Title	Indivisibility of Kato's Euler systems and Kurihara numbers (Algebraic Number Theory and Related Topics 2018)
Author(s)	Kim, Chan-Ho; Ghitza, Alexandru
Citation	数理解析研究所講究録別冊 (2021), B86: 63-86
Issue Date	2021-07
URL	http://hdl.handle.net/2433/265150
Right	© 2021 by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University. All rights reserved.
Type	Departmental Bulletin Paper
Textversion	publisher

RIMS Kôkyûroku Bessatsu
B86 (2021), 063–086

Indivisibility of Kato's Euler systems and Kurihara numbers

By

Chan-Ho Kim*
with an appendix by Alexandru Ghitza**

Abstract

In this survey article, we discuss our recent work [KKS20], [KN20] on the numerical verification of the Iwasawa main conjecture for modular forms of weight two at good primes and elliptic curves with potentially good reduction. The criterion is based on the Euler system method and the equality of the main conjecture can be checked via the non-vanishing of Kurihara numbers. We also discuss further arithmetic applications of Kurihara numbers to study the structure of Selmer groups following the philosophy of refined Iwasawa theory à la Kurihara. In the appendix by Alexandru Ghitza, the SageMath code for an effective computation of Kurihara numbers is illustrated.

§ 1. Overview

The main goal of my talk at RIMS was to explain the following rough statement (motto?) in detail.

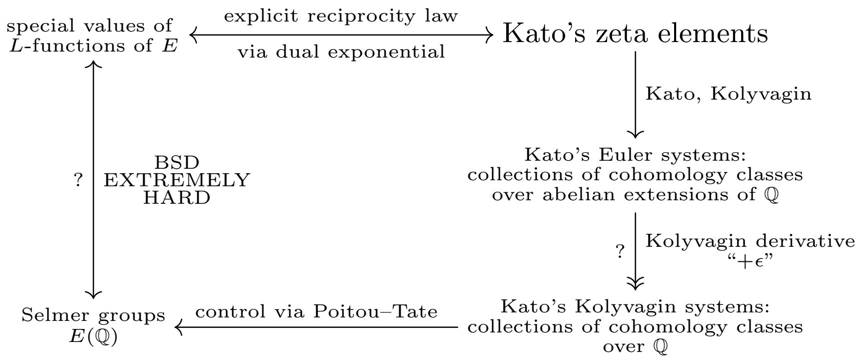
> The Iwasawa main conjecture for modular forms of weight two over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ can be numerically checked, for example, via SAGE (even when the work of Skinner–Urban [SU14] does not apply).

Received March 28, 2019. Revised September 4, 2020.
2020 Mathematics Subject Classification(s): 11F67; 11G05; 11R23
Key Words: *elliptic curves, Euler systems, Iwasawa main conjectures, Kato's Euler systems, Kurihara numbers, modular forms, modular symbols*
Chan-Ho Kim is partially supported by a KIAS Individual Grant (SP054102) via the Center for Mathematical Challenges at Korea Institute for Advanced Study, by Basic Science Research Program through the National Research Foundation of Korea (NRF-2018R1C1B6007009), and by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.
*Korea Institute for Advanced Study (KIAS), 85 Hoegiro, Dongdaemun-gu, Seoul 02455, Republic of Korea.
e-mail: `chanho.math@gmail.com`
**School of Mathematics and Statistics, University of Melbourne, Parkville VIC 3010, Australia.
e-mail: `aghitza@alum.mit.edu`

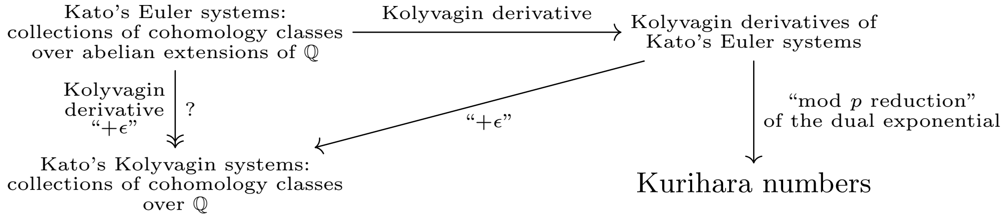
Our approach is purely based on the theory of Euler and Kolyvagin systems [Rub00], [MR04] arising from Kato's zeta elements [Kat04].

The very starting point of this work would be the following fundamental picture à la Mazur (for an elliptic curve E over $\mathbb{Q}$ in this overview)[1].

(1.1)



In the philosophy of special values of L-functions, the L-values and the size of Selmer groups are intimately related, and it is explicitly and precisely realized as the Birch and Swinnerton-Dyer conjecture for elliptic curves and the Bloch–Kato conjecture for more general motives. One way to attack these conjectures is to use Euler systems. In the case of elliptic curves and modular forms, Kato's zeta elements arising from Siegel units play the central role. Usually, the theory of Euler systems yields an upper bound of Selmer groups (if the Euler system is non-torsion) following the above picture. The main reason we only get an upper bound is that it is unclear whether the Kolyvagin derivative process is "surjective" or not. Such a surjectivity can be recognized as the p-indivisibility of derived Euler systems. In the anticyclotomic case, Kolyvagin conjectured the p-indivisibility of derived Heegner points and deduced the exact bound and the structure of the Selmer group of an elliptic curve over an imaginary quadratic field satisfying the Heegner condition from the indivisibility conjecture in [Kol91]. Kolyvagin's conjecture is proved by Wei Zhang [Zha14] *using* the relevant main conjecture (for the case violating the Heegner condition). In the cyclotomic case, we refine the lower-right part of the picture of Mazur as follows.



In the language of Kolyvagin systems à la Mazur–Rubin [MR04], the indivisibility of derived Euler systems is formulated as the primitivity of the corresponding Kolyvagin

[1] I remember I saw the picture from the video-recorded lecture of Mazur on *the mechanism of Kolyvagin systems* at École d'été sur la conjecture de Birch et Swinnerton-Dyer, 2002, France.

systems. If we understand the meaning of the "mod p reduction" of the dual exponential map in the *correct* way, then the primitivity can be checked by nonvanishing of Kurihara numbers. In order to define a suitable mod p reduction of the dual exponential map, we compute the image of an *integral* local Galois cohomology under the dual exponential map. In the weight two case, such a computation can be done by using the Tate local duality and the geometry of modular abelian varieties.

It is not the end of the story of Kurihara numbers. In fact, the notion of Kurihara numbers is observed by Kurihara in the completely different context, *refined Iwasawa theory*. We will explain the applications of (generalized) Kurihara numbers to refined Iwasawa theory at the end.

In §2, we review various Iwasawa main conjectures, modular symbols and p-adic L-functions, and the known results on the Iwasawa main conjectures. In §3, we state the main results of [KKS20] and [KN20]. In §4, we discuss the main idea of the proof and possible generalizations. In §5, following Kurihara's idea, we discuss Kolyvagin systems of Gauss sum type and refined Iwasawa theory emphasizing how Kurihara numbers are used. In Appendix A by Alexandru Ghitza, an effective computation of Kurihara numbers is illustrated.

Part I
Iwasawa main conjectures

§ 2. Review of Iwasawa main conjectures

§ 2.1. The formulation of Iwasawa main conjectures

Let p be an odd prime, $f = \sum_{n \geq 1} a_n(f)q^n \in S_2(\Gamma_1(N), \psi)$ a normalized new cuspidal eigenform, and $\mathbb{Q}_f$ the field generated by the Hecke eigenvalues of f over $\mathbb{Q}$.

Assumption 2.1. Throughout this article, we assume that one of the following conditions:

1. p does not divide N, or
2. p^2 divides N, $p > 7$, $\psi = \mathbf{1}$ (the trivial character), and $\mathbb{Q}_f = \mathbb{Q}$.

We fix embeddings $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Then we denote the completion of $\mathbb{Q}_f$ at the prime π induced from ι_p by $\mathbb{Q}_{f,\pi}$. The ring of integers of $\mathbb{Q}_{f,\pi}$ is denote by $\mathbb{Z}_{f,\pi}$ and $\mathbb{F}_\pi := \mathbb{Z}_{f,\pi}/\pi\mathbb{Z}_{f,\pi}$.

For any field F, denote by G_F the absolute Galois group of F. Let $\rho_f : G_\mathbb{Q} \to \mathrm{Aut}_{\mathbb{Q}_{f,\pi}}(V_f) \simeq \mathrm{GL}_2(\mathbb{Q}_{f,\pi})$ be the π-adic Galois representation attached to f in the sense of Deligne (i.e. the cohomological convention). See [Kat04, §14.10] for the normalization. Let T_f be a Galois stable $\mathbb{Z}_{f,\pi}$-lattice in V_f and denote by $\overline{\rho}$ the residual representation of ρ_f over $\mathbb{F}$ and by $N(\overline{\rho})$ the (prime-to-p) conductor of $\overline{\rho}$. Let $A_f := V_f/T_f$ be the associated discrete Galois module. Let $\overline{f} = \sum_{n\geq 1} \overline{a_n(f)} q^n$ be the dual modular form to f where $\overline{a_n(f)}$ is the complex conjugate of $a_n(f)$. The corresponding Galois representation and the lattice are denoted by $V_{\overline{f}}$ and $T_{\overline{f}}$.

Assumption 2.2. The image of $\overline{\rho}$ contains a conjugate of $\mathrm{SL}_2(\mathbb{F}_p)$.

Under Assumption 2.2, the choice of T_f does not affect any result in this paper.

Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and $\mathbb{Q}_n$ the cyclic subextension of degree p^n of $\mathbb{Q}$ in $\mathbb{Q}_\infty$. Let $\Lambda = \mathbb{Z}_{f,\pi}[\![\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]\!]$ be the Iwasawa algebra. Let $j : \mathrm{Spec}(\mathbb{Q}_n) \to \mathrm{Spec}(\mathcal{O}_{\mathbb{Q}_n}[1/p])$ be the natural map. We define the **global Iwasawa cohomology groups** by

$$\mathbb{H}^i := \varprojlim_n \mathrm{H}^i_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_{\mathbb{Q}_n}[1/p]), j_* T_{\overline{f}}(1))$$

for $i \geq 0$.

Theorem 2.3 (Kato). *Under Assumption 2.2, the following statements hold.*

1. *$\mathbb{H}^2$ is a finitely generated torsion Λ-module.*
2. *$\mathbb{H}^1$ is free of rank one over Λ.*

Let Σ be a finite set of places of $\mathbb{Q}$ containing the places dividing $Np\infty$ and $\mathbb{Q}_\Sigma$ be the maximal extension of $\mathbb{Q}$ unramified outside Σ. Then ρ_f factors through $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$. It is well known that $\mathbb{H}^1 \simeq \varprojlim_n \mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T_{\overline{f}}(1))$. See [Kur02, §6] and [Kob03, Proposition 7.1.(i)] for detail.

We recall various Iwasawa main conjectures for $A_f(1)$ over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Conjecture 2.4 (Kato's IMC without p-adic L-functions). *Let $\mathbf{z}_{\mathrm{Kato}} \in \mathbb{H}^1$ be Kato's zeta element. Then*

$$\mathrm{char}_\Lambda \left(\mathbb{H}^1/\Lambda \mathbf{z}_{\mathrm{Kato}}\right) \overset{?}{=} \mathrm{char}_\Lambda \left(\mathbb{H}^2\right).$$

It seems that the following form of the main conjecture is most famous and explicitly shows the connection between the analytic information ("the package of the congruences among twisted L-values" via p-adic L-functions) and the arithmetic information ("the growth behavior of arithmetic invariants" via the characteristic ideals of dual Selmer groups over the Iwasawa algebra) of given (automorphic) motives.

In the good ordinary case, i.e. $a_p(f)$ is a π-adic unit, f admits a unit root α of the Hecke polynomial $X^2 - a_p(f)X + \psi(p)p$. Denote by f_α the p-stabilization of f with U_p-eigenvalue α. Let $L_p(\mathbb{Q}_\infty, f_\alpha)$ be the p-adic L-function associated to f_α à la Mazur–Tate–Teitelbaum defined in (2.2). Under the good ordinary condition and Assumption 2.2, it is known that $L_p(\mathbb{Q}_\infty, f_\alpha) \in \Lambda$.

Conjecture 2.5 (**Mazur's IMC**). *Suppose that f is good ordinary at p. Then* $\mathrm{Sel}(\mathbb{Q}_\infty, A_f(1))$ *is Λ-cotorsion and*

$$(L_p(\mathbb{Q}_\infty, f_\alpha)) \overset{?}{=} \mathrm{char}_\Lambda \left(\mathrm{Sel}(\mathbb{Q}_\infty, A_f(1))^\vee\right)$$

as ideals of Λ.

When p divides $a_p(f)$, the situation becomes more complicated; for examples, the Selmer group is never Λ-cotorsion and the p-adic L-function is p-adically unbounded. When $a_p(f) = 0$, Kobayashi [Kob03] and Pollack [Pol03] formulated $\pm$-Selmer groups and $\pm$-p-adic L-functions, which behave well in the standard framework of Iwasawa theory.

Conjecture 2.6 (**Kobayashi's $\pm$-IMC**). *Suppose that $a_p(f) = 0$ and $\psi = \mathbf{1}$. Then*

$$\left(L^{\mp}_p(\mathbb{Q}_\infty, f)\right) \overset{?}{=} \mathrm{char}_\Lambda \left(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, A_f(1))^\vee\right)$$

as ideals of Λ.

There is also the $\sharp/\flat$-variant of Kobayashi-Pollack's $\pm$-Iwasawa theory for the case $p \mid a_p(f)$ and $a_p(f) \neq 0$ by Sprung [Spr12].

It is known that these main conjectures are equivalent under the relevant setting.

Theorem 2.7 (**[Kat04, §17.13], [Kob03, Theorem 7.4]**).

1. *If $a_p(f)$ is a π-adic unit, then Conjecture 2.4 is equivalent to Conjecture 2.5.*
2. *If $a_p(f) = 0$ and $\psi = \mathbf{1}$, then Conjecture 2.4 is equivalent to Conjecture 2.6.*

§ 2.2. Modular symbols, Mazur–Tate elements, and p-adic L-functions

In the case of elliptic curves, we always assume that a given elliptic curve is the strong Weil curve and the Manin constant is prime to p.

For $\frac{a}{n} \in \mathbb{Q}$, we define

$$\left[\frac{a}{n}\right]^+_f := \frac{1}{2 \cdot \Omega^+_f} \left(\int_{i\infty}^{a/n} f(z)dz + \int_{i\infty}^{-a/n} f(z)dz \right) \in \mathbb{Z}_{f,\pi}$$

where Ω^+_f is an integral canonical period of f if $p \nmid N$, or the real period of E (elaborated in the remark below) if f corresponds to an elliptic curve E and $p^2 \mid N$.

Note that the existence of integral canonical periods follows from Assumption 2.2.

Remark. Let $E_{\mathbb{Z}}$ be the (global) minimal Weierstrass model of E given by a minimal affine equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in \mathbb{Z}$. We define

$$\omega_E := \frac{dx}{2y + a_1x + a_3}.$$

Then $\pi^*(\omega_E) = c \cdot f(z)dz$ where $\pi : X_0(N) \to E$ is the optimal parametrization, c is the Manin constant for π, and f is the normalized newform corresponding to E. Let $\mathrm{H}^1(E(\mathbb{C}), \mathbb{Z})^{\pm}$ be the subspace of $\mathrm{H}^1(E(\mathbb{C}), \mathbb{Z})$ where the complex conjugation acts by ± 1, and $\delta^{\pm} \in H^1(E(\mathbb{C}), \mathbb{Z})^{\pm}$ its generator, respectively. Then the real and imaginary periods of E are defined by

$$\Omega^{\pm}_f := \Omega^{\pm}_E = a \cdot \int_{\delta^{\pm}} \omega_E \tag{2.1}$$

where $a = 1$ if $E(\mathbb{R})$ is connected and $a = 2$ otherwise. The integrality of the modular symbols normalized by (2.1) comes from the irreducibility of $E[p]$ and the assumption $(c, p) = 1$ on the Manin constant c (cf. [Pol03, Remark 5.4]).

The mod p reduction of $\left[\frac{a}{n}\right]^+_f$ is denoted by $\overline{\left[\frac{a}{n}\right]^+_f} \in \mathbb{F}_\pi$. Following [Kur14b, §1.1], we define **Mazur–Tate element at** $\mathbb{Q}(\mu_n)$ by

$$\widetilde{\theta}_{\mathbb{Q}(\mu_n)} := \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \left[\frac{a}{n}\right]^+_f \cdot \sigma_a \in \mathbb{Z}_{f,\pi}[\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})],$$

and, for general $K \subseteq \mathbb{Q}(\mu_n)$, following Kurihara, $\widetilde{\theta}_K$ is defined by the image of $\widetilde{\theta}_{\mathbb{Q}(\mu_n)}$ in $\mathbb{Z}_{f,\pi}[\mathrm{Gal}(K/\mathbb{Q})]$ under the natural projection. See [Kur02, §1], [Kur14b, §2.1] for details.

Now we assume that $a_p(f)$ is a π-adic unit and $(n, p) = 1$. Following [Kur14b, §2.3], we define the p**-stabilized Mazur–Tate element** by

$$\vartheta_{\mathbb{Q}(\mu_n)} := (1 - \frac{\sigma_p}{\alpha})(1 - \frac{\sigma_p^{-1}}{\alpha})\widetilde{\theta}_{\mathbb{Q}(\mu_n)}, \qquad \vartheta_{\mathbb{Q}(\mu_{np^r})} := \tfrac{1}{\alpha^r} \cdot \left(\widetilde{\theta}_{\mathbb{Q}(\mu_{np^r})} - \tfrac{1}{\alpha} \cdot \nu \left(\widetilde{\theta}_{\mathbb{Q}(\mu_{np^{r-1}})}\right)\right)$$

for $r \geq 2$ where $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ corresponds to $p \in (\mathbb{Z}/n\mathbb{Z})^\times$ and ν is the norm map. For general $K \subseteq \mathbb{Q}(\mu_{np^r})$, Kurihara defines ϑ_K by the natural image of $\vartheta_{\mathbb{Q}(\mu_{np^r})}$

in $\mathbb{Z}_{f,\pi}[\mathrm{Gal}(K/\mathbb{Q})]$. Then the sequence $(\vartheta_{\mathbb{Q}_r})_r$ forms a projective system and the limit defines the **p-adic L-function**

$$L_p(\mathbb{Q}_\infty, f_\alpha) := \varprojlim_r \vartheta_{\mathbb{Q}_r} \in \Lambda. \tag{2.2}$$

§ 2.3. Former results

Without a doubt, the following result of Kato using his Euler systems is the most important to us and this is the statement we want to *optimize*.

Theorem 2.8 (Kato [Kat04]). *Suppose that Assumption 2.2 holds. Then*

$$\mathrm{char}_\Lambda \left(\mathbb{H}^1/\Lambda \mathbf{z}_{\mathrm{Kato}}\right) \subseteq \mathrm{char}_\Lambda \left(\mathbb{H}^2\right).$$

Concerning the other inclusion of the main conjecture, the following results are proved by completely different methods. We do not specify the precise conditions here.

Theorem 2.9 (Skinner–Urban [SU14], X. Wan [Wan15]). *Suppose that Assumption 2.2 holds and $\psi = \mathbf{1}$. Assume that f is good ordinary at p.*

1. *(Skinner–Urban) If there exists a prime ℓ such that ℓ exactly divides $N(\overline{\rho})$, then Conjecture 2.5 holds.*
2. *(X. Wan) If a real quadratic field with certain properties exists, then Conjecture 2.5 holds.*

Recently, there have been a lot of progresses towards the non-ordinary case. However, these results are not fully refereed yet.

Remark. Suppose that Assumption 2.2 holds and $\psi = \mathbf{1}$.

1. (X. Wan [Wanb]) If f corresponds to an elliptic curve of square-free conductor and $a_p(f) = 0$, then Conjecture 2.6 holds.
2. (Sprung [Spr]) If f corresponds to an elliptic curve of square-free conductor and p divides $a_p(f)$, then Conjecture 2.4 holds via the $\sharp/\flat$-Iwasawa theory.
3. (X. Wan [Wana]) If $a_p(f)$ is divisible by π and the level satisfies a certain assumption, then Conjecture 2.4 holds.
4. (Castella–Çiperiani–Skinner–Sprung [CÇSS]) If $a_p(f)$ is divisible by π and the level is square-free, then Conjecture 2.4 holds.

§ 3. The statement of the main theorem

§ 3.1. Motivational examples

Question 3.1. Regarding the results on the equality of the main conjectures in §2.3, we may ask the following questions.

1. How to remove the assumptions on the level?
2. How to deal with the ordinary and non-ordinary cases on equal footing like Theorem 2.8?
3. How about even more general reduction types?

We briefly recall the notion of Iwasawa invariants. Any finitely generated torsion Λ-module M is pseudo-isomorphic to

$$\bigoplus_i \Lambda/\pi^{\mu_i} \oplus \bigoplus_j \Lambda/f_j^{a_j}$$

where f_j is a distinguished polynomial in $\Lambda \simeq \mathbb{Z}_{f,\pi}[\![X]\!]$. Then $\mu(M) := \sum_i \mu_i$ and $\lambda(M) := \sum_j \deg(f) \cdot a_j$. For $f \in \Lambda$, we define $\mu(f) := \mu(\Lambda/f)$ and $\lambda(f) := \lambda(\Lambda/f)$.

We recall two examples from [KKS20] and [KN20].

Example 3.2 (Elliptic curve of full-square conductor, [KKS20, §8]). Let $p = 7$ and E_1 the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = x^3 - 4062871x - 3152083138.$$

Then we have $N_1 = 3364 = 2^2 \cdot 29^2$, $7 \nmid a_7(E_1)$, $a_7(E_1) \not\equiv 1 \pmod{p}$, and $E_1[p]$ is a surjective Galois representaion. Also, we have $\mathrm{Tam}(E_1) = 1$, $\mu(L_p(\mathbb{Q}_\infty, E_1)) = 0$, $\lambda(L_p(\mathbb{Q}_\infty, E_1) = \lambda_{\mathrm{III}}(L_p(\mathbb{Q}_\infty, E_1) = 2$. Here, $\lambda_{\mathrm{III}}(L_p(\mathbb{Q}_\infty, E_1)$ is the number of zeros of $L_p(\mathbb{Q}_\infty, E_1)$ *not* of the form $\zeta_{p^n} - 1$ for any n. See [Pol03, §6.1] for detail. Since the conductor is a full-square, [SU14] does not apply.

Example 3.3 (Elliptic curve with additive reduction, [KN20, §5]). Let $p = 11$ and E_2 the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = x^3 - 584551x - 172021102.$$

Then we have $N_2 = 56144 = 2^4 \cdot 11^2 \cdot 29$ and observe that p^2 divides N_2, $E_2[p]$ is surjective, $11 \nmid \mathrm{Tam}(E_2/\mathbb{Q})$, $11 \nmid 29 - 1$ with $a_{29}(E_2) = 1$, and $\#\text{Ш}(E_2/\mathbb{Q})[11^\infty] = 121$, and $\mathrm{rk}_{\mathbb{Z}} E_2(\mathbb{Q}) = 0$. Since E_2 has additive reduction at 11, any former result on the *equality* of the main conjecture does not apply.

How can we verify the main conjecture for the above examples? In order to deal with this question, we focus more on Kato's theorem (Theorem 2.8) since it is insensitive to the reduction type. Then when does Kato's Euler system become "optimal" to make Theorem 2.8 an equality?

§ 3.2. Main results

Definition 3.4. A prime ℓ is a **Kolyvagin prime** (for $T_{f^*}(1)$) if ℓ does not divide Np, $\ell \equiv 1 \pmod{\pi}$, $\overline{a_\ell(f)} \equiv \ell + 1 \pmod{\pi}$, and $\overline{\psi(\ell)} \equiv 1 \pmod{\pi}$.

Remark. The notion of Kolyvagin primes is generalized and refined in §5.1.

Now we assume that n is a square-free product of Kolyvagin primes. Then we fix a primitive root η_ℓ modulo ℓ for a prime ℓ dividing n. Then we define the discrete logarithm $\log_{\mathbb{F}_\ell}(a) \in \mathbb{Z}/(\ell-1)\mathbb{Z}$ by $(\eta_\ell)^{\log_{\mathbb{F}_\ell}(a)} \equiv a \pmod{\ell}$ and denote its mod p reduction by $\overline{\log_{\mathbb{F}_\ell}(a)} \in \mathbb{F}_p \hookrightarrow \mathbb{F}_\pi$.

Theorem 3.5 (K–Kim–Sun [KKS20], K–Nakamura [KN20]). *Assume one of the following statements:*

(good) If p does not divide N, then $a_p(f) \not\equiv 1 \pmod{\pi}$ and $a_p(f) \not\equiv \psi(p) \pmod{\pi}$

(additive) If p^2 divides N, then $p > 7$ and f corresponds to an elliptic curve E over $\mathbb{Q}$ with potentially good reduction at p and the Manin constant is prime to p.

We also assume that

1. *the image of $\overline{\rho}$ contains a conjugate of $\mathrm{SL}_2(\mathbb{F}_p)$ (Assumption 2.2),*
2. *for a prime q dividing N with $q \not\equiv \pm 1 \pmod{p}$, $\mathrm{ord}_q\, N = \mathrm{ord}_q\, N(\overline{\rho})$, and*
3. *for a prime q dividing N with $q \equiv \pm 1 \pmod{p}$, q^2 divides N.*

If

$$\widetilde{\delta}_n := \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(\prod_{\ell \mid n} \overline{\log_{\mathbb{F}_\ell}(a)} \right) \cdot \overline{\left[\frac{a}{n}\right]^+_f} \neq 0$$

in $\mathbb{F}_\pi$ for some square-free product n of Kolyvagin primes, then

- *the derived Kato's Euler system does not vanish modulo π, and*
- *Kato's IMC (Conjecture 2.4) holds.*

Remark. The number $\widetilde{\delta}_n$ is called the **Kurihara number at** n. The number itself is not well-defined, but its mod π non-vanishing question is well-defined. The potentially good reduction assumption in the additive case is required to have a pseudo-isomorphism between $\mathbb{H}^2$ and the fine Selmer group $\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee$. Assumptions 2. and 3. correspond to the divisibility condition

$$p \nmid \mathrm{Tam}(f) \cdot \prod_{q|N_{\mathrm{sp}}} (q-1) \cdot \prod_{q|N_{\mathrm{ns}}} (q+1)$$

where $\mathrm{Tam}(f)$ is the product of local Tamagawa ideals for f at bad primes, N_{sp} is the product of split multiplicative primes (i.e. $q \| N$ and $a_q(f) = 1$), and N_{ns} is the product of non-split multiplicative primes (i.e. $q \| N$ and $a_q(f) = -1$).

Let us recall some corollaries of Theorem 3.5 due to [EPW06], [KN20], [GIP], and [KLP].

Corollary 3.6. *Suppose that all the assumptions of Theorem 3.5 holds.*

1. *In the good ordinary case, if we further assume $\mu = 0$ (i.e. the p-adic L-function is non-zero mod π), then the Iwasawa main conjecture holds for all members of Hida family of the residual representation without any tame level assumption.*

2. *In the additive reduction case, even without the potential good reduction assumption, the numerical criterion implies the p-part of the Birch and Swinnerton-Dyer conjecture for E. In other words, we have*

$$\mathrm{ord}_p\left(\#\text{Ш}(E/\mathbb{Q})[p^\infty]\right) = \mathrm{ord}_p\left(\frac{L(E,1)}{\Omega^+_E}\right).$$

3. *In the good supersingular case, if we further assume $\mu^\pm = 0$ (i.e. the $\pm$-p-adic L-function is non-zero mod π), then the $\pm$-main conjecture holds for modular forms of weight two with $a_p = 0$ without any tame level assumption.*

Now we apply Theorem 3.5 to verify the main conjecture for elliptic curves appeared in Example 3.2 and 3.3.

Ex. 3.2. For pair $(E_1, 7)$, we have

$$\widetilde{\delta}_{1289\cdot 1471} \neq 0.$$

Thus, the main conjecture for $(E_1, 7)$ holds and, furthermore, since $\mu = 0$, the main conjecture holds for all members of the Hida family of $E_1[7]$.

Ex. 3.3. For pair $(E_2, 11)$, we have

$$\widetilde{\delta}_{397\cdot 859} \neq 0.$$

Thus, the main conjecture for $(E_2, 11)$ holds. In addition, since $j(E_2)$ is 11-integral and $E_2(\mathbb{Q})$ is finite, the 11-part of the BSD formula

$$\mathrm{ord}_{11}\left(\#\text{Ш}(E_2/\mathbb{Q})[11^\infty]\right) = \mathrm{ord}_{11}\left(\frac{L(E_2,1)}{\Omega^+_{E_2}}\right) = 2$$

holds.

§ 4. The main idea and possible generalizations

The main idea of proof is fairly simple and straightforward. The following implications show how it works.

$$\begin{array}{c} \widetilde{\delta}_n \neq 0 \pmod{\pi} \\ \Downarrow ? \\ \text{derived Kato's Euler systems do not vanish mod } \pi \\ \text{i.e. Kato's Kolyvagin system is primitive} \\ \Downarrow \text{[Büy11]} \\ \text{Kato's } \Lambda\text{-adic Kolyvagin system is } \Lambda\text{-primitive} \\ \Downarrow \text{[MR04] + (potentially) good condition} \\ \text{Kato's main conjecture holds.} \end{array}$$

Before giving an answer to the question mark in the above, we quickly review how the latter two implications are obtained.

§ 4.1. Application of Kolyvagin systems

Kolyvagin systems are the "rigidified" version of Kolyvagin derivatives of Euler systems. We do not review the theory of Kolyvagin systems here. See [KKS20, §4] for a summary and [MR04] for detail.

Let $\boldsymbol{\kappa}$ be the Kolyvagin system for $T_{\overline{f}}(1)$ associated to Kato's Euler system and $\boldsymbol{\kappa}^\infty$ be the Λ-adic Kolyvagin system for $T_{\overline{f}}(1) \otimes \Lambda$, which lifts $\boldsymbol{\kappa}$.

A Kolyvagin system $\boldsymbol{\kappa}$ is **primitive** if $\boldsymbol{\kappa}$ does not vanish modulo π, i.e $\kappa_n \not\equiv 0 \pmod{\pi}$ for some square-free product n of Kolyvagin primes.

A Λ-adic Kolyvagin system $\boldsymbol{\kappa}^\infty$ is **Λ-primitive** if $\boldsymbol{\kappa}^\infty$ does not vanish modulo any height-one primes of Λ.

Proposition 4.1 (Büyükboduk [Büy11]). *If $\boldsymbol{\kappa}$ is primitive, then $\boldsymbol{\kappa}^\infty$ is Λ-primitive.*

Theorem 4.2 (Mazur–Rubin [MR04]). *If $\mathbb{H}^2$ and the fine Selmer group are pseudo-isomorphic over Λ and $\boldsymbol{\kappa}^\infty$ is Λ-primitive, then Conjecture 2.4 holds.*

§ 4.2. The integral lattice and Kurihara numbers

Let $G_n = \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$. Consider the following diagram

$$\begin{array}{ccc}
\mathrm{H}^1(\mathbb{Q}(\mu_n), T_{\overline{f}}(1)) & & \\
\downarrow D_n & & \\
\mathrm{H}^1(\mathbb{Q}(\mu_n), T_{\overline{f}}(1)) & \xrightarrow{\exp^* \circ \mathrm{loc}_p} & S(\overline{f}) \otimes \mathbb{Q}_{f,\pi} \otimes \mathbb{Q}_p(\mu_n) \\
\downarrow \bmod \pi & & \downarrow \langle \omega^*_{\overline{f}}, - \rangle_{\mathrm{dR}} \\
\left(\mathrm{H}^1(\mathbb{Q}(\mu_n), T_{\overline{f}}(1))/\pi\right)^{G_n} & & \mathbb{Q}_{f,\pi} \otimes \mathbb{Q}_p(\mu_n) \\
\hookdownarrow & & \\
\left(\mathrm{H}^1(\mathbb{Q}(\mu_n), \overline{\rho}_{\overline{f}}(1))\right)^{G_n} & & \\
\downarrow \mathrm{res}^{-1} & & \\
\mathrm{H}^1(\mathbb{Q}, \overline{\rho}_{\overline{f}}(1)) & & \\
\downarrow \text{[MR04, Appendix A]} & & \\
\mathrm{H}^1(\mathbb{Q}, \overline{\rho}_{\overline{f}}(1)) \otimes G_n & &
\end{array}
\qquad
\begin{array}{ccc}
c^+_{\mathbb{Q}(\mu_n)} & & \\
\downarrow & & \\
D_n c^+_{\mathbb{Q}(\mu_n)} & \longmapsto & D_n \exp^* \mathrm{loc}_p c^+_{\mathbb{Q}(\mu_n)} \\
\downarrow & & \downarrow \\
\vdots & & \langle \omega^*_{\overline{f}}, D_n \exp^* \mathrm{loc}_p c^+_{\mathbb{Q}(\mu_n)} \rangle_{\mathrm{dR}} \\
\downarrow & & \\
\kappa_n \pmod{\pi} & &
\end{array}$$

where $c^+_{\mathbb{Q}(\mu_n)}$ is the $+$-part of the *integral* Kato's Euler system at $\mathbb{Q}(\mu_n)$ as in [Kat04, Example 13.3], D_n is the Kolyvagin derivative with respect to certain choices of generators of $\mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ for ℓ dividing n (cf. §5.3), $S(\overline{f})$ is the $\mathbb{Q}_f$-vector space generated by $\overline{f}$ as in [Kat04, §6.3], $\omega^*_{\overline{f}}$ is the dual "integral" basis to $\overline{f}$ with respect to the de Rham pairing chosen by the mod p multiplicity one as in [KKS20, §5.5], $\overline{\rho}_{\overline{f}}$ is the residual representation of $\overline{f}$, res^{-1} is the inverse of the restriction map in the Hochschild–Serre spectral sequence defined on the image of the Kolyvagin derivative classes as in [Rub00, §4.4], and [MR04, Appendix A] is the "$+\epsilon$" in Diagram (1.1).

Remark. As we emphasized, the Euler system here must be an *integral* Euler system in order to consider the associated Kolyvagin system. See also [KN20, Appendix].

In order to have $\kappa_n \pmod{\pi} \neq 0$, it suffices to see $D_n c^+_{\mathbb{Q}(\mu_n)} \not\equiv 0 \pmod{\pi}$. This can be checked by considering how

$$\langle \omega^*_{\overline{f}}, D_n \exp^* \left(\mathrm{loc}_p c^+_{\mathbb{Q}(\mu_n)} \right) \rangle_{\mathrm{dR}}$$

lies in the integral lattice

$$\mathscr{L} = \langle \omega^*_{\overline{f}}, \exp^* \left(\mathrm{H}^1(\mathbb{Q}_p(\mu_n), T_{\overline{f}}(1)) \right) \rangle_{\mathrm{dR}} \subseteq \mathbb{Q}_{f,\pi} \otimes \mathbb{Q}_p(\mu_n).$$

By the Tate local duality, computing $\langle \omega^*_{\overline{f}}, \exp^* \left(\mathrm{H}^1(\mathbb{Q}_p(\mu_n), T_{\overline{f}}(1)) \right) \rangle_{\mathrm{dR}}$ is equivalent to computing $\langle \log \left(J_1(N)_{\overline{f},\pi}(\mathbb{Q}_p(\mu_n)) \right), \omega_{\overline{f}} \rangle_{\mathrm{dR}}$ where $J_1(N)_{\overline{f},\pi}$ is the $\mathbb{Q}_{f,\pi}$-component of the modular abelian variety of $\overline{f}$. Then the computation reduces to two parts:

- the image of the $\mathfrak{m}_{\mathbb{Q}_p(\mu_n)}$-points of the formal group of $J_1(N)_{\overline{f},\pi}(\mathbb{Q}_p(\mu_n))$ under the formal logarithm map, and
- the image of $J_1(N)_{\overline{f},\pi}(\mathbb{F}_p(\mu_n))$ under the mod p reduction of the logarithm map

where $\mathfrak{m}_{\mathbb{Q}_p(\mu_n)}$ is the maximal ideal of $\mathbb{Q}_p(\mu_n)$. This strategy is due to [Rub00, Proposition 3.5.1]. Note that here we use the geometry of modular abelian varieties explicitly.

Using the interpolation property of modular symbols and the factorization of the Gauss sum, it is not very difficult to show that $\langle \omega^*_{\overline{f}}, D_n \exp^* \left(\mathrm{loc}_p c^+_{\mathbb{Q}(\mu_n)} \right) \rangle_{\mathrm{dR}} \in \mathscr{L}$ modulo $\pi\mathscr{L}$ becomes $\widetilde{\delta}_n$. Thus, we have a proof of Theorem 3.5.

Remark. In general, if the variables are assigned values in the maximal ideal, the power series giving the formal group law converges. This is why we can take the $\mathfrak{m}_{\mathbb{Q}_p(\mu_n)}$-points of the formal group of elliptic curves. Using the explicit Weierstrass local model, we can even take the $\mathbb{Z}_p[\mu_n]$-points of the formal group of elliptic curves with additive reduction. This observation is the key input in the additive reduction case. We do not expect that this property easily generalizes to general modular abelian varieties.

Remark. Here are some possible generalizations and questions.

1. The method to use the geometry of modular abelian varieties is not available for higher weight forms. In order to overcome this issue, an integral refinement of Perrin-Riou's local Iwasawa theory seems useful. Also, Perrin-Riou's local Iwasawa theory seems useful to cover not only $\mathbb{Q}_\infty$ but also $\mathbb{Q}(\mu_{p^\infty})$. Note that the Teichmüller character is not crystalline. This is being investigated by the author.

2. It seems interesting and difficult to consider a similar problem for higher core rank Euler and Kolyvagin systems since the integrality issue becomes much more delicate.

Part II
Refined Iwasawa theory

§ 5. Further applications: refined Iwasawa theory à la Kurihara

Unfortunately, I had no time to discuss the relation of indivisibility of Kurihara numbers and refined Iwasawa theory when I gave a talk at RIMS.

The notion of Kurihara numbers has more applications than establishing the main conjecture. More precisely, it provides the information of the *structure* of Selmer groups, not just their size. In order to explain this nature, the rest of this article is devoted to explain Kolyvagin systems of Gauss sum type, which is developed by Kurihara, for elliptic curves by summarizing the content of [Kur14b]. Especially, we emphasize how Kurihara numbers appear and are used, but we do not go into detail. See also [Kur02], [Kur03], [Kur12], and [Kur14a] for details of refined Iwasawa theory. We follow almost same notation as in [Kur14b].

Let p be an odd prime and E an elliptic curve over $\mathbb{Q}$ of conductor N.

Assumption 5.1. In this section, we assume

1. $p \nmid 2 \cdot N \cdot a_p(E) \cdot \mathrm{Tam}(E) \cdot \# \widetilde{E}(\mathbb{F}_p)$.
2. The representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ arising from the action on the p-adic Tate module $\mathrm{Ta}_p(E)$ is surjective (Assumption 2.2).
3. The μ-invariant of $\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee$ is zero. Thus, $\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])$ is a cofinitely generated $\mathbb{Z}_p$-module.

Remark. Under Assumption 5.1.(2), it is expected that Assumption 5.1.(3) always holds. It is the famous $\mu = 0$ conjecture of Greenberg ([Gre99, Conjecture 1.11]).

§ 5.1. Setting the stage

For an integer $k > 0$, let

$$\begin{aligned}
\mathcal{P}_{\mathrm{good}} &:= \{\ell : \ell \text{ is a prime}, \ell \nmid Np\},\\
\mathcal{P}^{(k)} &:= \{\ell \in \mathcal{P}_{\mathrm{good}} : \ell \equiv 1 \pmod{p^k}\},\\
\mathcal{P}^{(k)}_0 &:= \{\ell \in \mathcal{P}_{\mathrm{good}} : \ell \equiv 1 \pmod{p^k}, \mathrm{H}^0(\mathbb{F}_\ell, E[p^k]) \text{ contains an element of order } p^k\},\\
(\mathcal{P}'_0)^{(k)} &:= \{\ell \in \mathcal{P}_{\mathrm{good}} : \ell \equiv 1 \pmod{p^k}, \mathrm{H}^0(\mathbb{F}_\ell, E[p^k]) = E[p^k]\}, \text{ and}\\
\mathcal{P}^{(k)}_1 &:= \{\ell \in \mathcal{P}_{\mathrm{good}} : \ell \equiv 1 \pmod{p^k}, \mathrm{H}^0(\mathbb{F}_\ell, E[p^k]) \simeq \mathbb{Z}/p^k\mathbb{Z}\}.
\end{aligned}$$

Note that $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ acts on $E[p^k]$ since $\ell \nmid Np$. Thus, we have

$$(\mathcal{P}'_0)^{(k)} \subseteq \mathcal{P}^{(k)}_0, \qquad \mathcal{P}^{(k)}_1 \subseteq \mathcal{P}^{(k)}_0, \qquad \text{and} \qquad (\mathcal{P}'_0)^{(k)} \cap \mathcal{P}^{(k)}_1 = \emptyset.$$

Suppose that $\ell \in \mathcal{P}^{(k)}_1$. Since $\ell \equiv 1 \pmod{p^k}$, we have an exact sequence of $G_{\mathbb{F}_\ell}$-modules

$$0 \longrightarrow \mathbb{Z}/p^k\mathbb{Z} \longrightarrow E[p^k] \longrightarrow \mathbb{Z}/p^k\mathbb{Z} \longrightarrow 0$$

and the (arithmetic) Frobenius at ℓ acts on $E[p^k]$ by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ for a suitable basis of $E[p^k]$. Thus, $\mathrm{H}^1(\mathbb{F}_\ell, E[p^k]) \simeq \mathbb{Z}/p^k\mathbb{Z}$ for $\ell \in \mathcal{P}^{(k)}_1$.

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

$$\mathcal{P}^{(k)}_{0,t} := \{\ell \in \mathcal{P}_{\mathrm{good}} : \ell \equiv 1 \pmod{p^k}, t \in \mathrm{H}^0(\mathbb{F}_\ell, E[p^k])\},$$
$$\mathcal{P}^{(k)}_{1,t} := \{\ell \in \mathcal{P}_{\mathrm{good}} : \ell \equiv 1 \pmod{p^k}, \mathrm{H}^0(\mathbb{F}_\ell, E[p^k]) = (\mathbb{Z}/p^k\mathbb{Z})t\}.$$

Let $\mathcal{P}^{(k)}_0 = \bigcup_t \mathcal{P}^{(k)}_{0,t}$ and $\mathcal{P}^{(k)}_1 = \bigcup_t \mathcal{P}^{(k)}_{1,t}$ where t runs over all elements of order p^k in $E[p^k]$. Under Assumption 5.1.(2), $(\mathcal{P}'_0)^{(k)}$ and $\mathcal{P}^{(k)}_{1,t}$ are infinite due to Chebotarev density theorem.

Let $\mathcal{K}_{(p)}$ be the set of number fields K such that $K/\mathbb{Q}$ is a finite abelian p-extension and unramified at all primes dividing N. Suppose that $K \in \mathcal{K}_{(p)}$. We define

$$(\mathcal{P}'_0)^{(k)}(K) := \{\ell \in \mathcal{P}_{\mathrm{good}} : \ell \equiv 1 \pmod{p^k}, \mathrm{H}^0(\mathbb{F}_\ell, E[p^k]) = E[p^k], \ell \text{ splits completely in } K/\mathbb{Q}\},$$
$$\mathcal{P}^{(k)}_1(K) := \{\ell \in \mathcal{P}_{\mathrm{good}} : \ell \equiv 1 \pmod{p^k}, \mathrm{H}^0(\mathbb{F}_\ell, E[p^k]) \simeq \mathbb{Z}/p^k\mathbb{Z}, \ell \text{ splits completely in } K/\mathbb{Q}\}.$$

Remark. These notions are generalized and refined versions of Kolyvagin primes (Definition 3.4).

For a prime ℓ with $\ell \nmid Np$ and a number field F, we have

$$\frac{\mathrm{H}^1(F_v, E[p^k])}{E(F_v) \otimes \mathbb{Z}/p^k\mathbb{Z}} = \mathrm{H}^0(\mathbb{F}_v, E[p^k](-1))$$

where v is a prime of F lying above ℓ and $\mathbb{F}_v$ is the residue field of v. We put

$$\mathcal{H}^2_\ell(F) = \bigoplus_{v \mid \ell} \mathrm{H}^0(\mathbb{F}_v, E[p^k](-1)).$$

For a prime $\ell \in \mathcal{P}^{(k)}_0$, we fix a prime $\overline{\ell}$ of an algebraic closure $\overline{\mathbb{Q}}$ lying above ℓ. For a number field F, write ℓ_F for the prime of F lying below $\overline{\ell}$. We fix $t_\ell \in \mathrm{H}^0(\mathbb{F}_\ell, E[p^k])$ and define

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

where $t_\ell \otimes \zeta_{p^k}^{\otimes(-1)}$ is the component at ℓ_K.

Let $K \in \mathcal{K}_{(p)}$ and K_∞/K the cyclotomic $\mathbb{Z}_p$-extension, and K_n the n-th layer. Due to Assumption 5.1.(3) (i.e. $\mu = 0$), $\mathrm{Sel}(K_\infty, E[p^\infty])^\vee$ is a finitely generated $\mathbb{Z}_p$-module; thus, the corestriction map

$$\mathrm{cores} : \mathrm{Sel}(K_m, E[p^k]) \to \mathrm{Sel}(K, E[p^k])$$

is the zero map for $m \gg 0$. We take the minimal such m and $K_{[1]} := K_m$ and $K_{[n]} := \left(K_{[n-1]}\right)_{[1]}$.

§ 5.2. Euler systems of Gauss sum type for elliptic curves

Let $K \in \mathcal{K}_{(p)}$ and $\ell \in \mathcal{P}^{(k)}_0(K_{[1]})$. By using the global duality theorem, we have an exact sequence

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

where $\mathrm{Sel}^{(\ell)}(K, E[p^k])$ is the ℓ-imprimitive Selmer group.

Let $\vartheta_{K_{[1]}} \in \mathbb{Z}_p[\mathrm{Gal}(K_{[1]}/\mathbb{Q})]$ be the p-stabilized Mazur–Tate element of E over $K_{[1]}$. We recall the Stickelberger theorem for elliptic curves.

Theorem 5.2 (**[Kur14b, Theorem 7]).** *Let K be a finite abelian p-extension and assume that any bad reduction prime for E is unramified in $K/\mathbb{Q}$. Then*

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

Remark. The proof of Theorem 5.2 depends heavily on a generalization of Kato's Euler system divisibility. See [Kur14b, Theorem 6.(1)] for detail. In other words, the construction of the Euler system of Gauss sum type for elliptic curves *uses* Kato's Euler system.

By Theorem 5.2, we know

$$w_\ell\left(\vartheta_{K_{[1]}} \cdot t_{\ell, K_{[1]}}\right) = \vartheta_{K_{[1]}} \cdot w_\ell\left(t_{\ell, K_{[1]}}\right) = 0.$$

Thus, there exists an element $g \in \mathrm{Sel}^{(\ell)}(K_{[1]}, E[p^k])$ such that $\partial_\ell(g) = \vartheta_{K_{[1]}} \cdot t_{\ell, K_{[1]}}$. We define the **Euler system of Gauss sum type** by

$$g_\ell = g^{(K)}_{\ell, t_\ell} := \mathrm{cores}_{K_{[1]}/K}(g) \in \mathrm{Sel}^{(\ell)}(K, E[p^k]).$$

It is proved in [Kur14b] that the element $g^{(K)}_{\ell, t_\ell}$ is independent of the choice of g.

§ 5.3. Kolyvagin derivatives and Kolyvagin systems of Gauss sum type

As we have already seen, for $\ell \in \mathcal{P}_{\mathrm{good}}$, we have a natural homomorphism

$$\partial_\ell : \mathrm{H}^1(K, E[p^k]) \to \mathcal{H}^2_\ell(K) = \bigoplus_{v|\ell} \mathrm{H}^0(\mathbb{F}_v, E[p^k](-1)).$$

Now we further assume $\ell \in \mathcal{P}^{(k)}_1(K)$. Let $\mathbb{Q}_\ell(\ell)$ be the maximal p-subextension of $\mathbb{Q}_\ell$ in $\mathbb{Q}(\mu_\ell)$ and $\mathcal{G}_\ell := \mathrm{Gal}(\mathbb{Q}_\ell(\ell)/\mathbb{Q}_\ell)$. For each $n \geq 1$, we fix a primitive p^n-th root of unity ζ_{p^n} such that $(\zeta_{p^n})_n \in \mathbb{Z}_p(1)$. By Kummer theory, we have an identification $\mathcal{G}_\ell \simeq \mu_{p^{n_\ell}}$ where $n_\ell = \mathrm{ord}_p(\ell - 1)$. Denote by $\tau_\ell \in \mathcal{G}_\ell$ the element corresponding to the fixed primitive p^{n_ℓ}-th root of unity $\zeta_{p^{n_\ell}}$ under the identification.

We define the map

$$\phi_\ell : \mathrm{H}^1(K, E[p^k]) \to \mathcal{H}^2_\ell(K) \tag{5.1}$$

by the composition of the following maps involving the finite-to-singular map (cf. [MR04, §1.2]):

$$\begin{aligned}
\mathrm{H}^1(K, E[p^k]) &\overset{\mathrm{loc}_\ell}{\to} \bigoplus_{v|\ell} \mathrm{H}^1(K_v, E[p^k]) \overset{(a)}{=} \bigoplus_{v|\ell} \mathrm{H}^1(\mathbb{Q}_\ell, E[p^k]) \overset{(b)}{=} \bigoplus_{v|\ell} \left(\mathrm{H}^1(\mathbb{F}_\ell, E[p^k]) \oplus \mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, E[p^k])\right) \\
&\overset{(c)}{\twoheadrightarrow} \bigoplus_{v|\ell} \mathrm{H}^1(\mathbb{F}_\ell, E[p^k]) = \bigoplus_{v|\ell} E[p^k]/(\mathrm{Frob}_\ell - 1) \underset{\simeq}{\overset{\mathrm{Frob}_\ell^{-1}-1}{\to}} \bigoplus_{v|\ell} E[p^k]^{\mathrm{Frob}_\ell = 1} \\
&= \bigoplus_{v|\ell} \mathrm{H}^0(\mathbb{F}_\ell, E[p^k]) = \mathcal{H}^2_\ell(K)(1) \overset{(d)}{=} \mathcal{H}^2_\ell(K)
\end{aligned}$$

where loc_ℓ is the localization map at ℓ, (a) comes from $\ell \in \mathcal{P}^{(k)}_1(K)$, (b) is the decomposition as an abelian group, (c) is the projection to the first part, (d) comes from the choice of p-power roots of unity, and $\mathrm{H}^1_{\mathrm{tr}}(\mathbb{Q}_\ell, E[p^k]) := \ker\left(\mathrm{H}^1(\mathbb{Q}_\ell, E[p^k]) \to \mathrm{H}^1(\mathbb{Q}_\ell(\ell), E[p^k])\right)$ (cf. [MR04, Definition 1.1.6.(iv)]).

For a prime $\ell \in \mathcal{P}^{(k)}_1(K)$, we identify $\mathcal{G}_\ell = \mathrm{Gal}(\mathbb{Q}(\ell)/\mathbb{Q})$ and take a generator τ_ℓ as before. Note that $[\mathbb{Q}(\ell) : \mathbb{Q}] = p^{n_\ell}$. We define the norm operator and the Kolyvagin derivative operator by

$$\mathrm{Nm}_\ell := \textstyle\sum_{i=0}^{p^{n_\ell}-1} \tau^i_\ell \in \mathbb{Z}[\mathcal{G}_\ell] \qquad \text{and} \qquad D_\ell := \textstyle\sum_{i=0}^{p^{n_\ell}-1} i\tau^i_\ell \in \mathbb{Z}[\mathcal{G}_\ell].$$

Let $\mathcal{N}^{(k)}_1(K)$ be the set of squarefree products of primes in $\mathcal{P}^{(k)}_1(K)$ including 1. For $n \in \mathcal{N}^{(k)}_1(K)$, we put $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}(n)/\mathbb{Q})$, $\mathrm{Nm}_n = \prod_{\ell|n} \mathrm{Nm}_\ell \in \mathbb{Z}[\mathcal{G}_n]$, and $D_n = \prod_{\ell|n} D_\ell \in \mathbb{Z}[\mathcal{G}_n]$.

Assume that $\ell \in (\mathcal{P}'_0)^{(k)}(K(n)_{[1]})$ and consider $g^{K(n)}_{\ell,t_\ell} \in \mathrm{Sel}^{(\ell)}(K(n), E[p^k])$. Then it is well known that $D_n g^{K(n)}_{\ell,t_\ell} \in \mathrm{Sel}^{(n\ell)}(K(n), E[p^k])^{\mathcal{G}_n}$. We define the **Kolyvagin derivative of Gauss sum type**

$$\kappa_{n,\ell} = \kappa^K_{n,\ell,t_\ell} \in \mathrm{Sel}^{(n\ell)}(K, E[p^k])$$

by the image of $D_n g^{K(n)}_{\ell,t_\ell}$ under the isomorphism via control theorem [Kur14b, Lemma 2, §3.3].

We say $n \in \mathcal{N}^{(k)}_1(K)$ is **admissible** if n admits a factorization

$$n = \ell_1 \cdot \cdots \cdot \ell_r$$

such that $\ell_{i+1} \in \mathcal{P}^{(k)}_1(K(\ell_1 \cdot \cdots \cdot \ell_i))$ for all $i = 1, \cdots, r-1$.

We define $\delta_n \in \mathbb{Z}/p^k\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ by

$$\vartheta_{K(n)} \equiv \delta_n \cdot \prod_{i=1}^{r}(1-\tau_{\ell_i}) \pmod{p^k, (\tau_{\ell_1}-1)^2, \cdots, (\tau_{\ell_r}-1)^2}. \tag{5.2}$$

where $\vartheta_{K(n)}$ is the p-stabilized Mazur–Tate element for $K(n)$. See [Kur14b, (25)].

Remark. This δ_n is a $\mathrm{Gal}(K/\mathbb{Q})$-equivariant p-stabilized version of Kurihara numbers. Note that the $k = 1$ is only considered when we define $\widetilde{\delta}_n$ in §3.2; however, it can be naturally generalized by considering $\ell \equiv 1 \pmod{p^k}$ in Definition 3.4. If $K = \mathbb{Q}$, then $\delta_n \in \mathbb{Z}/p^k\mathbb{Z}$. The **generalized Kurihara number** $\widetilde{\delta}_n \in \mathbb{Z}/p^k\mathbb{Z}$ is defined by

$$\widetilde{\theta}_{\mathbb{Q}(n)} \equiv \widetilde{\delta}_n \cdot \prod_{i=1}^{r}(\tau_{\ell_i}-1) \pmod{p^k, (\tau_{\ell_1}-1)^2, \cdots, (\tau_{\ell_r}-1)^2}$$

where $\widetilde{\theta}_{\mathbb{Q}(n)}$ is the Mazur–Tate element. It is easy to observe that

$$\mathrm{ord}_p(\widetilde{\delta}_n) = \mathrm{ord}_p(\delta_n).$$

See [Kur14b, (31) and (32) in §5.2]. Note that we tacitly make a relevant correspondence between generators of $\mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(\ell)/\mathbb{Q})$ for ℓ dividing n.

Proposition 5.3 (Properties of Kolyvagin derivatives of Gauss sum type). *Let $n \in \mathcal{N}_1^{(k)}(K)$, m_0 an integer such that every prime of K_{m_0} dividing n is inert in K_∞/K_{m_0}, and $\ell \in (\mathcal{P}'_0)^{(k)}(K_{m_0+k})$. Then*

1. *$\kappa_{n,\ell} \in \mathrm{Sel}^{(n\ell)}(K, E[p^k])$.*
2. *$\partial_r(\kappa_{n,\ell}) = \phi_r(\kappa_{n/r,\ell})$ for any prime divisor r of n.*
3. *$\partial_\ell(\kappa_{n,\ell}) = \delta_n t_{\ell,K}$.*
4. *If n is admissible, then $\phi_r(\kappa_{n,\ell}) = 0$ for any prime divisor r of n.*

We adjust Kolyvagin derivatives to obtain Kolyvagin systems "by replacing ℓ". The adjustment is needed for the computation of higher Fitting ideals of Selmer groups.

For any square-free product n of primes, we define $\epsilon(n)$ to be the number of prime divisors of n. Consider natural maps

$$w_K : \bigoplus_\ell \mathcal{H}^2_\ell(K) \to \mathrm{Sel}(K, E[p^k])^\vee \qquad \text{and} \qquad \partial_K : \mathrm{H}^1(K, E[p^k]) \to \bigoplus_\ell \mathcal{H}^2_\ell(K)$$

as in §5.2.

Assume that $n\ell \in \mathcal{N}_1^{(k)}(K_{\epsilon(n\ell)})$. By [Kur14b, Lemma 3, §3.4], we can take $\ell' \in (\mathcal{P}'_0)^{(k)}$ such that

- $\ell \in (\mathcal{P}_0')^{(k)}(K_{[\epsilon(n\ell)]}(n)K_{m_0+k})$ where m_0 is as in Proposition 5.3.
- $w_{K_{[\epsilon(n\ell)]}}(t_{\ell',K_{[\epsilon(n\ell)]}}) = w_{K_{[\epsilon(n\ell)]}}(t_{\ell,K_{[\epsilon(n\ell)]}})$.
- Let $\phi_r^{K_{[\epsilon(n\ell)]}} : \mathrm{H}^1(K_{[\epsilon(n\ell)]}, E[p^k]) \to \mathcal{H}^2_r(K_{[\epsilon(n\ell)]})$ be the map ϕ_r for $K_{[\epsilon(n\ell)]}$ as in (5.1). There is an element
$$b' \in \mathrm{Sel}^{(\ell\ell')}(K_{[\epsilon(n\ell)]}, E[p^k])$$
such that $\partial_{K_{[\epsilon(n\ell)]}}(b') = t_{\ell',K_{[\epsilon(n\ell)]}} - t_{\ell,K_{[\epsilon(n\ell)]}}$ and $\phi_r^{K_{[\epsilon(n\ell)]}}(b') = 0$ for all r dividing n.

We put $b = \mathrm{cores}_{K_{[\epsilon(n\ell)]}/K}(b')$. We define the **Kolyvagin system of Gauss sum type** by
$$\kappa_{n,\ell} := \kappa_{n,\ell'} - \delta_n \cdot b.$$
Note that this element is independent of the choice of ℓ' and b'. This is needed for computation of higher Fitting ideals of Selmer groups.

Proposition 5.4 (Properties of Kolyvagin systems of Gauss sum type). *Suppose that $n\ell \in \mathcal{N}_1^{(k)}(K_{[\epsilon(n\ell)]})$. Then*

1. $\kappa_{n,\ell} \in \mathrm{Sel}^{(n\ell)}(K, E[p^k])$.
2. $\partial_r(\kappa_{n,\ell}) = \phi_r(\kappa_{n/r,\ell})$ *for any prime divisor r of n.*
3. $\partial_\ell(\kappa_{n,\ell}) = \delta_n \cdot t_{\ell,K}$.
4. *If n is admissible, then $\phi_r\kappa_{n,\ell} = 0$ for any prime divisor r of n.*
5. *If $n\ell$ is admissible and $n\ell \in \mathcal{N}_1^{(k)}(K_{[\epsilon(n\ell)]+1})$, then we have*
$$\phi_\ell(\kappa_{n,\ell}) = \delta_n \cdot t_{\ell,K}.$$

We omit the modified Kolyvagin system of Gauss sum type. See [Kur14b, §5.1] for detail. The modification allows us to choose $n\ell \in \mathcal{N}_1^{(k)}(K)$; thus, is it useful for effective computations.

§ 5.4. Applications to determine the structure of Selmer groups

We state the main result of [Kur14b] regarding the structure of Selmer groups.

Theorem 5.5 (Kurihara). *Suppose that $n = \ell_1 \cdot \cdots \cdot \ell_a \in \mathcal{N}_1^{(k)}(K_{[a+1]})$. Assume that n is admissible and*
$$\delta_n \in \left(\mathbb{Z}/p^k\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]\right)^\times .$$
Then

1. $\mathrm{Sel}^{(m)}(K, E[p^k])$ *is a free module of rank* a *over* $\mathbb{Z}/p^k\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$.
2. *The Kolyvagin system of Gauss sum type* $\{\kappa_{n/\ell_i,\ell_i}\}_{1\leq i\leq a}$ *forms a basis of* $\mathrm{Sel}^{(m)}(K, E[p^k])$.
3. *Let*

$$\mathcal{A} := \begin{pmatrix} \delta_{n/\ell_1} & \phi_{\ell_1}(\kappa_{n/\ell_1\ell_2,\ell_2}) & \cdots & \phi_{\ell_1}(\kappa_{n/\ell_1\ell_a,\ell_a}) \\ \phi_{\ell_2}(\kappa_{n/\ell_2\ell_1,\ell_1}) & \delta_{n/\ell_2} & \cdots & \phi_{\ell_2}(\kappa_{n/\ell_2\ell_a,\ell_a}) \\ \vdots & \vdots & \vdots & \vdots \\ \phi_{\ell_a}(\kappa_{n/\ell_a\ell_1,\ell_1}) & \phi_{\ell_a}(\kappa_{n/\ell_a\ell_2,\ell_2}) & \cdots & \delta_{n/\ell_a} \end{pmatrix} \in \mathrm{M}_{a\times a}\left(\mathbb{Z}/p^k\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]\right)$$

and $f_{\mathcal{A}} : \left(\mathbb{Z}/p^k\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]\right)^{\oplus a} \to \left(\mathbb{Z}/p^k\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]\right)^{\oplus a}$ *be the linear map corresponding to* $\mathcal{A}$*. Then*

$$\mathrm{Sel}(K, E[p^k])^\vee \simeq \mathrm{coker}(f_{\mathcal{A}}).$$

Remark. See [Kur14b, Remark 5, §4.2] for the relation between $\mathcal{A}$ and the organizing matrix in the sense of Mazur–Rubin [MR05].

§ 5.5. Higher Fitting ideals of Selmer groups

Another aspect of refined Iwasawa theory is to deal with higher Fitting ideals of Selmer groups. We only record the following theorem [Kur14b, Corollary 1, §2.4] using generalized Kurihara numbers due to the page limit.

Theorem 5.6 (Kurihara). *Let* n *be a square-free product of primes in* $\mathcal{P}_0^{(k)}$ *and* $\epsilon(n) = r$*. Then*

$$\delta_n \in \mathrm{Fitt}_{r,\mathbb{Z}/p^k\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})]}\left(\mathrm{Sel}(\mathbb{Q}_m, E[p^k])^\vee\right)$$

where $\mathrm{Fitt}_{r,R}(M)$ *is the* r*-th Fitting ideal of* M *over* R*.*

Remark. For the initial Fitting ideal, the same result even holds for the supersingular case. See [KK19] for detail.

Acknowledgement

I would like to thank the organizers of *Algebraic Number Theory and Related Topics 2018*, RIMS, Kyoto, for giving me the chance to give a talk at RIMS and to write this survey paper; Kentaro Nakamura for recommending me as a speaker to the organizers; Masato Kurihara for his constant encouragement and very helpful comments on an earlier version of this paper; Alex Ghitza for providing me with an effective algorithm to compute Kurihara numbers and agreeing to write the appendix of this paper on the effective computation of Kurihara numbers; the referee for his or her careful reading and valuable comments.

This work was partially supported by a KIAS Individual Grant (SP054102) via the Center for Mathematical Challenges at Korea Institute for Advanced Study, by Basic Science Research Program through the National Research Foundation of Korea (NRF-2018R1C1B6007009), and by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

§ Appendix A. Effective computation of Kurihara numbers, by Alexandru Ghitza

Recall the Kurihara numbers discussed in Section 3.2:

$$\widetilde{\delta}_n = \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(\prod_{\ell \mid n} \overline{\log_{\mathbb{F}_\ell}(a)} \right) \cdot \overline{\left[\frac{a}{n}\right]_f^+} \in \mathbb{F}_p. \qquad \text{(Appendix A.1)}$$

Here n is a squarefree product of Kolyvagin primes for a rational elliptic curve E, $[\frac{a}{n}]_f^+$ is the modular symbol corresponding to the newform f attached to E, $\log_{\mathbb{F}_\ell}(a)$ is the discrete logarithm of a with respect to a fixed choice of primitive root mod ℓ, and $\bar{\cdot}$ denotes reduction modulo p.

Whether $\widetilde{\delta}_n$ is zero or not in $\mathbb{F}_p$ is well-defined independently of the choices of primitive roots. Our aim is to computationally decide this question of non-vanishing in an efficient manner. We performed these computations in SageMath [Dev19], which provides functionality for all the necessary ingredients. The challenge was to use this functionality while avoiding the overhead costs often associated with SageMath objects. In particular, the following implementation decisions greatly reduced the amount of time and memory required:

- Instead of using SageMath's modular symbol object, we rely on `ECModularSymbol`, which is a thin wrap of modular symbols from John Cremona's highly optimized eclib package [Cre19].

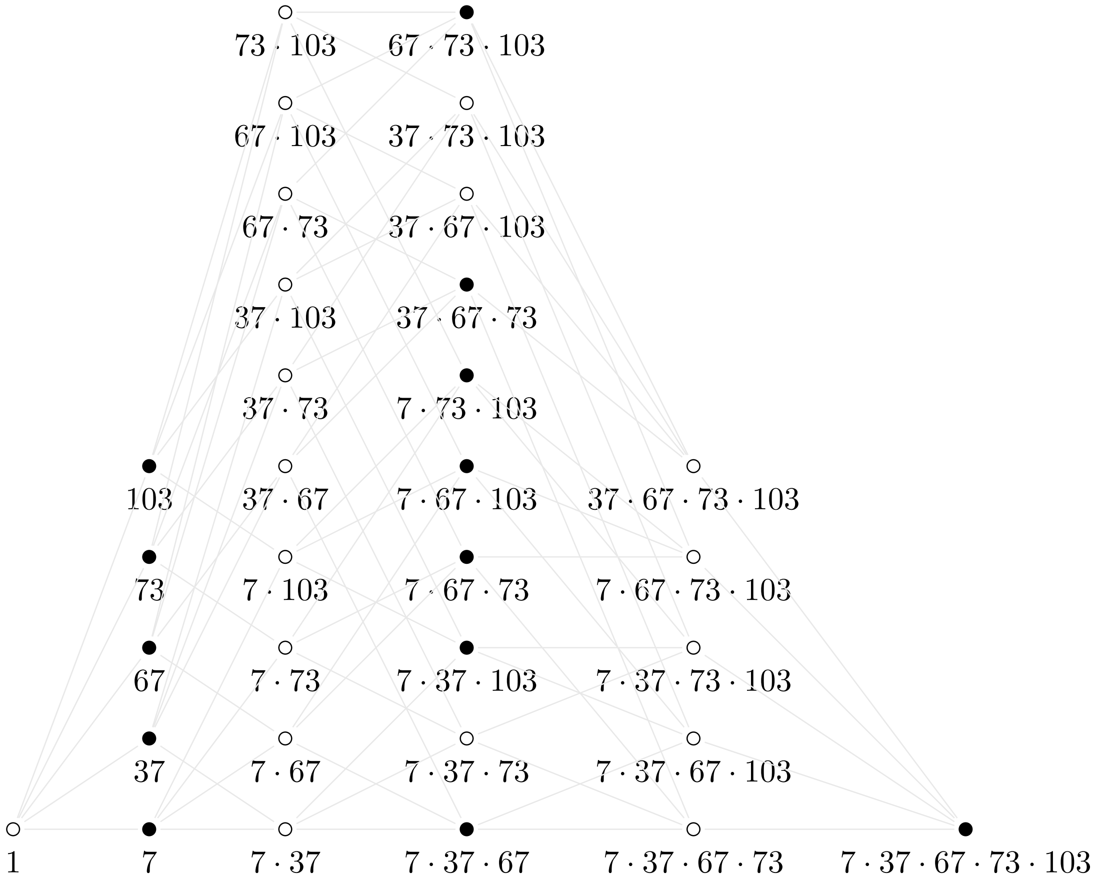
- Since the same discrete logarithm values are used many times in the computation, we cache each value the first time we compute it.

Here is an example of results produced by the code. Consider the elliptic curve 128A1, that is

$$E: \qquad y^2 = x^3 + x^2 + x + 1.$$

One can check that $p = 3$ satisfies the required properties for E, and that the first Kolyvagin primes for the pair (E, p) are $S = \{7, 37, 67, 73, 103\}$. We compute the

Kurihara numbers for all squarefree products of the primes in S and represent the result as the graph



The vertex representing a given Kurihara number is a white circle if the number is zero and a black circle otherwise. The vanishing of the Kurihara numbers illustrated by the red vertices in the third and fifth columns of the graph follows from the functional equation. See [Kur14b, Lemma 4 (Page 347)] for details.

The computation of the entire graph took about 14 minutes on a desktop computer. The code is available at

`https://github.com/aghitza/kurihara_numbers`

References

[Büy11] Kâzim Büyükboduk, Λ-*adic Kolyvagin systems*, Int. Math. Res. Not. IMRN (2011), no. 14, 3141–3206.

[ÇCSS] Francesc Castella, Mirela Çiperiani, Christopher Skinner, and Florian Sprung, *On the Iwasawa main conjectures for modular forms at non-ordinary primes*, preprint, arXiv:1804.10993.

[Cre19] John Cremona, *Eclib package*, https://github.com/JohnCremona/eclib, 2019, accessed from Sage 8.7.

[Dev19] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 8.7)*, 2019, http://www.sagemath.org.

[EPW06] Matthew Emerton, Robert Pollack, and Tom Weston, *Variation of Iwasawa invariants in Hida families*, Invent. Math. **163** (2006), no. 3, 523–580.

[GIP] Ralph Greenberg, Adrian Iovita, and Robert Pollack, *On the Iwasawa invariants for elliptic curves with supersingular reduction*, in preparation, July 2008.

[Gre99] Ralph Greenberg, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997) (Berlin) (C. Viola, ed.), Lecture Notes in Math., vol. 1716, Centro Internazionale Matematico Estivo (C.I.M.E.), Florence, Springer-Verlag, 1999, Lectures from the 3rd C.I.M.E. Session held in Cetraro, July 12–19, 1997, pp. 51–144.

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117–290.

[KK19] Chan-Ho Kim and Masato Kurihara, *On the refined conjectures on Fitting ideals of Selmer groups of elliptic curves with supersingular reduction*, Int. Math. Res. Not. IMRN (2019), rnz129, published online (5 July, 2019).

[KKS20] Chan-Ho Kim, Myoungil Kim, and Hae-Sang Sun, *On the indivisibility of derived Kato's Euler systems and the main conjecture for modular forms*, Selecta Math. (N.S.) **26** (2020), no. 2, 47 pages.

[KLP] Chan-Ho Kim, Jaehoon Lee, and Gautier Ponsinet, *On the Iwasawa invariants of Kato's zeta elements for modular forms*, submitted, arXiv:1909.01764.

[KN20] Chan-Ho Kim and Kentaro Nakamura, *Remarks on Kato's Euler systems for elliptic curves with additive reduction*, J. Number Theory **210** (2020), 249–279.

[Kob03] Shinichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.

[Kol91] Victor Kolyvagin, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2, 253–259.

[Kur02] Masato Kurihara, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I*, Invent. Math. **149** (2002), 195–224.

[Kur03] ———, *Iwasawa theory and Fitting ideals*, J. Reine Angew. Math. **561** (2003), 39–86.

[Kur12] ———, *Refined Iwasawa theory and Kolyvagin systems of Gauss sum type*, Proc. Lond. Math. Soc. (3) **104** (2012), no. 4, 728–769.

[Kur14a] ———, *Refined Iwasawa theory for p-adic representations and the structure of Selmer groups*, Münster J. of Math. **7** (2014), no. 1, 149–223.

[Kur14b] ———, *The structure of Selmer groups of elliptic curves and modular symbols*, Iwasawa Theory 2012: State of the Art and Recent Advances (Thanasis Bouganis and Otmar Venjakob, eds.), Contributions in Mathematical and Computational Sciences, vol. 7, Springer, 2014, pp. 317–356.

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin Systems*, Mem. Amer. Math. Soc., vol. 168, American Mathematical Society, March 2004.

[MR05] ———, *Organizing the arithmetic of elliptic curves*, Adv. Math. **198** (2005), 504–546.

[Pol03] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558.

[Rub00] Karl Rubin, *Euler Systems*, Ann. of Math. Stud., vol. 147, Princeton University Press, 2000.

[Spr] Florian Sprung, *The Iwasawa main conjecture for elliptic curves at odd supersingular primes*, preprint, arXiv:1610.10017.

[Spr12] ———, *Iwasawa theory for elliptic curves at supersingular primes: A pair of main conjectures*, J. Number Theory **132** (2012), no. 7, 1483–1506.

[SU14] Christopher Skinner and Eric Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195** (2014), no. 1, 1–277.

[Wana] Xin Wan, *Iwasawa main conjecture for non-ordinary modular forms*, preprint, February 2020, arXiv:1607.07729.

[Wanb] ———, *Iwasawa main conjecture for supersingular elliptic curves and BSD conjecture*, preprint, October 2019, arXiv:1411.6352.

[Wan15] ———, *The Iwasawa main conjecture for Hilbert modular forms*, Forum Math. Sigma **3** (2015), e18 (95 pages).

[Zha14] Wei Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2** (2014), no. 2, 191–253.