KATO'S EULER SYSTEM AND THE MAZUR-TATE REFINED CONJECTURE OF BSD TYPE

KAZUTO OTA

ABSTRACT. Mazur and Tate proposed a conjecture which compares the Mordell-Weil rank of an elliptic curve over $\mathbb{Q}$ with the order of vanishing of Mazur-Tate elements, which are analogues of Stickelberger elements. Under some relatively mild assumptions, we prove this conjecture. Our strategy of the proof is to study divisibility of certain derivatives of Kato's Euler system.

CONTENTS

1. INTRODUCTION

1.1. **The Mazur-Tate refined conjecture of BSD type.** Mazur-Tate [20] proposed a *refined conjecture of BSD type*, which predicts mysterious relations between arithmetic invariants of an elliptic curve E over $\mathbb{Q}$ and Mazur-Tate elements constructed from modular symbols. Mazur-Tate elements are analogues of Stickelberger elements and refine the p-adic L-function of E. As the Birch and Swinnerton-Dyer conjecture does, the Mazur-Tate refined conjecture of BSD type consists of two parts. One compares the Mordell-Weil rank with the "order of vanishing" of Mazur-Tate elements (the rank-part). The other describes the "leading coefficients" of the elements. The aim of this paper is to prove the rank-part under some mild assumptions. Now, we explain this part more precisely (see Section 2 for the other part).

We let S be a positive integer and put $G_S = \mathrm{Gal}(\mathbb{Q}(\zeta_S)/\mathbb{Q})$, where ζ_S is a primitive S-th root of unity. The *Mazur-Tate element* θ_S is an element of $\mathbb{Q}[G_S]$ such that for every character χ of

2010 *Mathematics Subject Classification.* Primary 11G40; Secondary 11G05, 11R34.

Key words and phrases. Elliptic curves, Mazur-Tate elements, Kato's Euler systems.

Research supported in part by Grant-in-Aid for JSPS Fellow 12J04338 and KAKENHI 26247004 .

G_S, the evaluation $\chi(\theta_S)$ equals the algebraic part of $L(E, \chi^{-1}, 1)$ up to an explicit factor. It is important that the denominators of θ_S are bounded as S varies, which implies the existence of non-trivial congruences between these special values as χ varies. If E is a strong Weil curve, then $\theta_S \in \mathbb{Z}[1/tc_E][G_S]$, where $t := |E(\mathbb{Q})_{\mathrm{tors}}|$, and c_E denotes the Manin constant, which is conjectured to be 1 in this case.

Let R be a subring of $\mathbb{Q}$ such that $\theta_S \in R[G_S]$. We denote by I_S the augmentation ideal of $R[G_S]$ and by $\mathrm{sp}(S)$ the number of split multiplicative primes of E dividing S. We put $r_E = \mathrm{rank}(E(\mathbb{Q}))$. The following is the rank-part of the Mazur-Tate refined conjecture of BSD type.

CONJECTURE 1.1 (Mazur-Tate). *The order of vanishing of θ_S at the trivial character is greater than or equal to $r_E + \mathrm{sp}(S)$, that is,*

$$\theta_S \in I_S^{r_E + \mathrm{sp}(S)}.$$

1.2. **The main result.** We assume that E does *not* have complex multiplication, and we denote by N the conductor. In this paper, a prime p is called an *admissible prime* if it satisfies the following conditions:

(A1) p does *not* divide $6N|E(\mathbb{F}_p)|\prod_{\ell|N}[E(\mathbb{Q}_\ell) : E_0(\mathbb{Q}_\ell)]$, where for a prime ℓ, we denote by $E_0(\mathbb{Q}_\ell)$ the group of points of $E(\mathbb{Q}_\ell)$ with non-singular reduction,

(A2) the Galois representation $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))$ is surjective, where $T_p(E)$ is the p-adic Tate module of E,

(A3) $p \geq r_E$.

Let R be a subring of $\mathbb{Q}$ in which every prime that is *not* admissible is invertible. The following is our main result.

THEOREM 1.2 (Theorem 6.1). *Let S be a square-free product of primes $\ell \nmid N$ such that for each prime p which is not invertible in R, the module $E(\mathbb{F}_\ell)[p]$ is cyclic, that is, $E(\mathbb{F}_\ell)[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or $\{0\}$. Then $\theta_S \in R[G_S]$, and Conjecture 1.1 holds, that is,*

$$\theta_S \in I_S^{r_E}.$$

Remark 1.3. (1) At least 99.7% of primes satisfy the assumption on ℓ of Theorem 1.2 (see Remark 6.2 for the detail). We also note that every good supersingular prime ℓ of E satisfies the assumption.

(2) We mention known results on Conjecture 1.1. If an admissible prime p is a good ordinary prime of E, then Kato's result ([11]) on the p-adic BSD conjecture implies that $\theta_{p^n} \in \mathbb{Z}_p \otimes I_{p^n}^{r_E}$ for $n \geq 1$. In the case where p is supersingular, by combining results of Kobayashi [13] and Pollack [27], the same assertion is proved. Kurihara's result implies that if p is good ordinary, then $\theta_S \in \mathbb{Z}_p \otimes I_S^{r_E}$, where S is a product of good primes and is not necessarily a power of p (cf. [15, Remark 2] and [20, Proposition 3]). However, he assumes the $\mu = 0$ conjecture. Although Tan's work ([33]) also implies Conjecture

1.1 for many S without extending the scalar to $\mathbb{Z}_p$, he assumes the *full* BSD conjecture not only for E but also for every base change $E \otimes_{\mathbb{Q}} K$, where K is a cyclic extension of $\mathbb{Q}$ inside $\mathbb{Q}(\zeta_S)$. Note that Theorem 1.2 does not require the validity of any conjecture.

(3) It may happen that θ_S has an extra zero, that is, $\theta_S \in I_S^{r_E+\mathrm{sp}(S)+1}$ (cf. Remark 2.5).

(4) Since E has no CM, Serre's work ([29]) shows that all but finitely many primes satisfy (A2). By [30], the density of primes p dividing $|E(\mathbb{F}_p)|$ is zero. In particular, the density of admissible primes is equal to one. Moreover, by [18, Lemma 8.18], if $E(\mathbb{Q})$ has a non-trivial torsion point, then there are at most three primes $p \nmid N$ dividing $|E(\mathbb{F}_p)|$, and hence there are only finitely many non-admissible primes in this case.

(5) By our assumption on R, for any S we have $\theta_S \in R[G_S]$ (cf. [19, Corollary 4.1]).

By [5, Theorem 2], [29, Théorèm $4'$] and [31, Chapter IV, Corollary 9.2 (d)], as a special case of Theorem 1.2, we have the following.

COROLLARY 1.4. *We assume that $E(\mathbb{Q})$ has a non-trivial torsion point. We put*

$$d = \max\left\{ r_E,\ \frac{4\sqrt{6}}{3} N \prod_{\ell \mid N} \left(1+\frac{1}{\ell}\right)^{\frac{1}{2}} + 1 \right\},$$

$$R = \mathbb{Z}\left[1/p, 1/\mathrm{ord}_l(j(E))\ ;\ p < d \text{ is a prime}, l \text{ is a split multiplicative prime}\right],$$

where $j(E)$ is the j-invariant of E. Then, for every square-free product S of good supersingular primes, $\theta_S \in I_S^{r_E}$.

In this paper, we also give some results involving trivial zeros, or exceptional zeros. See Corollary 6.3 and Theorem 7.1 for the details.

We next give a partial evidence of the part of the Mazur-Tate refined conjecture (Conjecture 2.4) which relates arithmetic invariants to the *leading coefficient* of θ_S defined as the image $\tilde{\theta}_S$ of θ_S in $I_S^{r_E}/I_S^{r_E+1}$ (if $\theta_S \in I_S^{r_E}$). The following is a special case of Theorem 6.4.

THEOREM 1.5. *Let p be a prime not invertible in R, and let S be an integer as in Theorem 1.2 such that $\ell \equiv 1 \bmod p$ for every prime $\ell | S$. If $\tilde{\theta}_S \not\equiv 0 \bmod p (I_S^{r_E}/I_S^{r_E+1})$, then*

$$Ш[p] = 0 \quad \textit{and} \quad p \nmid J_S,$$

where Ш denotes the Tate-Shafarevich group, and J_S is the order of the cokernel of the natural map $E(\mathbb{Q}) \to \left(\oplus_{\ell|S} E(\mathbb{F}_\ell)\right) \oplus \left(\oplus_{\ell|N} E(\mathbb{Q}_\ell)/E_0(\mathbb{Q}_\ell)\right)$.

1.3. **The plan of proof.** We briefly explain how to prove Theorem 1.2. By a group ring theoretic argument (Lemma 5.1), it suffices to prove that for each prime p not invertible in R,

$$\theta_S \in \mathbb{Z}_p \otimes_{\mathbb{Z}} I_S^{r_E}. \tag{1.1}$$

Our strategy of the proof of (1.1) is to show that *Darmon-Kolyvagin derivatives* of Kato's Euler system are divisible by powers of p. In order to investigate the divisibility, we modify an argument of Darmon [6], who proposed a refined conjecture for Heegner points and proved an analogue of Conjecture 1.1 in many cases. Next, by modifying ideas of Kurihara [14], Kobayashi

[13] and Otsuki [25], we relate Kato's Euler system with Mazur-Tate elements. Then, the derivatives of Kato's Euler system appear in the coefficients of the *Taylor expansion* of θ_S. By a group-ring theoretic argument, the divisibility of derivatives implies that θ_S lies in a power of the augmentation ideal. However, our modification of Darmon's argument implies only that

$$\theta_S \in \mathbb{Z}_p \otimes I_S^{\min\{r_{p^\infty}-1,p\}}, \tag{1.2}$$

where r_{p^∞} denotes the $\mathbb{Z}_p$-corank of the (discrete) Selmer group $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$. One might expect that Darmon's argument implies that $\theta_S \in \mathbb{Z}_p \otimes I_S^{\min\{r_{p^\infty},p\}}$. The obstruction is the difference between the local condition at p of Heegner points and that of Kato's Euler system. The localization of a Heegner point at p obviously comes from local rational points (i.e. it is crystalline at p), and then Heegner points are related to the usual Selmer group. However, the localization of Kato's Euler system is not necessarily crystalline at p, and then we can relate Kato's Euler system only with the strict Selmer group $H^1_{f,p}(\mathbb{Q}, E[p^\infty])$, whose local condition at p is zero. Since the corank of $H^1_{f,p}(\mathbb{Q}, E[p^\infty])$ is not necessarily greater than $r_{p^\infty}-1$, we have only (1.2).

Our idea for deducing (1.1) from (1.2) is to apply the p-parity conjecture, which is now a theorem (by [8], [12], [23], [24]). It asserts that $r_{p^\infty} \equiv \mathrm{ord}_{s=1}(L(E,s)) \bmod 2$. On the other hand, the functional equation of θ_S implies that if $\theta_S \in (\mathbb{Z}_p \otimes I_S^b) \setminus (\mathbb{Z}_p \otimes I_S^{b+1})$ for some $b > 0$, then $b \equiv \mathrm{ord}_{s=1} L(E,s) \bmod 2$. Combining these congruences with (1.2), we deduce (1.1).

Notation. Throughout this paper, let E be an elliptic curve over $\mathbb{Q}$ of conductor N without complex multiplication. We put $r_E = \mathrm{rank}(E(\mathbb{Q}))$ and $m_\ell = [E(\mathbb{Q}_\ell) : E_0(\mathbb{Q}_\ell)]$.

For an abelian group M and an integer n, we write $M/n = M/nM$ and denote by $M[n]$ the subgroup of n-torsion elements of M. We denote by M_{tors} the maximal torsion subgroup of M.

For a field K, we denote by G_K the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$, where $\overline{K}$ is a separable closure of K. We fix embeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ for every prime p. For a positive integer S, we put $\zeta_S = \exp(2\pi i/S)$ and $G_S = \mathrm{Gal}(\mathbb{Q}(\zeta_S)/\mathbb{Q})$.

Acknowledgements. This paper is based on the author's thesis. He would like to express his sincere gratitude to his advisor Professor Shinichi Kobayashi for his insightful advice and discussion. Part of this work was completed while the author was visiting l'Institute de Mathémetiques de Jussieu with a support by the JSPS Strategic Young Researcher Overseas Visits Program for Accelerating Brain Circulation. He is deeply grateful to Professor Jan Nekovář for his hospitality. Thanks are due to Professor Masato Kurihara for informing the author of work in [15]. The author is grateful to Professor Robert Pollack for answering a question on his joint work with Emerton and Weston which is unpublished. The author would like to thank Professors Henri Darmon, Tadashi Ochiai and Takuya Yamauchi for helpful comments. He would also like to thank Matteo Longo for discussion and Chan-Ho Kim for showing his note of talks by Pollack. Finally, he thanks the referee for useful suggestion.

2. MAZUR-TATE ELEMENTS

In this section, we recall the definition of Mazur-Tate elements, and we briefly review the Mazur-Tate refined conjecture of BSD type.

We fix a global minimal Weierstrass model of E over $\mathbb{Z}$ and denote by ω the Néron differential. Then, we have a natural homomorphism from the first homology group $H_1(E(\mathbb{C}),\mathbb{Z})$ to $\mathbb{C}$

$$H_1(E(\mathbb{C}),\mathbb{Z}) \to \mathbb{C}, \quad \gamma \mapsto \int_\gamma \omega.$$

Let Λ be the image of this map, and let $\Omega^+, -i\Omega^- > 0$ be the largest real numbers such that

$$\Lambda \subseteq \mathbb{Z}\Omega^+ \oplus \mathbb{Z}\Omega^-.$$

By [35], [34] and [4], let $f(z) = \sum_{n\geq 1} a_n \exp(2\pi i n z)$ be the newform corresponding to E. Let $L(E,s) = \sum_{n\geq 1} a_n n^{-s}$ be the Hasse-Weil L-function of E. For a Dirichlet character χ, we put $L(E,\chi,s) = \sum_{n\geq 1}\chi(n)a_n n^{-s}$. For integers a and S with $S>0$, we define $[a/S]_E^{\pm} \in \mathbb{R}$ by

$$2\pi \int_0^\infty f\left(\frac{a}{S}+it\right)dt = \left[\frac{a}{S}\right]_E^+ \Omega^+ + \left[\frac{a}{S}\right]_E^- \Omega^-.$$

The Manin-Drinfeld theorem ([9], [17]) implies that $[a/S]_E^{\pm} \in \mathbb{Q}$. In the terminology of [21],

$$\lambda(f,1;-a,S) = \left[\frac{a}{S}\right]_E^+ \Omega^+ + \left[\frac{a}{S}\right]_E^- \Omega^-. \tag{2.1}$$

Definition 2.1. For a positive integer S, we define an element θ_S of $\mathbb{Q}[G_S]$ by

$$\theta_S = \sum_{a\in(\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a}{S}\right]_E^+ + \left[\frac{a}{S}\right]_E^-\right)\delta_a \in \mathbb{Q}[G_S],$$

where $\delta_a \in G_S$ is the element satisfying $\delta_a\zeta_S = \zeta_S^a$. We call θ_S the *Mazur-Tate element*.

Remark 2.2. Our θ_S slightly differs from the original Mazur-Tate element, which is called the *modular element* in [20]. The image of $\frac{1}{2}\theta_S$ in $\mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\zeta_S)^+/\mathbb{Q})]$ coincides with the modular element, where $\mathbb{Q}(\zeta_S)^+$ is the maximal totally real subfield of $\mathbb{Q}(\zeta_S)$.

For $n|m$, we denote by $\pi_{m/n}$ the map $\mathbb{Q}[G_m] \to \mathbb{Q}[G_n]$ induced by the natural surjection $G_m \to G_n$. For a character χ of G_S, we put

$$\tau_S(\chi) = \sum_{\gamma\in G_S}\chi(\gamma)\zeta_S^\gamma.$$

By (2.1) and [21, Chapter 1, §4 and §8], we have the following.

PROPOSITION 2.3. (1) *Let S be a positive integer and ℓ a prime not dividing S. Then,*

$$\pi_{S\ell/S}\theta_{S\ell} = -\mathrm{Fr}_\ell(1 - a_\ell \mathrm{Fr}_\ell^{-1} + \epsilon(\ell)\mathrm{Fr}_\ell^{-2})\theta_S,$$

where ϵ is the trivial Dirichlet character modulo N, and $\mathrm{Fr}_\ell \in G_S$ denotes the arithmetic Frobenius of ℓ.

(2) *For a character χ of G_S with conductor S, we have*

$$\chi(\theta_S) = \tau_S(\chi)\frac{L(E,\chi^{-1},1)}{\Omega^{\pm}},$$

where $\pm = \chi(-1)$.

We briefly review the Mazur-Tate refined conjecture of BSD type. Let S be a square-free positive integer and R a subring of $\mathbb{Q}$ such that $|E(\mathbb{Q})_{\mathrm{tors}}| \in R^\times$ and $\theta_S \in R[G_S]$. We put $G_{S^+} = \mathrm{Gal}(\mathbb{Q}(\zeta_S)^+/\mathbb{Q})$ and denote by I_{S^+} the augmentation ideal of $R[G_{S^+}]$. For positive integer T, we denote by $\nu(T)$ the number of primes dividing T. For simplicity, we assume that S is relatively prime to N. For each positive divisor T of S, we denote by J_T the order of the cokernel of the natural map

$$E(\mathbb{Q}) \to \left(\oplus_{\ell|T} E(\mathbb{F}_\ell)\right) \oplus \left(\oplus_{\ell|N} E(\mathbb{Q}_\ell)/E_0(\mathbb{Q}_\ell)\right).$$

The following conjecture is what we call the Mazur-Tate refined conjecture of BSD type.

CONJECTURE 2.4 (Mazur-Tate). (1) *The Mazur-Tate element θ_S lies in $I_S^{r_E}$.*

(2) *The Tate-Shafarevich group $Ш$ of E over $\mathbb{Q}$ is finite, and if we denote by $\tilde{\theta}_S$ the image of $\frac{1}{2}\theta_S$ in $I_{S^+}^{r_E}/I_{S^+}^{r_E+1}$, then*

$$\tilde{\theta}_S = |Ш| \cdot \sum_{T|S>0} (-1)^{\nu(T)} J_T \cdot \eta_{r_E}\left(\mu_{S,T}(d_T)\right) \in I_{S^+}^{r_E}/I_{S^+}^{r_E+1},$$

where $d_T \in R \otimes_{\mathbb{Z}} \mathrm{Sym}_{\mathbb{Z}}^{r_E}(G_{T^+})$ is the discriminant ([20, (2.5.5)]) *defined by using an analogue of the Néron-Tate height pairing, $\mu_{S,T} : G_{T^+} \to G_{S^+}$ is a natural map* ([20, (2.6.1)])*, and $\eta_{r_E} : R \otimes_{\mathbb{Z}} \mathrm{Sym}_{\mathbb{Z}}^{r_E}(G_{S^+}) \to I_{S^+}^{r_E}/I_{S^+}^{r_E+1}$ is induced by the natural homomorphism $G_{S^+} \to I_{S^+}/I_{S^+}^2,\ \sigma \mapsto \sigma - 1$.*

Remark 2.5. (1) It may happen that $\theta_S \in I_S^{r_E+1}$. We give some cases where it happens.

(a) It is known that if $|G_S| \in R^\times$ then $I_S = I_S^2 = I_S^3 = \cdots$.

(b) Let ℓ be either a prime with $a_\ell = 2$ or a split multiplicative prime of E. Then, even if $r_E = 0$, Proposition 2.3 (1) implies that $\theta_\ell \in I_\ell$. For example, if E is defined by the equation $y^2 + y = x^3 - x^2 - 2x + 1$, then $r_E = 0$, and the primes $\ell \le 100000$ satisfying $a_\ell = 2$ are $\ell = 2$, 3, 5, 251, 983, 1009, 1051, 1669, 8219, 9397, 10477, 11789, 14461, 21773, 24019, 32117, 51239, 57737, 93199, 95747, 97859, 98711. The calculation is due to Sage [32].

It may also happen that the element $\eta_{r_E}(\mu_{S,T}(d_T)) \in I_{S^+}^{r_E}/I_{S^+}^{r_E+1}$ is trivial. Bertolini-Darmon [2] constructed a certain lift of $\eta_{r_E}(\mu_{S,T}(d_T))$ to $I_{S^+}^{r_E}$, which gives extra information in this case.

(2) See [20, Conjecture 4] for the general case, where S is not necessarily relatively prime to N. We note that our $\tilde{\theta}_S$ coincides with the leading coefficient considered in [20] (cf. Remark 2.2).

3. Darmon-Kolyvagin derivatives and Euler systems for elliptic curves

In this section, we fix notation on derivatives and Euler systems, and we recall their properties.

We fix a prime $p \geq 5$. For an integer S, we denote by $\mathbb{Q}(S)$ the maximal p-extension of $\mathbb{Q}$ inside $\mathbb{Q}(\zeta_S)$ and put $\Gamma_S = \mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$. For relatively prime integers m and n, by the canonical decomposition $\Gamma_{mn} = \Gamma_m \times \Gamma_n$, we regard Γ_m and Γ_n as subgroups of Γ_{mn}

3.1. **Darmon-Kolyvagin derivatives.**

Following [6], we introduce derivatives which we call Darmon-Kolyvagin derivatives as in [16].

As usual, for integers $j \geq 0$ and $k \geq 1$, we put

$$\binom{j}{k} = \frac{j(j-1)\cdots(j-k+1)}{k!}.$$

We put $\binom{j}{0} = 1$ for $j \geq 0$. For an element $\sigma \in \Gamma_S$ of order n and for an integer $k \geq 0$, we define

$$D_\sigma^{(k)} = \sum_{j=0}^{n-1} \binom{j}{k} \sigma^j \in \mathbb{Z}[\Gamma_S].$$

We note that $D_\sigma^{(k)} = 0$ if $k \geq n$. For $k < 0$, we define $D_\sigma^{(k)} = 0$.

Lemma 3.1. *If $\sigma \in \Gamma_S$ is of order n and $1 \leq k \leq n-1$, then*

$$(\sigma - 1)D_\sigma^{(k)} = \binom{n}{k} - \sigma D_\sigma^{(k-1)}.$$

In particular, if n is a power q of p and $0 < k < p$, then we have

$$(\sigma - 1)D_\sigma^{(k)} \equiv -\sigma D_\sigma^{(k-1)} \mod q.$$

Proof. This is proved by a straightforward computation. For the second assertion, note that $\binom{q}{k} \equiv 0 \bmod q$ for $0 < k < p$. □

Definition 3.2. In the following, for each prime ℓ we fix a generator σ_ℓ of Γ_ℓ, and we write $D_\ell^{(k)} = D_{\sigma_\ell}^{(k)}$. Let $S > 0$ be a square-free integer. We call an element D of $\mathbb{Z}[\Gamma_S]$ a *Darmon-Kolyvagin derivative*, or simply, a derivative if D is of the following form:

$$D_{\ell_1}^{(k_1)} \cdots D_{\ell_s}^{(k_s)} \in \mathbb{Z}[\Gamma_{\ell_1 \cdots \ell_s}] \subset \mathbb{Z}[\Gamma_S],$$

where $\ell_1, \ldots, \ell_s$ are distinct primes dividing S, and each k_i is an integer such that $0 \leq k_i < |\Gamma_{\ell_i}|$. We note that $\ell_1, \ldots, \ell_s, k_1, \ldots, k_s$ are uniquely determined. We define

$$\mathrm{Supp}(D) = \ell_1 \cdots \ell_s, \qquad \mathrm{Cond}(D) = \prod_{k_i > 0} \ell_i,$$

which we call the *support* and the *conductor* of D, respectively. We put

$$\mathrm{ord}(D) = k_1 + \cdots + k_s, \quad n(D) = \min_{k_i > 0}\{|\Gamma_{\ell_i}|\}, \quad e_{\ell_i}(D) = k_i.$$

We call $\mathrm{ord}(D)$ the *order* of D. Since each Γ_{ℓ_i} is a p-group, the natural number $n(D)$ is a power of p. When $k_i = 0$ for all i, we define $n(D) = 1$. When $S = \ell_1 \cdots \ell_s$, we define the norm operator as

$$N_S = D_{\ell_1}^{(0)} \cdots D_{\ell_s}^{(0)}.$$

Let S be a square-free positive integer and M a $\mathbb{Z}_p[\Gamma_S]$-module without p-torsion. We take an element $a \in M$, and put

$$\theta = \sum_{\gamma \in \Gamma_S} \gamma a \otimes \gamma \in M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Gamma_S].$$

The element θ has a *Taylor expansion* as follows.

PROPOSITION 3.3. *Let $S = \ell_1 \cdots \ell_s$ be the prime factorization of S. Then, we have*

$$\theta = \sum_{\underline{k}=(k_1,\dots,k_s) \in \mathbb{Z}_{\geq 0}^{\oplus s}} D_{\underline{k}} a \otimes (\sigma_{\ell_1} - 1)^{k_1} \cdots (\sigma_{\ell_s} - 1)^{k_s},$$

where $D_{\underline{k}} := D_{\ell_1}^{(k_1)} \cdots D_{\ell_s}^{(k_s)}$ for $\underline{k} = (k_1, \dots, k_s)$.

Remark 3.4. We note that $D_{\underline{k}} = 0$ for all but finitely many $\underline{k} \in \mathbb{Z}_{\geq 0}^{\oplus s}$

Proof. We prove the proposition by induction on the number of primes dividing S,

We first assume that S is a prime ℓ and put $\sigma = \sigma_\ell$. Since Γ_ℓ is generated by σ, we have

$$\theta = \sum_{j=0}^{|\Gamma_\ell|-1} \sigma^j a \otimes \sigma^j.$$

We note that for each j

$$\sigma^j = (\sigma - 1 + 1)^j = \sum_{k=0}^{j} \binom{j}{k} (\sigma - 1)^k = \sum_{k \geq 0} \binom{j}{k} (\sigma - 1)^k.$$

Hence, we have

$$\begin{aligned} \sum_{j=0}^{|\Gamma_\ell|-1} \sigma^j a \otimes \sigma^j &= \sum_{j=0}^{|\Gamma_\ell|-1} \sigma^j a \otimes \sum_{k \geq 0} \binom{j}{k} (\sigma - 1)^k = \sum_{j=0}^{|\Gamma_\ell|-1} \sum_{k \geq 0} \binom{j}{k} \sigma^j a \otimes (\sigma - 1)^k \\ &= \sum_{k \geq 0} \sum_{j=0}^{|\Gamma_\ell|-1} \binom{j}{k} \sigma^j a \otimes (\sigma - 1)^k = \sum_{k \geq 0} D_\ell^{(k)} a \otimes (\sigma - 1)^k. \end{aligned}$$

Then, we complete the case where S is a prime.

In the general case, we put $T = S/\ell_1$. Then, we have

$$\theta = \sum_{\gamma_1 \in \Gamma_{\ell_1}} \sum_{\gamma \in \Gamma_T} \gamma_1 \gamma a \otimes \gamma \gamma_1.$$

By the induction hypothesis,

$$\sum_{\gamma \in \Gamma_T} \gamma a \otimes \gamma = \sum_{\underline{k}' = (k_2,\dots,k_s) \in \mathbb{Z}_{\geq 0}^{\oplus s-1}} D_{\underline{k}'} a \otimes (\sigma_{\ell_2} - 1)^{k_2} \cdots (\sigma_{\ell_s} - 1)^{k_s}.$$

Hence, we have

$$\begin{aligned}\theta &= \sum_{\gamma_1\in\Gamma_{\ell_1}}\sum_{\gamma\in\Gamma_T}\gamma_1\gamma a\otimes\gamma\gamma_1\\ &= \sum_{\gamma_1\in\Gamma_{\ell_1}}\sum_{\underline{k}'=(k_2,\dots,k_s)\in\mathbb{Z}_{\geq 0}^{\oplus s-1}}\gamma_1 D_{\underline{k}'}a\otimes(\sigma_{\ell_2}-1)^{k_2}\cdots(\sigma_{\ell_s}-1)^{k_s}\gamma_1\\ &= \sum_{\underline{k}'} D_{\underline{k}'}\sum_{\gamma_1\in\Gamma_{\ell_1}}\gamma_1 a\otimes\gamma_1(\sigma_{\ell_2}-1)^{k_2}\cdots(\sigma_{\ell_s}-1)^{k_s}\\ &\overset{(*)}{=} \sum_{\underline{k}'} D_{\underline{k}'}\sum_{k_1\geq 0} D_{\ell_1}^{(k_1)}a\otimes(\sigma_{\ell_1}-1)^{k_1}(\sigma_{\ell_2}-1)^{k_2}\cdots(\sigma_{\ell_s}-1)^{k_s}\\ &= \sum_{\underline{k}=(k_1,\dots,k_s)\in\mathbb{Z}_{\geq 0}^{\oplus s}} D_{\underline{k}}a\otimes(\sigma_{\ell_1}-1)^{k_1}\cdots(\sigma_{\ell_s}-1)^{k_s},\end{aligned}$$

where the equality $(*)$ follows from the induction hypothesis. □

LEMMA 3.5. *Let G be a finite abelian p-group and σ an element of G with order q. Then,*

$$q(\sigma-1)\in I_{G,p}^p,$$

where $I_{G,p}$ denotes the augmentation ideal of $\mathbb{Z}_p[G]$.

Proof. We note that q is a power of p, and then the proposition is [6, Lemma 3.5]. □

Combining Proposition 3.3 and Lemma 3.5, we have the following.

LEMMA 3.6. *Let $t\geq 1$. Assume that $Da\equiv 0 \mod n(D)$ for every Darmon-Kolyvagin derivative D such that $\mathrm{Supp}(D)=S$ and $\mathrm{ord}(D)<\min\{t,p\}$. Then,*

$$\theta - N_S a\otimes 1\in M\otimes_{\mathbb{Z}_p} I_{\Gamma_S,p}^{\min\{t,p\}}.$$

Remark 3.7. This is [6, Lemma 3.8]. It seems that there is an error in the statement of [6, Lemma 3.8]. However, the error is not crucial when we consider Euler systems.

Proof. As in Proposition 3.3, we write

$$\theta = \sum_{\underline{k}=(k_1,\dots,k_s)\in\mathbb{Z}_{\geq 0}^{\oplus s}} D_{\underline{k}}a\otimes(\sigma_{\ell_1}-1)^{k_1}\cdots(\sigma_{\ell_s}-1)^{k_s}. \tag{3.1}$$

We pick an element $\underline{k}=(k_1,\dots,k_s)\in\mathbb{Z}_{\geq 0}^{\oplus s}\setminus\{(0,\dots,0)\}$ such that $k_1+\cdots+k_s<\min\{t,p\}$, that is, $0<\mathrm{ord}(D_{\underline{k}})<\min\{t,p\}$. By the definition of $n(D_{\underline{k}})$, there exists i such that $|\Gamma_{\ell_i}|=n(D_{\underline{k}})$ and $k_i>0$. Since $D_{\underline{k}}a\equiv 0 \mod n(D_{\underline{k}})$, Lemma 3.5 implies that

$$D_{\underline{k}}a\otimes(\sigma_{\ell_1}-1)^{k_1}\cdots(\sigma_{\ell_s}-1)^{k_s}\in M\otimes I_{\Gamma_S}^p. \tag{3.2}$$

This holds for each $D_{\underline{k}}$ such that $0<\mathrm{ord}(D_{\underline{k}})<\min\{t,p\}$. By (3.1), we complete the proof. □

3.2. **Preliminaries on Galois cohomology.** We denote by T the p-adic Tate module $T_p(E)$ of E. In this subsection, we assume (A2), that is,

$$\text{the Galois representation } \rho : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T) \text{ is surjective.}$$

Then by [28, Proposition 3.5.8 (ii)], there exists an element $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{p^\infty}))$ such that

$$T/(\tau - 1)T \cong \mathbb{Z}_p, \tag{3.3}$$

where μ_{p^∞} denotes the set of p-power roots of unity.

PROPOSITION 3.8. *For a power q of p and a finite abelian extension F of $\mathbb{Q}$, we have $E(F)[q] = 0$. Moreover, the restriction map induces an isomorphism*

$$H^1(\mathbb{Q}, E[q]) \cong H^0\left(F/\mathbb{Q}, H^1(F, E[q])\right).$$

Proof. For the first assertion, we only need to show that $E(F)[p] = 0$. We assume that $E(F)[p] \neq 0$ and take a non-trivial point $P \in E(F)[p]$. Since the Galois representation $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}/p\mathbb{Z}}(E[p])$ is surjective, for each non-trivial point $Q \in E[p]$ there exists an element $\sigma \in G_{\mathbb{Q}}$ such that $\sigma P = Q$. Since the extension $F/\mathbb{Q}$ is a Galois extension, we have $Q \in E(F)[p]$. Thus, $\mathbb{Q}(E[p]) \subseteq F$, which implies that $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q})$ is abelian. However, since $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is not abelian, we have a contradiction. Hence, $E(F)[q] = 0$. The second assertion follows from the exact sequence

$$0 \to H^1\left(F/\mathbb{Q}, E(F)[q]\right) \to H^1(\mathbb{Q}, E[q]) \to H^0\left(F/\mathbb{Q}, H^1(F, E[q])\right) \to H^2(F/\mathbb{Q}, E(F)[q])$$

which is induced by the Hochschild-Serre spectral sequence. □

For a torsion module M and an element $b \in M$, we denote by $\mathrm{ord}(b, M)$ the order of b.

LEMMA 3.9. *Let q be a power of p and L a finite Galois extension of $\mathbb{Q}$ such that G_L acts trivially on $E[q]$. Then for $\kappa, \eta \in H^1(\mathbb{Q}, E[q])$, there exists an element γ of G_L such that*

(1) $\mathrm{ord}\left(\kappa(\gamma\tau), E[q]/(\tau - 1)E[q]\right) \geq \mathrm{ord}(\kappa, H^1(L, E[q]))$,
(2) $\mathrm{ord}\left(\eta(\gamma\tau), E[q]/(\tau - 1)E[q]\right) \geq \mathrm{ord}(\eta, H^1(L, E[q]))$,

where τ is as in (3.3)*, and we regard κ, η as elements of $H^1(L, E[q]))$ by the restriction map $H^1(\mathbb{Q}, E[q]) \to H^1(L, E[q])$.*

Remark 3.10. For $\gamma \in G_L$ and $\kappa \in H^1(\mathbb{Q}, E[q])$, the image of $\kappa(\gamma\tau)$ in $E[q]/(\tau - 1)E[q]$ is independent of the choice of a cocycle representing κ.

Proof. This is [28, Lemma 5.2.1]. □

We fix some notation on local cohomology groups. Let M be $E[p^n], T$ or $V_p(E) := T \otimes_{\mathbb{Z}} \mathbb{Q}_p$. For a finite extension F of $\mathbb{Q}$ and a place λ of F, we denote by $\mathrm{loc}_\lambda : H^1(F, M) \to H^1(F_\lambda, M)$ the localization map, where F_λ denotes the completion at λ. If ℓ is a prime and if K is a finite extension of $\mathbb{Q}_\ell$, then we put

$$H^1_{\mathrm{ur}}(K, M) = \ker\left(H^1(K, M) \to H^1(K^{\mathrm{ur}}, M)\right),$$

where K^{ur} is the maximal unramified extension of K. As usual, we denote by $H^1_f(K, E[p^n])$ the image of the Kummer map $E(K)/p^n \hookrightarrow H^1(K, E[p^n])$, which we often identify with $E(K)/p^n$. We put $H^1_f(K,T) = \varprojlim_n H^1_f(K, E[p^n])$ and $H^1_f(K,V) = H^1_f(K,T) \otimes \mathbb{Q}_p$. One can check that if $\ell \nmid pN$, then $H^1_f(K,M) = H^1_{\mathrm{ur}}(K,M)$. We put

$$H^1_{/f}(K,M) = \frac{H^1(K,M)}{H^1_f(K,M)},$$

and we define $\mathrm{loc}_{/f,\lambda}$ as the composite

$$\mathrm{loc}_{/f,\lambda} : H^1(F,M) \to H^1(F_\lambda, M) \to H^1_{/f}(F_\lambda, M).$$

3.3. **Euler systems.** For a prime ℓ, we define $P_\ell(t) \in \mathbb{Z}[t]$ by

$$P_\ell(t) = 1 - a_\ell t + \epsilon(\ell) t^2, \tag{3.4}$$

where a_ℓ and ϵ are as in Section 2. Let Σ be a finite set of primes which contains all the primes dividing pN. We put

$$\mathscr{R} = \{\text{primes } \ell;\ \ell \notin \Sigma\},\ \ \mathscr{N} = \{\text{square-free products of primes in } \mathscr{R}\} \cup \{1\}.$$

Definition 3.11. We call $\{z_{Sp^n}\}_{S\in\mathscr{N}, n\geq 0} \in \prod_{S,n} H^1(\mathbb{Q}(Sp^n), T)$ an *Euler system* (for T and $\mathscr{N}$) if it satisfies the following conditions.

(1) Let $S \in \mathscr{N}$, and let $\ell \in \mathscr{R}$ be a prime not dividing S. Let $n \geq 0$. Then,

$$\mathrm{Cor}_{S\ell/S} z_{S\ell p^n} = P_\ell(\mathrm{Fr}_\ell^{-1}) z_{Sp^n},$$

where $\mathrm{Cor}_{S\ell p^n/Sp^n} : H^1(\mathbb{Q}(S\ell p^n), T) \to H^1(\mathbb{Q}(Sp^n), T)$ denotes the corestriction map, and $\mathrm{Fr}_\ell \in \Gamma_{Sp^n}$ denotes the arithmetic Frobenius at ℓ.

(2) For every $S \in \mathscr{N}$, the system $\{z_{Sp^n}\}_{n\geq 0}$ is a norm compatible system, that is,

$$\{z_{Sp^n}\}_{n\geq 0} \in \varprojlim_n H^1(\mathbb{Q}(Sp^n), T),$$

where the limit is taken with respect to the corestriction maps $\mathrm{Cor}_{Sp^{n+1}/Sp^n}$.

Remark 3.12. Our definition of Euler system slightly differs from the usual definition in [10], [26] and [28]. In the usual definition, instead of the condition (1) in Definition 3.11, every Euler system is required to satisfy

$$\mathrm{Cor}_{S\ell p^n/Sp^n}(z_{S\ell p^n}) = \left(1 - \frac{a_\ell}{\ell}\mathrm{Fr}_\ell^{-1} + \frac{1}{\ell}\mathrm{Fr}_\ell^{-2}\right) z_{Sp^n}.$$

However, since $P_\ell(t) \equiv \left(1 - \frac{a_\ell}{\ell}t + \frac{1}{\ell}t^2\right) \mod \ell - 1$, by [28, Lemma 9.6.1], the existence of an Euler system in our sense is equivalent to the existence of an Euler system in the usual sense.

PROPOSITION 3.13. *Let $\{z_{Sp^n}\}$ be an Euler system and $\lambda \nmid p$ a prime of $\overline{\mathbb{Q}}$. Then, for $S \in \mathscr{N}$ and $n \geq 0$, the image $\mathrm{loc}_\lambda(z_{Sp^n})$ of z_{Sp^n} in $H^1(\mathbb{Q}(Sp^n)_\lambda, T)$ is unramified, that is,*

$$\mathrm{loc}_\lambda(z_{Sp^n}) \in H^1_{\mathrm{ur}}(\mathbb{Q}(Sp^n)_\lambda, T).$$

Proof. This follows from [28, Proposition B.3.4]. □

3.4. **Local properties at primes not dividing p.** In this subsection, we study local properties of derivatives of Euler systems at primes *not* dividing p.

We fix a power q of p and an Euler system $\{z_{Sp^n}\}_{S\in\mathscr{N},n\geq 0}$. By taking Galois cohomology with respect to the exact sequence

$$0 \to T \xrightarrow{\times q} T \to E[q] \to 0,$$

we have a natural inclusion $H^1(K,T)/q \hookrightarrow H^1(K,E[q])$, where K is an extension field of $\mathbb{Q}$. By this inclusion, we regard an element of $H^1(K,T)/q$ as an element of $H^1(K,E[q])$.

3.4.1. *Unramifiedness at primes not dividing conductors.*

PROPOSITION 3.14. *Let D be a Darmon-Kolyvagin derivative with support S and conductor S'. We assume that the image of Dz_S in $H^1(\mathbb{Q}(S),T)/q$ is fixed by Γ_S, and we denote by $\kappa \in H^1(\mathbb{Q},E[q])$ the element corresponding to $Dz_S \bmod q \in H^1(\mathbb{Q}(S),E[q])$ under the isomorphism (cf. Proposition 3.8) $H^1(\mathbb{Q},E[q]) \cong H^0\left(\Gamma_S, H^1(\mathbb{Q}(S),E[q])\right)$. Then for every prime $\ell \nmid pS'$, we have $\mathrm{loc}_\ell(\kappa) \in H^1_{\mathrm{ur}}(\mathbb{Q}_\ell,E[q])$.*

Proof. First, we suppose that $\ell \nmid pS$. Since the extension $\mathbb{Q}(S)/\mathbb{Q}$ is unramified at ℓ, we have $(\mathbb{Q}(S)_\lambda)^{\mathrm{ur}} \cong \mathbb{Q}_\ell^{\mathrm{ur}}$ for a prime $\lambda|\ell$. Hence, we have $\mathrm{loc}_\ell(\kappa) = \mathrm{loc}_\lambda(Dz_S)$ as elements of $H^1(\mathbb{Q}_\ell^{\mathrm{ur}},E[q])$. Then, by Proposition 3.13, we have $\mathrm{loc}_\ell(\kappa) \in H^1_{\mathrm{ur}}(\mathbb{Q}_\ell,E[q])$.

We next consider a prime ℓ dividing S/S'. Then we have

$$Dz_S = D'N_\ell z_S = P_\ell(\mathrm{Fr}_\ell^{-1})D'z_{S/\ell},$$

where D' is a derivative such that $\mathrm{Supp}(D') = S/\ell$. Since the extension $\mathbb{Q}(S/\ell)/\mathbb{Q}$ is unramified at ℓ, for a prime λ of $\mathbb{Q}(S/\ell)$ we have $\mathrm{loc}_\ell(\kappa) = \mathrm{loc}_\lambda(D'P_\ell(\mathrm{Fr}_\ell^{-1})z_{S/\ell})$ in $H^1(\mathbb{Q}_\ell^{\mathrm{ur}},E[q])$. Then by Proposition 3.13, we complete the proof. □

COROLLARY 3.15. *Assume that $p \nmid \prod_{\ell|N} m_\ell$, where $m_\ell := [E(\mathbb{Q}_\ell),E_0(\mathbb{Q}_\ell)]$. Under the notation as above, for every prime $\ell \nmid pS'$ we have*

$$\mathrm{loc}_\ell(\kappa) \in H^1_f(\mathbb{Q}_\ell,E[q]).$$

Proof. Our proof is based on that of [6, Theorem 4.9]. By the exact sequence

$$0 \to E(\mathbb{Q}_\ell)/q \to H^1(\mathbb{Q}_\ell,E[q]) \to H^1(\mathbb{Q}_\ell,E)[q] \to 0,$$

it suffices to show that the image $\mathrm{loc}_{/f,\ell}(\kappa)$ of κ in $H^1(\mathbb{Q}_\ell,E)[q]$ is trivial. Proposition 3.14 implies that $\mathrm{loc}_{/f,\ell}(\kappa) \in H^1(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell,E(\mathbb{Q}_\ell^{\mathrm{ur}}))[q]$. Since $p \nmid m_\ell$ (if $\ell \nmid N$, then $m_\ell = 1$), by [22, Chapter I, Proposition 3.8], we have $H^1(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell,E(\mathbb{Q}_\ell^{\mathrm{ur}}))[q] = 0$. Hence $\mathrm{loc}_{/f,\ell}(\kappa) = 0$. □

3.4.2. *Local properties at primes dividing conductors.* In the rest of Subsection 3.4, we prove Theorem 3.18, following the proof of [28, Theorem 4.5.4].

We put

$$\begin{aligned} &\mathscr{R}_q = \{\ell \in \mathscr{R}\ ;\ q|\ell-1\}, \quad \mathscr{R}_{E,q} = \{\ell \in \mathscr{R}_q\ ;\ q|P_\ell(1)\},\\ &\mathscr{N}_q = \{\text{square-free products of primes in } \mathscr{R}_q\}. \end{aligned} \tag{3.5}$$

Definition 3.16. Let $S \in \mathscr{N}_p$. For a positive divisor S' of S, let $x_{S'}$ denote an indeterminate. We denote by Y_S the free $\mathbb{Z}_p[\Gamma_S]$-module generated by $\{x_{S'}\}_{S'|S>0}$, that is, $Y_S = \oplus_{S'|S>0}\mathbb{Z}_p[\Gamma_S]x_{S'}$. We denote by Z_S the $\mathbb{Z}_p[\Gamma_S]$-submodule of Y_S generated by the following elements:

$$\sigma x_{S'} - x_{S'} \text{ for } S'|S \text{ and } \sigma \in \Gamma_{S/S'}, \quad N_\ell x_{S'\ell} - P_\ell(\mathrm{Fr}_\ell^{-1})x_{S'} \text{ for primes } \ell \text{ with } \ell S'|S.$$

As in [28, Definition 4.2.1], we define a $\mathbb{Z}_p[\Gamma_S]$-module X_S by $X_S = Y_S/Z_S$.

If we regard $z_{S'}$ as an element of $H^1(\mathbb{Q}(S), T)$ for $S'|S$ by the restriction map, then there exists a unique Γ_S-homomorphism $g_S : X_S \to H^1(\mathbb{Q}(S), T)$ sending $x_{S'}$ to $z_{S'}$ for $S'|S$.

Let q be a power of p, and let $M_q = \mathrm{Ind}_{\{1\}}^{G_\mathbb{Q}}(E[q])$. We recall that the $G_\mathbb{Q}$-module $\mathrm{Ind}_{\{1\}}^{G_\mathbb{Q}}(E[q])$ is defined as the module of continuous maps from $G_\mathbb{Q}$ to $E[q]$, and $G_\mathbb{Q}$ acts on $\mathrm{Ind}_{\{1\}}^{G_\mathbb{Q}}(E[q])$ by $(\sigma f)(g) = f(g\sigma)$ for $\sigma, g \in G_\mathbb{Q}$. Then we have an exact sequence of $G_\mathbb{Q}$-modules

$$0 \to E[q] \to M_q \to M_q/E[q] \to 0,$$

where the map $E[q] \to M_q$ is defined as $y \mapsto (g \mapsto gy)$. For a finite extension L of $\mathbb{Q}$, by taking Galois cohomology, we obtain an exact sequence

$$0 \to E(L)[q] \to M_q^{G_L} \to (M_q/E[q])^{G_L} \xrightarrow{\delta_L} H^1(L, E[q]) \to 0, \tag{3.6}$$

where the surjectivity of the connecting map δ_L follows from [28, Proposition B.4.5].

PROPOSITION 3.17. *There exists a Γ_S-homomorphism d_S from X_S to $(M_q/E[q])^{G_{\mathbb{Q}(S)}}$ making the following diagram commutative*:

$$\begin{array}{ccc} & & (M_q/E[q])^{G_{\mathbb{Q}(S)}} \\ & \overset{d_S}{\nearrow} & \big\downarrow \delta_{\mathbb{Q}(S)} \\ X_S & \xrightarrow[g_S]{} & H^1(\mathbb{Q}(S), E[q]). \end{array}$$

Proof. This is [28, Proposition 4.4.8]. □

We take a prime $\ell \in \mathscr{R}_{E,q}$ which splits completely in $\mathbb{Q}(S)$. We denote by $\mathscr{D}_\ell \subseteq G_\mathbb{Q}$ a decomposition group of ℓ and by $\mathscr{I}_\ell \subset \mathscr{D}_\ell$ the inertia group. Then, the natural map $\mathscr{I}_\ell \to \Gamma_\ell$ is surjective. We fix a lift of the fixed generator $\sigma_\ell \in \Gamma_\ell$ to $\mathscr{I}_\ell$, which we denote by the same symbol σ_ℓ. We fix a lift $\mathrm{Fr}_\ell \in \mathscr{D}_\ell$ of the arithmetic Frobenius at ℓ. We put $n_\ell = |\Gamma_\ell|$, and by abuse of notation, we define

$$N_\ell = \sum_{i=1}^{n_\ell} \sigma_\ell^i, \quad D_\ell^{(1)} = \sum_{i=0}^{n_\ell - 1} i\sigma_\ell^i \ \in \mathbb{Z}[\mathscr{I}_\ell],$$

which are lifts of derivatives denoted by the same symbols in Definition 3.2. Then we have

$$(\sigma_\ell - 1)D_\ell^{(1)} = n_\ell \sigma_\ell^{n_\ell} - N_\ell \ \text{ in } \mathbb{Z}[\mathscr{I}_\ell]. \tag{3.7}$$

By [28, Lemma 1.4.7 (i)], we have two isomorphisms

$$\alpha_\ell : H^1_{/f}(\mathbb{Q}_\ell, E[q]) \cong E[q]^{\mathrm{Fr}_\ell=1}, \ \ c \mapsto c(\sigma_\ell),$$
$$\beta_\ell : H^1_f(\mathbb{Q}_\ell, E[q]) \cong E[q]/(\mathrm{Fr}_\ell - 1)E[q], \ \ c \mapsto c(\mathrm{Fr}_\ell),$$

where each element $c \in H^1(\mathbb{Q}_\ell, E[q])$ is regarded as a cocycle. Here, we note that the map α_ℓ depends on the choice of σ_ℓ. Since $\ell \in \mathscr{R}_{E,q}$, we have $P_\ell(1) = 2 - a_\ell \equiv 0 \mod q$, and then $a_\ell \equiv 2 \mod q$. Hence, $P_\ell(t) \equiv (t-1)^2 \bmod q$. Since $P_\ell(t) \equiv \det_{\mathbb{Z}_p}(1 - \mathrm{Fr}_\ell t | T) \mod q$, we have $P_\ell(\mathrm{Fr}_\ell^{-1})E[q] = 0$. Therefore, if we put $Q_\ell(t) = t - 1$, then we have a well-defined homomorphism

$$Q_\ell(\mathrm{Fr}_\ell^{-1}) : E[q]/(\mathrm{Fr}_\ell - 1)E[q] \to E[q]^{\mathrm{Fr}_\ell=1}, \ \ y \mapsto Q_\ell(\mathrm{Fr}_\ell^{-1})y.$$

We define

$$\phi_\ell^{fs} : H^1_f(\mathbb{Q}_\ell, E[q]) \to H^1_{/f}(\mathbb{Q}_\ell, E[q])$$

as the composite

$$H^1_f(\mathbb{Q}_\ell, E[q]) \xrightarrow{\beta_\ell} E[q]/(\mathrm{Fr}_\ell - 1)E[q] \xrightarrow{Q_\ell(\mathrm{Fr}_\ell^{-1})} E[q]^{\mathrm{Fr}_\ell=1} \xrightarrow{\alpha_\ell^{-1}} H^1_{/f}(\mathbb{Q}_\ell, E[q]).$$

THEOREM 3.18. *Let S be an element of $\mathscr{N}_p$ and q a power of p. We take a prime $\ell \in \mathscr{R}_{E,q}$ which splits completely in $\mathbb{Q}(S)$. Let λ be the prime of $\mathbb{Q}(S)$ above ℓ corresponding to the decomposition group $\mathscr{D}_\ell$ of $\mathbb{Q}$. For a Darmon-Kolyvagin derivative D whose support is S, we have the following.*

(1) *The image of* $\mathrm{loc}_\lambda(Dz_S)$ *in* $H^1(\mathbb{Q}(S)_\lambda, E[q]) = H^1(\mathbb{Q}_\ell, E[q])$ *lies in* $H^1_f(\mathbb{Q}_\ell, E[q])$.
(2) *The image of* $DD_\ell^{(1)} z_{S\ell}$ *in* $H^1(\mathbb{Q}(S\ell), T)/q$ *is fixed by* Γ_ℓ.
(3) *If* $\kappa^{(\ell)} \in H^1(\mathbb{Q}(S), E[q])$ *denotes the class corresponding to* $DD_\ell^{(1)} z_{S\ell} \mod q$ *under the isomorphism* $H^1(\mathbb{Q}(S), E[q]) \cong H^0\left(\Gamma_\ell, H^1(\mathbb{Q}(S\ell), E[q])\right)$, *then we have*

$$\mathrm{loc}_{/f,\lambda}(\kappa^{(\ell)}) = \phi_\ell^{fs}(\mathrm{loc}_\lambda(Dz_S \bmod q)) \in H^1_{/f}(\mathbb{Q}_\ell, E[q]).$$

(4) *In addition, if* $E[q]/(\mathrm{Fr}_\ell - 1)E[q] \cong \mathbb{Z}/q\mathbb{Z}$, *then*

$$\mathrm{ord}\left(\mathrm{loc}_{/f,\lambda}(\kappa^{(\ell)}), H^1_{/f}(\mathbb{Q}_\ell, E[q])\right) = \mathrm{ord}\left(\mathrm{loc}_\lambda(Dz_S \bmod q), H^1(\mathbb{Q}_\ell, E[q])\right).$$

Proof. The assertion (1) follows from Proposition 3.13. By Lemma 3.1, we have

$$(\sigma_\ell - 1)DD_\ell^{(1)} x_{S\ell} \equiv -\sigma_\ell D N_\ell x_{S\ell} \equiv -\sigma_\ell D P_\ell(\mathrm{Fr}_\ell^{-1}) x_S \equiv -\sigma_\ell D P_\ell(1) x_S \equiv 0 \mod qX_{S\ell},$$

where the third congruence follows from $\mathrm{Fr}_\ell = 1$ in Γ_S, and the last congruence follows from $\ell \in \mathscr{R}_{E,q}$. Hence, the image of $DD_\ell^{(1)} x_{S\ell}$ in $X_{S\ell}/q$ is fixed by Γ_ℓ. Since a homomorphism $d_{S\ell}$ as in Proposition 3.17 is $G_\mathbb{Q}$-equivariant, we have $d_{S\ell}(DD_\ell^{(1)} x_{S\ell}) \in H^0(\Gamma_\ell, (M_q/E[q])^{G_{\mathbb{Q}(S\ell)}})$. Hence, since $\delta_{\mathbb{Q}(S\ell)}(d_{S\ell}(x_{S\ell})) = z_{S\ell} \bmod q$, we have the assertion (2),

We take lifts $\hat{d}(x_{S\ell}), \hat{d}(x_S) \in M_q$ of $d_{S\ell}(x_{S\ell}), d_{S\ell}(x_S)$, respectively. We also take a lift of D to $\mathbb{Z}[G_\mathbb{Q}]$, which we denote by the same symbol D. To simplify the notation, we put

$\overline{z}_S = z_S \bmod q$. By the definition of ϕ_ℓ^{fs}, it suffices to show that

$$Q_\ell(\mathrm{Fr}_\ell^{-1})\left((D\overline{z}_S)(\mathrm{Fr}_\ell)\right) = \kappa^{(\ell)}(\sigma_\ell) \ \in E[q], \tag{3.8}$$

where we regard $D\overline{z}_S$ and κ as cocycles. We recall that $\delta_{\mathbb{Q}(S)}$ is the connecting map from $H^0\left(\mathbb{Q}(S), M_q/E[q]\right)$ to $H^1(\mathbb{Q}(S), E[q])$, and hence

$$(D\overline{z}_S)(\mathrm{Fr}_\ell) = (\mathrm{Fr}_\ell - 1)D\hat{d}(x_S), \quad \kappa^{(\ell)}(\sigma_\ell) = (\sigma_\ell - 1)D_\ell^{(1)}D\hat{d}(x_{S\ell}) \in E[q]. \tag{3.9}$$

Since $Q_\ell(\mathrm{Fr}_\ell^{-1})(\mathrm{Fr}_\ell^{-1} - 1)E[q] = P_\ell(\mathrm{Fr}_\ell^{-1})E[q] = 0$, we have

$$Q_\ell(\mathrm{Fr}_\ell^{-1})\left((D\overline{z}_S)(\mathrm{Fr}_\ell)\right) = Q_\ell(\mathrm{Fr}_\ell^{-1})\mathrm{Fr}_\ell^{-1}\left((D\overline{z}_S)(\mathrm{Fr}_\ell)\right).$$

Thus, by (3.9), (3.7) and [28, Lemma 4.7.1], we obtain

$$\begin{aligned}
&Q_\ell(\mathrm{Fr}_\ell^{-1})((D\overline{z}_S)(\mathrm{Fr}_\ell)) - \kappa^{(\ell)}(\sigma_\ell) \\
&= Q_\ell(\mathrm{Fr}_\ell^{-1})\mathrm{Fr}_\ell^{-1}((D\overline{z}_S)(\mathrm{Fr}_\ell)) - \kappa^{(\ell)}(\sigma_\ell) \\
&= Q_\ell(\mathrm{Fr}_\ell^{-1})\mathrm{Fr}_\ell^{-1}(\mathrm{Fr}_\ell - 1)D\hat{d}(x_S) - (\sigma_\ell - 1)D_\ell^{(1)}D\hat{d}(x_{S\ell}) \\
&= -P_\ell(\mathrm{Fr}_\ell^{-1})D\hat{d}(x_S) + N_\ell D\hat{d}(x_{S\ell}).
\end{aligned}$$

By [28, Lemma 4.7.3], this is zero, and then we conclude (3.8).

If $E[q]/(\mathrm{Fr}_\ell - 1)E[q] \cong \mathbb{Z}/q\mathbb{Z}$, then [28, Corollary A.2.7] says that ϕ_ℓ^{fs} is an isomorphism, and hence the assertion (4) follows. □

4. Divisibility of Euler systems

In this section, we study p-divisibility of derivatives of Euler systems (cf. Theorem 4.9), and we give its applications.

We keep the notation as in Section 3. In particular, $\{z_{Sp^n}\}_{S\in\mathscr{N},n\geq 0}$ denotes an Euler system for T and an $\mathscr{N}$ in the sense of Definition 3.11.

4.1. **The theorem on divisibility of Euler systems.**

The aim of this subsection is to prove Theorem 4.9. We also give a modification (Theorem 4.15) of Theorem 4.9, which is used to prove Theorems 4.21 and 6.4.

4.1.1. *Notation.* Let q be a power of p.

Definition 4.1. For a finitely generated $\mathbb{Z}_p$-module M, we define an integer $r_q(M)$ by

$$M \otimes \mathbb{Z}/q\mathbb{Z} \cong (\mathbb{Z}/q\mathbb{Z})^{\oplus r_q(M)} \oplus M',$$

where the exponent of M' is strictly less than q.

Lemma 4.2. *For an exact sequence of finite $\mathbb{Z}/q\mathbb{Z}$-modules $0 \to M' \to M \to M''$, we have*

$$r_q(M) \leq r_q(M') + r_p(M'').$$

Proof. This is [6, Lemma 5.1]. □

Definition 4.3. We define the Selmer group $\mathrm{Sel}(\mathbb{Q}, E[q])$ by

$$\mathrm{Sel}(\mathbb{Q}, E[q]) = \ker\left(H^1(\mathbb{Q}, E[q]) \to \prod_{w:\text{places}} \frac{H^1(\mathbb{Q}_w, E[q])}{E(\mathbb{Q}_w)/q} \right),$$

and for a positive integer S, we define a subgroup $H^1_{f,S}(\mathbb{Q}, E[q])$ of $\mathrm{Sel}(\mathbb{Q}, E[q])$ by

$$H^1_{f,S}(\mathbb{Q}, E[q]) = \ker\left(\mathrm{Sel}(\mathbb{Q}, E[q]) \to \oplus_{\ell|S} E(\mathbb{Q}_\ell)/q\right), \tag{4.1}$$

where ℓ ranges over all the primes dividing S. If there is no fear of confusion, then we simply write $H^1_{f,S} = H^1_{f,S}(\mathbb{Q}, E[q])$.

We put $A_q(S) = \oplus_{\ell|S} E(\mathbb{Q}_\ell)/q$.

LEMMA 4.4. *Let S be a positive integer and $\ell \nmid S$ a prime such that $E(\mathbb{Q}_\ell)/p$ is cyclic. Then, we have*

$$r_q(H^1_{f,S\ell}) + r_p(A_q(S\ell)) - 1 \leq r_q(H^1_{f,S}) + r_p(A_q(S)). \tag{4.2}$$

In addition, if $E(\mathbb{Q}_\ell)/p \cong \mathbb{Z}/p$, then we have

$$r_q(H^1_{f,S}) + r_p(A_q(S)) \leq r_q(H^1_{f,S\ell}) + r_p(A_q(S\ell)) \tag{4.3}$$

Proof. Since $H^1_{f,S\ell} \subseteq H^1_{f,S}$ and $r_p(A_q(S\ell)) \leq r_p(A_q(S)) + 1$, we have (4.2). We assume that $E(\mathbb{Q}_\ell)/p \cong \mathbb{Z}/p$. By Lemma 4.2 with the exact sequence $0 \to H^1_{f,S\ell} \to H^1_{f,S} \to E(\mathbb{Q}_\ell)/q$, we have

$$r_q(H^1_{f,S}) \leq r_q(H^1_{f,S\ell}) + r_p(E(\mathbb{Q}_\ell)/p) = r_q(H^1_{f,S\ell}) + 1.$$

Since $r_p(A_q(S)) + 1 = r_p(A_q(S\ell))$, we deduce that

$$r_q(H^1_{f,S}) + r_p(A_q(S)) \leq r_q(H^1_{f,S\ell}) + r_p(A_q(S\ell)).$$

□

Definition 4.5. Let D be a Darmon-Kolyvagin derivative whose support S lies in $\mathscr{N}_q$ (see (3.5) for the notation). Then, we define the *weight* of D as

$$w(D) = \mathrm{ord}(D) - |\{\ell \in \mathscr{R}_{E,q}\ ;\ \ell \text{ divides } S\}|.$$

Remark 4.6. In Darmon's argument ([6]) for Heegner points, the notion of weight also played an important role. We modify his weight for Euler systems in our sense. See [16] for Heegner cycles.

PROPOSITION 4.7. *Let D be a Darmon-Kolyvagin derivative and S its support. Suppose that $S \in \mathscr{N}_q$. If $w(D) < 0$ and $\max_{\ell|S}\{e_\ell(D)\} < p$ (see Definition 3.2 for $e_\ell(D)$), then we have*

$$Dz_S \equiv 0 \mod qH^1(\mathbb{Q}(S), T).$$

Proof. We note that the assumption $w(D) < 0$ implies that there exist a prime $\ell \in \mathscr{R}_{E,q}$ dividing S and a derivative D' such that

$$D = D'N_\ell, \quad \mathrm{Supp}(D') = S/\ell, \quad \mathrm{ord}(D') = \mathrm{ord}(D). \tag{4.4}$$

We prove the proposition by induction on the number of primes dividing S. If $S = \ell$ is a prime, then $\ell \in \mathscr{R}_{E,q}$ and $D = N_\ell$. Since $P_\ell(1) \equiv 0 \bmod q$, we have

$$Dz_\ell = N_\ell z_\ell = P_\ell(\mathrm{Fr}_\ell^{-1})z_1 \equiv P_\ell(1)z_1 \equiv 0 \mod q.$$

In general, since $w(D) < 0$, there exist a prime $\ell \in \mathscr{R}_{E,q}$ dividing S and a derivative D' as in (4.4). Then, we have

$$\begin{aligned} w(D') &= \mathrm{ord}(D') - |\{\ell' \in \mathscr{R}_{E,q} \,;\, \ell' \text{ divides } S/\ell\}| \\ &= \mathrm{ord}(D) - |\{\ell' \in \mathscr{R}_{E,q} \,;\, \ell' \text{ divides } S\}| + 1 \\ &= w(D) + 1 \leq 0. \end{aligned}$$

We write $S/\ell = \ell_1 \cdots \ell_a$. We first show that for $1 \leq i \leq a$,

$$(\sigma_{\ell_i} - 1)D'z_{S/\ell} \equiv 0 \mod q, \tag{4.5}$$

where σ_{ℓ_i} is the generator of Γ_{ℓ_i} fixed in Definition 3.2. It suffices to consider the case $i = 1$. We write $D' = D_{\ell_1}^{(k_1)} \cdots D_{\ell_a}^{(k_a)}$. In the case where $k_1 = 0$, we have $D' = N_{\ell_1} D_{\ell_2}^{(k_2)} \cdots D_{\ell_a}^{(k_a)}$, and hence (4.5) is clear. We may then assume that $k_1 \geq 1$. Since the order of σ_{ℓ_1} is divisible by q and since $0 < k_1 < p$, Lemma 3.1 implies that

$$(\sigma_{\ell_1} - 1)D' \equiv -\sigma_{\ell_1} D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_a}^{(k_a)} \mod q. \tag{4.6}$$

We note that

$$\mathrm{Supp}(D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_a}^{(k_a)}) = S/\ell, \quad w(D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_a}^{(k_a)}) = w(D') - 1 < 0.$$

Then, the induction hypothesis implies that $D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_a}^{(k_a)} z_{S/\ell} \equiv 0 \mod q$, and hence by (4.6), we deduce (4.5).

Since each Γ_{ℓ_i} is generated by σ_{ℓ_i}, the assertion (4.5) implies that

$$D'z_{S/\ell} \bmod q \in H^0\left(\Gamma_{S/\ell}, H^1(\mathbb{Q}(S/\ell), T)/q\right).$$

Hence, we have

$$Dz_S = D'N_\ell z_S = P_\ell(\mathrm{Fr}_\ell^{-1})D'z_{S/\ell} \equiv P_\ell(1)D'z_{S/\ell} \equiv 0 \mod q.$$

□

4.1.2. *The proof and an application.* In the rest of Subsection 4.1, we assume the following.

Assumption 4.8. The prime p does not divide the product $6N\prod_{\ell|N} m_\ell$, and the Galois representation $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T)$ is surjective.

Let q be a power of p.

THEOREM 4.9. *Let D be a Darmon-Kolyvagin derivative satisfying $\max_{\ell|S}\{e_\ell(D)\} < p$, where $S := \mathrm{Supp}(D)$. Suppose that $S \in \mathscr{N}_q$ and that for every prime $\ell|S$, the module $E(\mathbb{F}_\ell)[p]$ is cyclic, that is, $E(\mathbb{F}_\ell)[p] = 0$ or $E(\mathbb{F}_\ell)[p] \cong \mathbb{Z}/p\mathbb{Z}$. If $\mathrm{ord}(D) < r_q\left(H^1_{f,p}(\mathbb{Q}, E[q])\right)$, then*

$$Dz_S \equiv 0 \mod qH^1(\mathbb{Q}(S), T). \tag{4.7}$$

We prove it by induction on $w(D)$. Before the proof, we prove some lemmas.

LEMMA 4.10. *Let D be a Darmon-Kolyvagin derivative whose support S lies in $\mathscr{N}_q$. Assume that the image of Dz_S in $H^1(\mathbb{Q}(S), T)/q$ is fixed by Γ_S, and let $\kappa \in H^1(\mathbb{Q}, E[q])$ be as in Proposition 3.14. We put $S' = \mathrm{Cond}(D)$. If $r_q(H^1_{f,pS'}(\mathbb{Q}, E[q])) > 0$, then there exists a prime $\ell \in \mathscr{R}$ such that*

1. *$\ell \equiv 1 \mod q$, ℓ splits completely in $\mathbb{Q}(S)$, and $E(\mathbb{Q}_\ell)/q \cong \mathbb{Z}/q\mathbb{Z}$,*
2. *$\mathrm{ord}\,(Dz_S \bmod q, H^1(\mathbb{Q}(S), T)/q) = \mathrm{ord}(\mathrm{loc}_\ell(\kappa), H^1(\mathbb{Q}_\ell, E[q]))$,*
3. *the localization map $H^1_{f,pS'}(\mathbb{Q}, E[q]) \to E(\mathbb{Q}_\ell)/q$ is surjective.*

Proof. By the natural inclusion $H^1(\mathbb{Q}(S), T)/q \hookrightarrow H^1(\mathbb{Q}(S), E[q])$ and Proposition 3.8,

$$\mathrm{ord}\left(Dz_S \bmod q, H^1(\mathbb{Q}(S), T)/q\right) = \mathrm{ord}\left(\kappa, H^1(\mathbb{Q}, E[q])\right). \tag{4.8}$$

We put $d = \mathrm{ord}\,(\kappa, H^1(\mathbb{Q}, E[q]))$. Since $r_q(H^1_{f,pS'}(\mathbb{Q}, E[q])) > 0$, there exists an element $\eta \in H^1_{f,pS'}(\mathbb{Q}, E[q])$ of order q. We put $L = \mathbb{Q}(S)(E[q])$ (the composite of $\mathbb{Q}(S)$ and $\mathbb{Q}(E[q])$). Since $(S, pN) = 1$, we have $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q})$. By [3, Proposition 6.3 (2)], we have

$$H^1(L/\mathbb{Q}(S), E[q]) \cong H^1(\mathbb{Q}(E[q])/\mathbb{Q}, E[q]) = 0.$$

Then, the restriction map $H^1(\mathbb{Q}(S), E[q]) \to H^1(L, E[q])$ is injective, and hence by Proposition 3.8, the restriction map $H^1(\mathbb{Q}, E[q]) \to H^1(L, E[q])$ is injective. Therefore, the image of κ in $H^1(L, E[q])$ is of order d, and the image of η is of order q. For $\tau \in G_{\mathbb{Q}(\mu_{p^\infty})}$ as in (3.3), by Lemma 3.9, there exists an element γ of G_L such that

$$\mathrm{ord}(\kappa(\gamma\tau), E[q]/(\tau - 1)E[q]) = d, \quad \mathrm{ord}(\eta(\gamma\tau), E[q]/(\tau - 1)E[q]) = q. \tag{4.9}$$

We note that $H^1(L, E[q]) = \mathrm{Hom}(G_L, E[q])$. We regard κ, η as elements of $\mathrm{Hom}(G_L, E[q])$ and put $H = \ker(\kappa) \cap \ker(\eta) \subset G_L$. Let L' be a finite Galois extension of $\mathbb{Q}$ containing $\overline{\mathbb{Q}}^H$. For $\sigma \in G_{\mathbb{Q}}$, we denote by $[\sigma]$ the conjugacy class of the image of σ in $\mathrm{Gal}(L'/\mathbb{Q})$. By Chebotarev's density theorem, there exists a prime $\ell \in \mathscr{R}$ not dividing pNS such that

$$[\mathrm{Fr}_\ell] = [\gamma\tau]. \tag{4.10}$$

It remains to show that this ℓ satisfies the conditions (1), (2) and (3) above.

(1) Since $\gamma\tau = 1$ in $\mathrm{Gal}(\mathbb{Q}(S)(\zeta_q)/\mathbb{Q})$ (recall that $\mathbb{Q}(\zeta_q) \subseteq \mathbb{Q}(E[q])$ by the Weil pairing), we have $\ell \equiv 1 \bmod q$, and ℓ splits completely in $\mathbb{Q}(S)$. Since $\gamma \in G_L$ and $\mathbb{Q}(E[q]) \subseteq L$, by (4.10) we have $\mathrm{Fr}_\ell = \sigma\tau\sigma^{-1}$ in $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q})$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[q]/\mathbb{Q})$. Thus, we have

$$H^1_f(\mathbb{Q}_\ell, E[q]) \overset{\beta_\ell}{\cong} E[q]/(\mathrm{Fr}_\ell - 1)E[q] = E[q]/\sigma(\tau - 1)E[q] \cong \mathbb{Z}/q\mathbb{Z},$$

and then we complete (1).

(2) Proposition 3.14 implies that the localization $\mathrm{loc}_\ell(\kappa)$ lies in $H^1_f(\mathbb{Q}_\ell, E[q])$. By the isomorphism β_ℓ and (4.8), it suffices to show that for a lift $\mathrm{Fr}_\ell \in G_\mathbb{Q}$ of the arithmetic Frobenius at ℓ,

$$\mathrm{ord}\,(\kappa(\mathrm{Fr}_\ell), E[q]/(\mathrm{Fr}_\ell - 1)E[q]) = d. \tag{4.11}$$

By (4.10), we have $\mathrm{Fr}_\ell = \sigma\gamma\tau\sigma^{-1}g \in G_\mathbb{Q}$ for some $\sigma \in G_\mathbb{Q}$ and $g \in G_{L'}$. Then, for a cocycle $\xi \in H^1(\mathbb{Q}, E[q])$ which is unramified at ℓ and satisfies $\xi(g) = 0$, we have

$$\begin{aligned}
\xi(\mathrm{Fr}_\ell) = \xi(\sigma\gamma\tau\sigma^{-1}g) &\overset{\text{(i)}}{=} \xi(\sigma\gamma\tau\sigma^{-1}) = \sigma\xi(\gamma\tau\sigma^{-1}) + \xi(\sigma) \\
&= \sigma\left(\gamma\tau\xi(\sigma^{-1}) + \xi(\gamma\tau)\right) + \xi(\sigma) \overset{\text{(ii)}}{=} \sigma\tau\xi(\sigma^{-1}) + \xi(\sigma) + \sigma\xi(\gamma\tau) \\
&= -\sigma\tau\sigma^{-1}\xi(\sigma) + \xi(\sigma) + \sigma\xi(\gamma\tau) = -(\mathrm{Fr}_\ell - 1)\xi(\sigma) + \sigma\xi(\gamma\tau) \\
&\equiv \sigma\xi(\gamma\tau) \mod (\mathrm{Fr}_\ell - 1)E[q],
\end{aligned}$$

where the equality (i) follows from $\xi(g) = 0$, and (ii) follows from $\gamma \in G_L$. Since

$$(\mathrm{Fr}_\ell - 1)E[q] = \sigma(\tau - 1)E[q],$$

we have

$$\mathrm{ord}\,(\xi(\mathrm{Fr}_\ell), E[q]/(\mathrm{Fr}_\ell - 1)E[q]) = \mathrm{ord}\,(\xi(\gamma\tau), E[q]/(\tau - 1)E[q])\,. \tag{4.12}$$

By (4.9) and (4.12) with $\xi = \kappa$, we conclude (4.11).

(3) By definition, we have $\mathrm{loc}_\ell(\eta) \in H^1(\mathbb{F}_\ell, E[q])$. By (4.9) and (4.12) with $\xi = \eta$, we deduce that $\eta(\mathrm{Fr}_\ell)$ is of order q as an element of $E[q]/(\mathrm{Fr}_\ell - 1)E[q]$, and hence the image of η in $E(\mathbb{Q}_\ell)/q$ is of order q. Since $E(\mathbb{Q}_\ell)/q \cong \mathbb{Z}/q\mathbb{Z}$, we have the assertion (3). □

LEMMA 4.11. *Under the same notation and assumption as in Lemma 4.10, if the image of $DD^{(1)}_\ell z_S$ in $H^1(\mathbb{Q}(S\ell), T)/q$ is fixed by $\Gamma_{S\ell}$, then*

$$Dz_S \equiv 0 \mod qH^1(\mathbb{Q}(S), T).$$

Proof. We denote by $\kappa^{(\ell)} \in H^1(\mathbb{Q}, E[q])$ the inverse image of $DD^{(1)}_\ell z_{S\ell} \bmod q$ under the isomorphism $H^1(\mathbb{Q}, E[q]) \cong H^0\left(\Gamma_{S\ell}, H^1(\mathbb{Q}(S\ell), E[q])\right)$. Theorem 3.18 (4) implies that

$$\mathrm{ord}\left(\mathrm{loc}_{/f,\ell}(\kappa^{(\ell)}), H^1_{/f}(\mathbb{Q}_\ell, E[q])\right) = \mathrm{ord}\left(\mathrm{loc}_\ell(\kappa), H^1(\mathbb{Q}_\ell, E[q])\right).$$

Hence, by the condition (2) of Lemma 4.10, we have

$$\mathrm{ord}\left(\mathrm{loc}_{/f,\ell}(\kappa^{(\ell)}), H^1_{/f}(\mathbb{Q}_\ell, E[q])\right) = \mathrm{ord}\left(Dz_S \bmod q, H^1(\mathbb{Q}(S), T)/q\right). \tag{4.13}$$

Therefore, we are reduced to showing that $\mathrm{loc}_{/f,\ell}(\kappa^{(\ell)}) = 0$. For a prime w, we have the perfect pairing $(-,-)_w$ induced by the cup product and the Weil pairing

$$(-,-)_w : H^1_f(\mathbb{Q}_w, E[q]) \times H^1_{/f}(\mathbb{Q}_w, E[q]) \to \mathbb{Z}/q\mathbb{Z}.$$

Since the natural map $H^1_{f,pS'}(\mathbb{Q}, E[q]) \to E(\mathbb{Q}_\ell)/q \ \left(= H^1_f(\mathbb{Q}_\ell, E[q])\right)$ is surjective (Lemma 4.10 (3)), by taking the Pontryagin dual we have an injective homomorphism

$$H^1_{/f}(\mathbb{Q}_\ell, E[q]) \to \mathrm{Hom}\left(H^1_{f,pS'}(\mathbb{Q}, E[q]), \mathbb{Z}/q\mathbb{Z}\right), \ \ a \mapsto (y \mapsto (y,a)_\ell). \tag{4.14}$$

Hence, it suffices to show that $\mathrm{loc}_{/f,\ell}(\kappa^{(\ell)})$ is in the kernel of the map above. Since $p \neq 2$, the Hasse principle implies that for $x \in H^1_{f,pS'}(\mathbb{Q}, E[q])$

$$(x, \kappa^{(\ell)})_\ell = -\sum_{w \nmid \ell : \text{prime}} (x, \kappa^{(\ell)})_w. \tag{4.15}$$

If $w \nmid pS'\ell$, then by Corollary 3.15, we have $\mathrm{loc}_w(\kappa^{(\ell)}) \in H^1_f(\mathbb{Q}_w, E[q])$, and hence $(x, \kappa^{(\ell)})_w = 0$. If $w | pS'$, then by the definition of $H^1_{f,pS'}(\mathbb{Q}, E[q])$, we have $(x, \kappa^{(\ell)})_w = 0$. Therefore by (4.15), we obtain $(x, \kappa^{(\ell)})_\ell = 0$. Since $x \in H^1_{f,pS'}(\mathbb{Q}, E[q])$ is arbitrary, we deduce that $\mathrm{loc}_{/f,\ell}(\kappa^{(\ell)})$ is in the kernel of the injection (4.14), and hence it is trivial. □

LEMMA 4.12. *Let D be a Darmon-Kolyvagin derivative such that $\max_{\ell|S}\{e_\ell(D)\} < p$, where $S := \mathrm{Supp}(D)$, and put $w = w(D)$. Suppose that $S \in \mathscr{N}_q$ and that for every prime $\ell | S$, $E(\mathbb{F}_\ell)[p]$ is cyclic. We assume that Theorem 4.9 holds for every Darmon-Kolyvagin derivative whose weight is strictly less than w. If $\mathrm{ord}(D) \leq r_q\left(H^1_{f,p}(\mathbb{Q}, E[q])\right)$, then the image of Dz_S in $H^1(\mathbb{Q}(S), T)/q$ is fixed by Γ_S.*

Proof. We write $S = \ell_1 \cdots \ell_s$. It suffices to show that for each $1 \leq i \leq s$,

$$Dz_S \bmod q \in H^0\left(\Gamma_{\ell_i}, H^1(\mathbb{Q}(S), T)/q\right). \tag{4.16}$$

We only need to consider the case $i = 1$. If $e_{\ell_1}(D) = 0$, then we have $D = N_{\ell_1} D'$ for some derivative D', and hence we deduce (4.16). We assume that $e_{\ell_1}(D) \geq 1$. Then, by Lemma 3.1 we have

$$(\sigma_{\ell_1} - 1)D \equiv -\sigma_{\ell_1} D' \mod q\mathbb{Z}[\Gamma_S],$$

where D' is a derivative such that $\mathrm{ord}(D') = \mathrm{ord}(D) - 1$ and $\mathrm{Supp}(D') = S$. Hence, we have

$$w(D') = w(D) - 1.$$

Therefore, by our assumption, Theorem 4.9 holds for D', that is, $D'z_S \equiv 0 \bmod qH^1(\mathbb{Q}(S), T)$. Hence, we obtain

$$(\sigma_{\ell_1} - 1)Dz_S \equiv -\sigma_{\ell_1} D' z_S \equiv 0 \mod q,$$

which shows (4.16). □

Proof of Theorem 4.9. We prove the theorem by induction on $w(D)$. Note that the theorem obviously follows from Proposition 4.7 when $w(D) < 0$. Thus, we may assume that $w := w(D) \geq 0$ and that the theorem holds for every derivative whose weight is strictly less than w. Then, by Lemma 4.12, the image of Dz_S in $H^1(\mathbb{Q}(S), T)/q$ is fixed by Γ_S, and we let $\kappa \in H^1(\mathbb{Q}, E[q])$ be as in Proposition 3.14.

We claim that

$$r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) > 0. \tag{4.17}$$

We assume that $r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) = 0$. By Lemma 4.2 and the exact sequence

$$0 \to H^1_{f,pS'}(\mathbb{Q}, E[q]) \to H^1_{f,p}(\mathbb{Q}, E[q]) \to \oplus_{\ell|S'} E(\mathbb{Q}_\ell)/q,$$

we have

$$r_q\left(H^1_{f,p}(\mathbb{Q}, E[q])\right) \leq r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) + r_p(\oplus_{\ell|S'} E(\mathbb{Q}_\ell)/p),$$

and hence by our assumption,

$$\mathrm{ord}(D) < \sum_{\ell|S'} r_p(E(\mathbb{Q}_\ell)/p).$$

We note that for a prime $\ell \nmid pN$

$$E(\mathbb{Q}_\ell)/p \cong E(\mathbb{Q}_\ell)[p] \cong E(\mathbb{F}_\ell)[p],$$

where the first (non-canonical) isomorphism is due to the structure theorem for finite abelian groups and to that $E(\mathbb{Q}_\ell) \cong \mathbb{Z}_\ell \oplus E(\mathbb{Q}_\ell)_{\mathrm{tors}}$. For a prime $\ell|S$, since $E(\mathbb{F}_\ell)[p]$ is cyclic, we have $r_p(E(\mathbb{Q}_\ell)/p) \leq 1$. Hence,

$$\mathrm{ord}(D) < \sum_{\ell|S'} 1.$$

However, by the definition of $S' = \mathrm{Cond}(D)$, we have $\sum_{\ell|S'} 1 \leq \mathrm{ord}(D)$. Then, we have a contradiction, and hence $r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) > 0$.

By (4.17), there exists a prime ℓ satisfying the conditions (1), (2) and (3) in Lemma 4.10 for Dz_S. Since $\mathrm{ord}(DD^{(1)}_\ell) \leq r_q\left(H^1_{f,p}(\mathbb{Q}, E[q])\right)$ and $w(DD^{(1)}_\ell) = w$, by Lemma 4.12 we have

$$DD^{(1)}_\ell z_{S\ell} \bmod q \in H^0\left(\Gamma_{S\ell}, H^1(\mathbb{Q}(S\ell), T)/q\right).$$

Hence, Lemma 4.11 implies that $Dz_S \equiv 0 \mod q$. □

Remark 4.13. If the localization $\mathrm{loc}_p(\kappa^{(\ell)})$ of $\kappa^{(\ell)}$ at p always belonged to $H^1_f(\mathbb{Q}_p, E[q])$ as in [6, Theorem 4.9], then our proof of Theorem 4.9 would work under the weaker assumption that $\mathrm{ord}(D) < r_q(\mathrm{Sel}(\mathbb{Q}, E[q]))$.

We put $\mathfrak{r}_{\min} = \min_{n\geq 1}\left\{r_{p^n}\left(H^1_{f,p}(\mathbb{Q}, E[p^n])\right)\right\}$.

COROLLARY 4.14. *Let S be an element of $\mathscr{N}$ such that for each prime $\ell|S$, the module $E(\mathbb{F}_\ell)[p]$ is cyclic. Then, we have*

$$\sum_{\sigma\in\Gamma_S} z_S^{\sigma^{-1}}\otimes\sigma\in H^1(\mathbb{Q}(S),T)\otimes_{\mathbb{Z}_p} I_{\Gamma_S,p}^{\min\{\mathfrak{r}_{\min},p\}},$$

where $I_{\Gamma_S,p}$ is the augmentation ideal of $\mathbb{Z}_p[\Gamma_S]$.

Proof. We may assume that $\mathfrak{r}_{\min}\geq 1$. To apply Lemma 3.6 for $H^1(\mathbb{Q}(S),T)$ and z_S, we take a derivative D such that $\mathrm{Supp}(D)=S$ and $\mathrm{ord}(D)<\min\{\mathfrak{r}_{\min},p\}$. We denote by S' the conductor of D, and then $D=D'N_{\frac{S}{S'}}$, where the derivative D' satisfies

$$\mathrm{Supp}(D')=\mathrm{Cond}(D')=S',\quad n(D')=n(D),\quad \mathrm{ord}(D')=\mathrm{ord}(D).$$

Therefore,

$$Dz_S=\left(\prod_{\ell|(S/S')}P_\ell(\mathrm{Fr}_\ell^{-1})\right)D'z_{S'},$$

where ℓ ranges over all the primes dividing S/S'. By definition, if we put $q=n(D')$, which is a power of p, then $S'\in\mathscr{N}_q$. Since

$$\mathrm{ord}(D')=\mathrm{ord}(D)<\mathfrak{r}_{\min}\leq r_q\left(H^1_{f,p}(\mathbb{Q},E[q])\right),\quad \max_{\ell|S'}\{e_\ell(D')\}\leq\mathrm{ord}(D')<p,$$

Theorem 4.9 implies that $D'z_{S'}\equiv 0 \bmod q$, and hence $Dz_S\equiv 0 \bmod q$. Consequently, Lemma 3.6 shows that

$$\sum_{\sigma\in\Gamma_S} z_S^{\sigma^{-1}}\otimes\sigma - N_S z_S\otimes 1\in H^1(\mathbb{Q}(S),T)\otimes I_{\Gamma_S}^{\min\{\mathfrak{r}_{\min},p\}}. \tag{4.18}$$

Since the Galois representation $G_{\mathbb{Q}}\to\mathrm{Aut}_{\mathbb{Z}_p}(T)$ is assumed to be surjective, $E(\mathbb{Q})[p^\infty]=0$, and then the natural map $H^1(\mathbb{Q},E[p^n])\to H^1(\mathbb{Q},E[p^\infty])$ is injective for all $n\geq 1$. Hence, the inductive limit $H^1_{f,p}(\mathbb{Q},E[p^\infty]):=\varinjlim_n H^1_{f,p}(\mathbb{Q},E[p^n])$ is *not* finite, since $\mathfrak{r}_{\min}\geq 1$. By [28, Theorem 2.2.3] (our $H^1_{f,p}(\mathbb{Q},E[p^\infty])$ coincides with $\mathcal{S}_{\Sigma_p}(\mathbb{Q},E[p^\infty])$ in [28]), we have $z_1=0$, and then $N_Sz_S=\prod_{\ell|S}P_\ell(1)z_1=0$. From this and (4.18), we complete the proof. □

4.1.3. *A modification of the theorem.* Let q be a power of p.

THEOREM 4.15. *Let D be a Darmon-Kolyvagin derivative such that $\max_{\ell|S}\{e_\ell(D)\}<p$, where S is the support of D. Suppose that $S\in\mathscr{N}_q$ and that for each prime ℓ dividing S, the module $E(\mathbb{F}_\ell)[q]$ is isomorphic to $\mathbb{Z}/q\mathbb{Z}$ or $\{0\}$. We put $S'=\mathrm{Cond}(D)$ and recall that $A_q(S'):=\oplus_{\ell|S'}E(\mathbb{Q}_\ell)/q$. If $\mathrm{ord}(D)<r_q\left(H^1_{f,pS'}(\mathbb{Q},E[q])\right)+r_p(A_q(S'))$, then*

$$Dz_S\equiv 0 \mod qH^1(\mathbb{Q}(S),T).$$

Remark 4.16. (1) In Theorem 4.9, we do not assume that $E[q]$ is $\mathbb{Z}/q\mathbb{Z}$-free.

(2) By Lemma 4.2, we have

$$r_q(H^1_{f,p}(\mathbb{Q}, E[q])) \leq r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) + r_p(A_q(S')).$$

In particular, if $q = p$, then Theorem 4.15 implies Theorem 4.9.

LEMMA 4.17. *Let D be a Darmon-Kolyvagin derivative such that $\max_{\ell|S}\{e_\ell(D)\} < p$, where S is the support of D. Suppose that the same assumption on S as in Theorem 4.15 holds. We put $w = w(D)$ and $S' = \mathrm{Cond}(D)$, and we assume that Theorem 4.15 holds for every derivative whose weight is strictly less than w. If $\mathrm{ord}(D) \leq r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) + r_p(A_q(S'))$, then the image of Dz_S in $H^1(\mathbb{Q}(S), T)/q$ is fixed by Γ_S.*

Proof. We simply write $H^1_{f,*} = H^1_{f,*}(\mathbb{Q}, E[q])$. Let $S = \ell_1 \cdots \ell_s$ be the prime factorization. We write $D = D_{\ell_1}^{(k_1)} \cdots D_{\ell_s}^{(k_s)}$, and then for each $1 \leq i \leq s$, one of the following assertions holds:

(a) $k_i = 0$.
(b) $k_i \geq 2$.
(c) $k_i = 1$, $\ell_i \in \mathscr{R}_q \setminus \mathscr{R}_{E,q}$, and hence $E(\mathbb{Q}_{\ell_i})/q = 0$.
(d) $k_i = 1$, $\ell_i \in \mathscr{R}_{E,q}$, and hence $E(\mathbb{Q}_{\ell_i})/q \cong \mathbb{Z}/q\mathbb{Z}$.

It suffices to show that for each $1 \leq i \leq s$,

$$Dz_S \bmod q \in H^0\left(\Gamma_{\ell_i}, H^1(\mathbb{Q}(S), T)/q\right). \tag{4.19}$$

Step 1. For each i satisfying (a), (b) or (c) above, the assertion (4.19) holds.

We only need to consider the case $i = 1$. If $k_1 = 0$, then we have $D \in N_{\ell_1}\mathbb{Z}[\Gamma_S]$, and hence $Dz_S \in H^0\left(\Gamma_{\ell_1}, H^1(\mathbb{Q}(S), T)\right)$. Hence, we may assume that $k_1 \geq 1$. Then by Lemma 3.1,

$$(\sigma_{\ell_1} - 1)D \equiv -\sigma_{\ell_1} D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_s}^{(k_s)} \mod q\mathbb{Z}[\Gamma_S]. \tag{4.20}$$

We put $D' = D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_s}^{(k_s)}$. Then,

$$\mathrm{Supp}(D') = S, \quad \mathrm{ord}(D') = \mathrm{ord}(D) - 1,$$

and hence

$$w(D') = w(D) - 1.$$

Since σ_{ℓ_1} generates Γ_{ℓ_1}, by (4.20) it suffices to show that

$$D'z_S \equiv 0 \mod q.$$

We need to consider the cases (b) and (c).

Case (b). In this case, we have $\mathrm{Cond}(D') = S'$. We recall that

$$\mathrm{ord}(D') < \mathrm{ord}(D) \leq r_q(H^1_{f,pS'}) + r_p(A_q(S')).$$

Then, by our assumption, Theorem 4.15 holds for D', that is, $D'z_S \equiv 0 \mod q$.

Case (c). In this case, we have $\mathrm{Cond}(D') = S'/\ell_1$. Since $E(\mathbb{Q}_{\ell_1})/q = 0$, we have

$$r_q(H^1_{f,pS'/\ell_1}) = r_q(H^1_{f,pS'}), \quad r_p(A_q(S'/\ell_1)) = r_p(A_q(S')).$$

Then, we have

$$\mathrm{ord}(D') < r_q(H^1_{f,pS'/\ell_1}) + r_p(A_q(S'/\ell_1)).$$

Hence, Theorem 4.15 holds for D', that is, $D'z_S \equiv 0 \mod q$.

Step 2. We prove the lemma by induction on the number n of primes which divide S and satisfy (d). Without loss of generality, we may write $S = \ell_1 \cdots \ell_s$, where $\ell_1, \ell_2, \dots, \ell_n$ satisfy (d) and $\ell_{n+1}, \ell_{n+2}, \dots, \ell_s$ satisfy (a), (b) or (c).

The case $n = 0$. This case follows from Step 1.

The case $n \geq 1$. By Step 1, we are reduced to showing that for $1 \leq i \leq n$

$$Dz_S \bmod q \in H^0\left(\Gamma_{\ell_i}, H^1(\mathbb{Q}(S), T)/q\right).$$

It suffices to consider the case $i = 1$. Let $S_1 = S/\ell_1$ and $D_{S_1} = D_{\ell_2}^{(k_2)} \cdots D_{\ell_s}^{(k_s)}$. Then, we have

$$(\sigma_{\ell_1} - 1)Dz_S \equiv -N_{\ell_1} D_{S_1} z_S \equiv -P_{\ell_1}(\mathrm{Fr}_{\ell_1}^{-1}) D_{S_1} z_{S_1} \mod q. \tag{4.21}$$

By Lemma 4.4,

$$\begin{aligned}\mathrm{ord}(D_{S_1}) = \mathrm{ord}(D) - 1 &\leq r_q(H^1_{f,pS'}) + r_p(A(S')) - 1 \\ &\leq r_q(H^1_{f,pS'/\ell_1}) + r_p(A(S'/\ell_1)).\end{aligned}$$

We recall that $\mathrm{Cond}(D_{S_1}) = S'/\ell_1$. Since $\ell_1 \in \mathscr{R}_{E,q}$, we have $w(D_{S_1}) = w(D) = w$. Therefore, we may apply the induction hypothesis on n to D_{S_1}, and then

$$D_{S_1} z_{S_1} \bmod q \in H^0\left(\Gamma_{S_1}, H^1(\mathbb{Q}(S_1), T)/q\right).$$

Hence, we have

$$P_{\ell_1}(\mathrm{Fr}_{\ell_1}^{-1}) D_{S_1} z_{S_1} \equiv P_{\ell_1}(1) D_{S_1} z_{S_1} \equiv 0 \mod q.$$

Thus, by (4.21) we complete Step 2. □

Proof of Theorem 4.15. As in the proof of Theorem 4.9, Theorem 4.15 is proved by induction on $w(D)$. By Lemma 4.17, $Dz_S \bmod q \in H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), T)/q\right)$. Let κ be as in Proposition 3.14. Since $\mathrm{ord}(D) < r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) + r_p(A_q(S'))$, by the same argument as that in the proof of Theorem 4.9, we have $r_q(H^1_{f,pS'}(\mathbb{Q}, E[q])) > 0$. Hence, by Lemma 4.10 there exists a prime ℓ satisfying the conditions (1), (2) and (3) in Lemma 4.10 for Dz_S. Using (4.3), we have

$$\mathrm{ord}(DD_\ell^{(1)}) \leq r_q\left(H^1_{f,pS'\ell}(\mathbb{Q}, E[q])\right) + r_p(A_q(S'\ell)).$$

Since $\mathrm{Cond}(DD_\ell^{(1)}) = S'\ell$, by Lemma 4.17 we have

$$DD_\ell^{(1)} z_{S\ell} \bmod q \in H^0\left(\Gamma_{S\ell}, H^1(\mathbb{Q}(S\ell), T)/q\right).$$

Then, Lemma 4.11 implies that $Dz_S \equiv 0 \mod q$. □

4.2. **Local properties of derivatives of Euler systems at p.** In this subsection, we study relations between the localization of derivatives of Euler systems at p and arithmetic invariants such as the Tate-Shafarevich group (cf. Corollary 4.20).

We put $r_E = \mathrm{rank}(E(\mathbb{Q}))$ and denote by Ш the Tate-Shafarevich group of E over $\mathbb{Q}$. For a finte extension K of $\mathbb{Q}$, we put $H^1(K \otimes \mathbb{Q}_p, -) = \oplus_{\lambda|p} H^1(K_\lambda, -)$, where λ ranges over all the primes of K dividing p. For $M = T_p(E), V_p(E)$ or $E[p^n]$, we define

$$H^1_f(K \otimes \mathbb{Q}_p, M) = \oplus_{\lambda|p} H^1_f(K_\lambda, M), \quad H^1_{/f}(K \otimes \mathbb{Q}_p, M) = \oplus_{\lambda|p} H^1_{/f}(K_\lambda, M).$$

For $\eta \in H^1(K, A)$, we denote by $\mathrm{loc}_p(\eta)$ (resp. $\mathrm{loc}_{/f,p}(\eta)$) the image of η in $H^1(K \otimes \mathbb{Q}_p, A)$ (resp. $H^1_{/f}(K \otimes \mathbb{Q}_p, A)$).

THEOREM 4.18. *Suppose that Assumption 4.8 holds and that $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$. Let D be a Darmon-Kolyvagin derivative such that $\max_{\ell|S}\{e_\ell(D)\} < p$, where $S := \mathrm{Supp}(D)$. Suppose that $S \in \mathscr{N}_p$ and that for each prime $\ell|S$, the module $E(\mathbb{F}_\ell)[p]$ is cyclic. We put $S' = \mathrm{Cond}(D)$. If $\mathrm{ord}(D) < r_p\left(H^1_{f,S'}(\mathbb{Q}, E[p])\right) + r_p(A_p(S'))$, then the following assertions hold.*

(1) *The image of Dz_S in $H^1(\mathbb{Q}(S), T)/p$ is fixed by Γ_S.*
(2) *If we let $\kappa \in H^1(\mathbb{Q}, E[p])$ be as in Proposition 3.14 ($q = p$), then*

$$\mathrm{loc}_p(\kappa) \in H^1_f(\mathbb{Q}_p, E[p]).$$

Remark 4.19. For an odd prime $p \nmid N$, the assertion that $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$ is implied by the assertion that $p \nmid |E(\mathbb{F}_p)|$. This implication is proved as follows. If p is an odd prime relatively prime to N, then there exits an exact sequence $0 \to \hat{E}(\mathbb{Z}_p) \to E(\mathbb{Q}_p) \to E(\mathbb{F}_p) \to 0$, where $\hat{E}$ is the formal group over $\mathbb{Z}_p$ attached to E, and $\hat{E}(\mathbb{Z}_p) \cong \mathbb{Z}_p$. Hence, by the exact sequence, if $p \nmid |E(\mathbb{F}_p)|$, then $E(\mathbb{Q}_p)/p = \hat{E}(\mathbb{Z}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. (1) We write $H^1_{f,*} = H^1_{f,*}(\mathbb{Q}, E[p])$. Since $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$, by the exact sequence

$$0 \to H^1_{f,pS'} \to H^1_{f,S'} \to E(\mathbb{Q}_p)/p, \tag{4.22}$$

we have $r_p\left(H^1_{f,S'}\right) \leq r_p\left(H^1_{f,pS'}\right) + 1$, and then the assertion (1) follows from Lemma 4.17.

(2) If $r_p\left(H^1_{f,S'}\right) = r_p\left(H^1_{f,pS'}\right)$, then by Theorem 4.15, $Dz_S \equiv 0 \bmod pH^1(\mathbb{Q}(S), T)$, and hence $\kappa = 0$. We may assume that $r_p\left(H^1_{f,S'}\right) = r_p\left(H^1_{f,pS'}\right) + 1$. Then, by (4.22) the map $H^1_{f,S'} \to E(\mathbb{Q}_p)/p$ is surjective. Since the pairing

$$(-,-)_p : E(\mathbb{Q}_p)/p \times H^1_{/f}(\mathbb{Q}_p, E[p]) \to \mathbb{Z}/p\mathbb{Z}$$

is perfect, it suffices to show that

$$(c, \kappa)_p = 0 \quad \text{for } c \in E(\mathbb{Q}_p)/p.$$

We take an element $c \in E(\mathbb{Q}_p)/p$. Since $H^1_{f,S'} \to E(\mathbb{Q}_p)/p$ is surjective, there exists an element $\eta \in H^1_{f,S'}$ whose localization at p coincides with c. Then, by the Hasse principle,

$$(c, \kappa)_p = (\eta, \kappa)_p = -\sum_{w \nmid p : \mathrm{prime}} (\eta, \kappa)_w.$$

By the definition of $H^1_{f,S'}(\mathbb{Q}, E[p])$ and Corollary 3.15 for κ, we have $(\eta, \kappa)_w = 0$ for $w \nmid p$. Hence $(c, \kappa)_p = 0$. □

COROLLARY 4.20. *We assume Assumption 4.8, $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$ and $p \geq r_E$. Let D be a Darmon-Kolyvagin derivative and S its support. We suppose that $S \in \mathscr{N}_p$ and that $E(\mathbb{F}_\ell)[p]$ is cyclic for each prime $\ell | S$. If $\mathrm{ord}(D) = r_E$ and $\mathrm{loc}_{/f,p}(Dz_S \bmod p) \neq 0$, then we have*

(1) $Ш[p] = 0$,
(2) *the natural map $E(\mathbb{Q})/p \to \oplus_{\ell|S} E(\mathbb{Q}_\ell)/p$ is surjective.*

Proof. We put $S' = \mathrm{Cond}(D)$. Since $\mathrm{loc}_p(Dz_S \bmod p) \notin H^1_f(\mathbb{Q}(S) \otimes \mathbb{Q}_p, E[p])$, Theorem 4.18 implies that

$$r_E \geq r_p(H^1_{f,S'}) + r_p(A(S')).$$

On the other hand, by Lemma 4.2 we have

$$r_p(H^1_{f,S'}) + r_p(A(S')) \geq r_p(\mathrm{Sel}(\mathbb{Q}, E[p])),$$

and then

$$r_E = r_p(H^1_{f,S'}) + r_p(A(S')) = r_p(\mathrm{Sel}(\mathbb{Q}, E[p])). \tag{4.23}$$

This implies that $Ш[p] = 0$ and that the sequence

$$0 \to H^1_{f,S'} \to E(\mathbb{Q})/p \to \oplus_{\ell|S'} E(\mathbb{Q}_\ell)/p \to 0$$

is exact. Hence, it suffices to show that $E(\mathbb{Q}_\ell)/p = 0$ for every prime ℓ dividing S/S'. We assume that $E(\mathbb{Q}_\ell)/p \cong \mathbb{Z}/p\mathbb{Z}$ for some ℓ dividing S/S'. Since $\ell \nmid S'$, we have $D = N_\ell D'$, where D' is a derivative such that $\mathrm{Supp}(D') = S/\ell$ and $\mathrm{ord}(D') = r_E$. We claim that

$$\mathrm{loc}_{/f,p}(D' z_{S/\ell} \bmod p) \in H^0\left(\Gamma_{S/\ell}, H^1_{/f}\left(\mathbb{Q}(S/\ell) \otimes \mathbb{Q}_p, E[p]\right)\right). \tag{4.24}$$

Let ℓ' be a prime dividing S/ℓ. If $e_{\ell'}(D') = 0$, then $D' \in N_{\ell'}\mathbb{Z}[\Gamma_{S/\ell}]$, and hence we have $\mathrm{loc}_p(D' z_{S/\ell} \bmod p) \in H^0\left(\Gamma_{\ell'}, H^1_{/f}\left(\mathbb{Q}(S/\ell) \otimes \mathbb{Q}_p, E[p]\right)\right)$. We assume that $e_{\ell'}(D') \geq 1$. Then, we have $(\sigma_{\ell'} - 1)D' \equiv -\sigma_{\ell'} D'' \bmod p$, where D'' is a derivative with support S/ℓ satisfying $\mathrm{ord}(D'') = r_E - 1$. If we put $S'' = \mathrm{Cond}(D'')$, then by Lemma 4.2, we have

$$r_E - 1 < r_p(\mathrm{Sel}(\mathbb{Q}, E[p])) \leq r_p(H^1_{f,S''}) + r_p(A_p(S'')).$$

Hence, Theorem 4.18 implies that $\mathrm{loc}_{/f,p}(D'' z_{S/\ell} \bmod p) = 0$, and then

$$\mathrm{loc}_{/f,p}(D' z_{S/\ell} \bmod p) \in H^0(\Gamma_{\ell'}, H^1_{/f}(\mathbb{Q}(S/\ell) \otimes \mathbb{Q}_p, E[p])).$$

Therefore, we deduce (4.24).

By (4.24), in $H^1_{/f}(\mathbb{Q}(S) \otimes \mathbb{Q}_p, E[p]))$,

$$\mathrm{loc}_{/f,p}(Dz_S) = \mathrm{loc}_{/f,p}(N_\ell D' z_S) = P_\ell(\mathrm{Fr}_\ell^{-1})\mathrm{loc}_{/f,p}(D' z_{S/\ell}) = P_\ell(1)\mathrm{loc}_{/f,p}(D' z_{S/\ell}) = 0.$$

Then, we have a contradiction. □

4.3. **Rational points from derivatives of Euler systems.** In this subsection, we show that if a certain derivative of an Euler system is not divisible by p, then it gives a $\mathbb{Q}$-rational point of E. We assume that $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$ and that the natural map $E(\mathbb{Q})/p \to E(\mathbb{Q}_p)/p$ is surjective. Then, the localization map $\mathrm{Sel}(\mathbb{Q}, E[p]) \to E(\mathbb{Q}_p)/p$ is also surjective, and hence

$$r_p\left(H^1_{f,p}(\mathbb{Q}, E[p])\right) = r_p\left(\mathrm{Sel}(\mathbb{Q}, E[p])\right) - 1.$$

We put $C_p = \ker\left(E(\mathbb{Q})/p \to E(\mathbb{Q}_p)/p\right)$. Then, we have

$$r_p(C_p) = r_E - 1. \tag{4.25}$$

By applying the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/p & \longrightarrow & \mathrm{Sel}(\mathbb{Q}, E[p]) & \longrightarrow & Ш[p] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(\mathbb{Q}_p)/p & \longrightarrow & E(\mathbb{Q}_p)/p & \longrightarrow & 0 & \longrightarrow & 0, \end{array}$$

we have an exact sequence

$$0 \to C_p \to H^1_{f,p}(\mathbb{Q}, E[p]) \to Ш[p] \to 0. \tag{4.26}$$

THEOREM 4.21. *Assume Assumption 4.8, $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$ and $p \geq r_E$. We also assume that the map $E(\mathbb{Q})/p \to E(\mathbb{Q}_p)/p$ is surjective. Let D be a Darmon-Kolyvagin derivative and S its support. Suppose that $S \in \mathscr{N}_p$ and that for each prime $\ell | S$, $E(\mathbb{F}_\ell)[p]$ is cyclic. If $\mathrm{ord}(D) = r_E - 1$ and $Dz_S \not\equiv 0 \bmod pH^1(\mathbb{Q}(S), T)$, then the following assertions hold.*

1. $Ш[p] = 0$.
2. *The localization map $H^1_{f,p}(\mathbb{Q}, E[p]) \to \oplus_{\ell|S} E(\mathbb{Q}_\ell)/p$ is surjective.*
3. *The image of Dz_S in $H^1(\mathbb{Q}(S), T)/p$ is fixed by Γ_S.*
4. *If $\kappa \in H^1(\mathbb{Q}, E[p])$ denotes the inverse image of $Dz_S \bmod p$ under the isomorphism $H^1(\mathbb{Q}, E[p]) \cong H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), E[p])\right)$, then*

$$\kappa \in E(\mathbb{Q})/p,$$

which gives a non-trivial $\mathbb{Q}$-rational point of E modulo p.

Remark 4.22. For Heegner points, a similar result is obtained in [6, Proposition 5.10], where K-rational points are considered for imaginary quadratic fields K.

Proof. (1) Since $Dz_S \not\equiv 0 \bmod p$, Theorem 4.9 implies that $r_E - 1 \geq r_p(H^1_{f,p})$. Hence, by (4.25) and (4.26), we have $r_p(H^1_{f,p}) = r_E - 1$, and then $Ш[p] = 0$.

(2) Since $\mathrm{ord}(D) = r_p(H^1_{f,p})$ and $Dz_S \not\equiv 0 \bmod p$, Theorem 4.15 implies that

$$r_p(H^1_{f,p}) \geq r_p(H^1_{f,pS'}) + r_p(A_p(S')).$$

Hence, the sequence

$$0 \to H^1_{f,pS'} \to H^1_{f,p} \to \oplus_{\ell|S'} E(\mathbb{Q}_\ell)/p \to 0 \tag{4.27}$$

is exact. In order to deduce the assertion (2), it suffices to show that $E(\mathbb{Q}_\ell)/p = 0$ for every prime ℓ dividing S/S'. We assume that $E(\mathbb{Q}_\ell)/p \cong \mathbb{Z}/p\mathbb{Z}$ for some prime ℓ dividing S/S'. Since $\ell \nmid S'$, we have $D = N_\ell D'$, where D' is a derivative such that

$$\mathrm{Supp}(D') = S/\ell, \quad \mathrm{Cond}(D') = \mathrm{Cond}(D), \quad \mathrm{ord}(D') = \mathrm{ord}(D) = r_E - 1.$$

Lemma 4.12 implies that $D' z_{S/\ell} \in H^0\left(\Gamma_{S/\ell}, H^1(\mathbb{Q}(S/\ell), T)/p\right)$, and hence

$$Dz_S = N_\ell D' z_S = P_\ell(\mathrm{Fr}_\ell^{-1}) D' z_{S/\ell} \equiv P_\ell(1) D' z_{S/\ell} \equiv 0 \mod pH^1(\mathbb{Q}(S), T).$$

Hence, we obtain a contradiction.

(3) This assertion follows from Lemma 4.12.

(4) By the assertion (1), it suffices to show that $\kappa \in \mathrm{Sel}(\mathbb{Q}, E[p])$. By Corollary 3.15, we are reduced to showing that $\mathrm{loc}_\ell(\kappa) \in H^1_f(\mathbb{Q}_\ell, E[p])$ for every prime $\ell | pS'$. By taking the Pontryagin dual of (4.27), the induced map

$$\varphi : \bigoplus_{\ell | S'} H^1_{/f}(\mathbb{Q}_\ell, E[p]) \to \mathrm{Hom}\left(H^1_{f,p}(\mathbb{Q}, E[p]), \mathbb{Z}/p\mathbb{Z}\right), \ (g_\ell)_\ell \mapsto \left(\eta \mapsto \sum_{\ell | S'} (g_\ell, \eta)_\ell\right)$$

is injective. We claim that the image of κ in $\oplus_{\ell | S'} H^1_{/f}(\mathbb{Q}_\ell, E[p])$ belongs to the kernel of the map above. Indeed, if we take an element $\eta \in H^1_{f,p}(\mathbb{Q}, E[p])$, then by the Hasse principle,

$$\sum_{\ell | S'} (\kappa, \eta)_\ell = -\sum_{v \nmid S'} (\kappa, \eta)_v = -(\kappa, \eta)_p = 0,$$

where the second equality follows from Corollary 3.15, and the last equality follows from the definition of $H^1_{f,p}(\mathbb{Q}, E[p])$. Since the map φ is injective, $\mathrm{loc}_\ell(\kappa) \in H^1_f(\mathbb{Q}_\ell, E[p])$ for $\ell | S'$. In addition, by Theorem 4.18 we have $\mathrm{loc}_p(\kappa) \in H^1_f(\mathbb{Q}_p, E[p])$. Therefore, $\kappa \in \mathrm{Sel}(\mathbb{Q}, E[p])$. □

5. p-ADIC PROPERTIES OF MAZUR-TATE ELEMENTS

The aim of this section is to show that if we extend coefficients to $\mathbb{Z}_p$, then the order of vanishing of Mazur-Tate elements is greater than or equal to the corank of the Selmer group (see Theorem 5.17 for the precise statement). We fix a global minimal Weierstrass model of E over $\mathbb{Z}$, and denote by ω the Néron differential. Then, let $\Omega^\pm$ be the period as in Section 2.

5.1. **Preliminaries on group rings.** Let R be a proper subring of $\mathbb{Q}$. For a finite abelian group G and a prime p, we denote by I_G (resp. $I_{G,p}$) the augmentation ideal of $R[G]$ (resp. $\mathbb{Z}_p[G]$). We note that for a prime p which is not invertible in R, we have $R \subseteq \mathbb{Z}_p$, and then $I_{G,p} = \mathbb{Z}_p \otimes_{\mathbb{Z}} I_G = \mathbb{Z}_p \otimes_R I_G$.

LEMMA 5.1. *Let α be an element of $R[G]$. For a positive integer t, the following conditions are equivalent*:

(1) $\alpha \in I_G^t$,
(2) $\alpha \in \mathbb{Z}_p \otimes_{\mathbb{Z}} I_G^t$ *for all primes p which are not invertible in R.*

Proof. This is [6, Lemma 3.2]. □

In the following, let p be a prime and G a finite abelian group.

LEMMA 5.2. *If $\sigma \in G$ is an element whose order is relatively prime to p, then $\sigma - 1 \in I_{G,p}^t$ for $t \geq 1$. In particular, if the order of G is relatively prime to p, then $I_{G,p} = I_{G,p}^2 = I_{G,p}^3 = \cdots$.*

Proof. This is [6, Lemma 3.4]. □

LEMMA 5.3. *Suppose that we are given a decomposition $G = K \times H$ with $p \nmid |H|$. Let α be an element of $\mathbb{Z}_p[G]$. Let α_K denote the image of α under the map $\mathbb{Z}_p[G] \to \mathbb{Z}_p[K]$ induced by the projection $G \to K$. If $\alpha_K \in I_{K,p}^t$ for some $t \geq 1$, then $\alpha \in I_{G,p}^t$.*

Proof. By the natural inclusion $\mathbb{Z}_p[K] \hookrightarrow \mathbb{Z}_p[G]$, we regard α_K as an element of $\mathbb{Z}_p[G]$. Then, we have

$$\alpha - \alpha_K \in \ker(\mathbb{Z}_p[G] \to \mathbb{Z}_p[K]) = \mathbb{Z}_p[K] \otimes_{\mathbb{Z}_p} I_{H,p}.$$

Lemma 5.2 implies that $\mathbb{Z}_p[K] \otimes I_{H,p} = \mathbb{Z}_p[K] \otimes I_{H,p}^t$. Hence, by the assumption that $\alpha_K \in I_{K,p}^t$, we have $\alpha \in I_{G,p}^t$. □

LEMMA 5.4. *Under the same notation and assumption as in Lemma 5.3, we denote by $\tilde{\alpha}^{(p)}$ (resp. $\tilde{\alpha}_K^{(p)}$) the image of α (resp. α_K) in $\mathbb{Z}/p\mathbb{Z} \otimes I_{G,p}^t / I_{G,p}^{t+1}$ (resp. $\mathbb{Z}/p\mathbb{Z} \otimes I_{K,p}^t / I_{K,p}^{t+1}$). If $\tilde{\alpha}_K^{(p)} = 0$, then $\tilde{\alpha}^{(p)} = 0$.*

Proof. As in the poof of Lemma 5.3, we have

$$\alpha - \alpha_K \in \mathbb{Z}_p[K] \otimes I_{H,p}^t = \mathbb{Z}_p[K] \otimes I_{H,p}^{t+1} \subseteq I_{G,p}^{t+1}.$$

Then, the image $\tilde{\alpha}^{(p)} - \tilde{\alpha}_K^{(p)}$ in $\mathbb{Z}/p\mathbb{Z} \otimes I_{G,p}^t / I_{G,p}^{t+1}$ is trivial, where we regard $\tilde{\alpha}_K^{(p)}$ as an element of $\mathbb{Z}/p\mathbb{Z} \otimes I_{G,p}^t / I_{G,p}^{t+1}$ under the natural map induced by the inclusion $K \subseteq G$. Since $\tilde{\alpha}_K^{(p)} = 0$, we deduce that $\tilde{\alpha}^{(p)} = 0$. □

5.2. **Construction of a system of local points.** With a modification of ideas of [13], [14] and [25], we construct local points of E to connect Kato's Euler system with Mazur-Tate elements.

In the rest of Section 5, we fix a prime p such that $p \nmid 6N \cdot |E(\mathbb{F}_p)|$. For a positive integer S, let $\mathbb{Q}(S)$ and Γ_S be as in Section 3. Let $\mathscr{O}_S$ denote the ring of integers of $\mathbb{Q}(S)$. If we put $H_S = \mathrm{Gal}(\mathbb{Q}(\mu_S)/\mathbb{Q}(S))$, then we have the canonical decomposition $G_S = H_S \times \Gamma_S$. Let σ denote the arithmetic Frobenius at p. We denote by $\hat{E}$ the formal group law of E over $\mathbb{Z}_p$ (associated to ω) and by $\log_{\hat{E}}$ the logarithm of $\hat{E}$. Since p is odd, if $\mathscr{O}_K$ is the ring of integers of a finite unramified extension K of $\mathbb{Q}_p$, then $\log_{\hat{E}}$ induces an isomorphism $\hat{E}(\mathscr{O}_K) \to p\mathscr{O}_K$.

LEMMA 5.5. *We suppose that K is a finite unramified p-extension of $\mathbb{Q}_p$. Then, we have an isomorphism of $\mathbb{Z}_p$-modules defined as*

$$\hat{E}(\mathscr{O}_K) \to \mathscr{O}_K, \quad c \mapsto \left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) \log_{\hat{E}}(c).$$

Proof. Since $\log_{\hat{E}} : \hat{E}(\mathscr{O}_K) \to p\mathscr{O}_K$ is an isomorphism, it suffices to show that the homomorphism of $\mathbb{Z}_p$-modules $\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) : p\mathscr{O}_K \to \mathscr{O}_K$ is an isomorphism. We put $d = [K : \mathbb{Q}_p]$, which is a power of p.

We first assume that p is a good ordinary prime of E, that is, $p \nmid a_p$. Let $\alpha \in \mathbb{Z}_p^\times$ be the unit root of $X^2 - a_p X + p$ and $\beta \in p\mathbb{Z}_p$ the other root. Then we have

$$\left(1 - \frac{\sigma}{\alpha}\right)\left(1 - \frac{\sigma}{\beta}\right) = \left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right). \tag{5.1}$$

Since $p \nmid |E(\mathbb{F}_p)|$, we have $a_p \not\equiv 1 \bmod p$, and hence $\alpha \not\equiv 1 \bmod p$. We note that since d is a power of p, $\alpha^d - 1 \in \mathbb{Z}_p^\times$. For $A \in \mathscr{O}$, if we put

$$x_A = \frac{\alpha^d}{\alpha^d - 1}\left(\sum_{0 \le k \le d-1} \frac{A^{\sigma^k}}{\alpha^k}\right) \in \mathscr{O},$$

then

$$\left(1 - \frac{\sigma}{\alpha}\right) x_A = A.$$

Since $\beta \in p\mathbb{Z}_p$, the series $y_A := -\sum_{k \ge 1} \beta^k x_A^{\sigma^{-k}} \in p\mathscr{O}$ converges, and it satisfies

$$\left(1 - \frac{\sigma}{\beta}\right) y_A = x_A.$$

By (5.1), we have

$$\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) y_A = A.$$

Hence, the homomorphism of $\mathbb{Z}_p$-modules $\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) : p\mathscr{O} \to \mathscr{O}$ is surjective, and then it is an isomorphism.

We next assume that p is a good supersingular prime of E. Since $p \ge 5$, we have $a_p = 0$. For $A \in \mathscr{O}$, if we put $y_A = -\sum_{k \ge 1} (-p)^k A^{\sigma^{-2k}}$, then

$$\left(1 + \frac{1}{p}\sigma^2\right) y_A = A.$$

Hence, the homomorphism $\left(1 + \frac{1}{p}\sigma^2\right) : p\mathscr{O} \to \mathscr{O}$ is surjective, and then it is an isomorphism. □

For an integer S, we have $\mathscr{O}_S \otimes_{\mathbb{Z}} \mathbb{Z}_p = \prod_{\lambda | p} \mathscr{O}_{S,\lambda}$, where λ ranges over all the primes of $\mathbb{Q}(S)$ dividing p, and $\mathscr{O}_{S,\lambda}$ denotes the completion of $\mathscr{O}_S$ at λ. Hence, $\hat{E}(\mathscr{O}_S \otimes \mathbb{Z}_p) = \oplus_{\lambda | p} \hat{E}(\mathscr{O}_{S,\lambda})$, and then the logarithm $\log_{\hat{E}}$ naturally induces an isomorphism $\hat{E}(\mathscr{O}_S \otimes \mathbb{Z}_p) \to p\mathscr{O}_S \otimes \mathbb{Z}_p$.

Definition 5.6. For a square-free integer S relatively prime to p, we define a local point $c_S \in \hat{E}\left(\mathscr{O}_S \otimes \mathbb{Z}_p\right)$ by

$$\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) \log_{\hat{E}}(c_S) = \mathrm{tr}_{\mathbb{Q}(\zeta_S)/\mathbb{Q}(S)}\left(\zeta_S\right) \in \mathscr{O}_S \otimes \mathbb{Z}_p, \tag{5.2}$$

where we note that Lemma 5.5 shows the well-definedness of c_S.

PROPOSITION 5.7. *Let ℓ be a prime not dividing pS. Then, we have*

$$\mathrm{Tr}_{S\ell/S}(c_{S\ell}) = -c_S^{\mathrm{Fr}_\ell^{-1}},$$

where $\mathrm{Tr}_{S\ell/S} : \hat{E}(\mathscr{O}_{S\ell} \otimes \mathbb{Z}_p) \to \hat{E}(\mathscr{O}_S \otimes \mathbb{Z}_p)$ is the trace map with respect to the addition of $\hat{E}$.

Proof. By Lemma 5.5, it suffices to show that

$$\mathrm{tr}_{\mathbb{Q}(S\ell)/\mathbb{Q}(S)} \circ \mathrm{tr}_{\mathbb{Q}(\zeta_{S\ell})/\mathbb{Q}(S\ell)} (\zeta_{S\ell}) = -\mathrm{tr}_{\mathbb{Q}(\zeta_S)/\mathbb{Q}(S)} \left(\zeta_S^{\mathrm{Fr}_\ell^{-1}}\right).$$

Since $\mathrm{tr}_{\mathbb{Q}(S\ell)/\mathbb{Q}(S)} \circ \mathrm{tr}_{\mathbb{Q}(\zeta_{S\ell})/\mathbb{Q}(S\ell)} = \mathrm{tr}_{\mathbb{Q}(\zeta_S)/\mathbb{Q}(S)} \circ \mathrm{tr}_{\mathbb{Q}(\zeta_{S\ell})/\mathbb{Q}(\zeta_S)}$, we are reduced to showing that $\mathrm{tr}_{\mathbb{Q}(\zeta_{S\ell})/\mathbb{Q}(\zeta_S)}(\zeta_{S\ell}) = -\zeta_S^{\mathrm{Fr}_\ell^{-1}}$, which is not difficult to show. □

PROPOSITION 5.8. *Let χ be a character of Γ_S. Then, we have*

$$\left(1 - \frac{a_p}{p}\chi(p)^{-1} + \frac{1}{p}\chi(p)^{-2}\right) \sum_{\delta \in \Gamma_S} \log_{\hat{E}}(c_S^\delta)\chi(\delta) = \tau_S(\chi).$$

On the right hand side, we regard χ as a character of $G_S = \Gamma_S \times H_S$ by $\chi|_{H_S} = 1$.

Proof. By (5.2), we have

$$\begin{aligned}\sum_{\delta \in \Gamma_S} \delta \left(\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) \log_{\hat{E}}(c_S)\right) \chi(\delta) &= \sum_{\delta \in \Gamma_S} \delta \left(\mathrm{tr}_{\mathbb{Q}(\mu_S)/\mathbb{Q}(S)}(\zeta_S)\right) \chi(\delta) \\ &= \sum_{\gamma \in G_S} \zeta_S^\gamma \chi(\gamma) = \tau_S(\chi). \end{aligned} \tag{5.3}$$

On the other hand, we have

$$\begin{aligned}&\sum_{\delta \in \Gamma_S} \delta \left(\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) \log_{\hat{E}}(c_S)\right) \chi(\delta) \\ &= \sum_\delta \log_{\hat{E}}(c_S^\delta)\chi(\delta) - \frac{a_p}{p}\sum_\delta \log_{\hat{E}}(c_S^{\sigma\delta})\chi(\delta) + \frac{1}{p}\sum_\delta \log_{\hat{E}}(c_S^{\sigma^2\delta})\chi(\delta) \\ &= \sum_\delta \log_{\hat{E}}(c_S^\delta)\chi(\delta) - \frac{a_p}{p}\sum_\delta \log_{\hat{E}}(c_S^\delta)\chi(\sigma^{-1}\delta) + \frac{1}{p}\sum_\delta \log_{\hat{E}}(c_S^\delta)\chi(\sigma^{-2}\delta) \\ &\overset{\text{(a)}}{=} \sum_\delta \log_{\hat{E}}(c_S^\delta)\chi(\delta) - \frac{a_p}{p}\chi(p)^{-1}\sum_\delta \log_{\hat{E}}(c_S^\delta)\chi(\delta) + \frac{1}{p}\chi(p)^{-2}\sum_\delta \log_{\hat{E}}(c_S^\delta)\chi(\delta) \\ &= \left(1 - \frac{a_p}{p}\chi(p)^{-1} + \frac{1}{p}\chi(p)^{-2}\right)\sum_\delta \log_{\hat{E}}(c_S^\delta)\chi(\delta), \end{aligned} \tag{5.4}$$

where the equality (a) follows from $\chi(\sigma) = \chi(p)$. Combining (5.3) and (5.4), we complete the proof. □

5.3. **Kato's Euler system.** We keep the same notation as in Subsection 5.2. As in Section 3, we put $T = T_p(E)$ and $V = T \otimes \mathbb{Q}_p$. We assume that $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T)$ is surjective.

We first recall the definition of the dual exponential map. For an integer $S > 0$, we have the following pairings $(-,-)$ induced by the cup product and the Weil paring:

$$(-,-) : H^1_f(\mathbb{Q}(S) \otimes \mathbb{Q}_p, V) \times H^1_{/f}(\mathbb{Q}(S) \otimes \mathbb{Q}_p, V) \to \oplus_{\lambda | S} \mathbb{Q}_p \to \mathbb{Q}_p,$$

where the last map is given by $(a_\lambda)_\lambda \mapsto \sum_\lambda a_\lambda$. By taking the $\mathbb{Q}_p$-dual, we have a $\mathbb{Q}_p$-linear map as the composite

$$H^1(\mathbb{Q}(S) \otimes \mathbb{Q}_p, V) \to H^1_{/f}(\mathbb{Q}(S) \otimes \mathbb{Q}_p, V) \to \mathrm{Hom}_{\mathbb{Q}_p}\left(H^1_f(\mathbb{Q}(S) \otimes \mathbb{Q}_p, V), \mathbb{Q}_p\right). \tag{5.5}$$

Since the exponential map $\exp_{\hat{E}}$ of $\hat{E}$ induces an isomorphism

$$\mathbb{Q}(S) \otimes_{\mathbb{Q}} \mathbb{Q}_p \to H^1_f(\mathbb{Q}(S) \otimes \mathbb{Q}_p, V),$$

by taking its dual, we have a $\mathbb{Q}_p$-linear map

$$\mathrm{Hom}_{\mathbb{Q}_p}\left(H^1_f(\mathbb{Q}(S) \otimes \mathbb{Q}_p, V), \mathbb{Q}_p\right) \to \mathrm{Hom}_{\mathbb{Q}_p}(\mathbb{Q}(S) \otimes \mathbb{Q}_p, \mathbb{Q}_p) \cong \mathbb{Q}(S) \otimes \mathbb{Q}_p, \tag{5.6}$$

where the last isomorphism comes from the perfect pairing $(\mathbb{Q}(S) \otimes \mathbb{Q}_p) \times (\mathbb{Q}(S) \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$ given by $(x,y) \mapsto \mathrm{tr}_{\mathbb{Q}(S)/\mathbb{Q}}(xy)$. The *dual exponential map* (associated to ω)

$$\exp^*_S : H^1(\mathbb{Q}(S) \otimes \mathbb{Q}_p, V) \to \mathbb{Q}(S) \otimes \mathbb{Q}_p$$

is defined as the composite of (5.5) and (5.6). We note that the paring $(-,-)$ induces the paring

$$(-,-) : H^1_f(\mathbb{Q}(S) \otimes \mathbb{Q}_p, T) \times H^1_{/f}(\mathbb{Q}(S) \otimes \mathbb{Q}_p, T) \to \mathbb{Z}_p \tag{5.7}$$

and that for $c \in \hat{E}(\mathscr{O}_S \otimes \mathbb{Z}_p)$ and $z \in H^1(\mathbb{Q}(S) \otimes \mathbb{Q}_p, T)$,

$$(c, z) = \mathrm{tr}_{\mathbb{Q}(S)/\mathbb{Q}}\left(\log_{\hat{E}}(c) \cdot \exp^*_S(z)\right) \in \mathbb{Z}_p. \tag{5.8}$$

Let $\mathscr{N}$ be the set of square-free products of primes relatively prime to pN. By applying [28, Lemma 9.6.1] to Kato's Euler system (cf. [11, Theorems 9.7 and 12.5]), we have the following.

THEOREM 5.9 (Kato). *There exists a system $\{\mathfrak{z}_m\}_{m>0} \in \prod_m H^1(\mathbb{Q}(m), T)$ satisfying the following conditions.*

(1) *For $m > 0$ and a prime ℓ, we have*

$$\mathrm{Cor}_{m\ell/m}(\mathfrak{z}_{m\ell}) = \begin{cases} P_\ell(\mathrm{Fr}_\ell^{-1})\mathfrak{z}_m & \text{if } \ell \nmid pm \\ \mathfrak{z}_m & \text{if } \ell | pm. \end{cases}$$

In particular $\{\mathfrak{z}_{Sp^n}\}_{S \in \mathscr{N}, n \geq 0}$ is an Euler system in the sense of Definition 3.11.

(2) *For every character χ of Γ_m of conductor m, we have*

$$\sum_{\gamma \in \Gamma_m} \chi(\gamma) \exp^*_m(\mathfrak{z}_m^\gamma) = \left(1 - \frac{a_p \chi(p)}{p} + \frac{\chi^2(p)}{p}\right) \frac{L(E, \chi, 1)}{\Omega^+}.$$

For a square-free integer $S > 0$ relatively prime to p, we put

$$\Theta_S = \sum_{\gamma \in \Gamma_S} \mathfrak{z}_S^{\gamma^{-1}} \otimes \gamma \in H^1(\mathbb{Q}(S), T) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Gamma_S].$$

Although the following proposition is not used to prove the main result (Theorem 6.1), it is applied to prove Theorem 7.1, which concerns exceptional zeros.

PROPOSITION 5.10. *For a square-free integer $S > 0$ relatively prime to p, we have*

$$\Theta_S \in H^1(\mathbb{Q}(S), T) \otimes_{\mathbb{Z}_p} I_{\Gamma_S, p}^{\mathrm{sp}(S)+b_2(S)},$$

where $\mathrm{sp}(S)$ denotes the number of split multiplicative primes of E dividing S, and $b_2(S)$ denotes the number of good primes ℓ of E dividing S such that $a_\ell = 2$ (i.e. $P_\ell(1) = 0$).

Proof. Our proof is similar to that of [7, Theorem 4.2]. Let S_1 be the product of primes ℓ dividing S such that ℓ is either a split multiplicative prime or a good prime with $a_\ell = 2$. We prove the proposition by induction on the number a of primes dividing S_1 (i.e. $a = \mathrm{sp}(S) + b_2(S)$). The case where $a = 0$ is trivial. Then, we assume that $a \geq 1$ and write $S_1 = \ell_1 \cdots \ell_a, S' = S/S_1$. By using $\Gamma_S = \Gamma_{\ell_1} \times \cdots \times \Gamma_{\ell_a} \times \Gamma_{S'}$, for $\gamma \in \Gamma_S$ we write $\gamma = \gamma_{\ell_1} \cdots \gamma_{\ell_a} \gamma'$, where each γ_{ℓ_i} is an element of Γ_{ℓ_i}, and $\gamma' \in \Gamma_{S'}$. Let $\mu(\cdot)$ denote the Möbius function. Then,

$$\begin{aligned}
&\sum_{\gamma \in \Gamma_S} \mathfrak{z}_S^{\gamma^{-1}} \otimes (\gamma_{\ell_1} - 1) \cdots (\gamma_{\ell_a} - 1)\gamma' = \Theta_S + \sum_{\gamma \in \Gamma_S} \sum_{d | S_1, d \neq S_1} \mu(S_1/d) \mathfrak{z}_S^{\gamma^{-1}} \otimes \left(\gamma' \prod_{\ell_i | d} \gamma_{\ell_i} \right) \\
=&\Theta_S + \sum_{d | S_1, d \neq S_1} \mu(S_1/d) \sum_{\gamma_0 \in \Gamma_{dS'}} \left(\gamma_0^{-1} \mathrm{Cor}_{S/dS'} \mathfrak{z}_S \right) \otimes \gamma_0 \\
=&\Theta_S + \sum_{d | S_1, d \neq S_1} \mu(S_1/d) \sum_{\gamma_0 \in \Gamma_{dS'}} \left(\prod_{\ell | \frac{S_1}{d}} P_\ell(\mathrm{Fr}_\ell^{-1}) \mathfrak{z}_{dS'}^{\gamma_0^{-1}} \right) \otimes \gamma_0 \\
=&\Theta_S + \sum_{d | S_1, d \neq S_1} \mu(S_1/d) \left(\prod_{\ell | \frac{S_1}{d}} P_\ell(\mathrm{Fr}_\ell^{-1}) \right) \Theta_{dS'}.
\end{aligned}$$

Hence, we have

$$\Theta_S = \sum_{\gamma \in \Gamma_S} \mathfrak{z}_S^{\gamma^{-1}} \otimes (\gamma_1 - 1) \cdots (\gamma_a - 1)\gamma' - \sum_{d | S_1, d \neq S_1} \mu(S_1/d) \left(\prod_{\ell | \frac{S_1}{d}} P_\ell(\mathrm{Fr}_\ell^{-1}) \right) \Theta_{dS'}. \tag{5.9}$$

By assumption, for each prime ℓ dividing S_1/d, we have $P_\ell(1) = 0$, and then $P_\ell(\mathrm{Fr}_\ell^{-1}) \in I_S$. Hence, by the induction hypothesis and (5.9), we complete the proof. □

5.4. **Kato's Euler system and Mazur-Tate elements.** We keep the same notation and assumption as in the previous subsection.

Definition 5.11. For a square-free integer S relatively prime to p, we define $\vartheta(\mathfrak{z}_S)$ by

$$\vartheta(\mathfrak{z}_S) = \sum_{\gamma\in\Gamma_S} (c_S, \mathfrak{z}_S^{\gamma^{-1}})\gamma \in \mathbb{Z}_p[\Gamma_S],$$

where $(-,-)$ is the paring (5.7).

By abuse of notation, we denote by $\pi_{m/n}$ the natural map $\mathbb{Z}_p[\Gamma_m] \to \mathbb{Z}_p[\Gamma_n]$ for $n|m$.

PROPOSITION 5.12. *For a square-free integer $S > 0$ relatively prime to p, we have the following.*

(1) *Let ℓ be a prime not dividing pS. Then we have*

$$\pi_{S\ell/S}(\vartheta(\mathfrak{z}_{S\ell})) = -\mathrm{Fr}_\ell P_\ell(\mathrm{Fr}_\ell^{-1})\vartheta(\mathfrak{z}_S).$$

(2) *For every character χ of Γ_S of conductor S, we have*

$$\chi(\vartheta(\mathfrak{z}_S)) = \tau_S(\chi)\frac{L(E,\chi^{-1},1)}{\Omega^+}.$$

Proof. By (5.8), we have

$$\begin{aligned}
\vartheta(\mathfrak{z}_S) &= \sum_{\gamma\in\Gamma_S} (c_S, \mathfrak{z}_S^{\gamma^{-1}})\gamma = \sum_{\gamma\in\Gamma_S} \mathrm{tr}_{\mathbb{Q}(S)/\mathbb{Q}}\left(\log_{\hat{E}}(c_S)\exp_S^*(\mathfrak{z}_S^{\gamma^{-1}})\right)\gamma \\
&= \sum_{\gamma\in\Gamma_S}\sum_{\delta\in\Gamma_S} \log_{\hat{E}}(c_S^\delta)\exp_S^*(\mathfrak{z}_S^{\delta\gamma^{-1}})\gamma = \sum_{\gamma\in\Gamma_S}\sum_{\delta\in\Gamma_S} \log_{\hat{E}}(c_S^\delta)\exp_S^*(\mathfrak{z}_S^{\gamma^{-1}})\delta\gamma \\
&= \left(\sum_{\delta\in\Gamma_S} \log_{\hat{E}}(c_S^\delta)\delta\right) \times \left(\sum_{\gamma\in\Gamma_S} \exp_S^*(\mathfrak{z}_S^{\gamma^{-1}})\gamma\right) \quad \text{in } (\mathbb{Q}(S)\otimes\mathbb{Q}_p)[\Gamma_S]. \qquad (5.10)
\end{aligned}$$

By using Proposition 5.7, we have

$$\begin{aligned}
\pi_{S\ell/S}\left(\sum_{\delta\in\Gamma_{S\ell}} \log_{\hat{E}}(c_{S\ell}^\delta)\delta\right) &= \sum_{\delta\in\Gamma_S} \left(\mathrm{tr}_{\mathbb{Q}(S\ell)/\mathbb{Q}(S)}\left(\log_{\hat{E}} c_{S\ell}\right)\right)^\delta \delta \\
&= -\sum_{\delta\in\Gamma_S} \log_{\hat{E}}\left(c_S^{\mathrm{Fr}_\ell^{-1}\delta}\right)\delta \\
&= -\sum_{\delta\in\Gamma_S} \log_{\hat{E}}\left(c_S^\delta\right)(\delta\mathrm{Fr}_\ell). \qquad (5.11)
\end{aligned}$$

By Theorem 5.9, we have

$$\pi_{S\ell/S}\left(\sum_{\gamma\in\Gamma_{S\ell}} \exp_{S\ell}^*(\mathfrak{z}_{S\ell}^{\gamma^{-1}})\gamma\right) = \sum_{\gamma\in\Gamma_S} \exp_S^*(\mathfrak{z}_S^{\gamma^{-1}})\gamma P_\ell(\mathrm{Fr}_\ell^{-1}). \qquad (5.12)$$

By (5.10) (replacing S by $S\ell$), (5.11) and (5.12), we deduce the assertion (1). By (5.10), Proposition 5.8 and Theorem 5.9, we conclude (2). □

COROLLARY 5.13. *Let S be a square-free positive integer relatively prime to p, and Let $\theta_{S,p} \in \mathbb{Z}_p[\Gamma_S]$ be the image of the Mazur-Tate element θ_S under the natural projection $\mathbb{Z}_p[G_S] \to \mathbb{Z}_p[\Gamma_S]$. Then, we have*

$$\vartheta(\mathfrak{z}_S) = \theta_{S,p} \in \mathbb{Z}_p[\Gamma_S].$$

Proof. Combining the proposition above with Proposition 2.3, we have $\chi(\theta_{S,p}) = \chi(\vartheta(\mathfrak{z}_S))$ for all the characters χ of Γ_S, which shows that the element $\theta_{S,p} - \vartheta(\mathfrak{z}_S) \in \mathbb{Q}_p[\Gamma_S]$ belongs to all the maximal ideals of $\mathbb{Q}_p[\Gamma_S]$. Since $\mathbb{Q}_p[\Gamma_S]$ is isomorphic to a product of fields, we have $\theta_{S,p} = \vartheta(\mathfrak{z}_S)$. □

COROLLARY 5.14. *We assume that p satisfies the conditions (A1), (A2) of Subsection 1.2. Let S be a square-free product of primes ℓ relatively prime to N such that $E(\mathbb{F}_\ell)[p]$ is cyclic. Then, we have $\theta_S \in I_{G_S,p}^{\min\{\mathfrak{r}_{\min},\, p\}}$, where we recall that $\mathfrak{r}_{\min} := \min_{n\geq 1}\{r_{p^n}\left(H^1_{f,p}(\mathbb{Q}, E[p^n])\right)\}$.*

Proof. We first assume that $(S,p) = 1$. By Lemma 5.3, we are reduced to proving that $\theta_{S,p} \in I_{\Gamma_S,p}^{\min\{\mathfrak{r}_{\min},\, p\}}$, which follows from Corollaries 4.14 and 5.13.

Next, we assume that $(S,p) \neq 1$. If we put $S' = S/p$, then $p \nmid S'$. By the case above and Proposition 2.3, we have

$$\pi_{S/S'}(\theta_S) = -\mathrm{Fr}_p(1 - a_p\mathrm{Fr}_p^{-1} + \mathrm{Fr}_p^{-2})\theta_{S'} \in I_{G_{S'},p}^{\min\{\mathfrak{r}_{\min},\, p\}}.$$

Since $p \nmid |G_p|$, Lemma 5.3 implies that $\theta_S \in I_{G_S,p}^{\min\{\mathfrak{r}_{\min},\, p\}}$. □

We define $\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) = \varinjlim_n \mathrm{Sel}(\mathbb{Q}, E[p^n])$ and put

$$r_{p^\infty} = \mathrm{corank}_{\mathbb{Z}_p}\left(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])\right).$$

Since $\mathrm{Sel}(\mathbb{Q}, E[p^n]) \to \mathrm{Sel}(\mathbb{Q}, E[p^\infty])[p^n]$ is surjective (cf. [28, Lemma 1.5.4]), we have

$$r_{p^n}(\mathrm{Sel}(\mathbb{Q}, E[p^n])) \geq r_{p^n}\left(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])[p^n]\right) \geq r_{p^\infty} \quad \text{for } n \geq 1. \tag{5.13}$$

Since $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$ (cf. Remark 4.19), Lemma 4.2 implies that

$$r_{p^n}\left(H^1_{f,p}(\mathbb{Q}, E[p^n])\right) \geq r_{p^n}(\mathrm{Sel}(\mathbb{Q}, E[p^n])) - 1 \quad \text{for } n \geq 1. \tag{5.14}$$

Combining (5.13) and (5.14), we have $\mathfrak{r}_{\min} \geq r_{p^\infty} - 1$. Hence, by Corollary 5.14 we obtain the following corollary.

COROLLARY 5.15. *With notation as in Corollary 5.14, if $r_{p^\infty} \geq 1$, then $\theta_S \in I_{G_S,p}^{\min\{r_{p^\infty}-1,p\}}$.*

5.5. **Application of the p-parity conjecture.** First, following [20, Chapter 1, §6], we recall the functional equation of Mazur-Tate elements. Let w_N be the operator on $S_2(\Gamma_0(N))$ defined as $g \mapsto \frac{1}{N\tau^2} g\left(\frac{-1}{N\tau}\right)$. Let f be the newform corresponding to E. Then there exists $\varepsilon_f \in \{\pm 1\}$ such that $w_N(f) = -\varepsilon_f f$. It is known that

$$\varepsilon_f = (-1)^{\mathrm{ord}_{s=1}(L(E,s))}. \tag{5.15}$$

Let S be a positive integer relatively prime to N. By [21, Chapter 1, §6] and (2.1), for an integer a relatively prime to S, we have

$$[a/S]_E^{\pm} = \varepsilon_f \, [a'/S]_E^{\pm}, \tag{5.16}$$

where a' is an integer satisfying $a'aN \equiv -1 \mod S$. Let ι be the homomorphism of $\mathbb{Q}$-algebras $\mathbb{Q}[G_S] \to \mathbb{Q}[G_S]$ sending $\sigma \in G_S$ to σ^{-1}. We have a *functional equation* of θ_S as follows.

PROPOSITION 5.16.

$$\theta_S = \varepsilon_f \delta_{-N}^{-1} \iota(\theta_S).$$

Proof. We have

$$\begin{aligned}
&\varepsilon_f \delta_{-N}^{-1} \iota(\theta_S) \\
=&\varepsilon_f \delta_{-N}^{-1} \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a}{S}\right]_E^+ + \left[\frac{a}{S}\right]_E^- \right) \delta_a^{-1} = \varepsilon_f \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a}{S}\right]_E^+ + \left[\frac{a}{S}\right]_E^- \right) \delta_{(-aN)^{-1}} \\
\overset{\text{(a)}}{=} &\sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a'}{S}\right]_E^+ + \left[\frac{a'}{S}\right]_E^- \right) \delta_{a'} = \theta_S,
\end{aligned}$$

where the equation (a) follows from (5.16). □

We denote by I_{G_S} the augmentation ideal of $\mathbb{Z}[G_S]$. Then, we note that for $\gamma \in G_S$,

$$\iota(\gamma - 1) = \gamma^{-1} - 1 \equiv -\gamma^{-1}(\gamma - 1) \equiv -(\gamma - 1) \mod I_{G_S}^2.$$

Hence, we have $\iota = -1$ on $I_{G_S}/I_{G_S}^2$, and similarly $\iota = (-1)^t$ on $I_{G_S}^t/I_{G_S}^{t+1}$ for $t \geq 1$.

THEOREM 5.17. *Let p be a prime which satisfies the conditions (A1), (A2) of Subsection 1.2, and let S be a square-free product of good primes ℓ of E such that $E(\mathbb{F}_\ell)[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or $\{0\}$. We denote by I_{G_S} the augmentation ideal of $\mathbb{Z}[G_S]$. Then, we have*

$$\theta_S \in \mathbb{Z}_p \otimes_{\mathbb{Z}} I_{G_S}^{\min\{r_{p^\infty}, p\}}.$$

In particular, if p is admissible, then $\theta_S \in \mathbb{Z}_p \otimes I_{G_S}^{r_E}$.

Proof. By Corollary 5.15, we have $\theta_S \in \mathbb{Z}_p \otimes I_{G_S}^{\min\{r_{p^\infty}-1, p\}}$. If $p \leq r_{p^\infty} - 1$ or $r_{p^\infty} = 0$, then there is nothing to prove. Hence, we assume that $1 \leq r_{p^\infty} \leq p$, and then $\theta_S \in \mathbb{Z}_p \otimes I_{G_S}^{r_{p^\infty}-1}$. We note that the group G_S acts on $I_{G_S}^{r_{p^\infty}-1}/I_{G_S}^{r_{p^\infty}}$ trivially. Then, we have

$$\theta_S \equiv \varepsilon_f \delta_{-N}^{-1} \iota(\theta_S) \equiv \varepsilon_f \delta_{-N}^{-1} (-1)^{r_{p^\infty}-1} \theta_S \equiv \varepsilon_f (-1)^{r_{p^\infty}-1} \theta_S \mod \mathbb{Z}_p \otimes I_{G_S}^{r_{p^\infty}}, \tag{5.17}$$

where each term is regarded as an element of $\mathbb{Z}_p \otimes I_{G_S}^{r_{p^\infty}-1}$. By the p-parity conjecture (cf. [8, Theorem 1.4]),

$$(-1)^{\mathrm{ord}_{s=1}(L(E,s))} = (-1)^{r_{p^\infty}}.$$

Combining this with (5.15) and (5.17), we have $2\theta_S \in \mathbb{Z}_p \otimes I_{G_S}^{r_{p^\infty}}$. Since p is odd, we conclude that $\theta_S \in \mathbb{Z}_p \otimes I_{G_S}^{r_{p^\infty}}$. □

6. Proof of the main result

6.1. **The order of vanishing.** As in Subsection 1.2, let R be a subring of $\mathbb{Q}$ in which every non-admissible prime is invertible. For a positive integer S, we denote by I_S the augmentation ideal of $R[G_S]$.

THEOREM 6.1. *Let S be a square-free product of primes $\ell \nmid N$ such that for each prime p which is not invertible in R, the module $E(\mathbb{F}_\ell)[p]$ is cyclic. Then, we have*

$$\theta_S \in I_S^{r_E}.$$

Proof. For a prime p not invertible in R, we see that p and S satisfy the assumption of Theorem 5.17, and then $\theta_S \in \mathbb{Z}_p \otimes I_S^{r_E}$. By Lemma 5.1, we complete the proof. □

Remark 6.2. For distinct primes p and ℓ, the module $E(\mathbb{F}_\ell)[p]$ is isomorphic to $\{0\}, \mathbb{Z}/p\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$. Furthermore, $E(\mathbb{F}_\ell)[p] \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ if and only if ℓ splits completely in $\mathbb{Q}(E[p])$. Hence, by Chebotarev's density theorem, if the representation $G_\mathbb{Q} \to \mathrm{Aut}_{\mathbb{Z}/p\mathbb{Z}}(E[p])$ is surjective, then the density of primes ℓ satisfying $E(\mathbb{F}_\ell)[p] \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ is equal to $1/|\mathrm{GL}_2(\mathbb{F}_p)| = 1/(p^2-1)(p^2-p)$. Therefore, if we denote by δ_R the density of primes ℓ satisfying the assumption of Theorem 6.1, then

$$\delta_R \geq 1 - \sum_{p \notin R^\times} \frac{1}{(p^2-1)(p^2-p)} \geq 1 - \sum_{p \geq 5} \frac{1}{(p^2-1)(p^2-p)} > 0.997.$$

COROLLARY 6.3. *Let S be a square-free product of primes which are either good primes ℓ of E satisfying the condition Theorem 6.1 or split multiplicative primes of E. Assume that $\ell' - 1$ is invertible in R for every split multiplicative prime ℓ' of E dividing S. Then,*

$$\theta_S \in I_S^{r_E + \mathrm{sp}(S) + b_{2,R}(S)},$$

where $\mathrm{sp}(S)$ is as in Section 1, and $b_{2,R}(S)$ denotes the number of primes ℓ dividing S such that $a_\ell = 2$ and $\ell - 1 \in R^\times$.

Proof. By Lemma 5.1, it suffices to show that for each prime p which is not invertible in R,

$$\theta_S \in \mathbb{Z}_p \otimes I_S^{r_E + \mathrm{sp}(S) + b_{2,R}(S)}. \tag{6.1}$$

We denote by S' the product of split multiplicative primes dividing S and primes $\ell | S$ such that $a_l = 2$ and $\ell - 1 \in R^\times$. We put $S_0 = S/S'$. By Proposition 2.3 (1), we have

$$\pi_{S/S_0}(\theta_S) = \left(\prod_{\ell | S'} -\mathrm{Fr}_\ell P_\ell(\mathrm{Fr}_\ell^{-1}) \right) \theta_{S_0}.$$

We note that for each prime $\ell | S'$, we have $P_\ell(1) = 0$, and then $P_\ell(\mathrm{Fr}_\ell^{-1}) \in I_\ell$. Hence, by Theorem 6.1, we have $\pi_{S/S_0}(\theta_S) \in I_{S_0}^{r_E + \mathrm{sp}(S) + b_{2,R}(S)}$. Since each prime ℓ dividing S' satisfies $\ell - 1 \in \mathbb{Z}_p^\times$ (i.e. $|G_\ell| \in \mathbb{Z}_p^\times$), Lemma 5.3 implies (6.1). □

6.2. **The leading coefficients.** For a prime p, as in Section 3, let $\mathscr{R}_p$ be the set of good primes ℓ of E such that $\ell \equiv 1 \mod p$. For a positive integer S, we write $S = \ell_1 \cdots \ell_s$, where $\ell_1, \ell_2, \dots, \ell_n \in \mathscr{R}_p$, and $\ell_{n+1}, \dots, \ell_s \notin \mathscr{R}_p$. Then, we put $S_1 = \ell_1 \cdots \ell_n$ and $S_2 = \ell_{n+1} \cdots \ell_s$.

THEOREM 6.4. *Let p be an admissible prime (cf. Subsection 1.2) and S a square-free product of good primes ℓ of E such that the module $E(\mathbb{F}_\ell)[p]$ is cyclic. We write $S = S_1S_2$ as above. We denote by $I_{S,p}$ the augmentation ideal of $\mathbb{Z}_p[G_S]$ and by $\tilde{\theta}_S^{(p)}$ the image of θ_S in $\mathbb{Z}/p\mathbb{Z} \otimes I_{S,p}^{r_E}/I_{S,p}^{r_E+1}$ (cf. Theorem 5.17). If $\tilde{\theta}_S^{(p)} \neq 0$, then*

$$Ш[p] = 0, \quad p \nmid J_{S_1}, \quad p \nmid \prod_{\ell | S_2} (a_\ell - 2).$$

Remark 6.5. By the relation between our θ_S and the original Mazur-Tate element in [21], the same theorem for the leading coefficients considered in [21] also holds (cf. Section 2).

Proof. Let $\theta_{S,p}, \Gamma_S$ and $I_{\Gamma_S,p}$ be as in Section 5. First, we assume that $r_E \geq 1$. We denote by $\tilde{\theta}_{S,p}^{(p)}$ the image of $\theta_{S,p}$ in $\mathbb{Z}/p\mathbb{Z} \otimes I_{\Gamma_S,p}^{r_E}/I_{\Gamma_S,p}^{r_E+1}$. Since $G_S = H_S \times \Gamma_S$, where $p \nmid |H_S|$, by Lemma 5.4 we have

$$\tilde{\theta}_{S,p}^{(p)} \neq 0. \tag{6.2}$$

By applying Proposition 3.3 to $\sum_{\gamma \in \Gamma_S} \mathfrak{z}_S^{\gamma^{-1}} \otimes \gamma$ and by using Corollary 5.13, we have

$$\theta_{S,p} = \sum_{\underline{k}=(k_1,\dots,k_s) \in \mathbb{Z}_{\geq 0}^{\oplus s}} (c_S, D_{\underline{k}}\mathfrak{z}_S)(\sigma_{\ell_1}^{-1} - 1)^{k_1} \cdots (\sigma_{\ell_s}^{-1} - 1)^{k_s}.$$

Then, by Lemma 5.2,

$$\theta_{S,p} \equiv \sum_{\substack{k_1+\cdots+k_n \leq r_E, \\ k_{n+1}=\cdots=k_s=0}} (c_S, D_{\underline{k}}\mathfrak{z}_S)(\sigma_{\ell_1}^{-1} - 1)^{k_1} \cdots (\sigma_{\ell_s}^{-1} - 1)^{k_s} \mod I_{\Gamma_S,p}^{r_E+1}.$$

For $\underline{k}$ such that $k_1 + \cdots + k_n < r_E$ and $k_{n+1} = \cdots = k_s = 0$, we have $D_{\underline{k}} = N_{S_2}D'$, where we put $D' = D_{\ell_1}^{(k_1)} \cdots D_{\ell_n}^{(k_n)}$. We put $S' = \mathrm{Cond}(D')$. By Lemma 4.2, we have $r_E \leq r_p(H^1_{f,S'}(\mathbb{Q}, E[p])) + r_p(A(S'))$. Since $\mathrm{ord}(D') < r_E$, by applying Theorem 4.18 to $D'\mathfrak{z}_{S_1}$,

$$\begin{aligned} \mathrm{loc}_p(D_{\underline{k}}\mathfrak{z}_S \bmod p) = \mathrm{loc}_p(N_{S_2}D'\mathfrak{z}_S \bmod p) &= \prod_{\ell | S_2} P_\ell(\mathrm{Fr}_\ell^{-1}) \mathrm{loc}_p(D'\mathfrak{z}_{S_1} \bmod p) \\ &\in H_f^1(\mathbb{Q}(S) \otimes \mathbb{Q}_p, E[p]). \end{aligned} \tag{6.3}$$

Hence, $(c_S, D_{\underline{k}}\mathfrak{z}_S) \equiv 0 \mod p$ for any $\underline{k}$ such that $k_1 + \cdots + k_n < r_E$ and $k_{n+1} = \cdots = k_s = 0$. Then,

$$\theta_{S,p} \equiv \sum_{\substack{k_1+\cdots+k_n = r_E \\ k_{n+1}=\cdots=k_s=0}} (c_S, D_{\underline{k}}\mathfrak{z}_S)(\sigma_{\ell_1}^{-1} - 1)^{k_1} \cdots (\sigma_{\ell_s}^{-1} - 1)^{k_s} \mod p\mathbb{Z}_p[\Gamma_S] + I_{\Gamma_S,p}^{r_E+1}.$$

By (6.2), for some $\underline{k}$ such that $k_1 + \cdots + k_n = r_E$ and $k_{n+1} = \cdots = k_s = 0$, we have $(c_S, D_{\underline{k}}\mathfrak{z}_S) \not\equiv 0 \mod p$. For this $\underline{k}$, let D' be as above. Then, by (6.3), the localization $\mathrm{loc}_p(D'\mathfrak{z}_{S_1} \bmod p)$ does not lie in $H_f^1(\mathbb{Q}(S_1) \otimes \mathbb{Q}_p, E[p])$. Since $\mathrm{ord}(D') = r_E$, by applying

Corollary 4.20 to $D'\mathfrak{z}_{S_1}$, we have $Ш[p]=0$, and the map $E(\mathbb{Q})/p \to \oplus_{\ell|S_1} E(\mathbb{Q}_\ell)/p$ is surjective. Since $\oplus_{\ell|S_1} E(\mathbb{Q}_\ell)/p \cong \oplus_{\ell|S_1} E(\mathbb{F}_\ell)/p$ and $p \nmid \prod_{\ell|N} m_\ell$, the map

$$E(\mathbb{Q}) \to \left[\left(\oplus_{\ell|S_1} E(\mathbb{F}_\ell)\right) \oplus \left(\oplus_{\ell|N} E(\mathbb{Q}_\ell)/E_0(\mathbb{Q}_\ell)\right)\right] \otimes \mathbb{Z}/p\mathbb{Z}$$

is surjective, that is, $p \nmid J_{S_1}$. By Theorem 5.17, we have $\theta_{S_1} \in I_{S_1,p}^{r_E}$, and hence

$$\pi_{S/S_1}(\theta_S) \equiv \left(\prod_{\ell|S_2} -P_\ell(1)\right)\theta_{S_1,p} \equiv \left(\prod_{\ell|S_2}(a_\ell-2)\right)\theta_{S_1} \mod I_{S_1,p}^{r_E+1}. \tag{6.4}$$

Since $p \nmid |G_\ell|$ for $\ell|S_2$, and since $\tilde{\theta}_S^{(p)} \neq 0$, Lemma 5.4 implies that the image of $\pi_{S/S_1}(\theta_S)$ in $\mathbb{Z}/p\mathbb{Z} \otimes I_{S_1,p}^{r_E}/I_{S_1,p}^{r_E+1}$ is not zero. Hence, by (6.4) we have $p \nmid \prod_{\ell|S_2}(a_\ell-2)$.

We next assume that $r_E = 0$. By Proposition 2.3,

$$\pi_{S/1}(\theta_S) = \left(\prod_{\ell|S}(a_\ell-2)\right)\theta_1 = \left(\prod_{\ell|S}(a_\ell-2)\right)\frac{L(E,1)}{\Omega^+} \in \mathbb{Z}_p. \tag{6.5}$$

Since we assume that $\pi_{S/1}(\theta_S) \not\equiv 0 \bmod p$ and since $\theta_1 \in R$, we have $\frac{L(E,1)}{\Omega^+} \not\equiv 0 \bmod p$. Hence by the work of Kolyvagin and Kato (cf. [11, Chapter 14] or [28, Theorem 2.2.10]), $Ш[p]=0$. By (6.5), the assumption that $\pi_{S/1}(\theta_S) \not\equiv 0 \bmod p$ also implies that $p \nmid \prod_{\ell|S}(a_\ell-2)$. We note that $|E(\mathbb{F}_\ell)| \equiv 2-a_\ell \bmod p$ for $\ell \in \mathscr{R}_p$, and then we have $p \nmid \prod_{\ell|S_1} |E(\mathbb{F}_\ell)|$, that is, $p \nmid J_{S_1}$. □

7. Exceptional zeros

The aim of this section is to show that Mazur-Tate elements have exceptional zeros induced by split multiplicative primes and by good primes for which the Hasse-invariant is equal to 2. In this section, the Mordell-Weil rank is not involved, and we do not require the divisibility of derivatives of Euler systems or the p-parity conjecture.

Theorem 7.1. *Let R be a subring of $\mathbb{Q}$, and suppose that every prime which does not satisfy both the following conditions* (1) *and* (2) *is invertible in R:* (1) $p \nmid 6N \cdot |E(\mathbb{F}_p)|$, (2) *the Galois representation $G_\mathbb{Q} \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))$ is surjective. Let $S>0$ be a square-free integer. Then,*

$$\theta_S \in I_S^{\mathrm{sp}(S)+b_2(S)},$$

where I_S is the augmentation ideal of $R[G_S]$, and $b_2(S)$ is as in Proposition 5.10.

Remark 7.2. (1) In our setting, Theorem 7.1 implies Conjecture 1.1 when $r_E = 0$. Although Bergunde and Gehrmann [1] have announced that they proved that $\theta_S \in I_S^{\mathrm{sp}(S)}$ in the general case, exceptional zeros coming from good primes ℓ with $a_\ell = 2$ are not considered.

(2) We note that $b_{2,R}(S) \leq b_2(S)$ and that the assumption on S and R of Theorem 7.1 is weaker than that of Corollary 6.3.

Proof. We put $a = \mathrm{sp}(S) + b_2(S)$. By Lemma 5.1, it suffices to show that $\theta_S \in \mathbb{Z}_p \otimes I_S^a$ for each prime p not invertible in R. If $p \nmid S$, then by Lemma 5.3 and Corollary 5.13, it suffices to show that $\theta(\mathfrak{z}_S) \in \mathbb{Z}_p \otimes I^a_{\Gamma_S,p}$, which follows from Proposition 5.10. In the case where $p|S$, we have

$$\pi_{S/\frac{S}{p}}(\theta_S) = -\mathrm{Fr}_p P_p(\mathrm{Fr}_p^{-1})\theta_{S/p}.$$

Since $|G_p| \in \mathbb{Z}_p^\times$, by the case above and Lemma 5.3, we complete the proof. □

REFERENCES

[1] F. Bergunde and L. Gehrmann, On the order of vanishing of stickelberger elements of Hilbert modular forms, preprint, http://arxiv.org/abs/1506.04638.

[2] M. Bertolini and H. Darmon, Derived heights and generalized Mazur-Tate regulators, *Duke Math. J.* **76** (1994), no. 1, 75–111.

[3] A. Besser, On the finiteness of Ш for motives associated to modular forms, *Doc. Math.* **2** (1997), 31–46 (electronic).

[4] C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over **Q**: wild 3-adic exercises, *J. Amer. Math. Soc*. **14** (2001), no. 4, 843–939.

[5] A. C. Cojocaru, On the surjectivity of the Galois representations associated to non-CM elliptic curves, *Canad. Math. Bull.* **48** (2005), no. 1, 16–31.

[6] H. Darmon, A refined conjecture of Mazur-Tate type for Heegner points, *Invent. Math.* **110** (1992), no. 1, 123–146.

[7] H. Darmon, Thaine's method for circular units and a conjecture of Gross, *Canad. J. Math.* **47** (1995), no. 2, 302–317.

[8] T. Dokchitser and V. Dokchitser, On the Birch-Swinnerton-Dyer quotients modulo squares, *Ann. of Math.* (2) **172** (2010), no. 1, 567–596.

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

[10] K. Kato, Euler systems, Iwasawa theory, and Selmer groups, *Kodai Math. J.* **22** (1999), no. 3, 313–372.

[11] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, *Cohomologies p-adiques et applications, arithmétiques. III, Astérisque* **295** (2004), ix, 117–290.

[12] B. D. Kim, The parity conjecture for elliptic curves at supersingular reduction primes, *Compos. Math.* **143** (2007), no. 1, 47–72.

[13] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, *Invent. Math.* **152** (2003), no. 1, 1–36.

[14] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I, *Invent. Math.* **149** (2002), no. 1, 195–224.

[15] M. Kurihara, The structure of Selmer groups for elliptic curves and modular symbols, *Iwasawa theory 2012*, *Contrib. Math. Comput. Sci.* **7**, 317–356, Springer, Heidelberg, 2014.

[16] M. Longo and S. Vigni, A refined Beilinson-Bloch conjecture for motives of modular forms, to appear in *Trans. Amer. Math. Soc.*

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

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

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

[20] B. Mazur and J. Tate, Refined conjectures of the "Birch and Swinnerton-Dyer type", *Duke Math. J.* **54** (1987), no. 2, 711–750.

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

[22] J. S. Milne, *Arithmetic duality theorems*, Second, BookSurge, LLC, Charleston, SC, 2006.

[23] P. Monsky, Generalizing the Birch-Stephens theorem. I. Modular curves, *Math. Z.* **221** (1996), no. 3, 415–420.

[24] J. Nekovář, Selmer complexes, *Astérisque* **310** (2006), viii+559.

[25] R. Otsuki, Construction of a homomorphism concerning Euler systems for an elliptic curve, *Tokyo J. Math.* **32** (2009), no. 1, 253–278.

[26] B. Perrin-Riou, Systèmes d'Euler p-adiques et théorie d'Iwasawa, *Ann. Inst. Fourier* (Grenoble) **48** (1998), no. 5, 1231–1307.

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

[28] K. Rubin, *Euler systems, Annals of Mathematics Studies* **147**, Princeton University Press, Princeton, NJ, 2000.

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

[30] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401.

[31] J. H. SILVERMAN, *Advanced topics in the arithmetic of elliptic curves*, *Graduate Texts in Mathematics* **151**, Springer-Verlag, New York, 1994.

[32] W. A. Stein et al., *Sage Mathematics Software* (Version 5.6), The Sage Development Team, 2013, http://www.sagemath.org.

[33] K.-S. Tan, Refined theorems of the Birch and Swinnerton-Dyer type, *Ann. Inst. Fourier* (Grenoble) **45** (1995), no. 2, 317–374.

[34] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* (2) **141** (1995), no. 3, 553–572.

[35] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* (2) **141** (1995), no. 3, 443–551.

DEPARTMENT OF MATHEMATICS, KEIO UNIVERSITY, 3-14-1 KOHOKU-KU, HIYOSHI, YOKOHAMA, 223-8522, JAPAN

E-mail address: kazutoota@math.keio.ac.jp