Invent. math. 149, 195–224 (2002)
Digital Object Identifier (DOI) 10.1007/s002220100206

Inventiones mathematicae

On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I

Masato Kurihara

Department of Mathematics, Tokyo Metropolitan University, Hachioji, Tokyo, 192-0397, Japan (e-mail: kurihara@math.metro-u.ac.jp)

Oblatum 17-II-2000 & 15-XI-2001
Published online: 9 April 2002 –

0 Introduction

Let E be an elliptic curve defined over $\mathbf{Q}$. We fix a prime number p, and suppose that $K_\infty/\mathbf{Q}$ is the cyclotomic $\mathbf{Z}_p$-extension. Put $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/\mathbf{Q})]]$. A remarkable theorem by Rubin (CM case) and Kato (non CM case) [24] [14], which was a conjecture of Mazur, states that the Pontrjagin dual of the p-primary component of the Tate Shafarevich group of E over K_∞ is a torsion Λ-module if E has ordinary reduction at p. By this fact together with Mazur's control theorem [17] and the general theory of torsion Λ-modules which goes back to Iwasawa, we know the asymptotic behaviour of the Tate Shafarevich groups over K_n as $n \to \infty$ where K_n denotes the subfield of K_∞ such that $[K_n : \mathbf{Q}] = p^n$. Namely, if the p-primary components of the Tate Shafarevich groups of E over K_n are finite and if we denote the order by p^{e_n}, we know that there exist λ, $\mu \in \mathbf{Z}_{\geq 0}$ and $\nu \in \mathbf{Z}$ such that

$$e_n = \lambda n + \mu p^n + \nu$$

for all sufficiently large n. This is, of course, an analogue of Iwasawa's famous formula for the class numbers of the intermediate fields in a $\mathbf{Z}_p$-extension [12]. But if E does not have potentially ordinary reduction, we know almost nothing about the asymptotic behaviour of the Tate Shafarevich groups[1]. Our aim in this paper is to study the asymptotic behaviour in the case that E has supersingular reduction at p. (See [3] Chap. 4 and [6] §5 for more details on this problem.)

In this part I, we consider the simplest situation. Suppose that E has supersingular reduction at p. Let $L(E, s)$ be the L-function of E. Our main assumption is that p does not divide $L(E, 1)/\Omega_E$ where Ω_E is the Néron period. If the Birch and Swinnerton-Dyer conjecture is true, this would

[1] see "Note added in proof"

imply that rank $E(\mathbf{Q}) = 0$, and the p-component of the Tate Shafarevich group over $\mathbf{Q}$ is trivial, and that p does not divide the Tamagawa factor $\mathrm{Tam}(E) = \Pi c_\ell = \Pi(E(\mathbf{Q}_\ell) : E_0(\mathbf{Q}_\ell))$. (As usual, $E_0(\mathbf{Q}_\ell)$ is the subgroup which consists of the points whose reduction to $E(\mathbf{F}_\ell)$ is not a singular point.) Our main theorem in this paper is the following.

Theorem 0.1 *Let p be an odd prime number. We assume that E has supersingular reduction at p, and that p satisfies*

$$\mathrm{ord}_p(L(E, 1)/\Omega_E) = 0$$

and

$$p \nmid \mathrm{Tam}(E) = \Pi c_\ell.$$

Further, we assume that the Galois action

$$\rho_{E[p]} : G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(E[p]) \simeq GL_2(\mathbf{F}_p)$$

on the p-torsion points $E[p]$ is surjective. Let $K_\infty/\mathbf{Q}$ be the cyclotomic $\mathbf{Z}_p$-extension, and for $n \geq 0$, K_n denote the field satisfying $\mathbf{Q} \subset K_n \subset K_\infty$ and $[K_n : K] = p^n$. We put $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/\mathbf{Q})]]$.

(1) *The Pontrjagin dual $(Ш(E/K_\infty)\{p\})^\vee$ of the p-primary component of the Tate Shafarevich group of E/K_∞ is isomorphic to Λ as a Λ-module.*
(2) *For any $n \geq 0$, the rank of $E(K_n)$ is zero, and the p-primary component $Ш(E/K_n)\{p\}$ of the Tate Shafarevich group of E/K_n is finite.*
(3) *We define e_n by*

$$p^{e_n} = \#Ш(E/K_n)\{p\}.$$

Then we have

$$e_0 = e_1 = 0$$

and

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

(4) *For any $n > 0$, let θ_{K_n} be the modular element of Mazur and Tate (see §1 for the definition). For any m and n such that $0 \leq m < n$, let $\nu_{m,n} : \mathbf{Z}_p[\mathrm{Gal}(K_m/\mathbf{Q})] \longrightarrow \mathbf{Z}_p[\mathrm{Gal}(K_n/\mathbf{Q})]$ denote the ring homomorphism defined by $\sigma \mapsto \Sigma\tau$ for $\sigma \in \mathrm{Gal}(K_m/\mathbf{Q})$ where τ ranges over all elements of $\mathrm{Gal}(K_n/\mathbf{Q})$ projecting to σ. Then, the Pontrjagin dual $(Ш(E/K_n)\{p\})^\vee$ of the p-primary component of the Tate Shafarevich group over K_n is isomorphic to*

$$\mathbf{Z}_p[\mathrm{Gal}(K_n/\mathbf{Q})]/(\theta_{K_n}, \nu_{n-1,n}(\theta_{K_{n-1}}))$$

as a $\mathbf{Z}_p[\mathrm{Gal}(K_n/\mathbf{Q})]$-module.

Remark 0.2 (1) Let $[x]$ denote the maximal integer m such that $x \geq m$ for a real number x. Then, Theorem 0.1 (3) can be formulated as

$$e_n = [\mu p^n + \lambda n], \qquad \mu = \frac{p}{p^2-1}, \quad \lambda = -\frac{1}{2}$$

for *any* $n \geq 0$. The idea to use rational numbers as invariants in the formulation of Theorem 0.1 (3) was suggested to me by Y.Ihara.

(2) Theorem 0.1 (1) and (2) are not very difficult if we use a deep theorem of Kato [14]. In fact, we will prove $L(E/K_n, 1) \neq 0$ for all $n \geq 0$ in Proposition 1.2. This implies Theorem 0.1 (2) by Kato's theorem [14]. Further, if we denote by $\mathrm{Sel}(E/K_\infty)$ the Selmer group with respect to $E[p^\infty]$ (cf. Definition 4.1), the above implies that $\mathrm{Sel}(E/K_\infty)$ is equal to the p-component of $Ш(E/K_\infty)$. For the Selmer group, we know its Pontrjagin dual is isomorphic to Λ (cf. Coates and Sujatha [3] Theorem 4.5), so we obtain Theorem 0.1 (1). Our main results are Theorem 0.1 (3) and (4). (For several phenomena of Iwasawa theory of elliptic curves with supersingular reduction, see also Perrin-Riou [21] and [22].)

(3) Theorem 0.1 (3) is compatible with the Birch and Swinnerton-Dyer conjecture. More precisely, we can verify the p-part of the Birch and Swinnerton-Dyer conjecture for E over K_n by using Theorem 0.1 (3) (see Remark 1.3).

(4) By Theorem 0.1 (4), we know the structure of $Ш(E/K_n)\{p\}$ as an abelian group for all $n \geq 0$. See Theorem 7.4.

(5) An analogous case in the ordinary setting is the following. Assume that E has good ordinary reduction at p, and that $\mathrm{rank}\, E(\mathbf{Q}) = 0$, and that $E(\mathbf{Q})$ does not contain a point of order p, and that the p-component of the Tate Shafarevich group of E over $\mathbf{Q}$ is trivial. We further assume that $a_p \not\equiv 1 \pmod{p}$ where $a_p = p + 1 - \#E(\mathbf{F}_p)$, and that p does not divide $\mathrm{Tam}(E)$. Then, by the control theorem of Mazur ([17]), we obtain $e_n = 0$ for all $n \geq 0$, namely the p-component of the Tate Shafarevich group of E over K_n is trivial (cf. [5] Prop. 3.8).

Concerning the ideal class groups of number fields, the following is well known. Let K be a number field such that p is inert in $K/\mathbf{Q}$, and that p does not divide the class number of K. Suppose that K_∞/K is the cyclotomic $\mathbf{Z}_p$-extension, and that K_n is the n-th layer. Then, the p-primary part of the ideal class group of K_n is trivial for all $n \geq 0$ (Iwasawa [11]).

(6) We note that for a given elliptic curve E without complex multiplication, there exist infinitely many p's which satisfy the conditions in Theorem 0.1. For example, if $E = X_0(11)$, any odd supersingular prime ($p = 19, 29, \ldots$) satisfies the conditions.

(7) In the part II of this paper, we will study the asymptotic formula of the orders of the Tate Shafarevich groups without assuming the condition on the L-values.

Mazur and Tate conjectured that their modular element is in the Fitting ideal of the Pontrjagin dual of the Selmer group (Conjecture 3 in [19]). We propose

Conjecture 0.3 Let E be an elliptic curve over $\mathbf{Q}$, and p be an odd prime number, and K_n the n-th layer of the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Assume that E has good reduction at p, and that $E(\mathbf{Q})$ does not have a point of order p, and that p does not divide the Tamagawa factor $\mathrm{Tam}(E)$. Suppose that θ_{K_n} is the modular element of Mazur and Tate (see §1 for the definition), and $\mathrm{Sel}(E/K_n)^\vee$ is the Pontrjagin dual of the Selmer group concerning $E[p^\infty]$ (see §4 for the definition). Then, the Fitting ideal of the $\mathbf{Z}_p[\mathrm{Gal}(K_n/\mathbf{Q})]$-module $\mathrm{Sel}(E/K_n)^\vee$ is generated by θ_{K_n} and $\nu_{n-1,n}(\theta_{K_{n-1}})$, namely

$$\mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(K_n/\mathbf{Q})]}(\mathrm{Sel}(E/K_n)^\vee) = (\theta_{K_n}, \nu_{n-1,n}(\theta_{K_{n-1}})).$$

This conjecture gives more information than the usual Iwasawa Main Conjecture. For conjectures of this type for the ideal class groups of abelian fields, see [16].

Theorem 0.1 (4) says that under the assumption of Theorem 0.1 Conjecture 0.3 is true.

The organization of this paper is as follows. In §1 we study the value $L(E, \psi^{-1}, 1)$ for a character ψ of $\mathrm{Gal}(K_n/\mathbf{Q})$. In §2 and §3 we study an elliptic curve E over $\mathbf{Q}_p$. In §2 we study the norm map of the rational points of E over local fields, and we also introduce an analogue of Artin-Hasse-Shafarevich exponential for E. In §3 we introduce a certain pairing $P_n(x, z)$ which is related to the works of Perrin-Riou [23], [22] (cf. also Rubin [25] Appendix). This pairing has an integrality property, and plays an important role in §7. In §4 we define a certain subgroup $\mathrm{Sel}_0(E/F)$ of the Selmer group of an elliptic curve E over F, and give some results which are consequences of a control theorem for $\mathrm{Sel}_0(E/F)$. (If p is a supersingular prime, we do not have a control theorem for the Selmer groups, but a control theorem can be proved for $\mathrm{Sel}_0(E/F)$.) Using this subgroup of the Selmer group, we can formulate the Iwasawa Main Conjecture, which will be explained in §6. In §5 under the assumption of Theorem 0.1 we give a description of the Selmer group by using the zeta elements of Kato. In §7 we prove Theorem 0.1. We define r_n by

$$r_n = [\mu p^n + \lambda n] \qquad \mu = \frac{p}{p^2 - 1}, \quad \lambda = -\frac{1}{2}$$

as in Remark 0.2 (1), and e_n by $p^{e_n} = \#Ш(E/K_n)\{p\}$. Theorem 0.1 (3) says that $e_n = r_n$ for any $n \geq 0$. The inequality $e_n \geq r_n$ follows from some calculation of the formal groups in §2 and the finiteness of $\mathrm{Sel}(E/K_n)$. The inequality $e_n \leq r_n$ is more difficult, and we need the argument involving

the zeta elements of Kato, the modular elements of Mazur and Tate, and the pairing in §3.

I would like to express my hearty thanks to J. Coates and R. Greenberg for valuable discussions on this topic. Especially, the discussion with them at Nikko in 1998 was inspiring, and made me study the subject in this paper. I would also like to thank Y. Ihara heartily for giving me an important suggestion (cf. Remark 0.2 (1)). I am also grateful to K. Kato for constant discussions on Iwasawa theory.

Notation

For a group G and a G-module M, M^G denotes the G-invariant part and M_G denotes the G-coinvariant. For a prime number p, $\mathrm{ord}_p : \mathbf{Q}^\times \longrightarrow \mathbf{Z}$ is the normalized additive valuation such that $\mathrm{ord}_p(p) = 1$.

1 The values of L-functions

Suppose that E is a modular elliptic curve over $\mathbf{Q}$ and $L(E, s) = \Sigma a_n n^{-s}$ is the corresponding L-function.

For $n \geq 0$, we put $\mathcal{G}'_n = \mathrm{Gal}(\mathbf{Q}(\mu_{p^n})/\mathbf{Q})/\{\pm 1\} \simeq (\mathbf{Z}/p^n)^\times/\{\pm 1\}$, and denote by σ_a the element corresponding to $a \in (\mathbf{Z}/p^n)^\times/\{\pm 1\}$. Let

$$\theta_{p^n} = \sum_{a \in (\mathbf{Z}/p^n)^\times/\{\pm 1\}} \left[\frac{a}{p^n}\right] \sigma_a \in \mathbf{Q}[\mathcal{G}'_n]$$

be the modular element defined by Mazur and Tate [19] p.716. (Here, $[a/b]$ is defined as follows. Let $f(z) = \Sigma a_n \exp(2\pi i n z)$ be the modular form corresponding to E. We define $[a/b]$ by

$$2\pi \int_0^\infty f\left(\frac{a}{b} + iy\right) dy = \left[\frac{a}{b}\right] \Omega_E^+ + \left[\frac{a}{b}\right]^- \Omega_E^-$$

where $\Omega_E^\pm$ are the Néron periods. We write $\Omega_E = \Omega_E^+$.)

Let p be an odd prime. Suppose that θ_{p^n} is in $\mathbf{Z}_{(p)}[\mathcal{G}'_n]$ for every $n \geq 0$ where $\mathbf{Z}_{(p)}$ denotes the localization of $\mathbf{Z}$ at the prime ideal (p) (we will see later that if we assume the conditions of Theorem 0.1, $\theta_{p^n} \in \mathbf{Z}_{(p)}[\mathcal{G}'_n]$ certainly holds). We define $\theta_{K_n} \in \mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})]$ to be the image of $\theta_{p^{n+1}} \in \mathbf{Z}_{(p)}[\mathcal{G}'_{n+1}]$ by the natural map $\mathbf{Z}_{(p)}[\mathcal{G}'_{n+1}] \longrightarrow \mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})]$.

Suppose that m and n are integers such that $0 \leq m \leq n$. We denote by

$$\pi_{n,m} : \mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})] \longrightarrow \mathbf{Z}_{(p)}[\mathrm{Gal}(K_m/\mathbf{Q})]$$

the natural projection, and by

$$\nu_{m,n} : \mathbf{Z}_{(p)}[\mathrm{Gal}(K_m/\mathbf{Q})] \longrightarrow \mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})]$$

the trace map which sends σ to $\Sigma\tau$ where τ ranges through all elements of $\mathrm{Gal}(K_n/\mathbf{Q})$ projecting to σ in $\mathrm{Gal}(K_m/\mathbf{Q})$. We put $a_p = p + 1 - \#E(\mathbf{F}_p)$. Then, by the formula (1.3) (4) in [19], we have

$$\pi_{n,n-1}(\theta_{K_n}) = a_p\theta_{K_{n-1}} - \nu_{n-2,n-1}(\theta_{K_{n-2}})$$

for $n \geq 2$.

We define an ideal I_n of $\mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})]$ to be the ideal generated by all $\nu_{m,n}(\theta_{K_m})$ such that $0 \leq m \leq n$.

The following lemma can be checked easily by the above formula on θ_{K_n}, $\theta_{K_{n-1}}$, and $\theta_{K_{n-2}}$. (So $I_n \otimes \mathbf{Z}_p$ is the ideal appearing in the right hand side of Conjecture 0.3).

Lemma 1.1 *For $n \geq 1$, I_n is generated by θ_{K_n} and $\nu_{n-1,n}(\theta_{K_{n-1}})$. We also have $\pi_{n,m}(I_n) \subset I_m$ and $\nu_{m,n}(I_m) \subset I_n$ for any m and n with $0 \leq m \leq n$.*

For a Dirichlet character ψ, we denote by $L(E, \psi, s) = \Sigma a_n\psi(n)n^{-s}$ the twisted L-function.

Our aim in this section is to show

Proposition 1.2 *We assume that E has supersingular reduction at an odd prime p, and that $\mathrm{ord}_p(L(E, 1)/\Omega_E) = 0$. Let ψ be a Dirichlet character of conductor p^{n+1} which factors through $\mathrm{Gal}(K_n/\mathbf{Q})$, and $L(E, \psi^{-1}, s)$ be the twisted L-function by the character ψ^{-1}. We denote by $\tau(\psi)$ the Gauss sum $\Sigma\psi(a)\exp(2\pi ia/p^{n+1})$. Then, $\tau(\psi)L(E, \psi^{-1}, 1)/\Omega_E$ is in $\mathbf{Q}(\mu_{p^n})$ (where μ_{p^n} is the group of p^n-th roots of unity), and its p-adic valuation can be computed as follows. Let $\mathrm{ord}_p : \mathbf{Q}(\mu_{p^n})^\times \longrightarrow \mathbf{Q}$ be the additive valuation of the prime ideal of $\mathbf{Q}(\mu_{p^n})$ lying over p such that $\mathrm{ord}_p(p) = 1$. For $n = 1$, $\mathrm{ord}_p(\tau(\psi)L(E, \psi^{-1}, 1)/\Omega_E) = 0$. For any $n \geq 2$ we have*

$$\mathrm{ord}_p(\tau(\psi)L(E, \psi^{-1}, 1)/\Omega_E) = \frac{q_n}{p^{n-1}(p-1)}$$

where q_n is defined by

$$q_n = \begin{cases} p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \ldots + p - 1 & \text{for even } n \geq 2 \\ p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \ldots + p^2 - p & \text{for odd } n \geq 3. \end{cases}$$

First of all, we will show $\theta_{p^n} \in \mathbf{Z}_{(p)}[\mathcal{G}'_n]$. Since p is a supersingular prime, the Galois representation of $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the p-torsion points $E[p]$ is irreducible. Hence, by Corollary 4.1 in [18] and Proposition 3.3 in [7], the Manin constant of E for $X_1(N)$ is not divisible by p. Namely, we can take a parametrization $\rho : X_1(N) \longrightarrow E$ such that $\rho^*(\omega_E) = c_1 f(q)dq/q$ and $c_1 \not\equiv 0 \pmod{p}$. Here, ω_E is the Néron differential, and $f(q)$ is the normalized eigenform of level N corresponding to E. Further, since p is a supersingular prime, $E(\mathbf{Q}(\mu_{p^n}))$ does not contain a point of order p for any $n > 0$. These facts together with $L(E, 1)/\Omega_E \in \mathbf{Z}_{(p)}$

imply, by Theorem 3.14 in Stevens [26], that θ_{p^n} is in $\mathbf{Z}_{(p)}[\mathcal{G}_n']$. So θ_{K_n} is in $\mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})]$.

We extend ψ to a ring homomorphism $\psi : \mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})] \longrightarrow \mathbf{Z}_{(p)}[\mu_{p^n}]$. Then we have $\psi(\theta_{K_n}) = \tau(\psi)L(E, \psi^{-1}, 1)/2\Omega_E$ by (1.4) in [19]. So in order to prove this proposition, it is enough to compute $\mathrm{ord}_p(\psi(\theta_{K_n}))$.

For $n = 0$, by definition, $\theta_{K_0} = \pi(\theta_p)$ where π is the map $\sigma \mapsto 1$ for $\sigma \in \mathcal{G}_1'$. We have $\pi(\theta_p) = (a_p - 2)\theta_{p^0} = (a_p - 2)\theta_1 = (a_p - 2)L(E, 1)/2\Omega_E$ by (1.3) (1) in [19], so $\theta_{K_0} = (a_p - 2)L(E, 1)/2\Omega_E$, and it is a unit of $\mathbf{Z}_{(p)}$ by our assumption.

By (1.3) (4) in [19], we get $\pi_{1,0}(\theta_{K_1}) = a_p\theta_{K_0} - (p-1)\theta_1 = (a_p(a_p - 2) - (p-1))L(E, 1)/2\Omega_E$, so $\pi_{1,0}(\theta_{K_1})$ is a unit, and θ_{K_1} is also a unit. Hence, for $n = 1$, we obtain $\mathrm{ord}_p(\tau(\psi)L(E, \psi^{-1}, 1)/\Omega_E) = 0$.

Next, we consider the case $n \geq 2$. We take a generator γ of $\mathrm{Gal}(K_n/\mathbf{Q})$ and identify $\mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})]$ with $\mathbf{Z}_{(p)}[T]/((1+T)^{p^n} - 1)$ by identifying γ with $1 + T$. Then, from

$$\pi_{n,n-1}(\theta_{K_n}) = a_p\theta_{K_{n-1}} - \nu_{n-2,n-1}(\theta_{K_{n-2}}),$$

we can write

$$\theta_{K_n} = a_p\tilde{\theta}_{K_{n-1}} - \frac{(1+T)^{p^{n-1}} - 1}{(1+T)^{p^{n-2}} - 1}\tilde{\theta}_{K_{n-2}} + ((1+T)^{p^{n-1}} - 1)g$$

for some $g \in \mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})]$ where $\tilde{\theta}_{K_{n-1}}$ and $\tilde{\theta}_{K_{n-2}}$ are elements of $\mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})]$ which project to $\theta_{K_{n-1}}$ and $\theta_{K_{n-2}}$, respectively. By induction on n and the fact that p divides a_p, we can write

$$\theta_{K_n} = \begin{cases} \dfrac{(1+T)^{p^{n-1}} - 1}{(1+T)^{p^{n-2}} - 1}\dfrac{(1+T)^{p^{n-3}} - 1}{(1+T)^{p^{n-4}} - 1}\cdots\dfrac{(1+T)^{p} - 1}{T}u_n + p\alpha_n \\ + \dfrac{(1+T)^{p^{n-1}} - 1}{(1+T)^{p^{n-2}} - 1}\dfrac{(1+T)^{p^{n-3}} - 1}{(1+T)^{p^{n-4}} - 1}\cdots\{(1+T)^{p} - 1\}\beta_n \\ \qquad\qquad \text{for even } n \geq 2 \\ \dfrac{(1+T)^{p^{n-1}} - 1}{(1+T)^{p^{n-2}} - 1}\dfrac{(1+T)^{p^{n-3}} - 1}{(1+T)^{p^{n-4}} - 1}\cdots\dfrac{(1+T)^{p^2} - 1}{(1+T)^{p} - 1}u_n + p\alpha_n \\ + \dfrac{(1+T)^{p^{n-1}} - 1}{(1+T)^{p^{n-2}} - 1}\dfrac{(1+T)^{p^{n-3}} - 1}{(1+T)^{p^{n-4}} - 1}\cdots\dfrac{(1+T)^{p^2} - 1}{(1+T)^{p} - 1}T\beta_n \\ \qquad\qquad \text{for odd } n \geq 3 \end{cases}$$

for some $u_n \in \mathbf{Z}_{(p)}^{\times}$ and some α_n, $\beta_n \in \mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})]$. Put $\psi(\gamma) = \zeta$. Since ψ is of conductor p^{n+1}, ζ is a primitive p^n-th root of unity, and $\psi : \mathbf{Z}_{(p)}[\mathrm{Gal}(K_n/\mathbf{Q})] = \mathbf{Z}_{(p)}[T]/((1+T)^{p^n} - 1) \longrightarrow \mathbf{Z}_{(p)}[\mu_{p^n}]$ is given by $f(T) \mapsto f(\zeta - 1)$. Hence, we obtain

$$\mathrm{ord}_p(\psi(\theta_{K_n})) = \frac{q_n}{p^{n-1}(p-1)}.$$

This completes the proof of Proposition 1.2.

Remark 1.3 The Birch and Swinnerton-Dyer conjecture for E/K_n predicts

$$L(E/K_n, 1) = \frac{\#Ш(E/K_n)}{(\#E(K_n)_{\mathrm{tors}})^2}\,\mathrm{Tam}(E/K_n)\frac{1}{\sqrt{d_{K_n}}}(\Omega_E)^{p^n}$$

where d_{K_n} is the discriminant of K_n (cf. [1], see also [2] §5). Hence, by Proposition 1.2, $\mathrm{ord}_p(\#Ш(E/K_n))$ is conjectured to be $\Sigma_{i=2}^{n} q_i$ which is equal to e_n in Theorem 0.1 (3). Hence, Theorem 0.1 (3) implies the p-part of the Birch and Swinnerton-Dyer conjecture for E/K_n.

2 Preparation from formal groups

2.1. In this subsection, we study a one-dimensional formal group $\mathcal{F}$ defined over $\mathbf{Z}_p$ with height 2. For any finite extension k of $\mathbf{Q}_p$, m_k denotes the maximal ideal of the integer ring O_k, and $\mathcal{F}(m_k^i)$ denotes the group defined by $\mathcal{F}$ on m_k^i.

Let $k_\infty/\mathbf{Q}_p$ be the cyclotomic $\mathbf{Z}_p$-extension, and for $n \geq 0$, k_n be the field satisfying $\mathbf{Q}_p \subset k_n \subset k_\infty$ and $[k_n : \mathbf{Q}_p] = p^n$. For an integer $n > 0$, we consider the norm map

$$N : \mathcal{F}(m_{k_n}) \longrightarrow \mathcal{F}(m_{k_{n-1}}).$$

For $n = 1$, N is surjective by Theorem 6.1 in Hazewinkel [8]. For $n \geq 2$, we have

Proposition 2.1

$$\mathrm{ord}_p \#(\mathcal{F}(m_{k_{n-1}})/N\mathcal{F}(m_{k_n})) \geq q_n$$

where q_n is the number defined in Proposition 1.2.

Proof of Proposition 2.1. We use the method of Hazewinkel [9]. By Honda's theory [10], we may assume $\mathcal{F}$ is a formal group whose logarithm is of the form $\log_{\mathcal{F}}(T) = \Sigma a_n T^{p^n}$. By Lemma 2.4 in [9], we have $\mathrm{ord}_p(a_{2i}) = -i$ and $\mathrm{ord}_p(a_{2i+1}) \geq -i$. So, for a finite extension $k/\mathbf{Q}_p$, $\log_{\mathcal{F}} : \mathcal{F}(m_k) \longrightarrow k$ induces isomorphisms

$$\log_{\mathcal{F}} : \mathcal{F}\left(m_k^j\right) \xrightarrow{\simeq} m_k^j$$

for all $j > v_k(p)/(p^2 - 1)$.

We first consider a commutative diagram

$$\begin{array}{ccc} \mathcal{F}(m_{k_n}) & \xrightarrow{\log_{\mathcal{F}}} & k_n \\ \downarrow N & & \downarrow \mathrm{Tr} \\ \mathcal{F}(m_{k_{n-1}}) & \xrightarrow{\log_{\mathcal{F}}} & k_{n-1} \end{array}$$

where $N : \mathcal{F}(m_{k_n}) \longrightarrow \mathcal{F}(m_{k_{n-1}})$ (resp. $\mathrm{Tr} : k_n \longrightarrow k_{n-1}$) is the norm map (resp. the trace map). Put

$$s_n = \begin{cases} p^{n-2} + p^{n-4} + \ldots + p^2 + 2 & \text{for even } n \geq 2 \\ p^{n-2} + p^{n-4} + \ldots + p + 1 & \text{for odd } n \geq 3, \end{cases}$$

namely $s_n = [p^n/(p^2-1)] + 1$. By (3.1) and (3.4) in [9], if $i \geq s_n$, we have

$$\mathrm{Tr}\left(\log_{\mathcal{F}}\left(m_{k_n}^i\right)\right) = \mathrm{Tr}\left(m_{k_n}^i\right) = m_{k_{n-1}}^j$$

where

$$j = \left[p^{n-1} + 1 + \frac{i-2}{p}\right].$$

Put

$$\begin{aligned} t_n &= \left[p^{n-1} + 1 + \frac{s_n - 2}{p}\right] \\ &= \begin{cases} p^{n-1} + p^{n-3} + \ldots + p + 1 & \text{for even } n \geq 2 \\ p^{n-1} + p^{n-3} + \ldots + p^2 + 1 & \text{for odd } n \geq 3. \end{cases} \end{aligned}$$

Since $t_n > p^{n-1}/(p^2-1)$, $\log_{\mathcal{F}}$ induces an isomorphism $\log_{\mathcal{F}}(\mathcal{F}(m_{k_{n-1}}^{t_n})) \simeq m_{k_{n-1}}^{t_n}$. Hence, the above commutative diagram implies that

$$N\mathcal{F}\left(m_{k_n}^{s_n}\right) = \mathcal{F}\left(m_{k_{n-1}}^{t_n}\right).$$

Since $\#(\mathcal{F}(m_{k_n})/\mathcal{F}(m_{k_n}^{s_n})) = p^{s_n - 1}$ and $\#(\mathcal{F}(m_{k_{n-1}})/\mathcal{F}(m_{k_{n-1}}^{t_n})) = p^{t_n - 1}$, we have

$$\mathrm{ord}_p(\#(\mathcal{F}(m_{k_{n-1}})/N\mathcal{F}(m_{k_n}))) \geq (t_n - 1) - (s_n - 1).$$

From $t_n - s_n = q_n$, we get the conclusion of Proposition 2.1.

2.2. Let E be an elliptic curve over $\mathbf{Q}_p$ with good reduction. In this subsection, we will give an analogue of Artin-Hasse-Shafarevich exponential for E (Proposition 2.2). We also remark that in the case $a_p = 0$ (note that if p is a supersingular prime ≥ 5, we always have $a_p = 0$) the situation in this subsection is very simple (see Remark 2.3 (1)).

2.2.1. Let $\hat{E}$ be the formal group associated to E, and $\log_{\hat{E}}(X) = X + \ldots \in \mathbf{Q}_p[[X]]$ (resp. $\exp_{\hat{E}} = X + \ldots \in \mathbf{Q}_p[[X]]$) be the logarithm (resp. the exponential) of $\hat{E}$. $\hat{E}$ defines a group structure on $X\mathbf{Q}_p[[X]]$ which we denote by $\hat{E}(X\mathbf{Q}_p[[X]])$. As is well known, $\log_{\hat{E}}$ gives an isomorphism from $\hat{E}(X\mathbf{Q}_p[[X]])$ to $X\mathbf{Q}_p[[X]]$ and $\exp_{\hat{E}}$ gives the inverse. We define a ring homomorphism

$$\varphi : \mathbf{Q}_p[[X]] \longrightarrow \mathbf{Q}_p[[X]]$$

by $\varphi(\Sigma a_i X^i) = \Sigma a_i X^{ip}$.

We put $a_p = p + 1 - \#E(\mathbf{F}_p)$. We define a sequence $(c_n)_{n\geq 0}$ of rational numbers by $c_0 = 0$, $c_1 = 1$, and $c_{n+1} - p^{-1}a_p c_n + p^{-1}c_{n-1} = 0$. Put

$$g(X) = \sum_{n=0}^{\infty} c_{n+1} X^{p^n}.$$

Then, $(\varphi^2 - a_p\varphi + p)g(X) = pX$, so in the terminology of Honda [10] §2, $g(X)$ is of type $T^2 - a_pT + p$. Hence, there is a formal group $\mathcal{F}$ defined over $\mathbf{Z}_p$ whose logarithm is $g(X)$ ([10] Theorem 2). Since $\log_{\hat{E}}$ is also of type $T^2 - a_pT + p$ ([10] Theorem 9 (6.7)), $\mathcal{F}$ and $\hat{E}$ are isomorphic as formal groups over $\mathbf{Z}_p$ ([10] Prop. 3.5). Hence, $\exp_{\hat{E}}(g(X)) \in \mathbf{Z}_p[[X]]$.

Put $\mathbb{E} = \exp_{\hat{E}} \circ (\Sigma_{n=0}^{\infty} c_{n+1}\varphi^n)$. Then, we have $\mathbb{E}(X^i) = \exp_{\hat{E}}(g(X^i))$ for any $i > 0$, so $\mathbb{E}(X^i) \in \mathbf{Z}_p[[X]]$. Hence, for any $f(X) \in X\mathbf{Z}_p[[X]]$ we have $\mathbb{E}(f(X)) \in \mathbf{Z}_p[[X]]$, and $\mathbb{E}$ gives a homomorphism

$$\mathbb{E} : X\mathbf{Z}_p[[X]] \longrightarrow \hat{E}(X\mathbf{Z}_p[[X]])$$

(which can be proved to be bijective).

2.2.2. Let $\mathcal{E}$ be a smooth elliptic curve over $\mathbf{Z}_p$ whose generic fiber is E, and whose special fiber we denote by $\mathcal{E}_0$. We consider a crystalline cohomology $\mathcal{D} = H^1_{cris}(\mathcal{E}_0/\mathbf{Z}_p)$, which is a free $\mathbf{Z}_p$-module of rank 2, and has the Frobenius endomorphism $\Phi : \mathcal{D} \longrightarrow \mathcal{D}$. We write $D = \mathcal{D} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and define φ to be $\varphi = p^{-1}\Phi : D \longrightarrow D$, which satisfies $\varphi^{-2} - a_p\varphi^{-1} + p = 0$.

Let $\omega = \omega_E$ be the Néron differential of $\mathcal{E}$ which we regard as an element of $\mathcal{D}$. We denote by D^0 the subgroup of D generated by invariant differentials, so we have $D^0 = \mathbf{Q}_p\omega$. We have $[\varphi(\omega), \omega] \neq 0$.

Let k be a finite extension of $\mathbf{Q}_p$ and m_k be the maximal ideal of the ring of integers of k. The map

$$\log : \hat{E}(m_k) \longrightarrow \mathrm{Hom}(D^0, k)$$

is defined by $x \mapsto (\omega \mapsto \log_{\hat{E}}(x))$ where $\log_{\hat{E}}$ is the formal logarithm in 2.2.1. By using the cup product $[\ ,\ ] : D \times D \longrightarrow \mathbf{Q}_p$ of de Rham cohomology D, we regard log to be the map

$$\log : \hat{E}(m_k) \longrightarrow (D/D^0) \otimes k$$

which sends x to $\log_{\hat{E}}(x)\omega^*$ where ω^* is an element of D such that $[\omega^*, \omega] = 1$. The exponential map

$$\exp : \tan(E) \otimes k = D/D^0 \otimes k \longrightarrow \hat{E}(m_k) \otimes \mathbf{Q}_p$$

is defined as the inverse of log, and we have $\exp(x\omega^*) = \exp_{\hat{E}}(x)$ if $x \in (m_k)^i$

and i is sufficiently large. We define

$$\exp : X\mathbf{Q}_p[[X]] \otimes D \longrightarrow \hat{E}(X\mathbf{Q}_p[[X]])$$

by $\exp(f(X) \otimes (a\omega + b\omega^*)) = \exp_{\hat{E}}(bf(X))$.

Let $\varphi : \mathbf{Q}_p[[X]] \longrightarrow \mathbf{Q}_p[[X]]$ be the endomorphism as above. We define

$$\varphi : \mathbf{Q}_p[[X]] \otimes D \longrightarrow \mathbf{Q}_p[[X]] \otimes D$$

by $\varphi(f(X) \otimes \alpha) = \varphi(f(X)) \otimes \varphi(\alpha)$.

The following proposition is an analogue of Artin-Hasse-Shafarevich exponential for E.

Proposition 2.2 *Put* $\mathcal{E}xp = \exp \circ (1 + \varphi + \varphi^2 + ...)$. *For any* $f(X) \in X\mathbf{Z}_p[[X]]$, *we have*

$$\mathcal{E}xp(f(X) \otimes [\varphi(\omega), \omega]^{-1}\omega) \in \hat{E}(X\mathbf{Z}_p[[X]])$$

and

$$\mathcal{E}xp(f(X) \otimes [\varphi(\omega), \omega]^{-1}\varphi(\omega)) \in \hat{E}(X\mathbf{Z}_p[[X]]).$$

Proof. Let $(c_n)_{n\geq 0}$ be as in 2.2.1. Using $\varphi^2 = p^{-1}a_p\varphi - p^{-1}$ on D, we can show

$$\varphi^n(\omega) = -\frac{1}{p}c_{n-1}\omega + c_n\varphi(\omega).$$

By using $\mathbb{E}$ in 2.2.1, we get

$$\begin{aligned}
\mathcal{E}xp(f(X) \otimes [\varphi(\omega), \omega]^{-1}\omega) &= \exp(\sum_{n=0}^{\infty}(\varphi^n(f(X)) \otimes [\varphi(\omega), \omega]^{-1}c_n\varphi(\omega))) \\
&= \exp_{\hat{E}}(\sum_{n=0}^{\infty}\varphi^n(f(X))c_n) \\
&= \exp_{\hat{E}}(\sum_{n=0}^{\infty}c_{n+1}\varphi^n(\varphi(f(X)))) \\
&= \mathbb{E}(\varphi(f(X))).
\end{aligned}$$

Hence, we obtain $\mathcal{E}xp(f(X) \otimes [\varphi(\omega), \omega]^{-1}\omega) \in \hat{E}(X\mathbf{Z}_p[[X]])$.

By the same method, we have

$$\begin{aligned}
\mathcal{E}xp(f(X) \otimes [\varphi(\omega), \omega]^{-1}\varphi(\omega)) &= \exp_{\hat{E}}(\sum_{n=0}^{\infty}c_{n+1}\varphi^n(f(X))) \\
&= \mathbb{E}(f(X)),
\end{aligned}$$

so we get $\mathcal{E}xp(f(X) \otimes [\varphi(\omega), \omega]^{-1}\varphi(\omega)) \in \hat{E}(X\mathbf{Z}_p[[X]])$.

Remark 2.3 (1) Suppose that $a_p = 0$. Then, $(c_n)_{n\geq 0}$ becomes simple, and we have $g(X) = \Sigma_{k=0}^{\infty}(-1)^k p^{-k} X^{p^{2k}}$ and

$$\mathbb{E} = \exp_{\hat{E}} \circ \left(1 - \frac{\varphi^2}{p} + \frac{\varphi^4}{p^2} + ... + (-1)^k \frac{\varphi^{2k}}{p^k} + ...\right).$$

Hence, the function $\mathcal{E}xp$ in Proposition 2.2 also has a simple form.

(2) If the action of $G_{\mathbf{Q}_p}$ on the p-torsion points $E[p]$ is irreducible (for example, if E has supersingular reduction), we can show that $[\varphi(\omega), \omega]$ is a unit (cf. [4] §9) (though we do not use this fact in this paper).

3 The image of a certain pairing $P_n(x, z)$

In this section, we assume E is an elliptic curve over $\mathbf{Q}_p$, which has good supersingular reduction.

We use the same notation as in §2.2, and consider D, $\varphi : D \longrightarrow D$, $D^0 = \mathbf{Q}_p\omega$, etc.

We fix a generator (ζ_{p^n}) of $\mathbf{Z}_p(1)$, namely ζ_{p^n} is a primitive p^n-th root of unity, and $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ for any $n \geq 1$. For $n \geq 1$, we define

$$\gamma_n : D \longrightarrow D \otimes \mathbf{Q}_p(\mu_{p^n})$$

by

$$x \mapsto \frac{1}{p^n}\left(\sum_{i=0}^{n-1} \varphi^{i-n}(x) \otimes \zeta_{p^{n-i}} + (1-\varphi)^{-1}(x)\right).$$

This map plays an important role to define p-adic L-functions generally in a work of Perrin-Riou [23], but we do not mention p-adic L-functions here.

The following lemma can be checked easily (cf. Rubin [25] Lemma A1).

Lemma 3.1 (*i*) *For $n \geq 1$ we have*

$$\mathrm{Tr}_{\mathbf{Q}_p(\mu_{p^{n+1}})/\mathbf{Q}_p(\mu_{p^n})}(\gamma_{n+1}(x)) = \gamma_n(x)$$

and

$$\mathrm{Tr}_{\mathbf{Q}_p(\mu_p)/\mathbf{Q}_p}(\gamma_1(x)) = (1-\varphi)^{-1}\left(1 - \frac{\varphi^{-1}}{p}\right)(x).$$

(*ii*) *Assume that ψ is of conductor p^m such that $0 < m \leq n$. Put*

$$\mathcal{G}_n = \mathrm{Gal}(\mathbf{Q}_p(\mu_{p^n})/\mathbf{Q}_p).$$

We extend ψ by linearity to a ring homomorphism $\psi : D \otimes \mathbf{Q}_p(\mu_{p^n})[\mathcal{G}_n] \longrightarrow D \otimes \mathbf{Q}_p(\mu_{p^n})$. Then, we have

$$\psi\left(\sum_{\sigma \in \mathcal{G}_n} \gamma_n(x)^\sigma \sigma\right) = \frac{1}{p^m}\tau(\psi)\varphi^{-m}(x)$$

where $\tau(\psi) = \Sigma_{\sigma \in \mathcal{G}_m} \psi(\sigma)\zeta_{p^m}^\sigma$ is the Gauss sum.

Let $T = T_p(E)$ be the Tate module of E, and $V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. We consider a Galois cohomology group $H^1(\mathbf{Q}_p(\mu_{p^n}), V)$ and the dual exponential map $\exp^* : H^1(\mathbf{Q}_p(\mu_{p^n}), V) \longrightarrow D \otimes \mathbf{Q}_p(\mu_{p^n})$, which is defined by Tate duality as the dual of the exponential map $D \otimes \mathbf{Q}_p(\mu_{p^n}) \longrightarrow H^1(\mathbf{Q}_p(\mu_{p^n}), V)$ (cf. [13] Chap. II §1.2). Let

$$\begin{array}{ccc} D \times D & \longrightarrow & \mathbf{Q}_p \\ (x, y) & \mapsto & [x, y] \end{array}$$

be the cup product of the de Rham cohomology. We extend this product linearly to

$$D \otimes \mathbf{Q}_p(\mu_{p^n})[\mathcal{G}_n] \quad \times \quad D \otimes \mathbf{Q}_p(\mu_{p^n})[\mathcal{G}_n] \quad \longrightarrow \quad \mathbf{Q}_p(\mu_{p^n})[\mathcal{G}_n].$$

For $(x, z) \in D \times H^1(\mathbf{Q}_p(\mu_{p^n}), V)$, we define $P_n(x, z)$ by

$$P_n(x, z) = [\sum_{\sigma \in \mathcal{G}_n} \gamma_n(x)^\sigma \sigma, \sum_{\sigma \in \mathcal{G}_n} \exp^*(\sigma(z))\sigma^{-1}]$$

(cf. Rubin [25] p. 366).

Lemma 3.2

$$P_n(x, z) = \sum_{\sigma \in \mathcal{G}_n} \mathrm{Tr}_{\mathbf{Q}_p(\mu_{p^n})/\mathbf{Q}_p}[\gamma_n(x)^\sigma, \exp^*(z)]\sigma.$$

Proof (cf. [25] p. 366). In fact, we have

$$\begin{aligned} P_n(x, z) &= \sum_{\sigma \in \mathcal{G}_n} \sum_{\tau \in \mathcal{G}_n} [\gamma_n(x)^\tau, \exp^*(\tau\sigma^{-1}(z))]\sigma \\ &= \sum_{\sigma \in \mathcal{G}_n} \mathrm{Tr}_{\mathbf{Q}_p(\mu_{p^n})/\mathbf{Q}_p}[\gamma_n(x), \exp^*(\sigma^{-1}(z))]\sigma \\ &= \sum_{\sigma \in \mathcal{G}_n} \mathrm{Tr}_{\mathbf{Q}_p(\mu_{p^n})/\mathbf{Q}_p}[\gamma_n(x)^\sigma, \exp^*(z)]\sigma. \end{aligned}$$

By Lemma 3.2, we know that $P_n(x, z)$ is in $\mathbf{Q}_p[\mathcal{G}_n]$. Further, by a straightforward calculation using Lemma 3.2, we have

Lemma 3.3 *Let $\pi : \mathbf{Q}_p[\mathcal{G}_n] \longrightarrow \mathbf{Q}_p[\mathcal{G}_{n-1}]$ be the natural map. Then, we have*

$$\pi(P_n(x, z)) = P_{n-1}(x, N(z))$$

where $N : H^1(\mathbf{Q}_p(\mu_{p^n}), V) \longrightarrow H^1(\mathbf{Q}_p(\mu_{p^{n-1}}), V)$ is the corestriction map.

From the definition of $P_n(x, z)$ and Lemma 3.1, we have the following two lemmas (cf. [25] Proposition A2 (i)).

Lemma 3.4 *Let ψ be a character of $\mathcal{G}_n$, whose conductor is p^m such that $0 < m \leq n$. We extend ψ to $\psi : \mathbf{Q}_p[\mathcal{G}_n] \longrightarrow \mathbf{Q}_p(\mu_{p^m})$. Then, we have*

$$\psi(P_n(x, z)) = \frac{1}{p^m}\tau(\psi) \sum_{\sigma \in \mathcal{G}_n} \psi^{-1}(\sigma)[\varphi^{-m}(x), \exp^*(\sigma(z))]$$

where $\tau(\psi)$ is the Gauss sum in Lemma 3.1.

Lemma 3.5 *Let $\mathbf{1}$ denote the character of $\mathcal{G}_n$, whose conductor is* 1. *Then, we have*

$$\mathbf{1}(P_n(x, z)) = \left[(1 - \varphi)^{-1}\left(1 - \frac{\varphi^{-1}}{p}\right)(x), \exp^*(N(z))\right]$$

where $N : H^1(\mathbf{Q}_p(\mu_{p^n}), V) \longrightarrow H^1(\mathbf{Q}_p), V)$ is the corestriction map.

Our aim in this section is to prove

Proposition 3.6 *Let T be the Tate module of E. For any $n \geq 1$ and any $z \in H^1(\mathbf{Q}_p(\mu_{p^n}), T)$, we have*

$$p^n[\varphi(\omega), \omega]^{-1} P_n(\varphi^{n+1}(\omega), z) \in \mathbf{Z}_p[\mathcal{G}_n]$$

and

$$p^n[\varphi(\omega), \omega]^{-1} P_n(\varphi^{n}(\omega), z) \in \mathbf{Z}_p[\mathcal{G}_n].$$

Proof. Let $\hat{E}$ be the formal group over $\mathbf{Z}_p$ associated to E, and m be the maximal ideal of the ring of integers of $\mathbf{Q}_p(\mu_{p^n})$, and $\log_{\hat{E}}$ be the formal logarithm of $\hat{E}$. As in 2.2.2, we consider

$$\log : \hat{E}(m) \longrightarrow (D/D^0) \otimes \mathbf{Q}_p(\mu_{p^n})$$

which sends x to $\log_{\hat{E}}(x)\omega^*$ where ω^* is an element of D such that $[\omega^*, \omega] = 1$.

Then, by the definition of the dual exponential map, we have a commutative diagram

$$\begin{array}{ccccc} \hat{E}(m) & \times H^1(\mathbf{Q}_p(\mu_{p^n}), T) & \longrightarrow & H^2(\mathbf{Q}_p(\mu_{p^n}), \mathbf{Z}_p(1)) \simeq \mathbf{Z}_p \\ \downarrow \log & \downarrow \exp^* & & \downarrow i \\ D/D^0 \otimes \mathbf{Q}_p(\mu_{p^n}) & \times \quad D^0 \otimes \mathbf{Q}_p(\mu_{p^n}) & \longrightarrow & \mathbf{Q}_p \end{array}$$

where the upper horizontal arrow is defined as the composition of the Kummer map $\hat{E}(m) = E(\mathbf{Q}_p(\mu_{p^n})) \otimes \mathbf{Z}_p \longrightarrow H^1(\mathbf{Q}_p(\mu_{p^n}), T)$ and the cup product, the lower horizontal arrow is defined by $(x, y) \mapsto \mathrm{Tr}_{\mathbf{Q}_p(\mu_{p^n})/\mathbf{Q}_p}[x, y]$, $\exp^*$ is the restriction of $\exp^*$ to $H^1(\mathbf{Q}_p(\mu_{p^n}), T)$, and $i : \mathbf{Z}_p \longrightarrow \mathbf{Q}_p$ is the inclusion.

By Lemma 3.2 and the above commutative diagram, in order to show $p^n[\varphi(\omega), \omega]^{-1} P_n(\varphi^{n+1}(\omega), z) \in \mathbf{Z}_p[\mathcal{G}_n]$, it suffices to show

$$p^n[\varphi(\omega), \omega]^{-1}\gamma_n(\varphi^{n+1}(\omega)) \bmod D^0 \otimes \mathbf{Q}_p(\mu_{p^n}) \in \log(\hat{E}(m))$$

because if $p^n[\varphi(\omega), \omega]^{-1}\gamma_n(\varphi^{n+1}(\omega))$ can be written as $\log(y)$, we have $p^n[\varphi(\omega), \omega]^{-1} P_n(\varphi^{n+1}(\omega), z) = \Sigma(y^\sigma, z)\sigma$ where $(*, *)$ is the cup product of Galois cohomology.

For any $x \in D$, we have

$$\begin{aligned} p^n\gamma_n(x) &= \zeta_{p^n}\varphi^{-n}(x) + \zeta_{p^{n-1}}\varphi^{-(n-1)}(x) + \ldots + \zeta_p\varphi^{-1}(x) + (1-\varphi)^{-1}(x) \\ &= (\zeta_{p^n} - 1)\varphi^{-n}(x) + (\zeta_{p^{n-1}} - 1)\varphi^{-(n-1)}(x) + \ldots \\ &\quad + (\zeta_p - 1)\varphi^{-1}(x) + \varphi^{-n}(1-\varphi)^{-1}(x). \end{aligned}$$

Put $\pi = \zeta_{p^n} - 1$. We have

$$\begin{aligned} p^n\gamma_n(\varphi^{n+1}(\omega)) &= \pi\varphi(\omega) + ((1+\pi)^p - 1)\varphi^2(\omega) + \ldots \\ &\quad + ((1+\pi)^{p^{n-1}} - 1)\varphi^n(\omega) + (1-\varphi)^{-1}(\varphi(\omega)). \end{aligned}$$

Since $(1-\varphi)^{-1}(\varphi(\omega)) = (p - a + 1)^{-1} p\varphi(\omega) \bmod D^0$, we have $[\varphi(\omega), \omega]^{-1}(1-\varphi)^{-1}(\varphi(\omega)) \bmod D^0 \in \log(\hat{E}(m))$ because $p\omega^*$ is in $\log(\hat{E}(m))$. Thus, it suffices to show

$$\exp([\varphi(\omega), \omega]^{-1} \sum_{i=0}^{\infty}((1+\pi)^{p^i} - 1)\varphi^{i+1}(\omega)) \in \hat{E}(m).$$

We need the following lemma.

Lemma 3.7 *For any $i \geq 1$, there is a unique homogeneous polynomial $m_i(X, Y) \in \mathbf{Z}[X, Y]$ of degree p^i such that for any $n \geq 1$ $m_i(X, Y)$'s satisfy*

$$(X+Y)^{p^n} = X^{p^n} + Y^{p^n} + pm_1(X^{p^{n-1}}, Y^{p^{n-1}}) + \ldots + p^n m_n(X, Y).$$

This lemma can be checked by induction on n.

We use the function $\mathcal{E}xp$ in Proposition 2.2. Then, we have

$$\begin{aligned} &\exp([\varphi(\omega), \omega]^{-1} \sum_{i=0}^{\infty}((1+\pi)^{p^i} - 1)\varphi^{i+1}(\omega)) \\ &= \exp([\varphi(\omega), \omega]^{-1}(\sum_{i=0}^{\infty} \pi^{p^i}\varphi^{i+1}(\omega) + \sum_{i=1}^{\infty} pm_1(\pi^{p^{i-1}}, 1)\varphi^{i+1}(\omega) \\ &\quad + \sum_{i=2}^{\infty} p^2 m_2(\pi^{p^{i-2}}, 1)\varphi^{i+1}(\omega) + \ldots)) \end{aligned}$$

$$= \exp([\varphi(\omega), \omega]^{-1} \sum_{i=0}^{\infty} (\pi^{p^i} \varphi^{i+1}(\omega) + m_1(\pi^{p^i}, 1) p\varphi^{i+2}(\omega)$$
$$+ m_2(\pi^{p^i}, 1) p^2 \varphi^{i+3}(\omega) + \ldots))$$
$$= (\mathcal{E}xp(X \otimes [\varphi(\omega), \omega]^{-1} \varphi(\omega)) + \mathcal{E}xp(m_1(X, 1) \otimes [\varphi(\omega), \omega]^{-1} p\varphi^2(\omega))$$
$$+ \mathcal{E}xp(m_2(X, 1) \otimes [\varphi(\omega), \omega]^{-1} p^2 \varphi^3(\omega)) + \ldots)_{|X=\pi}.$$

By Proposition 2.2, $\mathcal{E}xp_E(X \otimes [\varphi(\omega), \omega]^{-1}\varphi(\omega))$, $\mathcal{E}xp_E(m_1(X, 1) \otimes [\varphi(\omega), \omega]^{-1} p\varphi^2(\omega))$, $\mathcal{E}xp_E(m_2(X, 1) \otimes [\varphi(\omega), \omega]^{-1} p^2\varphi^3(\omega))$,... are all in $\hat{E}(X\mathbf{Z}_p[[X]])$. Hence, $\exp([\varphi(\omega), \omega]^{-1} \sum_{i=0}^{\infty}((1+\pi)^{p^i} - 1)\varphi^{i+1}(\omega))$ is in $\hat{E}(m)$. This completes the proof of $p^n[\varphi(\omega), \omega]^{-1} P_n(\varphi^{n+1}(\omega), z) \in \mathbf{Z}_p[\mathcal{G}_n]$. The statement on $P_n(\varphi^n(\omega), z)$ can be proved by the same method.

4 A certain subgroup of Selmer groups

In this section, we define a subgroup $\mathrm{Sel}_0(E/F)$ of the Selmer group of an elliptic curve E over a number field F, and study their properties.

Let E be an elliptic curve over a number field F.

Definition 4.1 *We fix a rational prime p. For an algebraic extension F'/F, we define* $\mathrm{Sel}(E/F')$ *to be the Selmer group with respect to $E[p^\infty]$, namely*

$$\mathrm{Sel}(E/F') = \mathrm{Ker}\big(H^1(F', E[p^\infty]) \longrightarrow \prod_v H^1\big(F'_v, E[p^\infty]\big)/\big(E\big(F'_v\big) \otimes \mathbf{Q}_p/\mathbf{Z}_p\big)\big)$$

where v ranges over all primes of F'. We also define a subgroup $\mathrm{Sel}_0(E/F')$ *of* $\mathrm{Sel}(E/F')$ *to be*

$$\mathrm{Sel}_0(E/F') = \mathrm{Ker}(\mathrm{Sel}(E/F') \longrightarrow \prod_{v|p} H^1(F'_v, E[p^\infty]))$$

where v ranges over the primes of F' lying over p.

Let S be the subset of the primes of F consisting of the primes lying over p and the primes at which E has bad reductions. For a $\mathbf{Z}_p$-extension F_∞/F, we put $\Gamma = \mathrm{Gal}(F_\infty/F)$, and denote by F_n the subfield of F_∞ such that $[F_n : F] = p^n$. We consider the ring $O_F[1/S]$ of S-integers (elements whose additive valuations outside S are non-negative) of F, and its integral closure $O_{F_n}[1/S]$ in F_n, and consider the etale cohomology groups $H^*(O_{F_n}[1/S], \mathcal{F})$ $(= H^*(G_{F_n,S}, \mathcal{F})$ where $G_{F_n,S}$ is the Galois group of the maximal unramified extension of F_n outside S over $F_n)$. Let $T = T_p(E)$ be the Tate module of E. We define

$$\mathbf{H}^1(O_{F_\infty}[1/S], T) = \varprojlim H^1(O_{F_n}[1/S], T).$$

We assume p is an odd prime. Concerning $\mathrm{Sel}_0(E/F)$ we have a control theorem (cf. Remark 4.4), but for the proof of Theorem 0.1 we only need a special case of the control theorem, so here we prove the following two lemmas which can be easily verified.

Lemma 4.2 *Suppose that p does not divide the Tamagawa factor* $\mathrm{Tam}(E)$*, and $E(F_v)$ does not have a point of order p for any v above p. Then, we have a natural isomorphism*

$$\mathrm{Sel}_0(E/F) \xrightarrow{\simeq} \mathrm{Sel}_0(E/F_\infty)^\Gamma.$$

Lemma 4.3 *Suppose that p does not divide the Tamagawa factor* $\mathrm{Tam}(E)$*, $E(F_v)$ does not have a point of order p for any v above p, and* $\mathrm{Sel}_0(E/F)=0$*. Then, we have* $\mathrm{Sel}_0(E/F_n) = 0$*, and the natural map*

$$\mathbf{H}^1(O_{F_\infty}[1/S], T) \longrightarrow H^1(O_{F_n}[1/S], T)$$

is surjective for all $n \geq 0$.

Remark 4.4 In general, we have a control theorem for $\mathrm{Sel}_0(E/F)$, which implies the above two lemmas. Namely, we have an exact sequence

$$\begin{aligned}
&\mathrm{Image}(((\bigoplus_{v\in S_\infty} H^0(F_{\infty,v}, E[p^\infty]))/H^0(F_\infty, E[p^\infty]))^\Gamma \\
&\longrightarrow H^1(\Gamma, H^0(F_\infty, E[p^\infty])) \\
&\longrightarrow \mathrm{Sel}_0(E/F) \longrightarrow \mathrm{Sel}_0(E/F_\infty)^\Gamma \\
&\longrightarrow ((\bigoplus_{v\in S_\infty} H^0(F_{\infty,v}E[p^\infty]))/H^0(F_\infty, E[p^\infty]))_\Gamma \longrightarrow \\
&(\mathrm{Coker}(\mathbf{H}^1(O_{F_\infty}[1/S], T)_\Gamma \longrightarrow H^1(O_F[1/S], T)))^\vee \longrightarrow \\
&\mathrm{Sel}_0(E/F_\infty)_\Gamma \longrightarrow 0
\end{aligned}$$

where $(*)^\vee$ means the Pontrjagin dual of $(*)$, and S_∞ is the set of primes of F_∞ above S. This will be proved in Part II.

Proof of Lemma 4.2. We put $A = E[p^\infty]$. If v does not divide p, we have $E(F_v) \otimes \mathbf{Q}_p/\mathbf{Z}_p = 0$, hence by the definition of $\mathrm{Sel}_0(E/F)$, we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}_0(E/F) \longrightarrow H^1(O_F[1/S], A) \longrightarrow \bigoplus_{v\in S} H^1(F_v, A).$$

We denote by S_∞ the primes of F_∞ lying over S, and compare the above exact sequence with the exact sequence

$$0 \longrightarrow \mathrm{Sel}_0(E/F_\infty)^\Gamma \longrightarrow H^1(O_{F_\infty}[1/S], A)^\Gamma \longrightarrow (\bigoplus_{v\in S_\infty} H^1(F_{\infty,v}, A))^\Gamma.$$

Our assumption implies $E(F)[p] = 0$ which implies that $H^1(O_F[1/S], A) \xrightarrow{\simeq} H^1(O_{F_\infty}[1/S], A)^\Gamma$ is bijective. Since $p \nmid \mathrm{Tam}(E)$ and $E(F_v)[p] = 0$ for all v lying over p, we have $(\bigoplus_{v\in S_\infty} H^0(F_{\infty,v}, A))_\Gamma = 0$ (Greenberg [5] §3). Hence, $\bigoplus_{v\in S} H^1(F_v, A) \longrightarrow \bigoplus_{v\in S_\infty} H^1(F_{\infty,v}, A)$ is injective. Thus, by the snake lemma we get the conclusion of Lemma 4.2.

Proof of Lemma 4.3. By Lemma 4.2 and Nakayama's lemma, we get $\mathrm{Sel}_0(E/F_\infty) = 0$. Using Lemma 4.2 again for F_∞/F_n, we have $\mathrm{Sel}_0(E/F_n) = 0$.

In order to prove the second claim, we may assume $n = 0$ by replacing F_n with F. Concerning $\mathrm{Sel}(E/F)$, by Cassels-Tate-Poitou duality we have an exact sequence

$$\bigoplus_{v\in S} H^1(F_v, T)/(E(F_v)\otimes \mathbf{Z}_p) \longrightarrow \mathrm{Sel}(E/F)^\vee \longrightarrow H^2(O_F[1/S], T) \longrightarrow \bigoplus_{v\in S} H^2(F_v, T) \longrightarrow H^0(F, A)^\vee \longrightarrow 0.$$

Since $E(F_v)\otimes \mathbf{Q}_p/\mathbf{Z}_p = 0$ for a prime v which does not divide p, the above exact sequence yields an exact sequence

$$0 \longrightarrow \mathrm{Sel}_0(E/F)^\vee \longrightarrow H^2(O_F[1/S], T) \longrightarrow \bigoplus_{v\in S} H^2(F_v, T) \longrightarrow H^0(F, A)^\vee \longrightarrow 0.$$

This exact sequence together with $\mathrm{Sel}_0(E/F) = 0$ implies that $H^2(O_F[1/S], T)$ is finite, and $H^2(O_F[1/S], A) = 0$.

Hence, by Tate-Poitou duality, we have an exact sequence

$$0 \longrightarrow H^1(O_F[1/S], A) \xrightarrow{a} \bigoplus_{v\in S} H^1(F_v, A) \xrightarrow{b} H^1(O_F[1/S], T)^\vee \longrightarrow 0$$

where the injectivity of a follows from $\mathrm{Sel}_0(E/F) = 0$, and the surjectivity of b follows from $H^2(O_F[1/S], A) = 0$. We compare this exact sequence with the exact sequence

$$0 \longrightarrow H^1(O_{F_\infty}[1/S], A) \longrightarrow \bigoplus_{v\in S_\infty} H^1(F_{\infty,v}, A) \longrightarrow \mathbf{H}^1(O_{F_\infty}[1/S], T)^\vee \longrightarrow 0.$$

As we saw in the proof of Lemma 4.2, our assumption implies that $H^1(O_F[1/S], A) \xrightarrow{\simeq} H^1(O_{F_\infty}[1/S], A)^\Gamma$ is bijective, and $\bigoplus_{v\in S} H^1(F_v, A) \longrightarrow \bigoplus_{v\in S_\infty} H^1(F_{\infty,v}, A)$ is injective. Hence again by the snake lemma, we get the injectivity of $H^1(O_F[1/S], T)^\vee \longrightarrow \mathbf{H}^1(O_{F_\infty}[1/S], T)^\vee$. This completes the proof of Lemma 4.3.

For an algebraic extension F'/F, we define

$$\mathrm{Sel}'(E/F') = \mathrm{Ker}(H^1(F', E[p^\infty]) \longrightarrow \prod_{v \nmid p} H^1(F'_v, E[p^\infty]))$$

where v ranges over all primes which are prime to p. The following lemma can be proved by the same method as Lemma 4.2, and will be used in the next section.

Lemma 4.5 *Suppose that p does not divide the Tamagawa factor* $\mathrm{Tam}(E)$*, and $E(F)[p] = 0$. Then, we have a natural isomorphism*

$$\mathrm{Sel}'(E/F) \xrightarrow{\simeq} \mathrm{Sel}'(E/F_\infty)^\Gamma.$$

By definition, we have $\mathrm{Sel}_0(E/F) \subset \mathrm{Sel}(E/F) \subset \mathrm{Sel}'(E/F)$. We have control theorems for $\mathrm{Sel}_0(E/F)$ and $\mathrm{Sel}'(E/F)$, but a control theorem does not exist for $\mathrm{Sel}(E/F)$, in general.

5 The zeta elements by Kato and Selmer groups

In the following, we assume that E is a modular elliptic curve over $\mathbf{Q}$, and p is an odd prime number at which E has good reduction. Let S be the subset of the primes consisting of p and all bad primes of E, and $T = T_p(E)$ be the Tate module of E.

Suppose $K_\infty/\mathbf{Q}$ is the cyclotomic $\mathbf{Z}_p$-extension, and K_n is the n-th layer. Put $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/\mathbf{Q})]]$. Let v_n be the prime of K_n lying over p, and put $k = \mathbf{Q}_p$, $k_n = K_{n,v_n}$, and $k_\infty = \cup k_n$. Then, k_∞/k is the cyclotomic $\mathbf{Z}_p$-extension. We define

$$\mathbf{H}^q(O_{K_\infty}[1/S], T) = \varprojlim H^q(O_{K_n}[1/S], T)$$

and

$$\mathbf{H}^q(k_\infty, T) = \varprojlim H^q(k_n, T).$$

We use the following zeta elements constructed by K. Kato [14] Theorem 12.5.

Theorem 5.1 (K. Kato) *Assume that the Galois action $\rho_{E[p]} : G_\mathbf{Q} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(E[p]) \simeq GL_2(\mathbf{F}_p)$ on the p-torsion points $E[p]$ is surjective. Then, there exists a system of elements*

$$(z_n)_{n\geq 0} \in \mathbf{H}^1(O_{K_\infty}[1/S], T) = \varprojlim H^1(O_{K_n}[1/S], T)$$

$$(z_n \in H^1(O_{K_n}[1/S], T))$$

such that for any character ψ of $G_n = \mathrm{Gal}(K_n/\mathbf{Q})$ of order p^n with $n > 0$, we have

$$\sum_{\sigma \in G_n} \psi(\sigma) \exp^*(\sigma(z_n)) = \omega_E L(E, \psi, 1)/\Omega_E,$$

and

$$\exp^*(z_0) = \omega_E(1 - a_p/p + 1/p)L(E, 1)/\Omega_E$$

where

$$\exp^* : H^1(k_n, T) \longrightarrow H^0\big(E_{/k_n}, \Omega^1\big)$$

is the dual exponential map, and ω_E is the Néron differential, Ω_E is the Néron period, and $a_p = p + 1 - \#E(\mathbf{F}_p)$.

To get such a "good" (z_n), we also used the fact that the Néron period differs from the canonical period only by a p-adic unit (cf. [18] §4, [7] §3).

Our aim in this section is to prove

Proposition 5.2 *Let E be an elliptic curve over $\mathbf{Q}$, and p be an odd prime number at which E has supersingular reduction. We assume that $\mathrm{ord}_p(L(E, 1)/\Omega_E) = \mathrm{ord}_p \mathrm{Tam}(E) = 0$, and that the Galois action $\rho_{E[p]} : G_{\mathbf{Q}} \longrightarrow GL_2(\mathbf{F}_p)$ is surjective. Let (z_n) be the zeta elements in $\mathbf{H}^1(O_{K_\infty}[1/S], T)$ (Theorem 5.1). Then, we have*

(1) $\mathrm{Sel}_0(E/K_\infty) = 0$ *and* $\mathrm{Sel}_0(E/K_n) = 0$ *for all* $n \geq 0$.
(2) *We put* $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/\mathbf{Q})]]$, *and* $\Lambda_n = \mathbf{Z}_p[\mathrm{Gal}(K_n/\mathbf{Q})]$. *Then, the dual of* $\mathrm{Sel}(E/K_\infty)$ *is a free* Λ*-module of rank* 1, *and the dual of* $\mathrm{Sel}(E/K_n)$ *is isomorphic to* $H^1(k_n, T)/((E(k_n) \otimes \mathbf{Z}_p) + < z_n >)$ *for all* $n \geq 0$. *Here,* $< z_n >$ *is the* Λ_n*-module generated by the image of* z_n.
(3) $H^1(O_{K_n}[1/S], T)$ *is a free* Λ_n*-module of rank* 1, *and generated by* z_n *for all* $n \geq 0$.

Proof. The Cassels-Tate-Poitou duality yields an exact sequence

$$\varprojlim \mathrm{Sel}(E/\mathbf{Q}, E[p^n]) \longrightarrow H^1(\mathbf{Z}[1/S], T) \longrightarrow H^1(\mathbf{Q}_p, T)/(E(\mathbf{Q}_p) \otimes \mathbf{Z}_p)$$

where $\mathrm{Sel}(E/\mathbf{Q}, E[p^n])$ is the Selmer group with respect to p^n-torsion points $E[p^n]$. Since $L(E, 1) \neq 0$, by Kolyvagin [15] (or Kato [14]) we know that $\mathrm{Sel}(E/\mathbf{Q})$ is finite. Further, since p is a supersingular prime, $E(\mathbf{Q})$ does not contain a point of order p. Hence, $\varprojlim \mathrm{Sel}(E/\mathbf{Q}, E[p^n]) = 0$, so $H^1(\mathbf{Z}[1/S], T)$ is a free $\mathbf{Z}_p$-module of rank 1.

Note that the image of the dual exponential map

$$\exp^* : H^1(\mathbf{Q}_p, T) \longrightarrow H^0\big(E_{/\mathbf{Q}_p}, \Omega^1\big)$$

is in our case $p^{-1}\mathbf{Z}_p\omega_E$ ([25] Proposition 5.2), so the image of $H^1(\mathbf{Z}[1/S], T)$ under $\exp^*$ is contained in $p^{-1}\mathbf{Z}_p\omega_E$. By Theorem 5.1, we have $\exp^*(z_0) = \omega_E(1-a_p/p+1/p)L(E,1)/\Omega_E$, so our assumption $\mathrm{ord}_p(L(E,1)/\Omega_E) = 0$ implies that $\exp^*(z_0)$ generates $p^{-1}\mathbf{Z}_p\omega_E$, so z_0 generates $H^1(\mathbf{Z}[1/S], T) \simeq \mathbf{Z}_p$.

Further, since $\exp^*$ factors through $H^1(\mathbf{Q}_p, T)/(E(\mathbf{Q}_p)\otimes\mathbf{Z}_p)$ which is a free $\mathbf{Z}_p$-module of rank 1, the class of z_0 generates $H^1(\mathbf{Q}_p, T)/(E(\mathbf{Q}_p)\otimes\mathbf{Z}_p)$. Since $\rho_{E[p]} : G_{\mathbf{Q}} \longrightarrow GL_2(\mathbf{F}_p)$ is surjective, the argument of the Euler systems together with the above facts implies that $\mathrm{Sel}(E/\mathbf{Q}) = 0$ ([14] §14). (Concerning $\mathrm{Sel}(E/\mathbf{Q}) = 0$, cf. also [15].)

In particular, $\mathrm{Sel}_0(E/\mathbf{Q}) = 0$. Since p is a supersingular prime, we have $E(\mathbf{Q}_p)[p] = 0$. So we can apply Lemma 4.3, and we have $\mathrm{Sel}_0(E/K_n) = 0$ for any $n > 0$, and $\mathrm{Sel}_0(E/K_\infty) = 0$. Thus, we get (1).

Since $H^1(\mathbf{Z}[1/S], T)$ is generated by z_0 and $\mathbf{H}^1(O_{K_\infty}[1/S], T)$ is free of rank 1 as a Λ-module ([14] Theorem 12.4), the natural map $\mathbf{H}^1(O_{K_\infty}[1/S], T)_\Gamma \longrightarrow H^1(\mathbf{Z}[1/S], T)$ is bijective and (z_n) generates $\mathbf{H}^1(O_{K_\infty}[1/S], T)$ by Nakayama's lemma. Lemma 4.3 implies that for $n \geq 0$

$$H^1(O_{K_n}[1/S], T) \xleftarrow{\simeq} \mathbf{H}^1(O_{K_\infty}[1/S], T)_{\Gamma_n}$$

is bijective where $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$. Hence, $H^1(O_{K_n}[1/S], T)$ is a free Λ_n-module of rank 1, and generated by z_n. So we have proved (3).

Finally, we show (2). We first show $\mathrm{Sel}(E/K_\infty)^\vee \simeq \Lambda$. The proof is essentially the same as [3] Theorem 4.5 of Coates and Sujatha. Let $\mathrm{Sel}'(E/\mathbf{Q})$ be the group defined before Lemma 4.5. By definition, we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}(E/\mathbf{Q}) \longrightarrow \mathrm{Sel}'(E/\mathbf{Q}) \longrightarrow H^1(\mathbf{Q}_p, A)/(E(\mathbf{Q}_p)\otimes\mathbf{Q}_p/\mathbf{Z}_p).$$

Since $\mathrm{Sel}(E/\mathbf{Q}) = 0$, $\mathrm{Sel}'(E/\mathbf{Q})^\vee$ is a quotient of $\mathbf{Z}_p$. Hence, by Lemma 4.5 and Nakayama's lemma, $\mathrm{Sel}'(E/K_\infty)^\vee$ is generated by one element as a Λ-module. Since p is a supersingular prime, $\varprojlim E(k_n)\otimes\mathbf{Z}_p = 0$ ([8], [9]), and $H^1(k_\infty, E[p^\infty]) = E(k_\infty)\otimes\mathbf{Q}_p/\mathbf{Z}_p$. So we have $\mathrm{Sel}'(E/K_\infty) = \mathrm{Sel}(E/K_\infty)$. Since the Λ-rank of $\mathrm{Sel}(E/K_\infty)^\vee$ is ≥ 1, we have $\mathrm{Sel}(E/K_\infty)^\vee \simeq \Lambda$.

Next, we show the statement on $\mathrm{Sel}(E/K_n)$. By Cassels-Tate-Poitou duality, we have an exact sequence

$$\begin{aligned} H^1(O_{K_n}[1/S], T) \longrightarrow H^1(k_n, T)/(E(k_n)\otimes\mathbf{Z}_p) &\longrightarrow \mathrm{Sel}(E/K_n)^\vee \\ &\longrightarrow \mathrm{Sel}_0(E/K_n)^\vee. \end{aligned}$$

From Proposition 5.2 (1) and (3), we get the description of $\mathrm{Sel}(E/K_n)^\vee$ in Proposition 5.2 (2).

The claim $\mathrm{Sel}(E/K_\infty)^\vee \simeq \Lambda$ can be also obtained by taking the limit of the above description of $\mathrm{Sel}(E/K_n)^\vee$ because $\varprojlim E(k_n) \otimes \mathbf{Z}_p = 0$ and $\mathbf{H}^1(k_\infty, T)$ is a free Λ-module of rank 2 and (z_n) can be taken as a part of a basis.

6 Iwasawa Main Conjecture

In this section, we give some remarks on the Iwasawa Main Conjecture of an elliptic curve for cyclotomic $\mathbf{Z}_p$-extensions. We note that Iwasawa theory for an elliptic curve with supersingular reduction at p was studied by Perrin-Riou intensively [21], [22].

Let E be an elliptic curve defined over $\mathbf{Q}$. We assume that p is a prime number such that E has good reduction at p, and for simplicity assume that the Galois action $\rho_{E[p]} : G_{\mathbf{Q}} \longrightarrow GL_2(\mathbf{F}_p)$ on the p-torsion points $E[p]$ is surjective, and consider the cyclotomic $\mathbf{Z}_p$-extension $K_\infty/\mathbf{Q}$. Let K_n be the n-th layer, and $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/\mathbf{Q})]]$ as in the previous section. We consider the zeta elements $(z_n) \in \mathbf{H}^1(O_{K_\infty}[1/S], T) = \varprojlim H^1(O_{K_n}[1/S], T)$ of Kato in Theorem 5.1. We also consider the subgroup $\mathrm{Sel}_0(E/K_\infty)$ of the Selmer group in Definition 4.1. Its Pontrjagin dual $\mathrm{Sel}_0(E/K_\infty)^\vee$ is a torsion Λ-module by a result in [14] (cf. the discussion after Conjecture 6.1). Then, Iwasawa Main Conjecture can be written in the following simple form.

Conjecture 6.1 (Iwasawa Main Conjecture)

$$\mathrm{char}(\mathrm{Sel}_0(E/K_\infty)^\vee) = \mathrm{char}(\mathbf{H}^1(O_{K_\infty}[1/S], T)/ < (z_n) >).$$

Here, $\mathrm{char}(M)$ means the characteristic ideal of a torsion Λ-module M.

This formulation of Iwasawa Main Conjecture is an analogy of the formulation of the classical Iwasawa Main Conjecture which uses the cyclotomic units and the plus part of the ideal class groups.

This conjecture is equivalent to the usual Iwasawa Main Conjecture of Mazur [17] if E has good ordinary reduction. This conjecture is also equivalent to Conjecture 12.10 in Kato [14] and Perrin-Riou 3.4.2 in [22]. In [14], instead of $\mathrm{Sel}_0(E/K_\infty)$, $\mathbf{H}^2(j_*T) = \varprojlim H^2(\mathrm{Spec}\, O_{K_n}[1/p], j_*T)$ (where j is the natural inclusion $\mathrm{Spec}\, O_{K_n}[1/S] \xrightarrow{j} \mathrm{Spec}\, O_{K_n}[1/p]$) is used, but we have

$$\mathrm{char}(\mathbf{H}^2(j_*T)) = \mathrm{char}(\mathrm{Sel}_0(E/K_\infty)^\vee).$$

We will see this. Put $S' = S \setminus \{p\}$, and denote by S'_n (resp. S'_∞) the primes of K_n (resp. K_∞) lying over S'. From the localization sequence, we

have an exact sequence

$$\bigoplus_{v\in S'_n} H^0(\kappa(v), H^1((K_{n,v})_{nr}, T)) \longrightarrow H^2(O_{K_n}[1/p], j_*T)$$
$$\longrightarrow H^2(O_{K_n}[1/S], T) \longrightarrow \bigoplus_{v\in S'_n} H^2(K_{n,v}, T)$$

where $\kappa(v)$ is the residue field of v, and $(K_{n,v})_{nr}$ is the maximal unramified extension of $K_{n,v}$. Since $\varprojlim_n \bigoplus_{v\in S'_n} H^0(\kappa(v), H^1((K_{n,v})_{nr}, T)) = 0$, taking the projective limits, we have an exact sequence

$$0 \longrightarrow \mathbf{H}^2(j_*T) \longrightarrow \mathbf{H}^2(O_{K_\infty}[1/S], T) \longrightarrow \bigoplus_{v\in S'_\infty} \mathbf{H}^2(K_{n,v}, T).$$

On the other hand, taking the projective limits of the exact sequence on $\mathrm{Sel}_0(E/F)$ in the proof of Lemma 4.3, we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}_0(E/K_\infty)^\vee \longrightarrow \mathbf{H}^2(O_{K_\infty}[1/S], T) \longrightarrow \bigoplus_{v\in S_\infty} \mathbf{H}^2(K_{\infty,v}, T).$$

Kato proved that $\mathbf{H}^2(O_{K_\infty}[1/S], T)$ is a torsion Λ-module [14], so $\mathrm{Sel}_0(E/K_\infty)^\vee$ is also Λ-torsion as we stated before Conjecture 6.1. Let $k_\infty/\mathbf{Q}_p$ be the cyclotomic $\mathbf{Z}_p$-extension. Since p is a good reduction prime, there are only finite p-power torsion points in $E(k_\infty)$, so by Tate duality, $\mathbf{H}^2(k_\infty, T)$ is finite. Therefore, comparing two exact sequences, we have $\mathrm{char}(\mathbf{H}^2(j_*T)) = \mathrm{char}(\mathrm{Sel}_0(E/K_\infty)^\vee)$.

The following is an immediate consequence of Proposition 5.2.

Proposition 6.2 *Let E be an elliptic curve over $\mathbf{Q}$, and p be an odd prime number at which E has supersingular reduction. We assume that $\mathrm{ord}_p(L(E,1)/\Omega_E) = \mathrm{ord}_p \mathrm{Tam}(E) = 0$, and that the Galois action $\rho_{E[p]} : G_\mathbf{Q} \longrightarrow GL_2(\mathbf{F}_p)$ is surjective. Then, Conjecture 6.1 holds in the form $(1) = (1)$.*

Thus, we have a lot of examples (E, p) for which Iwasawa Main Conjecture is true even in the case that p is a supersingular prime for E.

7 Proof of Theorem 0.1

In this section, we will prove Theorem 0.1. We put

$$r_n = \begin{cases} 0 & \text{for } n = 0, 1 \\ p^{n-1} + p^{n-3} + \ldots + p - \frac{n}{2} & \text{for any even } n \geq 2 \\ p^{n-1} + p^{n-3} + \ldots + p^2 - \frac{n-1}{2} & \text{for any odd } n \geq 3. \end{cases}$$

Note that for $n \geq 2$ we have $r_n = \Sigma_{i=2}^n q_i$ where q_i is the number defined in Proposition 1.2.

We put $G_n = \mathrm{Gal}(K_n/\mathbf{Q})$ and $\Lambda_n = \mathbf{Z}_p[G_n]$.

Lemma 7.1 (1) $\#\Lambda_n/(\theta_{K_n}, \nu_{n-1,n}(\theta_{K_{n-1}})) \leq p^{r_n}$.
(2) $\mathrm{Sel}(E/K_n)^\vee$ *is killed by* θ_{K_n}.
(3) *There is a surjective homomorphism* $\Lambda_n/(\theta_{K_n}, \nu_{n-1,n}(\theta_{K_{n-1}})) \longrightarrow \mathrm{Sel}(E/K_n)^\vee$.
(4) $\#\mathrm{Sel}(E/K_n) \geq p^{r_n}$.

It is easy to see that this lemma implies Theorem 0.1. In fact, Lemma 7.1 (1), (3) and (4) imply that

$$p^{r_n} \geq \#\Lambda_n/(\theta_{K_n}, \nu_{n-1,n}(\theta_{K_{n-1}})) \geq \#\mathrm{Sel}(E/K_n) \geq p^{r_n}.$$

Thus we obtain Theorem 0.1 (3) and (4). In particular, $\mathrm{Sel}(E/K_n)$ is finite and we get Theorem 0.1 (2). Theorem 0.1 (1) follows from Theorem 0.1 (2) and Proposition 5.2 (2).

Proof of Lemma 7.1. We first show Lemma 7.1 (1). As we saw in the proof of Proposition 1.2, θ_{K_1} and θ_{K_0} are units, so the claim is clear for $n = 0$ and 1. Suppose that $n \geq 2$. Let ψ_n be a character of G_n of order p^n. We define $O_{\psi_n} = \mathbf{Z}_p[\mu_{p^n}]$, and extend ψ_n to Λ_n by linearity

$$\psi_n : \Lambda_n \longrightarrow O_{\psi_n}.$$

Put $I_n = (\theta_{K_n}, \nu_{n-1,n}(\theta_{K_{n-1}}))$. Then ψ_n induces $\psi_n : \Lambda_n/I_n \longrightarrow O_{\psi_n}/(\psi_n(\theta_{K_n}))$. By Lemma 1.1, $\nu_{n-1,n}$ induces $\nu_{n-1,n} : \Lambda_{n-1}/I_{n-1} \longrightarrow \Lambda_n/I_n$, and we have an exact sequence

$$\Lambda_{n-1}/I_{n-1} \xrightarrow{\nu_{n-1,n}} \Lambda_n/I_n \xrightarrow{\psi_n} O_{\psi_n}/(\psi_n(\theta_{K_n})).$$

By Proposition 1.2 and induction on n, we get

$$\#(\Lambda_n/I_n) \leq \#(\Lambda_{n-1}/I_{n-1})\#(O_{\psi_n}/(\psi_n(\theta_{K_n}))) \leq p^{r_{n-1}+q_n} = p^{r_n}.$$

This completes the proof of Lemma 7.1 (1).

Next, we proceed to the proof of Lemma 7.1 (2). We use the same notation as before. Let k_n be the n-th layer of the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}_p$, and for $x \in D$ and $z \in H^1(k_n, T)$, define $\mathcal{P}_n(x, z)$ by

$$\mathcal{P}_n(x, z) = \frac{1}{p-1}\pi P_{n+1}(x, i(z)) \in \mathbf{Q}_p[G_n]$$

where $P_{n+1}(*, *)$ is the pairing in §3, and $i : H^1(k_n, T) \longrightarrow H^1(\mathbf{Q}_p(\mu_{p^{n+1}}), T)$ is the natural map, and $\pi : \mathbf{Q}_p[\mathcal{G}_{n+1}] = \mathbf{Q}_p[\mathrm{Gal}(\mathbf{Q}_p(\mu_{p^{n+1}})/\mathbf{Q}_p)] \longrightarrow \mathbf{Q}_p[\mathrm{Gal}(k_n/\mathbf{Q}_p)] = \mathbf{Q}_p[G_n]$ is the natural projection. Let $z_n \in H^1(O_{K_n}[1/S], T)$ be the zeta element in Theorem 5.1.

Lemma 7.2

$$\theta_{K_n} = \frac{1}{2[\varphi(\omega), \omega]} p^{n+1} \mathcal{P}_n\big(\varphi^{n+2}(\omega), z_n\big),$$
$$\nu_{n-1,n}(\theta_{K_{n-1}}) = \frac{1}{2[\varphi(\omega), \omega]} p^{n+1} \mathcal{P}_n\big(\varphi^{n+1}(\omega), z_n\big).$$

Proof. As in 2.2.1, we define $(c_m)_{m\geq 0}$ by $c_0 = 0$, $c_1 = 1$, and $c_m = p^{-1}a_p c_{m-1} - p^{-1}c_{m-2}$. Since $\varphi^2 - p^{-1}a_p\varphi + p^{-1} = 0$, as in the proof of Proposion 2.2, we have

$$\varphi^m(\omega) = -\frac{1}{p}c_{m-1}\omega + c_m\varphi(\omega)$$

for any $m \geq 1$.

For i such that $1 \leq i \leq n$, let ψ_i be a character of G_n whose order is p^i. Hence, the conductor of ψ_i is p^{i+1}. By Lemma 3.4 and Theorem 5.1, we have

$$\begin{aligned}\psi_i(\mathcal{P}_n(\varphi^{n+2}(\omega), z_n)) &= \frac{1}{p^{i+1}}\tau(\psi_i)\sum_{\sigma\in G_n}\psi_i^{-1}(\sigma)[\varphi^{n-i+1}(\omega), \exp^*(\sigma(z_n))] \\ &= \frac{1}{p^{i+1}}[\varphi^{n-i+1}(\omega), \omega]\tau(\psi_i)L\big(E, \psi_i^{-1}, 1\big)/\Omega_E.\end{aligned}$$

Hence, using the above formula on $\varphi^{n-i+1}(\omega)$, we have

$$\psi_i(\mathcal{P}_n(\varphi^{n+2}(\omega), z_n)) = \frac{1}{p^{i+1}}c_{n-i+1}[\varphi(\omega), \omega]\tau(\psi_i)L\big(E, \psi_i^{-1}, 1\big)/\Omega_E.$$

On the other hand, from the distribution relation $\pi_{m,m-1}(\theta_{K_m}) = a_p\theta_{K_{m-1}} - \nu_{m-2,m-1}(\theta_{K_{m-2}})$ $(m \geq 2)$, by induction on $n - i$ we have

$$\pi_{n,i}(\theta_{K_n}) = p^{n-i}c_{n-i+1}\theta_{K_i} - p^{n-i-1}c_{n-i}\nu_{i-1,i}(\theta_{K_{i-1}})$$

for any i such that $1 \leq i \leq n$. Hence, by the formula $\psi_i(\theta_{K_i}) = \tau(\psi_i)L\big(E, \psi_i^{-1}, 1\big)/2\Omega_E$ of Mazur and Tate [19] (1.4), we have

$$\psi_i(\theta_{K_n}) = \psi_i(\pi_{n,i}(\theta_{K_n})) = p^{n-i}c_{n-i+1}\tau(\psi_i)L\big(E, \psi_i^{-1}, 1\big)/2\Omega_E.$$

It follows that

$$\psi_i(\theta_{K_n}) = \psi_i\left(\frac{1}{2[\varphi(\omega), \omega]}p^{n+1}\mathcal{P}_n(\varphi^{n+2}(\omega), z_n)\right).$$

Next we consider the trivial character $\mathbf{1}$ of G_n. By Lemma 3.5 and Theorem 5.1 and the computation

$$\begin{aligned}
&(1-\varphi)^{-1}(1-\varphi^{-1}/p)\varphi^{n+2}(\omega)\\
&=(1-\varphi)^{-1}(1-\varphi^{-1}/p)\varphi^2\left(-\frac{1}{p}c_{n-1}\omega+c_n\varphi(\omega)\right)\\
&\equiv\left(1-\frac{a_p}{p}+\frac{1}{p}\right)^{-1}\left(\frac{(a_p-1)^2-p}{p^2}c_n-\frac{a_p-2}{p^2}c_{n-1}\right)\varphi(\omega)\mod D^0,
\end{aligned}$$

we have

$$\begin{aligned}
&\mathbf{1}\big(\mathcal{P}_n\big(\varphi^{n+2}(\omega),z_n\big)\big)=\\
&\left(\frac{(a_p-1)^2-p}{p^2}c_n-\frac{a_p-2}{p^2}c_{n-1}\right)[\varphi(\omega),\omega]L(E,1)/\Omega_E.
\end{aligned}$$

On the other hand, let $\theta_1=L(E,1)/2\Omega_E$. Then, as we saw in the proof of Proposition 1.2, we have $\theta_{K_0}=(a_p-2)\theta_1$ and $\pi_{1,0}(\theta_{K_1})=((a_p-1)^2-p)\theta_1$. Hence, we have

$$\begin{aligned}
\pi_{n,0}(\theta_{K_n})&=\pi_{1,0}(\pi_{n,1}(\theta_{K_n}))=\pi_{1,0}\big(p^{n-1}c_n\theta_{K_1}-p^{n-2}c_{n-1}\nu_{0,1}(\theta_{K_0})\big)\\
&=p^{n-1}(((a_p-1)^2-p)c_n-(a_p-2)c_{n-1})\theta_1.
\end{aligned}$$

It follows that

$$\mathbf{1}(\theta_{K_n})=\mathbf{1}\left(\frac{1}{2[\varphi(\omega),\omega]}p^{n+1}\mathcal{P}_n(\varphi^{n+2}(\omega),z_n)\right).$$

Therefore, for any character of G_n, the image of θ_{K_n} coincides with the image of $(2[\varphi(\omega),\omega])^{-1}p^{n+1}\mathcal{P}_n(\varphi^{n+2}(\omega),z_n)$. This implies that

$$\theta_{K_n}=\frac{1}{2[\varphi(\omega),\omega]}p^{n+1}\mathcal{P}_n\big(\varphi^{n+2}(\omega),z_n\big).$$

The equation for $\nu_{n-1,n}(\theta_{K_{n-1}})$ can be proved by the same method. In fact, we have

$$\begin{aligned}
\psi_i(\nu_{n-1,n}(\theta_{K_{n-1}}))&=\psi_i\left(\frac{1}{2[\varphi(\omega),\omega]}p^{n+1}\mathcal{P}_n(\varphi^{n+1}(\omega),z_n)\right)\\
&=p^{n-i}c_{n-i}\tau(\psi_i)L\big(E,\psi_i^{-1},1\big)/2\Omega_E,
\end{aligned}$$

and

$$\begin{aligned}
\mathbf{1}(\nu_{n-1,n}(\theta_{K_{n-1}}))&=\mathbf{1}\left(\frac{1}{2[\varphi(\omega),\omega]}p^{n+1}\mathcal{P}_n(\varphi^{n+1}(\omega),z_n)\right)\\
&=p^{n-1}(((a_p-1)^2-p)c_{n-1}\\
&\quad-(a_p-2)c_{n-2})L(E,1)/2\Omega_E.
\end{aligned}$$

This completes the proof of Lemma 7.2.

We go back to the proof of Lemma 7.1 (2). By the computation in the proof of Lemma 7.2 and $L(E, \psi_i^{-1}, 1) \neq 0$ (Proposition 1.2) for any i with $0 \leq i \leq n$ (where we defined $\psi_0 = \mathbf{1}$), it is easy to see that there are infinitely many $a \in \mathbf{Z}_p$ such that $\psi_i(\mathcal{P}_n(\varphi^{n+2}(\omega) + a\varphi^{n+1}(\omega), z_n)) \neq 0$ for any i with $0 \leq i \leq n$ (note that there is no i such that $c_i = c_{i+1} = 0$). Take such a and put $x = \varphi^{n+2}(\omega) + a\varphi^{n+1}(\omega)$. For $z \in H^1(k_n, T)$, it follows from Proposition 3.6 that $[\varphi(\omega), \omega]^{-1} p^{n+1} \mathcal{P}_n(x, z)$ is in $\mathbf{Z}_p[G_n]$. We define a map

$$\Psi_x : H^1(k_n, T) \longrightarrow \Lambda_n = \mathbf{Z}_p[G_n]$$

by $z \mapsto (2[\varphi(\omega), \omega])^{-1} p^{n+1} \mathcal{P}_n(x, z)$.

Put $V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. In the following, we use the notation $H^1_f(k_n, V) = E(k_n) \otimes \mathbf{Q}_p$ and $H^1_f(k_n, T) = E(k_n) \otimes \mathbf{Z}_p$ in [2]. We write

$$A_n = H^1(k_n, T)/(H^1_f(k_n, T) + < z_n >)$$

where $< z_n >$ is the sub Λ_n-module generated by z_n. By Proposition 5.2 (2), A_n is isomorphic to $\mathrm{Sel}(E/K_n)^\vee$. Hence, it is sufficient to show $\theta_{K_n} A_n = 0$.

Since $\psi_i(\Psi_x(z_n)) \neq 0$ for any i, the extension of Ψ_x to $H^1(k_n, V) = H^1(k_n, T) \otimes \mathbf{Q}_p$ induces a bijective homomorphism

$$\begin{aligned} &\Psi_x \otimes \mathbf{Q}_p : H^1(k_n, V)/H^1_f(k_n, V) \\ &\xrightarrow{\simeq} \mathbf{Q}_p[G_n] \simeq \mathbf{Q}_p \oplus \mathbf{Q}_p(\mu_p) \oplus \ldots \oplus \mathbf{Q}_p(\mu_{p^n}). \end{aligned}$$

Since the natural map

$$H^1(k_n, T)/H^1_f(k_n, T) \hookrightarrow H^1(k_n, V)/H^1_f(k_n, V)$$

is injective, Ψ_x induces an injective homomorphism

$$\Psi_x : H^1(k_n, T)/H^1_f(k_n, T) \hookrightarrow \Lambda_n = \mathbf{Z}_p[G_n].$$

Hence, we have

$$A_n \xrightarrow{\simeq} \mathrm{Image}(\Psi_x)/ < \Psi_x(z_n) >$$

where $< \Psi_x(z_n) >$ is the sub Λ_n-module of Λ_n generated by $\Psi_x(z_n)$. In particular, $\Psi_x(z_n)$ kills A_n. By Lemma 7.2, we know $\Psi_x(z_n) = \theta_{K_n} + a\nu_{n-1,n}(\theta_{K_{n-1}})$, so A_n is killed by this element.

By induction on n, we have $\theta_{K_{n-1}} A_{n-1} = 0$. This implies that the composition $A_n \xrightarrow{\mathrm{Cor}} A_{n-1} \xrightarrow{\theta_{K_{n-1}}} A_{n-1} \xrightarrow{\mathrm{Res}} A_n$ is zero, but this composition coincides with $z \mapsto \nu_{n-1,n}(\theta_{K_{n-1}})z$, hence $\nu_{n-1,n}(\theta_{K_{n-1}})A_n = 0$. It follows that $\theta_{K_n} A_n = 0$. This completes the proof of Lemma 7.1 (2).

Next, we prove Lemma 7.1 (3). Lemma 7.1 (2) says that $\theta_{K_n}\,\mathrm{Sel}(E/K_n)^\vee = 0$. As we saw above, $\nu_{n-1,n}(\theta_{K_{n-1}})$ also kills $\mathrm{Sel}(E/K_n)^\vee$. On the other hand, since the natural map $\mathrm{Sel}(E/K_n) \longrightarrow \mathrm{Sel}(E/K_\infty)$ is injective, it follows from Proposition 5.2 (2) that $\mathrm{Sel}(E/K_n)^\vee$ is generated by one element as a Λ_n-module. Thus, we get Lemma 7.1 (3).

We proceed to the proof of Lemma 7.1 (4). In our original proof we used the properties of zeta elements heavily, but here we give a simple proof which uses only the finiteness of $\mathrm{Sel}(E/K_{n-1})$ by a suggestion of Greenberg. We thank Greenberg very much for his suggestion. Put $G = \mathrm{Gal}(K_n/K_{n-1})$. Let S be as in §5, and S_n (resp. S_{n-1}) be the set of primes of K_n (resp. K_{n-1}) lying over S. For a local field k we set $h(k) = H^1(k, E[p^\infty])/(E(k)\otimes \mathbf{Q}_p/\mathbf{Z}_p)$. By the definition of the Selmer group, we have a commutative diagram of exact sequences

$$\begin{array}{ccccccc} 0 \to \mathrm{Sel}(E/K_{n-1}) & \to & H^1\big(O_{K_{n-1}}[1/S], E[p^\infty]\big) & \xrightarrow{a} & \prod_{v\in S_{n-1}} h((K_{n-1})_v) \\ \downarrow b_1 & & \downarrow b_2 & & \downarrow b_3 \\ 0 \to \mathrm{Sel}(E/K_n)^G & \to & H^1\big(O_{K_n}[1/S], E[p^\infty]\big)^G & \to & (\prod_{v\in S_n} h((K_n)_v))^G. \end{array}$$

Since $\mathrm{Sel}(E/K_{n-1})$ is finite, a is surjective. We know the injectivity of b_2 because there is no point of order p in $E(K_n)$. Further, b_3 is the dual of the norm map $\Pi E((K_n)_v)\otimes \mathbf{Z}_p \longrightarrow \Pi E((K_{n-1})_v)\otimes \mathbf{Z}_p$. Hence, the order of the cokernel of b_1 is greater or equal to the order of the cokernel of the norm map $N : E(k_n)\otimes \mathbf{Z}_p \longrightarrow E(k_{n-1})\otimes \mathbf{Z}_p$. By Proposition 2.1, we have $\#((E(k_{n-1})\otimes \mathbf{Z}_p)/N(E(k_n)\otimes \mathbf{Z}_p)) \geq p^{q_n}$. Hence, by induction on n we obtain

$$\#\,\mathrm{Sel}(E/K_n) \geq \#\big(\mathrm{Sel}(E/K_n)^G\big) \geq \#\,\mathrm{Sel}(E/K_{n-1})p^{q_n} \geq p^{r_{n-1}+q_n} = p^{r_n}.$$

This completes the proof of Lemma 7.1 (4).

In the proof of Lemma 7.1 (4), we showed $\#(\mathrm{Sel}(E/K_n)^G) \geq p^{r_n}$. Since $\#\,\mathrm{Sel}(E/K_n) = p^{r_n}$, this implies that

$$\mathrm{Sel}(E/K_n)^G = \mathrm{Sel}(E/K_n).$$

Hence, we obtain

Proposition 7.3 *We put $G = \mathrm{Gal}(K_n/K_{n-1})$. Then, under the assumption of Theorem 0.1, every element in the Tate Shafarevich group of E/K_n with p-power order is G-invariant. Namely,*

$$Ш(E/K_n)\{p\}^G = Ш(E/K_n)\{p\}.$$

Next, we prove the structure theorem for $Ш(E/K_n)\{p\}$ as an abelian group.

Theorem 7.4 *Under the assumption of Theorem 0.1, for $n \geq 2$ we have*

$$Ш(E/K_n)\{p\} \simeq (\mathbf{Z}/p^{n-1}\mathbf{Z})^{q_2} \oplus (\mathbf{Z}/p^{n-2}\mathbf{Z})^{q_3-q_2} \oplus (\mathbf{Z}/p^{n-3}\mathbf{Z})^{q_4-q_3} \oplus \ldots$$
$$\ldots \oplus (\mathbf{Z}/p\mathbf{Z})^{q_n-q_{n-1}}$$

where q_n is the number defined in Proposition 1.2.

Proof. Put $I_n = (\theta_{K_n}, \nu_{n-1,n}(\theta_{K_{n-1}}))$. Since $\mathrm{Sel}(E/K_n)^\vee$ is isomorphic to Λ_n/I_n by Theorem 0.1 (4), it is enough to show that Λ_n/I_n has the structure as in Theorem 7.4. We denote by ψ_n a character of G_n with order p^n, and consider an exact sequence

$$\Lambda_{n-1}/I_{n-1} \xrightarrow{\nu_{n-1,n}} \Lambda_n/I_n \xrightarrow{\psi_n} O_{\psi_n}/(\psi_n(\theta_{K_n}))$$

in the proof of Lemma 7.1 (1). Comparing the orders of these three groups, we have an exact sequence

$$0 \longrightarrow \Lambda_{n-1}/I_{n-1} \xrightarrow{\nu_{n-1,n}} \Lambda_n/I_n \xrightarrow{\psi_n} O_{\psi_n}/(\psi_n(\theta_{K_n})) \longrightarrow 0.$$

Since $(\Lambda_n/I_n) \otimes \mathbf{F}_p = \mathbf{F}_p[T]/(T^{q_n})$, the p-rank of Λ_n/I_n is q_n. Hence, it coincides with the p-rank of $O_{\psi_n}/(\psi_n(\theta_{K_n}))$. Thus, by induction on n, we obtain Theorem 7.4.

References

1. Bloch, S., A note on height pairings, Tamagawa numbers, and the Birch Swinnerton-Dyer conjecture, Invent. math. **58** (1980), 65–76
2. Bloch, S., Kato, K., L-functions and Tamagawa numbers of motives, in: The Grothendieck Festschrift Vol I, Progress in Math. Vol. 86, Birkhäuser (1990), 333–400
3. Coates, J., Sujatha, R., Galois cohomology of elliptic curves, Tata Institute of Fundamental Research Lectures on Math. 88, Narosa Publishing House, New Delhi (2000)
4. Fontaine, J.-M., Laffaille, G., Construction de représentations p-adiques, Ann. scient. Éc. Norm. Sup. 4^e série **15** (1982), 547–608
5. Greenberg, R., Iwasawa theory for elliptic curves, in: Arithmetic theory of elliptic curves, Cetraro, Italy 1997, Springer Lecture Notes in Math. **1716** (1999), 51–144
6. Greenberg, R., Iwasawa theory – Past and Present, Class field theory – Its Centenary and Prospect, Advanced Studies in Pure Math. **30**, Kinokuniya, Tokyo (2001), 335–385
7. Greenberg, R., Vatsal, V., On the Iwasawa invariants of elliptic curves, Invent. math. **142** (2000), 17–63
8. Hazewinkel, M., On Norm maps for one dimensional formal groups I: The cyclotomic Γ-extension, J. Algebra **32** (1974), 89–108
9. Hazewinkel, M., On Norm maps for one dimensional formal groups III, Duke Math. J. **44** (1977), 305–314
10. Honda, T., On the theory of commutative formal groups, J. Math. Soc. Japan **22** (1970), 213–246
11. Iwasawa, K., A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258
12. Iwasawa, K., On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc. **65** (1959), 183–226

13. Kato, K., Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}, Part I, in: Arithmetic Algebraic Geometry, Trento, 1991, Springer Lecture Notes in Math. **1553** (1993), 50–163
14. Kato, K., p-adic Hodge theory and values of zeta functions of modular forms, preprint
15. Kolyvagin, V.A., Euler systems, in: The Grothendieck Festschrift Vol II, Progress in Math. **87** (1990), 435–483
16. Kurihara, M., Iwasawa theory and Fitting ideals, preprint
17. Mazur, B., Rational points of abelian varieties with values in towers of number fields, Invent. math. **18** (1972), 183–266
18. Mazur, B., Rational isogenies of prime degree, Invent. math. **44** (1978), 129–162
19. Mazur, B., Tate, J., Refined conjectures of the "Birch and Swinnerton-Dyer type", Duke Math. J. **54** (1987), 711–750
20. Milne, J. S, Arithmetic duality theorems, Perspectives in Math. 1, Academic Press (1986)
21. Perrin-Riou, B., Théorie d'Iwasawa p-adique locale et globale, Invent. math. **99** (1990), 247–292
22. Perrin-Riou, B., Fonctions L p-adiques d'une courbe elliptique et points rationnels, Ann. Inst. Fourier **43**, 4 (1993), 945–995
23. Perrin-Riou, B., Théorie d'Iwasawa des représentations p-adiques sur un corps local, Invent. math. **115** (1994), 81–149
24. Rubin, K., On the main conjecture of Iwasawa theory for imaginary quadratic fields, Invent. math. **93** (1988), 701–713
25. Rubin, K., Euler systems and modular elliptic curves, in: Galois representations in Arithmetic Algebraic Geometry, London Math. Soc., Lecture Note Series **254** (1998), 351–367
26. Stevens, G., Stickelberger elements and modular parametrizations of elliptic curves, Invent. math. **98** (1989), 75–106

Note added in proof.

After this paper was written, important progress was made on this subject by R. Pollack "On the p-adic L-function of a modular form at a supersingular prime" and by B. Perrin-Riou "Arithmétique des courbes elliptiques à réduction supersingulière en p" (preprints).