On the rank of 2-primary part of Selmer group of certain elliptic curves

by

KWANG HYUN KIM

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

2012

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirements for the degree of Doctor of Philosophy.

Professor Victor Kolyvagin

Date

Chair of Examining Committee

Executive Officer Jozef Dodziuk

Date

Executive Officer

Professor Victor Kolyvagin

Professor Kenneth Kramer

Professor Lucien Szpiro

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

On the rank of 2-primary part of Selmer group of certain elliptic curves

by

KWANG HYUN KIM

Advisor: Professor Victor Kolyvagin

Kolyvagin proved very remarkable results on Mordell-Weil groups and Shafarevich-Tate groups of certain elliptic curves when a given Heegner point P_K has infinite order in his series of papers [3], [4], [5] and [7]. In [6], he also extended his result to odd prime ℓ-primary part of Selmer group of higher rank with the assumption of existence of non-trivial Kolyvagin system(conjecture 1.0.4). In this thesis, we will follow his Euler system method and verify that his method also works to prove the result on the rank of 2-primary part of Selmer group of higher rank with Strong non-zero conjecture 1.0.9.

Acknowledgements

First and foremost, I would like to give my special thanks to my thesis advisor, professor Victor Kolyvagin for all his guidance and support. He has introduced me to deep and beautiful mathematics and kindly shared many important ideas with me. I also would like to thank professor Kenneth Kramer and professor Lucien Szpiro for being on my thesis committee and guiding me with helpful comments and suggestion.

Finally, I would like to thank my family as well. My parents, my wife Jiae and son Ian, without their support, I would have never finished.

Contents

1 Introduction **1**

2 Preliminaries **7**

3 Construction of Euler system **10**

3.1 Heegner points 10

3.2 Kolyvagin prime 12

3.3 Euler system 13

4 local properties **15**

4.1 local conditions 15

4.2 Selmer structure 17

4.3 Standard Selmer group at $\ell = 2$ 19

4.4 Kolyvagin's derivative classes 20

5 global properties **24**

5.1 Key properties of the Kolyvagin's derivative classes 25

5.2 Strong non-zero Kolyvagin conjecture 27

6 Main theorem **30**

7 Appendix **47**

7.1 Size of $H^1(V'_{n'}|K, E[\ell^n])$ 47

Bibliography **51**

Chapter 1

Introduction

Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field with the associated quadratic character ω on $\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}$. We assume all prime factors of N are split in K.(Heegner condition). Here D is a discriminant of K with $(D, 2N) = 1$. We also consider a Weierstrass minimal models of curve E with discriminant Δ. Let $P_K \in E(K)$ be the Heegner point over K, and Let $L(E/K, s) := L(E, \mathbb{Q}, s)L(E, \mathbb{Q}, \omega, s)$ be the complex L-function of $E_{/K}$ (over K). Gross and Zagier proved that P_K has infinite order if and only if $L'(E/K, 1) \neq 0$(analytic rank one). From Gross and Zagier's formula and Birch and Swinnerton-Dyer Conjecture for $E_{/K}$ with analytic rank one, we can get the following conjecture.

Conjecture 1.0.1 *(Conjecture 1.2 in [2]) Suppose P_K has an infinite order, then $E(K)$ has rank one, the Shafarevich-Tate group $Ш(E/K)$ is finite and*

its order is given by

$$|Ш(E/K)| = \left(\frac{[E(K) : \mathbb{Z}P_K]}{c \prod_{q|N} c_q} \right)^2$$

where c is Manin constant and $c_q = [E(\mathbb{Q}_q)|E^0(\mathbb{Q}_q)]$ *is the Tamagawa number at q.*

Using the theory of Euler system, Kolyvagin ([5],[7]) has shown the rank part of conjecture 1.0.1, the finiteness of $Ш(E/K)$ and the explicit upper bound of $Ш(E/K)$. To calculate more exact size of ℓ-primary part of $Ш(E/K)$, we assume the following condition.

Assumption 1.0.2 (Surjective condition) *We assume the ℓ-adic representation ρ_ℓ of a given elliptic curve E is surjective.*

$$\rho_\ell : G(\mathbb{Q}(E[\ell^\infty])|\mathbb{Q}) \to Aut(E[\ell^\infty])$$

Kolyvagin proved the structure theorem on $Ш(E/K)[\ell^\infty]$ if ℓ is odd. When ℓ is odd, we can decompose $Ш(E/K)$ as $Ш(E/K)^+$ and $Ш(E/K)^-$ via the complex conjugation.

Theorem 1.0.3 *(The structure theorem of Shafarevich group for odd ℓ, Theorem C in [7]) Assume P_K has infinite order. With the surjective condition*

on ρ_ℓ, for odd ℓ

$$Ш(E/K)^{\epsilon}[\ell^{\infty}] = \mathbb{Z}/\ell^{m_1-m_2}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m_1-m_2}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m_3-m_4}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m_3-m_4}\mathbb{Z} \dots$$

and

$$Ш(E/K)^{-\epsilon}[\ell^{\infty}] = \mathbb{Z}/\ell^{m_0-m_1}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m_0-m_1} \oplus \mathbb{Z}/\ell^{m_2-m_3}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m_2-m_3} \dots$$

where $-\epsilon$ is a sign of functional equation and m_i is a (non-negative) ℓ-divisible index of Heegner points with $m_i \geq m_{i+1}$(definition 4.4.5). In particular, we can conclude

$$Rank_{\mathbb{Z}}(E(K)) = 1$$

and

$$|Ш(E/K)[\ell^{\infty}]| = \ell^{2(m_0-m_{\infty})}$$

where $m_0 = ord_l([E(K) : \mathbb{Z}P_K])$ and m_∞ is a minimal ℓ-divisible index of Heegner points.

When P_K has a finite order, Kolyvagin also proved the structure theorem on odd prime ℓ-primary part of Selmer group over K with the following conjecture 1.0.4.

Conjecture 1.0.4 *(Kolyvagin conjecture for odd prime ℓ [6]) There is $r \in \mathbb{Z}_{\geq 0}$ such that $m_r < \infty$.*

Definition 1.0.5 *(minimum f for odd ℓ) Assume the Kolyvagin conjecture 1.0.4.*

$$f := \min\{r \in \mathbb{Z}_{\geq 0} | m_r < \infty\}$$

Remark 1.0.6 *If P_K has infinite order, $f = 0$.*

With Kolyvagin conjecture 1.0.4, Kolyvagin proved the following theorem for odd ℓ.

Theorem 1.0.7 *(Conditional structure theorem for odd ℓ, theorem 1 in [6]) Assume the conjecture 1.0.4. With the surjective condition on ρ_ℓ for odd prime ℓ and $n > m_f$,*

$$S(E, K, \ell^n)^{\epsilon(-1)^f} = \mathbb{Z}/\ell^{n_0} \ldots \mathbb{Z}/\ell^{n_{f+1}}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m_{f+1}-m_{f+2}}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m_{f+1}-m_{f+2}}\mathbb{Z} \oplus \ldots$$

and

$$S(E, K, \ell^n)^{\epsilon(-1)^{f+1}} = \mathbb{Z}/\ell^{n'_1} \ldots \mathbb{Z}/\ell^{n'_f}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m_f - m_{f+1}}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m_f - m_{f+1}} \oplus \ldots$$

where $n_i = n$ for $i = 0, \ldots f+1$ and n'_i for $i = 1, \ldots, f$ is unknown.

In particular,

$$rank_{\mathbb{Q}_\ell/\mathbb{Z}_\ell} \varinjlim (S(E, K, \ell^n)^{(-1)^f \epsilon}) = f + 1$$

and

$$rank_{\mathbb{Q}_\ell/\mathbb{Z}_\ell} \varinjlim (S(E, K, \ell^n)^{(-1)^{f+1} \epsilon}) \leq f$$

In this paper, we will prove the weaker results for $\ell = 2$. We will not prove the structure theorem for $\ell = 2$, but we will prove the rank part of theorem. Basically, we follow Kolyvagin's original ideas in his Euler system papers [4], [5], [7] and [6], but we adjust proofs slightly to fit $\ell = 2$ case when it is necessary.

For $\ell = 2$, Kolyvagin pointed out that we need a slightly stronger conjecture in [6]. This stronger conjecture means the Kolyvagin derivative classes $\{\tau_{\lambda,n} | \lambda \in \Lambda_n^r\}$ are not torsion[1].

Definition 1.0.8 *($V_{n,k}^r$, page 258 in [6])*

$$V_{n,k}^r := \{\tau_{\lambda,n} | \lambda \in \Lambda_{n+k}^r\}$$

where $\tau_{\lambda,n}$ is a Kolyvagin derivative class in definition 4.4.4.

Conjecture 1.0.9 *(strong non-zero system conjecture, conjecture B in [6]) There exists $r \in \mathbb{Z}_{\geq 0}$ such that*

$$\forall k \geq k_0, \ \exists \ n \mid V_{n,k}^r \neq 0$$

Definition 1.0.10 *(minimum f for even ℓ) Assume the strong non-zero sys-*

[1] Remark 5.2.6

tem conjecture 1.0.9.

$$f := \min\{r \in \mathbb{Z}_{\geq 0} | r \text{ holds the strong non} - \text{zero conjecture } 1.0.9\}$$

In this paper, we will prove the following result.

Theorem 1.0.11 *(Main theorem) Let $\ell = 2$. Assume assumption 2.0.13. If we assume the strong non-zero Kolyvagin conjecture 1.0.9 for ℓ, then*

$$rank_{\mathbb{Q}_\ell/\mathbb{Z}_\ell}(\varinjlim_n S(E, K, \ell^n)^{(-1)^f \epsilon}) = f + 1$$

and

$$rank_{\mathbb{Q}_\ell/\mathbb{Z}_\ell}(\varinjlim_n S(E, K, \ell^n)^{(-1)^{f+1} \epsilon}) \leq f$$

Chapter 2

Preliminaries

Remark 2.0.12 *For simplicity, we sometimes use* ± 1 *as* $\pm$ *sign.*

We always assume $\ell = 2$. Let E be a elliptic curve over $\mathbb{Q}$ with conductor N and a discriminant Δ.

Assumption 2.0.13 *(Basic assumption) We assume the* ℓ*-adic representation* $\rho_{E,\ell}$ *of a given* E *is surjective.*

$$\rho_{E,\ell} : G(\mathbb{Q}(E[\ell^\infty])|\mathbb{Q}) \to Aut(E[\ell^\infty])$$

So E *is a non-CM(complex multiplication) elliptic curve by classical results in the theory of complex multiplication.*

- $K = \mathbb{Q}(\sqrt{D})$ *with* $D < 0$ *and* $D \neq -2, -3, -4, -|\Delta|, -2|\Delta|$.
- $(D, 2N) = 1, (N, \ell) = 1$ *and* K *satisfies Heegner condition*[1].

[1]Heegner condition means that all prime factors of N are split in K.

Definition 2.0.14

$$\rho_{E,n,\ell} : G(\mathbb{Q}(E[\ell^n])|\mathbb{Q}) \to Aut(E[\ell^n])$$

Remark 2.0.15 *From [4] proposition 16,* $D \neq -2, -3, -4, -|\Delta|, -2|\Delta|$ *implies* $K \cap \mathbb{Q}(E[\ell^\infty]) = \mathbb{Q}$. *Therefore*

$$\rho_{E,\ell} : G(K(E[\ell^\infty])|K) \to GL_2(\mathbb{Z}_\ell)$$

is also surjective. We also get $E(K)[\ell] = 0$ *from surjective condition([4] proposition 3).*

Actually, if E is non-CM, there are only finitely many prime q such that $\rho_{E,q}$ is not surjective by Serre's result([13]).

Theorem 2.0.16 *(J.P. Serre [13]) Suppose that* E *is an elliptic curve with* $End(E) = \mathbb{Z}$*(Non-CM).*

$\exists c$ *such that*

$$\rho_{E,q} : G(\mathbb{Q}(E[q^\infty])|\mathbb{Q}) \to GL_2(\mathbb{Z}_q)$$

is surjective for $q \geq c$.

Definition 2.0.17 *Let* σ *is the complex conjugation.*

Let $g' \in G(K(E[\ell^\infty]|K)$ *such*

$$\rho_{E,\ell}(g') = \rho_{E,\ell}(\sigma) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Then

$$\mathfrak{c} := \begin{cases} \sigma & if\ \rho_{E,1,\ell}(\sigma) \neq I \\ \sigma g' & if\ \rho_{E,1,\ell}(\sigma) = I \end{cases}$$

For $\{1, \mathfrak{c}\}$*-module* A*,*

$$A^{\pm} := ker(1 \mp \mathfrak{c})$$

Definition 2.0.18 *(Projective system of basis* $\{e^{\pm}_{\ell^n}\}$ *on* $E[\ell^\infty]$*) From proposition 6, proposition 9 and the page 490 in [4],* $E[\ell^n]^{\pm} \cong \mathbb{Z}/\ell^n$*. So we can construct a projective (basis) system* $\{e^{\pm}_{\ell^n}\}$ *of* $E[\ell^n]$ *for all* $n \geq 1$*. So* $\ell e^{\pm}_{\ell^{n+1}} = e^{\pm}_{\ell^n}$*.*

Remark 2.0.19 *Because* $\mathfrak{c}|_K = \sigma|_K$*, actions on* $H^1(K, E[\ell^n])$ *are same.*

Chapter 3

Construction of Euler system

Now let us consider a family of Heegner points which is a key object in Kolyvagin's papers which we are following. In general, finding an algebraic point of a elliptic curve E is not easy question. Using complex multiplication theory, one can construct a large supply of algebraic points on E through the modular parametrization Φ_N.[1] These points are "Heegner points" on E. The existence of the modular parametrization[2] is proven by Andrew Wiles, Richard Taylor and other contributors. It also implies a famous Fermat Last Theorem due to ϵ-conjecture result of Kenneth Ribet([11]).

3.1 Heegner points

Definition 3.1.1 *We assume* $(\lambda, N) = 1$ *with* $\lambda \in \mathbb{N}$.

[1] For a detail construction, refer chapter 3 in [1]

[2] It is called Taniyama-Shimura-Weil conjecture.(Chapter 2.6 in [1])

- *$K[\lambda]$ is the ring class field of K with conductor λ*
- *By Heegner condition, there exists an ideal $\mathfrak{N} \subset O_K$ in the ring of integers of K such that $N = \mathfrak{N}\overline{\mathfrak{N}}$ and $O_K/\mathfrak{N} = \mathbb{Z}/N\mathbb{Z}$.*
- *$O[\lambda] := \mathbb{Z} + \lambda O_K$ a order with conductor λ*
- *$\mathfrak{N}[\lambda] := \mathfrak{N} \cap O[\lambda]$*
- *$(\lambda, N) = 1 \Rightarrow \mathfrak{N}[\lambda]$ is an invertible ideal in $O[\lambda]$*
- *$x_\lambda := [\mathbb{C}/O[\lambda] \to \mathbb{C}/\mathfrak{N}[\lambda]^{-1}] \in X_0(N)(K[\lambda])$*
- *Let $\pi : X_0(N) \to E$ be a fixed optimal modular parametrization which map the cusp $i\infty$ of $X_0(N)$ to the origin of F E*
- *$y_\lambda := \pi(x_\lambda) \in E(K[\lambda])$ is a Heegner point with conductor λ*
- *$P_K := N_{K[1]|K}(y_1) \in E(K)$*

One of Kolyvagin's main idea is using local conditions of local fields which is complete with respect to Kolyvagin primes to bound a given group. Kolyvagin proved that there are infinitely many Kolyvagin primes using Chebotarev density theorem[3].

[3]proposition 9 in [4]

3.2 Kolyvagin prime

Definition 3.2.1

- $n(p) := ord_\ell(p+1, a_p(E))$ *with* $a_p(E) := p+1-|E(F_p)|$ *and* $F_p := \mathbb{Z}/p\mathbb{Z}$.
- $n(\lambda) := min_{p|\lambda}\{n(p)\}$

Definition 3.2.2 *(Kolyvagin prime of level n, proposition 6 in [4])* *Kolyvagin prime p of level n is a prime in $\mathbb{Q}$ satisfying the following*

0. *p is inert in K*
1. $p \nmid 2 \cdot 3ND$
2. $n \leq n(p)$
3. $E[\ell]^+ = \mathbb{Z}/\ell$ *where* $E[\ell]^+$ *is a kernel of* $Fr_p - 1$ *and* Fr_p *is the Frobenius automorphism* $a \to a^p$ *of* $\overline{\mathbb{Z}/p}$ *over* $\mathbb{Z}/p$.

We also can define

- $\Lambda_n^r = \{p_1 \cdot p_2 \dots p_r | p_i$ *distinct Kolyvagin prime of level* $n\}$
- $\Lambda^r = \cup_n \Lambda_n^r$

Remark 3.2.3 *If ℓ is odd, $E[\ell]^+ = \mathbb{Z}/\ell$ condition is always true.*

Definition 3.2.4 $\mathfrak{L}_p \in \mathbb{Z}[G(K[\lambda]|K)]$

For $p \in \Lambda_n^1$,

$$\mathfrak{L}_p = a_p$$

Where $a_p := p + 1 - |E(F_p)|$ *and* $F_p := \mathbb{Z}/p\mathbb{Z}$.

3.3 Euler system

In [3], [5], Kolyvagin introduced collections of points with such properties and called them Euler systems. The Euler system of Heegner points is one of his main examples of Euler Systems.

Proposition 3.3.1 *(proposition 1 in [3] and proposition 1 [4])*

For $p \in \Lambda_n^1$ *and* $\lambda \in \Lambda_n^r$,

- $p \nmid \lambda \Rightarrow N_{K[p\lambda]|K[\lambda]}(y_{p\lambda}) = \mathfrak{L}_p y_\lambda$
- *For almost all* $p \in \Lambda^1$

$$red_{\mathfrak{p}(K[p\lambda])}(y_{p\lambda}) = Fr_p^{-1}(red_{\mathfrak{p}(K[\lambda])}(y_\lambda))$$

where Fr_p *is the Frobenius automorphism* $a \to a^p$ *of* $\overline{\mathbb{Z}/p}$ *over* $\mathbb{Z}/p$.

Using these properties, Kolyvagin constructed Kolyvagin derivative cohomology classes (we will recall their construction in the next chapter) which are

among main tools in his theory of Euler Systems. They are also called as Kolyvagin System by Berry Mazur and Karl Rubin in [9].

Chapter 4

local properties

In this chapter, we define several local conditions of Selmer structure. Using these local conditions, we will construct Selmer modules which are generalizations of classical Selmer group. We will also recall Kolyvagin's construction of derivative cohomology classes. We will use them to calculate the difference between two Selmer structures later.

4.1 local conditions

Definition 4.1.1 *(chapter 1 in [9]) Now for prime $w \in Spec(O_K)$,*

$$H^1_f(K_w, E[\ell^n]) := E(K_w)/\ell^n E(K_w)$$

$$H^1_s(K_w, E[\ell^n]) := H^1(K_w, E[\ell^n])/H^1_f(K_w, E[\ell^n])$$

Then we have the exact sequence

$$0 \longrightarrow H^1_f(K_w, E[\ell^n]) \xrightarrow{Kum} H^1(K_w, E[\ell^n]) \longrightarrow H^1_s(K_w, E[\ell^n]) \longrightarrow 0$$

$$\tau \longrightarrow (\tau)_s$$

Here we can identify

$$H^1_s(K_w, E[\ell^n]) \cong H^1(K_w, E)[\ell^n]$$

Of course, we can define similar cohomology groups for $\mathbb{Q}_v$ instead of K_w.

Definition 4.1.2 *If M is $\mathbb{Z}[Fr_p]$-module with $Fr_p^2 = 1$, we can define*

$$M^{\pm} := ker(Fr_p \mp 1 : M \to M)$$

Remark 4.1.3 *For $p \in \Lambda^1_n$, from 101-102 page of [7] [1], We can decompose*

$$H^1(K_{\mathfrak{p}}, E[\ell^n]) = H^1_f(K_{\mathfrak{p}}, E[\ell^n]) \oplus H^1_{tr}(K_{\mathfrak{p}}, E[\ell^n])$$

where $H^1_{tr}(K_{\mathfrak{p}}, E[\ell^n]) := H^1(L_{p,n}|K_{\mathfrak{p}}, A(L_{p,n})[\ell^n])$ and $L_{p,n}$ is the class field of $K_{\mathfrak{p}}$ which corresponds to the subgroup $K^*_{\mathfrak{p}^{\ell^n}} p^{\mathbb{Z}}$ of $K^*_{\mathfrak{p}}$.

We can also check

$$\left(H^1_{tr}(K_{\mathfrak{p}}, E[\ell^n])\right)_s = H^1(K_{\mathfrak{p}}, E)[\ell^n]$$

[1] Kolyvagin's augment also works well for $\ell = 2$ because $E[\ell^n] \cong H^1(K_p, E)[\ell^n]$ from page 479 in [7].

4.2 Selmer structure

Basically, we use Mazur and Rubin's definitions in chapter 2 of [9].

Definition 4.2.1 *(chapter 2 in [9]) Selmer structure $\mathcal{F}$ on $E[\ell^n]$ over K is a collection of local conditions $\{H^1_{\mathcal{F}}(K_v, E[\ell^n])\}$ such that*

- *Let $\sum(\mathcal{F})$ be a finite set of place of K, including ∞, ℓ and primes dividing ND.*
- *For each $v \in \sum(\mathcal{F})$, we choose some $\mathbb{Z}/\ell^n$-submodule*

$$H^1_{\mathcal{F}}(K_v, E[\ell^n]) \subset H^1(K_v, E[\ell^n])$$

- *$v \notin \sum(\mathcal{F})$ we define*

$$H^1_{\mathcal{F}}(K_v, E[\ell^n]) := H^1_f(K_v, E[\ell^n])$$

Definition 4.2.2 *(Selmer module, chapter 2 in [9])*

Selmer module $H^1_{\mathcal{F}}(K, E[\ell^n]) \subset H^1(K, E[\ell^n])$ is defined by

$$Ker\left(H^1(K, E[\ell^n]) \to \oplus \frac{H^1(K_v, E[\ell^n])}{H^1_{\mathcal{F}}(K_v, E[\ell^n])}\right)$$

Definition 4.2.3 *(chapter 2 in [9]) Given Selmer structure $\mathcal{F}$ and $abc \in \Lambda^r_n$, we can define $\mathcal{F}^a_b(c)$ on $E[\ell^n]$ over K as*

- $p|c \Rightarrow H^1_{\mathcal{F}^a_b(c)}(K_p, E[\ell^n]) = H^1_{tr}(K_p, E[\ell^n])$
- $p|a \Rightarrow H^1_{\mathcal{F}^a_b(c)}(K_p, E[\ell^n]) = H^1(K_p, E[\ell^n])$
- $p|b \Rightarrow H^1_{\mathcal{F}^a_b(c)}(K_p, E[\ell^n]) = 0$

Definition 4.2.4 **($\alpha(n, n')$)** *For $n' \geq n$, $\alpha(n, n')$ is the inclusion map from $E[\ell^n]$ to $E[\ell^{n'}]$*

$$E[\ell^n] \xhookrightarrow{\alpha(n,n')} E[\ell^{n'}]$$

Definition 4.2.5 *(Cartesian property of local condition $H^1_{\mathcal{F}}(K_v, E[\ell^n])$ on $\{E[\ell^n]|n \geq 1\}$)*[2]

$\mathcal{F}$ is cartesian at K_v on $\{E[\ell^n]|n \geq 1\}$ means For all $n' \geq n \geq 1$

$$H^1_{\mathcal{F}}(K_v, E[\ell^n]) = \alpha(n, n')^{-1}\left(H^1_{\mathcal{F}}(K_v, E[\ell^{n'}])\right)$$

$\mathcal{F}$ is cartesian on $\{E[\ell^n]|n \geq 1\}$ means that for all v, $\mathcal{F}$ is cartesian at K_v on $\{E[\ell^n]|n \geq 1\}$

Remark 4.2.6 *From page 104-105 in [7] because $E(K)[\ell^\infty] = 0$,*

$$H^1(K, E[\ell^n]) \cong H[\ell^n]$$

where $H := \varinjlim_n H^1(K, E[\ell^n])$.

So if $\mathcal{F}$ is cartesian on $\{E[\ell^n]|n \geq 1\}$, We can identify Selmer structure

[2]Definition 1.1.4 in [10]

$H^1_{\mathcal{F}}(K, E[\ell^n])$,

$$H^1_{\mathcal{F}}(K, E[\ell^n]) \cong H_{\mathcal{F}}[\ell^n]$$

where $H_{\mathcal{F}} := \varinjlim_n H^1(K, E[\ell^n])$

Remark 4.2.7 *(Examples of Cartesian condition)*

- $H^1(K_v, E[\ell^n])$ *is cartesian for all primes* v *in* K *from the definition of cartesian.*

- $H^1_f(K_v, E[\ell^n])$ *is cartesian for all primes* v *in* K*. Rubin's definition in [12] and our definition is same from proposition 1.6.7 in [12].*

- *For* $p \in \Lambda^1_n$ *and* $n \leq n(p)$, $H^1_{tr}(K_{\mathfrak{p}}, E[\ell^n])$ *is cartesian. For* $n \leq n(p)$, $H^1(K_{\mathfrak{p}}, E[\ell^n]) \cong H^1_f(K_{\mathfrak{p}}, E[\ell^n]) \oplus H^1_{tr}(K_{\mathfrak{p}}, E[\ell^n])$ *by remark 4.1.3. As* $H^1_f(K_{\mathfrak{p}}, E[\ell^n])$ *and* $H^1(K_{\mathfrak{p}}, E[\ell^n])$ *are cartesian, we can conclude that* $H^1_{tr}(K_{\mathfrak{p}}, E[\ell^n])$ *is also cartesian for* $n \leq n(p)$*.*

4.3 Standard Selmer group at $\ell = 2$

Definition 4.3.1 *Now we define the standard Selmer structure* $\mathcal{F}$ *as*

$$H^1_{\mathcal{F}}(K_v, E[\ell^n]) := H^1_f(K_v, E[\ell^n])$$

for all prime $v \in Spec(O_K)$*. It is same to the original definition of Selmer group.*

Definition 4.3.2 *For* $ab\lambda \in \Lambda_n^r$

$$S_b^a(\lambda)(E,K,\ell^n) := H^1_{\mathcal{F}_b^a(\lambda)}(K, E[\ell^n])$$

From remark 4.2.6 and 4.2.7, we can conclude the following proposition.

Proposition 4.3.3 *For* $ab\lambda \in \Lambda_{n+1}^r$,

$$S_b^a(\lambda)(E,K,\ell^{n+1})[\ell^n] \cong S_b^a(\lambda)(E,K,\ell^n)$$

4.4 Kolyvagin's derivative classes

Choose $p \in \Lambda_n^1$. Let $G[p] := G(K[p]|K[1]) =< t_p >$ with a generator t_p. We can also define $\widehat{G[\lambda]} := G(K[\lambda]|K)$. From proposition 5 in [3], $G[p]$ is cyclic with order $p+1$.

Definition 4.4.1

- $G[\lambda] := G(K[\lambda]|K[1])$
- *If* $p|\lambda$, *then we identify* $G[p] \cong G(K[\lambda]|K[\lambda/p])$
- $D_p := \sum_{i=1}^{p} i \cdot t_p^i (Derivative\ Operator)$[3]
- $D_\lambda := \prod_{p|\lambda} D_p$

[3]We use $D_p := \sum_{i=1}^p i \cdot t_p^i$ and [4] use $D_p := \sum_{i=1}^p (p+1-i) \cdot t_p^i$. It only change a sign in a explicit relation.

- *Let J_λ be a set of coset representatives of $\widehat{G[\lambda]} = G(K[\lambda]|K)$ with respect to $G[\lambda] = G(K[\lambda]|G[1])$*

Proposition 4.4.2 *((3.5) in [2])*

$$(t_p - 1)D_p = p + 1 - N_{K[p]|K[1]}$$

with $N_{K[p]|K[1]} := \sum_{i=0}^{p} t_p^i$

Proposition 4.4.3 *$\ell \nmid ND$ and $\rho_{E,\ell}$ is surjective implies*

$$E(K[\lambda])[\ell] = 0$$

Proof $\ell \nmid N \Rightarrow \mathbb{Q}(E[\ell])|\mathbb{Q}$ is only ramified at places dividing $N\ell$. $K[\lambda]|\mathbb{Q}$ is unramified at places dividing $N\ell$. $\mathbb{Q}(E[\ell]) \cap K[\lambda]$ is an unramified extension over $\mathbb{Q}$. But there is no unramified extension over $\mathbb{Q}$. So $\mathbb{Q}(E[\ell]) \cap K[\lambda] = \mathbb{Q}$ and it implies

$$\rho : G(K[\lambda](E[\ell])|K[\lambda]) \cong GL_2(\mathbb{Z}/\ell)$$

From the order augment of proposition 3 in [4], $E(K(\lambda))[\ell] = 0$. □

Consider $P_\lambda := \sum_{\sigma \in J_\lambda} \sigma D_\lambda y_\lambda$. Then from p 239-240 in [8],

$$[P_\lambda]_{\ell^n} \in H^1(K[\lambda], E[\ell^n])^{\widehat{G[\lambda]}}$$

Because $E(K[\lambda])[\ell] = 0 \Rightarrow H^i(\widehat{G[\lambda]}, E(K[\lambda])[\ell^n]) = 0$, for $i = 1, 2$ and

$$H^1(K, E[\ell^n]) \xrightarrow[\sim]{res_{K[\lambda]|K}} H^1(K[\lambda], E[\ell^n])^{\widehat{G[\lambda]}}$$

So we can define

Definition 4.4.4 (Kolyvagin's Derivative classes)

$$\tau_{\lambda,n} := res^{-1}_{K[\lambda]|K}([P_\lambda]_{\ell^n})$$

Definition 4.4.5 (ℓ-divisible index $m(\lambda)$ of P_λ)

- $m'(\lambda) := \begin{cases} max\{m \in \mathbb{N} | P_\lambda \in \ell^m E(K[\lambda])\} & P_\lambda \ non-torsion \\ \infty & otherwise \end{cases}$
- $m(\lambda) := \begin{cases} m'(\lambda) & m'(\lambda) < n(\lambda) \\ \infty & otherwise \end{cases}$
- $m_r(\lambda) := min\{m(\delta) | \delta \in \Lambda^r \ \lambda | \delta\}$
- $m_i := min\{m(\lambda) | \lambda \in \Lambda^i\}$
- $m_{i,n} := min\{m(\lambda) | \lambda \in \Lambda^i_{m(\lambda)+n}\}$[4]

[4]It is well-defined by remark 5.2.2

Definition 4.4.6 *$\#a$ means ℓ-power part of the order of a.* [5] *For a finite $\mathbb{Z}_\ell$-module M, we can also define*

$$\#M := max\{\#a | a \in M\}$$

Definition 4.4.7 *($ord_\ell(a)$ with $a \in \mathbb{Z}/\ell^n$) Let $a \in \mathbb{Z}/\ell^n$.*

$$ord_\ell(a) := max\{\alpha \mid \ \ell^\alpha | a \ and \ 0 \leq \alpha \leq n\}$$

Remark 4.4.8

- $m_0 = m(1)$
- $\#\tau_{\lambda,n} = n - m(\lambda)$ *if* $m(\lambda) \leq n$.
- *For* $a \in \mathbb{Z}/\ell^n$, $\#a = n - ord_\ell(a)$

[5] $< a > \cong \mathbb{Z}/\ell^k$ with a generator $a \Rightarrow \#a = k$

Chapter 5

global properties

In this chapter, we expose key properties of Kolyvagin's derivative classes proved in papers [4], [5], [7]. We will also discuss strong non-zero Kolyvagin conjecture.

Definition 5.0.9 *m is ℓ-power of the least common multiple of the period of the unramified cohomology groups $H^1(K_v, E)_{unr}$ for all primes v in K.*

Proposition 5.0.10 *(proposition 10 in [5] and proposition 1 in [7]) For $\lambda \in \Lambda^r_{n+m+1}$,*

$$\tau_{\lambda,n} \in S(\lambda)(E, K, \ell^n)^{(-1)^r \epsilon}$$

Proof Because $n(\lambda) \geq m + n$, we can consider $\tau_{\lambda,n+m}$. From theorem 10 in [5], for $v \nmid \lambda$, $(\tau_{\lambda,n}(v))_s = (\ell^m \tau_{\lambda,n+m}(v))_s = 0$. Namely, $\tau_{\lambda,n}(v) \in$

$H^1_f(K_\mathfrak{p}, E^{\epsilon(\lambda)}[\ell^n])$. From theorem 3 in [5] or proposition 1 in [7], for $p|\lambda$ with $n(p) \geq n+1$[1], $\tau_{\lambda,n}(p) \in H^1_{tr}(K_\mathfrak{p}, E^{\epsilon(\lambda)}[\ell^n])$. □

Remark 5.0.11 *From remark 4.2.7, for $p\lambda \in \Lambda^{r+1}_n$, $S^p(\lambda)(E,K,\ell^n)^\pm$ is cartesian.*

5.1 Key properties of the Kolyvagin's derivative classes

Proposition 5.1.1 *(proposition 2 in [4])*

For $\lambda \in \Lambda^r_{n+m+1}$ and $s \in H^1(K, E[\ell^n])^{\epsilon(\lambda)}$ with $s(p) \in H^1_f(K_p, E[\ell^n])^{\epsilon(\lambda)}$ For $p|\lambda$

$$\zeta_{n,p}^{<s,\tau_{\lambda,n}>_{E,K,p,n}} = [\frac{Fr_p^2-1}{\ell^n}s, (-1)^{r-1}\epsilon \cdot \frac{Fr_p^2-1}{\ell^n}\tau_{\lambda/p,n}]_{E,K,n}$$

where $\zeta_{n,p} \in \mu_{\ell^n}$ and $<\ ,\ >_{E,K,p,n}$: $H^1(K_p, E[\ell^n]) \times H^1(K_p, E^\pm[\ell^n]) \to \mathbb{Z}/\ell^n$ is the local Tate pairing and $[\ ,\ ]_{E,K,n} : E[\ell^n] \times E[\ell^n] \to \mu_{\ell^n}$ is the Weil pairing.

Remark 5.1.2 *We change a sign because we use a slightly different Derivative operator from [4].*

[1] In proof of proposition 1 in [7], we need $\tau_{\lambda,n}(p) = -(1+2+\ldots+p)Fr_p\widetilde{P_{\lambda/p}} = -\frac{p(p+1)}{2} \in \ell^n E(F)$. Because $\ell = 2$, we need$\ell^{n+1}|p+1$ and it implies $n(p) \geq n+1$

Proposition 5.1.3 *There is a local isomorphism ϕ_p for $p\lambda \in \Lambda^{r+1}_{n'+1}(n' \geq n)$.*

$$H^1_f(K_\mathfrak{p}, E[\ell^n]) \xrightarrow{\phi_p} H^1_{tr}(K_\mathfrak{p}, E[\ell^n])$$

$$\tau_{\lambda,n}(p) \longrightarrow \tau_{p\lambda,n}(p)$$

Proof From [5] p479, we have a isomorphism $\epsilon^{-1}_{E,p,n'} : E[\ell^{n'}] \cong H^1(K_\mathfrak{p}, E)[\ell^{n'}]$ by setting

$$\zeta_{n',p}^{<s,\epsilon^{-1}_{E,p,n'}(e)>_{K,E,p,n'}} = [\frac{Fr_p^2 - 1}{\ell^{n'}} s, e]_{\ell^{n'}}$$

with $s \in H^1_f(K_\mathfrak{p}, E[\ell^{n'}])$

Recall $\frac{Fr_p^2-1}{l^{n'}} : H^1_f(K_\mathfrak{p}, E[\ell^{n'}]) \to E[\ell^{n'}]$ is a isomorphism. So we have the following isomorphism

Definition 5.1.4

$$\phi_{p,n'}(\quad) := \epsilon^{-1}_{p,n'} \left((-1)^{r-1} \epsilon \frac{Fr_p^2 - 1}{\ell^{n'}} (\quad) \right)$$

□

Corollary 5.1.5 *With above assumption,*

$$\#\tau_{\lambda,n}(p) = \#\tau_{p\lambda,n}(p)$$

Remark 5.1.6 *Barry Mazur and Karl Rubin define Kolyvagin system in*

general. One of main properties is corollary 5.1.5.[2]

5.2 Strong non-zero Kolyvagin conjecture

We will look at the strong non-zero system.

Definition 5.2.1 *(k_0, page 258 in [6]) Let* $\mathfrak{K} = \prod_{\lambda \in \Lambda} K[\lambda]$. *Then*

$$k_0 := 2\#E(\mathfrak{K})[\ell^\infty]$$

Remark 5.2.2 *(well-defined $m_{f,n}$) Because* $\#E(\mathfrak{K})[\ell^\infty] = 0$ *from proposition 4.4.3, we have* $k_0 = 0$.

$$\forall k \geq 0,\ \exists\ n \mid V^r_{n,k} \neq 0$$

means

$$\forall k \geq 0,\ \exists\ \lambda \text{ such that } n(\lambda) > m(\lambda) + k$$

Now when we switch n *and* k, *we can also interpret it as*

$$\forall n \geq 0\ \exists\ \lambda \text{ such that } n(\lambda) > m(\lambda) + n$$

So $m_{f,n}$ *is well-defined.*

Definition 5.2.3 *For* $r = 0$,

$$s(r) := \begin{cases} 0 & if\ P_K\ finite\ order \\ \infty & if\ P_K\ infinite\ order \end{cases}$$

[2](5) of chapter 3 in [9].

For $r \geq 1$,

$$s(r) := max_{\lambda \in \Lambda^r}\{n(\lambda) - m(\lambda),\ 0\}$$

Remark 5.2.4 *Recall*

$$\forall n \geq 0\ \exists\ \lambda \text{ such that } n(\lambda) > m(\lambda) + n$$

We can conclude

$$Strong\ conjecture\ for\ r \Leftrightarrow\ s(r) = \infty$$

Remark 5.2.5 *So we can redefine* f *as*

$$f := min\{r | s(r) = \infty\}$$

Remark 5.2.6 *(*$\{\tau_{\lambda,n} | \lambda \in \Lambda_n^r\}$ *is torsion if* $r < f$*) By definition of* $s(r)$ *and* $\#\tau_{\lambda,n} = n - m(\lambda) \leq n(\lambda) - m(\lambda)$,

$$\#\{\tau_{\lambda,n} | \lambda \in \Lambda_n^r\} \leq s(r)$$

We will also prove $s(r) \leq m + 2re + 2$ *if* $r < f$ *(proposition 6.0.22) later. So if* $r < f$*, then*

$$\#\{\tau_{\lambda,n} | \lambda \in \Lambda_n^r\} \leq m + 2re + 2$$

Remark 5.2.7 *If we consider odd prime ℓ with surjective condition of $\rho_{E,\ell}$,*

$$(original)\ Kolyvagin\ conjecture \Leftrightarrow s(r) > 0$$

Actually theorem 3 in [6] implies

$$s(r) > 0 \Rightarrow s(r) = \infty$$

So original Kolyagin conjecture and Strong non-zero Kolyvagin conjecture are equivalent if ℓ is odd and $\rho_{E,\ell}$ is surjective.

Chapter 6

Main theorem

In this chapter, we will follow main idea of theorem 10 in [5] and the paper [6]. To handle higher rank case, we consider a decreasing sequence of Selmer groups

$$S^{(0)}_{(-1)^f\epsilon\ell^n} \supset S^{(1)}_{(-1)^f\epsilon\ell^n} \supset \ldots \supset S^{(f)}_{(-1)^f\epsilon\ell^n}$$

and

$$S^{(0)}_{(-1)^{f+1}\epsilon\ell^n} \supset S^{(1)}_{(-1)^{f+1}\epsilon\ell^n} \supset \ldots \supset S^{(f)}_{(-1)^{f+1}\epsilon\ell^n} \supset S^{(f+1)}_{(-1)^{f+1}\epsilon\ell^n}$$ [1]

Then we can directly use Kolyvagin's original idea to $S^{(f+1)}_{(-1)^f\epsilon\ell^n}$ and $S^{(f)}_{(-1)^{f+1}\epsilon\ell^n}$ After then, we will annihilate them to prove their finiteness.

Definition 6.0.8 *($\log_\ell$) we fix an isomorphism $\log_\ell : \mu_{\ell^n} \to \mathbb{Z}/\ell^n$.*

Definition 6.0.9 *(Subgroup of A generated by a)*

$< a >_A$ means the subgroup of A generated by a.

[1] In the definition 6.0.13.

Remark 6.0.10

- $V_{n'} := K(E[\ell^{n'}])$
- $a := max\{|H^1(V_{n'}|K, E[\ell^n])|\}$ *for all* $n' \geq n$. *From proposition 7.1.1,* $ord_\ell(a) = 1$
- $b := 2 \times b'$ *where* b' *satisfying* $b'A = 0$ *for all* G_n*-module such that* $A \subset E[\ell^n]^+$ *or* $A \subset E[\ell^n]^{-2}$. *From lemma 2 and 3 in [3],* $ord_\ell(b') = 0$. *So* $ord_\ell(b) = 1$.
- *Let* $e := ord_\ell(ab) = 2$
- *Let* $\overline{n} := m + 2ef + 3$ *and* $\overline{m} := m_{f,\overline{n}}$
- *In [5], Kolyvagin also used* c *for size of* ℓ*-torsion and* d *for action of complex conjugation. Here* $c = 1$ *and* $d = 1$ *because* $E(K)[\ell] = 0$ *and we use* $\mathfrak{c}$ *instead.*

Definition 6.0.11 *(*$rank_n$*)*

For $\mathbb{Z}_\ell$*-module* B,

$$rank_n(B) := rank_{\mathbb{Z}/\ell}(B/B[\ell^n] \otimes \mathbb{Z}/\ell)$$

In particular, $rank_0(B)$ *is the number of cyclic subgroups in the primary decomposition of* B.

[2]From page 473 in [5], $[e_{\pm\ell^n}, e_{\mp\ell^n}] = \zeta_{\ell^{n-1}}$ instead of ζ_{ℓ^n}. To handle this difference, we multiply 2.

Definition 6.0.12 *For a prime v in K,*

$$H^1(K, E[\ell^n])_{\widehat{v}} := Ker\left(H^1(K, E[\ell^n]) \to H^1(K_v, E)[\ell^n]\right)$$

Now let us make some definitions. Later, we will construct p_i with $i = 1, 2, \ldots, 2f+1$ in proposition 6.0.23.

Definition 6.0.13 *Let $n' > m + 4 + 2e(f-1) + n$ and $n > (f+2)(4fe + \overline{m} + 1) + e(f+4) + 1$. For given primes $p_1, , p_2, \ldots, p_{2f+1} \in \Lambda^1_{n'}$,*

- *Let $\lambda_k = p_0 p_k \cdot p_{k+1} \ldots p_{f+k-1}$ for $k = 1, \ldots f+1$ with $p_0 = 1$.*
- *$\chi^{(k)}_{\epsilon\mp,n} : H^1(K, E[\ell^n])_{\widehat{p_{f+k}}} \to \mu_{\ell^n}$ for $k = 1, \ldots, f+1$ such that*

$$\chi^{(k)}_{\epsilon\mp,n}(s) := [\frac{Fr^2_{p_{f+k}} - 1}{\ell^n} s, e_{\pm\epsilon\ell^n}]_{\ell^n}$$

- $S^{(0)}_{\pm\ell^n} := S(E, K, \ell^n)^{\pm}$
- $S^{(k)}_{\pm\ell^n} := kernel\left(\chi^{(k)}_{\epsilon\mp,n}|_{S^{(k-1)}_{\pm\ell^n}}\right)$ *for* $k = 1, \ldots f+1$
- $K_2 = S^{(f+1)}_{(-1)^f\epsilon\ell^n}$
- $K_1 = S^{(f)}_{(-1)^{f+1}\epsilon\ell^n}$
- *For a simplicity, we also use*

$$\chi_{p_{f+k}}(s_{\pm}) := \chi^{(k)}_{\pm,n}(s_{\pm})$$

with $s_{\pm} \in H^1(K, E[\ell^n])_{\widehat{p_{f+k}}}$

- $\eta_i = \tau_{\lambda_i,n}$ *with* $i = 1, \ldots f+1$
- $M := (M_{i,j})_{1 \leq i,j \leq f+1}$ *is a* $(f+1) \times (f+1)$ *matrix*

  with $M_{i,j} = log_{\ell}(\chi_{p_{f+j}}(\eta_i))$.

Most of proof of the main theorem 1.0.11 is carried from theorem 10 in [5], proposition 8 in [7] and theorem 3 in [6]. We split them as several propositions to adjust proofs for the $\ell = 2$ easily.

Definition 6.0.14 *(from theorem 10 in [5])*

- $S_{\pm}$ *is any finite subgroups of* ${H^1_{\ell^n}}^{\pm}$.
- $S'_{\pm} = res_{V|K}(S_{\pm})$
- $W(\pm)$ *be the M-periodic abelian extensions of* V *corresponding* $S'_{\pm}$
- $W = W(+)W(-)$
- $H(\pm) := G(W(\pm)|V)$ *and* $H := G(W|V)$
- $\varphi(\pm) : H \to S'^{*}_{\pm} := Hom(S'_{\pm}, \mu_{\ell^n})$ *such that*

$$\varphi(\pm)(\eta) : s_{\pm} \to [s_{\pm}((\eta\mathfrak{c})^2), e_{\pm\ell^n}]_{\ell^n}$$

- $\psi(\pm) : H \to S_{\pm}^{*} := Hom(S_{\pm}, \mu_{\ell^n})$ *via* $\psi(\pm) = res \circ \varphi(\pm)$
- $X(\pm) := \psi(\pm)(H)$

Proposition 6.0.15 *Assume* $n' \geq n > e + 1$. *Choose any finite subgroups* $S_{\pm} \subset {H_{\ell^n}^1}^{\pm}$. *then,* $\exists \eta \in H$ *such that* $\#\psi(\pm)(\eta) = \#X(\pm)$. *From* $abS_{\pm}^{*} \subset X(\pm)$ *with* $ord_{\ell}(ab) = e$,

$$\#S_{\pm} - e \leq \ \#\psi(\pm)(\eta) \leq \#S_{\pm}$$

Proof Proof can be found on page 477 - 478 in [5]. □

Proposition 6.0.16 *(from theorem 10 in [5]) With same assumption, for* $s_{\pm} \in {H_{\ell^n}^1}^{\pm}$, *there is infinitely many prime* $p \in \Lambda_{n''}^1$ *such that*

- *Let* $\chi_p(s_{\pm}) := \psi(\pm)(\eta)(s_{\pm})$ *then*

$$\#s_{\pm} - e \leq \chi_p(s_{\pm}) \leq \#s_{\pm}$$

- *(relation between local cohomology and global cohomology)*

$$\#s_{\pm}(p) \leq \#s_{\pm} \leq \#s_{\pm}(p) + e$$

Proof Proof is contained in the proof of theorem 10 in [5]. To help to understand our changed notations, we will write the proof.

Let $S_\pm = \{s_\pm^n | n \in \mathbb{Z}\}$. Let $\chi_p := \psi(\pm)(\eta)$ with above setting. Let $g \in G(W|\mathbb{Q})$, $g = \eta\mathfrak{c}$[3]. By Chebotrarev density theorem, $\exists$, There is infinitely many prime p of K such that p is unramified in W and $g = Fr_{W_v|\mathbb{Q}_p}$ where v is a prime of W satisfying $v|p$.

- $g|_K = \sigma|_K \Rightarrow (\frac{p}{K}) = -1(inert)$
- From proposition 6 in [4], we can check $p \in \Lambda^1_{n'}$ and p splits in $V_{n'}|K$.

$$\chi_p(s_\pm) := \psi(\pm)(\eta)(s_\pm) = [s_\pm(g^2), e_{\mp\ell^n}]_{\ell^n} = [\frac{Fr_p^2 - 1}{\ell^n} s_\pm, e_{\mp\ell^n}]_{\ell^n}$$

Claim 6.0.17 $\#\log_\ell(\chi_p(s_\pm)) = max\{\#s_\pm(p) - 1, 0\}$.

Proof From

$$\frac{Fr_p^2 - 1}{\ell^n} : E(K_p)/\ell^n \cong E[\ell^n]$$

we can write $\frac{Fr_p^2-1}{\ell^n} s_\pm = *\ell^{n-\#s_\pm(p)} e_{\pm\ell^n}$ with $* \in (\mathbb{Z}/\ell^n)^*$. Because $d = 1$, from page 473 in [5], $[e_{\pm\ell^n}, e_{\mp\ell^n}] = \zeta_{\ell^{n-1}}$. Therefore

$\#\log_\ell(\chi_p(s_\pm)) = max\{\#s_\pm(p) - 1, 0\}$. □

From $\#S_\pm - e \leq \ \#\psi(\pm)(\eta) \leq \#S_\pm$, we have

$$\#s_\pm - e \leq \chi_p(s_\pm) \leq \#s_\pm$$

[3]Definition 2.0.17

. From claim 6.0.17, $\#s_{\pm}(p) - 1 \leq \chi_p(s_{\pm}) \leq \#s_{\pm}(p)$. So we can conclude

$$\#s_{\pm}(p) \leq \#s_{\pm} \leq \#s_{\pm}(p) + e$$

□

Corollary 6.0.18 *(proposition 5 in [7]) If* $n' > n > e + \max\{m(\lambda), m(p\lambda)\}$ *with* $\lambda \in p\Lambda_{n'}^r$ *and* $\#\tau_{\lambda,n} \leq \#\tau_{\lambda,n}(p) + e$*, then* $m(p\lambda) - m(\lambda) \leq e$.

Proposition 6.0.19 *(proposition 4 in [7])*

For $p\lambda \in \Lambda_n^{r+1} \quad (r \geq 0)$

$$\#S^p(\lambda)(E, K, \ell^n)^{\pm} = n$$

Namely, there is $s \in S^p(\lambda)(E, K, \ell^n)^{\pm}$ *such that* $\#s = n$.

Proof From remark 5.0.11, $S^p(\lambda)(E, K, \ell^n)$ is cartesian. From proposition 6 in [4] and remark 4.1.3, $|H^1(K_p, E[\ell^n])^{\pm}| = \ell^{2n}$. Because isotropic properties also work for $\ell = 2$, the proof of proposition 4 in [7] also works for $\ell = 2$. □

Now we will state the proposition which allows us to switch a prime p to other prime q with arbitrarily large $n(q)$.

Proposition 6.0.20 *(proposition 8 in [7]) Assume* $n > 1+2e+m(p\delta)$, $n' \geq m + 1 + n, n'' > n'$ *with any* $p\delta \in \Lambda_{n'}^{r+1}$*. Then there is a prime* $q \in \Lambda_{n''}^1$ *such that* $\#\tau_{p\delta,n}(q) \leq \#\tau_{p\delta,n} \leq \#\tau_{p\delta,n}(q) + e$ *and* $m(q\delta) - m(p\delta) \leq 2e$.

Proof To keep track the conditions of n and n', we will write a proof. But the proof is exactly same to the proof of proposition 8 in [7]. Because we have a fudge factor e when $\ell = 2$, our result is a slightly weaker than original proposition.

Choose n such that $n > 1+2e+m(p\delta)$ and $n' > m+1+n$. Let $s_{\epsilon(-1)^r} = \tau_{p\delta,n}$ and $s_{-\epsilon(-1)^r} = s \in S^p(\delta)(E, K, \ell^n)^{-\epsilon(-1)^r}$ from proposition 6.0.19. Then from proposition 6.0.16, there is $q \in \Lambda^1_{n''}$ satisfying the following two conditions. Let $\epsilon_i(\tau_{qp\delta,n}) = x_i e_{(-1)^r\epsilon\ell^n}$ and $\frac{Fr_i^2-1}{\ell^n}s = s_i \cdot e_{(-1)^r\epsilon\ell^n}$ where $i = p, q$, $x_i \in \mathbb{Z}/\ell^n$. Then q satisfies

- $\#\tau_{p\delta,n}(q) \leq \#\tau_{p\delta,n} \leq \#\tau_{p\delta,n}(q) + e \Rightarrow ord_\ell(x_q) \leq e + m(p\delta)$
- $\#s(q) \leq \#s = n \leq \#s(q) + e \Rightarrow ord_\ell(s_q) = n - \#s(q) \leq e$

Let $\zeta_{\ell^n} = \zeta^{y_k}_{\ell^n,i}$ with $y_k \in (\mathbb{Z}/\ell^n)^*$

Because $s \in S^p(\delta)(E, K, \ell^n)^{-\epsilon(-1)^r}$ and $\tau_{pq\delta,n} \in S(pq\delta)(K, \ell^n)^{-\epsilon(-1)^r}$,

by global class field theory, we have the following orthogonal relation[4].

$$\sum_{i=p,q} < s, \tau_{pq\delta,n} >_{E,K,i,n} = 0$$

From $[e_+, e_-] = \zeta_{\ell^{n-1}} = \zeta^\ell_{\ell^n}$, we have

$$[\frac{Fr_i^2 - 1}{\ell^n}s, e_{(-1)^{r-1}\epsilon\ell^n}]^{y_i\cdot x_i}_{\ell^n} = *\zeta^{\ell s_i y_i x_i}_{\ell^n}$$

[4]page 480 in [5]

with $i = p, q$. From proposition 5.1.1,

$$\zeta_{n,i}^{<s,\tau_{pq\delta,n}>_{E,K,i,n}} = [\frac{Fr_i^2 - 1}{\ell^n} s, (-1)^{k+1}\epsilon \cdot \frac{Fr_i^2 - 1}{\ell^n} \tau_{pq\lambda/i,n}]_{E,K,n}$$

where $i = p, q$.

So we have

$$\ell^1 \cdot s_p \cdot x_p \equiv -\ell^1 \cdot s_q \cdot x_q \mod \ell^n$$

Because $1 \leq 1 + ord_\ell(s_q \cdot x_q) \leq 1 + 2e + m(p\delta) < n$,

$$1 \leq 1 + ord_\ell(s_p \cdot x_p) < n$$

and

$$ord_\ell(s_p) + ord_\ell(x_p) = ord_\ell(s_q) + ord_\ell(x_q)$$

$$n - m(q\delta) = \#\tau_{q\delta,n} \geq \#\tau_{q\delta,n}(p) = \#\tau_{qp\delta,n}(p) = n - ord_\ell(x_p)$$

implies $m(q\delta) \leq ord_\ell(x_p)$, so we can conclude that

$$m(q\delta) \leq ord_\ell(s_p) + ord_\ell(x_p) = ord_\ell(s_q) + ord_\ell(x_q) \leq e + e + m(p\delta)$$

and

$$m(q\delta) - m(p\delta) \leq 2e$$

□

Remark 6.0.21 *To use proposition 6.0.20, we need two conditions*

$$n' \geq m + 1 + n \text{ and } n > 1 + 2e + m(p\delta)$$

with $p\delta \in \Lambda^{r+1}_{n'}$.

Now let's assume we have $p_1 \cdot p_2 \dots p_k\delta' \in \Lambda^r_{n'}$ *and we want to switch it to* $q_1 \cdot q_2 \dots q_k\delta'$ *by repeating proposition 6.0.20 k-times.*

$m(q_1 \cdot q_2 \dots q_i \cdot p_{i+1} \dots p_k\delta') - m(q_1 \cdot q_2 \dots q_{i-1} \cdot p_i \dots p_k\delta') \leq 2e$ *implies* $m(q_1 \cdot q_2 \dots q_k\delta') - m(p_1 \cdot p_2 \dots p_k\delta'(\in \Lambda^r_{n'})) \leq 2ke$. *So we need these conditions.*

$$n' \geq m + 1 + n \text{ and } n > 1 + 2ke + m(p_1 \cdot p_2 \dots p_k\delta'(\in \Lambda^r_{n'}))$$

Proposition 6.0.22

$$s(r) > m + 2re + 2 \Rightarrow s(r) = \infty$$

Proof Because there is λ such that $(s(r) \geq)n(\lambda) - m(\lambda) > 2 + m + 2e \cdot r$, by applying proposition 6.0.20 r-times, we have $\lambda' \in \Lambda^r_{n''}$. Because we can increase n'' as many as we want, we can conclude $s(r) > m + 2re + 2 \Rightarrow s(r) = \infty$. $\square$

Proposition 6.0.23 *(Key proposition, from theorem 3 in [6]) Let* $n' > m + 4 + 2e(f-1) + n$ *and* $n > (f+2)(4fe + \overline{m} + 1) + e(f+4) + 1$. *There are*

$p_1, p_2, \ldots, p_{2f+1} \in \Lambda^1_{n'}$ *satisfying the following conditions.*

(R1) M *is upper-triangular and* $ord_\ell(M_{i,i}) \leq e + 1 + 4fe + \overline{m}$

(R2) $rank_{n-(4fe+\overline{m}+1)}(< \eta_i >_{i=1,\ldots,f+1}) = f + 1$ *where* $n > (f+2)(4fe + \overline{m} + 1) + e(f+1)$

(R3) $\tau_{\lambda_i,n} \in S_{(-1)^f \epsilon \ell^n}$

Proof The proof is analogous to the proof of theorem 3 in [6]. Because we have a fudge factor e when $\ell = 2$ and $\eta_i := \tau_{\lambda_i,n}$, our result is much weaker than original theorem. To show how to handle e, we will write a detail proof.

(Construction of λ_i and η_i)

By the following the proof of theorem 3 in [6], let us construction λ_i and η_i with $i = 1, \ldots, f+1$. From the conjecture 1.0.9 and remark 5.2.2, there is $\lambda = p_0 p'_1 \ldots p'_f \in \Lambda^f_{\overline{n}}$ such that $m(\lambda) = \overline{m}$. We repeat proposition 6.0.20 f-times to replace λ with $\lambda_1 := p_0 \cdot p_1 \ldots p_f \in \Lambda^f_{n''}$. Now we repeat proposition 6.0.20 f-times again by choosing p_{f+i} from proposition 6.0.20 with $p = p_i$ and $\delta = p_{i+1} \ldots p_{f+i-1}$ with $i = 1, \ldots, f$. We also choose p_{2f+1} from proposition 6.0.16 which is a part of theorem 10 in [5].

(Local properties of η_i)

By definition of f, $n' > n + m + 2(f-1)e + 2$ and proposition 6.0.22,

$\tau_{\lambda,n} = \alpha(n, n+m+2(f-1)e+2)^{-1}\left(\ell^{m+2(f-1)e+2}\tau_{\lambda,n+m+2(f-1)e+2}\right) = 0$ for $\forall\lambda \in \Lambda_{n'}^{f-1}$.

For λ_i and $k = i, \ldots, f+i-1$, from corollary 5.1.5

$$0 = \#\tau_{\lambda_i/p_k,n} \geq \#\tau_{\lambda_i/p_k,n}(p_k) = \#\tau_{\lambda_i,n}(p_k) \tag{6.0.1}$$

(R1 - M is upper-triangular and $ord_\ell(M_{i,i}) \leq e+1+4fe+\overline{m}$)

From (6.0.1), if $j < i$, then

$$\#M_{i,j} = \#\log_\ell(\chi_{p_{f+j}}(\tau_{\lambda_i,n})) = max\{\#\tau_{\lambda_i,n}(p_{f+j}) - 1, 0\} = 0 \tag{6.0.2}$$

So M is upper triangular.

Now let us prove $ord_\ell(M_{i,i}) \leq e+1+4fe+\overline{m}$. Because $m(\lambda_i) - m(\lambda_1) \leq 2e(i-1)$ and $m(\lambda_1) - \overline{m} \leq 2ef$ from proposition 6.0.20,

$$\#\eta_i = n - m(\lambda_i) \geq n - (4ef + \overline{m}) \tag{6.0.3}$$

From proposition 6.0.20 and (6.0.3),

$$\#\eta_i \leq \#\eta_i(p_{f+i}) + e \Rightarrow \#\eta_i(p_{f+i}) \geq n - (4fe+\overline{m}) - e > 0 \tag{6.0.4}$$

From claim 6.0.17,

$$\#M_{i,i} = max\{\#\eta_i(p_{f+i}) - 1, 0\} \geq n - (4fe+\overline{m}) - e - 1$$

So we can conclude

$$ord_\ell(M_{i,i}) \leq e + 1 + 4fe + \overline{m} \tag{6.0.5}$$

(R2 - Rank of $< \eta_i >_{i=1,\ldots,f+1}$)

For simplicity, let $\beta = e + 1 + 4fe + \overline{m}$. First, we will prove η_i is linearly-independent up to some torsions which are universally annihilated[5].

Suppose $\sum_{i=1}^{f+1} \alpha_i \eta_i = 0 \ (mod\ \ell^n)$ with $\alpha_i \in \mathbb{Z}/\ell^n$. Then we will prove the following inequality.

$$\#\alpha_i \leq \beta(f + 2 - i) \tag{6.0.6}$$

From $\chi_{p_{2f+1}}(\sum \alpha_i \eta_i) = 0$, we have $\alpha_{f+1} M_{f+1,f+1} = 0(\mod \ell^n)$ because of (6.0.2). From (6.0.5), we have the following inequality.

$$ord_\ell(\alpha_{f+1}) \geq n - \beta \ and \ \#\alpha_{f+1} \leq \beta$$

Now we will do induction on i reversely. Assume the inequalities (6.0.6) for $i = k+1, \ldots, f+1$ are true. From $\chi_{p_{f+k}}(\sum \alpha_i \eta_i) = 0$, we have

$$\alpha_k M_{k,k} + \alpha_{k+1} M_{k+1,k} + \ldots \alpha_{f+1} M_{f+1,k} = 0(\mod \ell^n)$$

If we multiply both sides by $\ell^{\beta(f+1-k)}$, by the induction, we get

$$\ell^{\beta(f+1-k)} \alpha_k M_{k,k} = 0(mod\ \ell^n)$$

[5]Here, universally means it is independent of n.

From (6.0.5), we can conclude

$$\#\alpha_k \leq \beta(f+2-k)$$

In particular, we have

$$\#\alpha_i \leq (e+1+4fe+\overline{m})(f+1) \tag{6.0.7}$$

Now we will prove the rank of η where $\eta =< \eta_i >_{i=1,\ldots,f+1}$.

Lemma 6.0.24

$$rank_{n-(4fe+\overline{m})-1}(< \eta_i >_{i=1,\ldots,f+1}) = f+1$$

where $n-(4fe+\overline{m})-1 > (e+1+4fe+\overline{m})(f+1)$.

Proof From (6.0.7), η_i are linearly independent in $\eta/\eta[\ell^{\beta(f+1)}]$. Since $\#\eta_i \geq n-(4ef+\overline{m})$(6.0.3), we can conclude

$$rank_{n-(4fe+\overline{m})-1}(\eta) = f+1$$

where $n-(4fe+\overline{m})-1 > (e+1+4fe+\overline{m})(f+1)$. □

(R3 $\eta_i \in S_{(-1)^f \epsilon \ell^n}$)

From proposition 5.0.10 and (6.0.1),

$$\eta_i := \tau_{\lambda_i,n} \in S_{(-1)^f \epsilon \ell^n}$$

□

Corollary 6.0.25 *(from theorem 10 in [5])* $\ell^{\alpha} K_i = 0 (i = 1, 2)$ *for* $\alpha > 0$ *which is independent of* n *and* $|K_i| < \infty$ *(independent of* n*).*

Proof The proof of theorem 10 in [5] (in the case r=2) proves equally the corollary 6.0.25 if simply we replace

- the Selmer groups $S_{\pm M}$ with the intersection of kernels of $\chi_{p_{f+1}}, \ldots, \chi_{p_{2f}}$ (in our notations) on them.
- $\lambda_0,\ \lambda_1,\ \lambda_2$ (in the notations of [5]) with $\lambda_{f+1},\ p_{2f+1},\ p_{2f+2}$ (in our notations)
- characters $\chi_{-\epsilon}$, $\chi_{\epsilon 2}$ corresponding to primes λ_1, λ_2 (in the notations of [5]) with characters $\chi_{p_{2f+1}}$, $\chi_{p_{2f+2}}$ corresponding to primes p_{2f+1}, p_{2f+2} (in our notations).

From theorem 10 in [5] with $r = 2$, we have

$$\#K_i \leq \mathfrak{m}_i + 2e \ (i = 1, 2)$$

where $\mathfrak{m}_i := m(p_{f+1} \cdot p_{f+2} \ldots p_{2f+i})$.

Let $\alpha = 4e(f + 1) + \overline{m} + 1$. Of course, α is independent of n. Because

$\mathfrak{m}_2 - \mathfrak{m}_1 \leq e$, $\mathfrak{m}_1 - m(\lambda_{f+1}) \leq e$ from corollary 6.0.18 and $m(\lambda_{f+1}) \leq 4ef + \overline{m}$ from proposition 6.0.20, we can conclude

$$\#K_i \leq \alpha$$

Namely,

$$\ell^\alpha K_i = 0 \tag{6.0.8}$$

Because $S_{\pm\ell^{\alpha+1}}[\ell^\alpha] = S_{\pm\ell^\alpha}$, it also implies $|K_i| < \infty$ (independent of n). $\square$

Definition 6.0.26 *($\widetilde{\chi}$) Let*

$$\widetilde{\chi_{(-1)^f\epsilon}} : S_{(-1)^f\epsilon\ell^n} \to (\mathbb{Z}/\ell^n)^{f+1}$$

with

$$\widetilde{\chi_{(-1)^f\epsilon}}(s) := \big(\chi_{p_{f+1}}(s), \chi_{p_{f+1}}(s), \ldots, \chi_{p_{2f+1}}(s)\big)$$

and

$$\widetilde{\chi_{(-1)^{f+1}\epsilon}} : S_{(-1)^{f+1}\epsilon\ell^n} \to (\mathbb{Z}/\ell^n)^{f}$$

with

$$\widetilde{\chi_{(-1)^{f+1}\epsilon}}(s) := \big(\chi_{p_{f+1}}(s), \chi_{p_{f+1}}(s), \ldots, \chi_{p_{2f}}(s)\big)$$

Now let's prove our main theorem.

Proof (Proof of Main theorem 1.0.11)

We have the following maps.

$$0 \longrightarrow K_1 \longrightarrow S_{(-1)^f \epsilon \ell^n} \xrightarrow{\widetilde{\chi_{(-1)^f}}_\epsilon} (\mathbb{Z}/\ell^n)^{f+1}$$

$$0 \longrightarrow K_2 \longrightarrow S_{(-1)^{f+1} \epsilon \ell^n} \xrightarrow{\widetilde{\chi_{(-1)^{f+1}}}_\epsilon} (\mathbb{Z}/\ell^n)^{f}$$

First, We also checked $|K_i| < \infty (independent\ of\ n)$ with $i = 1, 2$ from corollary 6.0.25. From lemma 6.0.24, $rank_{\mathbb{Q}_\ell/\mathbb{Z}_\ell}\big(\varinjlim_n (< \eta_i >_{i=1,\ldots,f+1})\big) = f + 1$.

So we can conclude that

$$rank_{\mathbb{Q}_\ell/\mathbb{Z}_\ell}\big(\varinjlim_n (S_{(-1)^f \ell^n})\big) = f + 1$$

and

$$rank_{\mathbb{Q}_\ell/\mathbb{Z}_\ell}\big(\varinjlim_n (S_{(-1)^{f+1} \ell^n})\big) \leq f$$

□

Chapter 7

Appendix

7.1 Size of $H^1(V'_{n'}|K, E[\ell^n])$

Proposition 7.1.1 *(Kolyvagin)*

$$H^1(G_n, E[2]) = \mathbb{Z}/2$$

for $n \geq 2$

Proof By proposition 14 in [4], we already know $H^1(G_n, E[\ell]) \subset \mathbb{Z}/2$. So we only check there is non-trivial elements in $H^1(G_2, E[\ell])(\subset H^1(G_n, E[\ell]))$. Recall $H^1(G_n, E[\ell]) \longrightarrow H^{\curvearrowright}(H_n, E[\ell])^{G_1} = Hom(H_n, E[\ell])^{G_1}$ and $H_2 \cong M2(\mathbb{Z}/2Z)$. Choose $\psi_0 : M_2(\mathbb{Z}/2\mathbb{Z}) \to E[\ell]$ such that

$$\psi_0 \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+d+b \\ a+d+c \end{pmatrix}$$

We can directly check $\psi_0 \in Hom(H_n, E[\ell])^{G_1}$. $\square$

Remark 7.1.2 *From proposition 14 in [4] and proposition 7.1.1*

$$H^1(G_n, E[2]) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & n \geq 2 \\ 0 & n = 1 \end{cases}$$

$$0 \longrightarrow H^1(G_n/D, E[2^n]^D) \longrightarrow H^1(G_n, E[2^n]) \longrightarrow H^1(D, E[2^n])^{G_n/D}$$

But $E[2^n]^D = E[2]$, $\{P \in E[2^n] | ((-I)+1)P = 0\} = E[2^n]$ *and*

$$H^1(D, E[2^n]) \cong E[2^n]/\big((-I)-1\big)E[2^n] \cong E[2^n]/2E[2^n] \cong E[2]$$

implies $H^1(D, E[2^n])^{G_n/D} \cong E[2]^{G_1} = 0$

$$0 \longrightarrow H^1(G_n/D, E[2]) \longrightarrow H^1(G_n, E[2]) \longrightarrow H^1(D, E[2])^{G_n/D} = 0$$

We can conclude

$$H^1(G_n, E[2]) \cong H^1(G_n, E[2^n])$$

So

$$H^1(G_n, E[2^n]) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & n \geq 2 \\ 0 & n = 1 \end{cases}$$

When $n' \geq n$ *from*

$$\longrightarrow H^0(G_n, E[2^{n'-n}]) = 0 \longrightarrow H^1(G_{n'}, E[\ell^n]) \longrightarrow \mathbb{Z}/2$$

[1] *and*

$$0 \longrightarrow H^1(G_n, E[2^n]) \cong \mathbb{Z}/2 \longrightarrow H^1(G_{n+1}, E[\ell^n])$$

[1] $H^0(G_n, E[2^{n'-n}]) = E(K)[2^{n'-n}] = 0$ and $H^1(G_{n'}, E[2^{n'}]) = \mathbb{Z}/2$

we con conclude

$$H^1(G_{n'}, E[2^n]) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & n' \geq 2 \text{ and } n' \geq n \geq 1 \\ 0 & n' = n = 1 \end{cases}$$

Bibliography

[1] Henri Darmon. *Rational points on modular elliptic curves*, volume 101 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[2] Benedict H. Gross. Kolyvagin's work on modular elliptic curves. In *L-functions and arithmetic (Durham, 1989)*, volume 153 of *London Math. Soc. Lecture Note Ser.*, pages 235–256. Cambridge Univ. Press, Cambridge, 1991.

[3] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $\mathrm{SH}(E, \mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[4] V. A. Kolyvagin. The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(6):1154–1180, 1327, 1988.

[5] V. A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 435–483. Birkhäuser Boston, Boston, MA, 1990.

[6] V. A. Kolyvagin. On the structure of Selmer groups. *Math. Ann.*, 291(2):253–259, 1991.

[7] V. A. Kolyvagin. On the structure of Shafarevich-Tate groups. In *Algebraic geometry (Chicago, IL, 1989)*, volume 1479 of *Lecture Notes in Math.*, pages 94–121. Springer, Berlin, 1991.

[8] V. A. Kolyvagin. Bounding Selmer groups via the theory of Euler systems. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*,

volume 17 of *CMS Conf. Proc.*, pages 233–248. Amer. Math. Soc., Providence, RI, 1995.

[9] Barry Mazur and Karl Rubin. Kolyvagin systems. *Mem. Amer. Math. Soc.*, 168(799):viii+96, 2004.

[10] Barry Mazur and Karl Rubin. Refined class number formulas and Kolyvagin systems. *Compos. Math.*, 147(1):56–74, 2011.

[11] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[12] Karl Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.

[13] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.