Heegner Points and Kolyvagin's Theorem

Ajay Prajapati

Indian Institute of Technology, Kanpur

April 16, 2022

Overview

1. Introduction to BSD conjecture
2. Heegner Points
3. Kolyvagin's Theorem

Overview

Elliptic Curves over Number Fields

One of the earliest and central results is:

Mordell-Weil Theorem

Let E be an elliptic curve defined over a number field K.

Elliptic Curves over Number Fields

One of the earliest and central results is:

Mordell-Weil Theorem

Let E be an elliptic curve defined over a number field K. Then the group of K-rational points, $E(K)$, is finitely generated.

Elliptic Curves over Number Fields

One of the earliest and central results is:

Mordell-Weil Theorem

Let E be an elliptic curve defined over a number field K. Then the group of K-rational points, $E(K)$, is finitely generated.

- By structure theorem of finitely generated abelian groups, we get that

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}.$$

Elliptic Curves over Number Fields

One of the earliest and central results is:

Mordell-Weil Theorem

Let E be an elliptic curve defined over a number field K. Then the group of K-rational points, $E(K)$, is finitely generated.

- By structure theorem of finitely generated abelian groups, we get that

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}.$$

Here r is called the (algebraic) rank of $E(K)$ and $E(K)_{tors}$ is the *torsion subgroup* of $E(K)$.

Elliptic Curves over Number Fields

One of the earliest and central results is:

Mordell-Weil Theorem

Let E be an elliptic curve defined over a number field K. Then the group of K-rational points, $E(K)$, is finitely generated.

- By structure theorem of finitely generated abelian groups, we get that

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}.$$

  Here r is called the (algebraic) rank of $E(K)$ and $E(K)_{tors}$ is the *torsion subgroup* of $E(K)$.
- By a theorem of Mazur, the torsion part $E(\mathbb{Q})_{tors}$ is completely understood.

Elliptic Curves over Number Fields

One of the earliest and central results is:

Mordell-Weil Theorem

Let E be an elliptic curve defined over a number field K. Then the group of K-rational points, $E(K)$, is finitely generated.

- By structure theorem of finitely generated abelian groups, we get that

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}.$$

  Here r is called the (algebraic) rank of $E(K)$ and $E(K)_{tors}$ is the *torsion subgroup* of $E(K)$.
- By a theorem of Mazur, the torsion part $E(\mathbb{Q})_{tors}$ is completely understood.
- We can also associate an L-function $L(E/K, s)$ to the elliptic curve which has analytic properties similar to the Riemann zeta function.

Birch and Swinnerton-Dyer (BSD) conjecture

Let $E/\mathbb{Q}$ be an elliptic curve and $L(E/\mathbb{Q}, s)$ be its L-function. Then

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

Birch and Swinnerton-Dyer (BSD) conjecture

Let $E/\mathbb{Q}$ be an elliptic curve and $L(E/\mathbb{Q}, s)$ be its L-function. Then

- $\operatorname{rank}(E(\mathbb{Q})) = \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s)$.
- **(BSD formula)** The leading term of the series expansion of $L(E/\mathbb{Q}, s)$ around $s = 1$ can be given in terms of certain arithmetic invariants of E.

Birch and Swinnerton-Dyer (BSD) conjecture

Let $E/\mathbb{Q}$ be an elliptic curve and $L(E/\mathbb{Q}, s)$ be its L-function. Then

- $\mathrm{rank}(E(\mathbb{Q})) = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$.
- **(BSD formula)** The leading term of the series expansion of $L(E/\mathbb{Q}, s)$ around $s = 1$ can be given in terms of certain arithmetic invariants of E.

$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$ is called the analytic rank of E.

Heegner Points and theorems of Gross-Zagier and Kolyvagin

Let $E/\mathbb{Q}$ be an elliptic curve and K is a quadratic imaginary field. Bryan Birch defined a special point y_K in $E(K)$ (unique upto sign and torsion) which he called Heegner Point.

Heegner Points and theorems of Gross-Zagier and Kolyvagin

Let $E/\mathbb{Q}$ be an elliptic curve and K is a quadratic imaginary field. Bryan Birch defined a special point y_K in $E(K)$ (unique upto sign and torsion) which he called Heegner Point.

Gross-Zagier Formula (1986)

Let K be a quadratic imaginary field and y_K in $E(K)$ is the Heegner point. Then

$$L'(E/K, 1) = (\text{some non-zero constant}) \cdot \hat{h}(y_K).$$

Heegner Points and theorems of Gross-Zagier and Kolyvagin

Let $E/\mathbb{Q}$ be an elliptic curve and K is a quadratic imaginary field. Bryan Birch defined a special point y_K in $E(K)$ (unique upto sign and torsion) which he called Heegner Point.

Gross-Zagier Formula (1986)

Let K be a quadratic imaginary field and y_K in $E(K)$ is the Heegner point. Then

$$L'(E/K,1) = \text{(some non-zero constant)} \cdot \hat{h}(y_K).$$

In particular, $L'(E/K,1) \neq 0$ if and only if y_K has infinite order.

Heegner Points and theorems of Gross-Zagier and Kolyvagin

Let $E/\mathbb{Q}$ be an elliptic curve and K is a quadratic imaginary field. Bryan Birch defined a special point y_K in $E(K)$ (unique upto sign and torsion) which he called Heegner Point.

Gross-Zagier Formula (1986)

Let K be a quadratic imaginary field and y_K in $E(K)$ is the Heegner point. Then

$$L'(E/K, 1) = (\text{some non-zero constant}) \cdot \hat{h}(y_K).$$

In particular, $L'(E/K, 1) \neq 0$ if and only if y_K has infinite order.

Kolyvagin (1989)

Assume that the Heegner point y_K has infinite order in $E(K)$.

Heegner Points and theorems of Gross-Zagier and Kolyvagin

Let $E/\mathbb{Q}$ be an elliptic curve and K is a quadratic imaginary field. Bryan Birch defined a special point y_K in $E(K)$ (unique upto sign and torsion) which he called Heegner Point.

Gross-Zagier Formula (1986)

Let K be a quadratic imaginary field and y_K in $E(K)$ is the Heegner point. Then

$$L'(E/K, 1) = (\text{some non-zero constant}) \cdot \hat{h}(y_K).$$

In particular, $L'(E/K, 1) \neq 0$ if and only if y_K has infinite order.

Kolyvagin (1989)

Assume that the Heegner point y_K has infinite order in $E(K)$. Then the group $E(K)$ has rank 1.

Heegner Points and theorems of Gross-Zagier and Kolyvagin

Let $E/\mathbb{Q}$ be an elliptic curve and K is a quadratic imaginary field. Bryan Birch defined a special point y_K in $E(K)$ (unique upto sign and torsion) which he called Heegner Point.

Gross-Zagier Formula (1986)

Let K be a quadratic imaginary field and y_K in $E(K)$ is the Heegner point. Then

$$L'(E/K,1) = (\text{some non-zero constant}) \cdot \hat{h}(y_K).$$

In particular, $L'(E/K,1) \neq 0$ if and only if y_K has infinite order.

Kolyvagin (1989)

Assume that the Heegner point y_K has infinite order in $E(K)$. Then the group $E(K)$ has rank 1. And the Shafarevich-Tate group, $\text{Ш}(E/K)$, is finite.

Theorem (Gross-Zagier, Kolyvagin)

Suppose $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = r$ with $r \in \{0, 1\}$. Then

Theorem (Gross-Zagier, Kolyvagin)

Suppose $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = r$ with $r \in \{0, 1\}$. Then

$$\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r \quad \text{and} \quad \text{Ш}(E/\mathbb{Q}) \text{ is finite}$$

with an upper bound consistent with the BSD formula.

Theorem (Gross-Zagier, Kolyvagin)

Suppose $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = r$ with $r \in \{0, 1\}$. Then

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r \quad \text{and} \quad Ш(E/\mathbb{Q}) \text{ is finite}$$

with an upper bound consistent with the BSD formula.

Weaker form of Kolyvagin's Theorem

Let p be an odd prime such that the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and

Theorem (Gross-Zagier, Kolyvagin)

Suppose $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = r$ with $r \in \{0, 1\}$. Then

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r \quad \text{and} \quad Ш(E/\mathbb{Q}) \text{ is finite}$$

with an upper bound consistent with the BSD formula.

Weaker form of Kolyvagin's Theorem

Let p be an odd prime such that the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and assume that p does not divide y_K in $E(K)/E(K)_{tors}$. Then:

Theorem (Gross-Zagier, Kolyvagin)

Suppose $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = r$ with $r \in \{0, 1\}$. Then

$$\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r \quad \text{and} \quad Ш(E/\mathbb{Q}) \text{ is finite}$$

with an upper bound consistent with the BSD formula.

Weaker form of Kolyvagin's Theorem

Let p be an odd prime such that the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and assume that p does not divide y_K in $E(K)/E(K)_{tors}$. Then:

1. The group $E(K)$ has rank 1.

Theorem (Gross-Zagier, Kolyvagin)

Suppose $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = r$ with $r \in \{0, 1\}$. Then

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r \quad \text{and} \quad Ш(E/\mathbb{Q}) \text{ is finite}$$

with an upper bound consistent with the BSD formula.

Weaker form of Kolyvagin's Theorem

Let p be an odd prime such that the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and assume that p does not divide y_K in $E(K)/E(K)_{tors}$. Then:

1. The group $E(K)$ has rank 1.
2. The p-torsion subgroup of the Shafarevich-Tate group, $Ш(E/K)[p]$, is trivial.

Consider the p-descent exact sequence

$$0 \longrightarrow \frac{E(K)}{pE(K)} \xrightarrow{\delta_E} \mathrm{Sel}^{(p)}(E/K) \longrightarrow Ш(E/K)[p] \longrightarrow 0$$

Consider the p-descent exact sequence

$$0 \longrightarrow \frac{E(K)}{pE(K)} \xrightarrow{\delta_E} \mathrm{Sel}^{(p)}(E/K) \longrightarrow Ш(E/K)[p] \longrightarrow 0$$

Kolyvagin's Theorem A'

Let p an odd prime such that the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and assume that p does not divide y_K in $E(K)/E(K)_{tors}$. Then

$$\mathrm{Sel}^{(p)}(E/K) = \mathbb{F}_p \delta_E(y_K).$$

Consider the p-descent exact sequence

$$0 \longrightarrow \frac{E(K)}{pE(K)} \xrightarrow{\delta_E} \mathrm{Sel}^{(p)}(E/K) \longrightarrow \text{Ш}(E/K)[p] \longrightarrow 0$$

Kolyvagin's Theorem A'

Let p an odd prime such that the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and assume that p does not divide y_K in $E(K)/E(K)_{tors}$. Then

$$\mathrm{Sel}^{(p)}(E/K) = \mathbb{F}_p\delta_E(y_K).$$

Remark: If $y_K \notin pE(K) \implies \dim_{\mathbb{F}_p} \mathrm{Sel}^{(p)}(E/K) \geq 1$. So we need a upper bound of dimension of Selmer group.

Consider the p-descent exact sequence

$$0 \longrightarrow \frac{E(K)}{pE(K)} \xrightarrow{\delta_E} \mathrm{Sel}^{(p)}(E/K) \longrightarrow Ш(E/K)[p] \longrightarrow 0$$

Kolyvagin's Theorem A'

Let p an odd prime such that the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and assume that p does not divide y_K in $E(K)/E(K)_{tors}$. Then

$$\mathrm{Sel}^{(p)}(E/K) = \mathbb{F}_p \delta_E(y_K).$$

Remark: If $y_K \notin pE(K) \implies \dim_{\mathbb{F}_p} \mathrm{Sel}^{(p)}(E/K) \geq 1$. So we need a upper bound of dimension of Selmer group.

The key to Kolyvagin's proof is that the Heegner point is not alone but lies at the bottom of a system of algebraic points defined over ring class fields.

Consider the p-descent exact sequence

$$0 \longrightarrow \frac{E(K)}{pE(K)} \xrightarrow{\delta_E} \mathrm{Sel}^{(p)}(E/K) \longrightarrow Ш(E/K)[p] \longrightarrow 0$$

Kolyvagin's Theorem A'

Let p an odd prime such that the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and assume that p does not divide y_K in $E(K)/E(K)_{tors}$. Then

$$\mathrm{Sel}^{(p)}(E/K) = \mathbb{F}_p \delta_E(y_K).$$

Remark: If $y_K \notin pE(K) \implies \dim_{\mathbb{F}_p} \mathrm{Sel}^{(p)}(E/K) \geq 1$. So we need a upper bound of dimension of Selmer group.

The key to Kolyvagin's proof is that the Heegner point is not alone but lies at the bottom of a system of algebraic points defined over ring class fields. This system satisfies some nice properties which allows us to construct cohomology classes and apply techniques from Galois cohomology to give upper bound on the Selmer group.

Overview

Notation

N A fixed positive integer

Notation

- N A fixed positive integer
- E An elliptic curve over $\mathbb{Q}$ of conductor N

Notation

- N A fixed positive integer
- E An elliptic curve over $\mathbb{Q}$ of conductor N
- K An imaginary quadratic field with discriminant $D \neq -3, -4$

Notation

- N A fixed positive integer
- E An elliptic curve over $\mathbb{Q}$ of conductor N
- K An imaginary quadratic field with discriminant $D \neq -3, -4$
- $\mathcal{O}_K$ the ring of integers of K

Notation

- N A fixed positive integer
- E An elliptic curve over $\mathbb{Q}$ of conductor N
- K An imaginary quadratic field with discriminant $D \neq -3, -4$
- $\mathcal{O}_K$ the ring of integers of K

  Heegner Hypothesis:

$$\text{every prime } p \text{ dividing } N \text{ splits in } K \tag{1}$$

Notation

- N A fixed positive integer
- E An elliptic curve over $\mathbb{Q}$ of conductor N
- K An imaginary quadratic field with discriminant $D \neq -3, -4$
- $\mathcal{O}_K$ the ring of integers of K

  Heegner Hypothesis:

$$\text{every prime } p \text{ dividing } N \text{ splits in } K \tag{1}$$

This gurantees the existence of an ideal $\mathcal{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Notation

- N A fixed positive integer
- E An elliptic curve over $\mathbb{Q}$ of conductor N
- K An imaginary quadratic field with discriminant $D \neq -3, -4$
- $\mathcal{O}_K$ the ring of integers of K

  Heegner Hypothesis:

$$\text{every prime } p \text{ dividing } N \text{ splits in } K \tag{1}$$

  This gurantees the existence of an ideal $\mathcal{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

- n a squarefree integer relatively prime to N

Notation

- N A fixed positive integer
- E An elliptic curve over $\mathbb{Q}$ of conductor N
- K An imaginary quadratic field with discriminant $D \neq -3, -4$
- $\mathcal{O}_K$ the ring of integers of K

  Heegner Hypothesis:

  $$\text{every prime } p \text{ dividing } N \text{ splits in } K \tag{1}$$

  This gurantees the existence of an ideal $\mathcal{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.
- n a squarefree integer relatively prime to N
- $\mathcal{O}_n$ $:= \mathbb{Z} + n\mathcal{O}_K$, the order of conductor n in $\mathcal{O}_K$

Notation

- N A fixed positive integer
- E An elliptic curve over $\mathbb{Q}$ of conductor N
- K An imaginary quadratic field with discriminant $D \neq -3, -4$
- $\mathcal{O}_K$ the ring of integers of K

  Heegner Hypothesis:

  $$\text{every prime } p \text{ dividing } N \text{ splits in } K \tag{1}$$

  This gurantees the existence of an ideal $\mathcal{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.
- n a squarefree integer relatively prime to N
- $\mathcal{O}_n$ $:= \mathbb{Z} + n\mathcal{O}_K$, the order of conductor n in $\mathcal{O}_K$
- H_n the ring class field of K of conductor n

Notation

- N A fixed positive integer
- E An elliptic curve over $\mathbb{Q}$ of conductor N
- K An imaginary quadratic field with discriminant $D \neq -3, -4$
- $\mathcal{O}_K$ the ring of integers of K

  Heegner Hypothesis:

$$\text{every prime } p \text{ dividing } N \text{ splits in } K \tag{1}$$

  This gurantees the existence of an ideal $\mathcal{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

- n a squarefree integer relatively prime to N
- $\mathcal{O}_n$ $:= \mathbb{Z} + n\mathcal{O}_K$, the order of conductor n in $\mathcal{O}_K$
- H_n the ring class field of K of conductor n
- $X_0(N)$ the level N modular curve

Notation

- N A fixed positive integer
- E An elliptic curve over $\mathbb{Q}$ of conductor N
- K An imaginary quadratic field with discriminant $D \neq -3, -4$
- $\mathcal{O}_K$ the ring of integers of K

  Heegner Hypothesis:

  $$\text{every prime } p \text{ dividing } N \text{ splits in } K \tag{1}$$

  This gurantees the existence of an ideal $\mathcal{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.
- n a squarefree integer relatively prime to N
- $\mathcal{O}_n$ $:= \mathbb{Z} + n\mathcal{O}_K$, the order of conductor n in $\mathcal{O}_K$
- H_n the ring class field of K of conductor n
- $X_0(N)$ the level N modular curve
- τ denotes the complex conjugation

Heegner Points on Modular curves

Recall that

$$Y_0(N)(\mathbb{C}) := X_0(N)(\mathbb{C}) - \{cusps\} \longleftrightarrow \{\mathbb{C}/\Lambda \xrightarrow{\varphi} \mathbb{C}/\Lambda' \text{ with } \ker\phi \ N\text{-cyclic}\}$$

Note that

$$\left[\frac{\mathbb{C}}{\mathcal{O}} \longrightarrow \frac{\mathbb{C}}{\mathcal{N}^{-1}}\right]$$

is a point on the modular curve $X_0(N)$.

Heegner Points on Modular curves

Recall that

$$Y_0(N)(\mathbb{C}) := X_0(N)(\mathbb{C}) - \{cusps\} \longleftrightarrow \{\mathbb{C}/\Lambda \xrightarrow{\varphi} \mathbb{C}/\Lambda' \text{ with } \ker\phi \ N\text{-cyclic}\}$$

Note that

$$\left[\frac{\mathbb{C}}{\mathcal{O}} \longrightarrow \frac{\mathbb{C}}{\mathcal{N}^{-1}}\right]$$

is a point on the modular curve $X_0(N)$.

Similarly letting $\mathcal{N}_n = \mathcal{O}_n \cap \mathcal{N}$, we get that $\mathcal{O}_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$.

Heegner Points on Modular curves

Recall that

$$Y_0(N)(\mathbb{C}) := X_0(N)(\mathbb{C}) - \{cusps\} \longleftrightarrow \{\mathbb{C}/\Lambda \xrightarrow{\varphi} \mathbb{C}/\Lambda' \text{ with } \ker\phi \ N\text{-cyclic}\}$$

Note that

$$\left[\frac{\mathbb{C}}{\mathcal{O}} \longrightarrow \frac{\mathbb{C}}{\mathcal{N}^{-1}}\right]$$

is a point on the modular curve $X_0(N)$.

Similarly letting $\mathcal{N}_n = \mathcal{O}_n \cap \mathcal{N}$, we get that $\mathcal{O}_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$. Hence

$$z_n := \left[\frac{\mathbb{C}}{\mathcal{O}_n} \longrightarrow \frac{\mathbb{C}}{\mathcal{N}_n^{-1}}\right] \tag{2}$$

is a point on the modular curve $X_0(N)$.

Heegner Points on Modular curves

Recall that

$$Y_0(N)(\mathbb{C}) := X_0(N)(\mathbb{C}) - \{cusps\} \longleftrightarrow \{\mathbb{C}/\Lambda \xrightarrow{\varphi} \mathbb{C}/\Lambda' \text{ with } \ker\phi\ N\text{-cyclic}\}$$

Note that

$$\left[\frac{\mathbb{C}}{\mathcal{O}} \longrightarrow \frac{\mathbb{C}}{\mathcal{N}^{-1}}\right]$$

is a point on the modular curve $X_0(N)$.

Similarly letting $\mathcal{N}_n = \mathcal{O}_n \cap \mathcal{N}$, we get that $\mathcal{O}_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$. Hence

$$z_n := \left[\frac{\mathbb{C}}{\mathcal{O}_n} \longrightarrow \frac{\mathbb{C}}{\mathcal{N}_n^{-1}}\right] \quad (2)$$

is a point on the modular curve $X_0(N)$.

Definition

z_n is called a Heegner Point of Conductor n on $X_0(N)$.

Heegner points on elliptic curves

Since $E/\mathbb{Q}$ be an elliptic curve of conductor N. By Wiles et. al, $\exists$ a modular parametrization (a map of algebraic curves over $\mathbb{Q}$)

$$\Phi : X_0(N) \longrightarrow E \tag{3}$$

Heegner points on elliptic curves

Since $E/\mathbb{Q}$ be an elliptic curve of conductor N. By Wiles et. al, $\exists$ a modular parametrization (a map of algebraic curves over $\mathbb{Q}$)

$$\Phi : X_0(N) \longrightarrow E \tag{3}$$

Definition

$y_n := \Phi(z_n)$ is called a Heegner Point of Conductor n on E.

Heegner points on elliptic curves

Since $E/\mathbb{Q}$ be an elliptic curve of conductor N. By Wiles et. al, $\exists$ a modular parametrization (a map of algebraic curves over $\mathbb{Q}$)

$$\Phi : X_0(N) \longrightarrow E \tag{3}$$

Definition

$y_n := \Phi(z_n)$ is called a Heegner Point of Conductor n on E.

By theory of CM, $z_n \in X_0(N)(H_n)$. Hence $y_n \in E(H_n)$.

Heegner points on elliptic curves

Since $E/\mathbb{Q}$ be an elliptic curve of conductor N. By Wiles et. al, $\exists$ a modular parametrization (a map of algebraic curves over $\mathbb{Q}$)

$$\Phi : X_0(N) \longrightarrow E \tag{3}$$

Definition

$y_n := \Phi(z_n)$ is called a Heegner Point of Conductor n on E.

By theory of CM, $z_n \in X_0(N)(H_n)$. Hence $y_n \in E(H_n)$.

The Heegner point $y_K \in E(K)$ in the statement of Gross-Zagier and Kolyvagin's theorem is

$$y_K := \mathrm{Norm}_{H_1/K}(y_1) = \sum_{\sigma \in \mathrm{Gal}(H_1/K)} y_1^\sigma \tag{4}$$

Overview

1. Introduction to BSD conjecture
2. Heegner Points
3. Kolyvagin's Theorem

Heegner points forms a Euler System

Proposition (Norm Relations)

Suppose $n = \ell \cdot m$ with $\ell \nmid m$ and ℓ is inert in K.

Heegner points forms a Euler System

Proposition (Norm Relations)

Suppose $n = \ell \cdot m$ with $\ell \nmid m$ and ℓ is inert in K. Then

$$\mathrm{Norm}_{H_n/H_m}(y_n) = a_\ell \cdot y_m \tag{5}$$

where $a_\ell = \ell + 1 - \#\widetilde{E}(\mathbb{F}_\ell)$ is the trace of Frobenius.

Proposition (Congruence Relations)

Suppose $n = \ell \cdot m$ with $\ell \nmid m$ inert in K and write $\ell\mathcal{O}_K = \lambda$. Then

1. λ splits completely in H_m.

Heegner points forms a Euler System

Proposition (Norm Relations)

Suppose $n = \ell \cdot m$ with $\ell \nmid m$ and ℓ is inert in K. Then

$$\mathrm{Norm}_{H_n/H_m}(y_n) = a_\ell \cdot y_m \tag{5}$$

where $a_\ell = \ell + 1 - \#\widetilde{E}(\mathbb{F}_\ell)$ is the trace of Frobenius.

Proposition (Congruence Relations)

Suppose $n = \ell \cdot m$ with $\ell \nmid m$ inert in K and write $\ell \mathcal{O}_K = \lambda$. Then

1. λ splits completely in H_m.
2. Every prime $\lambda_m | \lambda$ in H_m is totally ramified in H_n.

Heegner points forms a Euler System

Proposition (Norm Relations)

Suppose $n = \ell \cdot m$ with $\ell \nmid m$ and ℓ is inert in K. Then

$$\mathrm{Norm}_{H_n/H_m}(y_n) = a_\ell \cdot y_m \tag{5}$$

where $a_\ell = \ell + 1 - \#\widetilde{E}(\mathbb{F}_\ell)$ is the trace of Frobenius.

Proposition (Congruence Relations)

Suppose $n = \ell \cdot m$ with $\ell \nmid m$ inert in K and write $\ell\mathcal{O}_K = \lambda$. Then

1. λ splits completely in H_m.
2. Every prime $\lambda_m | \lambda$ in H_m is totally ramified in H_n.
3. If $\lambda_m = (\lambda_n)^{\ell+1}$ then $y_n \equiv \left(\frac{H_m/\mathbb{Q}}{\lambda_m}\right) y_m \pmod{\lambda_n}$.

Construction of cohomology classes

$p > 2$ was prime such that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$ with p not dividing y_K in $E(K)/E(K)_{tors}$.

Definition

A prime $\ell \nmid N \cdot D \cdot p$ is called a Kolyvagin prime if it satifies:

1. ℓ is inert in K.

Construction of cohomology classes

$p > 2$ was prime such that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$ with p not dividing y_K in $E(K)/E(K)_{tors}$.

Definition

A prime $\ell \nmid N \cdot D \cdot p$ is called a Kolyvagin prime if it satifies:

1. ℓ is inert in K.
2. $a_\ell \equiv \ell + 1 \equiv 0 \pmod p$, where $a_\ell = \ell + 1 - \#\widetilde{E}(\mathbb{F}_\ell)$.

Construction of cohomology classes

$p > 2$ was prime such that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$ with p not dividing y_K in $E(K)/E(K)_{tors}$.

Definition

A prime $\ell \nmid N \cdot D \cdot p$ is called a Kolyvagin prime if it satifies:

1. ℓ is inert in K.
2. $a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}$, where $a_\ell = \ell + 1 - \#\widetilde{E}(\mathbb{F}_\ell)$.

Now we let τ be the complex conjugation and we define the set

$$\mathcal{L}_E = \left\{ \ell \text{ prime } : \ell \nmid N \cdot D \cdot p, \left(\frac{K(E[p])/\mathbb{Q}}{\ell} \right) \sim \tau \text{ in } \mathrm{Gal}(K(E[p])/\mathbb{Q}) \right\}$$

Construction of cohomology classes

$p > 2$ was prime such that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$ with p not dividing y_K in $E(K)/E(K)_{tors}$.

Definition

A prime $\ell \nmid N \cdot D \cdot p$ is called a Kolyvagin prime if it satifies:

1. ℓ is inert in K.
2. $a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}$, where $a_\ell = \ell + 1 - \#\widetilde{E}(\mathbb{F}_\ell)$.

Now we let τ be the complex conjugation and we define the set

$$\mathcal{L}_E = \left\{ \ell \text{ prime } : \ell \nmid N \cdot D \cdot p, \left(\frac{K(E[p])/\mathbb{Q}}{\ell} \right) \sim \tau \text{ in } \mathrm{Gal}(K(E[p])/\mathbb{Q}) \right\}$$

where $\sim$ means that τ lies in the Frobenius conjugacy class

$$\left(\frac{K(E[p])/\mathbb{Q}}{\ell} \right) := \left\{ \left(\frac{K(E[p])/\mathbb{Q}}{\gamma} \right) : \gamma \text{ is a prime lying over } \ell \right\}$$

Construction of cohomology classes

$p > 2$ was prime such that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$ with p not dividing y_K in $E(K)/E(K)_{tors}$.

Definition

A prime $\ell \nmid N \cdot D \cdot p$ is called a Kolyvagin prime if it satifies:

1. ℓ is inert in K.
2. $a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}$, where $a_\ell = \ell + 1 - \#\widetilde{E}(\mathbb{F}_\ell)$.

Now we let τ be the complex conjugation and we define the set

$$\mathcal{L}_E = \left\{ \ell \text{ prime } : \ell \nmid N \cdot D \cdot p, \left(\frac{K(E[p])/\mathbb{Q}}{\ell} \right) \sim \tau \text{ in } \mathrm{Gal}(K(E[p])/\mathbb{Q}) \right\}$$

where $\sim$ means that τ lies in the Frobenius conjugacy class

$$\left(\frac{K(E[p])/\mathbb{Q}}{\ell} \right) := \left\{ \left(\frac{K(E[p])/\mathbb{Q}}{\gamma} \right) : \gamma \text{ is a prime lying over } \ell \right\}$$

Proposition

Every $\ell \in \mathcal{L}_E$ is a Kolyvagin prime.

Let $G_\ell := \mathrm{Gal}(H_\ell/H_1)$ then it is cyclic. Fix a generator σ_ℓ of G_ℓ.

Definition

The group ring element

$$D_\ell := \sum_{i=1}^{\ell} i\sigma_\ell^i = \sum_{i=0}^{\ell+1} \frac{\sigma_\ell^i - 1}{\sigma_\ell - 1} \quad \in \mathbb{Z}[G_\ell]$$

is called the Kolyvagin derivative operator.

Let $G_\ell := \mathrm{Gal}(H_\ell/H_1)$ then it is cyclic. Fix a generator σ_ℓ of G_ℓ.

Definition

The group ring element

$$D_\ell := \sum_{i=1}^{\ell} i\sigma_\ell^i = \sum_{i=0}^{\ell+1} \frac{\sigma_\ell^i - 1}{\sigma_\ell - 1} \quad \in \mathbb{Z}[G_\ell]$$

is called the Kolyvagin derivative operator. Let

$$\mathcal{N}_E := \{\text{square-free product of primes } \ell \in \mathcal{L}_E\} \text{ (with convention that } 1 \in \mathcal{N}_E)$$

and

Let $G_\ell := \mathrm{Gal}(H_\ell/H_1)$ then it is cyclic. Fix a generator σ_ℓ of G_ℓ.

Definition

The group ring element

$$D_\ell := \sum_{i=1}^{\ell} i\sigma_\ell^i = \sum_{i=0}^{\ell+1} \frac{\sigma_\ell^i - 1}{\sigma_\ell - 1} \quad \in \mathbb{Z}[G_\ell]$$

is called the Kolyvagin derivative operator. Let

$$\mathcal{N}_E := \{\text{square-free product of primes } \ell \in \mathcal{L}_E\} \text{ (with convention that } 1 \in \mathcal{N}_E)$$

and for every $n \in \mathcal{N}_E$, let

$$G_n := \mathrm{Gal}(H_n/H_1) \cong \prod_{\ell | n} \mathrm{Gal}(H_\ell/H_1) = \prod_{\ell | n} G_\ell$$

$$D_n := \prod_{\ell | n} D_\ell \quad \in \mathbb{Z}[G_n]$$

Let $G_\ell := \mathrm{Gal}(H_\ell/H_1)$ then it is cyclic. Fix a generator σ_ℓ of G_ℓ.

Definition

The group ring element

$$D_\ell := \sum_{i=1}^{\ell} i\sigma_\ell^i = \sum_{i=0}^{\ell+1} \frac{\sigma_\ell^i - 1}{\sigma_\ell - 1} \quad \in \mathbb{Z}[G_\ell]$$

is called the Kolyvagin derivative operator. Let

$$\mathcal{N}_E := \{\text{square-free product of primes } \ell \in \mathcal{L}_E\} \text{ (with convention that } 1 \in \mathcal{N}_E)$$

and for every $n \in \mathcal{N}_E$, let

$$G_n := \mathrm{Gal}(H_n/H_1) \cong \prod_{\ell \mid n} \mathrm{Gal}(H_\ell/H_1) = \prod_{\ell \mid n} G_\ell$$

$$D_n := \prod_{\ell \mid n} D_\ell \quad \in \mathbb{Z}[G_n]$$

with $G_1 := 1$ and $D_1 = 1$ by convention.

Let $n \in \mathcal{N}_E$ and $y_n \in E(H_n)$ be a Heegner point of conductor n. Then we define

$$[D_n y_n] := D_n y_n \pmod{pE(H_n)} \quad \in E(H_n)/pE(H_n)$$

Let $n \in \mathcal{N}_E$ and $y_n \in E(H_n)$ be a Heegner point of conductor n. Then we define

$$[D_n y_n] := D_n y_n \pmod{pE(H_n)} \quad \in E(H_n)/pE(H_n)$$

Proposition

$[D_n y_n] \in (E(H_n)/pE(H_n))^{G_n}$. (Recall $G_n = \mathrm{Gal}(H_n/H_1)$)

Let $n \in \mathcal{N}_E$ and $y_n \in E(H_n)$ be a Heegner point of conductor n. Then we define

$$[D_n y_n] := D_n y_n \pmod{pE(H_n)} \quad \in E(H_n)/pE(H_n)$$

Proposition

$[D_n y_n] \in (E(H_n)/pE(H_n))^{G_n}$. (Recall $G_n = \mathrm{Gal}(H_n/H_1)$)

We would like to construct a point in $E(H_n)/pE(H_n)$ which is invariant not only for $G_n = \mathrm{Gal}(H_n/H_1)$ but also for $\mathcal{G}_n := \mathrm{Gal}(H_n/K)$.

Let $n \in \mathcal{N}_E$ and $y_n \in E(H_n)$ be a Heegner point of conductor n. Then we define

$$[D_n y_n] := D_n y_n \pmod{pE(H_n)} \quad \in E(H_n)/pE(H_n)$$

Proposition

$[D_n y_n] \in (E(H_n)/pE(H_n))^{G_n}$. (Recall $G_n = \mathrm{Gal}(H_n/H_1)$)

We would like to construct a point in $E(H_n)/pE(H_n)$ which is invariant not only for $G_n = \mathrm{Gal}(H_n/H_1)$ but also for $\mathcal{G}_n := \mathrm{Gal}(H_n/K)$.

Fix a set $\mathfrak{S}$ of coset representatives for the subgroup G_n in $\mathcal{G}_n$ and

Let $n \in \mathcal{N}_E$ and $y_n \in E(H_n)$ be a Heegner point of conductor n. Then we define

$$[D_n y_n] := D_n y_n \pmod{pE(H_n)} \quad \in E(H_n)/pE(H_n)$$

Proposition

$[D_n y_n] \in (E(H_n)/pE(H_n))^{G_n}$. (Recall $G_n = \mathrm{Gal}(H_n/H_1)$)

We would like to construct a point in $E(H_n)/pE(H_n)$ which is invariant not only for $G_n = \mathrm{Gal}(H_n/H_1)$ but also for $\mathcal{G}_n := \mathrm{Gal}(H_n/K)$.

Fix a set $\mathfrak{S}$ of coset representatives for the subgroup G_n in $\mathcal{G}_n$ and define:

$$P_n := \sum_{\sigma \in \mathfrak{S}} \sigma D_n y_n \pmod{pE(H_n)} \quad \in E(H_n)/pE(H_n).$$

Let $n \in \mathcal{N}_E$ and $y_n \in E(H_n)$ be a Heegner point of conductor n. Then we define

$$[D_n y_n] := D_n y_n \pmod{pE(H_n)} \quad \in E(H_n)/pE(H_n)$$

Proposition

$[D_n y_n] \in (E(H_n)/pE(H_n))^{G_n}$. (Recall $G_n = \mathrm{Gal}(H_n/H_1)$)

We would like to construct a point in $E(H_n)/pE(H_n)$ which is invariant not only for $G_n = \mathrm{Gal}(H_n/H_1)$ but also for $\mathcal{G}_n := \mathrm{Gal}(H_n/K)$.

Fix a set $\mathfrak{S}$ of coset representatives for the subgroup G_n in $\mathcal{G}_n$ and define:

$$P_n := \sum_{\sigma \in \mathfrak{S}} \sigma D_n y_n \pmod{pE(H_n)} \quad \in E(H_n)/pE(H_n).$$

Then the class $[P_n]$ is in $(E(H_n)/pE(H_n))^{\mathcal{G}_n}$.

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

$$
\begin{array}{cccccccc}
 & & & & & & 0 & \\
 & & & & & & \downarrow & \\
 & & & & & & \mathrm{H}^1(H_n/K,E)[p] & \\
 & & & & & & \downarrow \mathrm{Inf} & \\
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & \mathrm{H}^1(K,E[p]) & \longrightarrow & \mathrm{H}^1(K,E)[p] & \longrightarrow \\
 & & \downarrow & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & \\
0 & \longrightarrow & (E(H_n)/pE(H_n))^{\mathcal{G}_n} & \xrightarrow{\delta_n} & \mathrm{H}^1(H_n,E[p])^{\mathcal{G}_n} & \longrightarrow & \mathrm{H}^1(H_n,E)[p]^{\mathcal{G}_n} &
\end{array}
$$

- Lower row is exact since Kummer map is $\mathcal{G}_n$-equivariant.
- Middle Res is an isomorphism because we can deduce that there are no p-torsion points defined over H_n. i.e., $E(H_n)[p] = 0$.

Let $c(n)$ be the unique class in $\mathrm{H}^1(K, E[p])$ such that:

$$\operatorname{Res} c(n) = \delta_n[P_n] \quad \text{in } \mathrm{H}^1(H_n, E[p])^{\mathcal{G}_n}.$$

Let $c(n)$ be the unique class in $\mathrm{H}^1(K, E[p])$ such that:

$$\operatorname{Res} c(n) = \delta_n[P_n] \quad \text{in } \mathrm{H}^1(H_n, E[p])^{\mathcal{G}_n}.$$

Let

$$d(n) = \operatorname{Image} c(n) \quad \text{in } \mathrm{H}^1(K, E)[p].$$

1. We study the property of these cohomology classes.

Let $c(n)$ be the unique class in $\mathrm{H}^1(K, E[p])$ such that:

$$\mathrm{Res}\, c(n) = \delta_n[P_n] \quad \text{in } \mathrm{H}^1(H_n, E[p])^{\mathcal{G}_n}.$$

Let

$$d(n) = \mathrm{Image}\, c(n) \quad \text{in } \mathrm{H}^1(K, E)[p].$$

1. We study the property of these cohomology classes. For example, As $p > 2$, the action of the complex conjugation $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ gives us the decomposition (as $\mathbb{F}_p$ vector spaces)

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

Let $c(n)$ be the unique class in $\mathrm{H}^1(K, E[p])$ such that:

$$\mathrm{Res}\, c(n) = \delta_n[P_n] \quad \text{in } \mathrm{H}^1(H_n, E[p])^{\mathcal{G}_n}.$$

Let

$$d(n) = \mathrm{Image}\, c(n) \quad \text{in } \mathrm{H}^1(K, E)[p].$$

1. We study the property of these cohomology classes. For example, As $p > 2$, the action of the complex conjugation $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ gives us the decomposition (as $\mathbb{F}_p$ vector spaces)

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

It turns out that classes $c(n)$ and $d(n)$ lies in the either $+$ or $-$ eigenspace.

Let $c(n)$ be the unique class in $\mathrm{H}^1(K, E[p])$ such that:

$$\mathrm{Res}\, c(n) = \delta_n[P_n] \quad \text{in } \mathrm{H}^1(H_n, E[p])^{\mathcal{G}_n}.$$

Let

$$d(n) = \mathrm{Image}\, c(n) \quad \text{in } \mathrm{H}^1(K, E)[p].$$

1. We study the property of these cohomology classes. For example, As $p > 2$, the action of the complex conjugation $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ gives us the decomposition (as $\mathbb{F}_p$ vector spaces)

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

   It turns out that classes $c(n)$ and $d(n)$ lies in the either $+$ or $-$ eigenspace.
2. We also derive criterion for when the classes $d(n)_v$ are locally trivial.

Local Tate duality

Theorem

Let ℓ be a Kolyvagin prime, $\lambda = \ell\mathcal{O}_K$, and K_λ be completion of K at λ.

Local Tate duality

Theorem

Let ℓ be a Kolyvagin prime, $\lambda = \ell\mathcal{O}_K$, and K_λ be completion of K at λ. Then there is a non-degenerate pairing of $\mathbb{F}_p$-vector spaces

$$\langle\cdot,\cdot\rangle : E(K_\lambda)/pE(K_\lambda) \times \mathrm{H}^1(K_\lambda, E)[p] \longrightarrow \mathbb{Z}/p\mathbb{Z}. \quad (6)$$

induced by local Tate duality, Cartier duality, and Weil pairing.

Local Tate duality

Theorem

Let ℓ be a Kolyvagin prime, $\lambda = \ell\mathcal{O}_K$, and K_λ be completion of K at λ. Then there is a non-degenerate pairing of $\mathbb{F}_p$-vector spaces

$$\langle\cdot,\cdot\rangle : E(K_\lambda)/pE(K_\lambda) \times \mathrm{H}^1(K_\lambda, E)[p] \longrightarrow \mathbb{Z}/p\mathbb{Z}. \quad (6)$$

induced by local Tate duality, Cartier duality, and Weil pairing.

This pairing relates the elements of the Selmer group to the cohomology classes construced above.

Local Tate duality

Theorem

Let ℓ be a Kolyvagin prime, $\lambda = \ell\mathcal{O}_K$, and K_λ be completion of K at λ. Then there is a non-degenerate pairing of $\mathbb{F}_p$-vector spaces

$$\langle \cdot, \cdot \rangle : E(K_\lambda)/pE(K_\lambda) \times \mathrm{H}^1(K_\lambda, E)[p] \longrightarrow \mathbb{Z}/p\mathbb{Z}. \quad (6)$$

induced by local Tate duality, Cartier duality, and Weil pairing.

This pairing relates the elements of the Selmer group to the cohomology classes construced above.

Using the properties of cohomology classes $c(n)$ and $d(n)$, we can derive an upper bound on the Selmer group $\mathrm{Sel}^{(p)}(E/K)$.

Thank You