The structure of Selmer groups of elliptic curves and modular symbols

Masato Kurihara

For an elliptic curve over the rational number field and a prime number p, we study the structure of the classical Selmer group of p-power torsion points. In our previous paper [12], assuming the main conjecture and the non-degeneracy of the p-adic height pairing, we proved that the structure of the Selmer group with respect to p-power torsion points is determined by some analytic elements $\tilde{\delta}_m$ defined from modular symbols (see Theorem 1.1.1 below). In this paper, we do not assume the main conjecture nor the non-degeneracy of the p-adic height pairing, and study the structure of Selmer groups (see Theorems 1.2.3 and 1.2.5), using these analytic elements and Kolyvagin systems of Gauss sum type.

1 Introduction

1.1 Structure theorem of Selmer groups

Let E be an elliptic curve over $\mathbf{Q}$. Iwasawa theory, especially the main conjecture gives a formula on the order of the Tate Shafarevich group by using the p-adic L-function (cf. Schneider [24]). In this paper, as a sequel of [10], [11] and [12], we show that we can derive more information than the order, on the structure of the Selmer group and the Tate Shafarevich group from analytic quantities, in the setting of our paper, from modular symbols.

In this paper, we consider a prime number p such that
(i) p is a good ordinary prime > 2 for E,
(ii) the action of $G_{\mathbf{Q}}$ on the Tate module $T_p(E)$ is surjective where $G_{\mathbf{Q}}$ is the absolute Galois group of $\mathbf{Q}$,
(iii) the (algebraic) μ-invariant of $(E, \mathbf{Q}_\infty/\mathbf{Q})$ is zero where $\mathbf{Q}_\infty/\mathbf{Q}$ is the cyclotomic $\mathbf{Z}_p$-extension, namely the Selmer group $\mathrm{Sel}(E/\mathbf{Q}_\infty, E[p^\infty])$ (for the definition, see below) is a cofinitely generated $\mathbf{Z}_p$-module,
(iv) p does not divide the Tamagawa factor $\mathrm{Tam}(E) = \Pi_{\ell:\mathrm{bad}}(E(\mathbf{Q}_\ell)$:

$E^0(\mathbf{Q}_\ell)$), and p does not divide $\#E(\mathbf{F}_p)$ (namely not anomalous).

We note that the property (iii) is a conjecture of Greenberg since we are assuming (ii).

For a positive integer $N > 0$, we denote by $E[p^N]$ the Galois module of p^N-torsion points, and $E[p^\infty] = \bigcup_{N>0} E[p^N]$. For an algebraic extension $F/\mathbf{Q}$, $\mathrm{Sel}(E/F, E[p^N])$ is the classical Selmer group defined by

$$\mathrm{Sel}(E/F, E[p^N]) = \mathrm{Ker}(H^1(F, E[p^N]) \longrightarrow \prod_v H^1(F_v, E[p^N])/E(F_v) \otimes \mathbf{Z}/p^N),$$

so $\mathrm{Sel}(E/F, E[p^N])$ sits in an exact sequence

$$0 \longrightarrow E(F) \otimes \mathbf{Z}/p^N \longrightarrow \mathrm{Sel}(E/F, E[p^N]) \longrightarrow Ш(E/F)[p^N] \longrightarrow 0$$

where $Ш(E/F)$ is the Tate Shafarevich group over F. We define $\mathrm{Sel}(E/F, E[p^\infty]) = \varinjlim \mathrm{Sel}(E/F, E[p^N])$.

Let $\mathcal{P}^{(N)}$ be the set of prime numbers ℓ such that ℓ is a good reduction prime for E and $\ell \equiv 1 \pmod{p^N}$. For each ℓ, we fix a generator η_ℓ of $(\mathbf{Z}/\ell\mathbf{Z})^\times$ and define $\log_{\mathbf{F}_\ell}(a) \in \mathbf{Z}/(\ell-1)$ by $\eta_\ell^{\log_{\mathbf{F}_\ell}(a)} \equiv a \pmod{\ell}$.

Let $f(z) = \Sigma a_n e^{2\pi i n z}$ be the modular form corresponding to E. For a positive integer m and the cyclotomic field $\mathbf{Q}(\mu_m)$, we denote by $\sigma_a \in \mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q})$ the element such that $\sigma_a(\zeta) = \zeta^a$ for any $\zeta \in \mu_m$. We consider the modular element $\sum_{a=1,(a,m)=1}^{m} [\frac{a}{m}]\sigma_a \in \mathbf{C}[\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q})]$ of Mazur and Tate ([16]) where $[\frac{a}{m}] = 2\pi i \int_\infty^{a/m} f(z)dz$ is the usual modular symbol. We only consider the real part

$$\tilde{\theta}_{\mathbf{Q}(\mu_m)} = \sum_{\substack{a=1 \\ (a,m)=1}}^{m} \frac{\mathrm{Re}([\frac{a}{m}])}{\Omega_E^+} \sigma_a \in \mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q})] \tag{1.1}$$

where $\Omega_E^+ = \int_{E(\mathbf{R})} \omega_E$ is the Néron period. Suppose that m is a squarefree product of primes in $\mathcal{P}^{(N)}$. Since we are assuming the $G_{\mathbf{Q}}$-module $E[p]$ of p-torsion points is irreducible, we know $\tilde{\theta}_{\mathbf{Q}(\mu_m)} \in \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q})]$ (cf. [27]). We consider the coefficient of $\tilde{\theta}_{\mathbf{Q}(\mu_m)}$ of "$\prod_{\ell|m}(\sigma_{\eta_\ell} - 1)$", more explicitly we define

$$\tilde{\delta}_m = \sum_{\substack{a=1 \\ (a,m)=1}}^{m} \frac{\mathrm{Re}([\frac{a}{m}])}{\Omega_E^+} (\prod_{\ell|m} \log_{\mathbf{F}_\ell}(a)) \in \mathbf{Z}/p^N \tag{1.2}$$

where $\log_{\mathbf{F}_\ell}(a)$ means the image of $\log_{\mathbf{F}_\ell}(a)$ under the canonical homomorphism $\mathbf{Z}/(\ell-1) \longrightarrow \mathbf{Z}/p^N$. Let $\mathrm{ord}_p : \mathbf{Z}/p^N \longrightarrow \{0, 1, ..., N-1, \infty\}$ be the p-adic valuation normalized as $\mathrm{ord}_p(p) = 1$ and $\mathrm{ord}_p(0) = \infty$. We note that $\mathrm{ord}_p(\tilde{\delta}_m)$ does not depend on the choices of η_ℓ for $\ell | m$. We define $\tilde{\delta}_1 = \theta_{\mathbf{Q}} = \mathrm{Re}([0])/\Omega_E^+ = L(E,1)/\Omega_E^+$.

For a squarefree product m of primes, we define $\epsilon(m)$ to be the number of prime divisors of m, namely $\epsilon(m) = r$ if $m = \ell_1 \cdot \ldots \cdot \ell_r$. Let $\mathcal{N}^{(N)}$ be the set of squarefree products of primes in $\mathcal{P}^{(N)}$. We suppose 1 is in $\mathcal{N}^{(N)}$. For each integer $i \geq 0$, we define the ideal $\Theta_i(\mathbf{Q})^{(N,\delta)}$ of $\mathbf{Z}/p^N$ to be the ideal generated by all $\tilde{\delta}_m$ such that $\epsilon(m) \leq i$ for all $m \in \mathcal{N}^{(N)}$;

$$\Theta_i(\mathbf{Q})^{(N,\delta)} = (\{\tilde{\delta}_m \mid \epsilon(m) \leq i \text{ and } m \in \mathcal{N}^{(N)}\}) \subset \mathbf{Z}/p^N. \tag{1.3}$$

We define $n_{i,N} \in \{0, 1, ..., N-1, \infty\}$ by $\Theta_i(\mathbf{Q})^{(N,\delta)} = p^{n_{i,N}}(\mathbf{Z}/p^N)$ (we define $n_{i,N} = \infty$ if $\Theta_i(\mathbf{Q})^{(N,\delta)} = 0$).

Theorem 1.1.1 ([12] Theorem B, Theorem 9.3.1 and (9.14)) *We assume that the main conjecture for* $(E, \mathbf{Q}_\infty/\mathbf{Q})$ (*see* (2.5)) *and the p-adic height pairing is non-degenerate.*
(1) $n_{i,N}$ *does not depend on N when N is sufficiently large (for example, when $N > 2\,\mathrm{ord}_p(\eta_0)$ where η_0 is the leading term of the p-adic L-function, see §9.4 in [12]). We put $n_i = n_{i,N}$ for $N \gg 0$. In other words, we define n_i by*

$$\varprojlim \Theta_i(\mathbf{Q})^{(N,\delta)} = p^{n_i}\mathbf{Z}_p \subset \mathbf{Z}_p.$$

We denote this ideal of $\mathbf{Z}_p$ by $\Theta_i(\mathbf{Q})^{(\delta)}$.
(2) *Consider the Pontrjagin dual* $\mathrm{Sel}(E/\mathbf{Q}, E[p^\infty])^\vee$ *of the Selmer group. Suppose that*

$$\mathrm{rank}_{\mathbf{Z}_p} \mathrm{Sel}(E/\mathbf{Q}, E[p^\infty])^\vee = r (\in \mathbf{Z}_{\geq 0}), \text{ and } \dim_{\mathbf{F}_p} \mathrm{Sel}(E/\mathbf{Q}, E[p])^\vee = a.$$

Then we have

$$\Theta_0(\mathbf{Q})^{(\delta)} = \ldots = \Theta_{r-1}(\mathbf{Q})^{(\delta)} = 0 \text{ and } \Theta_r(\mathbf{Q})^{(\delta)} \neq 0.$$

For any $i \geq r$, n_i is an even number, and

$$p^{n_r} = \#(\mathrm{Sel}(E/\mathbf{Q}, E[p^\infty])^\vee)_{\mathrm{tors}},$$

$$n_a = 0, \text{ and}$$

$$\mathrm{Sel}(E/\mathbf{Q}, E[p^\infty])^\vee \simeq \mathbf{Z}_p^{\oplus r} \oplus (\mathbf{Z}/p^{\frac{n_r - n_{r+2}}{2}})^{\oplus 2} \oplus (\mathbf{Z}/p^{\frac{n_{r+2} - n_{r+4}}{2}})^{\oplus 2} \oplus \ldots \oplus (\mathbf{Z}/p^{\frac{n_{a-2} - n_a}{2}})^{\oplus 2}$$

hold.

In particular, knowing $\Theta_i(\mathbf{Q})^{(\delta)}$ for all $i \geq 0$ completely determines the structure of $\mathrm{Sel}(E/\mathbf{Q}, E[p^\infty])^\vee$ as a $\mathbf{Z}_p$-module. Namely, the modular symbols determine the structure of the Selmer group under our assumptions.

1.2 Main Results

We define
$$\mathcal{P}_1^{(N)} = \{\ell \in \mathcal{P}^{(N)} \mid H^0(\mathbf{F}_\ell, E[p^N]) \simeq \mathbf{Z}/p^N\}.$$

This is an infinite set by Chebotarev density theorem since we are assuming (ii) (see [12] §4.3). We define $\mathcal{N}_1^{(N)}$ to be the set of squarefree products of primes in $\mathcal{P}_1^{(N)}$. Again, we suppose $1 \in \mathcal{N}_1^{(N)}$. We propose the following conjecture.

Conjecture 1.2.1 *There is $m \in \mathcal{N}_1^{(N)}$ such that $\tilde{\delta}_m$ is a unit in $\mathbf{Z}/p^N$, namely*
$$\mathrm{ord}_p(\tilde{\delta}_m) = 0.$$

Numerically, it is easy to compute $\tilde{\delta}_m$, so it is easy to check this conjecture.

Theorem 1.2.2 ([12] Theorem 9.3.1) *If we assume the main conjecture and the non-degeneracy of the p-adic height pairing, Conjecture 1.2.1 holds true.*

In fact, we obtain Conjecture 1.2.1, considering the case $i = a$ in Theorem 1.1.1 (cf. $i = s$ in Theorem 9.3.1 in [12]).

From now on, we do not assume the main conjecture (2.5) nor the non-degeneracy of the p-adic height pairing.

We define the Selmer group $\mathrm{Sel}(\mathbf{Z}[1/m], E[p^N])$ by
$$\mathrm{Sel}(\mathbf{Z}[1/m], E[p^N]) = \mathrm{Ker}(H^1(\mathbf{Q}, E[p^N]) \longrightarrow \prod_{v \nmid m} H^1(\mathbf{Q}_v, E[p^N])/E(\mathbf{Q}_v) \otimes \mathbf{Z}/p^N).$$

If all bad primes and p divide m, we know $\mathrm{Sel}(\mathbf{Z}[1/m], E[p^N])$ is equal to the étale cohomology group $H^1_{et}(\mathrm{Spec}\,\mathbf{Z}[1/m], E[p^N])$, which explains the notation "$\mathrm{Sel}(\mathbf{Z}[1/m], E[p^N])$". (We use $\mathrm{Sel}(\mathbf{Z}[1/m], E[p^N])$ for $m \in \mathcal{N}_1^{(N)}$ in this paper, but $E[p^N]$ is not an étale sheaf on $\mathrm{Spec}\,\mathbf{Z}[1/m]$ for such m.)

Let λ be the λ-invariant of $\mathrm{Sel}(E/\mathbf{Q}_\infty, E[p^\infty])^\vee$. We put $n_\lambda = \min\{n \in \mathbf{Z} \mid p^n - 1 \geq \lambda\}$ and $d_n = n_\lambda + Nn$ for $n \in \mathbf{Z}_{\geq 0}$. We define
$$\mathcal{P}_1^{(N,n)} = \{\ell \in \mathcal{P}_1^{(N)} \mid \ell \equiv 1 \pmod{p^{d_n}}\} \tag{1.4}$$

(then $\mathcal{P}_1^{(N,n)} \subset \mathcal{P}_1^{(N)}(\mathbf{Q}_{[n]})$ holds, see the end of §3.1 for this fact, and see §3.1 for the definition of the set $\mathcal{P}_1^{(N)}(\mathbf{Q}_{[n]})$). We denote by $\mathcal{N}_1^{(N,n)}$ the set of squarefree products of primes in $\mathcal{P}_1^{(N,n)}$.

In this paper, for any finite abelian p-extension $K/\mathbf{Q}$ in which all bad primes of E are unramified, we prove in §4 the following theorem for $\mathbf{Z}/p^N[\mathrm{Gal}(K/\mathbf{Q})]$-modules $\mathrm{Sel}(E/K, E[p^N])$ and $\mathrm{Sel}(O_K[1/m], E[p^N])$ (see Corollary 4.1.3 and Theorem 4.2.1). We simply state it in the case $K = \mathbf{Q}$ below. An essential ingredient in this paper is the Kolyvagin system of Gauss sum type. We construct Kolyvagin systems $\kappa_{m,\ell} \in \mathrm{Sel}(\mathbf{Z}[1/m\ell], E[p^N])$ for (m, ℓ) satisfying $\ell \in \mathcal{P}_1^{(N,\epsilon(m\ell)+1)}$ and $m\ell \in \mathcal{N}_1^{(N,\epsilon(m\ell)+1)}$ (see §3.4 and Propositions 3.4.2) by the method in [12]. (We can construct these elements, using the half of the main conjecture proved by Kato [7].) The essential difference between our Kolyvagin systems $\kappa_{m,\ell}$ of Gauss sum type and Kolyvagin systems in Mazur and Rubin [14] is that our $\kappa_{m,\ell}$ is related to L-values. In particular, $\kappa_{m,\ell}$ satisfies a remarkable property $\phi_\ell(\kappa_{m,\ell}) = -\delta_{m\ell} t_{\ell,K}$ (see Propositions 3.4.2 (4)) though we do not explain the notation here.

Theorem 1.2.3 *Assume that* $\mathrm{ord}_p(\tilde{\delta}_m) = 0$ *for some* $m \in \mathcal{N}_1^{(N)}$.
(1) *The canonical homomorphism*

$$s_m : \mathrm{Sel}(E/\mathbf{Q}, E[p^N]) \longrightarrow \bigoplus_{\ell | m} E(\mathbf{Q}_\ell) \otimes \mathbf{Z}/p^N \simeq \bigoplus_{\ell | m} E(\mathbf{Q}_\ell) \otimes \mathbf{Z}/p^N \simeq (\mathbf{Z}/p^N)^{\epsilon(m)}$$

is injective.
(2) *Assume further that* $m \in \mathcal{N}_1^{(N,\epsilon(m)+1)}$ *and that* m *is admissible (for the definition of the notion "admissible", see the paragraph before Proposition 3.3.2). Then* $\mathrm{Sel}(\mathbf{Z}[1/m], E[p^N])$ *is a free* $\mathbf{Z}/p^N$*-module of rank* $\epsilon(m)$*, and* $\{\kappa_{\frac{m}{\ell},\ell}\}_{\ell | m}$ *is a basis of* $\mathrm{Sel}(\mathbf{Z}[1/m], E[p^N])$.
(3) *We define a matrix* $\mathcal{A}$ *as in* (4.1) *in Theorem* 4.2.1*, using* $\kappa_{\frac{m}{\ell},\ell}$*. Then* $\mathcal{A}$ *is a relation matrix of the Pontrjagin dual* $\mathrm{Sel}(E/\mathbf{Q}, E[p^N])^\vee$ *of the Selmer group; namely if* $f_{\mathcal{A}} : (\mathbf{Z}/p^N)^{\epsilon(m)} \longrightarrow (\mathbf{Z}/p^N)^{\epsilon(m)}$ *is the homomorphism corresponding to the above matrix* $\mathcal{A}$*, then we have*

$$\mathrm{Coker}(f_{\mathcal{A}}) \simeq \mathrm{Sel}(E/\mathbf{Q}, E[p^N])^\vee.$$

It is worth noting that we get nontrivial (moreover, linearly independent) elements in the Selmer groups.

The ideals $\Theta_i(\mathbf{Q})^{(\delta)}$ in Theorem 1.1.1 are not suitable for numerical computations because we have to compute *infinitely many* $\tilde{\delta}_m$. On the other hand, we can easily find m with $\mathrm{ord}_p(\tilde{\delta}_m) = 0$ numerically. Since s_m is injective, we can get information of the Selmer group from the image of s_m, which is an advantage of Theorem 1.2.3 and the next Theorem 1.2.5 (see also the comment in the end of Example (5) in §5.3).

We next consider the case $N = 1$, so $\mathrm{Sel}(E/\mathbf{Q}, E[p])$. Now we regard $\tilde{\delta}_m$ as an element of $\mathbf{F}_p$ for $m \in \mathcal{N}_1^{(1)}$. We say m is *δ-minimal* if $\tilde{\delta}_m \neq 0$

and $\tilde{\delta}_d = 0$ for all divisors d of m with $1 \leq d < m$. Our next conjecture claims that the structure (the dimension) of $\mathrm{Sel}(E/\mathbf{Q}, E[p])$ is determined by a δ-minimal m, therefore can be easily computed numerically.

Conjecture 1.2.4 *If $m \in \mathcal{N}_1^{(1)}$ is δ-minimal, the canonical homomorphism*

$$s_m : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow \bigoplus_{\ell | m} E(\mathbf{Q}_\ell) \otimes \mathbf{Z}/p \simeq \bigoplus_{\ell | m} E(\mathbf{F}_\ell) \otimes \mathbf{Z}/p \simeq (\mathbf{Z}/p^N)^{\epsilon(m)}$$

is bijective. In particular, $\dim_{\mathbf{F}_p} \mathrm{Sel}(E/\mathbf{Q}, E[p]) = \epsilon(m)$.

If $m \in \mathcal{N}_1^{(1)}$ is δ-minimal, the above homomorphism $s_m : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow (\mathbf{Z}/p^N)^{\epsilon(m)}$ is injective by Theorem 1.2.3 (1), so we know

$$\dim_{\mathbf{F}_p} \mathrm{Sel}(E/\mathbf{Q}, E[p]) \leq \epsilon(m).$$

Therefore, the problem is in showing the other inequality.

We note that the analogue of the above conjecture for ideal class groups does not hold (see §5.4). But we hope that Conjecture 1.2.4 holds for the Selmer groups of elliptic curves. We construct in §5 a modified version $\kappa_{m,\ell}^{q,q',z}$ of Kolyvagin systems of Gauss sum type for any (m, ℓ) with $m\ell \in \mathcal{N}_1^{(N)}$. (The Kolyvagin system $\kappa_{m,\ell}$ in §3 is defined for (m, ℓ) with $m\ell \in \mathcal{N}_1^{(N,\epsilon(m\ell)+1)}$, but $\kappa_{m,\ell}^{q,q',z}$ is defined for more general (m, ℓ), namely for (m, ℓ) with $m\ell \in \mathcal{N}_1^{(N)}$.) Using the modified Kolyvagin system $\kappa_{m,\ell}^{q,q',z}$, we prove the following.

Theorem 1.2.5 (1) *If $\epsilon(m) = 0$, 1, then Conjecture* 1.2.4 *is true.*
(2) *If there is $\ell \in \mathcal{P}^{(1)}$ which is δ-minimal (so $\epsilon(\ell) = 1$), then*

$$\mathrm{Sel}(E/\mathbf{Q}, E[p^\infty]) \simeq \mathbf{Q}_p/\mathbf{Z}_p.$$

Moreover, if there is $\ell \in \mathcal{P}_1^{(1)}$ which is δ-minimal and which satisfies $\ell \equiv 1$ (mod $p^{n_{\lambda'}+2}$) where λ' is the analytic λ-invariant of $(E, \mathbf{Q}_\infty/\mathbf{Q})$, then the main conjecture (2.5) *for* $\mathrm{Sel}(E/\mathbf{Q}_\infty, E[p^\infty])$ *holds true. In this case,* $\mathrm{Sel}(E/\mathbf{Q}_\infty, E[p^\infty])^\vee$ *is generated by one element as a* $\mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$*-module.*
(3) *If $\epsilon(m) = 2$ and m is admissible, then Conjecture* 1.2.4 *is true.*
(4) *Suppose that $\epsilon(m) = 3$ and $m = \ell_1\ell_2\ell_3$. Assume that m is admissible and the natural maps $s_{\ell_i} : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow E(\mathbf{F}_{\ell_i}) \otimes \mathbf{Z}/p$ are surjective both for $i = 1$ and $i = 2$. Then Conjecture* 1.2.4 *is true.*

In this way, we can determine the Selmer groups by finite numbers of computations in several cases. We give several numerical examples in §5.2.

Remark 1.2.6 Concerning the Fitting ideals and the annihilator ideals of some Selmer groups, we prove the following in this paper. Let $K/\mathbf{Q}$ be a finite abelian p-extension in which all bad primes of E are unramified. We take a finite set S of good reduction primes, which contains all ramifying primes in $K/\mathbf{Q}$ except p. Let m be the product of primes in S. We prove that the initial Fitting ideal of the $R_K = \mathbf{Z}_p[\mathrm{Gal}(K/\mathbf{Q})]$-module $\mathrm{Sel}(O_K[1/m], E[p^\infty])^\vee$ is principal, and

$$\xi_{K,S} \in \mathrm{Fitt}_{0,R_K}(\mathrm{Sel}(O_K[1/m], E[p^\infty])^\vee)$$

where $\xi_{K,S}$ is an element of R_K which is explicitly constructed from modular symbols (see (2.13)). If the main conjecture (2.5) for $(E, \mathbf{Q}_\infty/\mathbf{Q})$ holds, the equality $\mathrm{Fitt}_{0,R_K}(\mathrm{Sel}(O_K[1/m], E[p^\infty])^\vee) = \xi_{K,S}R_K$ holds (see Remark 2.3.2). We prove the Iwasawa theoretical version in Theorem 2.2.2.

Let ϑ_K be the image of the p-adic L-function, which is also explicitly constructed from modular symbols. We show in Theorem 2.3.1

$$\vartheta_K \in \mathrm{Ann}_{R_K}(\mathrm{Sel}(O_K[1/m], E[p^\infty])^\vee).$$

Concerning the higher Fitting ideals (cf. §2.4), we show

$$\tilde{\delta}_m \in \mathrm{Fitt}_{\epsilon(m),\mathbf{Z}/p^N}(\mathrm{Sel}(E/\mathbf{Q}, E[p^N])^\vee)$$

where $\mathrm{Fitt}_{i,R}(M)$ is the i-th Fitting ideal of an R-module M. We prove a slightly generalized version for K which is in the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty$ of $\mathbf{Q}$ (see Theorem 2.4.1 and Corollary 2.4.2).

I would like to thank John Coates heartily for his helpful advice and for discussion with him, especially for the discussion in March 2013, which played an essential role in my producing this paper. I also thank heartily Kazuya Kato for his constant interest in the results of this paper. I also thank Kazuo Matsuno and Christian Wuthrich very much for their helping me to compute modular symbols.

2 Selmer groups and p-adic L-functions

2.1 Modular symbols and p-adic L-functions

Let E be an elliptic curve over $\mathbf{Q}$, and $f(z) = \Sigma a_n e^{2\pi i n z}$ the modular form corresponding to E. In this section, we assume that p is a prime number satisfying (i), (ii), (iii) in §1.1. We define $\mathcal{P}_{good} = \{\ell \mid \ell \text{ is a good reduction prime for } E\ \} \setminus \{p\}$. For any finite abelian extension $K/\mathbf{Q}$, we denote by K_∞/K the cyclotomic $\mathbf{Z}_p$-extension. For a real abelian field K of conductor

m, we define $\tilde{\theta}_K$ to be the image of $\tilde{\theta}_{\mathbf{Q}(\mu_m)}$ in $\mathbf{Q}[\mathrm{Gal}(K/\mathbf{Q})]$ where $\tilde{\theta}_{\mathbf{Q}(\mu_m)}$ is defined in (1.1).

We write

$$R_K = \mathbf{Z}_p[\mathrm{Gal}(K/\mathbf{Q})] \text{ and } \Lambda_{K_\infty} = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/\mathbf{Q})]].$$

For any positive integer n, we simply write $R_{\mathbf{Q}(\mu_n)} = R_n$ in this subsection. For any positive integers d, c such that $d \mid c$, we define the norm map $\nu_{c,d} : R_d = \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}(\mu_d)/\mathbf{Q})] \longrightarrow R_c = \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}(\mu_c)/\mathbf{Q})]$ by $\sigma \mapsto \sum \tau$ where for $\sigma \in \mathrm{Gal}(\mathbf{Q}(\mu_d)/\mathbf{Q})$, τ runs over all elements of $\mathrm{Gal}(\mathbf{Q}(\mu_c)/\mathbf{Q})$ such that the restriction of τ to $\mathbf{Q}(\mu_d)$ is σ. Let m be a squarefree product of primes in $\mathcal{P}_{good}$, and n a positive integer. By our assumption (ii), we know $\tilde{\theta}_{\mathbf{Q}(\mu_{mp^n})} \in R_{mp^n}$ (cf. [27]). Let $\alpha \in \mathbf{Z}_p^\times$ be the unit root of $x^2 - a_p x + p = 0$ and put

$$\vartheta_{\mathbf{Q}(\mu_{mp^n})} = \alpha^{-n}(\tilde{\theta}_{\mathbf{Q}(\mu_{mp^n})} - \alpha^{-1}\nu_{mp^n,mp^{n-1}}(\tilde{\theta}_{\mathbf{Q}(\mu_{mp^{n-1}})})) \in R_{mp^n}$$

as usual. Then $\{\vartheta_{\mathbf{Q}(\mu_{mp^n})}\}_{n\geq 1}$ is a projective system (cf. Mazur and Tate [16] the equation (4) on page 717) and we obtain an element $\vartheta_{\mathbf{Q}(\mu_{mp^\infty})} \in \Lambda_{\mathbf{Q}(\mu_{mp^\infty})}$, which is the p-adic L-function of Mazur and Swinnerton-Dyer.

We also use the notation $\Lambda_{np^\infty} = \Lambda_{\mathbf{Q}(\mu_{np^\infty})}$ for simplicity. Suppose that a prime ℓ does not divide mp, and $c_{m\ell,m} : \Lambda_{m\ell p^\infty} \longrightarrow \Lambda_{mp^\infty}$ is the natural restriction map. Then we know

$$c_{m\ell,m}(\vartheta_{\mathbf{Q}(\mu_{m\ell p^\infty})}) = (a_\ell - \sigma_\ell - \sigma_\ell^{-1})\vartheta_{\mathbf{Q}(\mu_{mp^\infty})} \tag{2.1}$$

(cf. Mazur and Tate [16] the equation (1) on page 717).

We will construct a slightly modified element $\xi_{\mathbf{Q}(\mu_{mp^\infty})}$ in Λ_{mp^∞}. We put $P'_\ell(x) = x^2 - a_\ell x + \ell$. Let m be a squarefree product of $\mathcal{P}_{good}$. For any divisor d of m and a prime divisor ℓ of m/d, $\sigma_\ell \in \mathrm{Gal}(\mathbf{Q}(\mu_{dp^\infty})/\mathbf{Q}) = \varprojlim \mathrm{Gal}(\mathbf{Q}(\mu_{dp^n})/\mathbf{Q})$ is defined as the projective limit of $\sigma_\ell \in \mathrm{Gal}(\mathbf{Q}(\mu_{dp^n})/\mathbf{Q})$. We consider $P'_\ell(\sigma_\ell) \in \Lambda_{dp^\infty}$. Note that

$$-\sigma_\ell^{-1} = (-\sigma_\ell^{-1}P'_\ell(\sigma_\ell) - (a_\ell - \sigma_\ell - \sigma_\ell^{-1}))/(\ell - 1) \in \Lambda_{dp^\infty}. \tag{2.2}$$

We put $\alpha_{d,m} = (\prod_{\ell \mid \frac{m}{d}}(-\sigma_\ell^{-1}))\vartheta_{\mathbf{Q}(\mu_{dp^\infty})} \in \Lambda_{dp^\infty}$ and

$$\xi_{\mathbf{Q}(\mu_{mp^\infty})} = \sum_{d \mid m} \nu_{m,d}(\alpha_{d,m}) \in \Lambda_{mp^\infty}$$

where $\nu_{m,d} : \Lambda_{dp^\infty} \longrightarrow \Lambda_{mp^\infty}$ is the norm map defined similarly as above. (This modification $\xi_{\mathbf{Q}(\mu_{mp^\infty})}$ is done by the same spirit as Greither [5] in which the Deligne-Ribet p-adic L-functions are treated.) Suppose that $\ell \in$

$\mathcal{P}_{good}$ is prime to m. Then by the definition of $\xi_{\mathbf{Q}(\mu_{mp^\infty})}$ and (2.1) and (2.2), we have

$$\begin{aligned}
c_{m\ell,m}(\xi_{\mathbf{Q}(\mu_{m\ell p^\infty})}) &= c_{m\ell,m}(\sum_{d|m}\nu_{m\ell,d}(\alpha_{d,m\ell})+\sum_{d|m}\nu_{m\ell,d\ell}(\alpha_{d\ell,m\ell})) \\
&= (\ell-1)\sum_{d|m}\nu_{m,d}(-\sigma_\ell^{-1}\alpha_{d,m})+\sum_{d|m}\nu_{m,d}(c_{d\ell,d}(\alpha_{d\ell,m\ell})) \\
&= (\ell-1)\sum_{d|m}\nu_{m,d}(-\sigma_\ell^{-1}\alpha_{d,m})+\sum_{d|m}\nu_{m,d}((a_\ell-\sigma_\ell-\sigma_\ell^{-1})\alpha_{d,m}) \\
&= (-\sigma_\ell^{-1}P'_\ell(\sigma_\ell))\sum_{d|m}\nu_{m,d}(\alpha_{d,m}) \\
&= (-\sigma_\ell^{-1}P'_\ell(\sigma_\ell))\xi_{\mathbf{Q}(\mu_{mp^\infty})}. \qquad (2.3)
\end{aligned}$$

We denote by $\vartheta_{\mathbf{Q}(\mu_m)}\in R_{\mathbf{Q}(\mu_m)}$ the image of $\vartheta_{\mathbf{Q}(\mu_{mp^\infty})}$ under the natural map $\Lambda_{\mathbf{Q}(\mu_{mp^\infty})}\longrightarrow R_{\mathbf{Q}(\mu_m)}$. We have

$$\vartheta_{\mathbf{Q}(\mu_m)}=(1-\frac{\sigma_p}{\alpha})(1-\frac{\sigma_p^{-1}}{\alpha})\tilde{\theta}_{\mathbf{Q}(\mu_m)}. \qquad (2.4)$$

Since we are assuming $a_p\not\equiv 1 \pmod p$, we also have $\alpha\not\equiv 1 \pmod p$, so $(1-\frac{\sigma_p}{\alpha})(1-\frac{\sigma_p^{-1}}{\alpha})$ is a unit in $R_{\mathbf{Q}(m)}$ where $\mathbf{Q}(m)$ is the maximal p-subextension of $\mathbf{Q}$ in $\mathbf{Q}(\mu_m)$.

2.2 Selmer groups

For any algebraic extension $F/\mathbf{Q}$, we denote by O_F the integral closure of $\mathbf{Z}$ in F. For a positive integer $m>0$, we define a Selmer group $\mathrm{Sel}(O_F[1/m],E[p^\infty])$ by

$$\mathrm{Sel}(O_F[1/m],E[p^\infty])=\mathrm{Ker}(H^1(F,E[p^\infty])\longrightarrow\prod_{v\nmid m}H^1(F_v,E[p^\infty])/E(F_v)\otimes\mathbf{Q}_p/\mathbf{Z}_p)$$

where v runs over all primes of F which are prime to m. Similarly, for a positive integer N, we define $\mathrm{Sel}(O_F[1/m],E[p^N])$ by

$$\mathrm{Sel}(O_F[1/m],E[p^N])=\mathrm{Ker}(H^1(F,E[p^N])\longrightarrow\prod_{v\nmid m}H^1(F_v,E[p^N])/E(F_v)\otimes\mathbf{Z}/p^N).$$

In the case $m=1$, we denote them by $\mathrm{Sel}(O_F,E[p^\infty])$, $\mathrm{Sel}(O_F,E[p^N])$, which are classical Selmer groups. We also use the notation $\mathrm{Sel}(E/F,E[p^\infty])$, $\mathrm{Sel}(E/F,E[p^N])$ for them, namely

$$\mathrm{Sel}(E/F,E[p^\infty])=\mathrm{Sel}(O_F,E[p^\infty]),\quad \mathrm{Sel}(E/F,E[p^N])=\mathrm{Sel}(O_F,E[p^N]).$$

For a finite abelian extension $K/\mathbf{Q}$, we denote by K_∞/K the cyclotomic $\mathbf{Z}_p$-extension, and put $\Lambda_{K_\infty} = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/\mathbf{Q})]]$. The Pontrjagin dual $\mathrm{Sel}(O_{K_\infty}, E[p^\infty])^\vee$ is a torsion Λ_{K_∞}-module (Kato [7] Theorem 17.4).

When the conductor of K is m, we define $\vartheta_{K_\infty} \in \Lambda_{K_\infty}$ to be the image of $\vartheta_{\mathbf{Q}(\mu_{mp^\infty})}$, and also $\xi_{K_\infty} \in \Lambda_{K_\infty}$ to be the image of $\xi_{\mathbf{Q}(\mu_{mp^\infty})}$. The Iwasawa main conjecture for $(E, \mathbf{Q}_\infty/\mathbf{Q})$ is the equality between the characteristic ideal of the Selmer group and the ideal generated by the p-adic L-function;

$$\mathrm{char}(\mathrm{Sel}(O_{\mathbf{Q}_\infty}, E[p^\infty])^\vee) = \vartheta_{\mathbf{Q}_\infty}\Lambda_{\mathbf{Q}_\infty}. \tag{2.5}$$

Since we are assuming the Galois action on the Tate module is surjective, we know $\vartheta_{\mathbf{Q}_\infty} \in \mathrm{char}(\mathrm{Sel}(O_{\mathbf{Q}_\infty}, E[p^\infty])^\vee)$ by Kato [7] Theorem 17.4. Skinner and Urban [26] proved the equality (2.5) under mild conditions. Namely, under our assumptions (i), (ii), they proved the main conjecture (2.5) if there is a bad prime ℓ which is ramified in $\mathbf{Q}(E[p])$ ([26] Theorem 3.33).

More generally, let ψ be an even Dirichlet character and K be the abelian field corresponding to the kernel of ψ, namely K is the field such that ψ induces a faithful character of $\mathrm{Gal}(K/\mathbf{Q})$. We assume $K \cap \mathbf{Q}_\infty = \mathbf{Q}$. In this paper, for any finite abelian p-group G, any $\mathbf{Z}_p[G]$-module M and any character $\psi : G \longrightarrow \overline{\mathbf{Q}}_p^\times$, we define the ψ-quotient M_ψ by $M \otimes_{\mathbf{Z}_p[G]} O_\psi$ where $O_\psi = \mathbf{Z}_p[\mathrm{Image}\,\psi]$ which is regarded as a $\mathbf{Z}_p[G]$-module by $\sigma x = \psi(\sigma)x$ for any $\sigma \in G$ and $x \in O_\psi$. We consider $(\mathrm{Sel}(O_{K_\infty}, E[p^\infty])^\vee)_\psi$, which is a Λ_ψ-module where $\Lambda_\psi = (\Lambda_{K_\infty})_\psi = O_\psi[[\mathrm{Gal}(K_\infty/K)]]$. We denote the image of ϑ_{K_∞} in Λ_ψ by $\psi(\vartheta_{K_\infty})$. Then the main conjecture states

$$\mathrm{char}((\mathrm{Sel}(O_{K_\infty}, E[p^\infty])^\vee)_\psi) = \psi(\vartheta_{K_\infty})\Lambda_\psi. \tag{2.6}$$

We also note that $\psi(\vartheta_{K_\infty})\Lambda_\psi = \psi(\xi_{K_\infty})\Lambda_\psi$. By Kato [7], we know $\psi(\vartheta_{K_\infty})$, $\psi(\xi_{K_\infty}) \in \mathrm{char}((\mathrm{Sel}(O_{K_\infty}, E[p^\infty])^\vee)_\psi)$.

Let $S \subset \mathcal{P}_{good}$ be a finite set of good primes, and $K/\mathbf{Q}$ be a finite abelian extension. We denote by $S_{\mathrm{ram}}(K)$ the subset of S which consists of all ramifying primes in K inside S. Recall that $P'_\ell(x) = x^2 - a_\ell x + \ell$. We define

$$\xi_{K_\infty,S} = \xi_{K_\infty} \prod_{\ell \in S \setminus S_{\mathrm{ram}}(K)} (-\sigma_\ell^{-1} P'_\ell(\sigma_\ell)).$$

So $\xi_{K_\infty,S} = \xi_{K_\infty}$ if S contains only ramifying primes in K. Suppose that S contains all ramifying primes in K and F is a subfield of K. We denote by $c_{K_\infty/F_\infty} : \Lambda_{K_\infty} \longrightarrow \Lambda_{F_\infty}$ the natural restriction map. Using (2.3) and the above definition of $\xi_{K_\infty,S}$, we have

$$c_{K_\infty/F_\infty}(\xi_{K_\infty,S}) = \xi_{F_\infty,S}. \tag{2.7}$$

For any positive integer m whose prime divisors are in $\mathcal{P}_{good}$, we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}(O_{K_\infty}, E[p^\infty]) \longrightarrow \mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty]) \longrightarrow \bigoplus_{v|m} H^1(K_{\infty,v}, E[p^\infty]) \longrightarrow 0$$

because $E(K_{\infty,v}) \otimes \mathbf{Q}_p/\mathbf{Z}_p = 0$ (for the surjectivity of the third map, see Greenberg Lemma 4.6 in [3]). For a prime v of K_∞, let $K_{\infty,v,nr}/K_{\infty,v}$ be the maximal unramified extension, and $\Gamma_v = \mathrm{Gal}(K_{\infty,v,nr}/K_{\infty,v})$. Suppose v divides m. Since v is a good reduction prime, we have $H^1(K_{\infty,v}, E[p^\infty]) = \mathrm{Hom}_{Cont}(G_{K_{\infty,v,nr}}, E[p^\infty])^{\Gamma_v} = E[p^\infty](-1)^{\Gamma_v}$ where (-1) is the Tate twist. By the Weil pairing, the Pontrjagin dual of $E[p^\infty](-1)$ is the Tate module $T_p(E)$. Therefore, taking the Pontrjagin dual of the above exact sequence, we have an exact sequence

$$0 \longrightarrow \bigoplus_{v|m} T_p(E)_{\Gamma_v} \longrightarrow \mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee \longrightarrow \mathrm{Sel}(O_{K_\infty}, E[p^\infty])^\vee \longrightarrow 0. \tag{2.8}$$

Note that $T_p(E)_{\Gamma_v}$ is free over $\mathbf{Z}_p$ because Γ_v is profinite of order prime to p.

Let $K/\mathbf{Q}$ be a finite abelian p-extension in which all bad primes of E are unramified. Suppose that S is a finite subset of $\mathcal{P}_{good}$ such that S contains all ramifying primes in $K/\mathbf{Q}$ except p. Let m be a squarefree product of all primes in S.

Theorem 2.2.1 (Greenberg) $\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee$ *is of projective dimension* ≤ 1 *as a* Λ_{K_∞}*-module.*

This is proved by Greenberg in [4] Theorem 1 (the condition (iv) in §1.1 in this paper is not needed here, see also Proposition 3.3.1 in [4]). For more general p-adic representations, this is proved in [12] Proposition 1.6.7. We will give a sketch of the proof because some results in the proof will be used later.

Since we can take some finite abelian extension $K'/\mathbf{Q}$ such that $K_\infty = K'_\infty$ and $K' \cap \mathbf{Q}_\infty = \mathbf{Q}$, we may assume that $K \cap \mathbf{Q}_\infty = \mathbf{Q}$ and p is unramified in K. Since we are assuming that $E[p]$ is an irreducible $G_{\mathbf{Q}}$-module, we know that $\mathrm{Sel}(O_{K_\infty}, E[p^\infty])^\vee$ has no nontrivial finite $\mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-submodule by Greenberg ([3] Propositions 4.14, 4.15). We also assumed that the μ-invariant of $\mathrm{Sel}(O_{\mathbf{Q}_\infty}, E[p^\infty])^\vee$ is zero, which implies the vanishing of the μ-invariant of $\mathrm{Sel}(O_{K_\infty}, E[p^\infty])^\vee$ by Hachimori and Matsuno [6]. Therefore, $\mathrm{Sel}(O_{K_\infty}, E[p^\infty])^\vee$ is a free $\mathbf{Z}_p$-module of finite rank. By the exact sequence (2.8), $\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee$ is also a free $\mathbf{Z}_p$-module of finite rank.

Put $G = \mathrm{Gal}(K/\mathbf{Q})$. By the definition of the Selmer group and our assumption that all primes dividing m are good reduction primes, we have $\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^G = \mathrm{Sel}(O_{\mathbf{Q}_\infty}[1/m], E[p^\infty])$. Since we assumed that the μ-invariant is zero, $\mathrm{Sel}(O_{\mathbf{Q}_\infty}[1/m], E[p^\infty])$ is divisible. This shows that the corestriction map $\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty]) \longrightarrow \mathrm{Sel}(O_{\mathbf{Q}_\infty}[1/m], E[p^\infty])$ is surjective. Therefore, $\hat{H}^0(G, \mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])) = 0$.

Next we will show that $H^1(G, \mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])) = 0$. Let N_E be the conductor of E and put $m' = mpN_E$. We know $\mathrm{Sel}(O_{K_\infty}[1/m'], E[p^\infty])$ is equal to the étale cohomology group $H^1_{et}(\mathrm{Spec}\, O_{K_\infty}[1/m'], E[p^\infty])$. We have an exact sequence

$$0 \longrightarrow \mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty]) \longrightarrow \mathrm{Sel}(O_{K_\infty}[1/m'], E[p^\infty]) \longrightarrow \bigoplus_{v \mid \frac{m'}{m}} H^2_v(K_{\infty,v}) \longrightarrow 0 \tag{2.9}$$

where $H^2_v(K_{\infty,v}) = H^1(K_{\infty,v}, E[p^\infty])/(E(K_{\infty,v}) \otimes \mathbf{Q}_p/\mathbf{Z}_p)$, and the surjectivity of the third map follows from Greenberg Lemma 4.6 in [3]. Let $E[p^\infty]^0$ be the kernel of $E[p^\infty] = E(\overline{\mathbf{Q}})[p^\infty] \longrightarrow E(\overline{\mathbf{F}}_p)[p^\infty]$ and $E[p^\infty]_{et} = E[p^\infty]/E[p^\infty]^0$. For a prime v of K_∞ above p, we denote by $K_{\infty,v,nr}$ the maximal unramified extension of $K_{\infty,v}$, and put $\Gamma_v = \mathrm{Gal}(K_{\infty,v,nr}/K_{\infty,v})$. We know the isomorphism $H^2_v(K_{\infty,v}) \xrightarrow{\simeq} H^1(K_{\infty,v,nr}, E[p^\infty]_{et})^{\Gamma_v}$ by Greenberg [2] §2. If v is a prime of K_∞ not above p, we know $H^2_v(K_{\infty,v}) = H^1(K_{\infty,v}, E[p^\infty])$. Therefore, we get an isomorphism

$$(\bigoplus_{v \mid \frac{m'}{m}} H^2_v(K_{\infty,v}))^G = \bigoplus_{u \mid \frac{m'}{m}} H^2_u(\mathbf{Q}_{\infty,v})$$

where v (resp. u) runs over all primes of K_∞ (resp. $\mathbf{Q}_\infty$) above $m'/m = pN_E$. Thus, $\mathrm{Sel}(O_{K_\infty}[1/m'], E[p^\infty])^G \longrightarrow \bigoplus_{v \mid \frac{m'}{m}} H^2_v(K_{\infty,v})^G$ is surjective. On the other hand, we have $H^2_{et}(\mathrm{Spec}\, O_{K_\infty}[1/m'], E[p^\infty]) = 0$ (see [2] Propositions 3, 4). This implies that

$$H^1(G, H^1_{et}(\mathrm{Spec}\, O_{K_\infty}[1/m'], E[p^\infty])) = H^1(G, \mathrm{Sel}(O_{K_\infty}[1/m'], E[p^\infty])) = 0.$$

Taking the cohomology of the exact sequence (2.9), we get

$$H^1(G, \mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])) = 0. \tag{2.10}$$

Therefore, $\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])$ is cohomologically trivial as a G-module by Serre [25] Chap. IX Théorème 8. This implies that $\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee$ is also cohomologically trivial. Since $\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee$ has no nontrivial finite submodule, the projective dimension of $\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee$ as a Λ_{K_∞}-module is ≤ 1 by Popescu [20] Proposition 2.3.

Theorem 2.2.2 *Let $K/\mathbf{Q}$ be a finite abelian p-extension in which all bad primes of E are unramified. We take a finite set S of good reduction primes which contains all ramifying primes in $K/\mathbf{Q}$ except p. Let m be the product of primes in S. Then*
(1) *$\xi_{K_\infty,S}$ is in the initial Fitting ideal* $\mathrm{Fitt}_{0,\Lambda_{K_\infty}}(\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee)$.
(2) *We have*

$$\mathrm{Fitt}_{0,\Lambda_{K_\infty}}(\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee) = \xi_{K_\infty,S}\Lambda_{K_\infty}$$

if and only if the main conjecture (2.5) for $(E, \mathbf{Q}_\infty/\mathbf{Q})$ holds.

Proof. As we explained in the proof of Theorem 2.2.1, we may assume that $K \cap \mathbf{Q}_\infty = \mathbf{Q}$. We recall that $\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee$ is a free $\mathbf{Z}_p$-module of finite rank under our assumptions.

(1) Let $\psi : \mathrm{Gal}(K/\mathbf{Q}) \longrightarrow \overline{\mathbf{Q}}_p^\times$ be a character of $\mathrm{Gal}(K/\mathbf{Q})$, not necessarily faithful. We study the Fitting ideal of the ψ-quotient $(\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee)_\psi = \mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee \otimes_{\mathbf{Z}_p[\mathrm{Gal}(K/\mathbf{Q})]} O_\psi$. We denote by F the subfield of K corresponding to the kernel of ψ. We regard ψ as a faithful character of $\mathrm{Gal}(F/\mathbf{Q})$. Since $\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^{\mathrm{Gal}(K/F)} = \mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])$, we have

$$(\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee)_\psi = (\mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])^\vee)_\psi$$

where the right hand side is defined to be $\mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])^\vee \otimes_{\mathbf{Z}_p[\mathrm{Gal}(F/\mathbf{Q})]} O_\psi$.

We put $\Lambda_\psi = (\Lambda_{F_\infty})_\psi$. The group homomorphism ψ induces the ring homomorphism $\Lambda_{F_\infty} \longrightarrow \Lambda_\psi$ which we also denote by ψ. The composition with $c_{K_\infty/F_\infty} : \Lambda_{K_\infty} \longrightarrow \Lambda_{F_\infty}$ and the above ring homomorphism ψ is also denoted by $\psi : \Lambda_{K_\infty} \longrightarrow \Lambda_\psi$. Note that $F/\mathbf{Q}$ is a cyclic extension of degree a power of p. We denote by F' the subfield of F such that $[F : F'] = p$. We put $N_0 = N_{\mathrm{Gal}(F/F')} = \Sigma_{\sigma \in \mathrm{Gal}(F/F')}\sigma$. If we put $[F : \mathbf{Q}] = p^c$ and take a generator γ of $\mathrm{Gal}(F/\mathbf{Q})$, $N_0 = \Sigma_{i=0}^{p-1}\gamma^{p^{c-1}i}$ is a cyclotomic polynomial and $O_\psi = \mathbf{Z}_p[\mu_{p^c}] \simeq \mathbf{Z}_p[\mathrm{Gal}(F/\mathbf{Q})]/N_0$. For any $\mathbf{Z}_p[\mathrm{Gal}(F/\mathbf{Q})]$-module M, we define $M^\psi = \mathrm{Ker}(N_0 : M \longrightarrow M)$. Then the Pontrjagin dual of M^ψ is $(M^\psi)^\vee = (M^\vee)/N_0 = (M^\vee)_\psi$. By the same method as the proof of (2.10), we have $H^1(\mathrm{Gal}(F/F'), \mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])) = 0$. Therefore, $\sigma - 1 : \mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty]) \longrightarrow \mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])^\psi$ is surjective where $\sigma = \gamma^{p^{c-1}}$ is a generator of $\mathrm{Gal}(F/F')$. Therefore, taking the dual, we know that there is an injective homomorphism from $(\mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])^\vee)_\psi$ to $\mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])^\vee$ which is a free $\mathbf{Z}_p$-module. Therefore, $(\mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])^\vee)_\psi$ contains no nontrivial finite Λ_ψ-submodule. This shows that

$$\mathrm{Fitt}_{0,\Lambda_\psi}((\mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])^\vee)_\psi) = \mathrm{char}((\mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])^\vee)_\psi).$$

Consider the ψ-quotient of the exact sequence (2.8);

$$(\bigoplus_{v|m} T_p(E)_{\Gamma_v})_\psi \longrightarrow (\mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])^\vee)_\psi \longrightarrow (\mathrm{Sel}(O_{F_\infty}, E[p^\infty])^\vee)_\psi \longrightarrow 0$$

where v runs over all primes of F_∞ above m. Since $\mathrm{Ext}^1_{\mathbf{Z}_p[\mathrm{Gal}(F/\mathbf{Q})]}(O_\psi, \mathrm{Sel}(O_{F_\infty}, E[p^\infty])) = \hat{H}^0(\mathrm{Gal}(F/\mathbf{Q}), \mathrm{Sel}(O_{F_\infty}, E[p^\infty]))$ is finite, the first map of the above exact sequence has finite kernel.

Suppose that ℓ is a prime divisor of m. If ℓ is unramified in F, we have

$$\mathrm{Fitt}_{0,\Lambda_\psi}((\bigoplus_{v|\ell} T_p(E)_{\Gamma_v})_\psi) = P'_\ell(\sigma_\ell)\Lambda_\psi$$

where $P'_\ell(x) = x^2 - a_\ell x + \ell$. If ℓ is ramified in F, $\psi(\ell) = 0$ and $(\bigoplus_{v|\ell} T_p(E)_{\Gamma_v})_\psi$ is finite. Therefore, we have

$$\mathrm{char}((\bigoplus_{v|m} T_p(E)_{\Gamma_v})_\psi) = (\prod_{\ell \in S \setminus S_{\mathrm{ram}}(F)} P'_\ell(\sigma_\ell))\Lambda_\psi.$$

Using the above exact sequence and Kato's theorem $\psi(\xi_{F_\infty}) \in \mathrm{char}((\mathrm{Sel}(O_{F_\infty}, E[p^\infty])^\vee)_\psi)$, we have

$$\mathrm{char}((\mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])^\vee)_\psi) \supset \psi(\xi_{F_\infty})(\prod_{\ell \in S \setminus S_{\mathrm{ram}}(F)} P'_\ell(\sigma_\ell))\Lambda_\psi.$$

Since $\xi_{F_\infty}(\prod_{\ell \in S \setminus S_{\mathrm{ram}}(F)} P'_\ell(\sigma_\ell)) = \xi_{F_\infty,S}$ modulo unit and $c_{K_\infty/F_\infty}(\xi_{K_\infty,S}) = \xi_{F_\infty,S}$ by (2.7), we obtain

$$\psi(\xi_{K_\infty,S}) \in \mathrm{Fitt}_{0,(\Lambda_{K_\infty})_\psi}((\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee)_\psi) \tag{2.11}$$

for any character ψ of $\mathrm{Gal}(K/\mathbf{Q})$. Since the μ-invariant of $\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee$ is zero as we explained above, (2.11) implies

$$\xi_{K_\infty,S} \in \mathrm{Fitt}_{0,\Lambda_{K_\infty}}(\mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^\vee)$$

(see Lemma 4.1 in [9], for example).

(2) We use the same notation ψ, F, etc. as above. At first, we assume (2.5). Then the algebraic λ-invariant of $\mathrm{Sel}(E/F_\infty, E[p^\infty])^\vee$ equals the analytic λ-invariant by Hachimori and Matsuno [6], [13], so the main conjecture $\mathrm{char}((\mathrm{Sel}(O_{F_\infty}, E[p^\infty])^\vee)_\psi) = \psi(\xi_{F_\infty})\Lambda_\psi$ also holds. Therefore, we have

$$\begin{aligned}\mathrm{char}((\mathrm{Sel}(O_{F_\infty}[1/m], E[p^\infty])^\vee)_\psi) &= \psi(\xi_{F_\infty})(\prod_{\ell \in S \setminus S_{\mathrm{ram}}(F)} P'_\ell(\sigma_\ell))\Lambda_\psi \\ &= \psi(\xi_{F_\infty,S})\Lambda_\psi = \psi(\xi_{K_\infty,S})\Lambda_\psi\end{aligned}$$

and

$$\mathrm{Fitt}_{0,(\Lambda_{K_\infty})_\psi}((\mathrm{Sel}(O_{K_\infty}[1/m],E[p^\infty])^\vee)_\psi)=\psi(\xi_{K_\infty,S}\Lambda_{K_\infty})\Lambda_\psi.$$

It follows from [9] Corollary 4.2 that

$$\mathrm{Fitt}_{0,\Lambda_{K_\infty}}(\mathrm{Sel}(O_{K_\infty}[1/m],E[p^\infty])^\vee)=\xi_{K_\infty,S}\Lambda_{K_\infty}.$$

On the other hand, if we assume the above equality, taking the $\mathrm{Gal}(K/\mathbf{Q})$-invariant part of $\mathrm{Sel}(O_{K_\infty}[1/m],E[p^\infty])$, we get

$$\mathrm{Fitt}_{0,\Lambda_{\mathbf{Q}_\infty}}(\mathrm{Sel}(O_{\mathbf{Q}_\infty}[1/m],E[p^\infty])^\vee)=\xi_{\mathbf{Q}_\infty,S}\Lambda_{\mathbf{Q}_\infty,S},$$

which implies (2.5).

2.3 An analogue of Stickelberger's theorem

Let $K/\mathbf{Q}$ be a finite abelian p-extension. When the conductor of K is m, we define $\vartheta_K\in R_K=\mathbf{Z}_p[\mathrm{Gal}(K/\mathbf{Q})]$ to be the image of $\vartheta_{\mathbf{Q}(\mu_{mp^\infty})}\in\Lambda_{\mathbf{Q}(\mu_{mp^\infty})}$. Therefore, if m is prime to p, ϑ_K is the image of $\vartheta_{\mathbf{Q}(\mu_m)}=(1-\frac{\sigma_p}{\alpha})(1-\frac{\sigma_p^{-1}}{\alpha})\tilde{\theta}_{\mathbf{Q}(\mu_m)}$ by (2.4). If $m=m'p^n$ for some m' which is prime to p and for some $n\geq 2$, ϑ_K is the image of $\vartheta_{\mathbf{Q}(\mu_{m'p^n})}=\alpha^{-n}(\tilde{\theta}_{\mathbf{Q}(\mu_{m'p^n})}-\alpha^{-1}\nu_{m'p^n,m'p^{n-1}}(\tilde{\theta}_{\mathbf{Q}(\mu_{m'p^{n-1}})}))$.

For any positive integer n, we denote by $\mathbf{Q}(n)$ the maximal p-subextension of $\mathbf{Q}$ in $\mathbf{Q}(\mu_n)$.

Theorem 2.3.1 *For any finite abelian p-extension K in which all bad primes of E are unramified, ϑ_K annihilates $\mathrm{Sel}(O_K,E[p^\infty])^\vee$, namely we have*

$$\vartheta_K\,\mathrm{Sel}(O_K,E[p^\infty])^\vee=0.$$

Proof. We may assume $K=\mathbf{Q}(mp^n)$ for some squarefree product m of primes in $\mathcal{P}_{good}$ and for some $n\in\mathbf{Z}_{\geq 0}$. By Theorem 2.2.2 (1), taking S to be the set of all prime divisors of m, we have $\xi_{K_\infty}\in\mathrm{Fitt}_{0,\Lambda_{K_\infty}}(\mathrm{Sel}(O_{K_\infty}[1/m],E[p^\infty])^\vee)$, which implies $\xi_{K_\infty}\,\mathrm{Sel}(O_{K_\infty},E[p^\infty])^\vee=0$. Let $\xi_K\in R_K=\mathbf{Z}_p[\mathrm{Gal}(K/\mathbf{Q})]$ be the image of ξ_{K_∞}. Since the natural map $\mathrm{Sel}(O_K,E[p^\infty])\longrightarrow\mathrm{Sel}(O_{K_\infty},E[p^\infty])$ is injective, we have $\xi_K\,\mathrm{Sel}(O_K,E[p^\infty])^\vee=0$.

By the definitions of $\xi_{\mathbf{Q}(\mu_{mp^\infty})}$, $\xi_{\mathbf{Q}(mp^n)}$, $\vartheta_{\mathbf{Q}(mp^n)}$, we can write

$$\xi_K=\xi_{\mathbf{Q}(mp^n)}=\vartheta_{\mathbf{Q}(mp^n)}+\sum_{d|m,d\neq m}\lambda_d\nu_{m,d}(\vartheta_{\mathbf{Q}(dp^n)})\tag{2.12}$$

for some $\lambda_d\in R_{\mathbf{Q}(mp^n)}$ where $\nu_{m,d}:R_{\mathbf{Q}(dp^n)}\longrightarrow R_{\mathbf{Q}(mp^n)}$ is the norm map defined similarly as in §2.1. We will prove this theorem by induction on

m. Since $d < m$, we have $\vartheta_{\mathbf{Q}(dp^n)} \in \mathrm{Ann}_{R_{\mathbf{Q}(dp^n)}}(\mathrm{Sel}(O_{\mathbf{Q}(dp^n)}, E[p^\infty])^\vee)$ by the hypothesis of the induction. This implies that $\nu_{m,d}(\vartheta_{\mathbf{Q}(dp^n)})$ annihilates $\mathrm{Sel}(O_{\mathbf{Q}(mp^n)}, E[p^\infty])^\vee$. Since ξ_K is in $\mathrm{Ann}_{R_K}(\mathrm{Sel}(O_K, E[p^\infty])^\vee)$, the above equation implies that ϑ_K is in $\mathrm{Ann}_{R_K}(\mathrm{Sel}(O_K, E[p^\infty])^\vee)$.

Remark 2.3.2 Let K, S, m be as in Theorem 2.2.2. Under our assumptions, the control theorem works completely;

$$\mathrm{Sel}(O_K[1/m], E[p^\infty]) \xrightarrow{\simeq} \mathrm{Sel}(O_{K_\infty}[1/m], E[p^\infty])^{\mathrm{Gal}(K_\infty/K)}.$$

Therefore, Theorem 2.2.2 (1) implies that $\mathrm{Fitt}_{0,R_K}(\mathrm{Sel}(O_K[1/m], E[p^\infty])^\vee)$ is principal and

$$\xi_{K,S} \in \mathrm{Fitt}_{0,R_K}(\mathrm{Sel}(O_K[1/m], E[p^\infty])^\vee) \tag{2.13}$$

where $\xi_{K,S}$ is the image of $\xi_{K_\infty,S}$ in R_K.

Theorem 2.2.2 (2) implies that if we assume the main conjecture (2.5), we have

$$\mathrm{Fitt}_{0,R_K}(\mathrm{Sel}(O_K[1/m], E[p^\infty])^\vee) = \xi_{K,S} R_K\ . \tag{2.14}$$

2.4 Higher Fitting ideals

For a commutative ring R and a finitely presented R-module M with n generators, let A be an $n \times m$ relation matrix of M. For an integer $i \geq 0$, $\mathrm{Fitt}_{i,R}(M)$ is defined to be the ideal of R generated by all $(n-i) \times (n-i)$ minors of A (cf. [19]; this ideal $\mathrm{Fitt}_{i,R}(M)$ does not depend on the choice of a relation matrix A).

Suppose that $K/\mathbf{Q}$ is a finite extension such that K is in the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty$ of $\mathbf{Q}$, and that m is a squarefree product of primes in $\mathcal{P}^{(N)}$. We define $K(m)$ by $K(m) = \mathbf{Q}(m)K$.

We put $\mathcal{G}_\ell = \mathrm{Gal}(\mathbf{Q}(\ell)/\mathbf{Q})$ and $\mathcal{G}_m = \mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q}) = \Pi_{\ell | m} \mathcal{G}_\ell$. We have $\mathrm{Gal}(K(m)/K) = \mathcal{G}_m$. We put $n_\ell = \mathrm{ord}_p(\ell - 1)$. Suppose that $m = \ell_1 \cdot \ldots \cdot \ell_r$. We take a generator τ_{ℓ_i} of $\mathcal{G}_{\ell_i}$ and put $S_i = \tau_{\ell_i} - 1 \in R_{K(m)}$. We write n_i for n_{ℓ_i}. We identify $R_{K(m)}$ with

$$R_K[\mathcal{G}_m] = R_K[S_1, ..., S_r]/((1+S_1)^{p^{n_1}} - 1, ..., (1+S_r)^{p^{n_r}} - 1).$$

We consider $\vartheta_{K(m)} \in R_{K(m)}$ and write

$$\vartheta_{K(m)} = \sum_{i_1, \ldots, i_r \geq 0} a^{(m)}_{i_1, \ldots, i_r} S_1^{i_i} \cdot \ldots \cdot S_r^{i_r}$$

where $a^{(m)}_{i_1, \ldots, i_r} \in R_K$. Put $n_0 = \min\{n_1, ..., n_r\}$. For $s \in \mathbf{Z}_{>0}$, we define c_s to be the maximal positive integer c such that

$$T^{-1}((1+T)^{p^{n_0}} - 1) \in p^c \mathbf{Z}_p[T] + T^{s+1} \mathbf{Z}_p[T].$$

For example, $c_1 = n_0$, ..., $c_{p-2} = n_0$, $c_{p-1} = n_0 - 1$, ..., $c_{p^2-1} = n_0 - 2$. If $i_1,...,i_r \leq s$, $a^{(m)}_{i_1,...,i_r}$ mod p^{c_s} is well-defined (it does not depend on the choice of $a^{(m)}_{i_1,...,i_r}$).

Theorem 2.4.1 *Let K be an intermediate field of the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty/\mathbf{Q}$ with $[K:\mathbf{Q}] < \infty$. Let c_s be the integer defined above for $s \in \mathbf{Z}_{>0}$ and m. Assume that $i_1,...,i_r \leq s$ and $i_1 + ... + i_r \leq i$. Then we have*

$$a^{(m)}_{i_1,...,i_r} \in \mathrm{Fitt}_{i,R_K/p^{c_s}}(\mathrm{Sel}(E/K, E[p^{c_s}])^\vee).$$

For $m = \ell_1 \cdot ... \cdot \ell_r$, we denote $(-1)^r$ times the coefficient of $S_1 \cdot ... \cdot S_r$ in $\vartheta_{K(m)}$ by δ_m. If ℓ_i splits completely in K for all $i = 1,...,r$, we can write

$$\vartheta_{K(m)} \equiv \delta_m \prod_{i=1}^{r}(1-\tau_{\ell_i}) = (-1)^r \delta_m S_1 \cdot ... \cdot S_r \pmod{p^N, S_1^2, ..., S_r^2} \quad (2.15)$$

(see [12] §6.3). Taking $s = 1$ and $i = r$ in Theorem 2.4.1, we get

Corollary 2.4.2 *Let $K/\mathbf{Q}$ be a finite extension such that $K \subset \mathbf{Q}_\infty$. We have*

$$\delta_m \in \mathrm{Fitt}_{r,R_K/p^N}(\mathrm{Sel}(E/K, E[p^N])^\vee)$$

where $m = \ell_1 \cdot ... \cdot \ell_r$.

Proof of Theorem 2.4.1. We may assume $K = \mathbf{Q}(p^n)$ for some $n \geq 0$, so $K(m) = \mathbf{Q}(mp^n)$. First of all, we consider the image $\xi_{K(m)} \in R_{K(m)}$ of $\xi_{K(m)_\infty}$. Since $\mathrm{Sel}(E/K(m), E[p^\infty]) \longrightarrow \mathrm{Sel}(E/K(m)_\infty, E[p^\infty])$ is injective, $\xi_{K(m)}$ is in $\mathrm{Fitt}_{0,R_{K(m)}}(\mathrm{Sel}(E/K(m), E[p^\infty])^\vee)$ by Theorem 2.2.2 (1). We write

$$\xi_{K(m)} = \sum_{i_1,...,i_r \geq 0} \alpha^{(m)}_{i_1,...,i_r} S_1^{i_i} \cdot ... \cdot S_r^{i_r}$$

where $\alpha^{(m)}_{i_1,...,i_r} \in R_K$. Assume that $i_1,...,i_r \leq s$ and $i_1 + ... + i_r \leq i$. Then by Lemma 3.1.1 in [12] we have

$$\alpha^{(m)}_{i_1,...,i_r} \in \mathrm{Fitt}_{i,R_K/p^{c_s}}(\mathrm{Sel}(E/K, E[p^{c_s}])^\vee).$$

On the other hand, since $K(m) = \mathbf{Q}(mp^n)$ for some $n \geq 0$, we have

$$\xi_{K(m)} = \vartheta_{K(m)} + \sum_{d|m, d\neq m} \lambda_d \nu_{m,d}(\vartheta_{\mathbf{Q}(dp^n)})$$

for some $\lambda_d \in R_{K(m)}$ by (2.12). This implies that the images of $\xi_{K(m)}$ and $\vartheta_{K(m)}$ under the canonical homomorphism

$$R_{K(m)} = R_K[S_1, ..., S_r]/I \longrightarrow R_K[[S_1, ..., S_r]]/J$$

coincide where $I = ((1+S_1)^{p^{n_1}} - 1, ..., (1+S_1)^{p^{n_r}} - 1)$ and $J = (S_1^{-1}(1+S_1)^{p^{n_1}} - 1, ..., S_r^{-1}(1+S_1)^{p^{n_r}} - 1, S_1^{s+1}, ..., S_r^{s+1})$. Therefore, $\alpha^{(m)}_{i_1,...,i_r} \equiv a^{(m)}_{i_1,...,i_r}$ mod p^{c_s} for i_1,...,$i_r \leq s$. It follows that $a^{(m)}_{i_1,...,i_r} \in \mathrm{Fitt}_{i,R_K/p^{c_s}}(\mathrm{Sel}(E/K, E[p^{c_s}])^\vee)$. This completes the proof of Theorem 2.4.1.

3 Review of Kolyvagin systems of Gauss sum type for elliptic curves

In this section, we recall the results in [12] on Euler systems and Kolyvagin systems of Gauss sum type in the case of elliptic curves. From this section we assume all the assumptions (i), (ii), (iii), (iv) in §1.1.

3.1 Some definitions

Recall that in §2 we defined $\mathcal{P}_{good}$ by $\mathcal{P}_{good} = \{\ell \mid \ell$ is a good reduction prime for E $\} \setminus \{p\}$, and $\mathcal{P}^{(N)}$ by

$$\mathcal{P}^{(N)} = \{\ell \in \mathcal{P}_{good} \mid \ell \equiv 1 \pmod{p^N}\}$$

for a positive integer $N > 0$. If ℓ is in $\mathcal{P}_{good}$, the absolute Galois group $G_{\mathbf{F}_\ell}$ acts on the group $E[p^N]$ of p^N-torsion points, so we consider $H^i(\mathbf{F}_\ell, E[p^N])$. We define

$$\begin{aligned}
\mathcal{P}_0^{(N)} &= \{\ell \in \mathcal{P}^{(N)} \mid H^0(\mathbf{F}_\ell, E[p^N]) \text{ contains an element of order } p^N\}, \\
(\mathcal{P}'_0)^{(N)} &= \{\ell \in \mathcal{P}^{(N)} \mid H^0(\mathbf{F}_\ell, E[p^N]) = E[p^N]\}, \text{ and} \\
\mathcal{P}_1^{(N)} &= \{\ell \in \mathcal{P}^{(N)} \mid H^0(\mathbf{F}_\ell, E[p^N]) \simeq \mathbf{Z}/p^N\}.
\end{aligned}$$

So $\mathcal{P}_0^{(N)} \supset (\mathcal{P}'_0)^{(N)}$, $\mathcal{P}_0^{(N)} \supset \mathcal{P}_1^{(N)}$, and $(\mathcal{P}'_0)^{(N)} \cap \mathcal{P}_1^{(N)} = \emptyset$. Suppose that ℓ is in $\mathcal{P}_1^{(N)}$. Then, since $\ell \equiv 1 \pmod{p^N}$, we have an exact sequence $0 \longrightarrow \mathbf{Z}/p^N \longrightarrow E[p^N] \longrightarrow \mathbf{Z}/p^N \longrightarrow 0$ of $G_{\mathbf{F}_\ell}$-modules where $G_{\mathbf{F}_\ell}$ acts on $\mathbf{Z}/p^N$ trivially. So the action of the Frobenius Frob_ℓ at ℓ on $E[p^N]$ can be written as $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ for a suitable basis of $E[p^N]$. Therefore, $H^1(\mathbf{F}_\ell, E[p^N])$ is also isomorphic to $\mathbf{Z}/p^N$ for $\ell \in \mathcal{P}_1^{(N)}$.

Let $t \in E[p^N]$ be an element of order p^N. We define

$$\begin{aligned}
\mathcal{P}_{0,t}^{(N)} &= \{\ell \in \mathcal{P}^{(N)} \mid t \in H^0(\mathbf{F}_\ell, E[p^N])\}, \\
\mathcal{P}_{1,t}^{(N)} &= \{\ell \in \mathcal{P}^{(N)} \mid H^0(\mathbf{F}_\ell, E[p^N]) = (\mathbf{Z}/p^N)t\}.
\end{aligned}$$

So, $\mathcal{P}_0^{(N)} = \bigcup_t \mathcal{P}_{0,t}^{(N)}$ and $\mathcal{P}_1^{(N)} = \bigcup_t \mathcal{P}_{1,t}^{(N)}$ where t runs over all elements of order p^N. Since we assumed that the Galois action on the Tate module is surjective, both $(\mathcal{P}'_0)^{(N)}$ and $\mathcal{P}_{1,t}^{(N)}$ are infinite by Chebotarev density theorem ([12] §4.3).

We define $\mathcal{K}_{(p)}$ to be the set of number fields K such that $K/\mathbf{Q}$ is a finite abelian p-extension in which all bad primes of E are unramified. Suppose that K is in $\mathcal{K}_{(p)}$. We define

$$\begin{aligned} (\mathcal{P}'_0)^{(N)}(K) &= \{\ell \in (\mathcal{P}'_0)^{(N)} \mid \ell \text{ splits completely in } K\}, \\ \mathcal{P}_1^{(N)}(K) &= \{\ell \in \mathcal{P}_1^{(N)} \mid \ell \text{ splits completely in } K\}. \end{aligned}$$

Again by Chebotarev density theorem, both $(\mathcal{P}'_0)^{(N)}(K)$ and $\mathcal{P}_1^{(N)}(K)$ are infinite (see [12] §4.3).

Suppose $\ell \in \mathcal{P}_{good}$. For a prime v above ℓ, we know $H^1(K_v, E[p^N])/(E(K_v) \otimes \mathbf{Z}/p^N) = H^0(\kappa(v), E[p^N](-1))$ where $\kappa(v)$ is the residue field of v. We put

$$\mathcal{H}^2_\ell(K) = \bigoplus_{v|\ell} H^0(\kappa(v), E[p^N](-1)). \tag{3.1}$$

If ℓ is in $(\mathcal{P}'_0)^{(N)}(K)$ (resp. $\mathcal{P}_1^{(N)}(K)$), $\mathcal{H}^2_\ell(K)$ is a free R_K/p^N-module of rank 2 (resp. rank 1) where $R_K = \mathbf{Z}_p[\mathrm{Gal}(K/\mathbf{Q})]$ as before.

From now on, for a prime $\ell \in \mathcal{P}_0^{(N)}$, we fix a prime $\ell_{\overline{\mathbf{Q}}}$ of an algebraic closure $\overline{\mathbf{Q}}$ above ℓ. For any algebraic number field F, we denote the prime of F below $\ell_{\overline{\mathbf{Q}}}$ by ℓ_F, so when we consider finite extensions F_1/k, F_2/k such that $F_1 \subset F_2$, the primes ℓ_{F_2}, ℓ_{F_1} satisfy $\ell_{F_2}|\ell_{F_1}$.

We take a primitive p^n-th root of unity ζ_{p^n} such that $(\zeta_{p^n})_{n\geq 1} \in \mathbf{Z}_p(1) = \varprojlim \mu_{p^n}$, and fix it.

In the following, for each ℓ in $\mathcal{P}_0^{(N)}(K)$, we take $t_\ell \in H^0(\mathbf{F}_\ell, E[p^N])$ and fix it. We define

$$t_{\ell,K} = (t_\ell \otimes \zeta_{p^N}^{\otimes(-1)}, 0, ..., 0) \in \mathcal{H}^2_\ell(K) \tag{3.2}$$

where the right hand side is the element whose ℓ_K-component is $t_\ell \otimes \zeta_{p^N}^{\otimes(-1)}$ and other components are zero.

Suppose that K is in $\mathcal{K}_{(p)}$. Let K_∞/K be the cyclotomic $\mathbf{Z}_p$-extension, and K_n be the n-th layer. Since $\mathrm{Sel}(O_{K_\infty}, E[p^\infty])^\vee$ is a finitely generated $\mathbf{Z}_p$-module, the corestriction map $\mathrm{Sel}(O_{K_m}, E[p^N]) \longrightarrow \mathrm{Sel}(O_K, E[p^N])$ is the zero map if m is sufficiently large. We take the minimal $m > 0$ satisfying this property, and put $K_{[1]} = K_m$. We define inductively $K_{[n]}$ by $K_{[n]} = (K_{[n-1]})_{[1]}$ where we applied the above definition to $K_{[n-1]}$ instead of K.

We can compute how large $K_{[n]}$ is. Let λ be the λ-invariant of $\mathrm{Sel}(O_{K_\infty}, E[p^\infty])^\vee$. We take $a \in \mathbf{Z}_{\geq 0}$ such that $p^{a+1} - p^a \geq \lambda$. Suppose that $K = K'_m$ (m-th layer of K'_∞/K') for some K' such that p is unramified in K'. The corestriction map $\mathrm{Sel}(O_{K'_{a+1}}, E[p]) \longrightarrow \mathrm{Sel}(O_{K'_a}, E[p])$ is the zero map. Therefore, $\mathrm{Sel}(O_{K'_{a+N}}, E[p^N]) \longrightarrow \mathrm{Sel}(O_{K'_a}, E[p^N])$ is the zero map. Put $a' = \max(a-m, 0)$. Then $\mathrm{Sel}(O_{K_{a'+N}}, E[p^N]) \longrightarrow \mathrm{Sel}(O_{K_{a'}}, E[p^N])$ is the zero map. Therefore, we have $K_{[1]} \subset K_{a'+N}$. Also we know $K_{[n]} \subset K_{a'+nN}$.

Let n_λ, d_n be the numbers defined just before (1.4) in §1.2. Then we can show that if $\ell \in \mathcal{P}_1^{(N)}$ satisfies $\ell \equiv 1 \pmod{p^{d_n}}$, ℓ is in $\mathcal{P}_1^{(N)}(\mathbf{Q}_{[n]})$ by the same method as above.

3.2 Euler systems of Gauss sum type for elliptic curves

We use the following lemma which is the global duality theorem (see Theorem 2.3.4 in Mazur and Rubin [14]).

Lemma 3.2.1 *Suppose that m is a product of primes in $\mathcal{P}_{good}$. We have an exact sequence*

$$0 \longrightarrow \mathrm{Sel}(O_K, E[p^N]) \longrightarrow \mathrm{Sel}(O_K[1/m], E[p^N]) \longrightarrow \bigoplus_{\ell | m} \mathcal{H}^2_\ell(K) \longrightarrow \mathrm{Sel}(O_K, E[p^N])^\vee.$$

We remark that we can take m such that the last map is surjective in our case (see Lemma 3.4.1 below).

Let K be a number field in $\mathcal{K}_{(p)}$ and $\ell \in \mathcal{P}_0^{(N)}(K_{[1]})$. We apply the above lemma to $K_{[1]}$ and obtain an exact sequence

$$\mathrm{Sel}(O_{K_{[1]}}[1/\ell], E[p^N]) \xrightarrow{\partial_\ell} \mathcal{H}^2_\ell(K_{[1]}) \xrightarrow{w_\ell} \mathrm{Sel}(O_{K_{[1]}}, E[p^N])^\vee.$$

Consider $\vartheta_{K_{[1]}} t_{\ell, K_{[1]}} \in \mathcal{H}^2_\ell(K_{[1]})$. By Theorem 2.3.1 we know $w_\ell(\vartheta_{K_{[1]}} t_{\ell, K_{[1]}}) = \vartheta_{K_{[1]}} w_\ell(t_{\ell, K_{[1]}}) = 0$. Therefore, there is an element $g \in \mathrm{Sel}(O_{K_{[1]}}[1/\ell], E[p^N])$ such that $\partial_\ell(g) = \vartheta_{K_{[1]}} t_{\ell, K_{[1]}}$. We define

$$g^{(K)}_{\ell, t_\ell} = \mathrm{Cor}_{K_{[1]}/K}(g) \in \mathrm{Sel}(O_K[1/\ell], E[p^N]). \tag{3.3}$$

This element $g^{(K)}_{\ell, t_\ell}$ does not depend on the choice of $g \in \mathrm{Sel}(O_{K_{[1]}}[1/\ell], E[p^N])$ ([12] §5.4). We write g_ℓ instead of $g^{(K)}_{\ell, t_\ell}$ when no confusion arises.

Remark 3.2.2 To define g_ℓ, we used in [12] the p-adic L-function θ_{K_∞} whose Euler factor at ℓ is $1 - \frac{a_\ell}{\ell}\sigma_\ell^{-1} + \frac{1}{\ell}\sigma_\ell^{-2}$. The element θ_{K_∞} can be constructed from ϑ_{K_∞} by the same method as when we constructed ξ_{K_∞} in §2.1. In the above definition (3.3), we used ϑ_K (namely ϑ_{K_∞}) instead of θ_{K_∞}.

3.3 Kolyvagin derivatives of Gauss sum type

Let ℓ be a prime in $\mathcal{P}_{good}$. We define ∂_ℓ as a natural homomorphism

$$\partial_\ell : H^1(K, E[p^N]) \longrightarrow \mathcal{H}^2_\ell(K) = \bigoplus_{v|\ell} H^0(\kappa(v), E[p^N](-1))$$

where we used $H^1(K_v, E[p^N])/(E(K_v) \otimes \mathbf{Z}/p^N) = H^0(\kappa(v), E[p^N](-1))$.

Next, we assume $\ell \in \mathcal{P}_1^{(N)}(K)$. We denote by $\mathbf{Q}_\ell(\ell)$ the maximal p-subextension of $\mathbf{Q}_\ell$ inside $\mathbf{Q}_\ell(\mu_\ell)$. Put $\mathcal{G}_\ell = \mathrm{Gal}(\mathbf{Q}_\ell(\ell)/\mathbf{Q}_\ell)$. By Kummer theory, $\mathcal{G}_\ell$ is isomorphic to $\mu_{p^{n_\ell}}$ where $n_\ell = \mathrm{ord}_p(\ell-1)$. We denote by τ_ℓ the corresponding element of $\mathcal{G}_\ell$ to $\zeta_{p^{n_\ell}}$ that is the primitive p^{n_ℓ}-th root of unity we fixed.

We consider the natural homomorphism $H^1(\mathbf{Q}_\ell, E[p^N]) \longrightarrow H^1(\mathbf{Q}_\ell(\ell), E[p^N])$ and denote the kernel by $H^1_{tr}(\mathbf{Q}_\ell, E[p^N])$. Let $\mathbf{Q}_{\ell,nr}$ be the maximal unramified extension of $\mathbf{Q}_\ell$. We identify $H^1(\mathbf{F}_\ell, E[p^N])$ with $H^1(\mathrm{Gal}(\mathbf{Q}_{\ell,nr}/\mathbf{Q}_\ell), E[p^N])$, and regard it as a subgroup of $H^1(\mathbf{Q}_\ell, E[p^N])$. Then both $H^1(\mathbf{F}_\ell, E[p^N])$ and $H^1_{tr}(\mathbf{Q}_\ell, E[p^N])$ are isomorphic to $\mathbf{Z}/p^N$, and we have decomposition

$$H^1(\mathbf{Q}_\ell, E[p^N]) = H^1(\mathbf{F}_\ell, E[p^N]) \oplus H^1_{tr}(\mathbf{Q}_\ell, E[p^N])$$

as an abelian group. We also note that $H^1(\mathbf{F}_\ell, E[p^N])$ coincides with the image of the Kummer map and is isomorphic to $E(\mathbf{Q}_\ell) \otimes \mathbf{Z}/p^N$. We consider the homomorphism

$$\phi' : H^1(\mathbf{Q}_\ell, E[p^N]) \longrightarrow H^1(\mathbf{F}_\ell, E[p^N]) \tag{3.4}$$

which is obtained from the above decomposition.

Note that $H^1(\mathbf{F}_\ell, E[p^N]) = E[p^N]/(\mathrm{Frob}_\ell - 1)$ where Frob_ℓ is the Frobenius at ℓ. Since ℓ is in $\mathcal{P}_1^{(N)}$, $\mathrm{Frob}_\ell^{-1} - 1 : E[p^N]/(\mathrm{Frob}_\ell - 1) \longrightarrow E[p^N]^{\mathrm{Frob}_\ell = 1} = H^0(\mathbf{F}_\ell, E[p^N])$ is an isomorphism. We define $\phi'' : H^1(\mathbf{Q}_\ell, E[p^N]) \longrightarrow H^0(\mathbf{F}_\ell, E[p^N])$ as the composition of ϕ' and $H^1(\mathbf{F}_\ell, E[p^N]) \stackrel{\mathrm{Frob}_\ell^{-1}-1}{\longrightarrow} H^0(\mathbf{F}_\ell, E[p^N])$. We define

$$\phi_\ell : H^1(K, E[p^N]) \longrightarrow \mathcal{H}^2_\ell(K)(1)$$

as the composition of the natural homomorphism $H^1(K, E[p^N]) \longrightarrow \bigoplus_{v|\ell} H^1(K_v, E[p^N])$ and ϕ'' for K_v. Using the primitive p^N-th root of unity ζ_{p^N} we fixed, we regard ϕ_ℓ as a homomorphism

$$\phi_\ell : H^1(K, E[p^N]) \longrightarrow \mathcal{H}^2_\ell(K).$$

For a prime $\ell \in \mathcal{P}_1^{(N)}(K)$, we put $\mathcal{G}_\ell = \mathrm{Gal}(\mathbf{Q}(\ell)/\mathbf{Q})$. We identify $\mathcal{G}_\ell$ with $\mathrm{Gal}(\mathbf{Q}_\ell(\ell)/\mathbf{Q}_\ell)$. Recall that we defined n_ℓ by $p^{n_\ell} = [\mathbf{Q}(\ell) : \mathbf{Q}]$, and we took a generator τ_ℓ of $\mathcal{G}_\ell$ above. We define

$$N_\ell = \sum_{i=0}^{p^{n_\ell}-1} \tau_\ell^i \in \mathbf{Z}[\mathcal{G}_\ell],\ D_\ell = \sum_{i=0}^{p^{n_\ell}-1} i\tau_\ell^i \in \mathbf{Z}[\mathcal{G}_\ell]$$

as usual.

We define $\mathcal{N}_1^{(N)}(K)$ to be the set of squarefree products of primes in $\mathcal{P}_1^{(N)}(K)$. We suppose $1 \in \mathcal{N}_1^{(N)}(K)$. For $m \in \mathcal{N}_1^{(N)}(K)$, we put $\mathcal{G}_m = \mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$, $N_m = \Pi_{\ell|m} N_\ell \in \mathbf{Z}[\mathcal{G}_m]$, and $D_m = \Pi_{\ell|m} D_\ell \in \mathbf{Z}[\mathcal{G}_m]$. Assume that ℓ is in $(\mathcal{P}'_0)^{(N)}(K(m)_{[1]})$ and consider $g_{\ell,t_\ell}^{K(m)} \in \mathrm{Sel}(O_{K(m)}[1/\ell], E[p^N])$. We can check that $D_m g_{\ell,t_\ell}^{K(m)}$ is in $\mathrm{Sel}(O_{K(m)}[1/m\ell], E[p^N])^{\mathcal{G}_m}$. Using the fact that $\mathrm{Sel}(O_K[1/m\ell], E[p^N]) \xrightarrow{\simeq} \mathrm{Sel}(O_{K(m)}[1/m\ell], E[p^N])^{\mathcal{G}_m}$ is bijective by Lemma 3.3.1 below (cf. also [12] Lemma 6.3.1), we define

$$\kappa_{m,\ell} = \kappa_{m,\ell,t_\ell}^{(K)} \in \mathrm{Sel}(O_K[1/m\ell], E[p^N]) \tag{3.5}$$

to be the unique element whose image in $\mathrm{Sel}(O_{K(m)}[1/m\ell], E[p^N])$ is $D_m g_{\ell,t_\ell}^{(K(m))}$.

The following lemma will be also used in the next section.

Lemma 3.3.1 *Suppose that K, $L \in \mathcal{K}_{(p)}$ and $K \subset L$. For any $m \in \mathbf{Z}_{>0}$, the restriction map* $\mathrm{Sel}(O_K[1/m], E[p^N]) \xrightarrow{\simeq} \mathrm{Sel}(O_L[1/m], E[p^N])^{\mathrm{Gal}(L/K)}$ *is bijective.*

Proof. Let N_E be the conductor of E, $m' = mpN_E$, and m'' the product of primes which divide pN_E and which do not divide m. Put $G = \mathrm{Gal}(L/K)$. We have a commutative diagram of exact sequences

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}(O_K[1/m], E[p^N]) & \longrightarrow & \mathrm{Sel}(O_K[1/m'], E[p^N]) & \longrightarrow & \bigoplus_{v|m''} H^2_{K,v} \\
 & & \downarrow \alpha_1 & & \downarrow \alpha_2 & & \downarrow \alpha_3 \\
0 & \longrightarrow & \mathrm{Sel}(O_L[1/m], E[p^N])^G & \longrightarrow & \mathrm{Sel}(O_L[1/m'], E[p^N])^G & \longrightarrow & (\bigoplus_{w|m''} H^2_{L,w})^G
\end{array}$$

where $H^2_{K,v} = H^1(K_v, E[p^N])/(E(K_v) \otimes \mathbf{Z}/p^N)$ and $H^2_{L,w} = H^1(L_w, E[p^N])/(E(L_w) \otimes \mathbf{Z}/p^N)$. Since $\mathrm{Sel}(O_L[1/m'], E[p^N]) = H^1_{et}(\mathrm{Spec}\, O_L[1/m'], E[p^N])$ and $H^0(L, E[p^N]) = 0$, α_2 is bijective. Suppose that v divides m'' and w is above v. When v divides N_E, since v is unramified in L and p is prime to $\mathrm{Tam}(E)$, $H^2_{K,v} \longrightarrow H^2_{L,w}$ is injective (Greenberg [3] §3). When v is above p, $H^2_{K,v} \longrightarrow H^2_{L,w}$ is injective because $a_p \not\equiv 1 \pmod p$ (Greenberg [3] §3). Hence α_3 is injective. Therefore, α_1 is bijective.

In [11], if m has a factorization $m = \ell_1 \cdot ... \cdot \ell_r$ such that $\ell_{i+1} \in \mathcal{P}_1^{(N)}(K(\ell_1 \cdot ... \cdot \ell_i))$ for all $i = 1,...,r-1$, we called m *well-ordered*. But the word "well-ordered" might cause confusion, so we call m *admissible* in this paper if m

satisfies the above condition. Note that we do not impose the condition $\ell_1 < ... < \ell_r$ in the above definition, and that m is admissible if there is one factorization as above. We sometimes call the set of prime divisors of m *admissible* if m is admissible.

Suppose that $m = \ell_1 \cdot ... \cdot \ell_r$. We define $\delta_m \in R_K/p^N$ by

$$\vartheta_{K(m)} \equiv \delta_m \prod_{i=1}^{r}(1-\tau_{\ell_i}) \pmod{p^N, (\tau_{\ell_1}-1)^2, ..., (\tau_{\ell_r}-1)^2} \tag{3.6}$$

(see [12] §6.3).

We simply write $\kappa_{m,\ell}$ for $\kappa_{m,\ell,t_\ell}^{(K)}$. We have the following Proposition ([12] Propositions 6.3.2, 6.4.5 and Lemma 6.3.4).

Proposition 3.3.2 *Suppose that m is in $\mathcal{N}_1^{(N)}(K)$, and $\ell \in (\mathcal{P}_0')^{(N)}(K(m)_{[1]})$. We take n_0 sufficiently large such that every prime of K_{n_0} dividing m is inert in K_∞/K_{n_0}. We further assume that $\ell \in (\mathcal{P}_0')^{(N)}(K_{n_0+N})$. Then*
(0) $\kappa_{m,\ell} \in \mathrm{Sel}(O_K[1/m\ell], E[p^N])$.
(1) $\partial_r(\kappa_{m,\ell}) = \phi_r(\kappa_{\frac{m}{r},\ell})$ *for any prime divisor r of m.*
(2) $\partial_\ell(\kappa_{m,\ell}) = \delta_m t_{\ell,K}$.
(3) *Assume further that m is admissible. Then $\phi_r(\kappa_{m,\ell}) = 0$ for any prime divisor r of m.*

3.4 Construction of Kolyvagin systems of Gauss sum type

In the previous subsection we constructed $\kappa_{m,\ell}$ for $m \in \mathcal{N}_1^{(N)}(K)$ and a prime $\ell \in (\mathcal{P}_0')^{(N)}(K)$ satisfying some properties. In this subsection we construct $\kappa_{m,\ell}$ for $\ell \in \mathcal{P}_1^{(N)}(K)$ satisfying some properties (see Proposition 3.4.2). The property (4) in Proposition 3.4.2 is a beautiful property of our Kolyvagin systems of Gauss sum type, which is unique for Kolyvagin systems of Gauss sum type.

For a squarefree product m of primes, we define $\epsilon(m)$ to be the number of prime divisors of m, namely $\epsilon(m) = r$ if $m = \ell_1 \cdot ... \cdot \ell_r$.

For any prime number ℓ, we write $\mathcal{H}_\ell^2(K) = \bigoplus_{v|\ell} H^1(K_v, E[p^N])/(E(K_v)\otimes \mathbf{Z}/p^N)$, and consider the natural map

$$w_K : \bigoplus_{\ell} \mathcal{H}_\ell^2(K) \longrightarrow \mathrm{Sel}(O_K, E[p^N])^\vee$$

which is obtained by taking the dual of $\mathrm{Sel}(O_K, E[p^N]) \longrightarrow \bigoplus_v E(K_v) \otimes \mathbf{Z}/p^N$. We also consider the natural map

$$\partial_K : H^1(K, E[p^N]) \longrightarrow \bigoplus_{\ell} \mathcal{H}_\ell^2(K).$$

We use the following lemma which was proved in [12] Proposition 4.4.3 and Lemma 6.2.1 (2).

Lemma 3.4.1 *Suppose that $K \in \mathcal{K}_{(p)}$ and $r_1,\ldots,r_s$ are s distinct primes in $\mathcal{P}_1^{(N)}(K)$. Assume that for each $i = 1,\ldots,s$, $\sigma_i \in \mathcal{H}^2_{r_i}(K)$ is given, and also $x \in \mathrm{Sel}(O_K, E[p^N])^\vee$ is given. Let K'/K be an extension such that $K' \in \mathcal{K}_{(p)}$. Then there are infinitely many $\ell \in \mathcal{P}_0^{(N)}(K)$ such that $w_K(t_{\ell,K}) = x$. We take such a prime ℓ and fix it. Then there are infinitely many $\ell' \in (\mathcal{P}'_0)^{(N)}(K')$ which satisfy the following properties:*
(i) *$w_K(t_{\ell',K}) = w_K(t_{\ell,K}) = x$.*
(ii) *There is an element $z \in \mathrm{Sel}(O_K[1/\ell\ell'], E[p^N])$ such that $\partial_K(z) = t_{\ell',K} - t_{\ell,K}$ and $\phi_{r_i}(z) = \sigma_i$ for each $i = 1,\ldots,s$.*

Assume that $m\ell$ is in $\mathcal{N}_1^{(N)}(K_{[\epsilon(m\ell)]})$. By Lemma 3.4.1 we can take $\ell' \in (\mathcal{P}'_0)^{(N)}$ satisfying the following properties:
(i) $\ell' \in (\mathcal{P}'_0)^{(N)}(K_{[\epsilon(m\ell)]}(m)_{[1]}K_{n_0+N})$ where n_0 is as in Proposition 3.3.2.
(ii) $w_{K_{[\epsilon(m\ell)]}}(t_{\ell',K_{[\epsilon(m\ell)]}}) = w_{K_{[\epsilon(m\ell)]}}(t_{\ell,K_{[\epsilon(m\ell)]}})$.
(iii) Let $\phi_r^{(K_{[\epsilon(m\ell)]})} : H^1(K_{[\epsilon(m\ell)]}, E[p^N]) \longrightarrow \mathcal{H}^2_r(K_{[\epsilon(m\ell)]})$ be the map ϕ_r for $K_{[\epsilon(m\ell)]}$. There is an element b' in $\mathrm{Sel}(O_{K_{[\epsilon(m\ell)]}}[1/\ell\ell'], E[p^N])$ such that

$$\partial_{K_{[\epsilon(m\ell)]}}(b') = t_{\ell',K_{[\epsilon(m\ell)]}} - t_{\ell,K_{[\epsilon(m\ell)]}}$$

and $\phi_r^{K_{[\epsilon(m\ell)]}}(b') = 0$ for all r dividing m.

We have already defined $\kappa_{m,\ell'}$ in the previous subsection. We put $b = \mathrm{Cor}_{K_{[\epsilon(m\ell)]}/K}(b')$ and define

$$\kappa_{m,\ell} = \kappa_{m,\ell'} - \delta_m b. \tag{3.7}$$

Then this element does not depend on the choice of ℓ' and b' (see [12] §6.4). In [12], we took b' which does not necessarily satisfy $\phi_r^{K_{[\epsilon(m\ell)]}}(b') = 0$ in the definition of $\kappa_{m,\ell}$. But we adopted the above definition here because it is simpler and there is no loss of generality.

The next proposition was proved in [12] Propositions 6.4.3, 6.4.5, 6.4.6.

Proposition 3.4.2 *Suppose that $m\ell$ is in $\mathcal{N}_1^{(N)}(K_{[\epsilon(m\ell)]})$. Then*
(0) *$\kappa_{m,\ell} \in \mathrm{Sel}(O_K[1/m\ell], E[p^N])$.*
(1) *$\partial_r(\kappa_{m,\ell}) = \phi_r(\kappa_{\frac{m}{r},\ell})$ for any prime divisor r of m.*
(2) *$\partial_\ell(\kappa_{m,\ell}) = \delta_m t_{\ell,K}$.*
(3) *Assume further that m is admissible. Then $\phi_r(\kappa_{m,\ell}) = 0$ for any prime divisor r of m.*
(4) *Assume further that $m\ell$ is admissible, and $m\ell$ is in $\mathcal{N}_1^{(N)}(K_{[\epsilon(m\ell)+1]})$. Then we have*

$$\phi_\ell(\kappa_{m,\ell}) = -\delta_{m\ell} t_{\ell,K}.$$

4 Relations of Selmer groups

In this section, we prove a generalized version of Theorem 1.2.3.

4.1 Injectivity theorem

Suppose that K is in $\mathcal{K}_{(p)}$ and that m is in $\mathcal{N}_1^{(N)}(K)$. For a prime divisor r of m, we denote by

$$w_r : \mathcal{H}^2_r(K) \longrightarrow \mathrm{Sel}(O_K, E[p^N])^\vee$$

the homomorphism which is the dual of $\mathrm{Sel}(O_K, E[p^N]) \longrightarrow \bigoplus_{v|r} E(K_v) \otimes \mathbf{Z}/p^N$. Recall that $\mathcal{H}^2_r(K)$ is a free R_K/p^N-module of rank 1, generated by $t_{r,K}$.

Proposition 4.1.1 *We assume that δ_m is a unit of R_K/p^N for some $m \in \mathcal{N}_1^{(N)}(K)$. Then the natural homomorphism $\oplus_{r|m} w_r : \bigoplus_{r|m} \mathcal{H}^2_r(K) \longrightarrow \mathrm{Sel}(O_K, E[p^N])^\vee$ is surjective.*

Remark 4.1.2 We note that δ_m is numerically computable, in principle.

Proof of Proposition 4.1.1. Let x be an arbitrary element in $\mathrm{Sel}(O_K, E[p^N])^\vee$. Let $w_r : \mathcal{H}^2_r(K) \longrightarrow \mathrm{Sel}(O_K, E[p^N])^\vee$ be the natural homomorphism for each $r \mid m$. We will prove that x is in the submodule generated by all $w_r(t_{r,K})$ for $r \mid m$. Using Lemma 3.4.1, we can take a prime $\ell \in (\mathcal{P}'_0)^{(N)}(K(m)_{[1]}K_{n_0+N})$ such that $w_\ell(t_{\ell,K}) = x$ and ℓ is prime to m. We consider the Kolyvagin derivative $\kappa_{m,\ell}$ which was defined in (3.5). Consider the exact sequence

$$\mathrm{Sel}(O_K[1/m\ell], E[p^N]) \xrightarrow{\partial} \bigoplus_{\ell'|m\ell} \mathcal{H}^2_{\ell'}(K) \xrightarrow{w_K} \mathrm{Sel}(O_K, E[p^N])^\vee$$

(see Lemma 3.2.1) where $\partial = (\oplus \partial_{\ell'})_{\ell'|m\ell}$ and $w_K((z_{\ell'})_{\ell'|m\ell}) = \sum_{\ell'|m\ell} w_{\ell'}(z_{\ell'})$. For each $r \mid m$ we define $\lambda_r \in R_K/p^N$ by $\partial_r(\kappa_{m,\ell}) = \lambda_r t_{r,K} \in \mathcal{H}^2_r(K)$. The above exact sequence and Proposition 3.3.2 (2) imply that

$$\delta_m x + \sum_{r|m} \lambda_r w_r(t_{r,K}) = 0$$

in $\mathrm{Sel}(O_K, E[p^N])^\vee$. Since we assumed that δ_m is a unit, x is in the submodule generated by all $w_r(t_{r,K})$'s. This completes the proof of Proposition 4.1.1.

For a prime $\ell \in \mathcal{P}_1^{(N)}(K)$, we define

$$\mathcal{H}^1_{\ell,f}(K) = \bigoplus_{v|\ell} E(\kappa(v)) \otimes \mathbf{Z}/p^N.$$

Since $\kappa(v) = \mathbf{F}_\ell$, $E(\kappa(v)) \otimes \mathbf{Z}/p^N$ is isomorphic to $\mathbf{Z}/p^N$ and $\mathcal{H}^1_{\ell,f}(K)$ is a free R_K/p^N-module of rank 1.

Corollary 4.1.3 *Suppose that $m = \ell_1 \cdot \ldots \cdot \ell_a$ is in $\mathcal{N}_1^{(N)}(K)$. We assume that δ_m is a unit of R_K/p^N. Then the natural homomorphism*

$$s_m : \mathrm{Sel}(O_K, E[p^N]) \longrightarrow \bigoplus_{i=1}^{a} \mathcal{H}^1_{\ell_i,f}(K)$$

is injective.

Proof. This is obtained by taking the dual of the statement in Proposition 4.1.1.

4.2 Relation matrices

Theorem 4.2.1 *Suppose that $m = \ell_1 \cdot \ldots \cdot \ell_a$ is in $\mathcal{N}_1^{(N)}(K_{[a+1]})$. We assume that m is admissible and that δ_m is a unit of R_K/p^N. Then*
(1) $\mathrm{Sel}(O_K[1/m], E[p^N])$ *is a free R_K/p^N-module of rank a.*
(2) $\{\kappa_{\frac{m}{\ell_i},\ell_i}\}_{1\leq i\leq a}$ *is a basis of* $\mathrm{Sel}(O_K[1/m], E[p^N])$*.*
(3) *The matrix*

$$\mathcal{A} = \begin{pmatrix} \delta_{\frac{m}{\ell_1}} & \phi_{\ell_1}(\kappa_{\frac{m}{\ell_1\ell_2},\ell_2}) & \ldots & \phi_{\ell_1}(\kappa_{\frac{m}{\ell_1\ell_a},\ell_a}) \\ \phi_{\ell_2}(\kappa_{\frac{m}{\ell_1\ell_2},\ell_1}) & \delta_{\frac{m}{\ell_2}} & \ldots & \phi_{\ell_2}(\kappa_{\frac{m}{\ell_2\ell_a},\ell_a}) \\ . & & . & \\ . & & . & \\ \phi_{\ell_a}(\kappa_{\frac{m}{\ell_1\ell_a},\ell_1}) & \phi_{\ell_a}(\kappa_{\frac{m}{\ell_2\ell_a},\ell_2}) & \ldots & \delta_{\frac{m}{\ell_a}} \end{pmatrix} \tag{4.1}$$

is a relation matrix of $\mathrm{Sel}(E/K, E[p^N])^\vee$*.*

In particular, if $a = 2$, the above matrix is $\mathcal{A} = \begin{pmatrix} \delta_{\ell_2} & \phi_{\ell_1}(g_{\ell_2}) \\ \phi_{\ell_2}(g_{\ell_1}) & \delta_{\ell_1} \end{pmatrix}$. This is described in Remark 10.6 in [11] in the case of ideal class groups.

Proof of Theorem 4.2.1 (1). By Proposition 4.1.1, $\bigoplus_{i=1}^a \mathcal{H}^2_{\ell_i}(K) \longrightarrow \mathrm{Sel}(O_K, E[p^N])^\vee$ is surjective. Therefore, by Lemma 3.2.1 we have an exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{Sel}(O_K, E[p^N]) &\longrightarrow \mathrm{Sel}(O_K[1/m], E[p^N]) \xrightarrow{\partial} \bigoplus_{i=1}^{a} \mathcal{H}^2_{\ell_i}(K) \\ &\longrightarrow \mathrm{Sel}(O_K, E[p^N])^\vee \longrightarrow 0. \end{aligned} \tag{4.2}$$

It follows that $\# \mathrm{Sel}(O_K[1/m], E[p^N]) = \# \bigoplus_{i=1}^a \mathcal{H}^2_{\ell_i}(K) = \#(R_K/p^N)^a$.

Let m_{R_K} be the maximal ideal of R_K. By Lemma 3.3.1, $\mathrm{Sel}(\mathbf{Z}[1/m], E[p^N]) \xrightarrow{\simeq} \mathrm{Sel}(O_K[1/m], E[p^N])^{\mathrm{Gal}(K/\mathbf{Q})}$ is bijective. Since $H^0(\mathbf{Q}, E[p^\infty]) = 0$, the kernel of the multiplication by p on $\mathrm{Sel}(\mathbf{Z}[1/m], E[p^N])$ is $\mathrm{Sel}(\mathbf{Z}[1/m], E[p])$. Therefore, we have an isomorphism $\mathrm{Sel}(O_K[1/m], E[p^N])^\vee \otimes_{R_K} R_K/m_{R_K} \simeq \mathrm{Sel}(\mathbf{Z}[1/m], E[p])^\vee$. From the exact sequence

$$0 \longrightarrow \mathrm{Sel}(\mathbf{Z}, E[p]) \longrightarrow \mathrm{Sel}(\mathbf{Z}[1/m], E[p]) \longrightarrow \bigoplus_{i=1}^{a} \mathcal{H}^2_{\ell_i}(\mathbf{Q}) \longrightarrow \mathrm{Sel}(\mathbf{Z}, E[p])^\vee \longrightarrow 0,$$

and $\mathcal{H}^2_{\ell_i}(\mathbf{Q}) = H^0(\mathbf{F}_{\ell_i}, E[p]) \simeq \mathbf{F}_p$, we know that $\mathrm{Sel}(\mathbf{Z}[1/m], E[p])$ is generated by a elements. Therefore, by Nakayama's lemma, $\mathrm{Sel}(O_K[1/m], E[p^N])^\vee$ is generated by a elements. Since $\#\,\mathrm{Sel}(O_K[1/m], E[p^N])^\vee = \#(R_K/p^N)^a$, $\mathrm{Sel}(O_K[1/m], E[p^N])^\vee$ is a free R_K/p^N-module of rank a. This shows that $\mathrm{Sel}(O_K[1/m], E[p^N])$ is also a free R_K/p^N-module of rank a because R_K/p^N is a Gorenstein ring.

(2) We identify $\bigoplus_{i=1}^a \mathcal{H}^2_{\ell_i}(K)$ with $(R_K/p^N)^a$, using a basis $\{t_{\ell_i,K}\}_{1\le i\le a}$. Consider $\phi_{\ell_i} : \mathrm{Sel}(O_K[1/m], E[p^N]) \longrightarrow \mathcal{H}^2_{\ell_i}(K)$ and the direct sum of ϕ_{ℓ_i}, which we denote by Φ;

$$\Phi = \oplus_{i=1}^a \phi_{\ell_i} : \mathrm{Sel}(O_K[1/m], E[p^N]) \longrightarrow \bigoplus_{i=1}^{a} \mathcal{H}^2_{\ell_i}(K) \simeq (R_K/p^N)^a.$$

Recall that $\kappa_{\frac{m}{\ell_i},\ell_i}$ is an element of $\mathrm{Sel}(O_K[1/m], E[p^N])$ (Proposition 3.4.2 (0)). By Proposition 3.4.2 (3), (4), we have

$$\Phi(\kappa_{\frac{m}{\ell_i},\ell_i}) = -\delta_m e_i$$

for each i where $\{e_i\}_{1\le i\le a}$ is the standard basis of the free module $(R_K/p^N)^a$. Since we are assuming that δ_m is a unit, Φ is surjective. Since both the target and the source are free modules of the same rank, Φ is bijective. This implies Theorem 4.2.1 (2).

(3) Using the exact sequence (4.2) and the isomorphism Φ, we have an exact sequence

$$(R_n/p^N)^a \xrightarrow{\partial\circ\Phi^{-1}} \bigoplus_{1\le i\le a} \mathcal{H}^2_{\ell_i}(K_n) \xrightarrow{r} \mathrm{Sel}(O_K, E[p^N])^\vee \longrightarrow 0.$$

We take a basis $\{-\delta_m e_i\}_{1\le i\le a}$ of $(R_n/p^N)^a$ and a basis $\{t_{\ell_i,K}\}_{1\le i\le a}$ of $\bigoplus_{1\le i\le a} \mathcal{H}^2_{\ell_i}(K_n)$. Then the (i,j)-component of the matrix corresponding to $\partial \circ \Phi^{-1}$ is $\partial_{\ell_i}(\kappa_{\frac{m}{\ell_j},\ell_j})$. If $i = j$, this is $\delta_{\frac{m}{\ell_i}}$ by Proposition 3.4.2 (2). If $i \neq j$, we have $\partial_{\ell_i}(\kappa_{\frac{m}{\ell_j},\ell_j}) = \phi_{\ell_i}(\kappa_{\frac{m}{\ell_i\ell_j},\ell_j})$ by Proposition 3.4.2 (1). This completes the proof of Theorem 4.2.1.

Remark 4.2.2 Suppose that ℓ is in $\mathcal{P}_1^{(N)}(K)$. We define

$$\Phi'_\ell : H^1(K, E[p^N]) \longrightarrow \mathcal{H}^1_{\ell,f}(K)$$

as the composition of the natural map $H^1(K, E[p^N]) \longrightarrow \bigoplus_{v|\ell} H^1(K_v, E[p^N])$ and $\phi' : H^1(K_v, E[p^N]) \longrightarrow H^1(\kappa(v), E[p^N]) = E(\kappa(v)) \otimes \mathbf{Z}/p^N$ in (3.4). For $m \in \mathcal{N}_1^{(N)}(K)$, we define

$$\Phi'_m : H^1(K, E[p^N]) \longrightarrow \bigoplus_{\ell|m} \mathcal{H}^1_{\ell,f}(K)$$

as the direct sum of Φ'_ℓ for $\ell \mid m$. By definition, the restriction of Φ'_m to $\mathcal{S} = \mathrm{Sel}(E/K, E[p^N])$ coincides with the canonical map s_m;

$$(\Phi'_m)_{|\mathcal{S}} = s_m : \mathrm{Sel}(E/K, E[p^N]) \longrightarrow \bigoplus_{\ell|m} \mathcal{H}^1_{\ell,f}(K)\ . \tag{4.3}$$

Since $\mathcal{H}^1_{\ell,f}(K)$ and $\mathcal{H}^2_\ell(K)$ are Pontrjagin dual each other, we can take the dual basis $t^*_{\ell,K}$ of $\mathcal{H}^1_{\ell,f}(K)$ as an R_K/p^N-module from the basis $t_{\ell,K}$ of $\mathcal{H}^2_\ell(K)$. Under the assumptions of Theorem 4.2.1, using the basis $\{t^*_{\ell_i,K}\}_{1\le i\le a}$ of $\bigoplus_{i=1}^a \mathcal{H}^1_{\ell,f}(K)$, $\{t_{\ell_i,K}\}_{1\le i\le a}$ of $\bigoplus_{i=1}^a \mathcal{H}^2_{\ell_i}(K)$ and the isomorphism Φ'_m, we have an exact sequence $\bigoplus_{\ell|m} \mathcal{H}^1_{\ell,f}(K) \xrightarrow{f} \bigoplus_{i=1}^a \mathcal{H}^2_{\ell_i}(K) \longrightarrow \mathrm{Sel}(E/K, E[p^N])^\vee \longrightarrow 0$. Then the matrix corresponding to f is an organizing matrix in the sense of Mazur and Rubin [15] (cf. [12] §9).

5 Modified Kolyvagin systems and numerical examples

5.1 Modified Kolyvagin systems of Gauss sum type

In §3.4 we constructed Kolyvagin systems $\kappa_{m,\ell}$ for (m, ℓ) such that $m\ell \in \mathcal{N}_1^{(N)}(K_{[\epsilon(m\ell)+1]})$. But the condition $\ell \in \mathcal{P}_1^{(N)}(K_{[\epsilon(m\ell)+1]})$ is too strict, and it is not suitable for numerical computation. In this subsection, we define a modified version of Kolyvagin systems of Gauss sum type for (m, ℓ) such that $m\ell \in \mathcal{N}_1^{(N)}(K)$.

Suppose that K is in $\mathcal{K}_{(p)}$. For each $\ell \in \mathcal{P}_1^{(N)}(K)$, we fix $t_\ell \in H^0(\mathbf{F}_\ell, E[p^N])$ of order p^N, and consider $t_{\ell,K} \in \mathcal{H}^2_\ell(K)$, whose ℓ_K-component is $t_\ell \otimes \zeta_{p^N}^{\otimes(-1)}$ and other components are zero. Using $t_{\ell,K}$, we regard ∂_ℓ and ϕ_ℓ as homomorphisms $\partial_\ell : H^1(K, E[p^N]) \longrightarrow R_K/p^N$ and $\phi_\ell : H^1(K, E[p^N]) \longrightarrow R_K/p^N$.

We will define an element $\kappa^{q,q',z}_{m,\ell}$ in $\mathrm{Sel}(O_K[1/m\ell], E[p^N])$ for (m, ℓ) such that $m\ell \in \mathcal{N}_1(K)$ (and for some primes q, q' and some z in $\mathrm{Sel}(O_K[1/qq'], E[p^N])$).

Consider (m, ℓ) such that ℓ is a prime and $m\ell \in \mathcal{N}_1(K)$. We take n_0 sufficiently large such that every prime of K_{n_0} dividing $m\ell$ is inert in K_∞/K_{n_0}. Then by Proposition 3.3.2 (1), for any $q \in (\mathcal{P}'_0)^{(N)}(K(m\ell)_{[1]}K_{n_0+N})$, $\kappa_{m\ell,q} \in \mathrm{Sel}(O_K[1/m\ell q], E[p^N])$ satisfies

$$\partial_r(\kappa_{m\ell,q}) = \phi_r(\kappa_{\frac{m\ell}{r},q})$$

for all r dividing $m\ell$. By Lemma 3.4.1, we can take $q, q' \in (\mathcal{P}'_0)^{(N)}(K(m\ell)_{[1]}K_{n_0+N})$ satisfying

- $w_K(t_{q,K}) = w_K(t_{q',K})$, and
- there is $z \in H^1_f(O_K[1/qq'], E[p^N])$ such that $\partial_K(z) = t_{q,K} - t_{q',K}$, $\phi_\ell(z) = 1$ and $\phi_r(z) = 0$ for any r dividing m.

For any $m \in \mathcal{N}_1(K)$, let δ_m be the element defined in (3.6). We define

$$\kappa^{q,q',z}_{m,\ell} = \kappa_{m\ell,q} - \kappa_{m\ell,q'} - \delta_{m\ell} z \ . \tag{5.1}$$

By Proposition 3.3.2 (2), we have $\kappa^{q,q',z}_{m,\ell} \in \mathrm{Sel}(O_K[1/m\ell], E[p^N])$.

Proposition 5.1.1 (0) $\kappa^{q,q',z}_{m,\ell}$ *is in* $\mathrm{Sel}(O_K[1/m\ell], E[p^N])$.
(1) *The element* $\kappa^{q,q',z}_{m,\ell}$ *satisfies* $\partial_r(\kappa^{q,q',z}_{m,\ell}) = \phi_r(\kappa^{q,q',z}_{\frac{m}{r},\ell})$ *for any prime divisor* r *of* m.
(2) *We further assume that* $m\ell$ *is admissible in the sense of the paragraph before Proposition 3.3.2. Then we have* $\phi_r(\kappa^{q,q',z}_{m,\ell}) = 0$ *for any prime divisor* r *of* m.
(3) *Under the same assumptions as* (2), $\phi_\ell(\kappa^{q,q',z}_{m,\ell}) = -\delta_{m\ell}$ *holds.*

Proof. (1) Using the definition of $\kappa^{q,q',z}_{m,\ell}$ and Proposition 3.3.2 (1), we have $\partial_r(\kappa^{q,q',z}_{m,\ell}) = \partial_r(\kappa_{m\ell,q} - \kappa_{m\ell,q'}) = \phi_r(\kappa_{\frac{m\ell}{r},q} - \kappa_{\frac{m\ell}{r},q'})$. Next, we use the definition of $\kappa^{q,q',z}_{\frac{m}{r},\ell}$ and $\phi_r(z) = 0$ to get $\phi_r(\kappa_{\frac{m\ell}{r},q} - \kappa_{\frac{m\ell}{r},q'}) = \phi_r(\kappa^{q,q',z}_{\frac{m}{r},\ell} + \delta_{\frac{m\ell}{r}} z) = \phi_r(\kappa^{q,q',z}_{\frac{m}{r},\ell})$. These computations imply (1).
(2) We have $\phi_r(\kappa_{m\ell,q}) = \phi_r(\kappa_{m\ell,q'}) = 0$ by Proposition 3.3.2 (3). This together with $\phi_r(z) = 0$ implies $\phi_r(\kappa^{q,q',z}_{m,\ell}) = \phi_r(\kappa_{m\ell,q} - \kappa_{m\ell,q'} - \delta_{m\ell} z) = 0$.
(3) We again use Proposition 3.3.2 (3) to get $\phi_\ell(\kappa_{m\ell,q}) = \phi_\ell(\kappa_{m\ell,q'}) = 0$. Since $\phi_\ell(z) = 1$, we have $\phi_\ell(\kappa^{q,q',z}_{m,\ell}) = \phi_\ell(\kappa_{m\ell,q} - \kappa_{m\ell,q'} - \delta_{m\ell} z) = -\delta_{m\ell}$. This completes the proof of Proposition 5.1.1.

5.2 Proof of Theorem 1.2.5

In this subsection we take $K = \mathbf{Q}$. For $m \in \mathcal{N}^{(N)} = \mathcal{N}^{(N)}(\mathbf{Q})$, we consider $\delta_m \in \mathbf{Z}/p^N$, which is defined from $\vartheta_{\mathbf{Q}(m)}$ by (3.6). We define $\tilde{\delta}_m \in \mathbf{Z}/p^N$ by

$$\tilde{\theta}_{\mathbf{Q}(m)} \equiv \tilde{\delta}_m \prod_{i=1}^{r} (\tau_{\ell_i} - 1) \pmod{p^N, (\tau_{\ell_1} - 1)^2, ..., (\tau_{\ell_r} - 1)^2} \tag{5.2}$$

where $m = \ell_1 \cdot ... \cdot \ell_r$. By (2.4), $\tilde{\theta}_{\mathbf{Q}(m)} = u\vartheta_{\mathbf{Q}(m)}$ for some unit $u \in R^{\times}_{\mathbf{Q}(m)}$. This together with (3.6) and (5.2) implies that

$$\mathrm{ord}_p(\tilde{\delta}_m) = \mathrm{ord}_p(\delta_m). \tag{5.3}$$

We take a generator $\eta_\ell \in (\mathbf{Z}/\ell\mathbf{Z})^\times$ such that the image of $\sigma_{\eta_\ell} \in \mathrm{Gal}(\mathbf{Q}(\mu_\ell)/\mathbf{Q}) \simeq (\mathbf{Z}/\ell)^\times$ in $\mathrm{Gal}(\mathbf{Q}(\ell)/\mathbf{Q}) \simeq (\mathbf{Z}/\ell)^\times \otimes \mathbf{Z}_p$ is τ_ℓ which is the generator we took. Then, using (5.2) and (1.1), we can easily check that the equation (1.2) in §1.1 holds.

In the rest of this subsection, we take $N = 1$. We simply write $\mathcal{P}_1$ for $\mathcal{P}_1^{(1)}$, so

$$\mathcal{P}_1 = \{\ell \in \mathcal{P}_{good} \mid \ell \equiv 1 \pmod{p} \text{ and } E(\mathbf{F}_\ell) \simeq \mathbf{Z}/p\}.$$

The set of squarefree products of primes in $\mathcal{P}_1$ is denoted by $\mathcal{N}_1$.

We first prove the following lemma which is related to the functional equation of an elliptic curve.

Lemma 5.2.1 *Let ϵ be the root number of E. Suppose that $m \in \mathcal{N}_1$ is δ-minimal (for the definition of δ-minimalness, see the paragraph before Conjecture 1.2.4). Then we have $\epsilon = (-1)^{\epsilon(m)}$.*

Proof. By the functional equation (1.6.2) in Mazur and Tate [16] and the above definition of $\tilde{\delta}_m$, we have $\epsilon(-1)^{\epsilon(m)}\tilde{\delta}_m \equiv \tilde{\delta}_m \pmod{p}$. Since $\tilde{\delta}_m \not\equiv 0 \pmod{p}$ is equivalent to $\delta_m \not\equiv 0 \pmod{p}$ by (5.3), we get the conclusion.

For each $\ell \in \mathcal{P}_1$, we fix a generator $t_\ell \in \mathcal{H}^2_\ell(\mathbf{Q}) = H^0(\mathbf{F}_\ell, E[p](-1)) \simeq \mathbf{Z}/p = \mathbf{F}_p$, and regard ϕ_ℓ as a map $\phi_\ell : H^1(\mathbf{Q}, E[p]) \longrightarrow \mathbf{F}_p$. Note that the restriction of ϕ_ℓ to $\mathrm{Sel}(E/\mathbf{Q}, E[p])$ is the zero map if and only if the natural map $s_\ell : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow E(\mathbf{F}_\ell) \otimes \mathbf{Z}/p \simeq \mathbf{F}_p$ is the zero map.

I) Proof of Theorem 1.2.5 (1), (2).
Suppose that $\epsilon(m) = 0$, namely $m = 1$. Then $\delta_1 = \theta_{\mathbf{Q}} \bmod p = L(E, 1)/\Omega^+_E \bmod p$. If $\delta_1 \neq 0$, $\mathrm{Sel}(E/\mathbf{Q}, E[p]) = 0$ and s_1 is trivially bijective. Suppose next $\epsilon(m) = 1$, so $m = \ell \in \mathcal{P}_1$. It is sufficient to prove the next two propositions.

Proposition 5.2.2 *Assume that $\ell \in \mathcal{P}_1$ is δ-minimal. Then* $\mathrm{Sel}(E/\mathbf{Q}, E[p])$ *is 1-dimensional over $\mathbf{F}_p$, and $s_\ell : \mathrm{Sel}(E/\mathbf{Z}, E[p]) \longrightarrow \mathbf{F}_p$ is bijective. Moreover, the Selmer group* $\mathrm{Sel}(E/\mathbf{Q}, E[p^\infty])^\vee$ *with respect to the p-power torsion points $E[p^\infty]$ is a free $\mathbf{Z}_p$-module of rank 1, namely* $\mathrm{Sel}(E/\mathbf{Q}, E[p^\infty])^\vee \simeq \mathbf{Z}_p$.

Proof. We first assume $\mathrm{Sel}(E/\mathbf{Q}, E[p]) = 0$ and will obtain the contradiction. We consider $\kappa_{1,\ell}^{q,q',z} = \kappa_{\ell,q} - \kappa_{\ell,q'} - \delta_\ell z$, which was defined in (5.1). By Proposition 3.3.2 (1), we know $\partial_\ell(\kappa_{1,\ell}^{q,q',z}) = \phi_\ell(g_q - g_{q'})$. Consider the exact sequence (see Lemma 3.2.1)

$$0 \longrightarrow \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow \mathrm{Sel}(\mathbf{Z}[1/r], E[p]) \longrightarrow \mathcal{H}_r^2(\mathbf{Q})$$

for any $r \in \mathcal{P}_1$ where $\mathrm{Sel}(\mathbf{Z}[1/r], E[p]) \longrightarrow \mathcal{H}_r^2(\mathbf{Q}) \simeq \mathbf{F}_p$ is nothing but ∂_r. Since we assumed $\mathrm{Sel}(E/\mathbf{Q}, E[p]) = 0$, $\mathrm{Sel}(\mathbf{Z}[1/r], E[p]) \longrightarrow \mathcal{H}_r^2(\mathbf{Q}) \simeq \mathbf{F}_p$ is injective for any $r \in \mathcal{P}_1$. So $\partial_q(g_q) = \delta_1 = 0$ implies that $g_q = 0$. By the same method, we have $g_{q'} = 0$. Therefore, $\partial_\ell(\kappa_{1,\ell}^{q,q',z}) = \phi_\ell(g_q - g_{q'}) = 0$, which implies that $\kappa_{1,\ell}^{q,q',z} \in \mathrm{Sel}(E/\mathbf{Q}, E[p])$.

But Proposition 5.1.1 (3) tells us that $\phi_\ell(\kappa_{1,\ell}^{q,q',z}) = -\delta_\ell \neq 0$. Therefore, $\kappa_{1,\ell}^{q,q',z} \neq 0$, which contradicts our assumption $\mathrm{Sel}(E/\mathbf{Q}, E[p]) = 0$. Thus we get $\mathrm{Sel}(E/\mathbf{Q}, E[p]) \neq 0$.

On the other hand, by Corollary 4.1.3 we know that $s_\ell : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow \mathbf{F}_p$ is injective, therefore bijective.

By Lemma 5.2.1, the root number ϵ is -1. This shows that $\mathrm{Sel}(E/\mathbf{Q}, E[p^\infty])^\vee$ has positive $\mathbf{Z}_p$-rank by the parity conjecture proved by Nekovář ([18]). Therefore, we finally have $\mathrm{Sel}(E/\mathbf{Q}, E[p^\infty])^\vee \simeq \mathbf{Z}_p$, which completes the proof of Proposition 5.2.2.

If we assume a slightly stronger condition on ℓ, we also obtain the main conjecture. Let $\lambda' = \lambda^{an}$ be the analytic λ-invariant of the p-adic L-function $\vartheta_{\mathbf{Q}_\infty}$. We put $n_{\lambda'} = \min\{n \in \mathbf{Z} \mid p^n - 1 \geq \lambda'\}$.

Proposition 5.2.3 *Suppose that there is $\ell \in \mathcal{P}_1$ such that*

$$\ell \equiv 1 \pmod{p^{n_{\lambda'}+2}} \text{ and } \tilde{\delta}_\ell \neq 0.$$

Then the main conjecture for $(E, \mathbf{Q}_\infty/\mathbf{Q})$ is true and $\mathrm{Sel}(E/\mathbf{Q}_\infty, E[p^\infty])^\vee$ *is generated by one element as a $\Lambda_{\mathbf{Q}_\infty}$-module.*

Proof. We use our Euler system $g_\ell^{(K)}$ in §3.2 instead of $\kappa_{1,\ell}^{q,q',z}$ which was used in the proof of Proposition 5.2.2. Let λ be the algebraic λ-invariant, namely the rank of $\mathrm{Sel}(E/\mathbf{Q}_\infty, E[p^\infty])^\vee$. Then $\lambda \leq \lambda'$ and $\vartheta_{\mathbf{Q}_\infty} \in \mathrm{char}(\mathrm{Sel}(O_{\mathbf{Q}_\infty}, E[p^\infty])^\vee)$ by Kato's theorem.

Put $K=\mathbf{Q}_{n_{\lambda'}}$ and $f=p^{n_{\lambda'}}$. Consider the group ring $R_K/p=\mathbf{F}_p[\mathrm{Gal}(K/\mathbf{Q})]$. We identify a generator γ of $\mathrm{Gal}(K/\mathbf{Q})$ with $1+\mathfrak{t}$, and identify R_K/p with $\mathbf{F}_p[[\mathfrak{t}]]/(\mathfrak{t}^f)$. The norm $N_{\mathrm{Gal}(K/\mathbf{Q})}=\Sigma_{i=0}^{f-1}\gamma^i$ is $\mathfrak{t}^{f-1}$ by this identification, so our assumption $\lambda'\leq f-1$ implies that the corestriction map $\mathrm{Sel}(E/K,E[p])\longrightarrow\mathrm{Sel}(E/\mathbf{Q},E[p])$ is the zero map because $\lambda\leq\lambda'$. Therefore, we have $\mathbf{Q}_{[1]}\subset K$. Since $p^{n_{\lambda'}+1}-p^{n_{\lambda'}}>p^{n_{\lambda'}}-1\geq\lambda'\geq\lambda$, the corestriction map $\mathrm{Sel}(E/\mathbf{Q}_{n_{\lambda'}+1},E[p])\longrightarrow\mathrm{Sel}(E/\mathbf{Q}_{n_{\lambda'}},E[p])=\mathrm{Sel}(E/K,E[p])$ is also the zero map. This shows that $\mathbf{Q}_{[2]}\subset\mathbf{Q}_{n_{\lambda'}+1}$.

Our assumption $\ell\equiv 1 \pmod{p^{n_{\lambda'}+2}}$ implies that ℓ splits completely in $\mathbf{Q}_{n_{\lambda'}+1}$, so we have $\ell\in\mathcal{P}_1(\mathbf{Q}_{[2]})=\mathcal{P}_1(K_{[1]})$. Therefore, we can define

$$g_\ell^{(K)}\in\mathrm{Sel}(O_K[1/\ell],E[p])$$

in §3.2. Since $\ell\in\mathcal{P}_1(\mathbf{Q}_{[2]})$, we also have

$$\phi_\ell(g_\ell^{(\mathbf{Q})})=-\delta_\ell^{(\mathbf{Q})}=-\delta_\ell$$

by Proposition 3.4.2 (4). It follows from our assumption $\delta_\ell\neq 0$ that $g_\ell^{(\mathbf{Q})}\neq 0$. Since $\mathrm{Cor}_{K/\mathbf{Q}}(g_\ell^{(K)})=g_\ell^{(\mathbf{Q})}$ and the natural map $i:\mathrm{Sel}(\mathbf{Z}[1/\ell],E[p])\longrightarrow\mathrm{Sel}(O_K[1/\ell],E[p])$ is injective, we get

$$i(g_\ell^{(\mathbf{Q})})=N_{\mathrm{Gal}(K/\mathbf{Q})}g_\ell^{(K)}=\mathfrak{t}^{f-1}g_\ell^{(K)}\neq 0.$$

Consider $\partial_\ell:\mathrm{Sel}(O_K[1/\ell],E[p])\longrightarrow R_K/p$. By definition, we have $\partial_\ell(g_\ell^{(K)})=u\mathfrak{t}^{\lambda'}$ for some unit u of R_K/p. This shows that $\partial_\ell(\mathfrak{t}^{f-\lambda'}g_\ell^{(K)})=0$, which implies that $\mathfrak{t}^{f-\lambda'}g_\ell^{(K)}\in\mathrm{Sel}(E/K,E[p])$. The fact $\mathfrak{t}^{f-1}g_\ell^{(K)}\neq 0$ implies the submodule generated by $\mathfrak{t}^{f-\lambda'}g_\ell^{(K)}$ is isomorphic to $R_K/(p,\mathfrak{t}^{\lambda'})$ as an R_K-module. Namely, we have

$$\mathrm{Sel}(E/K,E[p])\supset\langle\mathfrak{t}^{f-\lambda'}g_\ell^{(K)}\rangle\simeq R_K/(p,\mathfrak{t}^{\lambda'}).$$

This implies that $\lambda=\lambda'$, and $\mathrm{Sel}(E/K,E[p])\simeq R_K/(p,\mathfrak{t}^{\lambda})$. Therefore, we have $\mathrm{Sel}(E/\mathbf{Q}_\infty,E[p])^\vee\simeq\Lambda_{\mathbf{Q}_\infty}/(p,\vartheta_{\mathbf{Q}_\infty})$. This together with Kato's theorem we mentioned implies that $\mathrm{Sel}(E/\mathbf{Q}_\infty,E[p^\infty])^\vee\simeq\Lambda_{\mathbf{Q}_\infty}/(\vartheta_{\mathbf{Q}_\infty})$.

II) Proof of Theorem 1.2.5 (3).
Suppose that $m=\ell_1\ell_2\in\mathcal{N}_1$ and m is δ-minimal. As in the proof of Proposition 5.2.2, we assume $\mathrm{Sel}(E/\mathbf{Q},E[p])=0$ and will get the contradiction. We consider $\kappa_{\ell_1,\ell_2}^{q,q',z}$ defined in (5.1). Consider the exact sequence (see Lemma 3.2.1)

$$0\longrightarrow\mathrm{Sel}(E/\mathbf{Q},E[p])\longrightarrow\mathrm{Sel}(\mathbf{Z}[1/\ell_1\ell_2qq'],E[p])\xrightarrow{\partial}\bigoplus_{v\in\{\ell_1,\ell_2,q,q'\}}\mathcal{H}_v^2(\mathbf{Q}).$$

By the same method as the proof of Proposition 5.2.2, $g_q = g_{q'} = 0$. Therefore, $\partial_{\ell_1}(\kappa_{\ell_1,q} - \kappa_{\ell_1,q'}) = \phi_{\ell_1}(g_q - g_{q'}) = 0$ by Proposition 3.3.2 (1). We have $\partial_q(\kappa_{\ell_1,q}) = \delta_{\ell_1} = 0$, $\partial_q(\kappa_{\ell_1,q'}) = 0$, $\partial_{q'}(\kappa_{\ell_1,q}) = 0$, $\partial_{q'}(\kappa_{\ell_1,q'}) = \delta_{\ell_1} = 0$. Therefore, $\partial(\kappa_{\ell_1,q} - \kappa_{\ell_1,q'}) = 0$. This together with $\mathrm{Sel}(E/\mathbf{Q}, E[p]) = 0$ shows that $\kappa_{\ell_1,q} - \kappa_{\ell_1,q'} = 0$. Therefore, using Proposition 3.3.2 (1), we have

$$\partial_{\ell_2}(\kappa^{q,q',z}_{\ell_1,\ell_2}) = \partial_{\ell_2}(\kappa_{m,q} - \kappa_{m,q'}) = \phi_{\ell_2}(\kappa_{\ell_1,q} - \kappa_{\ell_1,q'}) = 0.$$

By the same method as the above proof of $\kappa_{\ell_1,q} - \kappa_{\ell_1,q'} = 0$, we get $\kappa^{q,q',z}_{1,\ell_2} = 0$. This implies that $\partial_{\ell_1}(\kappa^{q,q',z}_{\ell_1,\ell_2}) = \phi_{\ell_1}(\kappa^{q,q',z}_{1,\ell_2}) = 0$ by Proposition 5.1.1 (1). It follows that $\partial(\kappa^{q,q',z}_{\ell_1,\ell_2}) = 0$, which implies $\kappa^{q,q',z}_{\ell_1,\ell_2} \in \mathrm{Sel}(E/\mathbf{Q}, E[p])$. But this is a contradiction because we assumed $\mathrm{Sel}(E/\mathbf{Q}, E[p]) = 0$ and

$$\phi_{\ell_2}(\kappa^{q,q',z}_{\ell_1,\ell_2}) = -\delta_m \neq 0$$

by Proposition 5.1.1 (3). Thus, we get $\mathrm{Sel}(E/\mathbf{Q}, E[p]) \neq 0$.

Now the root number is 1 by Lemma 5.2.1, therefore, by the parity conjecture proved by Nekovář ([18]), we obtain $\dim_{\mathbf{F}_p} \mathrm{Sel}(E/\mathbf{Q}, E[p]) \geq 2$. On the other hand, by Corollary 4.1.3 we know that $s_m : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow (\mathbf{F}_p)^{\oplus 2}$ is injective. Therefore, the injectivity of s_m implies the bijectivity of s_m. This completes the proof of Theorem 1.2.5 (3).

We give a simple corollary.

Corollary 5.2.4 *Suppose that there is $m \in \mathcal{N}_1$ such that m is δ-minimal and $\epsilon(m) = 2$. We further assume that the analytic λ-invariant λ' is 2. Then the main conjecture for $(E, \mathbf{Q}_\infty/\mathbf{Q})$ holds.*

Proof. Put $\mathfrak{t} = \gamma - 1$ and identify $\Lambda_{\mathbf{Q}_\infty}/p$ with $\mathbf{F}_p[[\mathfrak{t}]]$. Let $\mathcal{A}$ be the relation matrix of $S = \mathrm{Sel}(E/\mathbf{Q}_\infty, E[p^\infty])^\vee$. Since $S/(p, \mathfrak{t}) = \mathrm{Sel}(E/\mathbf{Q}, E[p])^\vee \simeq \mathbf{F}_p \oplus \mathbf{F}_p$, $\mathfrak{t}^2$ divides $\det \mathcal{A}$ mod p. Therefore, the algebraic λ-invariant is also 2. This implies the main conjecture because $\det \mathcal{A}$ divides $\vartheta_{\mathbf{Q}_\infty}$ in $\Lambda_{\mathbf{Q}_\infty}$ (Kato [7]).

III) Proof of Theorem 1.2.5 (4).

Lemma 5.2.5 *Suppose that ℓ, ℓ_1, ℓ_2 are distinct primes in $\mathcal{P}_1$ satisfying $\delta_\ell = \delta_{\ell\ell_1} = \delta_{\ell\ell_2} = 0$. Assume also that $s_\ell : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow \mathbf{F}_p$ is bijective, and that $\ell\ell_1$, $\ell\ell_2$ are both admissible. We take q, q' such that they satisfy the conditions when we defined $\kappa^{q,q',z}_{\ell_1\ell_2,\ell}$. Then we have*
(1) $\mathrm{Sel}(E/\mathbf{Q}, E[p]) = \mathrm{Sel}(\mathbf{Z}[1/\ell], E[p])$,
(2) $\kappa^{q,q',z}_{\ell_1,\ell} = 0$, $\kappa^{q,q',z}_{\ell_2,\ell} = 0$, and
(3) $\kappa^{q,q',z}_{\ell_1\ell_2,\ell} \in \mathrm{Sel}(E/\mathbf{Q}, E[p])$.

Proof. (1) Since s_ℓ is bijective, taking the dual, we get the bijectivity of $\mathcal{H}^2_\ell(\mathbf{Q}) \longrightarrow \mathrm{Sel}(E/\mathbf{Q}, E[p])^\vee = \mathrm{Sel}(\mathbf{Z}, E[p])^\vee$. By the exact sequence

$$0 \longrightarrow \mathrm{Sel}(\mathbf{Z}, E[p]) \longrightarrow \mathrm{Sel}(\mathbf{Z}[1/\ell], E[p]) \xrightarrow{\partial_\ell} \mathcal{H}^2_\ell(\mathbf{Q}) \longrightarrow \mathrm{Sel}(\mathbf{Z}, E[p])^\vee \longrightarrow 0$$

in Lemma 3.2.1, we get $\mathrm{Sel}(E/\mathbf{Q}, E[p]) = \mathrm{Sel}(\mathbf{Z}, E[p]) = \mathrm{Sel}(\mathbf{Z}[1/\ell], E[p])$.
(2) We first note that the bijectivity of $s_\ell : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow \mathbf{F}_p$ implies the bijectivity of $\phi_\ell : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow \mathbf{F}_p$. Since $\partial_q(\kappa_{\ell,q}) = \delta_\ell = 0$, $\kappa_{\ell,q} \in \mathrm{Sel}(\mathbf{Z}[1/\ell], E[p]) = \mathrm{Sel}(E/\mathbf{Q}, E[p])$ where we used the property (1) which we have just proved. Proposition 3.3.2 (3) implies $\phi_\ell(\kappa_{\ell,q}) = 0$, which implies $\kappa_{\ell,q} = 0$ by the bijectivity of ϕ_ℓ. By the same method, we have $\kappa_{\ell,q'} = 0$. Therefore, we have

$$\kappa^{q,q',z}_{1,\ell} = \kappa_{\ell,q} - \kappa_{\ell,q'} - \delta_\ell z = 0.$$

Therefore, Proposition 5.1.1 (1) implies $\partial_{\ell_1}(\kappa^{q,q',z}_{\ell_1,\ell}) = \phi_{\ell_1}(\kappa^{q,q',z}_{1,\ell}) = 0$. This implies $\kappa^{q,q',z}_{\ell_1,\ell} \in \mathrm{Sel}(\mathbf{Z}[1/\ell], E[p]) = \mathrm{Sel}(E/\mathbf{Q}, E[p])$. Using Proposition 5.1.1 (3), we have

$$\phi_\ell(\kappa^{q,q',z}_{\ell_1,\ell}) = -\delta_{\ell\ell_1} = 0,$$

which implies $\kappa^{q,q',z}_{\ell_1,\ell} = 0$ by the bijectivity of ϕ_ℓ. The same proof works for $\kappa^{q,q',z}_{\ell_2,\ell}$.
(3) It follows from Proposition 5.1.1 (1) and Lemma 5.2.5 (2) that $\partial_{\ell_i}(\kappa^{q,q',z}_{\ell_1\ell_2,\ell}) = \phi_{\ell_i}(\kappa^{q,q',z}_{\frac{\ell_1\ell_2}{\ell_i},\ell}) = 0$ for each $i = 1, 2$. This implies $\kappa^{q,q',z}_{\ell_1\ell_2,\ell} \in \mathrm{Sel}(\mathbf{Z}[1/\ell], E[p])$. Using $\mathrm{Sel}(\mathbf{Z}[1/\ell], E[p]) = \mathrm{Sel}(E/\mathbf{Q}, E[p])$ which we proved in (1), we get the conclusion. This completes the proof of Lemma 5.2.5.

We next prove Theorem 1.2.5 (4). Assume that $m = \ell_1\ell_2\ell_3 \in \mathcal{N}_1$, m is δ-minimal, m is admissible, and $s_{\ell_i} : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow \mathbf{F}_p$ is surjective for each $i = 1, 2$.

We assume $\dim_{\mathbf{F}_p} \mathrm{Sel}(E/\mathbf{Q}, E[p]) = 1$ and will get the contradiction. By this assumption, $s_{\ell_i} : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow \mathbf{F}_p$ for each $i = 1, 2$ is bijective. This implies that $\phi_{\ell_i} : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow \mathbf{F}_p$ for each $i = 1, 2$ is also bijective. By Lemma 5.2.5 (3) we get $\kappa^{q,q',z}_{\ell_2\ell_3,\ell_1} \in \mathrm{Sel}(E/\mathbf{Q}, E[p])$, taking q, q' satisfying the conditions when we defined this element. By Proposition 5.1.1 (3), we have $\phi_{\ell_1}(\kappa^{q,q',z}_{\ell_2\ell_3,\ell_1}) = -\delta_m \neq 0$, which implies $\kappa^{q,q',z}_{\ell_2\ell_3,\ell_1} \neq 0$. But by Proposition 5.1.1 (2), we have $\phi_{\ell_2}(\kappa^{q,q',z}_{\ell_2\ell_3,\ell_1}) = 0$. This contradicts the bijectivity of ϕ_{ℓ_2}. Therefore, we obtain $\dim_{\mathbf{F}_p} \mathrm{Sel}(E/\mathbf{Q}, E[p]) > 1$.

By Lemma 5.2.1 and our assumption that m is δ-minimal, we know that the root number ϵ is -1. This shows that $\dim_{\mathbf{F}_p} \mathrm{Sel}(E/\mathbf{Q}, E[p]) \geq 3$ by the parity conjecture proved by Nekovář ([18]). On the other hand, Corollary

4.1.3 implies that $\dim_{\mathbf{F}_p} \mathrm{Sel}(E/\mathbf{Q}, E[p]) \leq 3$ and $s_m : \mathrm{Sel}(E/\mathbf{Q}, E[p]) \longrightarrow \mathbf{F}_p^{\oplus 3}$ is injective. Therefore, the above map s_m is bijective. This completes the proof of Theorem 1.2.5 (4).

5.3 Numerical examples

In this section, we give several numerical examples.

Let $E = X_0(11)^{(d)}$ be the quadratic twist of $X_0(11)$ by d, namely $dy^2 = x^3 - 4x^2 - 160x - 1264$. We take $p = 3$. Then if $d \equiv 1 \pmod{p}$, p is a good ordinary prime which is not anomalous (namely $a_p(= a_3)$ for E satisfies $a_p \not\equiv 1 \pmod{p}$), and $p = 3$ does not divide $\mathrm{Tam}(E)$, and the Galois representation on $T_3(E)$ is surjective. In the following examples, we checked $\mu' = 0$ where μ' is the analytic μ-invariant. Then this implies that the algebraic μ-invariant is also zero (Kato [7] Theorem 17.4 (3)) under our assumptions. In the computations of $\tilde{\delta}_m$ below, we have to fix a generator of $\mathrm{Gal}(\mathbf{Q}(\ell)/\mathbf{Q}) \simeq (\mathbf{Z}/\ell\mathbf{Z})^\times$ for a prime ℓ. We always take the least primitive root η_ℓ of $(\mathbf{Z}/\ell\mathbf{Z})^\times$. We compute $\tilde{\delta}_m$ using the formula in (1.2).

(1) $d = 13$. We take $N = 1$. Since $\tilde{\delta}_7 = 20 \not\equiv 0 \pmod 3$, we know that $\mathrm{Fitt}_{1,\mathbf{F}_3}(\mathrm{Sel}(E/\mathbf{Q}, E[3])^\vee) = \mathbf{F}_3$ by Theorem 2.4.1, so $\mathrm{Sel}(E/\mathbf{Q}, E[3])$ is generated by one element.

The root number is $\epsilon = (\frac{13}{11}) = -1$, so $L(E, 1) = 0$. We compute $\mathcal{P}_1 = \{7, 31, 73, ...\}$. Therefore, $\tilde{\delta}_7 \not\equiv 0 \pmod 3$ implies $\mathrm{Sel}(E/\mathbf{Q}, E[3]) \simeq \mathbf{F}_3$ and

$$\mathrm{Sel}(E/\mathbf{Q}, E[3^\infty])^\vee \simeq \mathbf{Z}_3$$

by Proposition 5.2.2. Also, it is easily computed that $\lambda' = 1$ in this case. This implies that $\mathrm{Sel}(E/\mathbf{Q}_\infty, E[3^\infty])^\vee \simeq \mathbf{Z}_3$, so the main conjecture also holds.

We can find a point $P = (7045/36, -574201/216)$ of infinite order on the minimal Weierstrass model $y^2 + y = x^3 - x^2 - 1746x - 50295$ of $E = X_0(11)^{(13)}$. Therefore, we know $Ш(E/\mathbf{Q})[3^\infty] = 0$. We can easily check that $E(\mathbf{F}_7)$ is cyclic of order 6, and that the image of the point P in $E(\mathbf{F}_7)/3E(\mathbf{F}_7)$ is non-zero. So we also checked numerically that $s_7 : \mathrm{Sel}(E/\mathbf{Q}, E[3]) \longrightarrow E(\mathbf{F}_7)/3E(\mathbf{F}_7)$ is bijective as Proposition 5.2.2 claims.

(2) $d = 40$. We know $\epsilon = (\frac{40}{11}) = -1$. We take $N = 1$. We can compute $\mathcal{P}_1 = \{7, 67, 73, ...\}$, and $\tilde{\delta}_7 = -40 \not\equiv 0 \pmod 3$. This implies that $\mathrm{Sel}(E/\mathbf{Q}, E[3]) \simeq \mathbf{F}_3$ and $\mathrm{Sel}(E/\mathbf{Q}, E[3^\infty])^\vee \simeq \mathbf{Z}_3$ by Proposition 5.2.2.

In this case, we know $\lambda' = 7$. Therefore, $n_{\lambda'} = 2$. We can check $5347 \in \mathcal{P}_1$ (where $5347 \equiv 1 \pmod{3^5}$) and $\tilde{\delta}_{5347} = -412820 \not\equiv 0 \pmod 3$. Therefore, the main conjecture holds by Proposition 5.2.3. In this case, we can check that the p-adic L-function $\vartheta_{\mathbf{Q}_\infty}$ is divisible by $(1+\mathfrak{t})^3-1$, so we have

$$\mathrm{rank}_{\mathbf{Z}_3}\,\mathrm{Sel}(E/\mathbf{Q}_1, E[3^\infty])^\vee = 3$$

where $\mathbf{Q}_1$ is the first layer of $\mathbf{Q}_\infty/\mathbf{Q}$.

In the following, for a prime $\ell \in \mathcal{P}$, we take a generator τ_ℓ of $\mathrm{Gal}(\mathbf{Q}(\ell)/\mathbf{Q}) \simeq (\mathbf{Z}/\ell\mathbf{Z})^\times$ and put $S = \tau_\ell - 1$. We write $\vartheta_{\mathbf{Q}(\ell)} = \Sigma a_i^{(\ell)} S^i$ where $a_i^{(\ell)} \in \mathbf{Z}_p$. Note that $\tilde{\delta}_\ell = a_1^{(\ell)}$.

(3) $d = 157$. We know $\epsilon = (\frac{157}{11}) = 1$ and $L(E,1)/\Omega_E^+ = 45$. We take $N = 1$. We compute $a_2^{(37)} = -14065/2 \not\equiv 0 \pmod 3$. Since $37 \equiv 1 \pmod{3^2}$, $c_2 = 2-1 = 1$ and $a_2^{(37)}$ is in $\mathrm{Fitt}_{2,\mathbf{F}_3}(\mathrm{Sel}(E/\mathbf{Q}, E[3])^\vee)$ by Theorem 2.4.1, which implies that $\mathrm{Fitt}_{2,\mathbf{F}_3}(\mathrm{Sel}(E/\mathbf{Q}, E[3])) = \mathbf{F}_3$. Therefore, $\mathrm{Sel}(E/\mathbf{Q}, E[3])$ is generated by at most two elements.

We compute $\mathcal{P}_1 = \{7, 67, 73, 127, ...\}$. Since $127 \equiv 1 \pmod 7$, 7×127 is admissible. We compute $\tilde{\delta}_{7\times 127} = 83165 \not\equiv 0 \pmod 3$. Therefore, 7×127 is δ-minimal. It follows from Theorem 1.2.5 (3) that $\mathrm{Sel}(E/\mathbf{Q}, E[3]) \simeq \mathbf{F}_3 \oplus \mathbf{F}_3$. In this example, we can check $\lambda' = 2$, so Corollary 5.2.4 together with the above computation implies the main conjecture. Since $L(E,1)/\Omega_E^+ = 45 \neq 0$, $\mathrm{rank}\,E(\mathbf{Q}) = 0$ by Kato, which implies $\mathrm{Sel}(E/\mathbf{Q}, E[3^\infty]) = Ш(E/\mathbf{Q})[3^\infty]$. Since $45 \in \mathrm{Fitt}_{0,\mathbf{Z}_3}(\mathrm{Sel}(E/\mathbf{Q}, E[3^\infty])^\vee)$, we have $\#Ш(E/\mathbf{Q})[3^\infty] \leq 9$, and

$$Ш(E/\mathbf{Q})[3^\infty] \simeq \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}.$$

(4) $d = 265$. In this case, $\epsilon = (\frac{265}{11}) = 1$ and $L(E,1) = 0$. We take $N = 1$. As in Example (3), we compute $a_2^{(37)} = 16985 \not\equiv 0 \pmod 3$, which implies that $\mathrm{Sel}(E/\mathbf{Q}, E[3])$ is generated by at most two elements as above. We compute $\mathcal{P}_1 = \{7, 13, 31, 67, 103, 109, 127, ...\}$. For an admissible pair $\{7, 127\}$, we have $\tilde{\delta}_{7\times 127} = -138880 \not\equiv 0 \pmod 3$. Therefore, 7×127 is δ-minimal and $\mathrm{Sel}(E/\mathbf{Q}, E[3]) \simeq \mathbf{F}_3 \oplus \mathbf{F}_3$ by Theorem 1.2.5 (3). Since $\lambda' = 2$ in this case, by Corollary 5.2.4 we know that the main conjecture holds.

Since $L(E,1) = 0$, we know $\mathrm{rank}\,\mathrm{Sel}(E/\mathbf{Q}, E[3^\infty])^\vee > 0$ by the main conjecture. This implies that

$$\mathrm{Sel}(E/\mathbf{Q}, E[3^\infty])^\vee \simeq \mathbf{Z}_3 \oplus \mathbf{Z}_3.$$

Now E has a minimal Weierstrass model $y^2 + y = x^3 - x^2 - 725658x - 430708782$. We can find rational points $P = (2403, 108146)$ and $Q = (5901, -448036)$ on this curve. We can also easily check that $E(\mathbf{F}_7)$ is cyclic group of order 6 and $E(\mathbf{F}_{31})$ is cyclic of order 39. The image of P in $E(\mathbf{F}_7)/3E(\mathbf{F}_7) \simeq \mathbf{Z}/3\mathbf{Z}$ is 0 (the identity element), and the image of

Q in $E(\mathbf{F}_7)/3E(\mathbf{F}_7) \simeq \mathbf{Z}/3\mathbf{Z}$ is of order 3. On the other hand, the images of P and Q in $E(\mathbf{F}_{31})/3E(\mathbf{F}_{31}) \simeq \mathbf{Z}/3\mathbf{Z}$ do not vanish and coincide. This shows that P and Q are linearly independent over $\mathbf{Z}_3$. Therefore,

$$\operatorname{rank} E(\mathbf{Q}) = 2 \text{ and } \text{Ш}(E/\mathbf{Q})[3^\infty] = 0.$$

In the above argument we considered the images of $E(\mathbf{Q})$ in $E(\mathbf{F}_7)/3E(\mathbf{F}_7)$ and $E(\mathbf{F}_{31})/3E(\mathbf{F}_{31})$. What we explained above implies that the natural map $s_{7\times 31} : E(\mathbf{Q})/3E(\mathbf{Q}) \longrightarrow E(\mathbf{F}_7)/3E(\mathbf{F}_7) \oplus E(\mathbf{F}_{31})/3E(\mathbf{F}_{31})$ is bijective. In this example, $\tilde{\delta}_{7\times 31} = -15290 \not\equiv 0 \pmod 3$, so Conjecture 1.2.4 holds for $m = 7 \times 31$.

(5) $d = 853$. We know $\epsilon = (\frac{853}{11}) = -1$. Take $N = 1$ at first. For $\ell = 271$, we have $a_3^{(271)} = 900852395/2 \not\equiv 0 \pmod 3$, which implies that $\dim_{\mathbf{F}_3} \mathrm{Sel}(E/\mathbf{Q}, E[3]) \leq 3$. We compute $\mathcal{P}_1 = \{7, 13, 67, 103, 109, ..., 463, ...\}$. We can find a rational point $P = (1194979057/51984, 40988136480065/11852352)$ on the minimal Weierstrass equation $y^2+y = x^3-x^2-7518626x-14370149745$ of $E = X_0(11)^{(853)}$. We know that $E(\mathbf{F}_7)$ is cyclic of order 6, and $E(\mathbf{F}_{13})$ is cyclic of order 18. Both of the images of P in $E(\mathbf{F}_7)/3E(\mathbf{F}_7)$ and $E(\mathbf{F}_{13})/3E(\mathbf{F}_{13})$ are of order 3. Therefore, $s_\ell : \mathrm{Sel}(E/\mathbf{Q}, E[3]) \longrightarrow E(\mathbf{F}_\ell)/3E(\mathbf{F}_\ell)$ is surjective for each $\ell = 7,\ 13$. Since $13 = -1 \in (\mathbf{F}_7^\times)^3$, $463 = 1 \in (\mathbf{F}_7^\times)^3$ and $463 = 8 \in (\mathbf{F}_{13}^\times)^3$, $\{7, 13, 463\}$ is admissible. We can compute $\tilde{\delta}_{7\times 13\times 463} = -8676400 \not\equiv 0 \pmod 3$, and can check that $m = 7 \times 13 \times 463$ is δ-minimal. By Theorem 1.2.5 (4), we have

$$\mathrm{Sel}(E/\mathbf{Q}, E[3]) \simeq \mathbf{F}_3 \oplus \mathbf{F}_3 \oplus \mathbf{F}_3. \tag{5.4}$$

We have a rational point P of infinite order, so the rank of $E(\mathbf{Q})$ is ≥ 1. Take $N = 3$ and consider $\ell = 271$. Since $\tilde{\delta}_{271} = a_1^{(271)} = 35325 \equiv 9 \pmod{27}$, 9 is in $\mathrm{Fitt}_{1,\mathbf{Z}/p^3\mathbf{Z}}(\mathrm{Sel}(E/\mathbf{Q}, E[3^3])^\vee)$ by Corollary 2.4.2. This implies that $\operatorname{rank} E(\mathbf{Q}) = 1$ and $\#\text{Ш}(E/\mathbf{Q})[3^\infty] \leq 9$. This together with (5.4) implies that

$$\text{Ш}(E/\mathbf{Q})[3^\infty] \simeq \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}. \tag{5.5}$$

Note that if we used only Theorem 1.1.1 and these computations, we could not get (5.4) nor (5.5) because we could not determine $\Theta_1(\mathbf{Q})^{(\delta)}$ by finite numbers of computations. We need Theorem 1.2.5 to obtain (5.4) and (5.5).

(6) For positive integers d which are conductors of even Dirichlet characters (so $d = 4m$ or $d = 4m + 1$ for some m) satisfying $1 \leq d \leq 1000$, $d \equiv 1 \pmod 3$, and $d \not\equiv 0 \pmod{11}$, we computed $\mathrm{Sel}(E/\mathbf{Q}, E[3])$. Then

$\dim \mathrm{Sel}(E/\mathbf{Q}, E[3]) = 0, 1, 2, 3$, and the case of dimension $= 3$ occurs only for $d = 853$ in Example (5).

(7) We also considered negative twists. Take $d = -2963$. In this case, we know $L(E, 1) \neq 0$ and $L(E, 1)/\Omega_E^+ = 81$. We know from the main conjecture that the order of the 3-component of $\text{Ш}(E/\mathbf{Q})$ is 81, but *the main conjecture does not tell the structure of this group.* Take $N = 1$ and $\ell = 19$. Then we compute $a_2^{(19)} = 2753/2 \not\equiv 0 \pmod 3$ (we have $\vartheta_{\mathbf{Q}(19)} \equiv -432S + (2753/2)S^2 \bmod (9, S^3)$). Since $c_2 = 1$, this shows that $a_2^{(19)}$ is in $\mathrm{Fitt}_{2,\mathbf{F}_3}(\mathrm{Sel}(E/\mathbf{Q}, E[3])^\vee)$ by Theorem 2.4.1. Therefore, we have $\mathrm{Fitt}_{2,\mathbf{F}_3}(\mathrm{Sel}(E/\mathbf{Q}, E[3])) = \mathbf{F}_3$, which implies that $\mathrm{Sel}(E/\mathbf{Q}, E[3]) \simeq (\mathbf{F}_3)^{\oplus 2}$. This denies the possibility of $\text{Ш}(E/\mathbf{Q})[3^\infty] \simeq (\mathbf{Z}/3\mathbf{Z})^{\oplus 4}$, and we have

$$\text{Ш}(E/\mathbf{Q})[3^\infty] \simeq \mathbf{Z}/9\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z}.$$

(8) Let E be the curve $y^2 + xy + y = x^3 + x^2 - 15x + 16$ which is 563A1 in Cremona's book [1]. We take $p = 3$. Since $a_3 = -1$, $\mathrm{Tam}(E) = 1$, $\mu = 0$ and the Galois representation on $T_3(E)$ is surjective, all the conditions we assumed are satisfied. We know $\epsilon = 1$ and $L(E, 1) = 0$. Take $N = 1$. We compute $\mathcal{P}_1 = \{13, 61, 103, 109, 127, 139, ...\}$. For admissible pairs $\{13, 103\}$, $\{13, 109\}$, we compute $\tilde{\delta}_{13\times103} = -6819 \equiv 0 \pmod 3$ and $\tilde{\delta}_{13\times109} = -242 \not\equiv 0 \pmod 3$. From the latter, we know that

$$s_{13\times109} : \mathrm{Sel}(E/\mathbf{Q}, E[3]) \xrightarrow{\simeq} (\mathbf{F}_3)^{\oplus 2}$$

is bijective by Theorem 1.2.5 (3). Since $\lambda' = 2$, the main conjecture also holds by Corollary 5.2.4. We know $L(E, 1) = 0$, so $\mathrm{Sel}(E/\mathbf{Q}, E[3^\infty]) \simeq (\mathbf{Z}_3)^{\oplus 2}$.

Numerically, we can find rational points $P = (2, -2)$ and $Q = (-4, 7)$ on this elliptic curve. We can check that $E(\mathbf{F}_{13})$ is cyclic of order 12, $E(\mathbf{F}_{103})$ is cyclic of order 84, and $E(\mathbf{F}_{109})$ is cyclic of order 102. The points P and Q have the same image and do not vanish in $E(\mathbf{F}_{13})/3E(\mathbf{F}_{13})$, but the image of P in $E(\mathbf{F}_{109})/3E(\mathbf{F}_{109})$ is zero, and the image of Q in $E(\mathbf{F}_{109})/3E(\mathbf{F}_{109})$ is non-zero. This shows that P and Q are linearly independent over $\mathbf{Z}_3$, and $s_{13\times109}$ is certainly bijective. Since all the elements in $\mathrm{Sel}(E/\mathbf{Q}, E[3^\infty])$ come from the points, we have $\text{Ш}(E/\mathbf{Q})[3^\infty] = 0$. On the other hand, the image of P in $E(\mathbf{F}_{103})/3E(\mathbf{F}_{103})$ coincides with the image of Q, so $s_{13\times103}$ is not bijective. This is an example for which $\tilde{\delta}_{13\times103} \equiv 0 \pmod 3$ and $s_{13\times103}$ is not bijective.

(9) Let E be the elliptic curve $y^2 + xy + y = x^3 + x^2 - 10x + 6$ which has conductor 18097. We take $p = 3$. We know $a_3 = -1$, $\mathrm{Tam}(E) = 1$, $\mu = 0$

and the Galois representation on $T_3(E)$ is surjective, so all the conditions we assumed are satisfied. In this case, $\epsilon = -1$ and $L(E,1) = 0$. Take $N = 1$. We compute $\mathcal{P}_1 = \{7, 19, 31, 43, 79, ..., 601, ...\}$. We know $\{7, 43, 601\}$ is admissible. We have $\tilde{\delta}_{7\times 43\times 601} = -2424748 \not\equiv 0 \pmod 3$, and $7 \times 43 \times 601$ is δ-minimal. We thank K. Matsuno heartily for his computing this value for us. The group $E(\mathbf{F}_7)$ is cyclic of order 9 and $E(\mathbf{F}_{43})$ is cyclic of order 42. The point $(0,2)$ is on this elliptic curve, and has non-zero image both in $E(\mathbf{F}_7)/3E(\mathbf{F}_7)$ and $E(\mathbf{F}_{43})/3E(\mathbf{F}_{43})$. So both s_7 and s_{43} are surjective, and we can apply Theorem 1.2.5 (4) to get

$$s_{7\times 43\times 601} : \mathrm{Sel}(E/\mathbf{Q}, E[3]) \xrightarrow{\simeq} (\mathbf{F}_3)^{\oplus 3}$$

is bijective.

Numerically, we can find 3 rational points $P = (0,2)$, $Q = (2,-1)$, $R = (3,2)$ on this elliptic curve, and easily check that the restriction of $s_{7\times 43\times 601}$ to the subgroup generated by P, Q, R in $\mathrm{Sel}(E/\mathbf{Q}, E[3])$ is surjective. Therefore, we have checked numerically that $s_{7\times 43\times 601}$ is bijective. This also implies that $\mathrm{rank}\, E(\mathbf{Q}) = 3$ since $E(\mathbf{Q})_{\mathrm{tors}} = 0$. Therefore, all the elements of $\mathrm{Sel}(E/\mathbf{Q}, E[3^\infty])$ come from the rational points, and we have $\text{Ш}(E/\mathbf{Q})[3^\infty] = 0$.

5.4 A Remark on ideal class groups

We consider the classical Stickelberger element

$$\tilde{\theta}^{St}_{\mathbf{Q}(\mu_m)} = \sum_{\substack{a=1 \\ (a,m)=1}}^{m} \left(\frac{1}{2} - \frac{a}{m}\right)\sigma_a^{-1} \in \mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q})]$$

(cf. (1.1)). Let $K = \mathbf{Q}(\sqrt{-d})$ be an imaginary quadratic field with conductor d, and χ be the corresponding quadratic character. Let m be a squarefree product whose prime divisors ℓ split in K and satisfy $\ell \equiv 1 \pmod p$. Using the above classical Stickelberger element, we define $\tilde{\delta}^{St}_{m,K}$ by

$$\tilde{\delta}^{St}_{m,K} = -\sum_{\substack{a=1 \\ (a,md)=1}}^{md} \frac{a}{md}\chi(a)\left(\prod_{\ell | m} \log_{\mathbf{F}_\ell}(a)\right)$$

(cf. (1.2)). We denote by Cl_K the class group of K, and define the notion "δ^{St}_K-minimalness" analogously. We consider the analogue of Conjecture 1.2.4 for $\tilde{\delta}^{St}_{m,K}$ and $\dim_{\mathbf{F}_p}(Cl_K/p)$. Namely, we ask whether $\dim_{\mathbf{F}_p}(Cl_K/p) = \epsilon(m)$ for a δ^{St}_K-minimal m. Then the analogue does not hold. For example, take $K = \mathbf{Q}(\sqrt{-23})$ and $p = 3$. We know $Cl_K \simeq \mathbf{Z}/3\mathbf{Z}$. Put $\ell_1 = 151$

and $\ell_2 = 211$. We compute $\tilde{\delta}^{St}_{\ell_1,K} = -270 \equiv 0 \pmod 3$, $\tilde{\delta}^{St}_{\ell_2,K} = -1272 \equiv 0 \pmod 3$, and $\tilde{\delta}^{St}_{\ell_1 \cdot \ell_2,K} = -415012 \equiv 2 \pmod 3$. This means that $\ell_1 \cdot \ell_2$ is δ^{St}_K-minimal. But, of course, we know $\dim_{\mathbf{F}_p}(Cl_K/p) = 1 < 2 = \epsilon(\ell_1 \cdot \ell_2)$.

References

[1] Cremona, J.E., *Algorithms for modular elliptic curves*, Cambridge University Press, 1992.

[2] Greenberg, R., Iwasawa theory for p-adic representations, in *Algebraic Number Theory – in honor of K. Iwasawa*, Advanced Studies in Pure Math 17 (1989), 97-137.

[3] Greenberg, R., Iwasawa theory for elliptic curves, in *Arithmetic theory of elliptic curves*, Cetraro, Italy 1997, Springer Lecture Notes in Math 1716 (1999), 51-144.

[4] Greenberg, R., *Iwasawa theory, projective modules, and modular representation*, Memoirs of the AMS Number 992 (2011).

[5] Greither, C., Computing Fitting ideals of Iwasawa modules, Math. Zeitschrift 246 (2004), 733-767.

[6] Hachimori, Y. and Matsuno K., An analogue of Kida's formula for the Selmer groups of elliptic curves, J. Algebraic Geometry 8 (1999), 581-601.

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

[8] Kolyvagin, V.A., Euler systems, The Grothendieck Festschrift Vol II (1990), 435-483.

[9] Kurihara, M., Iwasawa theory and Fitting ideals, J. reine angew. Math. 561 (2003), 39-86.

[10] Kurihara, M., On the structure of ideal class groups of CM-fields, Documenta Mathematica, Extra Volume Kato (2003), 539-563.

[11] Kurihara, M., Refined Iwasawa theory and Kolyvagin systems of Gauss sum type, Proceedings of the London Mathematical Society 104 (2012), 728-769.

[12] Kurihara, M., Refined Iwasawa theory for p-adic representations and the structure of Selmer groups, to appear in Münster Journal of Mathematics http://www.math.keio.ac.jp/ kurihara/

[13] Matsuno K., An analogue of Kida's formula for the p-adic L-functions of modular elliptic curves, J. Number Theory 84 (2000), 80-92.

[14] Mazur, B. and Rubin, K, *Kolyvagin systems*, Memoirs of the AMS Vol 168, Number 799 (2004).

[15] Mazur, B. and Rubin, K, Organizing the arithmetic of elliptic curves, Advances in Mathematics 198 (2005), 504-546.

[16] Mazur, B. and Tate J., Refined conjectures of the "Birch and Swinnerton-Dyer type", Duke Math. J. 54 (1987), 711-750.

[17] Nekovář, J., On the parity of ranks of Selmer groups. II, C. R. Acad. Sci. Paris Sér. I Math. 332 (2001), 99-104.

[18] Nekovář, J., *Selmer complexes*, Astérisque No. 310 (2006).

[19] Northcott, D. G., *Finite free resolutions*, Cambridge Univ. Press (1976).

[20] Popescu, C. D., On the Coates-Sinnott conjecture, Mathematische Nachrichten 282 (2009), 1370-1390.

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

[22] Rubin, K., Kolyvagin's system of Gauss sums, *Arithmetic Algebraic Geometry*, G. van der Geer et al eds, Progress in Math 89 (1991) 309-324.

[23] Rubin, K., *Euler systems*, Annals of Math. Studies 147, Princeton Univ. Press 2000.

[24] Schneider, P., Iwasawa L-functions of varieties over algebraic number fields, A first approach, Invent. math. 71 (1983), 251-293.

[25] Serre, J.-P., *Corps Locaux*, Hermann, Paris 1968 (troisième édition).

[26] Skinner, C. and Urban, E., The Iwasawa main conjecture for GL_2, Invent. math. 195 (2014), 1-277.

[27] Stevens, G., Stickelberger elements and modular parametrizations of elliptic curves, Invent math 98 (1989), 75-106.

Masato Kurihara
Department of Mathematics,
Keio University,
3-14-1 Hiyoshi, Kohoku-ku,
Yokohama, 223-8522, Japan
kurihara@math.keio.ac.jp