Heegner points and Kolyvagin's theorem on modular elliptic curves

Graduate Student Seminar, organized by H. Darmon (McGill University)

Samy MKHININI

University of Ottawa

29 October 2026



Let K be an imaginary quadratic field of discriminant $-D$, where $D \notin \{3, 4\}$, and let N be an integer satisfying the Heegner hypothesis in $K/\mathbb{Q}$.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and let $\varphi : X_0(N) \longrightarrow E$ be a modular parametrization. There exists a unique normalized newform

$$f_E(z) = \sum_{n \geq 1} a_n q^n \in S_2(\Gamma_0(N)), \qquad q = e^{2\pi i z}$$

associated to the elliptic curve $E/\mathbb{Q}$.

Consider a Heegner point $x_1 \in X_0(N)(H_K)$ and its image $y_1 = \varphi(x_1) \in E(H_K)$. Then, define:

$$y_K := \mathrm{Tr}_{H_K/K}(y_1) \in E(K).$$

Theorem (Kolyvagin)

Suppose that y_K has infinite order in $E(K)$. Then:

1. $E(K)$ has rank 1.
2. $Ш(E/K)$ is finite and has order dividing $t_{E/K}(I_K)^2$, where $t_{E/K}$ is an integer whose prime factors depend only on E and $I_K = [E(K) : \mathbb{Z}y_K]$.

Let K be an imaginary quadratic field of discriminant $-D$, where $D \notin \{3, 4\}$, and let N be an integer satisfying the Heegner hypothesis in $K/\mathbb{Q}$.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and let $\varphi : X_0(N) \longrightarrow E$ be a modular parametrization. There exists a unique normalized newform

$$f_E(z) = \sum_{n \geq 1} a_n q^n \in S_2(\Gamma_0(N)), \qquad q = e^{2\pi i z}$$

associated to the elliptic curve $E/\mathbb{Q}$.

Consider a Heegner point $x_1 \in X_0(N)(H_K)$ and its image $y_1 = \varphi(x_1) \in E(H_K)$. Then, define:

$$y_K := \mathrm{Tr}_{H_K/K}(y_1) \in E(K).$$

Theorem (Kolyvagin)

Suppose that y_K has infinite order in $E(K)$. Then:

1. $E(K)$ has rank 1.
2. $Ш(E/K)$ is finite and has order dividing $t_{E/K}(I_K)^2$, where $t_{E/K}$ is an integer whose prime factors depend only on E and $I_K = [E(K) : \mathbb{Z}y_K]$.

Let K be an imaginary quadratic field of discriminant $-D$, where $D \notin \{3, 4\}$, and let N be an integer satisfying the Heegner hypothesis in $K/\mathbb{Q}$.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and let $\varphi : X_0(N) \longrightarrow E$ be a modular parametrization. There exists a unique normalized newform

$$f_E(z) = \sum_{n \geq 1} a_n q^n \in S_2(\Gamma_0(N)), \qquad q = e^{2\pi i z}$$

associated to the elliptic curve $E/\mathbb{Q}$.

Consider a Heegner point $x_1 \in X_0(N)(H_K)$ and its image $y_1 = \varphi(x_1) \in E(H_K)$. Then, define:

$$y_K := \mathrm{Tr}_{H_K/K}(y_1) \in E(K).$$

Theorem (Kolyvagin)

Suppose that y_K has infinite order in $E(K)$. Then:

1. $E(K)$ has rank 1.
2. $Ш(E/K)$ is finite and has order dividing $t_{E/K}(I_K)^2$, where $t_{E/K}$ is an integer whose prime factors depend only on E and $I_K = [E(K) : \mathbb{Z}y_K]$.

Let K be an imaginary quadratic field of discriminant $-D$, where $D \notin \{3, 4\}$, and let N be an integer satisfying the Heegner hypothesis in $K/\mathbb{Q}$.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and let $\varphi : X_0(N) \longrightarrow E$ be a modular parametrization. There exists a unique normalized newform

$$f_E(z) = \sum_{n \geq 1} a_n q^n \in S_2(\Gamma_0(N)), \qquad q = e^{2\pi i z}$$

associated to the elliptic curve $E/\mathbb{Q}$.

Consider a Heegner point $x_1 \in X_0(N)(H_K)$ and its image $y_1 = \varphi(x_1) \in E(H_K)$. Then, define:

$$y_K := \mathrm{Tr}_{H_K/K}(y_1) \in E(K).$$

Theorem (Kolyvagin)

Suppose that y_K has infinite order in $E(K)$. Then:

1. $E(K)$ has rank 1.
2. $Ш(E/K)$ is finite and has order dividing $t_{E/K}(I_K)^2$, where $t_{E/K}$ is an integer whose prime factors depend only on E and $I_K = [E(K) : \mathbb{Z}y_K]$.

Theorem (Kolyvagin; weak form)

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 assume that p does not divide y_K in $E(K)$. Then:

1. $E(K)$ has rank 1.
2. $Ш(E/K)_p$ is trivial.

Key proposition: 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 assume that p does not divide y_K in $E(K)$. Then:

$$\mathrm{Sel}_p(E/K) \text{ is cyclic, generated by } \delta(y_K).$$

Theorem (Kolyvagin; weak form)

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 assume that p does not divide y_K in $E(K)$. Then:

1. $E(K)$ has rank 1.
2. $Ш(E/K)_p$ is trivial.

Key proposition: 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 assume that p does not divide y_K in $E(K)$. Then:

$$\mathrm{Sel}_p(E/K) \text{ is cyclic, generated by } \delta(y_K).$$

Heegner hypothesis: all prime factors of N are split in $K/\mathbb{Q}$.

$\longrightarrow \exists\, \mathcal{N} \leq \mathcal{O}_K$ such that

$$\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

$\longrightarrow \exists\, \varphi : \mathbb{C}/\mathcal{O}_K \longrightarrow \mathbb{C}/\mathcal{N}^{-1}$ cyclic of order N.

Definition (Heegner point)

The point x_1 defined by

$$x_1 = (\mathbb{C}/\mathcal{O}_K, \mathcal{N}^{-1}/\mathcal{O}_K) \in X_0(N),$$

is called **"Heegner point"** (of conductor 1).

$\longrightarrow$ x_1 is rational over H_K, the Hilbert class field of K.

Heegner hypothesis: all prime factors of N are split in $K/\mathbb{Q}$.

$\longrightarrow \exists\, \mathcal{N} \leq \mathcal{O}_K$ such that

$$\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

$\longrightarrow \exists\, \varphi : \mathbb{C}/\mathcal{O}_K \longrightarrow \mathbb{C}/\mathcal{N}^{-1}$ cyclic of order N.

Definition (Heegner point)

The point x_1 defined by

$$x_1 = (\mathbb{C}/\mathcal{O}_K, \mathcal{N}^{-1}/\mathcal{O}_K) \in X_0(N),$$

is called **"Heegner point"** (of conductor 1).

$\longrightarrow$ x_1 is rational over H_K, the Hilbert class field of K.

Heegner hypothesis: all prime factors of N are split in $K/\mathbb{Q}$.

$\longrightarrow \exists\ \mathcal{N} \leq \mathcal{O}_K$ such that

$$\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

$\longrightarrow \exists\ \varphi : \mathbb{C}/\mathcal{O}_K \longrightarrow \mathbb{C}/\mathcal{N}^{-1}$ cyclic of order N.

Definition (Heegner point)

The point x_1 defined by

$$x_1 = (\mathbb{C}/\mathcal{O}_K, \mathcal{N}^{-1}/\mathcal{O}_K) \in X_0(N),$$

is called **"Heegner point"** (of conductor 1).

$\longrightarrow$ x_1 is rational over H_K, the Hilbert class field of K.

Heegner hypothesis: all prime factors of N are split in $K/\mathbb{Q}$.

$\longrightarrow \exists\, \mathcal{N} \leq \mathcal{O}_K$ such that

$$\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

$\longrightarrow \exists\, \varphi : \mathbb{C}/\mathcal{O}_K \longrightarrow \mathbb{C}/\mathcal{N}^{-1}$ cyclic of order N.

Definition (Heegner point)

The point x_1 defined by

$$x_1 = (\mathbb{C}/\mathcal{O}_K, \mathcal{N}^{-1}/\mathcal{O}_K) \in X_0(N),$$

is called **"Heegner point"** (of conductor 1).

$\longrightarrow$ x_1 is rational over H_K, the Hilbert class field of K.

Heegner hypothesis: all prime factors of N are split in $K/\mathbb{Q}$.

$\longrightarrow \exists\ \mathcal{N} \leq \mathcal{O}_K$ such that

$$\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}.$$

$\longrightarrow \exists\ \varphi : \mathbb{C}/\mathcal{O}_K \longrightarrow \mathbb{C}/\mathcal{N}^{-1}$ cyclic of order N.

Definition (Heegner point)

The point x_1 defined by

$$x_1 = (\mathbb{C}/\mathcal{O}_K, \mathcal{N}^{-1}/\mathcal{O}_K) \in X_0(N),$$

is called **"Heegner point"** (of conductor 1).

$\longrightarrow$ x_1 is rational over H_K, the Hilbert class field of K.

Let $n \geq 1$ be an integer such that $n \wedge N = 1$, and $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$.

Set $\mathcal{N}_n := \mathcal{N} \cap \mathcal{O}_n$. The point

$$x_n = (\mathbb{C}/\mathcal{O}_n, \mathcal{N}_n^{-1}/\mathcal{O}_n) \in X_0(N)(K_n)$$

is called **"Heegner point"** (of conductor n).

Proposition

Let $\sigma \in \mathrm{Gal}(K_n/K)$. We have:

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

where $\mathfrak{a}_\sigma$ denotes an invertible ideal representing the class of σ in $\mathrm{Pic}(\mathcal{O}_n) \cong \mathrm{Gal}(K_n/K)$.

Proposition

Let $n = m\ell$, where ℓ is a prime inert in K such that $\ell \nmid m$. Then:

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

Let $n \geq 1$ be an integer such that $n \wedge N = 1$, and $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$.

Set $\mathcal{N}_n := \mathcal{N} \cap \mathcal{O}_n$. The point

$$x_n = (\mathbb{C}/\mathcal{O}_n, \mathcal{N}_n^{-1}/\mathcal{O}_n) \in X_0(N)(K_n)$$

is called **"Heegner point"** (of conductor n).

Proposition

Let $\sigma \in \mathrm{Gal}(K_n/K)$. We have:

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

where $\mathfrak{a}_\sigma$ denotes an invertible ideal representing the class of σ in $\mathrm{Pic}(\mathcal{O}_n) \cong \mathrm{Gal}(K_n/K)$.

Proposition

Let $n = m\ell$, where ℓ is a prime inert in K such that $\ell \nmid m$. Then:

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

Let $n \geq 1$ be an integer such that $n \wedge N = 1$, and $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$.

Set $\mathcal{N}_n := \mathcal{N} \cap \mathcal{O}_n$. The point

$$x_n = (\mathbb{C}/\mathcal{O}_n, \mathcal{N}_n^{-1}/\mathcal{O}_n) \in X_0(N)(K_n)$$

is called **"Heegner point"** (of conductor n).

Proposition

Let $\sigma \in \mathrm{Gal}(K_n/K)$. We have:

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

where $\mathfrak{a}_\sigma$ denotes an invertible ideal representing the class of σ in $\mathrm{Pic}(\mathcal{O}_n) \cong \mathrm{Gal}(K_n/K)$.

Proposition

Let $n = m\ell$, where ℓ is a prime inert in K such that $\ell \nmid m$. Then:

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

Let $n \geq 1$ be an integer such that $n \wedge N = 1$, and $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$.

Set $\mathcal{N}_n := \mathcal{N} \cap \mathcal{O}_n$. The point

$$x_n = (\mathbb{C}/\mathcal{O}_n, \mathcal{N}_n^{-1}/\mathcal{O}_n) \in X_0(N)(K_n)$$

is called **"Heegner point"** (of conductor n).

Proposition

Let $\sigma \in \mathrm{Gal}(K_n/K)$. We have:

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

where $\mathfrak{a}_\sigma$ denotes an invertible ideal representing the class of σ in $\mathrm{Pic}(\mathcal{O}_n) \cong \mathrm{Gal}(K_n/K)$.

Proposition

Let $n = m\ell$, where ℓ is a prime inert in K such that $\ell \nmid m$. Then:

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

The points $y_n = \varphi(x_n) \in E(K_n)$ are called **"Heegner points"** on E. From now on, n is square-free and no prime divisor ℓ of n divides pND.

Let $\mathrm{Frob}(\ell)$ be the conjugacy class in $\mathrm{Gal}(K(E_p)/\mathbb{Q})$ of each Frobenius of $\mathrm{Gal}(\mathbb{F}_\gamma/\mathbb{F}_\ell)$, for every prime γ above ℓ.

Definition (Kolyvagin prime)

A prime ℓ as above satisfying the relation

$$\mathrm{Frob}(\ell) = \mathrm{Frob}(\infty)$$

is called a **"Kolyvagin prime"**.

$\longrightarrow$ Let λ be the unique prime of K lying above ℓ.

Proposition

If ℓ is a Kolyvagin prime, then:

$$a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}.$$

The points $y_n = \varphi(x_n) \in E(K_n)$ are called **"Heegner points"** on E. From now on, n is square-free and no prime divisor ℓ of n divides pND.

Let Frob(ℓ) be the conjugacy class in Gal($K(E_p)/\mathbb{Q}$) of each Frobenius of Gal($\mathbb{F}_\gamma/\mathbb{F}_\ell$), for every prime γ above ℓ.

Definition (Kolyvagin prime)

A prime ℓ as above satisfying the relation

$$\text{Frob}(\ell) = \text{Frob}(\infty)$$

is called a **"Kolyvagin prime"**.

$\longrightarrow$ Let λ be the unique prime of K lying above ℓ.

Proposition

If ℓ is a Kolyvagin prime, then:

$$a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}.$$

The points $y_n = \varphi(x_n) \in E(K_n)$ are called **"Heegner points"** on E. From now on, n is square-free and no prime divisor ℓ of n divides pND.

Let Frob(ℓ) be the conjugacy class in Gal($K(E_p)/\mathbb{Q}$) of each Frobenius of Gal($\mathbb{F}_\gamma/\mathbb{F}_\ell$), for every prime γ above ℓ.

Definition (Kolyvagin prime)

A prime ℓ as above satisfying the relation

$$\text{Frob}(\ell) = \text{Frob}(\infty)$$

is called a **"Kolyvagin prime"**.

$\longrightarrow$ Let λ be the unique prime of K lying above ℓ.

Proposition

If ℓ is a Kolyvagin prime, then:

$$a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}.$$

The points $y_n = \varphi(x_n) \in E(K_n)$ are called **"Heegner points"** on E. From now on, n is square-free and no prime divisor ℓ of n divides pND.

Let Frob(ℓ) be the conjugacy class in Gal($K(E_p)/\mathbb{Q}$) of each Frobenius of Gal($\mathbb{F}_\gamma/\mathbb{F}_\ell$), for every prime γ above ℓ.

Definition (Kolyvagin prime)

A prime ℓ as above satisfying the relation

$$\text{Frob}(\ell) = \text{Frob}(\infty)$$

is called a **"Kolyvagin prime"**.

$\longrightarrow$ Let λ be the unique prime of K lying above ℓ.

Proposition

If ℓ is a Kolyvagin prime, then:

$$a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}.$$

The points $y_n = \varphi(x_n) \in E(K_n)$ are called **"Heegner points"** on E. From now on, n is square-free and no prime divisor ℓ of n divides pND.

Let Frob(ℓ) be the conjugacy class in $\mathrm{Gal}(K(E_p)/\mathbb{Q})$ of each Frobenius of $\mathrm{Gal}(\mathbb{F}_\gamma/\mathbb{F}_\ell)$, for every prime γ above ℓ.

Definition (Kolyvagin prime)

A prime ℓ as above satisfying the relation

$$\mathrm{Frob}(\ell) = \mathrm{Frob}(\infty)$$

is called a **"Kolyvagin prime"**.

$\longrightarrow$ Let λ be the unique prime of K lying above ℓ.

Proposition

If ℓ is a Kolyvagin prime, then:

$$a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}.$$

Let $\mathcal{N} = \{n : n \wedge N = 1, n \text{ is square-free, and every } \ell \mid n \text{ is a Kolyvagin prime}\}$.

Consider the collection $(y_n)_{n\in\mathcal{N}}$ of Heegner points.

The system of Heegner points satisfies the Euler system properties:

Proposition

If $n = m\ell \in \mathcal{N}$, then:

1. $\mathrm{Tr}_\ell(y_n) = a_\ell y_m \in E(K_m)$;
2. Every prime λ_n lying above ℓ in K_n lies above a unique prime λ_m of K_m. Moreover,

$$y_n \equiv \mathrm{Frob}(\lambda_m)(y_m) \pmod{\lambda_n}.$$

Let $\mathcal{N} = \{n : n \wedge N = 1, n \text{ is square-free, and every } \ell \mid n \text{ is a Kolyvagin prime}\}$.

Consider the collection $(y_n)_{n\in\mathcal{N}}$ of Heegner points.

The system of Heegner points satisfies the Euler system properties:

Proposition

If $n = m\ell \in \mathcal{N}$, then:

1. $\mathrm{Tr}_\ell(y_n) = a_\ell y_m \in E(K_m)$;
2. Every prime λ_n lying above ℓ in K_n lies above a unique prime λ_m of K_m. Moreover,

$$y_n \equiv \mathrm{Frob}(\lambda_m)(y_m) \pmod{\lambda_n}.$$

Let $\mathcal{N} = \{n : n \wedge N = 1, n \text{ is square-free, and every } \ell \mid n \text{ is a Kolyvagin prime}\}$.

Consider the collection $(y_n)_{n\in\mathcal{N}}$ of Heegner points.

The system of Heegner points satisfies the Euler system properties:

Proposition

If $n = m\ell \in \mathcal{N}$, then:

1. $\mathrm{Tr}_\ell(y_n) = a_\ell y_m \in E(K_m)$;
2. Every prime λ_n lying above ℓ in K_n lies above a unique prime λ_m of K_m. Moreover,

$$y_n \equiv \mathrm{Frob}(\lambda_m)(y_m) \pmod{\lambda_n}.$$

Let $\mathcal{N} = \{n : n \wedge N = 1, n \text{ is square-free, and every } \ell \mid n \text{ is a Kolyvagin prime}\}$.

Consider the collection $(y_n)_{n\in\mathcal{N}}$ of Heegner points.

The system of Heegner points satisfies the Euler system properties:

Proposition

If $n = m\ell \in \mathcal{N}$, then:

1. $\mathrm{Tr}_\ell(y_n) = a_\ell y_m \in E(K_m)$;
2. Every prime λ_n lying above ℓ in K_n lies above a unique prime λ_m of K_m. Moreover,

$$y_n \equiv \mathrm{Frob}(\lambda_m)(y_m) \pmod{\lambda_n}.$$

Let ℓ be a Kolyvagin prime as above and write $n = m\ell$.

Fix a generator σ_ℓ of $G_\ell = \mathrm{Gal}(K_n/K_m) \leq G_n = \mathrm{Gal}(K_n/K_1)$. Consider the equation:

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

where $\mathrm{Tr}_\ell := \sum_{\sigma \in G_\ell} \sigma \in \mathbb{Z}[G_\ell]$.

Let D_n be the product of the chosen solutions D_ℓ, over all prime divisors ℓ of n. Kolyvagin uses the solution

$$D_\ell^0 = \sum_{i=1}^{\ell} i.\sigma_\ell^i = -\sum_{i=1}^{\ell+1} \frac{\sigma_\ell^i - 1}{\sigma_\ell - 1}.$$

$\longrightarrow$ By construction, $D_n(y_n)$ lies in $E(K_n)$, and the class $[D_n(y_n)] \in E(K_n)/pE(K_n)$ satisfies the relation:

$$\sigma([D_n(y_n)]) = [D_n(y_n)], \quad \forall \sigma \in G_n.$$

Next goal: Construct a point in $E(K_n)/pE(K_n)$ invariant under $\mathcal{G}_n := \mathrm{Gal}(K_n/K)$.

Let ℓ be a Kolyvagin prime as above and write $n = m\ell$.

Fix a generator σ_ℓ of $G_\ell = \mathrm{Gal}(K_n/K_m) \leq G_n = \mathrm{Gal}(K_n/K_1)$. Consider the equation:

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

where $\mathrm{Tr}_\ell := \sum_{\sigma \in G_\ell} \sigma \in \mathbb{Z}[G_\ell]$.

Let D_n be the product of the chosen solutions D_ℓ, over all prime divisors ℓ of n. Kolyvagin uses the solution

$$D_\ell^0 = \sum_{i=1}^{\ell} i.\sigma_\ell^i = -\sum_{i=1}^{\ell+1} \frac{\sigma_\ell^i - 1}{\sigma_\ell - 1}.$$

$\longrightarrow$ By construction, $D_n(y_n)$ lies in $E(K_n)$, and the class $[D_n(y_n)] \in E(K_n)/pE(K_n)$ satisfies the relation:

$$\sigma([D_n(y_n)]) = [D_n(y_n)], \quad \forall \sigma \in G_n.$$

Next goal: Construct a point in $E(K_n)/pE(K_n)$ invariant under $\mathcal{G}_n := \mathrm{Gal}(K_n/K)$.

Let ℓ be a Kolyvagin prime as above and write $n = m\ell$.

Fix a generator σ_ℓ of $G_\ell = \mathrm{Gal}(K_n/K_m) \leq G_n = \mathrm{Gal}(K_n/K_1)$. Consider the equation:

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

where $\mathrm{Tr}_\ell := \sum_{\sigma \in G_\ell} \sigma \in \mathbb{Z}[G_\ell]$.

Let D_n be the product of the chosen solutions D_ℓ, over all prime divisors ℓ of n. Kolyvagin uses the solution

$$D_\ell^0 = \sum_{i=1}^{\ell} i.\sigma_\ell^i = -\sum_{i=1}^{\ell+1} \frac{\sigma_\ell^i - 1}{\sigma_\ell - 1}.$$

$\longrightarrow$ By construction, $D_n(y_n)$ lies in $E(K_n)$, and the class $[D_n(y_n)] \in E(K_n)/pE(K_n)$ satisfies the relation:

$$\sigma([D_n(y_n)]) = [D_n(y_n)], \quad \forall \sigma \in G_n.$$

Next goal: Construct a point in $E(K_n)/pE(K_n)$ invariant under $\mathcal{G}_n := \mathrm{Gal}(K_n/K)$.

Let ℓ be a Kolyvagin prime as above and write $n = m\ell$.

Fix a generator σ_ℓ of $G_\ell = \mathrm{Gal}(K_n/K_m) \leq G_n = \mathrm{Gal}(K_n/K_1)$. Consider the equation:

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

where $\mathrm{Tr}_\ell := \sum_{\sigma \in G_\ell} \sigma \in \mathbb{Z}[G_\ell]$.

Let D_n be the product of the chosen solutions D_ℓ, over all prime divisors ℓ of n. Kolyvagin uses the solution

$$D_\ell^0 = \sum_{i=1}^{\ell} i.\sigma_\ell^i = -\sum_{i=1}^{\ell+1} \frac{\sigma_\ell^i - 1}{\sigma_\ell - 1}.$$

$\longrightarrow$ By construction, $D_n(y_n)$ lies in $E(K_n)$, and the class $[D_n(y_n)] \in E(K_n)/pE(K_n)$ satisfies the relation:

$$\sigma([D_n(y_n)]) = [D_n(y_n)], \quad \forall \sigma \in G_n.$$

Next goal: Construct a point in $E(K_n)/pE(K_n)$ invariant under $\mathcal{G}_n := \mathrm{Gal}(K_n/K)$.

Let ℓ be a Kolyvagin prime as above and write $n = m\ell$.

Fix a generator σ_ℓ of $G_\ell = \mathrm{Gal}(K_n/K_m) \leq G_n = \mathrm{Gal}(K_n/K_1)$. Consider the equation:

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

where $\mathrm{Tr}_\ell := \sum_{\sigma \in G_\ell} \sigma \in \mathbb{Z}[G_\ell]$.

Let D_n be the product of the chosen solutions D_ℓ, over all prime divisors ℓ of n. Kolyvagin uses the solution

$$D_\ell^0 = \sum_{i=1}^{\ell} i.\sigma_\ell^i = -\sum_{i=1}^{\ell+1} \frac{\sigma_\ell^i - 1}{\sigma_\ell - 1}.$$

$\longrightarrow$ By construction, $D_n(y_n)$ lies in $E(K_n)$, and the class $[D_n(y_n)] \in E(K_n)/pE(K_n)$ satisfies the relation:

$$\sigma([D_n(y_n)]) = [D_n(y_n)], \quad \forall \sigma \in G_n.$$

Next goal: Construct a point in $E(K_n)/pE(K_n)$ invariant under $\mathcal{G}_n := \mathrm{Gal}(K_n/K)$.

Here we use the Galois group hypothesis for the first time.

Let S be a set of coset representatives for G_n in $\mathcal{G}_n$. Define $P_n = \sum_{\sigma \in S} \sigma(D_n(y_n)) \in E(K_n)$.

Lemma

The curve E has no p-torsion rational over K_n.

Corollary

There is an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(K_n, E_p)^{\mathcal{G}_n}$.

The Hochschild-Serre spectral sequence gives:

$$0 \to H^1(\mathcal{G}_n, H^0(G_{K_n}, E_p)) \overset{\text{Inf}}{\to} H^1(K, E_p) \overset{\text{Res}_1}{\to} H^1(K_n, E_p)^{\mathcal{G}_n} \overset{\text{Trans}}{\to} H^2(\mathcal{G}_n, H^0(G_{K_n}, E_p)).$$

Here we use the Galois group hypothesis for the first time.

Let S be a set of coset representatives for G_n in $\mathcal{G}_n$. Define $P_n = \sum_{\sigma \in S} \sigma(D_n(y_n)) \in E(K_n)$.

Lemma

The curve E has no p-torsion rational over K_n.

Corollary

There is an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(K_n, E_p)^{\mathcal{G}_n}$.

The Hochschild-Serre spectral sequence gives:

$$0 \to H^1(\mathcal{G}_n, H^0(G_{K_n}, E_p)) \xrightarrow{\text{Inf}} H^1(K, E_p) \xrightarrow{\text{Res}_1} H^1(K_n, E_p)^{\mathcal{G}_n} \xrightarrow{\text{Trans}} H^2(\mathcal{G}_n, H^0(G_{K_n}, E_p)).$$

Here we use the Galois group hypothesis for the first time.

Let S be a set of coset representatives for G_n in $\mathcal{G}_n$. Define $P_n = \sum_{\sigma \in S} \sigma(D_n(y_n)) \in E(K_n)$.

Lemma

The curve E has no p-torsion rational over K_n.

Corollary

There is an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(K_n, E_p)^{\mathcal{G}_n}$.

The Hochschild-Serre spectral sequence gives:

$$0 \to H^1(\mathcal{G}_n, H^0(G_{K_n}, E_p)) \xrightarrow{\text{Inf}} H^1(K, E_p) \xrightarrow{\text{Res}_1} H^1(K_n, E_p)^{\mathcal{G}_n} \xrightarrow{\text{Trans}} H^2(\mathcal{G}_n, H^0(G_{K_n}, E_p)).$$

Here we use the Galois group hypothesis for the first time.

Let S be a set of coset representatives for G_n in $\mathcal{G}_n$. Define $P_n = \sum_{\sigma \in S} \sigma(D_n(y_n)) \in E(K_n)$.

Lemma

The curve E has no p-torsion rational over K_n.

Corollary

There is an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(K_n, E_p)^{\mathcal{G}_n}$.

The Hochschild-Serre spectral sequence gives:

$$0 \to H^1(\mathcal{G}_n, H^0(G_{K_n}, E_p)) \xrightarrow{\text{Inf}} H^1(K, E_p) \xrightarrow{\text{Res}_1} H^1(K_n, E_p)^{\mathcal{G}_n} \xrightarrow{\text{Trans}} H^2(\mathcal{G}_n, H^0(G_{K_n}, E_p)).$$

Here we use the Galois group hypothesis for the first time.

Let S be a set of coset representatives for G_n in $\mathcal{G}_n$. Define $P_n = \sum_{\sigma \in S} \sigma(D_n(y_n)) \in E(K_n)$.

Lemma

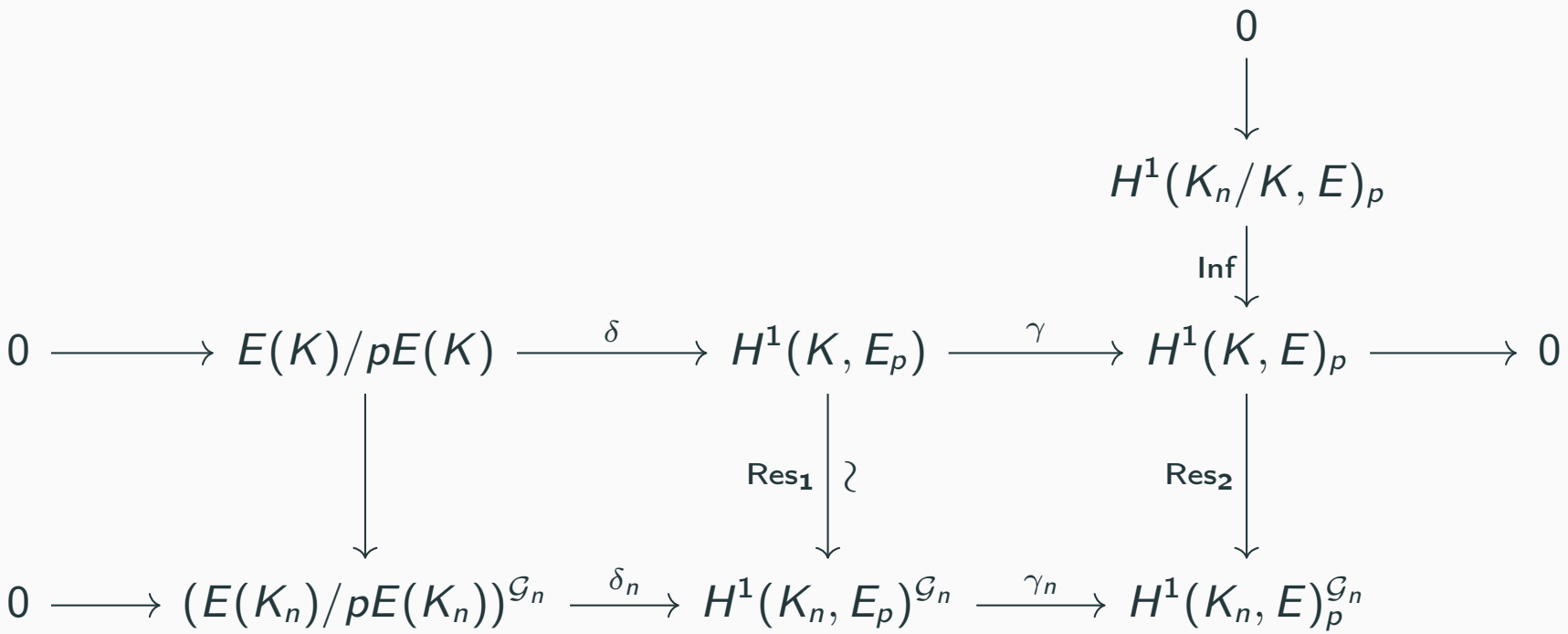
The curve E has no p-torsion rational over K_n.

Corollary

There is an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(K_n, E_p)^{\mathcal{G}_n}$.

The Hochschild-Serre spectral sequence gives:

$$0 \to H^1(\mathcal{G}_n, H^0(G_{K_n}, E_p)) \overset{\text{Inf}}{\to} H^1(K, E_p) \overset{\text{Res}_1}{\to} H^1(K_n, E_p)^{\mathcal{G}_n} \overset{\text{Trans}}{\to} H^2(\mathcal{G}_n, H^0(G_{K_n}, E_p)).$$

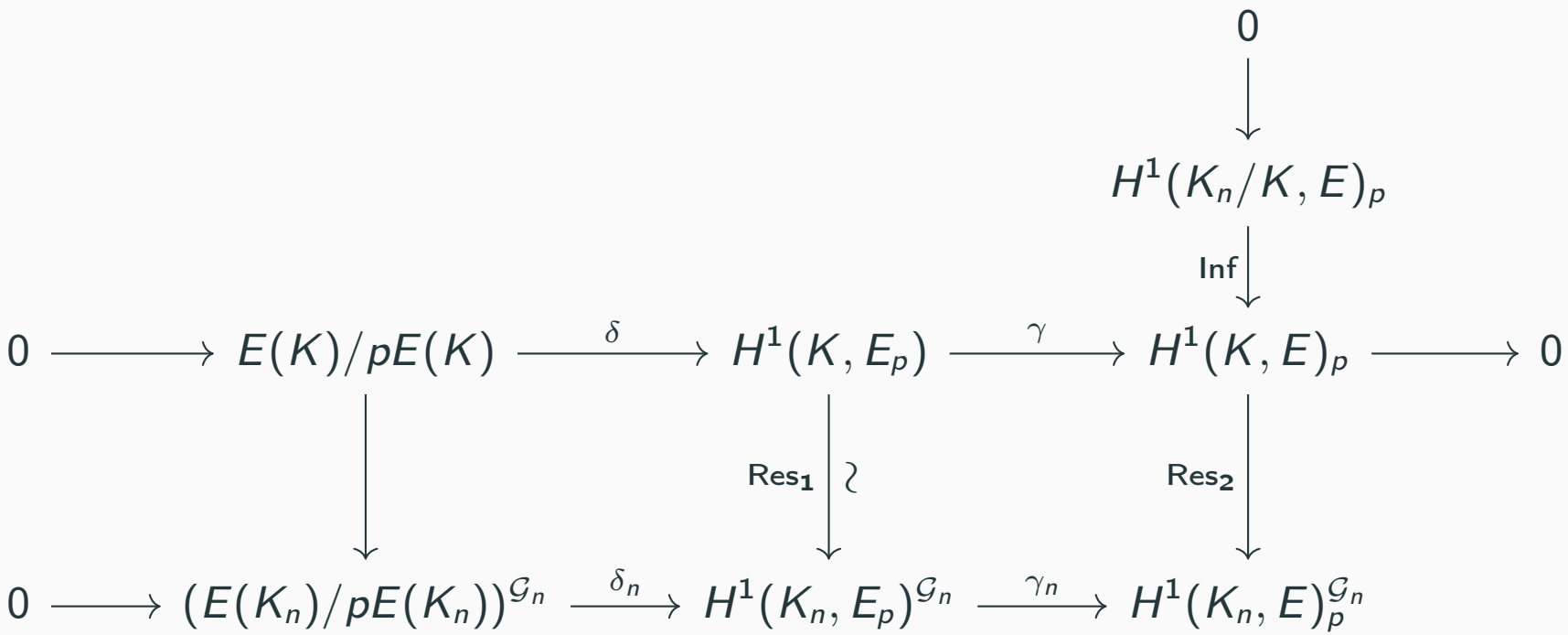


Definition (cohomology classes $c(n)$)

Define $c(n) \in H^1(K, E_p)$ as the unique class satisfying

$$\mathrm{Res}_1(c(n)) = \delta_n([P_n]).$$

Let $d(n) = \gamma(c(n))$ and let $\widetilde{d(n)}$ be defined by $\mathrm{Inf}(\widetilde{d(n)}) = d(n)$.



Definition (cohomology classes $c(n)$)

Define $c(n) \in H^1(K, E_p)$ as the unique class satisfying

$$\mathrm{Res}_1(c(n)) = \delta_n([P_n]).$$

Let $d(n) = \gamma(c(n))$ and let $\widetilde{d(n)}$ be defined by $\mathrm{Inf}(\widetilde{d(n)}) = d(n)$.

$\longrightarrow$ $c(n)$ is trivial iff $P_n \in pE(K_n)$.

$\longrightarrow$ $d(n)$ and $\widetilde{d(n)}$ are trivial iff $P_n \in pE(K_n) + E(K)$.

Fact: The complex conjugation τ acts on y_n by:

$$\tau(y_n) = \epsilon\sigma'(y_n) + \text{ (torsion)},$$

for some $\sigma' \in \mathcal{G}_n$, where $\epsilon = \pm 1$ is the eigenvalue of the Fricke involution ω_N on the eigenform f associated to the modular curve E.

Proposition

Set $\epsilon_n := \epsilon.(-1)^{\#\{\ell|n\}}$.

1. $[P_n]$ lies in the ϵ_n-eigenspace for τ in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$.
2. $c(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E_p)$ and $d(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E)_p$.

Corollary

$d(n)$ is trivial in $H^1(K, E)_p^{\epsilon_n}$ iff $P_n \in pE(K_n) + E(K)^{\epsilon_n}$.

$\longrightarrow$ $c(n)$ is trivial iff $P_n \in pE(K_n)$.

$\longrightarrow$ $d(n)$ and $\widetilde{d(n)}$ are trivial iff $P_n \in pE(K_n) + E(K)$.

Fact: The complex conjugation τ acts on y_n by:

$$\tau(y_n) = \epsilon\sigma'(y_n) + \text{ (torsion)},$$

for some $\sigma' \in \mathcal{G}_n$, where $\epsilon = \pm 1$ is the eigenvalue of the Fricke involution ω_N on the eigenform f associated to the modular curve E.

Proposition

Set $\epsilon_n := \epsilon.(-1)^{\#\{\ell|n\}}$.

1. $[P_n]$ lies in the ϵ_n-eigenspace for τ in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$.
2. $c(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E_p)$ and $d(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E)_p$.

Corollary

$d(n)$ is trivial in $H^1(K, E)_p^{\epsilon_n}$ iff $P_n \in pE(K_n) + E(K)^{\epsilon_n}$.

$\longrightarrow$ $c(n)$ is trivial iff $P_n \in pE(K_n)$.

$\longrightarrow$ $d(n)$ and $\widetilde{d(n)}$ are trivial iff $P_n \in pE(K_n) + E(K)$.

Fact: The complex conjugation τ acts on y_n by:

$$\tau(y_n) = \epsilon\sigma'(y_n) + \text{ (torsion)},$$

for some $\sigma' \in \mathcal{G}_n$, where $\epsilon = \pm 1$ is the eigenvalue of the Fricke involution ω_N on the eigenform f associated to the modular curve E.

Proposition

Set $\epsilon_n := \epsilon.(-1)^{\#\{\ell | n\}}$.

1. $[P_n]$ lies in the ϵ_n-eigenspace for τ in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$.
2. $c(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E_p)$ and $d(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E)_p$.

Corollary

$d(n)$ is trivial in $H^1(K, E)_p^{\epsilon_n}$ iff $P_n \in pE(K_n) + E(K)^{\epsilon_n}$.

$\longrightarrow$ $c(n)$ is trivial iff $P_n \in pE(K_n)$.

$\longrightarrow$ $d(n)$ and $\widetilde{d(n)}$ are trivial iff $P_n \in pE(K_n) + E(K)$.

Fact: The complex conjugation τ acts on y_n by:

$$\tau(y_n) = \epsilon\sigma'(y_n) + \text{ (torsion)},$$

for some $\sigma' \in \mathcal{G}_n$, where $\epsilon = \pm 1$ is the eigenvalue of the Fricke involution ω_N on the eigenform f associated to the modular curve E.

Proposition

Set $\epsilon_n := \epsilon.(-1)^{\#\{\ell | n\}}$.

1. $[P_n]$ lies in the ϵ_n-eigenspace for τ in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$.
2. $c(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E_p)$ and $d(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E)_p$.

Corollary

$d(n)$ is trivial in $H^1(K, E)_p^{\epsilon_n}$ iff $P_n \in pE(K_n) + E(K)^{\epsilon_n}$.

$\longrightarrow$ $c(n)$ is trivial iff $P_n \in pE(K_n)$.

$\longrightarrow$ $d(n)$ and $\widetilde{d(n)}$ are trivial iff $P_n \in pE(K_n) + E(K)$.

Fact: The complex conjugation τ acts on y_n by:

$$\tau(y_n) = \epsilon\sigma'(y_n) + \text{ (torsion)},$$

for some $\sigma' \in \mathcal{G}_n$, where $\epsilon = \pm 1$ is the eigenvalue of the Fricke involution ω_N on the eigenform f associated to the modular curve E.

Proposition

Set $\epsilon_n := \epsilon.(-1)^{\#\{\ell|n\}}$.

1. $[P_n]$ lies in the ϵ_n-eigenspace for τ in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$.
2. $c(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E_p)$ and $d(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E)_p$.

Corollary

$d(n)$ is trivial in $H^1(K, E)_p^{\epsilon_n}$ iff $P_n \in pE(K_n) + E(K)^{\epsilon_n}$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \xrightarrow{\gamma} & H^1(K, E)_p & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow g & & \\ 0 & \longrightarrow & \prod_v E(K_v)/pE(K_v) & \longrightarrow & \prod_v H^1(K_v, E_p) & \longrightarrow & \prod_v H^1(K_v, E)_p & \longrightarrow & 0 \end{array}$$

$$\mathrm{Sel}_p(E/K) = \ker\left(H^1(K, E_p) \xrightarrow{g\circ\gamma} \prod_v H^1(K_v, E)_p\right)$$

$\longrightarrow c(n) \in \mathrm{Sel}_p(E/K) \iff d(n)_v = 0$ for every place v of K.

Proposition

1. $d(n)_v$ is trivial at $v = \infty$ and at all finite places v of K such that $v \nmid n$.
2. If $n = m\ell$, then $d(n)_\lambda$ is trivial iff $P_m \in pE(K_{\lambda_m}) = pE(K_\lambda)$, where λ is the unique prime of K lying above ℓ, and λ_m is a place of K_m lying above λ.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \xrightarrow{\gamma} & H^1(K, E)_p & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow g & & \\ 0 & \longrightarrow & \prod_v E(K_v)/pE(K_v) & \longrightarrow & \prod_v H^1(K_v, E_p) & \longrightarrow & \prod_v H^1(K_v, E)_p & \longrightarrow & 0 \end{array}$$

$$\mathrm{Sel}_p(E/K) = \ker\left(H^1(K, E_p) \xrightarrow{g\circ\gamma} \prod_v H^1(K_v, E)_p\right)$$

$\longrightarrow c(n) \in \mathrm{Sel}_p(E/K) \iff d(n)_v = 0$ for every place v of K.

Proposition

1. $d(n)_v$ is trivial at $v = \infty$ and at all finite places v of K such that $v \nmid n$.
2. If $n = m\ell$, then $d(n)_\lambda$ is trivial iff $P_m \in pE(K_{\lambda_m}) = pE(K_\lambda)$, where λ is the unique prime of K lying above ℓ, and λ_m is a place of K_m lying above λ.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \xrightarrow{\gamma} & H^1(K, E)_p & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow g & & \\ 0 & \longrightarrow & \prod_v E(K_v)/pE(K_v) & \longrightarrow & \prod_v H^1(K_v, E_p) & \longrightarrow & \prod_v H^1(K_v, E)_p & \longrightarrow & 0 \end{array}$$

$$\mathrm{Sel}_p(E/K) = \ker\left(H^1(K, E_p) \xrightarrow{g\circ\gamma} \prod_v H^1(K_v, E)_p\right)$$

$\longrightarrow c(n) \in \mathrm{Sel}_p(E/K) \iff d(n)_v = 0$ for every place v of K.

Proposition

1. $d(n)_v$ is trivial at $v = \infty$ and at all finite places v of K such that $v \nmid n$.
2. If $n = m\ell$, then $d(n)_\lambda$ is trivial iff $P_m \in pE(K_{\lambda_m}) = pE(K_\lambda)$, where λ is the unique prime of K lying above ℓ, and λ_m is a place of K_m lying above λ.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \xrightarrow{\gamma} & H^1(K, E)_p & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle g} & & \\ 0 & \longrightarrow & \prod_v E(K_v)/pE(K_v) & \longrightarrow & \prod_v H^1(K_v, E_p) & \longrightarrow & \prod_v H^1(K_v, E)_p & \longrightarrow & 0 \end{array}$$

$$\text{Sel}_p(E/K) = \ker\left(H^1(K, E_p) \xrightarrow{g\circ\gamma} \prod_v H^1(K_v, E)_p\right)$$

$\longrightarrow c(n) \in \text{Sel}_p(E/K) \iff d(n)_v = 0$ for every place v of K.

Proposition

1. $d(n)_v$ is trivial at $v = \infty$ and at all finite places v of K such that $v \nmid n$.
2. If $n = m\ell$, then $d(n)_\lambda$ is trivial iff $P_m \in pE(K_{\lambda_m}) = pE(K_\lambda)$, where λ is the unique prime of K lying above ℓ, and λ_m is a place of K_m lying above λ.

The Weil pairing induces a cup-product pairing in Galois cohomology:

$$H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Local Tate duality: The pairing $\langle \cdot, \cdot \rangle : H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}$ is symmetric and non-degenerate.

Proposition

The pairing $\langle \cdot, \cdot \rangle$ induces a non-degenerate pairing of $\mathbb{Z}/p\mathbb{Z}$-vector spaces

$$\langle \cdot, \cdot \rangle : E(K_\lambda)/pE(K_\lambda) \times H^1(K_\lambda, E)_p \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Theorem

Assume that the class $d(n) \in H^1(K, E)_p^{\pm}$ is locally trivial for all places $v \neq \lambda$ of K and $d(n)_\lambda$ is non-trivial in $H^1(K_\lambda, E)_p^{\pm}$. Then, for any class $s \in \mathrm{Sel}_p(E/K)^{\pm} \subset H^1(K, E_p)^{\pm}$,

$$s_\lambda = 0 \in H^1(K_\lambda, E_p)^{\pm}.$$

The Weil pairing induces a cup-product pairing in Galois cohomology:

$$H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Local Tate duality: The pairing $\langle \cdot, \cdot \rangle : H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}$ is symmetric and non-degenerate.

Proposition

The pairing $\langle \cdot, \cdot \rangle$ induces a non-degenerate pairing of $\mathbb{Z}/p\mathbb{Z}$-vector spaces

$$\langle \cdot, \cdot \rangle : E(K_\lambda)/pE(K_\lambda) \times H^1(K_\lambda, E)_p \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Theorem

Assume that the class $d(n) \in H^1(K, E)_p^{\pm}$ is locally trivial for all places $v \neq \lambda$ of K and $d(n)_\lambda$ is non-trivial in $H^1(K_\lambda, E)_p^{\pm}$. Then, for any class $s \in \mathrm{Sel}_p(E/K)^{\pm} \subset H^1(K, E_p)^{\pm}$,

$$s_\lambda = 0 \in H^1(K_\lambda, E_p)^{\pm}.$$

The Weil pairing induces a cup-product pairing in Galois cohomology:

$$H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Local Tate duality: The pairing $\langle \cdot, \cdot \rangle : H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}$ is symmetric and non-degenerate.

Proposition

The pairing $\langle \cdot, \cdot \rangle$ induces a non-degenerate pairing of $\mathbb{Z}/p\mathbb{Z}$-vector spaces

$$\langle \cdot, \cdot \rangle : E(K_\lambda)/pE(K_\lambda) \times H^1(K_\lambda, E)_p \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Theorem

Assume that the class $d(n) \in H^1(K, E)_p^{\pm}$ is locally trivial for all places $v \neq \lambda$ of K and $d(n)_\lambda$ is non-trivial in $H^1(K_\lambda, E)_p^{\pm}$. Then, for any class $s \in \mathrm{Sel}_p(E/K)^{\pm} \subset H^1(K, E_p)^{\pm}$,

$$s_\lambda = 0 \in H^1(K_\lambda, E_p)^{\pm}.$$

The Weil pairing induces a cup-product pairing in Galois cohomology:

$$H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Local Tate duality: The pairing $\langle \cdot, \cdot \rangle : H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}$ is symmetric and non-degenerate.

Proposition

The pairing $\langle \cdot, \cdot \rangle$ induces a non-degenerate pairing of $\mathbb{Z}/p\mathbb{Z}$-vector spaces

$$\langle \cdot, \cdot \rangle : E(K_\lambda)/pE(K_\lambda) \times H^1(K_\lambda, E)_p \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Theorem

Assume that the class $d(n) \in H^1(K, E)_p^{\pm}$ is locally trivial for all places $v \neq \lambda$ of K and $d(n)_\lambda$ is non-trivial in $H^1(K_\lambda, E)_p^{\pm}$. Then, for any class $s \in \mathrm{Sel}_p(E/K)^{\pm} \subset H^1(K, E_p)^{\pm}$,

$$s_\lambda = 0 \in H^1(K_\lambda, E_p)^{\pm}.$$

Proof of Kolyvagin's theorem (weak form)

From now on, assume that D is prime to pN and $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $L = K(E_p)$ and set $\mathcal{G} := \mathrm{Gal}(L/K) = \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Fact (Serre): For all $n \geq 0$, $H^n(\mathcal{G}, E_p) = 0$. Moreover, the restriction induces an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(L, E_p)^{\mathcal{G}}$.

$\longrightarrow$ There exists a pairing $[\cdot,\cdot] : H^1(K, E_p) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow E_p(L)$ such that:

$$[\sigma(s), \sigma(\rho)] = [s, \sigma(\rho)] = \sigma([(s, \rho]),$$

for all $s \in H^1(K, E_p)$, $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, and $\sigma \in \mathcal{G}$.

Let S be a finite subgroup of $H^1(K, E_p)$, and L_S be the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ defined by $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \left\{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) : [s, \rho] = 0,\ \forall s \in S\right\}$.

Proposition

The induced pairing $[\cdot,\cdot] : S \times \mathrm{Gal}(L_S/L) \longrightarrow E_p(L)$ is non-degenerate.

$\longrightarrow$ It induces an isomorphism of $\mathcal{G}$-modules $\mathrm{Gal}(L_S/L) \xrightarrow{\sim} \mathrm{Hom}(S, E_p(L))$ and an isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules $S \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p(L))$.

Next goal: Apply these results to $S = \mathrm{Sel}_p(E/K)$.

Proof of Kolyvagin's theorem (weak form)

From now on, assume that D is prime to pN and $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $L = K(E_p)$ and set $\mathcal{G} := \mathrm{Gal}(L/K) = \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Fact (Serre): For all $n \geq 0$, $H^n(\mathcal{G}, E_p) = 0$. Moreover, the restriction induces an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(L, E_p)^{\mathcal{G}}$.

$\longrightarrow$ There exists a pairing $[\cdot,\cdot] : H^1(K, E_p) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow E_p(L)$ such that:

$$[\sigma(s), \sigma(\rho)] = [s, \sigma(\rho)] = \sigma([(s, \rho]),$$

for all $s \in H^1(K, E_p)$, $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, and $\sigma \in \mathcal{G}$.

Let S be a finite subgroup of $H^1(K, E_p)$, and L_S be the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ defined by $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \left\{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) : [s, \rho] = 0,\ \forall s \in S\right\}$.

Proposition

The induced pairing $[\cdot,\cdot] : S \times \mathrm{Gal}(L_S/L) \longrightarrow E_p(L)$ is non-degenerate.

$\longrightarrow$ It induces an isomorphism of $\mathcal{G}$-modules $\mathrm{Gal}(L_S/L) \xrightarrow{\sim} \mathrm{Hom}(S, E_p(L))$ and an isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules $S \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p(L))$.

Next goal: Apply these results to $S = \mathrm{Sel}_p(E/K)$.

Proof of Kolyvagin's theorem (weak form)

From now on, assume that D is prime to pN and $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $L = K(E_p)$ and set $\mathcal{G} := \mathrm{Gal}(L/K) = \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Fact (Serre): For all $n \geq 0$, $H^n(\mathcal{G}, E_p) = 0$. Moreover, the restriction induces an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(L, E_p)^{\mathcal{G}}$.

$\longrightarrow$ There exists a pairing $[\cdot,\cdot] : H^1(K, E_p) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow E_p(L)$ such that:

$$[\sigma(s), \sigma(\rho)] = [s, \sigma(\rho)] = \sigma([(s, \rho]),$$

for all $s \in H^1(K, E_p)$, $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, and $\sigma \in \mathcal{G}$.

Let S be a finite subgroup of $H^1(K, E_p)$, and L_S be the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ defined by $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \left\{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) : [s, \rho] = 0,\ \forall s \in S\right\}$.

Proposition

The induced pairing $[\cdot,\cdot] : S \times \mathrm{Gal}(L_S/L) \longrightarrow E_p(L)$ is non-degenerate.

$\longrightarrow$ It induces an isomorphism of $\mathcal{G}$-modules $\mathrm{Gal}(L_S/L) \xrightarrow{\sim} \mathrm{Hom}(S, E_p(L))$ and an isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules $S \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p(L))$.

Next goal: Apply these results to $S = \mathrm{Sel}_p(E/K)$.

Proof of Kolyvagin's theorem (weak form)

From now on, assume that D is prime to pN and $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $L = K(E_p)$ and set $\mathcal{G} := \mathrm{Gal}(L/K) = \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Fact (Serre): For all $n \geq 0$, $H^n(\mathcal{G}, E_p) = 0$. Moreover, the restriction induces an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(L, E_p)^{\mathcal{G}}$.

$\longrightarrow$ There exists a pairing $[\cdot,\cdot] : H^1(K, E_p) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow E_p(L)$ such that:

$$[\sigma(s), \sigma(\rho)] = [s, \sigma(\rho)] = \sigma([(s, \rho]),$$

for all $s \in H^1(K, E_p)$, $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, and $\sigma \in \mathcal{G}$.

Let S be a finite subgroup of $H^1(K, E_p)$, and L_S be the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ defined by $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \left\{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) : [s, \rho] = 0,\ \forall s \in S\right\}$.

Proposition

The induced pairing $[\cdot,\cdot] : S \times \mathrm{Gal}(L_S/L) \longrightarrow E_p(L)$ is non-degenerate.

$\longrightarrow$ It induces an isomorphism of $\mathcal{G}$-modules $\mathrm{Gal}(L_S/L) \xrightarrow{\sim} \mathrm{Hom}(S, E_p(L))$ and an isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules $S \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p(L))$.

Next goal: Apply these results to $S = \mathrm{Sel}_p(E/K)$.

Proof of Kolyvagin's theorem (weak form)

From now on, assume that D is prime to pN and $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $L = K(E_p)$ and set $\mathcal{G} := \mathrm{Gal}(L/K) = \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Fact (Serre): For all $n \geq 0$, $H^n(\mathcal{G}, E_p) = 0$. Moreover, the restriction induces an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(L, E_p)^{\mathcal{G}}$.

$\longrightarrow$ There exists a pairing $[\cdot,\cdot] : H^1(K, E_p) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow E_p(L)$ such that:

$$[\sigma(s), \sigma(\rho)] = [s, \sigma(\rho)] = \sigma([(s, \rho]),$$

for all $s \in H^1(K, E_p)$, $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, and $\sigma \in \mathcal{G}$.

Let S be a finite subgroup of $H^1(K, E_p)$, and L_S be the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ defined by $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \left\{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) : [s, \rho] = 0,\ \forall s \in S\right\}$.

Proposition

The induced pairing $[\cdot,\cdot] : S \times \mathrm{Gal}(L_S/L) \longrightarrow E_p(L)$ is non-degenerate.

$\longrightarrow$ It induces an isomorphism of $\mathcal{G}$-modules $\mathrm{Gal}(L_S/L) \xrightarrow{\sim} \mathrm{Hom}(S, E_p(L))$ and an isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules $S \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p(L))$.

Next goal: Apply these results to $S = \mathrm{Sel}_p(E/K)$.

Proof of Kolyvagin's theorem (weak form)

From now on, assume that D is prime to pN and $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $L = K(E_p)$ and set $\mathcal{G} := \mathrm{Gal}(L/K) = \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Fact (Serre): For all $n \geq 0$, $H^n(\mathcal{G}, E_p) = 0$. Moreover, the restriction induces an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(L, E_p)^{\mathcal{G}}$.

$\longrightarrow$ There exists a pairing $[\cdot,\cdot] : H^1(K, E_p) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow E_p(L)$ such that:

$$[\sigma(s), \sigma(\rho)] = [s, \sigma(\rho)] = \sigma([(s, \rho]),$$

for all $s \in H^1(K, E_p)$, $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, and $\sigma \in \mathcal{G}$.

Let S be a finite subgroup of $H^1(K, E_p)$, and L_S be the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ defined by $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \left\{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) : [s, \rho] = 0,\ \forall s \in S\right\}$.

Proposition

The induced pairing $[\cdot,\cdot] : S \times \mathrm{Gal}(L_S/L) \longrightarrow E_p(L)$ is non-degenerate.

$\longrightarrow$ It induces an isomorphism of $\mathcal{G}$-modules $\mathrm{Gal}(L_S/L) \xrightarrow{\sim} \mathrm{Hom}(S, E_p(L))$ and an isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules $S \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p(L))$.

Next goal: Apply these results to $S = \mathrm{Sel}_p(E/K)$.

Proof of Kolyvagin's theorem (weak form)

From now on, assume that D is prime to pN and $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $L = K(E_p)$ and set $\mathcal{G} := \mathrm{Gal}(L/K) = \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Fact (Serre): For all $n \geq 0$, $H^n(\mathcal{G}, E_p) = 0$. Moreover, the restriction induces an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(L, E_p)^{\mathcal{G}}$.

$\longrightarrow$ There exists a pairing $[\cdot,\cdot] : H^1(K, E_p) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow E_p(L)$ such that:

$$[\sigma(s), \sigma(\rho)] = [s, \sigma(\rho)] = \sigma([(s, \rho]),$$

for all $s \in H^1(K, E_p)$, $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, and $\sigma \in \mathcal{G}$.

Let S be a finite subgroup of $H^1(K, E_p)$, and L_S be the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ defined by $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \left\{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) : [s, \rho] = 0,\ \forall s \in S\right\}$.

Proposition

The induced pairing $[\cdot,\cdot] : S \times \mathrm{Gal}(L_S/L) \longrightarrow E_p(L)$ is non-degenerate.

$\longrightarrow$ It induces an isomorphism of $\mathcal{G}$-modules $\mathrm{Gal}(L_S/L) \xrightarrow{\sim} \mathrm{Hom}(S, E_p(L))$ and an isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules $S \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p(L))$.

Next goal: Apply these results to $S = \mathrm{Sel}_p(E/K)$.

Proof of Kolyvagin's theorem (weak form)

From now on, assume that D is prime to pN and $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $L = K(E_p)$ and set $\mathcal{G} := \mathrm{Gal}(L/K) = \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Fact (Serre): For all $n \geq 0$, $H^n(\mathcal{G}, E_p) = 0$. Moreover, the restriction induces an isomorphism $H^1(K, E_p) \xrightarrow{\sim} H^1(L, E_p)^{\mathcal{G}}$.

$\longrightarrow$ There exists a pairing $[\cdot,\cdot] : H^1(K, E_p) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow E_p(L)$ such that:

$$[\sigma(s), \sigma(\rho)] = [s, \sigma(\rho)] = \sigma([(s, \rho]),$$

for all $s \in H^1(K, E_p)$, $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, and $\sigma \in \mathcal{G}$.

Let S be a finite subgroup of $H^1(K, E_p)$, and L_S be the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ defined by $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \left\{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) : [s, \rho] = 0,\ \forall s \in S\right\}$.

Proposition

The induced pairing $[\cdot,\cdot] : S \times \mathrm{Gal}(L_S/L) \longrightarrow E_p(L)$ is non-degenerate.

$\longrightarrow$ It induces an isomorphism of $\mathcal{G}$-modules $\mathrm{Gal}(L_S/L) \xrightarrow{\sim} \mathrm{Hom}(S, E_p(L))$ and an isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$-modules $S \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p(L))$.

Next goal: Apply these results to $S = \mathrm{Sel}_p(E/K)$.

Proof of Kolyvagin's theorem (weak form)

Hypothesis: y_K is not divisible by p in $E(K)$.

$\longrightarrow$ Let $\delta(y_K)$ be its non-zero image in $\mathrm{Sel}_p(E/K)$.

Let H be the Galois group of L_S/L and I be the subgroup of H fixing the subfield $L\left(\frac{1}{p}y_K\right) = L_{\langle\delta(y_K)\rangle}$ of L_S.

Proof of Kolyvagin's theorem (weak form)

Hypothesis: y_K is not divisible by p in $E(K)$.

$\longrightarrow$ Let $\delta(y_K)$ be its non-zero image in $\mathrm{Sel}_p(E/K)$.

Let H be the Galois group of L_S/L and I be the subgroup of H fixing the subfield $L\left(\frac{1}{p}y_K\right) = L_{\langle\delta(y_K)\rangle}$ of L_S.

Proof of Kolyvagin's theorem (weak form)

Hypothesis: y_K is not divisible by p in $E(K)$.

$\longrightarrow$ Let $\delta(y_K)$ be its non-zero image in $\mathrm{Sel}_p(E/K)$.

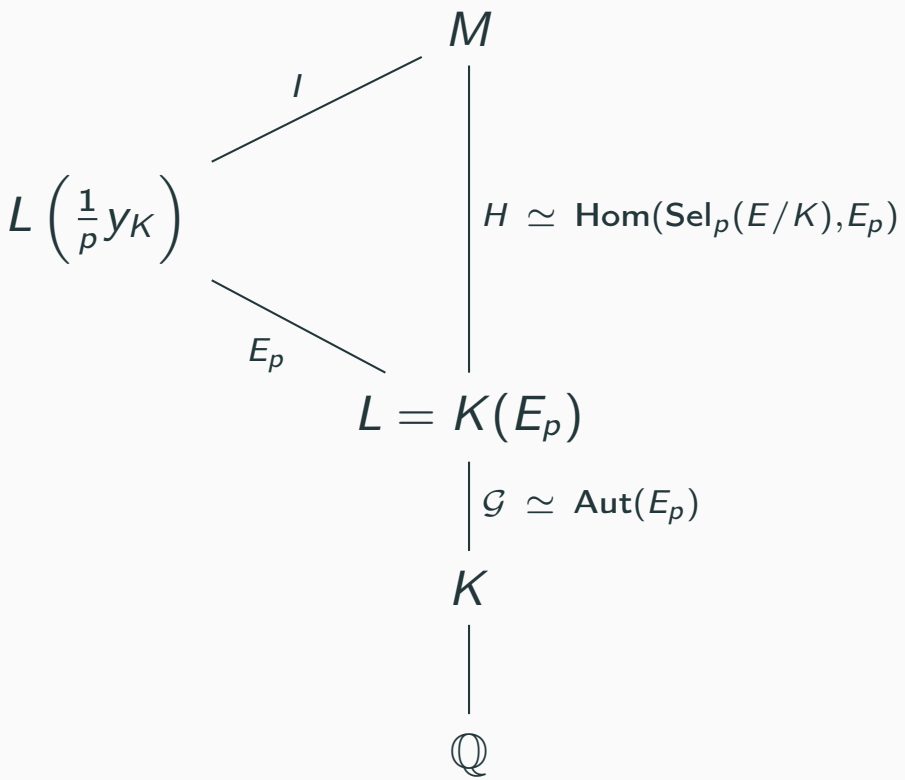
Let H be the Galois group of L_S/L and I be the subgroup of H fixing the subfield $L\left(\frac{1}{p}y_K\right) = L_{\langle\delta(y_K)\rangle}$ of L_S.

Proof of Kolyvagin's theorem (weak form)

Hypothesis: y_K is not divisible by p in $E(K)$.

$\longrightarrow$ Let $\delta(y_K)$ be its non-zero image in $\mathrm{Sel}_p(E/K)$.

Let H be the Galois group of L_S/L and I be the subgroup of H fixing the subfield $L\left(\frac{1}{p}y_K\right) = L_{\langle\delta(y_K)\rangle}$ of L_S.



Proof of Kolyvagin's theorem (weak form)

Let τ be a fixed lifting of complex conjugation in $\mathrm{Gal}(M/\mathbb{Q})$, and H^+ and I^+ denote the $+1$-eigenspaces for (acting by conjugation) on H and I.

$\longrightarrow H^+ = \left\{(\tau h)^2 : h \in H\right\}$, $I^+ = \left\{(\tau i)^2 : i \in I\right\}$ and $H^+/I^+ \cong \mathbb{Z}/p\mathbb{Z}$.

Proposition

If $s \in \mathrm{Sel}(E/K)_p^{\pm}$, then the following are equivalent:

1. $[s, \rho] = 0, \ \forall \rho \in H$;
2. $[s, \rho] = 0, \ \forall \rho \in H^+$;
3. $[s, \rho] = 0, \ \forall \rho \in H^+ \backslash I^+$;
4. $s = 0$.

Proposition

Let $s \in \mathrm{Sel}(E/K)_p$. The following are equivalent:

1. $[s, \mathrm{Fr}_{\lambda_M/\lambda}] = 0$;
2. $[s, \mathrm{Frob}(\lambda)] = 0$;
3. $s_\lambda = 0$ in $H^1(K_\lambda, E_p)$.

Proof of Kolyvagin's theorem (weak form)

Let τ be a fixed lifting of complex conjugation in $\mathrm{Gal}(M/\mathbb{Q})$, and H^+ and I^+ denote the $+1$-eigenspaces for (acting by conjugation) on H and I.

$\longrightarrow H^+ = \{(\tau h)^2 : h \in H\}$, $I^+ = \{(\tau i)^2 : i \in I\}$ and $H^+/I^+ \cong \mathbb{Z}/p\mathbb{Z}$.

Proposition

If $s \in \mathrm{Sel}(E/K)_p^{\pm}$, then the following are equivalent:

1. $[s, \rho] = 0, \ \forall \rho \in H$;
2. $[s, \rho] = 0, \ \forall \rho \in H^+$;
3. $[s, \rho] = 0, \ \forall \rho \in H^+ \backslash I^+$;
4. $s = 0$.

Proposition

Let $s \in \mathrm{Sel}(E/K)_p$. The following are equivalent:

1. $[s, \mathrm{Fr}_{\lambda_M/\lambda}] = 0$;
2. $[s, \mathrm{Frob}(\lambda)] = 0$;
3. $s_\lambda = 0$ in $H^1(K_\lambda, E_p)$.

Proof of Kolyvagin's theorem (weak form)

Let τ be a fixed lifting of complex conjugation in $\mathrm{Gal}(M/\mathbb{Q})$, and H^+ and I^+ denote the $+1$-eigenspaces for (acting by conjugation) on H and I.

$\longrightarrow H^+ = \{(\tau h)^2 : h \in H\}$, $I^+ = \{(\tau i)^2 : i \in I\}$ and $H^+/I^+ \cong \mathbb{Z}/p\mathbb{Z}$.

Proposition

If $s \in \mathrm{Sel}(E/K)_p^{\pm}$, then the following are equivalent:

1. $[s, \rho] = 0, \ \forall \rho \in H$;
2. $[s, \rho] = 0, \ \forall \rho \in H^+$;
3. $[s, \rho] = 0, \ \forall \rho \in H^+ \backslash I^+$;
4. $s = 0$.

Proposition

Let $s \in \mathrm{Sel}(E/K)_p$. The following are equivalent:

1. $[s, \mathrm{Fr}_{\lambda_M/\lambda}] = 0$;
2. $[s, \mathrm{Frob}(\lambda)] = 0$;
3. $s_\lambda = 0$ in $H^1(K_\lambda, E_p)$.

Proof of Kolyvagin's theorem (weak form)

Let τ be a fixed lifting of complex conjugation in $\mathrm{Gal}(M/\mathbb{Q})$, and H^+ and I^+ denote the $+1$-eigenspaces for (acting by conjugation) on H and I.

$\longrightarrow H^+ = \{(\tau h)^2 : h \in H\}$, $I^+ = \{(\tau i)^2 : i \in I\}$ and $H^+/I^+ \cong \mathbb{Z}/p\mathbb{Z}$.

Proposition

If $s \in \mathrm{Sel}(E/K)_p^{\pm}$, then the following are equivalent:

1. $[s, \rho] = 0, \ \forall \rho \in H$;
2. $[s, \rho] = 0, \ \forall \rho \in H^+$;
3. $[s, \rho] = 0, \ \forall \rho \in H^+ \backslash I^+$;
4. $s = 0$.

Proposition

Let $s \in \mathrm{Sel}(E/K)_p$. The following are equivalent:

1. $[s, \mathrm{Fr}_{\lambda_{M/\lambda}}] = 0$;
2. $[s, \mathrm{Frob}(\lambda)] = 0$;
3. $s_\lambda = 0$ in $H^1(K_\lambda, E_p)$.

Recall: The Heegner point $y_K = P_1$ lies in the ϵ-eigenspace for complex conjugation on $E(K)/pE(K)$.

$\longrightarrow$ $\delta(y_K)$ lies in the ϵ-eigenspace of $\mathrm{Sel}_p(E/K)^\epsilon$.

Proposition

$\mathrm{Sel}_p(E/K)^{-\epsilon} = 0$.

Proposition

Assume that y_K is not divisible by p in $E(K)$. Let ℓ be a rational prime which is unramified in $M/\mathbb{Q}$ and has a prime λ_M lying above it, and whose Frobenius element is equal to τh in $\mathrm{Gal}(M/\mathbb{Q})$, with $h \in H$. The following are all equivalent:

1. $c(\ell) \in \mathrm{Sel}(E/K)_p \subset H^1(K, E_p)$;
2. P_ℓ is divisible by p in $E(K_l)$;
3. $d(\ell) = 0$ in $H^1(K, E)_p$;
4. $d(\ell)_\lambda = 0$ in $H^1(K_\lambda, E)_p$;
5. $P_1 = y_K$ is locally divisible by p in $E(K_\lambda)$;
6. $h^{1+\tau}$ lies in the subgroup $I^+ = H^+ \cap I$ of H.

Proof of Kolyvagin's theorem (weak form)

Recall: The Heegner point $y_K = P_1$ lies in the ϵ-eigenspace for complex conjugation on $E(K)/pE(K)$.

$\longrightarrow \delta(y_K)$ lies in the ϵ-eigenspace of $\mathrm{Sel}_p(E/K)^\epsilon$.

Proposition

$\mathrm{Sel}_p(E/K)^{-\epsilon} = 0$.

Proposition

Assume that y_K is not divisible by p in $E(K)$. Let ℓ be a rational prime which is unramified in $M/\mathbb{Q}$ and has a prime λ_M lying above it, and whose Frobenius element is equal to τh in $\mathrm{Gal}(M/\mathbb{Q})$, with $h \in H$. The following are all equivalent:

1. $c(\ell) \in \mathrm{Sel}(E/K)_p \subset H^1(K, E_p)$;
2. P_ℓ is divisible by p in $E(K_l)$;
3. $d(\ell) = 0$ in $H^1(K, E)_p$;
4. $d(\ell)_\lambda = 0$ in $H^1(K_\lambda, E)_p$;
5. $P_1 = y_K$ is locally divisible by p in $E(K_\lambda)$;
6. $h^{1+\tau}$ lies in the subgroup $I^+ = H^+ \cap I$ of H.

Recall: The Heegner point $y_K = P_1$ lies in the ϵ-eigenspace for complex conjugation on $E(K)/pE(K)$.

$\longrightarrow \delta(y_K)$ lies in the ϵ-eigenspace of $\mathrm{Sel}_p(E/K)^\epsilon$.

Proposition

$\mathrm{Sel}_p(E/K)^{-\epsilon} = 0$.

Proposition

Assume that y_K is not divisible by p in $E(K)$. Let ℓ be a rational prime which is unramified in $M/\mathbb{Q}$ and has a prime λ_M lying above it, and whose Frobenius element is equal to τh in $\mathrm{Gal}(M/\mathbb{Q})$, with $h \in H$. The following are all equivalent:

1. $c(\ell) \in \mathrm{Sel}(E/K)_p \subset H^1(K, E_p)$;
2. P_ℓ is divisible by p in $E(K_l)$;
3. $d(\ell) = 0$ in $H^1(K, E)_p$;
4. $d(\ell)_\lambda = 0$ in $H^1(K_\lambda, E)_p$;
5. $P_1 = y_K$ is locally divisible by p in $E(K_\lambda)$;
6. $h^{1+\tau}$ lies in the subgroup $I^+ = H^+ \cap I$ of H.

Recall: The Heegner point $y_K = P_1$ lies in the ϵ-eigenspace for complex conjugation on $E(K)/pE(K)$.

$\longrightarrow \delta(y_K)$ lies in the ϵ-eigenspace of $\mathrm{Sel}_p(E/K)^\epsilon$.

Proposition

$\mathrm{Sel}_p(E/K)^{-\epsilon} = 0$.

Proposition

Assume that y_K is not divisible by p in $E(K)$. Let ℓ be a rational prime which is unramified in $M/\mathbb{Q}$ and has a prime λ_M lying above it, and whose Frobenius element is equal to τh in $\mathrm{Gal}(M/\mathbb{Q})$, with $h \in H$. The following are all equivalent:

1. $c(\ell) \in \mathrm{Sel}(E/K)_p \subset H^1(K, E_p)$;
2. P_ℓ is divisible by p in $E(K_l)$;
3. $d(\ell) = 0$ in $H^1(K, E)_p$;
4. $d(\ell)_\lambda = 0$ in $H^1(K_\lambda, E)_p$;
5. $P_1 = y_K$ is locally divisible by p in $E(K_\lambda)$;
6. $h^{1+\tau}$ lies in the subgroup $I^+ = H^+ \cap I$ of H.

Proof of Kolyvagin's theorem (weak form)

Proposition

$\mathrm{Sel}(E/K)_p^{\epsilon} \cong \mathbb{Z}/p\mathbb{Z}.\delta(y_K)$.

Consequence (Kolyvagin + Gross-Zagier):

Kolyvagin: If y_K has infinite order in $E(K)$, then $\mathrm{rank}(E(K)) = 1$.

Gross-Zagier: $L'(E/K, 1) = \frac{\iint_{E(\mathbb{C})} \omega \wedge \overline{i\omega}}{\sqrt{D}} \hat{h}(y_K)$.

$\longrightarrow$ If $\mathrm{ord}_{s=1} L(E/K, s) = 1$, then

$$\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{rank}(E(K)).$$

Proposition

$\mathrm{Sel}(E/K)_p^{\epsilon} \cong \mathbb{Z}/p\mathbb{Z}.\delta(y_K)$.

Consequence (Kolyvagin + Gross-Zagier):

Kolyvagin: If y_K has infinite order in $E(K)$, then $\mathrm{rank}(E(K)) = 1$.

Gross-Zagier: $L'(E/K, 1) = \frac{\iint_{E(\mathbb{C})} \omega \wedge \overline{i\omega}}{\sqrt{D}} \hat{h}(y_K)$.

$\longrightarrow$ If $\mathrm{ord}_{s=1} L(E/K, s) = 1$, then

$$\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{rank}(E(K)).$$

Proposition

$\mathrm{Sel}(E/K)_p^{\epsilon} \cong \mathbb{Z}/p\mathbb{Z}.\delta(y_K)$.

Consequence (Kolyvagin + Gross-Zagier):

Kolyvagin: If y_K has infinite order in $E(K)$, then $\mathrm{rank}(E(K)) = 1$.

Gross-Zagier: $L'(E/K, 1) = \frac{\iint_{E(\mathbb{C})} \omega \wedge \overline{i\omega}}{\sqrt{D}} \hat{h}(y_K)$.

$\longrightarrow$ If $\mathrm{ord}_{s=1} L(E/K, s) = 1$, then

$$\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{rank}(E(K)).$$

Proposition

$\mathrm{Sel}(E/K)_p^{\epsilon} \cong \mathbb{Z}/p\mathbb{Z}.\delta(y_K)$.

Consequence (Kolyvagin + Gross-Zagier):

Kolyvagin: If y_K has infinite order in $E(K)$, then $\mathrm{rank}(E(K)) = 1$.

Gross-Zagier: $L'(E/K, 1) = \frac{\iint_{E(\mathbb{C})} \omega \wedge \overline{i\omega}}{\sqrt{D}} \hat{h}(y_K)$.

$\longrightarrow$ If $\mathrm{ord}_{s=1} L(E/K, s) = 1$, then

$$\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{rank}(E(K)).$$

Proposition

$\mathrm{Sel}(E/K)_p^{\epsilon} \cong \mathbb{Z}/p\mathbb{Z}.\delta(y_K)$.

Consequence (Kolyvagin + Gross-Zagier):

Kolyvagin: If y_K has infinite order in $E(K)$, then $\mathrm{rank}(E(K)) = 1$.

Gross-Zagier: $L'(E/K, 1) = \frac{\iint_{E(\mathbb{C})} \omega \wedge \overline{i\omega}}{\sqrt{D}} \hat{h}(y_K)$.

$\longrightarrow$ If $\mathrm{ord}_{s=1} L(E/K, s) = 1$, then

$$\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{rank}(E(K)).$$