi(f) = 0 \text{ for } \chi \text{ a char. of } G_n \text{ of even (resp. odd) order}\}.$$

Remark 1.2. The above theorem is false for $p = 2$. If $E = X_0(19)$ then $E(\mathbf{Q})$ is finite, $\mathrm{Tam}(E/\mathbf{Q})$ is odd and $\text{Ш}(E/\mathbf{Q})[2] = 0$. However, $E(\mathbf{Q}(\sqrt{2}))$ is infinite and $\mathbf{Q}(\sqrt{2})$ is the first step in the cyclotomic $\mathbf{Z}_2$-extension.

Remark 1.3. The conclusion of Theorem 1.1 is identical to Kurihara's theorem; it is only the hypotheses that have changed. For supersingular p, the Birch and Swinnerton-Dyer conjecture predicts that $\mathrm{ord}_p(L(E,1)/\Omega_E) = 0$ if and only if $E(\mathbf{Q})$ is finite, $p \nmid \mathrm{Tam}(E/\mathbf{Q})$ and $\text{Ш}(E/\mathbf{Q})[p] = 0$. The "if part" is still unknown, but the "only if" part is known via Kato's Euler system when the Galois representation on the p-torsion is surjective. Hence the above hypotheses are logically weaker than Kurihara's since we make no assumptions on the Galois representation. In particular, our results apply to CM curves.

The analogue of Theorem 1.1 in the ordinary case follows from Mazur's control theorem. However, in the supersingular case the control theorem fails (due to the triviality of the universal norms of the formal group $\hat{E}/\mathbf{Q}_p$ along the local cyclotomic

$\mathbf{Z}_p$-extension). We will make a careful study of the how the control theorem fails in terms of $\hat{E}$ and combining this with a precise enough description of this formal group, we will be able to prove Theorem 1.1.

These techniques are not new as they form the basis of Perrin–Riou's construction of an algebraic p-adic L-function in [12]. Also, many of the calculations in this paper were inspired by the beautiful ideas of Kurihara in [8]. It should also be mentioned that similar results were announced by Nasybullin [11] over 25 years ago, but in his short paper no proofs were given.

One advantage to the algebraic approach of this paper is that it can be generalized more easily to $\mathbf{Z}_p$-extensions of a number field that are not necessarily cyclotomic. To successfully carry out such a generalization, the key local input that is needed is a good understanding of the Galois module structure of $\hat{E}$ along the $\mathbf{Z}_p$-extensions of some finite extension of $\mathbf{Q}_p$. In a forthcoming paper with Adrian Iovita (see [6]) a strong enough local result is obtained to generalize the results of this paper to any $\mathbf{Z}_p$-extension of a number field in which p splits completely.

The format of the paper will be as follows: in the following section we will implement the needed Iwasawa theory to precisely describe the failure of the control theorem in terms of $\hat{E}$. The third section will state results of Kobayashi on the structure of $\hat{E}$ as a Galois module. In the fourth section, we will define μ and λ-invariants of elements of Λ_n and discuss their basic properties. In the final section, we will perform the needed computations to complete the proof of Theorem 1.1.

2. Iwasawa theory

Let $E/\mathbf{Q}$ be an elliptic curve, p some prime of good reduction and K some finite extension of $\mathbf{Q}$. We define the p-Selmer group of E over K by

$$\mathrm{Sel}_p(E/K) = \ker\left(H^1(K, E[p^\infty]) \longrightarrow \prod_v H^1(K_v, E)\right),$$

where v runs over the places of K. Also, define a looser Selmer group by dropping the condition at p, i.e.

$$\mathrm{Sel}'_p(E/K) = \ker\left(H^1(K, E[p^\infty]) \longrightarrow \prod_{v \nmid p} H^1(K_v, E)\right).$$

We then have the following exact sequence relating these two Selmer groups:

$$0 \longrightarrow \mathrm{Sel}_p(E/K) \longrightarrow \mathrm{Sel}'_p(E/K) \longrightarrow \prod_{v \mid p} H^1(K_v, E)[p^\infty]. \tag{1}$$

For the infinite extension $\mathbf{Q}_\infty$ we define $\mathrm{Sel}_p(E/\mathbf{Q}_\infty) = \varinjlim \mathrm{Sel}_p(E/\mathbf{Q}_n)$ and $\mathrm{Sel}'_p(E/\mathbf{Q}_\infty) = \varinjlim \mathrm{Sel}'_p(E/\mathbf{Q}_n)$. As mentioned in the introduction, the control theorem for $\mathrm{Sel}_p(E/\mathbf{Q}_\infty)$ fails for supersingular p. However, the control theorem for $\mathrm{Sel}'_p(E/\mathbf{Q}_\infty)$ is always true.

Theorem 2.1. *Let p be a prime of good reduction for $E/\mathbf{Q}$. Then the natural map*

$$\mathrm{Sel}'_p(E/\mathbf{Q}_n) \longrightarrow \mathrm{Sel}'_p(E/\mathbf{Q}_\infty)^{\Gamma_n}$$

has finite kernel and cokernel that are bounded independent of n.

Moreover, if $E(\mathbf{Q})[p] = 0$, $p \nmid \mathrm{Tam}(E/\mathbf{Q})$ and $a_p \not\equiv 1 \pmod p$ then the above map is an isomorphism.

Proof. This theorem was originally proven by Mazur in [10]. See also [9] and [3, Chapter 3] for an exposition of this theorem that uses Galois cohomology instead of flat cohomology. Note that in all of these papers the ordinary hypothesis is only used in studying the primes over p. Since we are dealing with Sel′, and not Sel these proofs apply to our situation. □

We now work under the hypotheses of Theorem 1.1, namely that p is supersingular for E, $E(\mathbf{Q})$ is finite, $p \nmid \mathrm{Tam}(E/\mathbf{Q})$ and $Ш(E/\mathbf{Q})[p] = 0$. Since p is supersingular, $a_p \not\equiv 1 \pmod p$ and $E(\mathbf{Q})[p] = 0$. Hence, the map in Theorem 2.1 is an isomorphism and (1) becomes

$$0 \longrightarrow \mathrm{Sel}_p(E/\mathbf{Q}_n) \longrightarrow \mathrm{Sel}'_p(E/\mathbf{Q}_\infty)^{\Gamma_n} \longrightarrow H^1(\mathbf{Q}_{n,p}, E)[p^\infty], \tag{2}$$

where $\mathbf{Q}_{n,p}$ denotes the completion of $\mathbf{Q}_n$ at the unique prime over p.

The main reason for the failure of the control theorem in the supersingular case is that the local condition defining the Selmer group at p disappears over $\mathbf{Q}_\infty$.

Proposition 2.2. *For p supersingular*

$$H^1(\mathbf{Q}_{\infty,p}, E)[p^\infty] = 0$$

and hence

$$\mathrm{Sel}_p(E/\mathbf{Q}_\infty) = \mathrm{Sel}'_p(E/\mathbf{Q}_\infty).$$

Proof. By Tate local duality, the vanishing of $H^1(\mathbf{Q}_{\infty,p}, E)[p^\infty]$ is equivalent to the triviality of the universal norms of $\hat{E}$ along $\mathbf{Q}_{\infty,p}/\mathbf{Q}_p$. This vanishing of universal norms was originally proven by Hazewinkel in [4]. See [1] for a general discussion of this phenomenon for deeply ramified extensions. □

Hence $X_\infty := \mathrm{Sel}_p(E/\mathbf{Q}_\infty)^\wedge \cong \mathrm{Sel}'_p(E/\mathbf{Q}_\infty)^\wedge$. Dualizing (2) and applying Tate local duality yields

$$\hat{E}(\mathbf{Q}_{n,p}) \longrightarrow (X_\infty)_{\Gamma_n} \longrightarrow \mathrm{Sel}_p(E/\mathbf{Q}_n)^\wedge \longrightarrow 0, \tag{3}$$

where M_{Γ_n} denotes the Γ_n-coinvariants of M. The above sequence can be thought of as describing the failure of the control theorem in terms of the formal group.

We make one last alteration of the above sequence by explicitly describing X_∞. The following is well known, but we include a proof for completeness.

Proposition 2.3. *Under our hypotheses, X_∞ is a free Λ-module of rank* 1.

Proof. When p is supersingular, it is always true that the Λ-rank of X_∞ is greater than or equal to 1 by a result of Schneider (see [13, Corollary 5]). For a discussion of this theorem using Galois cohomology rather than flat cohomology see [2, Proposition 2.6].

Under our hypotheses, we prove an upper bound on the Λ-rank of X_∞ and establish that it is a free Λ-module. Note that since $E(\mathbf{Q})$ is finite and $\text{Ш}(E/\mathbf{Q})[p] = 0$ we have that $\mathrm{Sel}_p(E/\mathbf{Q}) = 0$. Hence, taking $n = 0$ in (3) yields

$$\hat{E}(\mathbf{Q}_p) \twoheadrightarrow (X_\infty)_\Gamma .$$

Furthermore, $\hat{E}(\mathbf{Q}_p) \cong \mathbf{Z}_p$ and since $(X_\infty)_\Gamma$ is infinite the above map is an isomorphism. A compact version of Nakayama's lemma then implies that X_∞ is a free Λ-module of rank 1. □

Therefore, we can choose an isomorphism $i : X_\infty \cong \Lambda$ which induces isomorphisms $(X_\infty)_{\Gamma_n} \cong \Lambda_n$ for each n. Then (3) becomes

$$\hat{E}(\mathbf{Q}_{n,p}) \xrightarrow{F_n} \Lambda_n \longrightarrow \mathrm{Sel}_p(E/\mathbf{Q}_n)^\wedge \longrightarrow 0. \tag{4}$$

One can verify the commutativity of

$$\begin{tikzcd} \hat{E}(\mathbf{Q}_{n,p}) \arrow[r, "F_n"] \arrow[d, "\mathrm{Tr}_{n/n-1}"'] & \Lambda_n \arrow[d, "\pi_{n/n-1}"] \\ \hat{E}(\mathbf{Q}_{n-1,p}) \arrow[r, "F_{n-1}"] & \Lambda_{n-1} \end{tikzcd} \tag{5}$$

and

$$\begin{tikzcd}
\hat{E}(\mathbf{Q}_{n,p}) \arrow[r, "F_n"] & \Lambda_n \\
\hat{E}(\mathbf{Q}_{n-1,p}) \arrow[r, "F_{n-1}"] \arrow[u, "i_{n-1/n}"] & \Lambda_{n-1} \arrow[u, "\nu_{n-1/n}"']
\end{tikzcd} \tag{6}$$

where $\mathrm{Tr}_{n/n-1}$ is the trace map, $\pi_{n/n-1}$ is the natural projection, $i_{n-1/n}$ is the natural inclusion and $\nu_{n-1/n}$ is defined by

$$\nu_{n-1/n}(\sigma) = \sum_{\substack{\tau \to \sigma \\ \tau \in G_n}} \tau$$

for $\sigma \in G_{n-1}$. (See [6, Proposition 6.3] for a detailed explanation of why these diagrams commute.)

3. Formal groups

We now state a result of Kobayashi that describes generators of $\hat{E}(\mathbf{Q}_{n,p})$ as a Galois module.

Theorem 3.1. *Let p be an odd prime. For each $n \geqslant 0$ there exists $c_n \in \hat{E}(\mathbf{Q}_{n,p})$ such that*

(1) $\mathrm{Tr}_{n/n-1} c_n = a_p c_{n-1} - i_{n-2/n-1}(c_{n-2})$ *for* $n \geqslant 2$.
(2) $\mathrm{Tr}_{1/0} c_1 = \left(a_p - \frac{p-1}{a_p - 2}\right) c_0$.

Furthermore, as a Galois module, $\hat{E}(\mathbf{Q}_{n,p})$ is generated by c_n and $i_{n-1/n}(c_{n-1})$ for $n \geqslant 1$ and $\hat{E}(\mathbf{Q}_p)$ is generated by c_0.

Proof. The points c_n were originally constructed by Perrin-Riou in [12]. In [7], Kobayashi gives an alternate construction of these points using Honda theory and proves that they generate the formal group as a Galois module (see [7, Proposition 8.12]).

We point out that Kobayashi assumes that $a_p = 0$, but with minor modifications his arguments would work for any a_p divisible by p. Namely, in the notation of [7], one has a formal group $\mathcal{F} := \mathcal{F}_{ss}$ whose logarithm is of Honda type $t^2 + p$. We must replace $\mathcal{F}$ with a formal group whose logarithm is of Honda type $t^2 - a_p t + p$.

Consider the sequence $\{x_k\}$ defined by $x_{-1} = 0$, $x_0 = 1$ and

$$p x_k - a_p x_{k-1} + x_{k-2} = 0$$

for $k \geqslant 1$. Then there exists a formal group $\mathcal{F}(a_p)$ such that

$$\log_{\mathcal{F}(a_p)}(X) = \sum_{k=0}^{\infty} x_k((X+1)^{p^k} - 1)$$

and its logarithm is of Honda type $t^2 - a_p t + p$ (see [5, p. 221]).

A second change that needs to be made is that Kobayashi chooses an element $\varepsilon \in p\mathbf{Z}_p$ such that $\log_{\mathcal{F}}(\varepsilon) = p/(p+1)$. To make the computations of [7, Lemma 8.9] work out for general a_p, we must choose $\varepsilon \in p\mathbf{Z}_p$ such that $\log_{\mathcal{F}(a_p)}(\varepsilon) = p/(p+1-a_p)$. With these two modifications, Kobayashi's arguments apply to this more general setting. □

4. μ and λ-invariants

The proof of Theorem 1.1 will boil down to understanding the size of certain explicit quotients of Λ_n. In this section, we introduce the notion of μ and λ-invariants of elements of Λ_n to help in determining the size of such quotients.

Definition 4.1. For non-zero $f \in \Lambda_n$ the μ-invariant of f is the unique integer $\mu(f)$ such that $f \in p^{\mu(f)}\Lambda_n - p^{\mu(f)+1}\Lambda_n$.

Let I_n be the augmentation ideal of Λ_n and let $\widetilde{I}_n$ be the augmentation ideal of $\widetilde{\Lambda}_n := \mathbf{F}_p[G_n]$.

Definition 4.2. For non-zero $f \in \Lambda_n$ the λ-invariant of f is the unique integer $\lambda(f)$ such that the reduction mod p of $p^{-\mu(f)}f$ lands in $\widetilde{I}_n^{\lambda(f)} - \widetilde{I}_n^{\lambda(f)+1}$.

Remark 4.3. These μ and λ-invariants of elements of Λ_n are related to the standard Iwasawa invariants of elements of Λ. Namely, if $f \in \Lambda$ and f_n is its image in Λ_n then

$$\mu(f) = \mu(f_n) \quad \text{and} \quad \lambda(f) = \lambda(f_n)$$

if $\lambda(f) < p^n$.

Since the ring Λ_n is not a domain, these invariants do not share all of the basic properties of standard μ and λ-invariants. For instance, since $p\Lambda_n$ is not a prime ideal, there exist $f, g \in \Lambda_n$ such that $\mu(f) = \mu(g) = 0$ but $\mu(f \cdot g) > 0$. The following simple lemma states some weaker properties that are true of these invariants.

Lemma 4.4. *For $f, g \in \Lambda_n$ we have*

(1) $\mu(f \cdot g) \geqslant \mu(f) + \mu(g)$.
(2) *If $\mu(f \cdot g) = 0$ then $\lambda(f \cdot g) = \lambda(f) + \lambda(g)$.*

These invariants can be used to describe the valuations of elements of Λ_n evaluated at finite order characters as demonstrated in the following lemma.

Lemma 4.5. *Let $f \in \Lambda_n$ and let χ be a character of G_n of order p^n. If $\lambda(f) < p^{n-1}(p-1)$ then*

$$\operatorname{ord}_p(\chi(f)) = \mu(f) + \frac{\lambda(f)}{p^{n-1}(p-1)}.$$

Proof. Let γ be a generator of G_n. Then $\gamma - 1$ is a generator of the augmentation ideal I_n. From the definitions of μ and λ-invariants, we have that

$$f = p^{\mu(f)} \left((\gamma - 1)^{\lambda(f)} \cdot u + p \cdot g \right)$$

for $u \in \Lambda_n^\times$ and $g \in \Lambda_n$. Hence

$$\begin{aligned} \operatorname{ord}_p(\chi(f)) &= \mu(f) + \min\left\{\lambda(f) \cdot \operatorname{ord}_p(\chi(\gamma) - 1), 1 + \operatorname{ord}_p(\chi(g))\right\} \\ &= \mu(f) + \frac{\lambda(f)}{p^{n-1}(p-1)} \end{aligned}$$

since $\lambda(f) < p^{n-1}(p-1)$. □

We will need to understand how these invariants are affected by the maps $\nu_{n-1/n}$ and $\pi_{n/n-1}$. We first give a lemma that describes the relations between these two maps.

Lemma 4.6. *For $f \in \Lambda_{n-1}$ and $g \in \Lambda_n$ we have*

(1) $\pi_{n/n-1}(\nu_{n-1/n}(f)) = p \cdot f$
(2) $\nu_{n-1/n}(\pi_{n/n-1}(g)) = \xi_n \cdot g$
(3) $\operatorname{im}(\nu_{n-1/n}) = \xi_n \Lambda_n$,

where $\xi_n = \sum_{\sigma^p = 1} \sigma \in \mathbf{Z}_p[G_n]$.

Proof. This lemma follows directly from the definitions. □

We now compute the μ and λ-invariant of the element ξ_n defined in the previous lemma.

Lemma 4.7. *We have that $\mu(\xi_n) = 0$ and $\lambda(\xi_n) = p^n - p^{n-1}$.*

Proof. Let γ be a generator of G_n. Then both I_n and $\widetilde{I_n}$ are principal generated by $\gamma - 1$. So

$$\xi_n = \sum_{\sigma^p=1} \sigma = \sum_{a=0}^{p-1} \gamma^{ap^{n-1}} = \frac{\gamma^{p^n} - 1}{\gamma^{p^{n-1}} - 1} \equiv (\gamma - 1)^{p^n - p^{n-1}} \pmod p$$

and hence $\mu(\xi_n) = 0$ and $\lambda(\xi_n) = p^n - p^{n-1}$. □

Remark 4.8. If we fix a generator of G_n and thus an isomorphism

$$\Lambda_n \cong \mathbf{Z}_p[[T]]/((1+T)^{p^n} - 1),$$

the element $\xi_n \in \Lambda_n$ is identified with $\Phi_n(1+T)$ where Φ_n is the $p^{n\text{-th}}$ cyclotomic polynomial. Note that the computations of the previous lemma agree with the computations of the standard μ and λ-invariants of $\Phi_n(1+T)$ as predicted by Remark 4.3.

The following proposition summarizes how the Iwasawa invariants interact with the maps $v_{n-1/n}$ and $\pi_{n/n-1}$.

Proposition 4.9. *For $f \in \Lambda_{n-1}$ and $g, h \in \Lambda_n$ we have*

(1) $\mu(\pi_{n/n-1}(g)) \geqslant \mu(g)$ *and thus if* $\mu(\pi_{n/n-1}(g)) = 0$ *then* $\mu(g) = 0$.
(2) *If* $\mu(\pi_{n/n-1}(g)) = \mu(g)$ *then* $\lambda(\pi_{n/n-1}(g)) = \lambda(g)$.
(3) $\mu(v_{n-1/n}(f)) = \mu(f)$.
(4) $\lambda(v_{n-1/n}(f)) = p^n - p^{n-1} + \lambda(f)$.

Proof. Part 1 follows directly from the definitions. For part 2, we have that $\widetilde{g} \in \widetilde{I}_n^a$ if and only if $\pi_{n/n-1}(\widetilde{g}) \in \widetilde{I}_{n-1}^a$ since these augmentation ideals are principal. (Here $\widetilde{g}$ represents the reduction of $g \bmod p$.) Thus, $\lambda(\pi_{n/n-1}(g)) = \lambda(g)$ since the μ-invariant of both of these elements are the same.

For part 3, write $f = p^{\mu(f)} f'$ with $\mu(f') = 0$. Then $v_{n-1/n}(f) = p^{\mu(f)} v_{n-1/n}(f')$ and if we knew that $\mu(v_{n-1/n}(f')) = 0$ then we would have $\mu(v_{n-1/n}(f)) = \mu(f)$. Hence, we have reduced to the case where $\mu(f) = 0$. Now pick any $g \in \Lambda_n$ such that $\pi_{n/n-1}(g) = f$. (Note then by part 1, $\mu(g) = 0$.) So

$$v_{n-1/n}(f) = v_{n-1/n}(\pi_{n/n-1}(g)) = \xi_n \cdot g$$

by Lemma 4.6.2 and thus

$$\mu(v_{n-1/n}(f)) = \mu(\xi_n \cdot g) = \mu(g) = 0 = \mu(f).$$

For the last part, as in part 3, we may assume that $\mu(f) = 0$. Then pick $g \in \Lambda_n$ lifting f and thus

$$\begin{aligned}
\lambda(\nu_{n-1/n}(f)) &= \lambda(\xi_n \cdot g) \\
&= \lambda(\xi_n) + \lambda(g) && \text{(by part 3 and Lemma 4.4)} \\
&= p^n - p^{n-1} + \lambda(\pi_{n/n-1}(f)) && \text{(by Lemma 4.7)} \\
&= p^n - p^{n-1} + \lambda(f) && \text{(by part 2).} \quad \square
\end{aligned}$$

We introduce one more lemma which will be useful in the following section.

Lemma 4.10. *Let f, g be elements of Λ_n such that $f \cdot g \in \operatorname{im}(\nu_{n-1/n})$. If $\mu(f) = 0$ and $\lambda(f) < p^{n-1}$ then $g \in \operatorname{im}(\nu_{n-1/n})$.*

Proof. By Lemma 4.6.3, $\operatorname{im}(\nu_{n-1/n}) = \xi_n \Lambda_n$. Thus, $\operatorname{im}(\nu_{n-1/n})$ is a prime ideal in Λ_n since $\Lambda_n/\xi_n\Lambda_n \cong \mathbf{Z}_p[\mu_{p^n}]$ which is a domain. Hence $f \cdot g \in \operatorname{im}(\nu_{n-1/n})$ implies that either $f \in \operatorname{im}(\nu_{n-1/n})$ or $g \in \operatorname{im}(\nu_{n-1/n})$.

If $f \in \operatorname{im}(\nu_{n-1/n})$ then $f = \xi_n h$ for some $h \in \Lambda_n$. Since $\mu(f) = 0$,

$$\lambda(f) \geqslant \lambda(\xi_n) = p^n - p^{n-1} \geqslant p^{n-1}$$

by Lemma 4.4. This contradicts our hypothesis and thus $g \in \operatorname{im}(\nu_{n-1/n})$. $\square$

5. Main argument

Recall the map $F_n : \hat{E}(\mathbf{Q}_{n,p}) \longrightarrow \Lambda_n$ defined in (4). For $c_n \in \hat{E}(\mathbf{Q}_{n,p})$ defined in Theorem 3.1, set

$$P_n = F_n(c_n) \in \Lambda_n.$$

The trace relations between the c_n then yield relations between the P_n by diagrams (5) and (6). We have

$$\pi_{n+1/n}(P_{n+1}) = a_p P_n - \nu_{n-1/n}(P_{n-1}),$$

$$\pi_{1/0}(P_1) = u P_0 \quad \text{with } u \in \mathbf{Z}_p^{\times}. \tag{7}$$

Since c_n and $i_{n-1/n}(c_{n-1})$ generate $\hat{E}(\mathbf{Q}_{n,p})$ as a Galois module, (4) yields

$$\Lambda_n/(P_n, \nu_{n-1/n}(P_{n-1})) \cong \mathrm{Sel}_p(E/\mathbf{Q}_n)^{\wedge} \text{ for } n \geqslant 1 \text{ and}$$

$$\Lambda_0/(P_0) \cong \mathrm{Sel}_p(E/\mathbf{Q})^{\wedge}. \tag{8}$$

Our goal is thus to compute the size of $\Lambda_n/(P_n, \nu_{n-1/n}(P_{n-1}))$.

We first compute the μ and λ-invariants of P_n. For $n \geqslant 2$, let

$$q_n = \begin{cases} p^{n-1} - p^{n-2} + \cdots + p - 1 & \text{for } 2 \mid n \\ p^{n-1} - p^{n-2} + \cdots + p^2 - p & \text{for } 2 \nmid n \end{cases}$$

and set $q_0 = q_1 = 0$.

Lemma 5.1. *For* $n \geqslant 0$,

(1) $\mu(P_n) = 0$.
(2) $\lambda(P_n) = q_n$.

Proof. We have $\Lambda_0/(P_0) \cong \mathrm{Sel}_p(E/\mathbf{Q})^\wedge = 0$. Hence P_0 is a unit and thus P_1 is a unit since $\pi_{1/0}(P_1) = uP_0$ with $u \in \mathbf{Z}_p^\times$. Therefore, $\mu(P_0) = \mu(P_1) = 0$. Proceeding by induction, we assume that $\mu(P_k) = 0$ for $k \leqslant n$. We have

$$\begin{aligned} \mu(\pi_{n+1/n}(P_{n+1})) &= \mu(a_p P_n - \nu_{n-1/n}(P_{n-1})) && \text{(by (7))} \\ &= \mu(\nu_{n-1/n}(P_{n-1})) && \text{(since } p \mid a_p\text{)} \\ &= \mu(P_{n-1}) && \text{(by Proposition 4.9.3)} \\ &= 0. \end{aligned}$$

Thus, by Proposition 4.9.1, $\mu(P_{n+1}) = 0$ which completes the proof of part 1.

As for part 2, we have already seen that P_0 and P_1 are units and hence $\lambda(P_0) = \lambda(P_1) = 0 = q_0 = q_1$. Again, proceeding by induction, assume that $\lambda(P_k) = q_k$ for $k \leqslant n$. We have

$$\begin{aligned} \lambda(\pi_{n+1/n}(P_{n+1})) &= \lambda(a_p P_n - \nu_{n-1/n}(P_{n-1})) \\ &= \lambda(\nu_{n-1/n}(P_{n-1})) \\ &= p^n - p^{n-1} + \lambda(P_{n-1}) && \text{(by Proposition 4.9.4)} \\ &= p^n - p^{n-1} + q_{n-1} \\ &= q_{n+1}. \end{aligned}$$

Since we have already seen that $\mu(\pi_{n+1/n}(P_{n+1})) = 0$, by Proposition 4.9.2, we conclude that $\lambda(P_{n+1}) = \lambda(\pi_{n+1/n}(P_{n+1})) = q_{n+1}$ completing the proof. □

The following lemma will be key in performing the necessary induction to compute the size of $\Lambda/(P_n, \nu_{n-1/n}(P_{n-1}))$.

Lemma 5.2. *We have an exact sequence*

$$0 \longrightarrow \Lambda_{n-1}/J_{n-1} \xrightarrow{\nu_{n-1/n}} \Lambda/J_n \xrightarrow{\chi} \mathbf{Z}_p[\mu_{p^n}]/(\chi(P_n)) \longrightarrow 0$$

where $J_n = (P_n, \nu_{n-1/n}(P_{n-1}))$ *for* $n > 0$, $J_0 = (P_0)$ *and* χ *is a character of* G_n *of order* p^n.

Proof. We check that $\nu_{n-1/n}(J_{n-1}) \subseteq J_n$ and that the first map is injective. The other details are straightforward to verify.

We have that

$$\begin{aligned}\nu_{n-1/n}(\nu_{n-2/n-1}(P_{n-2})) &= \nu_{n-1/n}(a_p P_{n-1} - \pi_{n/n-1}(P_n)) \quad \text{(by (7))}\\ &= a_p \nu_{n-1/n}(P_{n-1}) - \xi_n P_n,\end{aligned}$$

which lies in J_n and thus

$$\nu_{n-1/n}(J_{n-1}) = \big(\nu_{n-1/n}(P_{n-1}), \nu_{n-1/n}(\nu_{n-2/n-1}(P_{n-2}))\big) \subseteq J_n.$$

Thus the first map is well-defined.

To check injectivity, let $f \in \Lambda_{n-1}$ such that $\nu_{n-1/n}(f) \in J_n$. Then

$$\nu_{n-1/n}(f) = \alpha \cdot P_n + \beta \cdot \nu_{n-1/n}(P_{n-1})$$

and we see that $\alpha \cdot P_n \in \mathrm{im}(\nu_{n-1/n})$. By Lemma 4.10, $\alpha = \nu_{n-1/n}(\alpha')$ for some $\alpha' \in \Lambda_{n-1}$ since $\mu(P_n) = 0$ and $\lambda(P_n) = q_n < p^{n-1}$. Hence

$$\nu_{n-1/n}(f) = \nu_{n-1/n}(\alpha') \cdot P_n + \beta \cdot \nu_{n-1/n}(P_{n-1})$$

and applying $\pi_{n/n-1}$ yields

$$\begin{aligned}p \cdot f &= p \cdot \alpha' \cdot \pi_{n/n-1}(P_n) + p \cdot \pi_{n/n-1}(\beta) \cdot P_{n-1}\\ &= p \cdot \alpha' \cdot (a_p P_{n-1} - \nu_{n-2/n-1}(P_{n-2})) + p \cdot \pi_{n/n-1}(\beta) \cdot P_{n-1}\end{aligned}$$

which lies in pJ_{n-1}. Since Λ_n is p-torsion free, we have that $f \in J_{n-1}$ which establishes the injectivity of the first map. □

Recall the quantity e_n defined in Section 1.

Proposition 5.3. *For* $n \geqslant 0$,

$$\mathrm{ord}_p\,(\#\Lambda_n/J_n) = e_n.$$

Proof. For $n = 0$ we have $\Lambda_0/J_0 \cong \Lambda_0/(P_0) = 0 = e_0$ since P_0 is a unit. We proceed by induction on n. By direct computation, Lemma 5.1 and Lemma 4.5, we have that

$$\mathrm{ord}_p\left(\#(\mathbf{Z}_p[\mu_{p^n}]/\chi(P_n))\right) = p^{n-1}(p-1) \cdot \mathrm{ord}_p(\chi(P_n)) = q_n,$$

where χ is a character on G_n of order p^n. Therefore, by induction and Lemma 5.2, we have

$$\begin{aligned}\mathrm{ord}_p\,(\#\Lambda_n/J_n) &= \mathrm{ord}_p\,(\#\Lambda_{n-1}/J_{n-1}) + \mathrm{ord}_p\left(\#(\mathbf{Z}_p[\mu_{p^n}]/\chi(P_n))\right)\\ &= e_{n-1} + q_n = e_n. \qquad \Box\end{aligned}$$

Proof of Theorem 1.1. By (8), we have for $n \geqslant 0$,

$$\mathrm{Sel}_p(E/\mathbf{Q}_n)^\wedge \cong \Lambda_n/J_n.$$

Hence, by Proposition 5.3,

$$\mathrm{ord}_p(\#\mathrm{Sel}_p(E/\mathbf{Q}_n)) = e_n$$

and, in particular, it is a finite group. Thus, $E(\mathbf{Q}_n)$ is finite (proving part 1) and $\mathrm{ord}_p(\#\text{Ш}(E/\mathbf{Q}_n)[p^\infty]) = e_n$ (proving part 2).

Now, if $a_p = 0$ we have

$$\begin{aligned}\mathrm{Tr}_{n/m}(c_n) &= \mathrm{Tr}_{n-1/m}(-i_{n-2/n-1}(c_{n-2}))\\ &= -p\,\mathrm{Tr}_{n-2/m}(c_{n-2}) = \cdots = \pm p^r i_{m-1/m}(c_{m-1})\end{aligned}$$

for some r when m and n have different parities. Thus, by diagram (6),

$$\pi_{n/m}(P_n) \in \mathrm{im}(v_{m-1/m})$$

and, by Lemma 4.6.3, $\chi(P_n) = 0$ for χ of order p^m. Therefore, $P_n \in J_n^\varepsilon$ for $\varepsilon = (-1)^{n+1}$ and

$$J_n = (P_n, v_{n-1/n}(P_{n-1})) \subseteq J_n^+ + J_n^-.$$

Then, comparing sizes, we see that

$$\text{Ш}(E/\mathbf{Q}_n)[p^\infty]^\wedge \cong \Lambda_n/(P_n, v_{n-1/n}(P_{n-1})) \cong \Lambda_n/(J_n^+ + J_n^-)$$

completing the proof of part 3. $\Box$

Remark 5.4. Note that under Kurihara's hypotheses, [8, Proposition 1.2] implies that

$$J_n^+ + J_n^- = (\theta_n, v_{n-1/n}(\theta_{n-1})),$$

where $\theta_n \in \Lambda_n$ is the Mazur-Tate-Teitelbaum element defined via modular symbols. Hence part 3 of Theorem 1.1 is consistent with the isomorphism

$$Ш(E/\mathbf{Q}_n)[p^\infty]^\wedge \cong \Lambda/(\theta_n, \nu_{n-1/n}(\theta_{n-1}))$$

proven in [8].

Acknowledgments

We thank Ralph Greenberg and Adrian Iovita for many interesting conversations on the Iwasawa theory of elliptic curves at supersingular primes. We also thank the anonymous referee for pointing out an important detail that was not verified.

References

[1] J. Coates, R. Greenberg, Kummer theory for abelian varieties over local fields, Invent. Math. 124 (1–3) (1996) 129–174.

[2] J. Coates, R. Sujatha, Galois Cohomology of Elliptic Curves, Narosa Publishing House, New Delhi, 2000.

[3] R. Greenberg, Iwasawa theory for elliptic curves, in: Arithmetic Theory of Elliptic Curves (Cetraro, 1997), Lecture Notes in Mathematics, vol. 1716, Springer, Berlin, 1999, pp. 51–144.

[4] M. Hazewinkel, On norm maps for one dimensional formal groups I, The cyclotomic Γ-extension, J. Algebra 32 (1974) 89–108.

[5] T. Honda, On the theory of commutative formal groups, J. Math. Soc. Japan 22 (1970) 213–246.

[6] A. Iovita, R. Pollack, Iwasawa theory of elliptic curves at supersingular primes over $\mathbf{Z}_p$-extensions of number fields, MSRI Proceedings, to appear.

[7] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, Invent. Math. 152 (1) (2003) 1–36.

[8] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, Invent. Math. 149 (2002) 195–224.

[9] Y.I. Manin, Cyclotomic fields and modular curves, Uspehi Mat. Nauk 26 (162) (1971) 7–71.

[10] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Invent. Math. 18 (1972) 183–266.

[11] A.G. Nasybullin, Elliptic curves with supersingular reduction over Γ-extensions (Russian), Uspehi Mat. Nauk 32 (194) (1977) 221–222.

[12] B. Perrin-Riou, Théorie d'Iwasawa p-adique locale et globale (French) [Local and global p-adic Iwasawa theory], Invent. Math. 99 (2) (1990) 247–292.

[13] P. Schneider, p-adic height pairings II, Invent. Math. 79 (2) (1985) 329–374.