# Kolyvagin's Theorem

Weixiao Lu

September 27, 2022

## Contents



# 1 Introduction

Let's begin with the initial story of arithmetic of elliptic curve, the following famous Mordell-Weil theorem:

## 1.1 Mordell-Weil and Selmer Groups

**Theorem 1.1** (Mordell-Weil)**.** Let $F$ be a number field, $E/F$ be an elliptic curve, then $E(F)$ is a finitely generated abelian group.

The rank of free part of $E(F)$ is called **algebraic rank** or **Mordell-Weil rank** of $E$, denoted by $r_{\mathrm{alg}}(E)$. (Indeed, the theorem holds for any global field, but we will concentrate on the number field case)

The (traditional) proof of Mordell-Weil theorem has two steps:

- **Step 1:** Prove a weak version, so called "weak Mordell-Weil theorem".

- **Step 2:** Use height machine to deduce Mordell-Weil from weak Mordell-Weil.

While both steps become prototype of many other arguments, Step 1 is closely related to the topic today. So we will say more words on it. Let's first recall

**Theorem 1.2** (Weak Mordell-Weil)**.** For any positive integer $n$, $E(F)/nE(F)$ is a finite abelian group.

The idea is embed $E(F)/nE(F)$ into an abelian group which is easier to describe. Consider the exact sequence of discrete $G_F := \mathrm{Gal}(F^{\mathrm{sep}}/F)$-module (or étale sheaf)

$$0 \to E[n](\bar{F}) \to E(\bar{F}) \to E(\bar{F}) \to 0$$

Taking cohomology we get the Kummer map

$$\delta : E(F)/nE(F) \hookrightarrow H^1(F, E[n])$$

**Remark.** We use the usual notation that $H^i(F, M) := H^i(G_F, M)$. We also fix embeddings $\bar{F} \hookrightarrow \bar{F}_v$ for all place $v$, thus $G_{F_v}$ is regard as a subgroup of $G_F$ which is well-defined up to conjugacy.

We would hope that $H^1(F, E[n])$ is finite, which is, unfortunately always not. (e.g. when $E[n]$ is defined over $F$, $H^1(F, E[n]) = \mathrm{Hom}(G_F, (\mathbb{Z}/n\mathbb{Z})^2)$ which is infinite by global class field theory. However, by local class field theory, for any place $v$, $H^1(F_v, E[n])$ is finite. This motivates that we can find a finite subgroup inside $H^1(F, E[n])$ called **Selmer group** which is characterized by local condition, and turns out to be finite and contains image of $\delta$.

**Definition 1.3** (Selmer group)**.** Consider the following diagram:

$$\begin{array}{ccc} E(F)/nE(F) & \overset{\delta}{\hookrightarrow} & H^1(F, E[n]) \\ \downarrow & & \downarrow \mathrm{loc}_v \\ E(F_v)/nE(F_v) & \overset{\delta_v}{\hookrightarrow} & H^1(F_v, E[n]) \end{array}$$

Define the $n$-**Selmer group** to be

$$\mathrm{Sel}_n(E) = \{\alpha \in H^1(F, E[n]) | \mathrm{loc}_v(\alpha) \in \mathrm{im}(\delta_v) \text{ for any place } v\}$$

**Proposition 1.4.** $\mathrm{Sel}_n(E)$ is a finite abelian group.

In order to prove it, let's take this opportunity to introduce some important concept.
Let $M$ be a finite discrete $G_F$ module, and $v$ is place of $F$ such that $|M|$ and $q_v$ are coprime.
We have the following inflation-restriction sequence

$$0 \to H^1(F_v^{\mathrm{ur}}/F_v, M^{I_v}) \to H^1(F_v, M) \to H^1(I_v, M)^{\mathrm{Gal}(F_v^{\mathrm{ur}}/F_v)} \to H^2(F_v^{\mathrm{ur}}/F, M^{I_v})$$

Note that $\mathrm{Gal}(F_v^{\mathrm{ur}}/F_v)$ is topologically generated by Frob and has cohomological dimension 1. We actually have

$$0 \to H^1(F_v^{\mathrm{ur}}/F_v, M^{I_v}) \to H^1(F_v, M) \to H^1(I_v, M)^{\mathrm{Frob}=1} \to 0$$

**Definition 1.5.** Assume $q_v$ and $|M|$ are coprime. Define the **finite part** or **unramified part** of $H^1(F_v, M)$ to be

$$H^1_f(K_v, M) := H^1(K_v^{\mathrm{ur}}, M)$$

The quotient $H^1(I_v, M)^{\mathrm{Frob}=1}$ is called the **singular part**. Denoted by $H^1_s(F_v, M)$.

We can then introducte Selmer structure

**Definition 1.6.** Let $M$ be a finite discrete $G_F$ module, A **Selmer structure** for $M$ is a collection of subgroup $\mathcal{L}_v \subset H^1(F_v, M)$ such that $\mathcal{L}_v = H^1_f(K_v, M)$ for almost all $v$.

**Proposition 1.7.** For elliptic curve $E$ over $F$, $\mathcal{L}_v = \mathrm{im}(\delta_v)$ is a Selmer structure. That is $\mathrm{im}(\delta_v) = H^1_f(K_v, E[n])$ for almost all place $v$ of $F$.

*Sketch of the Proof.* We show that when $E$ has good reduction at $E$, then $\mathrm{im}(\delta_v) = H^1_f(F_v, E[n])$.
Using Néron model $\mathcal{E}$, we get exact sequence of étale sheaves

$$0 \to \mathcal{E}[n] \to \mathcal{E} \to \mathcal{E} \to 0$$

Take long exact sequence of étale cohomology, using the fact that $\mathcal{E}(\mathcal{O}_v) = E(F_v)$ and $H^1(\mathcal{O}_v, \mathcal{E}) = H^1(k_v, E_v) = 0$. where $k_v$ is the residue field. □

From a Selmer structure, one can introduce Selmer groups

**Definition 1.8.** Let $\mathcal{L}$ be a Selmer structure for $M$, define **Selmer group** of $\mathcal{L}$ to be

$$H^1_{\mathcal{L}}(F, M) = \{\alpha \in H^1(K, M) | \mathrm{loc}_v(\alpha) \in \mathcal{L}_v \text{ for all } v\}$$

**Proposition 1.9.** For any Selmer structure $\mathcal{L}$,$H^1_{\mathcal{L}}(F, M)$ is finite.

*Sketch of the proof.* After passing to finite extension (using inflation-restriction sequence), we can assume the action of $G_F$ on $M$ is trivial. Then it follows from the fact that, for any number field $F$, the maximal unramified abelian extension of index $n$ is finite over $F$ for any integer $n$. □

**Corollary 1.10.** Weak Mordell-Weil theorem 1.2 holds.

$n$-Selmer group also has close relationship with $n$-torsion part of Tate-Shafarevich group, which we recall now

**Definition 1.11.** Define $Ш(E) = \{\alpha \in H^1(F, E) | \mathrm{loc}_v(\alpha) = 0\}$ for all place $v$.

**Conjecture 1.12** (Tate-Shafarevich)**.** $|Ш(E)| < \infty$.

We have the following useful short exact sequence

$$0 \to E(F)/nE(F) \to \mathrm{Sel}_n(E) \to Ш(E)[n] \to 0$$

Which is easily deduce from the diagram with exact rows below

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(F)/nE(F) & \longrightarrow & H^1(F, E[n]) & \longrightarrow & H^1(F, E)[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(F_v)/nE(F_v) & \longrightarrow & H^1(F_v, E[n]) & \longrightarrow & H^1(F_v, E)[n] & \longrightarrow & 0
\end{array}$$

## 1.2 Birch-Swinnerton-Dyer

After Mordell-Weil, a natural question is how to understand $r_{\text{alg}}(E)$. Recall that for any ellptic curve over $F$ we have associated Hasse-Weil $L$-series:

$$L(E,s) = L(\rho_E, s) = \prod_v L_v(E,s)$$

where $L_v(E,s) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}$ when $E$ has good reduction at $v$ and $L_v(E,s) = (1 - a_v q_v^{-s})^{-1}$ when $E$ has bad reduction at $v$.

**Theorem 1.13** (Wiles,Taylor-Wiles,Breuil-Conrad-Diamond-Taylor)**.** Assume conductor of $E$ is $N$, then $L(E,s) = L(f,s)$ for a newform of weight 2 and level $\Gamma_0(N)$. In particular,$L(E,s)$ has analytic continuation to $\mathbb{C}$ and a functional equation $L(E,s) \leftrightarrow \epsilon L(E, 2-s)$,$\epsilon \in \{\pm 1\}$ is the **sign** of E.

Equivalently, there is a non-trivial morphism $X_0(N) \to E$, such morphism is called a **modular parametrization**

Conjecturally, this generalize to

**Conjecture 1.14** (Modularity)**.** There is a cuspidal automorphic representation of $\pi$ $\mathrm{GL}_2(\mathbb{A}_F)$ with same conductor of $E$ such that $L(E,s) = L(\pi, s)$. In particular, $L(E,s)$ has analytic continuation to $\mathbb{C}$.

Denote $r_{\text{an}}(E) = \text{ord}_{s=1} L(E,s)$, called the **analytic rank** of $E$, by some numerical evidence, Birch and Swinnerton-Dyer formulate the following conjecture

**Conjecture 1.15** (Birch-Swinnerton-Dyer)**.** Let $E$ be an elliptic curve over $F$, then $r_{\text{alg}}(E) = r_{\text{an}}(E)$

## 1.3 Gross-Zagier and Kolyvagin

By combining the work of Gross-Zagier and Kolyvagin, we have the following theorem:

**Theorem 1.16** (Gross-Zagier,Kolyvagin)**.** For $E$ over $\mathbb{Q}$ and $k \in \{0,1\}$,If $r_{\text{an}}(E) = k$ then $r_{\text{alg}}(E) = k$ and $|\text{Ш}(E)| < \infty$

The key is to relate both $r_{\text{alg}}(E)$ and $r_{\text{an}}(E)$ with the Selmer group, we will explain this in next section with more details.

## 1.4 Bloch-Kato

Now we fix a prime $p$, we get the exact sequence

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \text{Sel}_p(E) \to \text{Ш}(E)[p] \to 0$$

The first term is related to algebraic rank (up to a finite group), and the third term is conjecturally zero (up to a finite group), we can eliminate finite group, by consider for all $n$, the exact sequence

$$0 \to E(\mathbb{Q})/p^n E(\mathbb{Q}) \to \text{Sel}_{p^n}(E) \to \text{Ш}(E)[p^n] \to 0$$

The take colimit

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E) \to Ш(E)[p^\infty] \to 0$$

Define $r_p(E) = \mathrm{corank}(\mathrm{Sel}_{p^\infty}(E))$, then if $|Ш(E)[p^\infty]| < \infty$, then $r_p(E) = r_{\mathrm{alg}}(E)$.

**Conjecture 1.17** (Bloch-Kato)**.** $r_p(E) = r_{\mathrm{an}}(E)$.

Thus, if Tate-Shafarevich conjecture holds, then Bloch-Kato conjecture would imply BSD conjecture. And Bloch-Kato conjecture has a vast generalization to all pure geometric $p$-adic Galois representations.

**Remark.** Instead of taking colimit, one can also take limit and get another version of $\mathrm{Sel}_{p^\infty}(E)$. Which can be recovered from Tate module of $E$ by a theorem of Bloch-Kato.

# 2 Overview of Kolyvagin's work

### Notations

Now we will fix the notation:

- $E$ is an elliptic curve ovre $\mathbb{Q}$ with conductor $N$.
- $K$ is an imaginary quadratic field with discriminant $-D$ and $\mathcal{O}_K^\times = \{\pm 1\}$. We assume $K$ and $N$ satifies the Heegner hypothesis: any prime $p$ divides $N$ split in $K$. (in particular, $N$ and $D$ are coprime.) By Chebaterov density, for a fixed $N$ there is infinitely many such $K$.
- $\mathcal{O}_n$ be the order of conductor $n$. And $K_n$ will be the corresponding ring class field, $\mathcal{N}_n = \mathcal{O}_n \cap \mathcal{N}$
- Denote $G_n$ to be the Galois group $\mathrm{Gal}(K_n/K_1) \cong (\mathcal{O}_K/n\mathcal{O}_K)^\times/(\mathbb{Z}/n\mathbb{Z})^\times$

  Indeed, we have the exact sequence

  $$1 \to (\mathbb{Z}/n)^\times \to (\mathcal{O}_K/n\mathcal{O}_K)^\times \to I_{K,n} \cap P_K/P_{K,\mathbb{Z}}$$
- $p$ will be a prime number which we will concentrate on $H^1(K, E[p])$ or $\mathrm{Sel}_p(E)$ later.
- $\ell$ will be other specified prime (Kolyvagin prime), which we will use such $\ell$ to bound Selmer group.

## 2.1 Heegner points

Suppose now we have an elliptic curve over $\mathbb{Q}$, with $r_{\mathrm{an}}(E) = 1$, we want to show $r_{\mathrm{alg}}(E) = 1$. That is $E(\mathbb{Q}) = \mathbb{Z} \oplus \{\text{finite abelian group}\}$. Thus, we first need to know that $E(\mathbb{Q})$ contains a copy of $\mathbb{Z}$ in it. That is, we need to construct a non-torsion point. How to find rational points on elliptic curve? The Heegner points provide an answer.

**Theorem 2.1** (Main theorem of complex multiplication)**.** Let $\mathcal{O} \subset K$ be an order, then there is a bijection

$$\{\text{elliptic curves over } \mathbb{C} \text{ with CM by } \mathcal{O}\}/\sim \longleftrightarrow \{\mathbb{C}/\mathfrak{a} | \mathfrak{a} \in \mathrm{Pic}(\mathcal{O})\}$$

And all these points are defined over the ring class field of $\mathcal{O}$.

Let $\mathcal{O}_n$ be the order of conductor $n$ and $\mathcal{N}_n = \mathcal{O}_n \cap \mathcal{N}$. For $n$ prime to $N$, $\mathcal{N}_n$ is an invertible $\mathcal{O}_n$ module with $\mathcal{O}_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$. (since $\mathcal{N}_n = \prod(\mathfrak{p}^i \cap \mathcal{O}_n)$.)

Thus $\mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathcal{N}^{-1}$ is a cyclic isogeny of degree $N$, which defines a point on $X_0(N)(\mathbb{C})$, by the main theorem of complex multiplication, it indeed lines in $X_0(N)(K_n)$. Denote this point by $x_n$. Using the modular parametrization $\varphi : X_0(N) \to E$, we get a point $y_n := \varphi(x_n) \in E(K_n)$. These are called **Heegner points**.

In particular, $y_1 \in E(K_1)$, where $K_1$ is the Hilbert class field of $K$. Define $y_K = \mathrm{Tr}_{K_1/K}(y_1) = \sum_{\sigma \in \mathrm{Gal}(K_1/K)} \sigma(y_1) \in E_0(K)$. We have the famous Gross-Zagier formula

**Theorem 2.2** (Gross-Zagier)**.**

$$L'(E_K, 1) \sim \hat{h}(y_K)$$

As a corollary,

**Corollary 2.3.** If $\mathrm{ord}_{s=1} L(E_K, s) = 1$ then $r_{\mathrm{alg}}(E_K) \geq 1$.

The work of Kolyvagin gives another direction of this equality.

**Remark.** The corollary is about the rank of $E$ over $K$, thus not the same as that stated in 1.16. We will come back later to see how to deduce theorem 1.16 from the theorem over $K$.

## 2.2 Kolyvagin's theorem

Following [Gro91], we will prove a weak version of Kolyvagin's theorem

**Theorem 2.4** (Prop. 2.1 of [Gro91])**.** Let $p$ be an odd prime such that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, and $p$ does not divide $y_K$ in $E(K)$, then

(1) $r_{\mathrm{alg}}(E_K) = 1$.

(2) $Ш(E_K)[p] = 0$

**Remark.**
- With the same idea but more intricate argument, Kolyvagin proves $Ш(E/K)$ is finite.
- A theorem of Serre states that for almost all $p$, $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

To prove the theorem 2.4, one first makes the following observation

**Lemma 2.5.** Assume $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, then $E(K)[p] = 0$.

*Proof.* Note that $\mathbb{Q}(E[p])$ and $K$ are linearly disjoint, since they have different set of ramified primes. Thus $\mathrm{Gal}(K(E[p])/K) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Thus $E[p](K) \neq 0$ will yield a contradiction (fixing a line). □

Recall that we have the short excat sequence

$$0 \to E(K)/pE(K) \to \mathrm{Sel}_p(E/K) \to Ш(E/K)[p] \to 0$$

From the lemma above, $r_{\mathrm{alg}}(E/K) = \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K)$. Thus we are reduced to prove that $E(K)/pE(K) \to \mathrm{Sel}_p(E/K)$ is an isomorphism. Indeed, we show

**Proposition 2.6.** Let $p$ as in Theorem 2.4, then $\mathrm{Sel}_p(E/K)$ is cyclic and generated by $\delta y_K$.

The method to prove Proposition 2.6 is as follows:

$$\text{CM points} \longrightarrow \text{Coh. class with controlled ramification} \xrightarrow{\text{Tate duality}} \text{bound } \mathrm{loc}_\ell \mathrm{Sel}_p \xrightarrow{\text{Chebaterov density}} \text{bound } \mathrm{Sel}_p$$

More precisely, from the Heegner points $y_n$, we will construct a cohomology class $c(n) \in H^1(K, E[p])$ with controlled ramification for good $n$: firstly, we define an operator $D_n$ called **Kolyvagin derivative**. It has the properties that $\delta(D_n y_n) \in H^1(K_n, E[p])^{G_n}$. Thus, taking avarage if $D_n y_n$, we arrive at an element in $H^1(K_n, E[p])^{\mathcal{G}_n}$, which turns out to be isomorphic $H^1(K, E[p])$. Hence get $c(n)$.

The $c(n) \in H^1(K, E[p])$ has the properties that it lies in the **relaxed Selmer group**. Which means that it lies at almost all local Selmer group (i.e. has controlled ramification).

Assume now we have $c(n)$, we then need a global argument to bound Selmer group.

Then from $c(n)$, by some global duality argument, we control $\mathrm{Sel}_p$ hence prove Proposition 2.6.

# 3 Euler System Relation

We now start with the actual proof of the theorem. We will discuss some parts of the proof, and remaining will be settled by next talk by Mikeyal. We start with the relations between the Heegener points.

## 3.1 Kolyvagin prime

As mentioned, we will define the cohomology class $c(n)$ for good $n$, now we specified such $n$.

**Definition 3.1** (Kolyvagin prime)**.** A prime number $\ell$ is called a **Kolyvagin prime** if $\ell$ does not divide $NDp$ and $\mathrm{Frob}(\ell) = \mathrm{Frob}(\infty) \in \mathrm{Gal}(K(E_p)/\mathbb{Q})$.

Equivalently, this means $\tau \in \mathrm{Frob}(\ell)$, where $\tau$ is a complex conjugation.

**Remark.** Since $\ell$ not divide $pN$, $K(E_p)/K$ is unramified at $\ell$. Thus $\ell \not| pDN$ implies $K(E_p)/\mathbb{Q}$ is unramified at $\ell$. Also, we have $E$ has good reduction at $\ell$.

By definition and Chebaterov density, there are infinitely many Kolyvagin prime.

**Proposition 3.2.** Kolyvagin prime $\ell$ has the following properties:

(1) $\ell$ is inert in $K$.

(2) $p|\ell+1$ and $p|a_\ell$.

*Proof.* (1) $\mathrm{Frob}(\ell)|_K$ is complex conjugation on $K$, thus $\ell$ is inert.

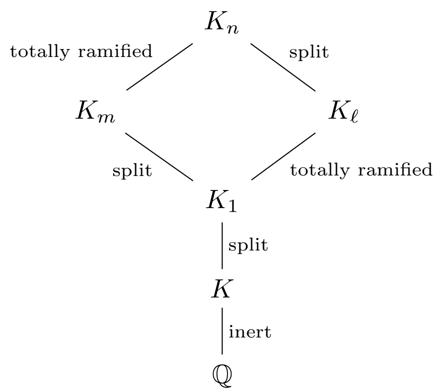
(2) We have $\mathrm{Frob}(\ell) = \mathrm{Frob}(\infty)$ in $\mathbb{Q}(E[p])/\mathbb{Q}$. So they have same characteristic polynomial. Charateristic polynomial of $\mathrm{Frob}(\ell)$ is $x^2 - a_\ell x + \ell$ and characteristic polynomial of complex conjugation is $x^2 - 1$. Since it acts semisimply on Tate moule with sqaure identity and determinant $-1$ (the cyclotomic character)

□

From now on, we assume $n$ is a product of distinct Kolyvagin prime, and use conductor of order $n$ to construct cohomology class $c(n)$.

We begin with some preliminaries on the fields $K_n$.

**Lemma 3.3.** Let $n$ be product of distinct Kolyvagin prime, write $n = \ell m$ with $\ell$ prime. The we have following field diagram.




which described the ramification behavior of $\ell$.

In particular $K_m \cap K_\ell = K$ thus $G_n \cong G_m \times G_\ell$.

*Proof.* We have observed before that $\ell$ is inert in $K/\mathbb{Q}$.

By definition of ring class group, the Artin map gives an isormophism $\mathrm{Pic}(\mathcal{O}_n) \to \mathrm{Gal}(K_n/K)$, which maps a prime $\mathfrak{p}$ to $\mathrm{Frob}(\mathfrak{p})$ when $\mathfrak{p}$ is prime to conductor. However, since $(\ell)$ is principal, so it maps to the trivial element. Thus $\ell$ split in $K_m$.

Finally, since $K_1/K$ is the maximal unramified abelian extension. The ramification index of $\ell$ in $K_\ell$ must be $[K_\ell : K_1]$ (otherwise, since $K_\ell/K$ is unramified outside $\ell$, we will have unramified abelian extension of larger degree.) □

**Remark.** In the above proof, we only use the fact that $\ell$ is inert in $K$.

By result above, we know $G_\ell = (\mathcal{O}_K/\ell\mathcal{O}_K)^\times/(\mathbb{Z}/\ell\mathbb{Z})^\times \cong \mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times$ is a cyclic group of order $\ell+1$, denote $\sigma_\ell$ a generator of it.

## 3.2 Euler System Relation

Define $\mathrm{Tr}_\ell = \sum_{\sigma \in G_\ell} \sigma \in \mathbb{Z}[G_\ell]$. For $x \in E(K_n)$ with $n = m\ell$, $\mathrm{Tr}_\ell$ is a well-defined element in $E(K_m)$.

The **Euler system relation** is the relation connecting Heegner points $y_n$ (Heegner points of different conductor.)

**Proposition 3.4** (Euler system relation)**.** For $n = m\ell$, where $\ell$ is inert in $K$ and $\ell$ does not divide $m$.

(1) $\mathrm{Tr}_\ell y_{m\ell} = a_\ell y_m \in E(K_m)$.

(2) Let $\lambda_n$ be any prime of $K_n$ over $\ell$, $y_n \equiv \mathrm{Frob}(y_m) \pmod{\lambda_n} \in \bar{E}(\kappa(\lambda_n))$

*Proof.* (1) Let's recall that as a consequence of main theorem of complex multiplication, the action of $\sigma \in \mathrm{Gal}(K_n/K)$ on $x_n \in X_0(K_n)$ is given by

$$\sigma x_n = (\mathbb{C}/\mathfrak{a}_\sigma^{-1}, \mathbb{C}/\mathcal{N}^{-1}\mathfrak{a}_\sigma^{-1})$$

where $\mathfrak{a}_\sigma$ is the invertible ideal of $\mathcal{O}_n$ under the Artin map.

Then, using definition of $T_\ell$ and check using complex uniformization yields the equality of divisor on $X_0(N)$:

$$T_\ell x_n = \mathrm{Tr}_\ell x_m$$

Apply $\varphi$ then get the result.

(2) By (1), in $E_\kappa(\lambda_n)$, the identity reduce to $(\ell+1)x_n = T_\ell x_m$ (since $K_n/K_m$ is totally ramified at $\ell$, so all Galois conjugate reduce to id). Then, using Eichler shimura correpondence, we get $(\ell+1)x_n = \mathrm{Frob}x_m + \ell\mathrm{Frob}^{-1}(x_m)$ as divisors(not diviosr class). In particular, we get (2).

□

# 4 Kolyvagin Derivative

How to use the Heegner points $y_n$ to produce cohomology class in $H^1(K, E[p])$? A naive try is simply take the trace: for $y_n \in E(K_n)$, use trace to produce an element in $E(K)$. However, by Euler system relations, it just gives $y_K$. Thus we need to modify them.

We seek to produce a cohomology class in $H^1(K_\ell, E[p)$ which is invariant by $G_\ell$ from the point $y_\ell$, that is, a class invariant under $\sigma_\ell$. If we try to solve the equation $(\sigma_\ell - 1)x = 0$ for $x \in \mathbb{Z}[G_\ell]$, we again arrive at $\mathrm{Tr}_\ell$. We need a modification of it.

**Definition 4.1.** Define **Kolyvagin derivative operator** as a solution of

$$(\sigma_\ell - 1)D_\ell = -\mathrm{Tr}_\ell + \ell + 1 \in \mathbb{Z}[G_\ell]$$

in $\mathbb{Z}[G_\ell]$ (Such $D_\ell$ exists, for example, one can take $D_\ell = \sum_{i=1}^{\ell} i \cdot \sigma_\ell^i$.)

In general, for $n$ a product of distinct Kolyavgin primes, define $D_n = \prod_{\ell|n} D_\ell$ in the decomposition $G_n \cong \prod G_\ell$.

**Proposition 4.2.** $D_n y_n \in E(K_n)/pE(K_n)$ is invariant under $G_n$.

*Proof.* It suffices to prove $(\sigma - 1)D_n y_n \in pE(K_n)$. Indeed, write $n = m\ell$, then

$$(\sigma_\ell - 1)D_n y_n = (\ell+1)D_m y_n - D_m(\mathrm{Tr}_\ell y_n) \in pE(K_n).$$

By the properites of Kolyvagin primes. □

$$
\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & H^1(K_n/K,E)[p] & & \\
 & & & & & & \downarrow{\scriptstyle \mathrm{Inf}} & & \\
0 & \longrightarrow & E(K)/pE(K) & \longrightarrow & H^1(K,E[p]) & \longrightarrow & H^1(K,E)[p] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\
0 & \longrightarrow & (E(K_n)/pE(K_n))^{\mathcal{G}_n} & \longrightarrow & H^1(K_n,E[p])^{\mathcal{G}_n} & \longrightarrow & H^1(K_n,E[p])[p]^{\mathcal{G}_n} & &
\end{array}
$$

Remark on action of complex conjugation:

**Proposition 4.3.** Let $\tau$ be a complex conjugation, then $y_n^\tau = \epsilon \cdot \sigma'(y_n) = E(K_n)/\{\text{torsion}\}$ for some $\sigma' \in \mathcal{G}_n$

**Proposition 4.4.** (1) $[P_n] \in \epsilon_n = \epsilon \cdot (-1)^{f_n}$ eigen space of $\tau$ for $(E(K_n)/pE(K_n))_n^{\mathcal{G}}$.

(2) $c(n)$ lies in $H^1(K, E[p])$

# References

[Gro91] Benedict H. Gross. *Kolyvagin's work for modular elliptic curves*, page 235–256. London Mathematical Society Lecture Note Series. Cambridge University Press, 1991.