Chapter 4
Kolyvagin's method

4.1 Eichler-Shimura construction

Let N a positive integer. We have seen that $\dim_{\mathbb{C}}(S_2(N)) = g$, where g is the genus of the compact Riemann surface $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H}^*$. Let $\mathbb{T}$ be the algebra generated by all Hecke operator T_n over $\mathbb{Z}$. In the proof of the rank of $\mathbb{T}$ over $\mathbb{Z}$ is g, we know $S_2(N)$ has a basis $f_1, \ldots, f_g$ whose coefficients of their q-expansions are integers.

From Jacobi-Abel's theorem (Ref. Forster O. Lecture Notes on Riemann Surface (GTM 81) §21), one knows that $H_1(X_0(N)(\mathbb{C}), \mathbb{Z})$ has dimension $2g$ over $\mathbb{Z}$, and when fixing any any basis $\omega_1, \ldots, \omega_g$ of $\Omega(X_0(N)(\mathbb{C}))$ (typically, fix a basis $f_1, \ldots, f_g$ of $S_2(N)$, then choose say) $\omega_j = 2\pi i f_j(z)dz$, $j = 1, \ldots, g$), we have

$$\Lambda_N := \left\{ \left(\int_\alpha \omega_1, \int_\alpha \omega_2, \ldots, \int_\alpha \omega_g \right) \middle| \, \alpha \in H_1(X_0(N)(\mathbb{C}), \mathbb{Z}) \right\}$$

is a lattice in $\mathbb{C}^g$.

Eichler-Shimura construction shows that for any normalized newform $f \in S_2(N)$ whose coefficients in its q-expansion are all integers, then f corresponds to an elliptic curve E_f such that $L(E_f, s) \doteq L(f, s)$, $\doteq$ means their Euler product coincide except finitely many primes (i.e. those primes $p \mid N$). E_f is quotient of the Jacobian $J_0(N)$ of $X_0(N)(\mathbb{C})$ with a subabelian variety A_f. Some preparation is needed before we can show such construction.

• **Universal property of the quotient of abelian varieties.** Let A be an abelian variety and C be an abelian subvariety of C. Then A/C is defined as an abelian variety in the following sense: There exists an abelian variety A' and a surjective homomorphism $f : A \to A'$ whose kernel is C. Moreover, any homomorphism $g : A \to A''$ of abelian varieties such that $C \subseteq \ker g$, $\exists h : A' \to A''$ such that the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "g"'] & A' \arrow[d, dashed, "h"] \\ & A'' \end{tikzcd}$$

(A', f) is unique up to isomorphism and if A and C are defined over $\mathbb{Q}$, then A' and F are also defined over $\mathbb{Q}$.

• **Universal property of $X \to J(X)$.** Let X be a compact Riemann surface of genus g with its Jacobian $J(X)$. Fix a base point x_0 in X to obtain a canonical map $\overline{\Phi} : X \to J(X)$ with the following universal property: for any homomorphic map $F : X \to T$ for any complex torus (i.e. $\mathbb{C}^n/\Lambda$), we have the following diagram:

$$\begin{tikzcd} X \arrow[r, "\overline{\Phi}"] \arrow[dr, "F"'] & J(X) \arrow[d, dashed, "f"] \\ & T \end{tikzcd}$$

where f is a holomorphic homomorphism satisfying

$$F = f \circ \overline{\Phi} + F(x_0).$$

• Since $J_0(N) = \mathbb{C}^g/\Lambda_N$ is an abelian variety, the set of left invariant vector spaces of $J_0(N)$ can be identified with the tangent space $\mathfrak{J}$ at origin O of $J_0(N)$, which is isomorphic to $\mathbb{C}^g$. Distinct element in $\mathrm{End}(J_0(N))$ gives a distinct linear homomorphism on $\mathfrak{J} \cong \mathbb{C}^g$. Hence one has

$$\mathrm{End}(J_0(N)) \hookrightarrow M_g(\mathbb{C}).$$

• We know canonically $\mathfrak{J} \cong \mathrm{Hom}_{\mathbb{C}}(\Omega(J_0(N)), \mathbb{C}) = \Omega(J_0(N))^*$. Use $z_1, \ldots, z_g$ as coordinates on $J_0(N)$, then

$$\Omega(J_0(N)) = \oplus_{j=1}^{g} \mathbb{C} dz_j.$$

One has a pairing:

$$< dz_i, e_j >= \delta_{ij},$$

where δ_{ij} is the Kronecker's δ and $e_1, \ldots, e_g$ are the standard basis of $\mathbb{C}^g$. [or more generally, define $< u, v >= v(u)$ for any $u \in \Omega(J_0(N))$ and $v \in \mathfrak{J}$, regarding $\mathfrak{J}$ as dual of $\Omega(J_0(N))$ over $\mathbb{C}$.]

• For any $\alpha \in \mathrm{End}(J_0(N))$, define α^* to be an endomorphism of $\Omega(J_0(N))$ by

$$< \alpha^*(u), v >=< u, (d\alpha)v >, \ \forall u \in \Omega(J_0(N)),\ v \in \mathfrak{J}.$$

[This makes sense as follows: for any endomorphism $\alpha : J_0(N) \to J_0(N)$, it induces map $\mathcal{O}_{J_0(N),\alpha(0)} \to \mathcal{O}_{J_0(N),0}$, which in turns induces map

$$\alpha^* : \mathcal{M}^2_{J_0(N),\alpha(0)}/\mathcal{M}_{J_0(N),\alpha(0)} = \Omega(J_0(N)) \to \mathcal{M}^2_{J_0(N),0}/\mathcal{M}_{J_0(N),0} = \Omega(J_0(N)).$$

α^* also induces the map $d\alpha$:

$$d\alpha : \mathrm{Hom}_{\mathbb{C}}(\mathcal{M}^2_{J_0(N),0}/\mathcal{M}_{J_0(N),0}, \mathbb{C}) = \mathfrak{J} \to \mathrm{Hom}_{\mathbb{C}}(\mathcal{M}^2_{J_0(N),\alpha(0)}/\mathcal{M}_{J_0(N),\alpha(0)}, \mathbb{C}) = \mathfrak{J},$$

by for any $v \in \mathrm{Hom}_{\mathbb{C}}(\mathcal{M}^2_{J_0(N),0}/\mathcal{M}_{J_0(N),0}, \mathbb{C})$,

$$d\alpha(v)(u) = v(\alpha^* u),\ \forall u \in \mathcal{M}^2_{J_0(N),\alpha(0)}/\mathcal{M}_{J_0(N),\alpha(0)},$$

i.e.

$$< \alpha^* u, v >=< u, (d\alpha)v > .$$

• Define Φ as follows:

$$\Phi : \mathcal{H}^* \xrightarrow{\pi} \Gamma_0(N)\backslash\mathcal{H}^* \xrightarrow{\overline{\Phi}} J_0(N).$$

Put $\pi^*(\omega_j) = f_j(z)dz$, then $f_1, \ldots, f_g$ is a basis for $S_2(N)$.

One can easily verify $\Phi^*(dz_j) = f_j(z)dz$.

$$< \Phi^*(dz_j), \frac{d}{dz} >=< dz_j, d\Phi(\frac{d}{dz}) =< dz_j, \begin{pmatrix} f_1(z) \\ \vdots \\ f_g(z) \end{pmatrix} >= f_j(z)$$

Hence Φ^* maps basis to basis.

• Therefore it makes sense to define $\mu : S_2(N) \to \Omega(J_0(N))$ by

$$\Phi^*(\mu(f)) = f(z)dz,\ f \in S_2(N).$$

In particular, $\mu(f_j) = dz_j$.

- For any $n \in \mathbb{N}$, one has the Hecke operator $T_n : X_0(N) \to \mathrm{Div}(X_0(N))$. For any $\tau \in X_0(N)(\mathbb{C})$,

$$T_n(\tau) = \sum \alpha_i \tau,$$

where α_i runs through the elements in the set $\left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \,\middle|\, ad = n,\ d > 0,\ (a, N) = 1 \right\}$. $\overline{\Phi}$ can also extend linearly to $\mathrm{Div}(X_0(N)) \to J_0(N)$. Hence one obtain $\overline{T}_n = \overline{\Phi} \circ T_n : X_0(N) \to J_0(N)$. From the universal property, one can define t_n in the following diagram:

$$\begin{tikzcd} X_0(N) \arrow[r, "\Phi"] \arrow[dr, "\overline{T}_n"'] & J_0(N) \arrow[d, dashed, "t_n"] \\ & J_0(N) \end{tikzcd}$$

where t_n satisfies

$$\overline{T}_n = t_n \circ \Phi + \overline{T}_n(\tau_0). \tag{4.1}$$

(4.1) has the explicit expression:

$$t_n \begin{pmatrix} \int_{\tau_0}^{\tau} f_1(z)dz \\ \vdots \\ \int_{\tau_0}^{\tau} f_g(z)dz \end{pmatrix} = \begin{pmatrix} \sum_i \int_{\alpha_i\tau_0}^{\alpha_i\tau} f_1(z)dz \\ \vdots \\ \sum_i \int_{\alpha_i\tau_0}^{\alpha_i\tau} f_g(z)dz \end{pmatrix}$$

Hence

$$
\begin{aligned}
dt_n \begin{pmatrix} f_1(\tau) \\ \vdots \\ f_g(\tau) \end{pmatrix} &= \begin{pmatrix} \sum_i f_1(\alpha_i(\tau)) \frac{\alpha_i \tau}{d\tau} \\ \vdots \\ \sum_i f_g(\alpha_i(\tau)) \frac{\alpha_i \tau}{d\tau} \end{pmatrix} \\
&= \begin{pmatrix} \sum_i f_1 \circ [\alpha_i]_2(\tau) \\ \vdots \\ \sum_i f_g \circ [\alpha_i]_2(\tau) \end{pmatrix} \\
&= \begin{pmatrix} T_n f_1 \\ \vdots \\ T_n f_g \end{pmatrix} \\
&= A_n \begin{pmatrix} f_1 \\ \vdots \\ f_g \end{pmatrix}.
\end{aligned}
$$

Here A_n becomes A_n^t when dt_n acts on the dual of $\Omega(J_0(N))$, which is $\mathfrak{J} \cong \mathbb{C}^g$.

• **Shimura-Taniyama**. For any $f \in S_2(N)$,

$$t_n^*(\mu(f)) = \mu(T_n f).$$

For any f_j,

$$
\begin{aligned}
< t_n^*(\mu(f_j)), e_l > &=< \mu(f), dt_n e_l > \\
&=< dz_j, dt_n e_l > \\
&= (A_n^t)_{lj} = (A_n)_{jl},
\end{aligned}
$$

and

$$\begin{aligned} < \mu(T_n(f_j)), e_l > &= \sum_{i=1}^{g} < \mu((A_n)_{ji} f_i), e_l > \\ &= \sum_{i=1}^{g} (A_n)_{ji} < dz_i, e_l > \\ &= (A_n)_{jl}. \end{aligned}$$

• **Eichler-Shimura construction** Let $f \in S_2(N)$ be a normalized newform with integer coefficients in its q-expansion $f(z) = \sum_{n>0} c_n q^n$, where $q = e^{2\pi i z}$. Then there exists an elliptic curve E_f defined over $\mathbb{Q}$, which is the quotient of $J_0(N)$, i.e. there is a homomorphism: $\nu : J_0(N) \to E_f$. Also

- $t_n(\mathrm{ker}\nu) = \mathrm{ker}\nu$.
- $t_n E_f = c_n E_f$.
- $\mu(f)$ is a nonzero multiple of $\nu^*(\omega)$, where ω is the invariant differential of E_f.
- $E_f \cong \mathbb{C}/\Lambda_f$, where

$$\Lambda_f := \Big\{ \int_{\tau_0}^{\gamma\tau_0} f(z)dz \,\Big|\, \gamma \in \Gamma_0(N) \Big\}$$

- $L(E_f, s)$ equals to $L(f, s)$ except at finitely many primes dividing N.

Proof. Let $\mathcal{T}$ be the commutative $\mathbb{Q}$-subalgebra of $\mathrm{End}_{\mathbb{Q}}(J_0(N)) := \mathrm{End}(J_0(N)) \otimes \mathbb{Q}$ generated by all t_n. Clearly $\mathcal{T}$ can be embedded into $M_g(\mathbb{Q})$, hence $\dim_{\mathbb{Q}} \mathcal{T}$ is finite.

Let $\mathcal{N}$ be the nilradical ideal of $\mathcal{T}$, then by Wedderburn's theorem,

$$\mathcal{T} \cong (k_1 \oplus \cdots \oplus k_r) \oplus \mathcal{N},$$

for some number fields $k_1, \ldots, k_r$. One has

$$t_n^*(\mu(f)) = \mu(T_n(f)) = c_n\mu(f).$$

Hence the following map:

$$\rho : \mathcal{T} \to \mathbb{Q},\, t_n \mapsto c_n$$

is a homomorphism as $\mathbb{Q}$ algebras. Clearly $\rho(\mathcal{N}) = 0$, hence WLOG, assume $\rho(k_1) = \mathbb{Q}$, which implies $k_1 \cong \mathbb{Q}$ and ρ is an isomorphism. One obtains an ideal $I := (k_2 \oplus \cdots \oplus k_r) \oplus \mathcal{R}$.

Now define A_f be the abelian subvariety which is the sum of all $\alpha(J_0(N))$ for all $\alpha \in I \cap \mathrm{End}(J_0(N))$. **It can be proved t_n is defined over $\mathbb{Q}$ (Ref. Knapp, Elliptic curves §11, Ch.XI)**, hence A_f is defined over $\mathbb{Q}$. Hence one can form the quotient (E_f, ν) of $J_0(N)$ by A (i.e. $\nu : J_0(N) \to E_f$ with $\ker\nu = A_f$) and everything is defined over $\mathbb{Q}$. Since I is an ideal, it is easy to see $\beta A_f \subseteq A_f$ for any $\beta \in \mathcal{T} \cap \mathrm{End}(J_0(N))$. In particular $t_n(A_f) \subseteq A_f$. Hence $\ker(\nu \circ t_n) \supseteq \ker\nu$, so by universal mapping property, one has the following commutative diagram:

$$\begin{tikzcd} J_0(N) \arrow[r, "\nu"] \arrow[dr, "\nu\circ t_n"'] & E_f \arrow[d, dashed, "\exists \bar{t}_n"] \\ & E_f \end{tikzcd} \tag{4.2}$$

Hence t_n acts on E_f as $\bar{t}_n$. From the definition of ρ, one has $t_n - \rho^{-1}(c_n) \in I$ and $\rho^{-1}(c_n) - [c_n] \in I$, hence $t_n - [c_n] \in I \cap \mathrm{End}(J_0(N))$. So $t_n - [c_n]$ acts as 0 on E_f. I.e. $t_n(E_f) = [c_n]E_f$.

Let m be the largest integer for which $k_1\mathcal{N}^m \neq 0$. Let $0 \neq \beta \in k_1\mathcal{N}^m$. WLOG, assume $\beta \in \mathrm{End}(J_0(N))$ (after multiplying some $m \in \mathbb{N}$ since $\beta(J_0(N)) = m\beta(J_0(N))$). For any $\alpha \in I$, $\beta\alpha = 0$ since $k_1 k_j = 0$ for any $j \neq 1$ and $\mathcal{R}^m\mathcal{R} = 0$. Therefore

$\beta(A_f) = 0$. Since $\beta(J_0(N)) \neq 0$ because $\beta \neq 0$, hence $A_f \neq J_0(N)$, i.e. $\dim E_f > 0$.

Since $\dim E_f \neq 0$, $\exists \omega' \in \Omega(E_f)$ which is non-zero. $\nu : J_0(N) \to E_f$ induces $\nu^* : \Omega(E_f) \to \Omega(J_0(N))$. ν^* is injective. From (4.2), one has

$$\nu^* \circ \bar{t}_n^* = t_n^* \circ \nu^*.$$

Since $\bar{t}_n = [c_n]$, $\bar{t}_n^* = c_n$, i.e.

$$t_n^*(\nu^*(\omega')) = c_n \nu^*(\omega').$$

Put $f' = \mu^{-1}(\nu^*(\omega'))$, then

$$\mu(T_n f') = t_n^*(\mu(f')) = t_n^*(\nu^*(\omega')) = c_n \nu^*(\omega') = c_n \mu(f').$$

So

$$T_n f' = c_n f'.$$

Suppose $\dim E_f > 1$, then one has linearly independent ω' and ω''. Let $f'' = \mu^{-1}(\nu^*(\omega''))$, we have f'' and f' are linearly independent and

$$T_n f'' = c_n f''.$$

This is a contradiction. Hence $\dim E = 1$.

[Uniqueness. Suppose A' and (E', ν') are also satisfies the theorem with invariant differential ω'. Then $\nu'^*(\omega')$ and $\nu^*(\omega)$ are multiples of each other. Hence they annihilate the same subset of $\mathfrak{J}$ — the tangent space of A' and A. Since A_f and A' are the connected Lie subgroup of $J_0(N)$ with same Lie subalgebra, $A_f = A'$.]

$J_0(N) \cong \mathbb{C}^g/\Lambda$, where Λ has basis

$$l_k = \begin{pmatrix} \int_{c_k} f_1 dz \\ \vdots \\ \int_{c_k} f_g dz \end{pmatrix}, \ k = 1, \ldots, 2g,$$

where $c_1, \ldots, c_{2g}$ are a basis of $H_1(X_0(N)(\mathbb{C}), \mathbb{Z})$ over $\mathbb{Z}$. Write $f = \sum_j r_j f_j$, and consequently

$$\begin{aligned}\mu(f)(l_k) =&< \mu(f), l_k >=< \sum_j r_j \mu(f_j), l_k >= \sum_j r_j < dz_j, l_k > \\ &= \sum_j r_j \int_{c_k} f_j dz = \int_{c_k} f dz.\end{aligned}$$

Hence

$$\mu(f)(\Lambda) = \Lambda_f.$$

Let $\mathfrak{a} \subset \mathfrak{J}$ be the tangent space of A.

$$\begin{aligned}\ker\mu(f) &= \{u \in \mathfrak{J} \,\big|\, < \nu^*(\omega), u >= 0\} \\ &= \{u \in \mathfrak{J} \,\big|\, < \omega, (d\nu)(u) >= 0\} \\ &= \{u \in \mathfrak{J} \,\big|\, d\nu(u) = 0\} \\ &= \ker(d\nu) \\ &= \mathfrak{a}.\end{aligned}$$

From Lie theory, one has exponential map $\mathfrak{J} \to J_0(N)$ with kernel Λ, whose restriction to $\mathfrak{a}$ is the exponential map $\mathfrak{a} \to A$. Since A is compact, $\mathfrak{a} \cap \Lambda$ is a lattice in $\mathfrak{a}$ of rank $2g-2$. Let $x_1, \ldots, x_{2g-2}$ be a $\mathbb{Z}$-basis for it and adding x_{2g-1} and x_{2g} to make $\Lambda' = \sum_{j=1}^{2g} \mathbb{Z}x_j$ has rank $2g$. Hence Λ' has finite index m in Λ. So $\Lambda \subset \frac{1}{m}\Lambda'$. So one has

$$\mathbb{C} = \mu(f)(\mathfrak{J}) = \mu(f)(\sum \mathbb{R}x_j) = \mu(f)(\mathbb{R}x_{2g-1} + \mathbb{R}x_{2g}).$$

Hence $\mu(f)(x_{2g-1})$ and $\mu(f)(x_{2g})$ are linearly independent over $\mathbb{R}$. On the other hand

$$\begin{aligned}\mu(f)(\mathbb{Z}x_{2g-1}+\mathbb{Z}x_{2g}) &= \mu(f)(\sum_j \mathbb{Z}x_j)\\ &= \mu(f)(\Lambda')\\ &\subseteq \mu(f)(\Lambda)\\ &\subseteq \mu(f)(\frac{1}{m}\Lambda') = \mu(f)(m^{-1}\mathbb{Z}x_{2g-1}+m^{-1}\mathbb{Z}x_{2g}).\end{aligned}$$

Hence one concludes Λ_f is a free abelian subgroup of $\mathbb{C}$ of rank 2 over $\mathbb{Z}$ that spans $\mathbb{C}$ over $\mathbb{R}$, i.e. Λ_f is a lattice in $\mathbb{C}$.

Hence $E = \mathbb{C}/\Lambda_f$ is an elliptic over $\mathbb{C}$. One has the map

$$\delta : \mathfrak{J} \xrightarrow{\mu(f)} \mathfrak{J}/\mathfrak{a} \cong \mathbb{C} \to \mathbb{C}/\Lambda_f = E.$$

$\ker(\delta) = \mu(f)^{-1}(\Lambda_f) = \mathfrak{a} + \Lambda$. Hence δ factors through the exponential map $\exp : \mathfrak{J} \to J_0(N)$:

$$\delta = \epsilon \circ \exp,$$

for some holomorphic homomorphism $\epsilon : J_0(N) \to E$ with kernel $\exp(\mathfrak{a}+\Lambda) = A$. Hence ϵ is a morphism over $\mathbb{C}$. The universal property says the following diagram commutes:

$$\begin{tikzcd} J_0(N) \arrow[r, "\nu"] \arrow[dr, "\epsilon"'] & E_f \arrow[d, dashed, "\exists\theta"] \\ & E \end{tikzcd}$$

Since $\ker\epsilon = \ker\nu = A$, $\ker\theta$ is trivial, hence $E_f \cong E$.

For the equality of $L(E_f, s)$ and $L(f, s)$, this is a consequence of Eichler-Shimura congruence. (Ref. Diamond & Shurman A first course in modular forms Chapter 8). One has the following result:

Let E be an elliptic curve defined over $\mathbb{Q}$ and E has good reduction over prime p, then

$$a_p(E) = \sigma_{p,*} + \sigma_p^*$$

as endomorphisms on $\mathrm{Pic}^0(\widetilde{E})$. From Eichler-Shimura congruence:

$$\begin{array}{ccc} \mathrm{Pic}^0(X_0(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_0(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_0(N)) & \xrightarrow[\sigma_{p,*}+\sigma_p^*]{} & \mathrm{Pic}^0(\widetilde{X}_0(N)) \end{array}$$

As we proved T_p acts on $\widetilde{E}_f$ as $[c_p]$, hence $[c_p] = [a_p(E_f)]$. Since $\mathrm{End}(E_f)$ has no zero divisors, $a_p(E_f) = c_p$. [for T_p acts in $\mathrm{Pic}^0(X_1(N))$ as follows:

$$T_p[E, Q] = \sum_C [E/C, Q + C],$$

where C runs through all subgroup of E of order p such that $C \cap < Q >$ is trivial. In particular if $p \nmid N$, then the sum runs through all such subgroups. Let C_0 be the kernel of the reduction map $E[p] \to \overline{E}[p]$, where E is defined over $\overline{\mathbb{Q}}$ (with ordinary reduction at $\mathfrak{p} \mid p$, which is not necessary). Then

Lemma 4.1.1. $[\overline{E/C}, \overline{Q+C}] = \begin{cases} [\overline{E}^{\sigma_p}, \overline{Q}^{\sigma_p}] & C = C_0 \\ [\overline{E}^{\sigma_p^{-1}}, [p]\overline{Q}^{\sigma_p^{-1}}] & C \neq C_0 \end{cases}$

Let $MS(N)$ be the moduli space of $X_1(N)$, one has the following diagram:

$$\begin{array}{ccc} \mathrm{Div}^0(MS(N)) & \xrightarrow{T_p} & \mathrm{Div}^0(MS(N)) \\ \downarrow & & \downarrow \\ \mathrm{Div}^0(\overline{MS}(N)) & \xrightarrow{\sigma_p + p\overline{<p>}\sigma_p^{-1}} & \mathrm{Div}^0(\overline{MS}(N)) \end{array}$$

and

$$\begin{array}{ccc}
\mathrm{Div}^0(\overline{MS}(N)) & \xrightarrow{\sigma_p+p\overline{<p>}\sigma_p^{-1}} & \mathrm{Div}^0(\overline{MS}(N)) \\
\downarrow & & \downarrow \\
\mathrm{Div}^0(\overline{X}_1(N)) & \xrightarrow{\sigma_{p,*}+\overline{<p>}_*\sigma_p^*} & \mathrm{Div}^0(\overline{X}_1(N))
\end{array}$$

Under $X_0(N)$, $< p >$ is trivial, hence one obtains $\sigma_{p,*} + \sigma_p^*$.

One has the modular parametrization:

$$\phi : X_0(N) \to E_f.$$

$\sigma_{p,*} + \sigma_p^*$ commutes with ϕ_*, hence $\sigma_{p,*} + \sigma_p^*$ on $\mathrm{Pic}^0(\widetilde{X}_0(N))$ becomes $\sigma_{p,*} + \sigma_p^*$ on $\mathrm{Pic}^0(\widetilde{E}_f)$ □

4.2 CM points

The converse of Eichler-Schimura theorem is also true. The converse is a deep result due to Wiles, Taylor etc. From their results, for any elliptic curve $E/\mathbb{Q}$ of conductor N, $\exists f \in S_2(N)$ which is a new form such that E is isogenous to E_f over $\mathbb{Q}$, where E_f is constructed from f via Eichler-Shimura construction and consequently $L(E_f, s) = L(E, s) = L(f, s)$. Hence it is often enough to study E_f for some newform $f \in S_2(N)$. In such case and when N is square free, one has an explicit modular parametrisation:

$$\Phi_N : X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H}^* \xrightarrow{\Phi_1} \mathbb{C}/\Lambda_f \xrightarrow{\Phi_W} E_f(\mathbb{C}),$$

where Φ_1 is given by

$$\tau \mapsto \int_{i\infty}^{\tau} 2\pi i f dz,$$

and Φ_W is the Weierstrass uniformisation. Φ_N can be used to construct algebraic points on E defined over some abelian extension of $\mathbb{Q}$. Class field theory tells us where these points, which are called Heegnar points, lie exactly. To construct such points, one starts with a quadratic imaginary field $K = \mathbb{Q}(\sqrt{D})$ for some square free negative integer D. It is a well-known fact that its ring of integers $\mathcal{O}_K$ is

$$\mathcal{O}_K = \mathbb{Z}[\omega_D], \text{ where } \omega_D = \begin{cases} \sqrt{D} & D \not\equiv 1 (\text{mod } 4) \\ \frac{1+\sqrt{D}}{2} & D \equiv 1 (\text{mod } 4). \end{cases}$$

$\mathcal{O}_K$ is the maximal order of K (i.e. its conductor is 1) and any order $\mathcal{O}$ of K can be written as

$$\mathcal{O} = \mathbb{Z} \oplus c\mathbb{Z}\omega_D,$$

for some integer $c > 0$ and vice versa. One as a bijection

$$\mathrm{Ell}(\mathcal{O}) := \left\{ \text{isomorphism classes of } E/\mathbb{C} \text{ with CM of } \mathcal{O} \right\} \xleftrightarrow{\cong} \mathrm{Pic}(\mathcal{O}),$$

where $\mathrm{Pic}(\mathcal{O})$ is the Picard group, which has several equivalent definitions, here it is defined as the group generated by all invertible fractional $\mathcal{O}$-ideals prime to c (hence invertible) modulo the subset of principal $\mathcal{O}$-ideals. It can be proved that $\mathrm{Pic}(\mathcal{O})$ is finite and its order is

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|c} \left(1 - (\frac{d_K}{p})\frac{1}{p}\right)$$

It can be proved that

$$\mathrm{Pic}(\mathcal{O}) \cong I_K(c)/P_{K,\mathbb{Z}}(c),$$

where $P_{K,\mathbb{Z}}(f)$ is the subgroup of $I_K(c)$ (the group of all $\mathcal{O}_K$-ideals prime to c) generated by principal ideals of the form $\alpha\mathcal{O}_K$ for some $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv a \bmod (c\mathcal{O}_K)$ for some integer a prime to c(Cox, Primes of forms $X^2 + nY^2$, §7). Class field theory gives the following result:

Theorem 4.2.1. ***For any proper fractional $\mathcal{O}$-ideal $\mathfrak{a}$,$K(j(\mathfrak{a}))$ is the ring class field of the order $\mathcal{O}$, where $j(\mathfrak{a})$ is the j-invariant ($\mathfrak{a}$ can be naturally***

identified with a lattice in $\mathbb{C}$ ***). The Artin map:***

$$\varphi : \mathcal{O} \xrightarrow{\cong} \mathbf{Gal}(K(j(\mathfrak{a}))/K)$$

is defined as

$$\mathfrak{a} \mapsto \sigma_{\mathfrak{a}},$$

where

$$\sigma_{\mathfrak{a}}(j(\mathfrak{b})) = j(\bar{\mathfrak{a}}\mathfrak{b}),$$

for any fractional $\mathcal{O}$***-ideal*** $\mathfrak{a}$ ***and*** $\mathfrak{b}$ ***prime to*** c***.***

[The class field theory is as follows:

Let L/K **be an abelian extension and** $zfrakm$ **be a modulus divisible by all primes of** K **(including infinite primes) ramified in** L**, then the Artin map** $\varphi : I_K(\mathfrak{m}) \to \mathbf{Gal}(L/K)$ **is surjective and if the exponents of finite primes in** $\mathfrak{m}$ **are sufficiently large, ker(**φ**) is a congruence subgroup for** $\mathfrak{m}$**, i.e.** $P_{K,1}(\mathfrak{m}) \subset \mathbf{ker}(\varphi) \subset I_K(\mathfrak{m})$**, and one has the isomorphism:**

$$I_K(\mathfrak{m})/\mathbf{ker}(\varphi) \xrightarrow{\cong} \mathbf{Gal}(L/K).$$

Conversely, for any modulus $\mathfrak{m}$ **of** K **and for any congruence subgroup** H **for** $\mathfrak{m}$ **(i.e.** $P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$**), there exists a unique abelian extension** L/K **whose ramified primes (including infinite primes) divide** $\mathfrak{m}$ **and the Artin map induces an isomorphism:**

$$I_K(\mathfrak{m})/H \xrightarrow{\cong} \mathbf{Gal}(L/K).$$

In particular, let $\mathfrak{m} = f\mathcal{O}_K$ for some positive integer f, clearly

$$P_{K,1}(f) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f),$$

hence class field theory guarantees the unique existence of the abelian extension H_f/K such that

$$I_K(f)/P_{K,\mathbb{Z}} \cong \mathrm{Gal}(H_f/K).$$

Furthermore, if K is a quadratic imaginary field, then this is equivalent saying each order corresponds uniquely an abelian extension of K which is called the ring class field.

This can also be interpreted in the following way via CM: $\mathrm{Pic}(\mathcal{O})$ acts on $\mathrm{Ell}(\mathcal{O})$ as follows: for any $\mathfrak{a}$ whose norm $(\#\mathcal{O}/\mathfrak{a})$ is prime to the conductor c of $\mathcal{O}$,

$$[\mathfrak{a}] \cdot [\mathbb{C}/\Lambda] := [\mathbb{C}/\mathfrak{a}^{-1}\Lambda].$$

This is well-defined: $\mathrm{End}(\mathbb{C}/\Lambda) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\} = \{\alpha\mathfrak{a}^{-1}\Lambda \subseteq \mathfrak{a}^{-1}\Lambda\} = \mathrm{End}(\mathbb{C}/\mathfrak{a}^{-1}\Lambda)$, which implies $[\mathfrak{a}] \cdot [\mathbb{C}/\Lambda] \in \mathrm{Ell}(\mathcal{O})$. Further, $\mathbb{C}/\mathfrak{a}^{-1}\Lambda \cong \mathbb{C}/\mathfrak{a}'^{-1}\Lambda \iff \exists a \in \mathbb{C}$, such that $\mathfrak{a}^{-1}\Lambda = a(\mathfrak{a}')^{-1}\Lambda \iff \Lambda = a\mathfrak{a}(\mathfrak{a}')^{-1}\Lambda = a^{-1}\mathfrak{a}^{-1}\mathfrak{a}'\Lambda \iff a\mathfrak{a}(\mathfrak{a}')^{-1}, a^{-1}\mathfrak{a}^{-1}\mathfrak{a}' \subseteq \mathcal{O}$ (by the definition of proper ideals) $\iff a\mathfrak{a} \subseteq \mathfrak{a}'$, and $\mathfrak{a}' \subseteq a\mathfrak{a} \iff a\mathfrak{a} = \mathfrak{a}' \iff \mathfrak{a} \cong \mathfrak{a}'$ as $\mathcal{O}$-modules.

The action is transitive since for any $\mathbb{C}/\Lambda$ with CM $\mathcal{O}$, Λ is homothetic to a lattice contained in K and $\mathbb{C}/\Lambda' \cong \mathbb{C}/\Lambda(\Lambda'\Lambda^{-1})$. Since one can always assume Λ and $\mathfrak{a}$ are in K, the action of $\mathrm{Pic}(\mathcal{O})$ and that of $G_K := \mathrm{Gal}(\overline{K}/K)$ on $\mathrm{Ell}(\mathcal{O})$ commute with each other. One can define a group homomorphism:

$$\eta : G_K \to \mathrm{Pic}(\mathcal{O}),\ (\mathbb{C}/\Lambda)^\sigma = \eta(\sigma) \cdot (\mathbb{C}/\Lambda), \forall \sigma \in G_K.$$

For some other lattice Λ such that $\mathbb{C}/\Lambda \in \mathrm{Ell}(\mathcal{O})$ which defines η', since $\mathrm{Pic}(\mathcal{O})$ acts on $\mathrm{Ell}(\mathcal{O})$ transitively, $[\mathfrak{b}] \cdot [\mathbb{C}/\Lambda] = [\mathbb{C}/\Lambda']$ for some $\mathfrak{b} \in \mathrm{Pic}(\mathcal{O})$ prime to $\mathcal{O}$. Hence

$$([\mathfrak{b}] \cdot [\mathbb{C}/\Lambda])^\sigma = [\mathfrak{b}]([\mathbb{C}/\Lambda])^\sigma = [\mathfrak{b}] \cdot \eta(\sigma) \cdot (\mathbb{C}/\Lambda) = [\mathfrak{b}\eta(\sigma)] \cdot (\mathbb{C}/\Lambda).$$

On the other hand

$$(\mathbb{C}/\Lambda')^\sigma = \eta'(\sigma)(\mathbb{C}/\Lambda') = \eta'(\sigma) \cdot ([\mathfrak{b}] \cdot (\mathbb{C}/\Lambda)) = [\eta'(\sigma)\mathfrak{b}] \cdot (\mathbb{C}/\Lambda).$$

So from the commuativity of $\mathrm{Pic}(\mathcal{O})$,

$$[\mathfrak{b}\eta(\sigma)](\mathbb{C}/\Lambda) = [\mathfrak{b}\eta'(\sigma)](\mathbb{C}/\Lambda).$$

The result proved earlier shows that $\mathfrak{b}\eta'(\sigma) \cong \mathfrak{b}\eta(\sigma)$ as $\mathcal{O}$-module, i.e. $\eta'(\sigma) = \eta(\sigma)$ in $\mathrm{Pic}(\mathcal{O})$. It is easy to verify η is a group homomorphism.

The class field theory tells us there is an abelian extension H_c/K which is unramified for all prime $\mathfrak{p} \nmid c$ whose Galois group $\mathrm{Gal}(H_c/K) \cong \mathrm{Pic}(\mathcal{O})$. One has the reciprocity map:

$$\varphi_c : \mathrm{Pic}(\mathcal{O}) \to G_c := \mathrm{Gal}(H_c/K),\ \mathfrak{p} \mapsto \sigma_{\mathfrak{p}},\ \forall \mathfrak{p} \nmid c.$$

Let $H := (\overline{K})^{\ker \eta}$, Galois theory tells us H/K is an abelian (hence Galois) extension.

Lemma 4.2.2. *$H = H_c$.*

Proof. Clearly $j(E) \in H$ by the definition of H for any $E \in \mathrm{Ell}(\mathcal{O})$. Hence each such E is defined over some abelian extension L/K. Fix such an E. From class field theory (using uniqueness) and Galois theory, it is enough to show η is onto. Let $\mathfrak{p}$ be a prime in K unramified in H/K such that E has good reduction at all the primes of

H above $\mathfrak{p}$ and $\mathfrak{p}$ splits in $K/\mathbb{Q}$ and $\mathfrak{p} \nmid j(A') - j(A'')$ for all distinct A, A'' in $\mathrm{Ell}(\mathcal{O})$. For the set of such primes (has Dirichlet density 1 (Only finitely many primes are excluded) and hence), the corresponding Frobenius elements generate $\mathrm{Gal}(H/K)$.

Let $\mathfrak{P}$ be a prime of L over $\mathfrak{p}$ such that E/L has the good reduction $\overline{E}_{\mathfrak{P}}$. The inclusion $\mathfrak{p} \to \mathcal{O}$ induces $\theta : E \cong \mathbb{C}/\Lambda = \mathbb{C}/\Lambda\mathcal{O} = \mathbb{C}/\Lambda\mathcal{O}^{-1} \to \mathbb{C}/\Lambda\mathfrak{p}^{-1}$, whose degree is $N\mathfrak{p} = p = \mathcal{O}_K/\mathfrak{p} = \mathcal{O}/\mathcal{O} \cap \mathfrak{p}$ since $\mathfrak{p}$ is not inert in $K/\mathbb{Q}$. Their reduction at $\mathfrak{P}$, $\overline{\theta} : \overline{E} \to \overline{\mathfrak{p} \cdot E}$ has degree p, whose duality is purely inseparable, hence the only possibility is the Frobenius map: $\widehat{\overline{\theta}} : \overline{E/E[\mathfrak{p}]} \to \overline{E/E[\mathfrak{p}]}^{(p)} = \overline{E}$. Hence

$$E \equiv (\mathfrak{p} \cdot E)^{(p)} = \sigma_{\mathfrak{p}}(\mathfrak{p} \cdot E) = \mathfrak{p} \cdot (\sigma_{\mathfrak{p}}(E)) (\mathrm{mod}\ \mathfrak{P}).$$

Hence $\eta(\sigma_{\mathfrak{p}}^{-1}) = [\mathfrak{p}]$. To prove $\widehat{\overline{\theta}}$ is purely inseparable, ~~one uses the following theorem: Suppose E/L is an elliptic curve with CM in K and has the good reduction at $\mathfrak{P} \mid p$ for some prime in $\mathbb{Q}$, then E has Hasse invariant 0 iff p is not split in K. (see Lang Ch 13 §4).~~ One knows from Silverman's AEC (p.78), the isogeny $\overline{\theta} : \overline{E} \to \overline{E}/\overline{E}[\mathfrak{p}]$ is separable. Consider $\widehat{\overline{\theta}} \circ \overline{\theta} : \overline{E} \to \overline{E}$, which is the map $[p]$, since the characteristic of the residue field is p, $[p]^* \overline{\omega}_E = p\overline{\omega}_E = 0$. Hence $[p]$ is not separable. Since $\overline{\theta}$ is separable, $\widehat{\overline{\theta}} : \overline{E}/\overline{E}[\overline{\mathfrak{p}}] \to \overline{E}$ must be purely inseparable with degree p, hence $\overline{E} \cong (\overline{E}/\overline{E}[\overline{\mathfrak{p}}])^p$ and $\widehat{\overline{\theta}}$ is the Frobenius map: $\overline{E/E[\mathfrak{p}]} \to \overline{E/E[\mathfrak{p}]}^{(p)}$. $\square$

For $\tau \in \mathcal{H}$, define

$$\mathcal{O}_\tau := \{\gamma \in M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q}),\ \gamma\tau = \tau\} \cup \{0_{2\times 2}\}.$$

It is easy to see

$$\mathcal{O}_\tau = \{\gamma \in M_2(\mathbb{Z}) \,\big|\, \gamma \text{ has eigenvectors } \binom{\tau}{1} \text{ and } \binom{\overline{\tau}}{1}\}. \qquad (4.3)$$

For each $\gamma \in \mathcal{O}_\tau$, define z_γ to be the eigenvalue associated with the eigenvector $\binom{\tau}{1}$, consequently the map $\gamma \mapsto z_\gamma$ gives $\mathcal{O}_\tau \hookrightarrow \mathbb{C}$. Under this identification, one has

Lemma 4.2.3. *$\mathcal{O}_\tau \cong \mathrm{End}(E_\tau)$, where $E_\tau = \mathbb{C}/ < 1, \tau >$, $\tau \in \mathcal{H}$.*

Proof. From (4.3), $z_\gamma(< 1, \tau >) \subseteq < 1, \tau >$, hence induces an endomorphism σ_γ of E_τ. The map $\gamma \mapsto \sigma_\gamma$ is clearly injective and surjective. $\square$

Define $CM(\mathcal{O}) = \{\tau \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \mid \mathcal{O}_\tau = \mathcal{O}\}$. The class group $\mathrm{Pic}(\mathcal{O})$ acts on $CM(\mathcal{O})$ as follows: for any class $\mathfrak{b} \in \mathrm{Pic}(\mathcal{O})$, it can be represented by an integral ideal $B \subset \mathcal{O}$ such that $\mathcal{O}/B$ is cyclic (Cox, P. 236). For any $\tau \in CM(\mathcal{O})$, $< 1, \tau > B^{-1}$ is a lattice, hence is homothetic to $< 1, \tau' >$ for some $\tau' \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$, define $\mathfrak{b} * \tau = \tau'$. It is easy to see $*$ is an action and compatible with the action on $\mathrm{Ell}(\mathcal{O})$. From the class field theory, one has for any prime $[\mathfrak{p}] \in \mathrm{Pic}(\mathcal{O})$,

$$j(\mathfrak{b} * \tau) = j(\mathfrak{p} \cdot \mathbb{C}/ < 1, \tau >) = j((\mathbb{C}/ < 1, \tau >)^{\sigma_\mathfrak{p}}) = j(\mathbb{C}/ < 1, \tau >)^{\sigma_\mathfrak{p}} = j(\tau)^{\sigma_\mathfrak{p}} = \varphi(\mathfrak{p})j(\tau)$$

The main theorem of CM asserts for any $\tau \in \mathcal{H} \cap K$ where K is a quadratic imaginary field, $j(\tau) \in H$, where H/K is the ring class field associated with the order $\mathcal{O}_\tau$. Define $\mathcal{O}_{\tau,N} := \mathcal{O}_\tau \cap \mathcal{O}_{N\tau}$ and let Φ_N and E_f be as before, one has

Theorem 4.2.4. *For any $\tau \in \mathcal{H} \cap K$, $\Phi_N(\tau) \in E_f(H)$, where H is the ring class field with respect to $\mathcal{O}_{\tau,N}$.*

Proof. $j(\tau)$ and $j(N\tau)$ are in H. Hence $\Phi_N(\tau)$ is the image of a point in $X_0(N)(H)$ and Φ_N is defined over $\mathbb{Q}$. $\square$

Remark One can easily prove $\mathcal{O}_{\tau,N} = \{\gamma \in M_0(N) \mid \gamma\tau = \tau\} \cup \{0_{2\times 2}\}$, where $M_0(N) \subset M_2(\mathbb{Z})$ whose element is upper triangular modulo N.

(The following data are extracted from Darmon's Rational points over modular elliptic curves). Take $N = 11$, the elliptic curve with this conductor is (the dimension of $S_2(11)$ is 1):

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

The order with smallest discriminant embedded in $M_0(11)$ is $\mathcal{O}_K = \mathbb{Z}(\frac{1+\sqrt{-7}}{2}) \subset K := \mathbb{Q}(\sqrt{-7})$ which has class number 1. $\mathcal{O}_K$ in $M_0(11)$ is $\mathbb{Z}+\mathbb{Z}\left(\begin{smallmatrix} -4 & -2 \\ 11 & 5 \end{smallmatrix}\right)$ whose fixed point is $\tau = \frac{-9+\sqrt{-7}}{22}$, which corresponds to a point $(\frac{1-\sqrt{-7}}{2}, -2-2\sqrt{-7})$ in $E(\mathbb{C})$ to 25 decimal digits of accuracy.

4.3 Euler System

Let K be an imaginary quadratic extension of $\mathbb{Q}$ which is not $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. For any positive integer λ, denote K_λ to be the ring class field of K with conductor λ. Let E/Q be an elliptic curve of conductor N and ℓ be a fixed prime number satisfying some conditions. One has the following field towers:

$$\begin{array}{c} K_\lambda \\ | \\ K \\ | \\ \mathbb{Q} \end{array}$$

Let Σ be the set of positive integers relative prime to N. Define the set T to be

$$T := \{\tau_\lambda \in \varprojlim H^1(K_\lambda, E[\ell^n]) \,\big|\, \lambda \in \Sigma\}.$$

Here the projective limit is induced by the natural map $H^1(K_\lambda, E[\ell^{n_2}]) \to H^1(K_\lambda, E[\ell^{n_1}])$ for any $n_2 \geq n_1$, which is induced by $E[\ell^{n_2}] \to E[\ell^{n_1}]$. T is called the 0-th Euler system if for any prime number $\delta \neq 2$ relative prime to N (so $\delta\lambda \in \Sigma$) and λ such that the prime divisor δ' of δ in K is unramified in K_λ, then

$$\mathrm{cor}_{\delta\lambda/\lambda}(\tau_{\delta\lambda}) = y_\delta \tau_\lambda,$$

where $\mathrm{cor}_{\delta\lambda/\lambda}$ is the corestriction map:

$$H^1(K_{\lambda\delta}, E[\ell^n]) \to H^1(K_\lambda, E[\ell^n]),$$

and

$$y_\delta = \mathrm{Fr}_{\delta'}^{-1}(x_\delta - P_\delta(\mathrm{Fr}_{\delta'})) \in \mathbb{Z}[G(K_\lambda/K)].$$

Here

$$x_\delta := [K_\delta : K_1],$$

and $\mathrm{Fr}_{\delta'}$ and P_δ are defined as follows: From class field theory, one has Artin map:

$$\theta : I_K^{S(\lambda)}/K_{(\lambda),1}\mathrm{Nm}(I_{K_\lambda}^{S(\lambda)}) \xrightarrow{\cong} \mathrm{Gal}(K_\lambda/K),$$

we define $\mathrm{Fr}_{\delta'} = \theta(\delta')$. Since δ is a prime number which is not a divisor of N, E has good reduction over δ, $P_\delta(X) := X^2 - a_\delta X + \delta$ is the characteristic polynomial of the Frobenius automorphism on the Tate module T_q for any prime number $q \neq \delta$.

[corestriction map: In functorial way, suppose H is a subgroup of G with finite index. Let M be a G-module, then for any $m \in M^H$,

$$\mathrm{Nm}_{G/H} m := \sum_{[s]\in G/H} sm$$

is independent of the choice of S, and is clearly fixed by G. Hence $\mathrm{Nm}_{G/H}$ defines a homomorphism:

$$M^H \to M^G,$$

which can be extended uniquely to $H^r(H, M) \to H^r(G, M)$, which is called the corestriction map. This map can also be constructed explicitly: One has a natural map:

$$\mathrm{Ind}_H^G M \to M,\ \varphi \mapsto \sum_{[s]\in G/H} s\varphi(s^{-1}),$$

which in turn gives

$$H^r(G, \mathrm{Ind}_G^H M) \to H^r(G, M).$$

From Shapiro's lemma, one has the composition:

$$H^r(H, M) \xrightarrow{\cong} H^r(G, \mathrm{Ind}_G^H M) \to H^r(G, M),$$

which is the corestriction map. One has the following property:

$$\mathrm{Cor} \circ \mathrm{Res} = [G : H].$$

]

Lemma 4.3.1. *y_δ is independent of the choice of δ'.*

Proof. If δ is ramified or inert in K, then δ' is unique. Suppose δ splits in K, then $\delta = \delta'\delta^\sigma$, where σ is the complex conjugation.

Since δ is a prime,

$$x_\delta = [K_\delta : K_1] = \#(\mathcal{O}_K/\delta\mathcal{O}_K)^\times/(\mathbb{Z}/\delta\mathbb{Z})^\times.$$

On the other hand,

$$\mathcal{O}_K/\delta\mathcal{O}_K = \big(\mathbb{Z} \oplus \frac{1+\sqrt{D}}{2}\mathbb{Z}\big)\Big/\delta\big(\mathbb{Z} \oplus \frac{1+\sqrt{D}}{2}\mathbb{Z}\big) \cong \mathbb{Z}/\delta\mathbb{Z} \oplus \mathbb{Z}/\delta\mathbb{Z}.$$

Hence

$$x_\delta = \delta - 1.$$

So

$$y_\delta = \mathrm{Fr}_{\delta'}^{-1}(\delta - 1 - \mathrm{Fr}_{\delta'}^2 + a_\delta \mathrm{Fr}_{\delta'} - \delta) = a_\delta - \mathrm{Fr}_{\delta'} - \mathrm{Fr}_{\delta'}^{-1}.$$

Since $\theta(\delta) = 1$ and $\delta = \delta'(\delta')^\sigma$, $\mathrm{Fr}_{\delta'}^{-1} = \mathrm{Fr}_{\delta'^\sigma}$, i.e.

$$\mathrm{Fr}_{\delta'} + \mathrm{Fr}_{\delta'}^{-1} = \mathrm{Fr}_{\delta'^\sigma} + \mathrm{Fr}_{\delta'^\sigma}^{-1}.$$

This proves the independence. □

4.4 Basic assumption

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field in which all prime factors of N are split. Gross and Zagier prove that if $L'(E/K, 1) \neq 0$, then $\hat{h}(y_k) \neq 0$, where $\hat{h}$ is the Néron-Tate canonical height and $y_k = \mathrm{Tr}_{H_K/K}(y_1)$, where y_1 is a Heegnar point defined over H_K, the Hilbert class field of K. This implies the rank of $E(K)$ is at least 1.

Kolyvagin proves in this case $E(K)$ has rank 1. Here I give the Kolyvagin's main idea in his proof, following Gross.

First, we assume E is not CM over $\mathbb{C}$. In this case, $\mathbb{Q}(E[p])/\mathbb{Q}$ is Galois and Serre proves $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for all sufficient large primes p.

By assumption, the order of y_K which is defined over K is infinite. Since $E(K)$ is finitely generated, there are only finitely many integers n such that $y_K = nP$ for some $P \in E(K)$. The argument is as follows: Suppose the rank of $E(K)$ is 2 (similar argument for other cases), which is generated by Q_1 and Q_2. Ignoring the torsion part, we can assume

$$y_k = b_1 Q_1 + b_2 Q_2.$$

Suppose $y_K = nP$ for some $P \in E(K)$ and $P = a_1Q_1 + a_2Q_2$. Then

$$nP = na_1Q_1 + na_2Q_2 = b_1Q_1 + b_2Q_2.$$

The sum is the direct sum as $\mathbb{Z}$-modules. Hence

$$b_1 = na_1; \quad b_2 = na_2.$$

When y_K is fixed, b_1 and b_2 are fixed and there are only finitely many ways to write a given integer into a product of two integers.

From now on, we assume p is a sufficiently large prime (i.e. to ensure $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$) and $y_K \neq pP$ for any $P \in E(K)$.

4.5 Definitions of Selmer groups and Shafarevich groups (for my own reference)

Let K be a number field. Let E and E' be elliptic curves defined over K and $\phi : E \to E'$ be an isogeny defined over K. The sequence

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0$$

is exact as G_K-modules, where $G_K = \mathrm{Gal}(\overline{K}/K)$. This yields the exact sequence:

$$0 \to E(K)[\phi] \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(G_K, E[\phi]) \to H^1(G_K, E) \xrightarrow{\phi} H^1(G_K, E'),$$

which in turn gives the exact sequence:

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(G_K, E[\phi]) \to H^1(G_K, E)[\phi] \to 0.$$

For any place $\mathfrak{p}$ of K, the inclusion $G_{\mathfrak{p}} := \mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}}) \subset G_K$ and $E(\overline{K}) \subset E(\overline{K}_{\mathfrak{p}})$ gives the restriction map $H^1(G_K, E[\phi]) \to H^1(G_{\mathfrak{p}}, E)$. The ϕ-Selmer group of E/K is defined by

$$S^{\phi}(E/K) := \ker\Big\{H^1(G_K, E[\phi]) \to \prod_{\mathfrak{p}} H^1(G_{\mathfrak{p}}, E)\Big\}.$$

The Shafarevich group $\mathfrak{S}\mathfrak{H}(E/K)$ is defined by

$$\mathfrak{S}\mathfrak{H}(E/K) := \ker\Big\{H^1(G_K, E) \to \prod_{\mathfrak{p}} H^1(G_{\mathfrak{p}}, E)\Big\}.$$

Further by these definitions, we have the exact sequence

$$0 \to E'(K)/\phi(E(K)) \to S^{\phi}(E/K) \to \mathfrak{S}\mathfrak{H}(E/K)[\phi] \to 0.$$

In particular, let $\phi = [p]$, we have the exact sequence

$$0 \to E(K)/pE(K) \xrightarrow{\delta} S^{p}(E/K) \to \mathfrak{S}\mathfrak{H}(E/K)[p] \to 0. \tag{4.4}$$

Here δ is the connection map induced from the exact sequence $0 \to E[p] \to E \xrightarrow{[p]} E \to 0$.

4.6 Kolyvagin's proof

Kolyvagin actually proves the following result: Under the conditions mentioned above, $S^p(E/K)$ is cyclic and generated by δy_K. Then the exact sequence (4.4) asserts $E(K)$ has rank 1 and $\mathfrak{S}\mathfrak{H}(E/K)[p]$ is trivial.

1. Construct cohomology classes $c(n) \in H^1(G_K, E[p])$ based on Heegnar points of conductor n prime to N.

Assume $\mathcal{O}_K^\times = \pm 1$. Take an ideal $\mathcal{N} \subset \mathcal{O}_K$ such that $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Take an order $\mathcal{O}_n := \mathbb{Z} + n\mathcal{O}_K$. Define $\mathcal{N}_n := \mathcal{N} \cap \mathcal{O}_n$, which is an invertible $\mathcal{O}_n$-ideal. This is because $\mathrm{Nm}(\mathcal{N}) = N$ which is prime to n, i.e. $\mathcal{N}$ is an $\mathcal{O}_K$-ideal prime to n, and hence $\mathcal{N}_n$ is an $\mathcal{O}_n$-ideal prime to n with same norm, which also implies $\mathcal{N}_n$ is also invertible. See Cox p144.

The isogeny $\mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathcal{N}_n^{-1}$ with kernel $\mathcal{O}_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$ defines a point x_n on $X_0(N)$ according to the moduli interpretation. x_n is defined over K_n, the ring class field of modulus $n\mathcal{O}_K$. We have the following diagram:

$$\begin{tikzcd}
K_n \arrow[d, dash, "(\mathcal{O}_K/n\mathcal{O}_K)^\times/(\mathbb{Z}/n\mathbb{Z})^\times"'] \arrow[dd, dash, bend left=60, "\mathrm{Pic}(\mathcal{O}_n)"] \\
K_1 \arrow[d, dash, "\mathrm{Pic}(\mathcal{O}_K)"'] \\
K \arrow[d, dash, "<1,\tau>"'] \\
\mathbb{Q}
\end{tikzcd}$$

The diagram comes from class field theory. $\mathrm{Gal}(K_n/K_1)$ comes from the following two exact sequences:

$$0 \to I_K(n) \cap P_K/P_{K,\mathbb{Z}}(n) \to I_K(n)/P_{K,\mathbb{Z}}(n) = \mathrm{Pic}(\mathcal{O}_n) \to I_K/P_K = I_K(1)/P_{K,\mathbb{Z}}(n) = \mathrm{Pic}(O_K) \to 0,$$

and when $\mathcal{O}_K^\times = \pm 1$,

$$1 \to (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathcal{O}_K/n\mathcal{O}_K)^\times \to I_K(n) \cap P_K/P_{K,\mathbb{Z}}(n) \to 1,$$

where $P_{K,\mathbb{Z}}(n)$ is the set of principle ideas $\mathfrak{p}$ satisfying $\mathfrak{p} \equiv a(\mathrm{mod}\ n)$ for some $a \in \mathbb{Z}$.

Here we add some background on Heegnar points. A Heegnar corresponds to pairs (E, E') of two N-isogenous elliptic curves with the same $\mathcal{O}$ of complex multiplications. From the moduli interpretation of $X_0(N)$, such pair determines a point y on $X_0(N)$. Such a point can also be identified with $y = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$, where $\mathfrak{n}$ is a proper (hence invertible) $\mathcal{O}$-ideal such that $\mathcal{O}/\mathfrak{n}$ is cyclic with order N and $[\mathfrak{a}]$ denotes an element in the class group of $\mathcal{O}$. One has the natural map $E = \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1} = E'$ with kernel $\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$. To find the real point, choose an oriented basis $< \omega_1, \omega_2 >$ of $\mathfrak{a}$ such that $\mathfrak{a}\mathfrak{n}^{-1} =< \omega_1, \omega_2/N >$, and y corresponds to ω_1/ω_2.

The conductor of y is the conductor of $\mathcal{O}$. For the complex conjugation τ, one has

$$(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^\tau = (\mathcal{O}, \mathfrak{n}^\tau, [\mathfrak{a}^\tau]),$$

since τ is continuous. Note $[\mathfrak{a}^\tau] = [\mathfrak{a}]^{-1}$

Let K_c be the ring of class field corresponding to the conductor of $\mathcal{O}$. Then one has the Artin map: $\theta :$ $\mathrm{Pic}(\mathcal{O}) \to \mathrm{Gal}(K_c/K)$, and

$$(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^{\theta([\mathfrak{b}])} = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^{-1}]) = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^\tau]).$$

For the Fricket involution w_N,

$$w_N(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \mathfrak{n}^\tau, [\mathfrak{a}\mathfrak{n}^{-1}] = (\mathcal{O}, \mathfrak{n}^\tau, [\mathfrak{a}\mathfrak{n}^\tau]).$$

We also have the Hecke operator T_ℓ on y with prime number $\ell \nmid N$ and $(c, N) = 1$, in this case

$$T_\ell(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = \sum_{\mathfrak{a}/\mathfrak{b}=\mathbb{Z}/\ell\mathbb{Z}} (\mathcal{O}_\mathfrak{b} := \mathrm{End}(\mathfrak{b}), \mathfrak{n}_\mathfrak{b} := \mathfrak{n}\mathcal{O}_\mathfrak{b} \cap \mathcal{O}_\mathfrak{b}, [\mathfrak{b}]),$$

where the sum is over $\ell + 1$ sub-lattices in $\mathfrak{a}$.

$\Longrightarrow\Longrightarrow\Longrightarrow\Longrightarrow\Longrightarrow\Longrightarrow\Longrightarrow\Longrightarrow\Longrightarrow\Longrightarrow\Longrightarrow\Longrightarrow\Longrightarrow$

Back to our original setting. We also assume n is square-free and $n \nmid NDp$. This implies for any prime divisor ℓ of n, ℓ is unramified in the extension $K(E[p])$. We also assume

$$\mathrm{Frob}(\ell) = \mathrm{Frob}(\tau) \tag{4.5}$$

as conjugate classes in $\mathrm{Gal}(K(E[p])/\mathbb{Q})$. Hence $\mathrm{Frob}(\ell) = \tau$ in $\mathrm{Gal}(K/\mathbb{Q})$ and so l is inert in K, we use λ to denote (l) in K. We also have

$$a_\ell \equiv \ell + 1 \equiv 0 (\mathrm{mod}\ p).$$

The reason is as follows: from the Galois representation from Tate modules of elliptic curves defined over $\mathbb{Q}$, for any $\ell \nmid pN$, the characteristic polynomial for $\mathrm{Frob}(\ell)$ acting on $E[p]$ is

$$x^2 - a_\ell x + \ell.$$

The characteristic polynomial for $\mathrm{Frob}(\tau)$ acting on $E[p]$ is $x^2 - 1$. Since $\mathrm{Frob}(\ell) = \mathrm{Frob}(\tau)$ and characteristic polynomial depends only on the conjugacy class, one must have these two characteristic polynomials are equal mod p, i.e.

$$a_\ell \equiv 0 (\mathrm{mod}\ p), \text{ and } \ell \equiv -1 (\mathrm{mod}\ p).$$

$F_\lambda := \mathcal{O}_K/\lambda$, the residue field. It has ℓ^2 elements, since ℓ is inert in K. From the condition (4.5), we know the residue field $\mathcal{O}_{K(E[p])}/\mathfrak{p}$ is a quadratic extension of $\mathbb{Z}/(\ell) = \mathbb{F}_\ell$ for any prime $\mathfrak{p}$ in $K(E[p]$ over ℓ , but ℓ is inert in K, which means in K, we already have

$$[\mathcal{O}_K/(\lambda) : \mathbb{F}_\ell] = 2.$$

Hence λ in K splits completely in $K(E[p])$. Let $F_\lambda := \mathcal{O}_K/(\lambda)$. The above discussion implies that the reduction $\widetilde{E}$ of E over ℓ have all its p-torsion points over F_λ(Note E has good reduction over ℓ), i.e.

$$\widetilde{E}[p] = \widetilde{E}(F_\lambda)[p] \cong (\mathbb{Z}/p\mathbb{Z})^2.$$

One can also obtain the eigen values for τ. Points in $\widetilde{E}(F_\lambda) = \widetilde{E}(\mathbb{F}_{\ell^2})$ fixed by τ must be in $\widetilde{E}(\mathbb{F}_\ell)$ and vise versa. Hence $\#\widetilde{E}(F_\lambda)^+ = \ell + 1 - a_\ell$. One has

$$\widetilde{E}(F_\lambda) = \widetilde{E}(F_\lambda)^+ \oplus \widetilde{E}(F_\lambda)^-,$$

and Weil's conjecture gives

$$\#\widetilde{E}(F_{\ell^2}) = (\ell+1)^2 - a_\ell^2 = (\ell + 1 - a_\ell)(\ell + 1 + a_\ell),$$

So

$$\widetilde{\#}E(F_\lambda)^- = \ell + 1 + a_\ell.$$

$n = \prod \ell$. $G_n := \mathrm{Gal}(K_n/K_1)$. hen $G_n = \prod G_\ell$. $G_\ell \cong F_\lambda^\times/F_\ell^\times$, which is cyclic of order $\ell+1$. Fix a generator σ_l and define $\mathrm{Tr}_\ell = \sum_{\sigma\in G_\ell} \sigma$ in $\mathbb{Z}[G_\ell]$. Let D_ℓ be a solution of

$$(\sigma_l - 1)D_l = \ell + 1 - \mathrm{Tr}_\ell. \tag{4.6}$$

Suppose D_ℓ and D'_ℓ are two resolutions of (4.6), then

$$(\sigma_\ell - 1)D_\ell - (\sigma_\ell - 1)D'_\ell = (\sigma_\ell - 1)(D_\ell - D'_\ell) = 0,$$

hence D_ℓ is well-defined up to elements in $\mathbb{Z} \cdot \mathrm{Tr}_\ell$. $D_n := \prod D_\ell$.

$D_n y_n$ in $E(K_n)$ gives a class in $E(K_n)/pE(K_n)$ and is fixed by G_n.

Proof. $G_n = \prod \ell$. Hence it is enough to prove $(\sigma_\ell - 1)D_n y_n \in pE(K_n)$. $n = \ell m$. Hence

$$(\sigma_\ell - 1)D_n = (\sigma_\ell - 1)D_\ell D_m = (\ell + 1 - \mathrm{Tr}_\ell)D_m,$$

so

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

$p \mid \ell + 1$, hence it is enough to show $\mathrm{Tr}_\ell y_n \in pE(K_m)$. But $\mathrm{Tr}_\ell y_n = a_\ell \cdot y_m$ and $p \mid a_\ell$. Another property is that each prime factor λ_n of ℓ in K_n divides a unique prime λ_m of K_m, and $y_n \equiv \mathrm{Frob}(\lambda_m)(y_m)(\mathrm{mod}\ \lambda_n)$. □

[The proof of the two properties used in the above proof: By definition, x_m can be identified with $(\mathcal{O}_m, \mathcal{N}_m, [\mathcal{O}_m])$, where $\mathcal{N}_m = \mathcal{N} \cap \mathcal{O}_m$, then

$$T_\ell x_m = \sum_{\mathcal{O}_m/\mathfrak{b} = \mathbb{Z}/\ell\mathbb{Z}} (\mathrm{End}(\mathfrak{b}), \mathcal{N}_m \mathrm{End}(\mathfrak{b}) \cap \mathrm{End}(\mathfrak{b}), [\mathfrak{b}]).$$

One has that $\mathcal{O}_m = \mathbb{Z} + m\mathcal{O}_K = \mathbb{Z} + m \cdot \frac{1+\sqrt{d_K}}{2} = [1, md]$, where d_K is the discriminant of K and $d = \frac{1+\sqrt{d_K}}{2}$. From Cox p235, the cyclic sublattices of $\mathcal{O}_m$ are:

$$[1, \ell md],\ [\ell, md + j],\ j = 0, \ldots, \ell - 1.$$

For $\mathfrak{b} = [1, \ell md]$, since $\ell m = n$, $[1, \ell md] = [1, nd] = \mathcal{O}_n$, and so in this case, $\mathrm{End}(\mathfrak{b}) = \mathfrak{b} = \mathcal{O}_n$. For $\mathfrak{b} = [\ell, md + j]$, from Cox p.135 Lemma 7.5 and p.209 Theorem 10.4, we only need to consider the lattice $[1, \frac{md+j}{\ell}]$. $\frac{md+j}{\ell}$ satisfies the quadratic equation in $\mathbb{Z}[x]$:

$$\ell^2 x^2 + (-m - 2j)x + ((\frac{m}{2} + j)^2 + \frac{m^2}{4}|d_K|).$$

Note since $d_K \equiv 1 (\mathrm{mod}\ 4)$, $(\frac{m}{2} + j)^2 + \frac{m^2}{4}|d_K| \in \mathbb{Z}$. Hence $[1, \frac{md+j}{\ell}]$ is a proper ideal for the order $[1, \ell^2 \cdot \frac{md+j}{\ell}] = [1, \ell md] = [1, nd] = \mathcal{O}_n$, i.e. $\mathrm{End}(\mathfrak{b}) = \mathcal{O}_n$. Hence

$$T_\ell x_m = (\mathcal{O}_n, \mathcal{N}_n, [\mathcal{O}_n]) + \sum_{j=0}^{\ell-1} \big(\mathcal{O}_n, \mathcal{N}_n, [[1, \frac{md+j}{\ell}]]\big).$$

G_ℓ is the subgroup of $G_n = \mathrm{Gal}(K_n/K_1)$ fixing K_m, i.e. $G_\ell = \mathrm{Gal}(K_n/K_m)$ which is the subgroup of $\mathrm{Gal}(K_n/K)$ fixing K_m. Since n is square free, all sublattices of $\mathcal{O}_m$ of index ℓ, which are orders in $\mathcal{O}_n$ are those whose images of Artin map fix $j(\mathcal{O}_m)$. I.e.

$$T_\ell x_m = \mathrm{Tr}_\ell(x_n) = \sum_{\sigma \in G_\ell} (\mathcal{O}_n, \mathcal{N}_n, [\mathcal{O}_n])^\sigma. \tag{4.7}$$

From Eichler-Shimura construction, one has $\varphi(\mathrm{Tr}_\ell(x_n)) = a_\ell \cdot \varphi(x_n)$.

For the second property, since $\ell \nmid m$, λ is unramified in K_m/K. Since (λ) is also principal, λ is totally split in K_m since Artin map maps λ to the identity in $\mathrm{Gal}(K_m/K) \cong \mathrm{Pic}(\mathcal{O}_m)$. Since $\mathrm{Gal}(K_n/K_m) \cong G_\ell \cong F_\lambda^\times / F_\ell^\times$, so all primes above λ in K_n has trivial residue field extension, but factors λ_m of λ in K_m are ramified in K_n, thus must be totally ramified, i.e. $\lambda_m = (\lambda_n)^{\ell+1}$. So the residue field F_{λ_n} has ℓ^2 elements and is canonically isomorphic to F_λ. From (4.7), one sees that any point in the divisor $T_\ell(x_m)$ is the conjugate of x_n over K_n/K_m. Since λ_m is totally ramified in K_n, any point in the divisor $T_\ell(x_m) \equiv x_n (\mathrm{mod}\ \lambda_n)$.

The properties of $\{y_n\}$ forms an Euler system in the sense of Kolyvagin.

We have the following tower of Galois extension:

$$\begin{tikzcd} K_n \arrow[d, dash, "G_n"'] \arrow[dd, dash, bend left, "\mathscr{G}_n"] \\ K_1 \arrow[d, dash] \\ K \arrow[d, dash] \\ Q \end{tikzcd}$$

Let S be a set of coset rep., define

$$P_n := \sum_{\sigma \in S} \sigma(D_n y_n) \in E(K_n).$$

Then $[P_n]$ is fixed by $\mathscr{G}_n$. Use the same set S to define P_m for any $m \mid n$. Note $P_1 = y_K$. The exact sequence

$$0 \to E[p] \to E \xrightarrow{p} E \to 0$$

gives

$$0 \to E[p](K_n) \to E(K_n) \xrightarrow{p} E(K_n) \to H^1(K_n, E[p]) \to H^1(K_n, E) \xrightarrow{p} H^1(K_n, E).$$

This gives the following commutative diagram:

$$
\begin{tikzcd}
 & & & 0 \arrow[d] & \\
 & & & H^1(K_n/K, E)[p] \arrow[d, "\mathrm{Inf}"'] \arrow[d, bend left, "\widetilde{d}(n)\mapsto d(n)"] & \\
0 \arrow[r] & E(K)/pE(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[p]) \arrow[r] \arrow[r, bend left, "c(n)\mapsto d(n)"] \arrow[d, "\mathrm{Res}"', "\cong"] & H^1(K, E)[p] \arrow[r] \arrow[d, "\mathrm{Res}"] & 0 \\
0 \arrow[r] & (E(K_n)/pE(K_n))^{\mathscr{G}_n} \arrow[r, "\delta_n"] \arrow[r, bend right, "{[P_n]\mapsto\delta_n[P_n]}"'] & H^1(K_n, E[p])^{\mathscr{G}_n} \arrow[r] \arrow[u, bend right, "{\delta_n[P_n]\mapsto c(n)}"'] & H^1(K_n, E)[p]^{\mathscr{G}_n} &
\end{tikzcd}
\tag{4.8}
$$

$c(n)$ is also defined in the diagram.

The middle restriction is $\cong$. 1. the exact sequence

$$0 \to H^1(K_n/K, E(K_n)[p]) \to H^1(K, E[p]) \xrightarrow{\mathrm{Res}} H^1(K_n, E[p])^{\mathscr{G}_n}.$$

(see e.g. Serre Galois Cohomology, p15).

[Or from the usual inflation-restriction map: G is a pro-finite group, $H \triangleleft G$ with G-module M, then we have the exact sequence:

$$0 \to H^1(G/H, M^H) \to H^1(G, M) \to H^1(H, M).$$

On the other hand, for any $[\alpha] \in G/N$ and $[\sigma] \in H^1(H, M)$ which comes from the image of some element in $H^1(G, M)$, one has

$$
\begin{aligned}
\sigma^\alpha(g) &= \alpha\sigma(\alpha^{-1}g\alpha) \\
&= \alpha(\sigma(\alpha^{-1}g) + \alpha^{-1}\sigma(\alpha)) \\
&= \cdots \\
&= \alpha\sigma(\alpha^{-1}) + g\sigma(\alpha) + \sigma(\alpha),
\end{aligned}
$$

while

$$0 = \sigma(1) = \sigma(\alpha\alpha^{-1}) = \sigma(\alpha) + \alpha\sigma(\alpha^{-1}),$$

so

$$\sigma^{\alpha}(g) - \sigma(g) = g\sigma(\alpha) - \sigma(\alpha),$$

i.e.

$$[\alpha] = [\alpha^{\sigma}]$$

in $H^1(H, M)$. $\Big]$

The cokernel of the middle map: From Hochschild-Serre-Leray spectral sequence, One has

$$0 \to H^1(G/H, M^H) \to H^1(G, M) \to H^1(H, M)^{G/H} \to H^2(G/H, M^H) \to H^2(G, H),$$

one sees the cokernel maps injectively into $H^2(K_n/K, E(K_n)[p])$. Since E has no p-torsion in K_n, the middle homomorphism is $\cong$.

$c(n)$ is represented by 1-cocycle

$$f(\sigma) = \sigma(\frac{1}{p}P_n) - \frac{1}{p}P_n - \frac{(\sigma - 1)P_n}{p}.$$

τ, the complex multiplication acts on $H^1(K, E[p])$. We have a direct decomposition with respect to τ's eigenvalues ± 1:

$$H^1(K, E[p]) = H^1(K, E[p])^{+} \oplus H^1(K, E[p])^{-}.$$

Denote w_n to be the Fricke involution, then for eigenform f associate to E,

$$f\big|w_N = \epsilon f,$$

where $\epsilon = \pm 1$.

Proposition 4.6.1. *$y_n^\tau - \epsilon y_n^\sigma$ is a torsion point in $E(K_n)$ for some $\sigma \in \mathscr{G}_n$.*

Proof. The various actions on Heegnar points given above show that for any $\sigma \in \mathscr{G}_n$, one has $\mathfrak{b} \in \mathrm{Pic}(\mathcal{O})$ such that $\theta(\mathfrak{b}) = \sigma$ and

$$w_N(x_n^\sigma) = w_N(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^\tau]) = (\mathcal{O}, \mathfrak{n}^\tau, [\mathfrak{a}\mathfrak{b}^\tau\mathfrak{n}^\tau]).$$

So take $\mathfrak{b} = \mathfrak{n}^\tau(\mathfrak{a})^2$, then

$$w_N(x_n^\sigma) = x_n^\tau,$$

where $\sigma = \theta(\mathfrak{b})$. So

$$(x_n - \infty)^\tau = w_N(x_n - \infty)^\sigma + (w_N\infty - \infty).$$

Here $(w_N\infty - \infty) = (0 - \infty)$ is the torsion point in $J_0(N)$. □

Proposition 4.6.2. *$[P_n]$ is in $\epsilon_n := \epsilon(-1)^{f_n}$ eigenspace for τ, where f_n is the number of prime divisors of n. The similar results hold for $c(n)$ and $d(n)$.*

Proof. $P_n = \sum_{[\sigma] \in \mathscr{G}_n/G_n} \sigma D_n y_n$. One has $\mathrm{Gal}(K_n/\mathbb{Q}) \cong \mathscr{G}_n \rtimes \mathbb{Z}/2\mathbb{Z}$, hence

$$\sigma\tau\sigma = (\sigma, 1)\cdot(1,\tau)\cdot(\sigma,1) = (\sigma,\tau)(\sigma,1) = (\sigma(\tau\cdot\sigma),\tau) = (\sigma\sigma^{-1},\tau) = (1,\tau),$$

i.e.

$$\tau\sigma = \sigma^{-1}\tau.$$

Therefore

$$\tau P_n = \sum_{[\sigma]\in\mathscr{G}_n/G_n} \tau\sigma D_n y_n = \sum_{[\sigma]\in\mathscr{G}_n/G_n} \sigma^{-1}\tau D_n y_n.$$

Here n is square free and $D_n = \prod_{\text{prime } \ell|n} D_\ell$. Hence we only need to handle D_ℓ. Since $(\sigma_e ll - 1)D_\ell = \ell + 1 - \mathrm{Tr}_\ell$ and G_ℓ is cyclic which implies the commutativity, hence

$$(\sigma_\ell - 1)D_\ell\tau = \tau(\sigma_\ell - 1)D_\ell = (\sigma_\ell^{-1} - 1)\tau D_\ell = -\sigma_\ell^{-1}(\sigma_\ell - 1)\tau D_\ell,$$

i.e.

$$(\sigma_\ell - 1)(\tau D_\ell + \sigma_\ell D_\ell \tau) = 0,$$

so

$$\tau D_\ell = -\sigma_\ell D_\ell \tau + m\mathrm{Tr}_l,$$

for some $m \in \mathbb{Z}$. $\mathrm{Tr}_\ell y_n = a_\ell y_{n/\ell} = 0$ in $pE(K_n)$ since $p \mid a_\ell$. Also

$$\begin{aligned}
\tau D_n &= \tau \prod_{\ell|n} D_\ell \\
&= \tau D_{\ell_1} D_{\ell_2} \cdots D_{\ell_{f_n}} \\
&= -\sigma_{\ell_1} D_{\ell_1} \tau D_{\ell_2} \cdots D_{\ell_{f_n}} \\
&= \cdots \\
&= (-1)^{f_n} \prod_{\ell|n} \sigma_\ell \cdot D_n \tau.
\end{aligned}$$

Hence in $E(K_n)/pE(K_n)$,

$$\begin{aligned}
\tau P_n &= \sum_{[\sigma]\in\mathscr{G}_n/G_n} \sigma^{-1}\Big((-1)^{f_n} \prod_{\ell|n} \sigma_\ell \cdot D_n \tau(y_n)\Big) \\
&= (-1)^{f_n} \prod_{\ell|n} \sigma_\ell \cdot \sum_{[\sigma]\in\mathscr{G}_n/G_n} \sigma^{-1} \cdot D_n(\tau y_n).
\end{aligned}$$

On the other hand, $\tau y_n = \epsilon \cdot \delta(y_n) + Q$ for some $\delta \in \mathscr{G}_n$ and some torsion point in $E(K_n)$. Since $E(K_n)$ has no p-torsion points, Q actually resides in $pE(K_n)$, therefore in $E(K_n)/pE(K_n)$,

$$\tau P_n = \epsilon_n \prod_{\ell | n} \sigma_\ell \cdot \delta \cdot \sum_{[\sigma] \in \mathscr{G}_n / G_n} \sigma^{-1} D_n y_n.$$

Since in $E(K_n)/pE(K_n)$, $D_n y_n$ is fixed by G_n and $\{\sigma^{-1}\}$ is another set of representatives of $\mathscr{G}_n/G_n$, one has

$$\prod_{\ell | n} \sigma_\ell \cdot \delta \cdot \sum_{[\sigma] \in \mathscr{G}_n / G_n} \sigma^{-1} D_n y_n = P_n,$$

i.e.

$$\tau P_n = \epsilon_n P_n.$$

□

Proposition 4.6.3. 1. *The class $d(n)_v$ is locally trivial in $H^1(K_v, E)[p]$ at the archimedean place $v = \infty$, and at all finite places v of K which do not divide n.*
2. *If $n = \ell n$ and λ is the unique prime of K dividing ℓ, the class $d(n)_\lambda$ is locally trivial in $H^1(K_\lambda, E)[p]$ iff $P_m \in pE(K_{\lambda m}) = pE(K_\lambda)$ for one places λ_m of K_m dividing λ.*

Proof. Let $v = \infty$, then $K_v = \mathbb{C}$ and the Galois cohomology of E is trivial. If $v \neq \infty$ and $v \nmid n$, $d(n)$ comes from $H^1(K_n/K, E)[p]$, where K_n is unramified at v since $v \nmid n$. Hence $d(n)_v$ lies in the subgroup $H^1(K_v^{\mathrm{nr}}/K_v, E)$ which is trivial when E has good reduction at v, i.e. $v \nmid N$.

If $v \mid N$, E has bad reduction at v. Let E^0 be the connected component of the Néron module. Since $H^1(K_v^{\mathrm{nr}}/K_v, E^0) = 0$, $H^1(K_v^{\mathrm{nr}}/K_v, E) \hookrightarrow H^1(F_v, E/E^0)$. Let J_0 be the Jacobian of $X_0(N)$, then for any place $\omega \mid v$ in K_n, the class of the Heegner divisor $(x_n)-(\infty)$ in $J_0(K_{n,\omega})$ lies in J_0 up to translation by rational point $(0)-(\infty)$. Hence y_n is in E^0 up to translation by rational torsion. Since $E(\mathbb{Q})[p]$ is trivial, y_n (so $D_n y_n$ and P_n) lies in a subgroup E' whose image in E/E^0 has order prime to p. But $d(n)_v$ is killed by p, so $d(n)_v = 0$. $\square$

We need some Tate local duality. Let K_λ be a local field with ring of integers $\mathcal{O}_\lambda$ and finite residue field F_λ of characteristic ℓ. Let E be an elliptic curve over K_λ with good reduction over F_λ. One has the exact sequence

$$0 \to E[p] \to E \xrightarrow{p} E \to 0$$

for any prime number $p \neq \ell$. Hence

$$E(K_\lambda) \xrightarrow{p} E(K_\lambda) \xrightarrow{\delta} H^1(\mathrm{Gal}(K_\lambda^{\mathrm{nr}}/K_\lambda), E[p]) \to H^1(\mathrm{Gal}(K_\lambda^{\mathrm{nr}}/K_\lambda), E) = 0$$

is exact. Hence

$$E(K_\lambda)/p(K_\lambda) \cong H^1(\mathrm{Gal}(K_\lambda^{\mathrm{nr}}/K_\lambda), E[p]).$$

Weil pairing $E[p] \times E[p] \to \mu_p$ gives $E[p] \otimes E[p] \to \mu_p$ which induces the following pair by cup product:

$$<,>:\ H^1(K_\lambda, E[p]) \times H^1(K_\lambda, E[p]) \to H^2(K_\lambda, E[p] \otimes E[p]) \to H^2(K_\lambda, \mu_p) \xrightarrow[\cong]{\mathrm{inv}} \mathbb{Z}/p\mathbb{Z}. \tag{4.9}$$

Tate porves this pair is alternating and non-degenerate. We also have the exact sequence

$$0 \to E(K_\lambda)/pE(K_\lambda) \to H^1(K_\lambda, E[p]) \to H^1(K_\lambda, E)[p] \to 0.$$

Since $E(K_\lambda)/pE(K_\lambda)$ is isotropic for the pairing in (4.9), one has the non-degenerate pair:

$$<,>\colon\ E(K_\lambda)/pE(K_\lambda) \times H^1(K_\lambda, E)[p] \to \mathbb{Z}/p\mathbb{Z}. \tag{4.10}$$

[(form A course in Arithmetic by Serre). Let V be an A-module, $(V, Q : V \to A)$ is a quadratic module if Q satisfies: 1). $Q(av) = a^2 v$, $\forall a \in A, v \in V$; 2). $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bi-linear form.

Let A be a field with char $\neq 2$. Define $x \cdot y = \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$, then $(x, y) \mapsto x \cdot y$ is a bilinear symmetric form and $Q(x) = x \cdot x$. $x \in V$ is called isotropic if $Q(x) = 0$. $x \perp y$ if $x \cdot y = 0$. Q is called non-degenerate if $V^\perp = 0$. Q is called U-isotropic if $U \subset U^\perp$.]

Suppose all p-torsion points on E are define in K_λ, then fix a primitive p-th root ζ of unity in K_λ and then

$$\zeta^{<c_1, c_2>} = \{e_1, e_2\},$$

where $\{,\}$ is the Weil pairing, $e_1 = (\frac{1}{p} c_1)^{\mathrm{Frob}(\lambda) - 1}$, and c_2 corresponds to a homomorphism $\phi_2 : \mu_p \to E_p(K_\lambda)$ and $e_2 = \phi_2(\zeta)$.

Now we apply our assumption on K, l and λ (i.e. l is inert in K, $(l) = (\lambda)$ in K, $p \mid \ell + 1, a_\ell$. In this case $\mathrm{Gal}(K_\lambda/Q_\ell) \cong \mathrm{Gal}(K/Q) = \{1, \tau\}$, where τ is the complex conjugation.

Proposition 4.6.4. 1. *The eigenspaces* $(E(K_\lambda)/pE(K_\lambda))^\pm$ *and* $H^1(K_\lambda, E)[p]^\pm$ *for* τ *each has dimension* 1 *over* $\mathbb{Z}/p\mathbb{Z}$.

2. *The pairing in* (4.10) *induces non-degenerate pairings of $\mathbb{Z}/p\mathbb{Z}$-pairings as $\mathbb{Z}/p\mathbb{Z}$-vector spaces:*

$$<,>^{\pm}\colon\ (E(K_\lambda)/pE(K_\lambda))^{\pm} \times H^1(K_\lambda, E)[p]^{\pm} \to \mathbb{Z}/p\mathbb{Z}.$$

Hence if $0 \neq 0d_\lambda \in H^1(K_\lambda, E)[p]^{\pm}$ *and* $s_\lambda \in (E(K_\lambda)/pE(K_\lambda))^{\pm}$ *such that* $< s_\lambda, d_\lambda >= 0$*, then* $s_\lambda = 0$.

Proof. □

From this result, we can prove a stronger result:

Proposition 4.6.5. *Suppose $d \in H^1(K, E)[p]^{\pm}$ is locally trivial except at place λ in K. Then for any $s \in \mathrm{Sel}(E/K)[p]^{\pm}$, one has the restriction s_λ of s is* 0.

Proof. $s_\lambda \in (E(K_\lambda)/pE(K_\lambda))^{\pm}$. Indeed, from the exact sequence

$$0 \to E[p] \to E \xrightarrow{p} E \to 0,$$

one has the exact sequence

$$0 \to E(K_\lambda)/pE(K_\lambda) \to H^1(K_\lambda, E[p]) \to H^1(K_\lambda, E).$$

By definition, The image of s in $H^1(K_\lambda, E)$ is 0, hence s comes from $(E(K_\lambda)/pE(K_\lambda))^{\pm}$. Hence we only need to prove $< s_\lambda, d_\lambda >= 0$ by the proposition above.

Using (4.8), one can lift d to $H^1(K, E[p])$. The difference of two lifts is in $E(K)/pE(K)$. one has

$$\sum_v < s_v, c_v >= 0,$$

by global class field theory and from assumption, $< s_v, c_v >= 0$ for any $v \neq \lambda$, hence $< s_\lambda, c_\lambda >=< s_\lambda, d_\lambda >= 0$. □

Now from our hypothesis, p is big enough such that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. $(D, NP) = 1$ implies $K \cap \mathbb{Q}(E[p]) = \mathbb{Q}$. Hence one has the following diagram:

$$\begin{tikzcd}
 & L = K(E[p]) \arrow[dl, dash, "\mathcal{G}"'] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \mathbb{Q}(E[p]) \arrow[dl, dash, "\mathcal{G} \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})"] \\
 & \mathbb{Q} = K \cap \mathbb{Q}(E[p]) &
\end{tikzcd} \tag{4.11}$$

The center of $\mathcal{G}$ is $Z \cong (\mathbb{Z}/p\mathbb{Z})^\times$ acting on $E[p]$ as multiplication. Hence $H^0(Z, E[p]) = 0 = H^0_T(Z, E[p])$. Since both Z and $E[p]$ are finite, the Herbrand quotient $h(E[p]) = 1$, hence $H^1(E[p]) = 0$. Since Z is cyclic, $H^n(Z, E[p]) = 0$ for all $n \geq 0$.

Proposition 4.6.6. *$H^n(\mathcal{G}, E[p]) = 0$ for $n \geq 0$ and*

$$\mathrm{Res}: H^1(K, E[p]) \xrightarrow{\cong} H^1(L, E[p])^{\mathcal{G}} = Hom_{\mathcal{G}}(\mathrm{Gal}(\overline{\mathbb{Q}}/L), E(L)[p])$$

is an isomorphism as $\mathrm{Gal}(K/Q)$*-modules.*

Proof. One has the spectral sequence $H^m(\mathcal{G}/Z, H^n(Z, E[p])) \Rightarrow H^{m+n}(\mathcal{G}, E[p])$. Since $H^n(Z, E[p]) = 0$, the spectral sequence satisfies $^*(n)$ condition in the sense of Ribes'. Hence one has the exact sequence for $n \geq 1$:

$$0 \to H^n(\mathcal{G}/Z, E[p]^Z) \xrightarrow{\mathrm{Inf}} H^n(\mathcal{G}, E[p]) \xrightarrow{\mathrm{Res}} H^n(Z, E[p])^{\mathcal{G}/Z} \xrightarrow{\mathrm{tr}} H^{n+1}(\mathcal{G}/Z, E[p]^Z) \xrightarrow{\mathrm{Inf}} H^{n+1}(\mathcal{G}, E[p]).$$

Since both $E[p]^Z$ and $H^n(Z, E[p])$ are trivial, $H^n(\mathcal{G}, E[p])$ is trivial. For $n = 0$, $H^0(\mathcal{G}, E[p]) = E[p]^{\mathcal{G}} \subset E[p]^Z = 0$.

Since $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \lhd \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and their quotient is $\mathrm{Gal}(L/K) = \mathcal{G}$, one has the

Leray-Serre long exact sequence

$$0 \to H^1(\mathcal{G}, E(L)[p]) \xrightarrow{\text{Inf}} H^1(K, E[p]) \xrightarrow{\text{Res}} H^1(L, E[p])^{\mathcal{G}} \to H^2(\mathcal{G}, E[p]) = 0.$$

By the definition of L, $E(L)[p] = E[p]$, hence $H^1(\mathcal{G}, E(L)[p]) = 0$, so the restriction map is actually an isomorphism:

$$H^1(K, E[p]) \xrightarrow{\cong} H^1(L, E[p])^{\mathcal{G}} = \text{Hom}_{\mathcal{G}}(\text{Gal}(\overline{\mathbb{Q}}/L), E[p]).$$

Here $s \in \text{Hom}_{\mathcal{G}}(\text{Gal}(\overline{\mathbb{Q}}/L), E[p])$ means s is a homomorphism from $\text{Gal}(\overline{\mathbb{Q}}/L)$ to $E[p])$ such that for any $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K)$,

$$\sigma s(\sigma^{-1}\rho\sigma) = s(\rho),$$

for any $\rho \in \text{Gal}(\overline{\mathbb{Q}}/L)$. $\square$

From this proposition, we obtain a pairing:

$$[,]:\ H^1(K, E[p]) \times \text{Gal}(\overline{\mathbb{Q}}/L) \to E(L)[p], \tag{4.12}$$

which satisfies $[s^\alpha, \rho^\sigma] = [s, \rho^\sigma] = f(\sigma^{-1}\rho\sigma) = \sigma^{-1}s(\rho) = [s, \rho]^{\sigma^{-1}}$.

Now Let $S \subset H^1(K, E[p])$ be a finite subgroup, i.e. finite dimensional vector space over $\mathbb{F}_p$. Let $\text{Gal}_S(\overline{\mathbb{Q}}/L)$ be the subgroup of $\rho \in \text{Gal}(\overline{\mathbb{Q}}/L)$ such that $[s, \rho] = 0$ for all $s \in S$. Define $L_S := \overline{\mathbb{Q}}^{\text{Gal}_S(\overline{\mathbb{Q}}/L)}$. Then L_S/L is Galois. Indeed, for any $\alpha \in \text{Gal}(\overline{\mathbb{Q}}/L)$ and $\rho \in \text{Gal}_S(\overline{\mathbb{Q}}/L)$,

$$[s, \alpha^{-1}\rho\alpha] = s(\alpha^{-1}) + s(\rho) + s(\alpha) = 0,$$

since $s(\rho) = [s, \rho] = 0$. So $\alpha^{-1}\rho\alpha \in \text{Gal}_S(\overline{\mathbb{Q}}/L)$, i.e. L_S/L is Galois.

Proposition 4.6.7. *The induced pairing:*

$$[,] : S \times \mathrm{Gal}(L_S/L) \to E(L)[p] \tag{4.13}$$

is non-degenerate and it induces two isomorphisms:

$$\mathrm{Gal}(L_S/L) \xrightarrow{\cong} \mathrm{Hom}(S, E(L)[p]) \tag{4.14}$$

as $\mathcal{G}$-modules and

$$S \xrightarrow{\cong} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E(L)[p]) \tag{4.15}$$

Proof. Injectivities are obvious. Let $r = \dim_{\mathbb{F}_p}(S)$. Then $\mathrm{Gal}(L_S/L)$ is a $\mathcal{G}$-submodule of $\mathrm{Hom}(S, E[p]) \cong E[p]^r$. $E[p]$ is a simple $\mathcal{G}$-module, hence $\mathrm{Hom}(S, E[p])$ is semi-simple. Hence $\mathrm{Gal}(L_S/L) \cong E[p]^s$ for some $s \leq r$. So $\mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E[p]) \cong (\mathbb{Z}/p\mathbb{Z})^s$. Hence $r \leq s$. So $r = s$. □

Now let $S = \mathrm{Sel}^{[p]}(E/K) \subset H^1(K, E[p])$. By our assumption, y_K is not divisible by p in $E(K)$. δy_K is its image in $\mathrm{Sel}(E/K)[p]$, which is not zero. We have the following diagram:

$$\begin{tikzcd}
M := L_S \arrow[d, dash, "I"] \arrow[dd, dash, bend left=60, "H\cong\mathrm{Hom}(\mathrm{Sel}^{[p]}(E/K),E[p])"] \\
L(\frac{1}{p}y_K) = L_{<\delta y_K>} \arrow[d, dash, "{E[p]}"'] \\
L = K(E[p]) \arrow[d, dash, "\mathcal{G}"'] \\
K \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Remark: (a) from the exact sequence:

$$0 \to E[p] \to E \xrightarrow{p} E \to 0,$$

one has the exact sequence

$$0 \to E(K)/pE(K) \xrightarrow{\delta} H^1(K, E[p]) \xrightarrow{\iota} H^1(K, E).$$

From the definition of Selmer group,

$$\mathrm{Sel}^{[p]}(E/K) = \ker\{H^1(K, E[p]) \to \prod_{\mathfrak{p}} H^1(G_{\mathfrak{p}}, E)\},$$

which factors through $H^1(K, E[p]) \to H^1(K, E)$. Hence δy_K is in the Selmer group since $\iota(\delta y_K) = 0$.

(b) The connecting function δ is defined as follows:

$$\delta y_K = \big(g \mapsto (-\frac{1}{p} y_K) + g(\frac{1}{p} y_K)\big).$$

[The general theory is: for the exact sequence

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0,$$

written additively as G-modules, one has $\delta : H^0(G, C) \to H^1(G, A)$ as follows: for any $c \in C$, $\exists b \in B$ such that $p(b) = c$. Let $c \in H^0(G, C)$, then $\delta(c) = (\sigma \mapsto [i^{-1}(-b + \sigma(b))])$.] By definition, $L_{<\delta y_K>}$ is the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$, which is in turn defined as

$$\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) := \{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) \,\big|\, [\delta y_K, \rho] = 0, \forall\, s \in S\}.$$

But in this case

$$[\delta y_K, \rho] = (\delta y_K)(\rho) = -\frac{1}{p} y_K + \rho(\frac{1}{p} y_K).$$

Hence we must have

$$\rho(\frac{1}{p} y_K) = \frac{1}{p} y_K,$$

iff $\rho \in \mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$, i.e. $L(\frac{1}{p}y_K) = L_{<\delta y_K>}$.

(3). $\mathrm{Gal}(L(\frac{1}{p}y_K)/L) \cong \mathrm{Hom}(<\delta y_K>, E[p])$ which is defined by where δy_K is mapped. Hence is isomorphic to $E[p]$.

Let τ is the complex conjugation in $\mathbb{C}$. τ acts on H by conjugation. Its eigenvalues are ± 1. Now to calculate H^+ and I^+, which have the obvious meaning.

Any $\sigma \in H$ is identified by an element in $\mathrm{Hom}(\mathrm{Sel}^{[p]}, E[p])$ by $s \mapsto [s, \sigma]$, $\forall\, s \in \mathrm{Sel}^{[p]}(E/K)$. Hence σ^τ corresponds to $s \mapsto [s, \tau\sigma\tau]$ (notice that $\tau^{-1} = \tau$). Since $[s, \tau\sigma\tau]^\tau = [s, \sigma]$ ($\tau^2 = 1$), to fix by τ, we must have the form $[s, \sigma] + [s, \tau\sigma\tau]$, i.e. $H^+ = H^{\tau+1} := \{h^\tau \cdot h \,\big|\, h \in H\} = \{(\tau h)^2 \,\big|\, h \in H\}$, similarly, $I^+ = \{(\tau i)^2 \,\big|\, i \in I\}$, and so $H^+/I^+ = (H/I)^+ = E[p]^+ \cong \mathbb{Z}/p\mathbb{Z}$. Also one has

Proposition 4.6.8. *Let $s \in Sel^{[p]}(E/K)^\pm$, then the followings are equivalent:*

- *(a) $[s, \rho] = 0$, for all $\rho \in H$;*
- *(b) $[s, \rho] = 0$, for all $\rho \in H^+$;*
- *(c) $[s, \rho] = 0$, for all $\rho \in H^+ - I^+$;*
- *(d) $s = 0$.*

Proof. It is enough to prove $(c) \Rightarrow (b) \Rightarrow (a)$. $(c) \Rightarrow (b)$ is trivial by group theory. For $(b) \Rightarrow (a)$, for any $s \in \mathrm{Sel}^{[p]}(E/K)$, it induces a $\mathcal{G}$-homomorphism $H \to E[p]$ which maps $H^+ \to E[p]^\pm$ and $H^- \to E[p]^\mp$. If $[s, H^+] = 0$, then $s(H) \subset E[p]^\mp$. But $s(H)$ is a $\mathcal{G}$-submodule of the simple module $E[p]$, hence form $s(H) \neq E[p]$, one has $s(H) = 0$. $\square$

Let λ be a prime of K which does not divide Np. Then λ is unramified in $M = L_S/K$.

We assume λ splits completely in L/K and λ_M be a prime factor of λ in M. The Frobenius element ρ of λ_M in $\mathrm{Gal}(M/K)$ lies in H since λ is totally split in L/K by our assumption. Denote $\mathrm{Frob}(\lambda) = \{\rho^g \,\big|\, g \in \mathcal{G}\}$.

Proposition 4.6.9. *Let $s \in Sel^{[p]}(E/K)$. The followings are equivalent:*

(a) $[s, \rho] = 0$;

(b) $[s, \mathrm{Frob}(\lambda)] = 0$;

(c) $s_\lambda \equiv 0$ *in* $H^1(K_\lambda, E[p])$.

Proof. (a) and (b) are equivalent because of $[s, \rho^g] = [s, \rho]^g$ for any $g \in \mathcal{G}$. For $(a) \Leftrightarrow (c)$, we have the commutative diagram

$$\begin{tikzcd} H^1(K, E[p]) \arrow[r] \arrow[d, dashed] & \prod_\lambda H^1(K_\lambda, E) , \\ H^1(K_\lambda, E[p]) \arrow[ur, dashed] & \end{tikzcd}$$

and exact sequence

$$0 \to E(K_\lambda)/pE(K_\lambda) \to H^1(K_\lambda, E[p]) \to H^1(K_\lambda, E).$$

Hence from the definition of Selmer group, s_λ can be identified with an element in $E(K_\lambda)/pE(K_\lambda)$, say $s_\lambda = P_\lambda$ in $E(K_\lambda)/pE(K_\lambda)$. Then clearly $\frac{1}{p}P_\lambda$ is defined over M_{λ_M} and $[s, \rho] = -(\frac{1}{p}P_\lambda) + \rho(\frac{1}{p}P_\lambda)$ in $E(M_{\lambda_M}) = E(M)$ from the definition of the connection map which is given above. Hence $[s, \rho] = 0$ iff $P_\lambda = 0$ in $E(K_\lambda)/pE(K_\lambda)$. $\square$

Finally we reach the point to prove our main result which is given in the following two results:

Theorem 4.6.10. $\mathrm{Sel}^{[p]}(E/K)^{-\epsilon} = 0$.

Proof. Let $s \in Sel^{[p]}(E/K)^{-\epsilon}$, then is is enough to prove $[s,\rho] = 0$ for any $\rho \in H^{+} - I^{+}$. Such element has the form $\rho = (\tau h)^2$ for some $h \in H - I$. Let ℓ be a rational prime which is unramified in $M/\mathbb{Q}$, and has a factor λ_M whose Frobenius is τh. Then $(\ell) = \lambda$ inert in K and λ splits completely in L. Hence the Frobenius of F_{λ_M}/F_λ is $(\tau h)^2$. So it is enough to prove $s_\lambda = 0$ in $H^1(K_\lambda, E[p])$.

Let $c(\ell)$ and $d(\ell)$ be those constructed above. Then both are in $-\epsilon$ eigenspace. We want to prove $d(\ell)_\lambda \neq 0$. If not, then $y_K = P_1 \in pE(K_\lambda)$, hence λ splits completely in $L(\frac{1}{1}y_K)$. But $\mathrm{Frob}(\lambda) = \rho$ is not in I^{+}, this does not occur. □

Using the notation in the proof of Theorem 4.6.10, one has

Theorem 4.6.11. *The followings are equivalent:*

(1) $c(\ell) = 0$ *in* $H^1(K, E[p])$;

(2) $c(\ell) \in \mathrm{Sel}^{[p]}(E/K) \subset H^1(K, E[p])$;

(3) P_ℓ *is divisible by* p *in* $E(K_\ell)$;

(4) $d(\ell) = 0$ *in* $H^1(K, E[p])$;

(5) $d(\ell)_\lambda = 0$ *in* $H^1(K_\lambda, E[p])$;

(6) $P_1 = y_K$ *is locally divisible by* p *in* $E(K_\lambda)$;

(7) $h^{1+\tau}$ *is in* I^{+}.

Proof. Easy. □

Theorem 4.6.12. $Sel^{[p]}(E/K)^{\epsilon} \cong \mathbb{Z}/p\mathbb{Z} \cdot \delta y_K$

Proof. For $s \in zSel^{[p]}(E/K)^{\epsilon}$, it is enough to show $[s, \rho] = 0$ for all $\rho \in I$. This is because then from proposition 4.6.7, one has $s \in \mathrm{Hom}_{\mathcal{G}}(H/I, E_p) \cong \mathbb{Z}/pzZ \cdot \delta y_K$. The argument in the proof of proposition 4.6.8 gives that it is enough to show $[s, I^+] = 0$ (Replace H with I in the argument).

Let ℓ' be a prime with non-zero image $c(\ell')$ in $H^1(K, E[p])$. From theorem 4.6.11, we can select ℓ' such that its Frobenius is conjugate to τh in $\mathrm{Gal}(M/\mathbb{Q})$ for some $h \in H$ and $h^{1+\tau} \notin I^+$(Given $h \in H$ and $h^{1+\tau} \notin I^+$, from Chebotarev density theorem, prime ℓ' whose Frobenius element is conjugate to τh in $\mathrm{Gal}(M/\mathbb{Q})$ has positive Dirichlet density, for such ℓ', the proposition above implies $c(\ell')$ is non-trivial in $H^1(K, E[p])$). Hence $c(\ell') \notin \mathrm{Sel}^{[p]}$, hence the field extension $L' := L_{<c(\ell')>}$ of L has Galois group $\cong E[p]$ and $L' \cap M = L$. One obtain the following field tower:

$$
\begin{tikzcd}
 & \overline{\mathbb{Q}} \arrow[d, dash] & \\
 & M := L_S \arrow[d, dash, "I"'] \arrow[dd, dash, bend left=60, "\mathrm{Hom}(S,E[p])"] & \\
L' = L_{<c(\ell')>} \arrow[dr, dash, "E[p]"'] & L(\frac{1}{p} y_K) \arrow[d, dash, "E[p]"] & \\
 & L = K(E[p]) \arrow[d, dash, "\mathcal{G}"] & \\
 & K \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}
$$

where $S := \mathrm{Sel}^{[p]}(E/K)$. We have the prime ideal $(\ell) = \lambda$ in K which splits completely in L. It splits completely in L' iff $P_{\ell'}$ is locally a p-th power in $E(K_{\lambda_{\ell'}}) = E(K_\lambda)$ for all factors $\lambda_{\ell'}$ of λ in $K_{\ell'}$. (?)

Let ℓ be a prime whose Frobenius element is conjugate to τi in $\mathrm{Gal}(M/\mathbb{Q})$ with $i \in I$ and whose Frobenius element is conjugate to τj in $\mathrm{Gal}(L'/\mathbb{Q})$ where $j \in \mathrm{Gal}(L'/L)$ such that $j^{1+\tau} \neq 1$. Claim $d(\ell\ell')$ in $H^1(K, E)[p]^\epsilon$ is locally trivial for all places $v \neq \lambda$ and $d(\ell\ell')_\lambda \neq 0$. The local triviality for $v \neq \lambda, \lambda'$ is clear. $i \in I \implies c(\ell) = 0$ and $p \mid P_\ell$. By proposition 4.6.3, in the completion at a place dividing λ', P_ℓ is locally divisible by p and $d(\ell\ell')_{\lambda'} = 0$. Suppose $d(\ell\ell')_\lambda = 0$, then $P_{\ell'}$ is locally divisible by p in $E(K_\lambda)$, but this means λ splits in L', so $(\tau j)^2 = j^{1+\tau} = 1$, which is a contradiction.

Now we have $s_\lambda = 0$, and hence $[s, I^+] = 0$. $\square$