Every L has their own story 1 : L-function connecting Number Fields and Elliptic Curves

서성욱

서울대학교 수리과학부 25학번, 수학문제연구회

October 1st, 2025

Outline

Outline

Introduction to the Seminar

- L-functions : 깊고 심오한... 수학의 아름다운 심장

Introduction to the Seminar

- L-functions : 깊고 심오한... 수학의 아름다운 심장
- ∃ **많고 중요한** L-functions!

Introduction to the Seminar

- L-functions : 깊고 심오한... 수학의 아름다운 심장
- ∃ **많고 중요한** L-functions!
- 각자 다양한 분야의 **아주 많은 아주 중요한** 정보를 함유!

Introduction to the Seminar

- L-functions : 깊고 심오한... 수학의 아름다운 심장
- ∃ **많고 중요한** L-functions!
- 각자 다양한 분야의 **아주 많은 아주 중요한** 정보를 함유!

오늘은 대수적정수론의 두 산맥인 수체와 타원곡선을 L-function을 통해 꿰뚫어볼 것!

Introduction to the Seminar

- L-functions : 깊고 심오한... 수학의 아름다운 심장
- ∃ **많고 중요한** L-functions!
- 각자 다양한 분야의 **아주 많은 아주 중요한** 정보를 함유!

오늘은 대수적정수론의 두 산맥인 수체와 타원곡선을 L-function을 통해 꿰뚫어볼 것!

(다음 번엔 아마도 Hasse-Weil L-function?)

Caution!

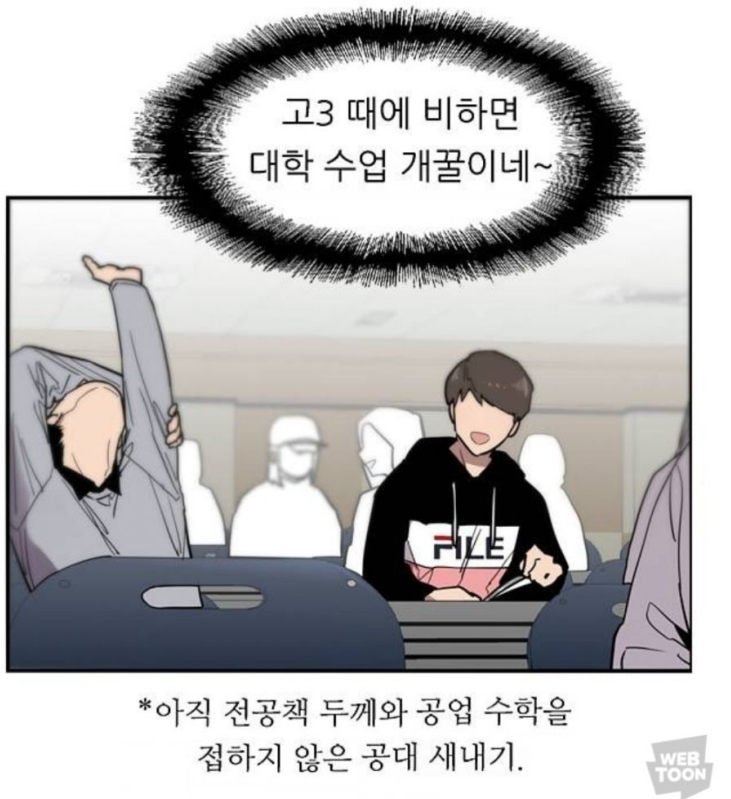
- Aim : motivation and pleasure, 정수론 홍보

Caution!

- Aim : motivation and pleasure, 정수론 홍보
- Talk about : definitions and analogy, where analogy comes from / Not talk about : Why analogy happens.(Too hard)

Caution!

- Aim : motivation and pleasure, 정수론 홍보
- Talk about : definitions and analogy, where analogy comes from / Not talk about : Why analogy happens.(Too hard)
- 아직 귀여운 신입생 ⇒ 저도 모로는 게 많아요...



Outline

Motivation

Theorem(Fermat's two square theorem).

All primes $p \equiv 1 (\mathrm{mod}\ 4)$ is sum of two square numbers. i.e., $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$

Motivation

Theorem(Fermat's two square theorem).

All primes $p \equiv 1 (\mathrm{mod}\ 4)$ is sum of two square numbers. i.e., $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$

Remark : $p \equiv 3 (\mathrm{mod}\ 4)$ cannot be sum of two squares.

Motivation

Theorem(Fermat's two square theorem).

All primes $p \equiv 1 (\mathrm{mod}\ 4)$ is sum of two square numbers. i.e., $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$

Remark : $p \equiv 3 (\mathrm{mod}\ 4)$ cannot be sum of two squares.
Idea :

- $a^2 + b^2 = (a + bi)(a - bi)$

Motivation

Theorem(Fermat's two square theorem).

All primes $p \equiv 1 (\mathrm{mod}\ 4)$ is sum of two square numbers. i.e., $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$

Remark : $p \equiv 3 (\mathrm{mod}\ 4)$ cannot be sum of two squares.
Idea :

- $a^2 + b^2 = (a + bi)(a - bi)$
- Define $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, similar to $\mathbb{Z}$

Motivation

Theorem(Fermat's two square theorem).

All primes $p \equiv 1 (\mathrm{mod}\ 4)$ is sum of two square numbers. i.e., $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$

Remark : $p \equiv 3 (\mathrm{mod}\ 4)$ cannot be sum of two squares.
Idea :

- $a^2 + b^2 = (a + bi)(a - bi)$
- Define $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, similar to $\mathbb{Z}$
- Then FTST states : which prime in $\mathbb{Z}$ is not prime in $\mathbb{Z}[i]$?

Motivation

Theorem(Fermat's two square theorem).

All primes $p \equiv 1 (\mathrm{mod}\ 4)$ is sum of two square numbers. i.e., $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$

Remark : $p \equiv 3 (\mathrm{mod}\ 4)$ cannot be sum of two squares.
Idea :

- $a^2 + b^2 = (a + bi)(a - bi)$
- Define $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, similar to $\mathbb{Z}$
- Then FTST states : which prime in $\mathbb{Z}$ is not prime in $\mathbb{Z}[i]$?

Hence, we have to know what $\mathbb{Z}[i]$ "looks" like. Similarly, for other number theoretic questions, knowing structures like $\mathbb{Z}, \mathbb{Z}[i]$ helps.

Number Fields

Definition(Number Field).

Field $K/\mathbb{Q}$ with finite index $[K:\mathbb{Q}] < \infty$ is called **Number Field**.

Number Fields

Definition(Number Field).

Field $K/\mathbb{Q}$ with finite index $[K:\mathbb{Q}] < \infty$ is called **Number Field**.

i.e., Number fields are finite $\mathbb{Q}$-vector spaces.

Number Fields

Definition(Number Field).

Field $K/\mathbb{Q}$ with finite index $[K:\mathbb{Q}] < \infty$ is called **Number Field**.

i.e., Number fields are finite $\mathbb{Q}$-vector spaces.

- e.g. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, $\cdots$

Number Fields

Definition(Number Field).

Field $K/\mathbb{Q}$ with finite index $[K:\mathbb{Q}] < \infty$ is called **Number Field**.

i.e., Number fields are finite $\mathbb{Q}$-vector spaces.

- e.g. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, $\cdots$
- counter e.g. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\pi)$, $\bar{\mathbb{Q}} \cdots$

Number Fields

Definition(Number Field).

Field $K/\mathbb{Q}$ with finite index $[K:\mathbb{Q}] < \infty$ is called **Number Field**.

i.e., Number fields are finite $\mathbb{Q}$-vector spaces.

- e.g. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, $\cdots$
- counter e.g. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\pi)$, $\bar{\mathbb{Q}} \cdots$

They are the main topics of Algebraic Number Theory, for short, **ANT**, and developed with history of ANT.

Number Fields

Definition(Number Field).

Field $K/\mathbb{Q}$ with finite index $[K:\mathbb{Q}] < \infty$ is called **Number Field**.

i.e., Number fields are finite $\mathbb{Q}$-vector spaces.

- e.g. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, $\cdots$
- counter e.g. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\pi)$, $\bar{\mathbb{Q}} \cdots$

They are the main topics of Algebraic Number Theory, for short, **ANT**, and developed with history of ANT.
One of major objects about # field K is its **Ring of Integers** $\mathcal{O}_K$.

Definition(Ring of Integers).

$\mathcal{O}_K = \{a \in K : f(a) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\}$ with ring structure.

Number Fields

Definition(Number Field).

Field $K/\mathbb{Q}$ with finite index $[K:\mathbb{Q}] < \infty$ is called **Number Field**.

i.e., Number fields are finite $\mathbb{Q}$-vector spaces.

- e.g. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, $\cdots$
- counter e.g. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\pi)$, $\bar{\mathbb{Q}} \cdots$

They are the main topics of Algebraic Number Theory, for short, **ANT**, and developed with history of ANT.
One of major objects about # field K is its **Ring of Integers** $\mathcal{O}_K$.

Definition(Ring of Integers).

$\mathcal{O}_K = \{a \in K : f(a) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\}$ with ring structure.

- e.g. $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$

Number Fields

Definition(Number Field).

Field $K/\mathbb{Q}$ with finite index $[K:\mathbb{Q}] < \infty$ is called **Number Field**.

i.e., Number fields are finite $\mathbb{Q}$-vector spaces.

- e.g. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, $\cdots$
- counter e.g. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\pi)$, $\bar{\mathbb{Q}} \cdots$

They are the main topics of Algebraic Number Theory, for short, **ANT**, and developed with history of ANT.
One of major objects about # field K is its **Ring of Integers** $\mathcal{O}_K$.

Definition(Ring of Integers).

$\mathcal{O}_K = \{a \in K : f(a) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\}$ with ring structure.

- e.g. $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
- $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$

Number Fields

The relation between $\mathcal{O}_K$ and K is analogous to the relation between $\mathbb{Z}$ and $\mathbb{Q}$.

Number Fields

The relation between $\mathcal{O}_K$ and K is analogous to the relation between $\mathbb{Z}$ and $\mathbb{Q}$.

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- $\operatorname{Frac} \mathcal{O}_K = K$

Number Fields

The relation between $\mathcal{O}_K$ and K is analogous to the relation between $\mathbb{Z}$ and $\mathbb{Q}$.

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- $\operatorname{Frac} \mathcal{O}_K = K$

We can ask many "good" questions about $\mathcal{O}_K$ such as

Number Fields

The relation between $\mathcal{O}_K$ and K is analogous to the relation between $\mathbb{Z}$ and $\mathbb{Q}$.

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- $\operatorname{Frac} \mathcal{O}_K = K$

We can ask many "good" questions about $\mathcal{O}_K$ such as

- Which $\mathbb{Z}$-primes remain 'prime' in $\mathcal{O}_K$?

Number Fields

The relation between $\mathcal{O}_K$ and K is analogous to the relation between $\mathbb{Z}$ and $\mathbb{Q}$.

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- $\operatorname{Frac} \mathcal{O}_K = K$

We can ask many "good" questions about $\mathcal{O}_K$ such as

- Which $\mathbb{Z}$-primes remain 'prime' in $\mathcal{O}_K$?
- Which $\mathbb{Z}$-primes ramify in $\mathcal{O}_K$?

Number Fields

The relation between $\mathcal{O}_K$ and K is analogous to the relation between $\mathbb{Z}$ and $\mathbb{Q}$.

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- $\operatorname{Frac} \mathcal{O}_K = K$

We can ask many "good" questions about $\mathcal{O}_K$ such as

- Which $\mathbb{Z}$-primes remain 'prime' in $\mathcal{O}_K$?
- Which $\mathbb{Z}$-primes ramify in $\mathcal{O}_K$?
- Is $\mathcal{O}_K$ UFD? etc.

Number Fields

The relation between $\mathcal{O}_K$ and K is analogous to the relation between $\mathbb{Z}$ and $\mathbb{Q}$.

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- $\operatorname{Frac} \mathcal{O}_K = K$

We can ask many "good" questions about $\mathcal{O}_K$ such as

- Which $\mathbb{Z}$-primes remain 'prime' in $\mathcal{O}_K$?
- Which $\mathbb{Z}$-primes ramify in $\mathcal{O}_K$?
- Is $\mathcal{O}_K$ UFD? etc.

Such questions can be answered via some invariants about K. For example,

Number Fields

The relation between $\mathcal{O}_K$ and K is analogous to the relation between $\mathbb{Z}$ and $\mathbb{Q}$.

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- $\operatorname{Frac} \mathcal{O}_K = K$

We can ask many "good" questions about $\mathcal{O}_K$ such as

- Which $\mathbb{Z}$-primes remain 'prime' in $\mathcal{O}_K$?
- Which $\mathbb{Z}$-primes ramify in $\mathcal{O}_K$?
- Is $\mathcal{O}_K$ UFD? etc.

Such questions can be answered via some invariants about K. For example,

Theorem(Chebotarev density theorem).

For number field K with degree n, ratio of $\mathbb{Z}$-primes that remain prime is $\frac{1}{n}$.

Remark

$\mathbb{Z}[i]$: From FTST, every prime $p \equiv 1 (\mathrm{mod}\, 4)$ is $a^2 + b^2 = (a - bi)(a + bi)$, hence not prime. As mentioned, $p \equiv 3$ remains prime.
$(2 = -i(1 + i)^2$ is ramified)
$\therefore$ (ratio of 'inert' prime)$= \frac{1}{2} = \frac{1}{[\mathbb{Q}(i):\mathbb{Q}]}$

Remark

$\mathbb{Z}[i]$: From FTST, every prime $p \equiv 1 (\mathrm{mod}\, 4)$ is $a^2 + b^2 = (a - bi)(a + bi)$, hence not prime. As mentioned, $p \equiv 3$ remains prime.
$(2 = -i(1 + i)^2$ is ramified)
$\therefore$ (ratio of 'inert' prime)$= \frac{1}{2} = \frac{1}{[\mathbb{Q}(i):\mathbb{Q}]}$

We can answer second question with discriminant of number field.

Remark

$\mathbb{Z}[i]$: From FTST, every prime $p \equiv 1 (\mathrm{mod}\, 4)$ is $a^2 + b^2 = (a - bi)(a + bi)$, hence not prime. As mentioned, $p \equiv 3$ remains prime.
$(2 = -i(1+i)^2$ is ramified)
$\therefore$ (ratio of 'inert' prime)$= \frac{1}{2} = \frac{1}{[\mathbb{Q}(i):\mathbb{Q}]}$

We can answer second question with discriminant of number field.

Definition(Discriminant of Number field).

$$D_K = \det \begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(b_1) & \cdots & \sigma_n(b_n) \end{pmatrix}^2 \in \mathbb{Z}$$

where b_i are integral basis of $\mathcal{O}_K$, $\sigma_i : K \to \mathbb{C}$ are injective ring homomorphisms.

Number Fields

Examples :

Number Fields

Examples :

- $\mathbb{Q} : D_{\mathbb{Q}} = \det(1)^2 = 1$
- $\mathbb{Q}(\sqrt{2}) : D_{\mathbb{Q}(\sqrt{2})} = \det \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}^2 = 8$
- $\mathbb{Q}(i) : D_{\mathbb{Q}(i)} = \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = -4$

Number Fields

Examples :

- $\mathbb{Q} : D_{\mathbb{Q}} = \det(1)^2 = 1$
- $\mathbb{Q}(\sqrt{2}) : D_{\mathbb{Q}(\sqrt{2})} = \det \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}^2 = 8$
- $\mathbb{Q}(i) : D_{\mathbb{Q}(i)} = \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = -4$

Theorem.

$\mathbb{Z}$-prime p ramify in K iff $p | D_K$.

Number Fields

Examples :

- $\mathbb{Q} : D_{\mathbb{Q}} = \det(1)^2 = 1$
- $\mathbb{Q}(\sqrt{2}) : D_{\mathbb{Q}(\sqrt{2})} = \det \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}^2 = 8$
- $\mathbb{Q}(i) : D_{\mathbb{Q}(i)} = \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = -4$

Theorem.

$\mathbb{Z}$-prime p ramify in K iff $p | D_K$.

$\Rightarrow$2 is ramified in $\mathbb{Q}(i)$ since $2 | \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = -4$

Number Fields

Q. Why UFD-ness of $\mathcal{O}_K$ important?

Number Fields

Q. Why UFD-ness of $\mathcal{O}_K$ important?
A. (e.g.)If a $\mathbb{Z}[\zeta_n]$ is always UFD for $\forall n \in \mathbb{N}$, FLT is true!

Number Fields

Q. Why UFD-ness of $\mathcal{O}_K$ important?
A. (e.g.)If a $\mathbb{Z}[\zeta_n]$ is always UFD for $\forall n \in \mathbb{N}$, FLT is true!

We can answer UFD-ness question via invariants.

Number Fields

Q. Why UFD-ness of $\mathcal{O}_K$ important?
A. (e.g.)If a $\mathbb{Z}[\zeta_n]$ is always UFD for $\forall n \in \mathbb{N}$, FLT is true!

We can answer UFD-ness question via invariants.

Definition(Ideal Class Group).

For number field K, $Cl(K) = F_K/P_k$ is the **ideal class group** of K, where F_K, P_K is its group of fractional ideals, and group of principal fractional ideals.

Number Fields

Q. Why UFD-ness of $\mathcal{O}_K$ important?
A. (e.g.)If a $\mathbb{Z}[\zeta_n]$ is always UFD for $\forall n \in \mathbb{N}$, FLT is true!

We can answer UFD-ness question via invariants.

Definition(Ideal Class Group).

For number field K, $Cl(K) = F_K/P_k$ is the **ideal class group** of K, where F_K, P_K is its group of fractional ideals, and group of principal fractional ideals.

Intuition : F_K, P_K is group of ideals/principal ideals.
(For those who wonders, $I \subset R$ for ring R is fractional ideal if aI is ideal of R for some $a \in R$. If that ideal is principal, it's principal fractional ideal.)

Number Fields

Definition(Class Number).

The **class number** h_K of number field K is the cardinality of the ideal class group, i.e., $h_K = \#Cl(K)$.

Number Fields

Definition(Class Number).

The **class number** h_K of number field K is the cardinality of the ideal class group, i.e., $h_K = \#Cl(K)$.

Remark 1. :

$\mathcal{O}_K$ is PID $\iff$ $F_K = P_K$ $\iff$ $Cl(K) \cong 1$ $\iff$ $h_K = 1$

Number Fields

Definition(Class Number).

The **class number** h_K of number field K is the cardinality of the ideal class group, i.e., $h_K = \#Cl(K)$.

Remark 1. :

$\mathcal{O}_K$ is PID $\iff$ $F_K = P_K$ $\iff$ $Cl(K) \cong 1$ $\iff$ $h_K = 1$

i.e., h_K measures how "far" $\mathcal{O}_K$ is from PID!

Number Fields

Definition(Class Number).

The **class number** h_K of number field K is the cardinality of the ideal class group, i.e., $h_K = \#Cl(K)$.

Remark 1. :

$\mathcal{O}_K$ is PID $\iff$ $F_K = P_K$ $\iff$ $Cl(K) \cong 1$ $\iff$ $h_K = 1$

i.e., h_K measures how "far" $\mathcal{O}_K$ is from PID!

Remark 2. :

A ring of algebraic integer $\mathcal{O}_K$ is UFD $\iff$ $\mathcal{O}_K$ is PID

Number Fields

Definition(Class Number).

The **class number** h_K of number field K is the cardinality of the ideal class group, i.e., $h_K = \#Cl(K)$.

Remark 1. :

$\mathcal{O}_K$ is PID $\iff$ $F_K = P_K$ $\iff$ $Cl(K) \cong 1$ $\iff$ $h_K = 1$

i.e., h_K measures how "far" $\mathcal{O}_K$ is from PID!

Remark 2. :

A ring of algebraic integer $\mathcal{O}_K$ is UFD $\iff$ $\mathcal{O}_K$ is PID

Remark 2. is from the fact that every $\mathcal{O}_K$ is Dedekind domain.

Number Fields

- Lamé : I proved FLT!
- Kummer : Only for primes $p \nmid h_{\mathbb{Q}(\zeta_p)}$.

Number Fields

- Lamé : I proved FLT!
- Kummer : Only for primes $p \nmid h_{\mathbb{Q}(\zeta_p)}$.

Hence, we can answer

- Is $\mathcal{O}_K$ UFD?

by calculating h_K... which is difficult.

Number Fields

So now, we use L-function!

So now, we use L-function!

Definition(Dedekind zeta functions).

For number field K, we define **Dedekind zeta function** $\zeta_K(s)$ as

$$\zeta_K(s) = \sum_{\text{Ideal } I \subset \mathcal{O}_K} \frac{1}{|\mathcal{O}_K/I|^s}$$

So now, we use L-function!

Definition(Dedekind zeta functions).

For number field K, we define **Dedekind zeta function** $\zeta_K(s)$ as

$$\zeta_K(s) = \sum_{\text{Ideal } I \subset \mathcal{O}_K} \frac{1}{|\mathcal{O}_K/I|^s}$$

- e.g., $\zeta_{\mathbb{Q}}(s) = \sum_{(n)} \frac{1}{|\mathbb{Z}/(n)|^s} = \sum_n \frac{1}{n^s} = \zeta(s)$

So now, we use L-function!

Definition(Dedekind zeta functions).

For number field K, we define **Dedekind zeta function** $\zeta_K(s)$ as

$$\zeta_K(s) = \sum_{\text{Ideal } I \subset \mathcal{O}_K} \frac{1}{|\mathcal{O}_K/I|^s}$$

- e.g., $\zeta_{\mathbb{Q}}(s) = \sum_{(n)} \frac{1}{|\mathbb{Z}/(n)|^s} = \sum_n \frac{1}{n^s} = \zeta(s)$

$\zeta_K(s)$ shares good conditions with $\zeta(s)$.

Properties of $\zeta(s)$

- Dirichlet series converges on $\mathrm{Re}(s) > 1$
- Reflection formula :
  $\xi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s) = \xi(1-s)$
- Hence, analytically continued to $\mathbb{C}$, except for the pole $s = 1$.

Number Fields

Properties of $\zeta(s)$

- Dirichlet series converges on $\mathrm{Re}(s) > 1$
- Reflection formula :
  $\xi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s) = \xi(1-s)$
- Hence, analytically continued to $\mathbb{C}$, except for the pole $s = 1$.

Properties of $\zeta_K(s)$

- Dirichlet series converges on $\mathrm{Re}(s) > 1$
- Reflection formula : $\Lambda_K(s) = |D_K|^{\frac{s}{2}}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s) = \Lambda_K(1-s)$
- Hence, analytically continued to $\mathbb{C}$, except for the pole $s = 1$.

Where $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$, $\Gamma_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s)$, r_1, r_2 is the number of real/complex(up to conjugation) homomorphism of K.

Number Fields

Now, one can compute the residue of $\zeta_K(s)$ at $s = 1$, then one can get one of the most important formulas of $\zeta_K(s)$.

Number Fields

Now, one can compute the residue of $\zeta_K(s)$ at $s = 1$, then one can get one of the most important formulas of $\zeta_K(s)$.

Theorem(Class number formula).

ζ_K has a simple pole at $s = 1$ and

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} \cdot Reg_K \cdot h_K}{\sqrt{|D_K|} \cdot w_K}$$

where $w_K = \#\{\text{root of unity} \in K\}$, Reg_K is regulator of K.

Now, one can compute the residue of $\zeta_K(s)$ at $s = 1$, then one can get one of the most important formulas of $\zeta_K(s)$.

Theorem(Class number formula).

ζ_K has a simple pole at $s = 1$ and

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} \cdot Reg_K \cdot h_K}{\sqrt{|D_K|} \cdot w_K}$$

where $w_K = \#\{\text{root of unity} \in K\}$, Reg_K is regulator of K.

e.g. $K = \mathbb{Q}(i)$. Well known : $Res_{s=1}\zeta_{\mathbb{Q}(i)} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4}$. So,

$$\begin{aligned} \frac{\pi}{4} &= \frac{2^0 \cdot (2\pi)^1 \cdot 1 \cdot h_{\mathbb{Q}(i)}}{\sqrt{|-4|} \cdot 4} \\ &= \frac{\pi}{4} \cdot h_{\mathbb{Q}(i)}, \end{aligned}$$

hence $h_{\mathbb{Q}(i)} = 1$, i.e. $\mathbb{Z}[i]$ is UFD.(Overkill...)

Outline

Elliptic Curves

Definition

Solution set of $E : y^2 = x^3 + ax + b$ for $a, b \in \mathbb{Q}$ with $4a^3 + 27b^2 \neq 0$ is called the **Elliptic Curve**.($E(\mathbb{C})$, $E(\mathbb{Q})$,etc.)

Elliptic Curves

Definition

Solution set of $E : y^2 = x^3 + ax + b$ for $a, b \in \mathbb{Q}$ with $4a^3 + 27b^2 \neq 0$ is called the **Elliptic Curve**.($E(\mathbb{C})$, $E(\mathbb{Q})$,etc.)

Q. Why EC is important?

Elliptic Curves

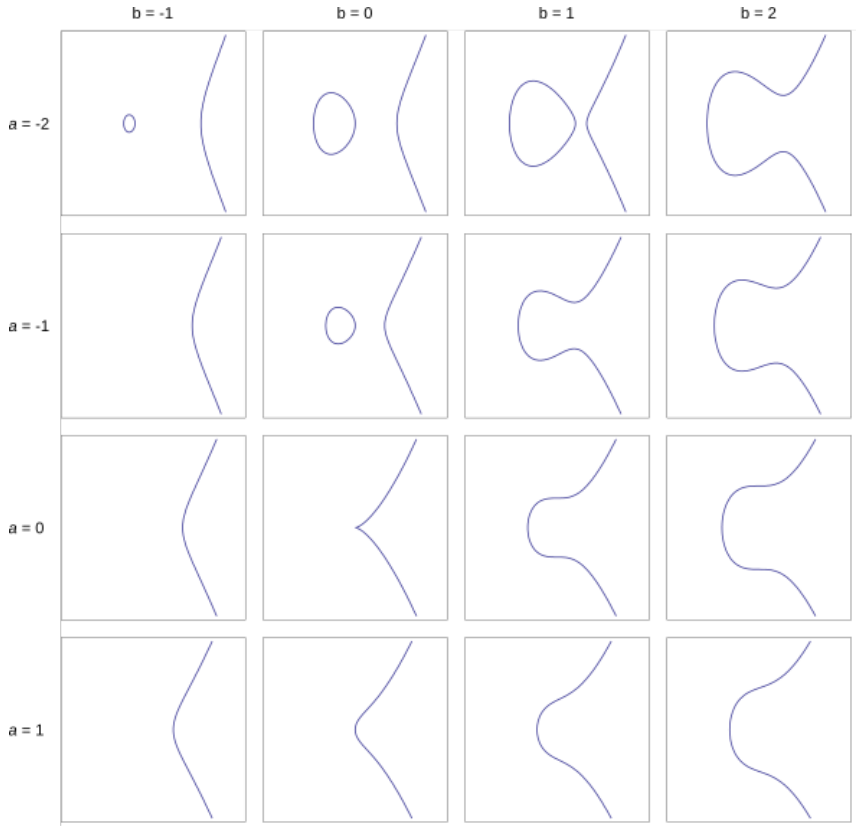
Definition

Solution set of $E : y^2 = x^3 + ax + b$ for $a, b \in \mathbb{Q}$ with $4a^3 + 27b^2 \neq 0$ is called the **Elliptic Curve**.($E(\mathbb{C})$, $E(\mathbb{Q})$,etc.)

Q. Why EC is important?

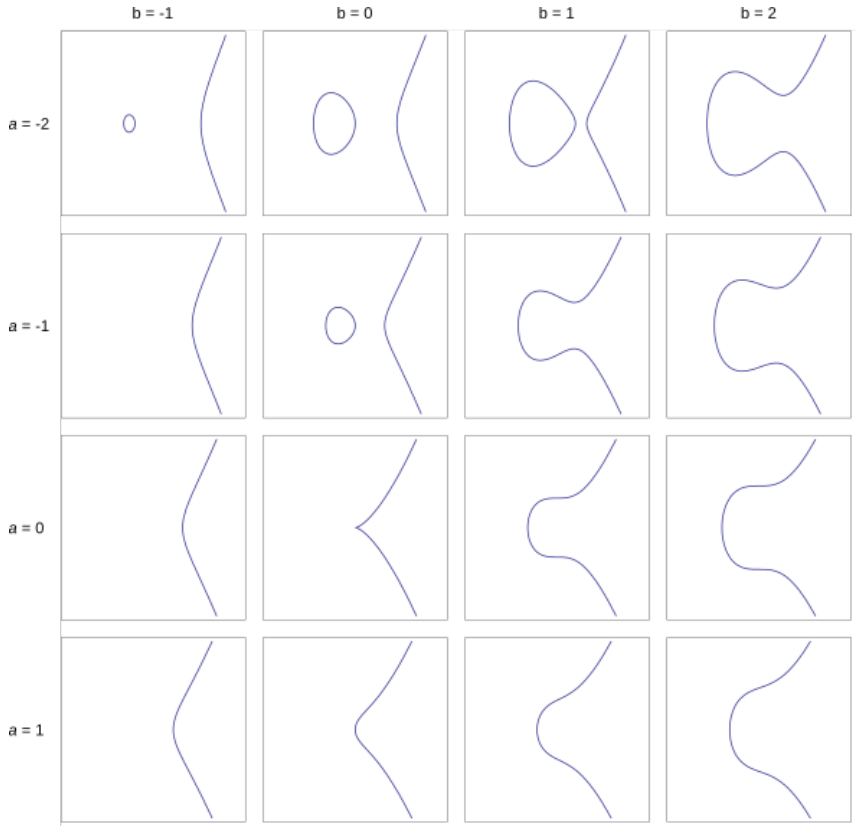
A. Unique unsolved and unknown Diophantine eq. with 2 variables.

Elliptic Curves



In terms of # of $\mathbb{Q}$-Solution set :

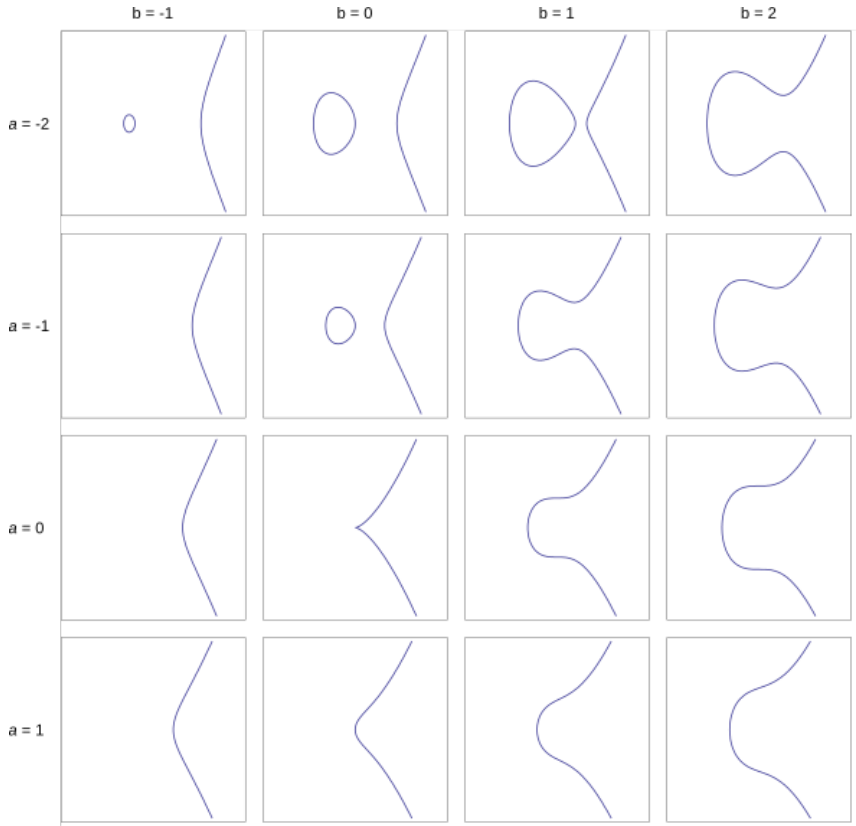
Elliptic Curves



In terms of # of $\mathbb{Q}$-Solution set :

- degree 1,2 - ∞ or 0(trivial and easy)

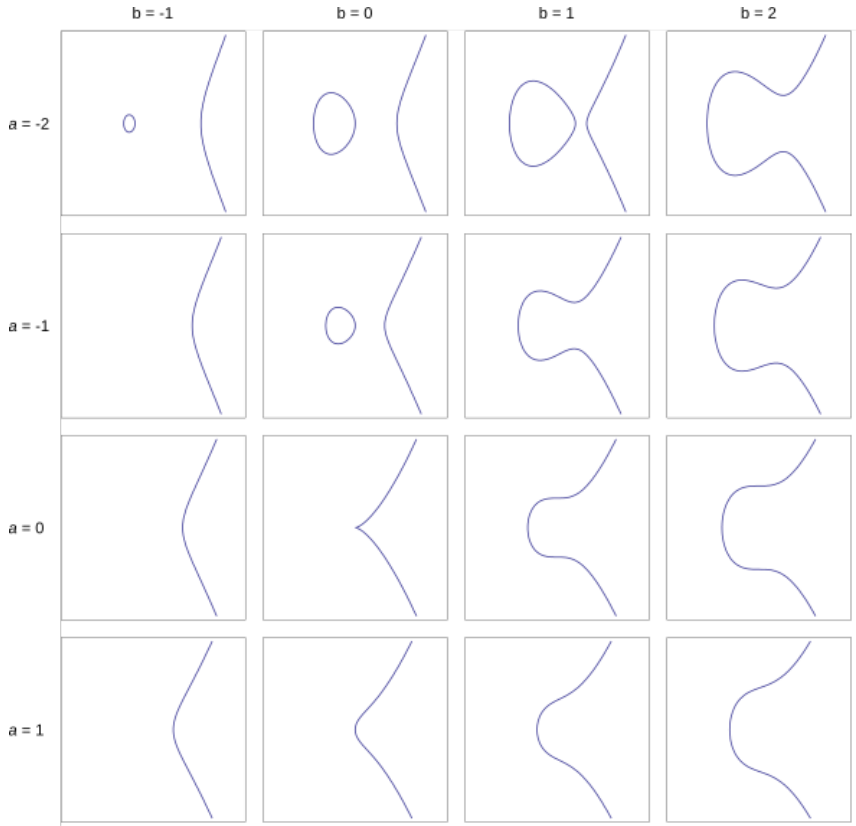
Elliptic Curves



In terms of # of $\mathbb{Q}$-Solution set :

- degree 1,2 - ∞ or 0(trivial and easy)
- degree $\geq$ 4 - finite!(Faltings, 1983)

Elliptic Curves



In terms of # of $\mathbb{Q}$-Solution set :

- degree 1,2 - ∞ or 0(trivial and easy)
- degree $\geq$ 4 - finite!(Faltings, 1983)
- degree 3 - 0 or finite or ∞ = 엄..

Elliptic Curve

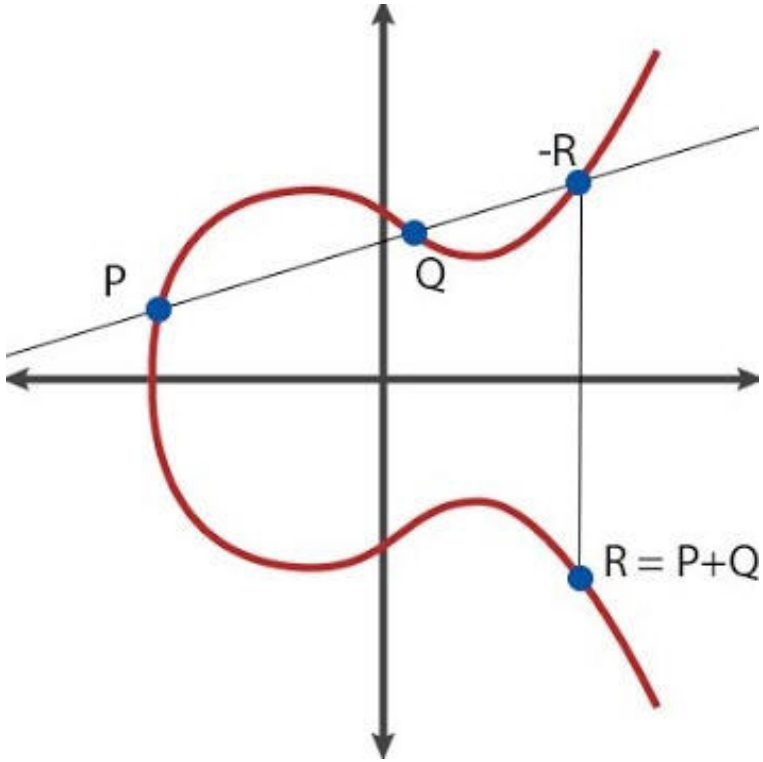
Our interest $= E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$

Elliptic Curve

Our interest $= E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$
To borrow the power of algebra, endows group structure in EC as follows.

Elliptic Curve

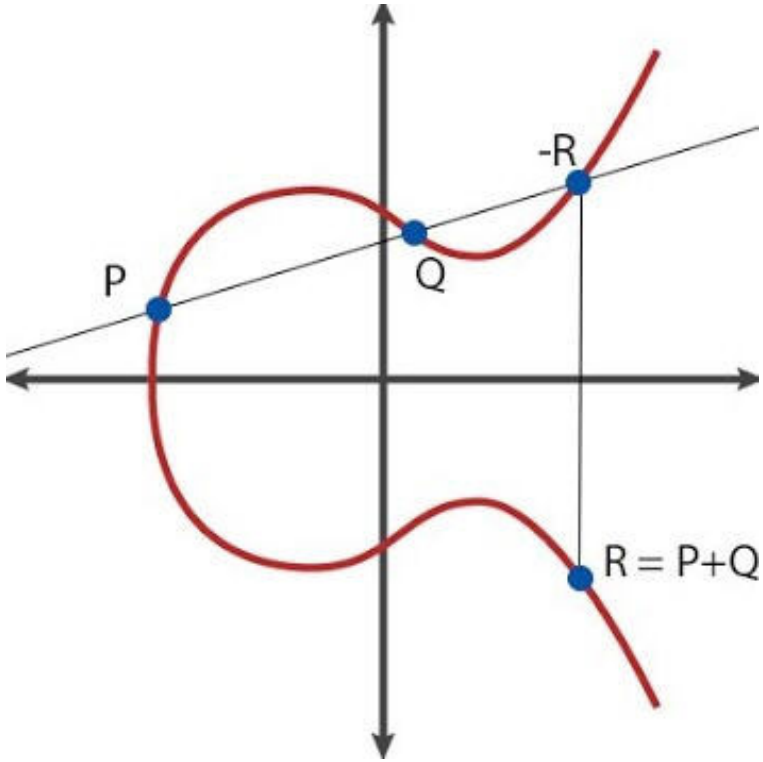
Our interest = $E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$
To borrow the power of algebra, endows group structure in EC as follows.



Here, identity is $O = \infty$. We can check EC forms **abelian group**!(c.f. associativity is the most non trivial property.)

Elliptic Curve

Our interest = $E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$
To borrow the power of algebra, endows group structure in EC as follows.



Here, identity is $O = \infty$. We can check EC forms **abelian group**!(c.f. associativity is the most non trivial property.)

- We call them **Mordell-Weil group** of E.

Elliptic Curves

Theorem(Mordell-Weil Theorem).

For every elliptic curve E, $E(\mathbb{Q})$ is finitely generated abelian group. i.e., we can write $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}$

Elliptic Curves

Theorem(Mordell-Weil Theorem).

For every elliptic curve E, $E(\mathbb{Q})$ is finitely generated abelian group. i.e., we can write $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tor}}$

- torsion part : trivial(?) and easy.

Elliptic Curves

Theorem(Mordell-Weil Theorem).

For every elliptic curve E, $E(\mathbb{Q})$ is finitely generated abelian group. i.e., we can write $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}$

- torsion part : trivial(?) and easy.
- rank part : 엄...

Elliptic Curves

Theorem(Mordell-Weil Theorem).

For every elliptic curve E, $E(\mathbb{Q})$ is finitely generated abelian group. i.e., we can write $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}$

- torsion part : trivial(?) and easy.
- rank part : 엄...

Theorem(Mazur's torsion theorem).

$E(\mathbb{Q})_{\text{tor}}$ is isomorphic to one of these :

- $\mathbb{Z}/n\mathbb{Z}$ for $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$
- $(\mathbb{Z}/2n\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$ for $n = 1, 2, 3, 4$

Elliptic Curves

Theorem(Mordell-Weil Theorem).

For every elliptic curve E, $E(\mathbb{Q})$ is finitely generated abelian group. i.e., we can write $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}$

- torsion part : trivial(?) and easy.
- rank part : 엄...

Theorem(Mazur's torsion theorem).

$E(\mathbb{Q})_{\text{tor}}$ is isomorphic to one of these :

- $\mathbb{Z}/n\mathbb{Z}$ for $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$
- $(\mathbb{Z}/2n\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$ for $n = 1, 2, 3, 4$

Theorem(Elkies & Zev Klagsbrun ; 2024).

The rank of the elliptic curve $E_{29} : y^2 + xy = x^3 - ax + b$ is ≥ 29, and equality holds if Riemann hypothesis for $L(E, s)$ holds true.

Elliptic Curves

Here, the L-function for elliptic curve is defined as follows.

Elliptic Curves

Here, the L-function for elliptic curve is defined as follows.

Definition(Hasse-Weil L-function for Elliptic Curve).

For elliptic curve E, **Hasse-Weil L-function** of $L(E,s)$ is defined as the following Euler product

$$L(E,s) = \prod_p L_p(E,s)^{-1}$$

where

$$L_p(E,s) = \begin{cases} 1 & \text{if } p^2 \mid N \\ 1 \pm p^{-s} & \text{if } p \mid\mid N \\ 1 - a_p p^{-s} + p^{1-2s} & \text{if } p \nmid N \end{cases}$$

and $a_p := (p+1) - \#E(\mathbb{F}_p)$, N is the conductor of E.

Elliptic Curves

Here, the L-function for elliptic curve is defined as follows.

Definition(Hasse-Weil L-function for Elliptic Curve).

For elliptic curve E, **Hasse-Weil L-function** of $L(E,s)$ is defined as the following Euler product

$$L(E,s) = \prod_p L_p(E,s)^{-1}$$

where

$$L_p(E,s) = \begin{cases} 1 & \text{if } p^2 \mid N \\ 1 \pm p^{-s} & \text{if } p \mid\mid N \\ 1 - a_p p^{-s} + p^{1-2s} & \text{if } p \nmid N \end{cases}$$

and $a_p := (p+1) - \#E(\mathbb{F}_p)$, N is the conductor of E.

c.f. E remains elliptic curve(i.e., has no multiple zero) on $\mathbb{F}_p$ iff $p \nmid N$

Elliptic Curves

For those who misunderstand : $\#E(\mathbb{F}_p) = \#\{a, b \in \mathbb{F}_p : y^2 \equiv x^3 + ax + b\}$

Elliptic Curves

For those who misunderstand : $\#E(\mathbb{F}_p) = \#\{a, b \in \mathbb{F}_p : y^2 \equiv x^3 + ax + b\}$

Again, similar to $\zeta(s)$

Properties of $\zeta(s)$

- Dirichlet series converges on $\mathrm{Re}(s) > 1$
- Reflection formula :
  $\xi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s) = \xi(1-s)$
- Hence, analytically continued to $\mathbb{C}$, except for the pole $s = 1$.

Elliptic Curves

For those who misunderstand : $\#E(\mathbb{F}_p) = \#\{a, b \in \mathbb{F}_p : y^2 \equiv x^3 + ax + b\}$

Again, similar to $\zeta(s)$

Properties of $\zeta(s)$

- Dirichlet series converges on $\mathrm{Re}(s) > 1$
- Reflection formula :
  $\xi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s) = \xi(1-s)$
- Hence, analytically continued to $\mathbb{C}$, except for the pole $s = 1$.

Properties of $L(E, s)$

- Dirichlet series converges on $\mathrm{Re}(s) > \frac{3}{2}$
- Reflection formula : $\Lambda(E, s) = N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E, s) = \omega\Lambda(E, 2-s)$ for some $\omega = \pm 1$. (This is from Modularity theorem!)
- Hence, analytically continued to $\mathbb{C}$ except for some poles.

Elliptic curves

1M$ Millennium problem about $L(E, s)$: BSD!

Elliptic curves

1M$ Millennium problem about $L(E, s)$: BSD!

Conjecture(Birch and Swinnerton-Dyer conjecture).

For any elliptic curve E,

$$\mathrm{rank} E(\mathbb{Q}) = \operatorname*{ord}_{s=1} L(E, s)$$

Elliptic curves

1M$ Millennium problem about $L(E, s)$: BSD!

Conjecture(Birch and Swinnerton-Dyer conjecture).

For any elliptic curve E,

$$\mathrm{rank} E(\mathbb{Q}) = \operatorname*{ord}_{s=1} L(E, s)$$

i.e.,

$$L(E, s) = c_1(s-1)^{\mathrm{rank} E(\mathbb{Q})} + O((s-1)^{\mathrm{rank} E(\mathbb{Q})+1})$$

Elliptic curves

1M$ Millennium problem about $L(E, s)$: BSD!

Conjecture(Birch and Swinnerton-Dyer conjecture).

For any elliptic curve E,

$$\mathrm{rank} E(\mathbb{Q}) = \operatorname*{ord}_{s=1} L(E, s)$$

i.e.,

$$L(E, s) = c_1(s-1)^{\mathrm{rank} E(\mathbb{Q})} + O((s-1)^{\mathrm{rank} E(\mathbb{Q})+1})$$

- BSD connects the algebraic data(Mordell-Weil group) with analytic data(Hasse-Weil L-function).

Elliptic Curves

One way to calculate rank$E(\mathbb{Q})$: descent!(for short, calculating $E(\mathbb{Q})/mE(\mathbb{Q})$). In the process, we need to know one more invariant about EC.

One way to calculate rank$E(\mathbb{Q})$: descent!(for short, calculating $E(\mathbb{Q})/mE(\mathbb{Q})$). In the process, we need to know one more invariant about EC.

Definition(Tate-Shafarevich group).

We define Tate-Shafarevich group of an elliptic curve E as following :

$$Ш(E/\mathbb{Q}) := \bigcap_{\text{place } v} \ker\left(H^1(G(\mathbb{Q}), E) \to H^1(G(\mathbb{Q}_v), E_v)\right)$$

where v runs for all places of $\mathbb{Q}$.

One way to calculate rank$E(\mathbb{Q})$: descent!(for short, calculating $E(\mathbb{Q})/mE(\mathbb{Q})$). In the process, we need to know one more invariant about EC.

Definition(Tate-Shafarevich group).

We define Tate-Shafarevich group of an elliptic curve E as following :

$$Ш(E/\mathbb{Q}) := \bigcap_{\text{place } v} \ker\left(H^1(G(\mathbb{Q}), E) \to H^1(G(\mathbb{Q}_v), E_v)\right)$$

where v runs for all places of $\mathbb{Q}$.

Precise definition of $Ш$... skip.

- Intuition : $Ш$ measures the failure of local-global principal!

Outline

The Analogy

Object in EC and NF **aligns**.

The Analogy

Object in EC and NF **aligns**.

1st example :

Number Field : Theorem.

h_K is always finite.

The Analogy

Object in EC and NF **aligns**.

1st example :

Number Field : Theorem.

h_K is always finite.

Elliptic Curve : Conjecture(Tate-Shafarevich Conjecture).

$Ш(E/\mathbb{Q})$ is always finite.

The Analogy

The Analogy

But, there is one more thing. Remind :

The Analogy

But, there is one more thing. Remind :

Elliptic Curve : Theorem(Mordell-Weil theorem).

$E(\mathbb{Q})$ is finitely generated. i.e., $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tor}}$ where $E(\mathbb{Q})_{\mathrm{tor}}$ is one of particular finite abelian groups.

The Analogy

But, there is one more thing. Remind :

Elliptic Curve : Theorem(Mordell-Weil theorem).

$E(\mathbb{Q})$ is finitely generated. i.e., $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tor}}$ where $E(\mathbb{Q})_{\mathrm{tor}}$ is one of particular finite abelian groups.

While in the NF side, we have the following important theorem.

The Analogy

But, there is one more thing. Remind :

Elliptic Curve : Theorem(Mordell-Weil theorem).

$E(\mathbb{Q})$ is finitely generated. i.e., $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tor}}$ where $E(\mathbb{Q})_{\mathrm{tor}}$ is one of particular finite abelian groups.

While in the NF side, we have the following important theorem.

Number Field : Theorem(Dirichlet unit theorem).

$\mathcal{O}_K^\times$ is finitely generated. i.e., $\mathcal{O}_K^\times \cong \mathbb{Z}^r \oplus (\mathcal{O}_K^\times)_{\mathrm{tor}}$ where $r = r_1 + r_2 - 1$, $(\mathcal{O}_K^\times)_{\mathrm{tor}} = \mathcal{O}_K \cap \mathbb{S}^1$.

The Analogy

The Analogy

In NF side, we have Reflection formula

- $|D_K|^{\frac{s}{2}}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s) = |D_K|^{\frac{1-s}{2}}\Gamma_{\mathbb{R}}(1-s)^{r_1}\Gamma_{\mathbb{C}}(1-s)^{r_2}\zeta_K(1-s)$
- Where $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$, $\Gamma_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s)$

The Analogy

In NF side, we have Reflection formula

- $|D_K|^{\frac{s}{2}}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s) = |D_K|^{\frac{1-s}{2}}\Gamma_{\mathbb{R}}(1-s)^{r_1}\Gamma_{\mathbb{C}}(1-s)^{r_2}\zeta_K(1-s)$
- Where $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$, $\Gamma_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s)$

Checking order at $s = 1$, we have $\mathrm{ord}_{s=0}\,\zeta_K(s) = r_1 + r_2 - 1$

The Analogy

In NF side, we have Reflection formula

- $|D_K|^{\frac{s}{2}}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s) = |D_K|^{\frac{1-s}{2}}\Gamma_{\mathbb{R}}(1-s)^{r_1}\Gamma_{\mathbb{C}}(1-s)^{r_2}\zeta_K(1-s)$
- Where $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$, $\Gamma_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s)$

Checking order at $s = 1$, we have $\mathrm{ord}_{s=0}\,\zeta_K(s) = r_1 + r_2 - 1$
...which is $= \mathbf{rank}\mathcal{O}_K^{\times}$

The Analogy

So we get the second analogy :

The Analogy

So we get the second analogy :

Elliptic Curve : Conjecture(Birch and Swinnerton-Dyer conjecture).

$$\mathrm{rank} E(\mathbb{Q}) = \operatorname*{ord}_{s=1} L(E, s)$$

The Analogy

So we get the second analogy :

Elliptic Curve : Conjecture(Birch and Swinnerton-Dyer conjecture).

$$\mathrm{rank} E(\mathbb{Q}) = \operatorname*{ord}_{s=1} L(E, s)$$

Number Field : Theorem.

$$\mathrm{rank} \mathcal{O}_K^{\times} = \operatorname*{ord}_{s=0} \zeta_K(s)$$

The Analogy

So we get the second analogy :

Elliptic Curve : Conjecture(Birch and Swinnerton-Dyer conjecture).

$$\mathrm{rank} E(\mathbb{Q}) = \operatorname*{ord}_{s=1} L(E, s)$$

Number Field : Theorem.

$$\mathrm{rank} \mathcal{O}_K^{\times} = \operatorname*{ord}_{s=0} \zeta_K(s)$$

well well well.... not end yet.

The Analogy

In fact, we have precise version of BSD.

The Analogy

In fact, we have precise version of BSD.

Conjecture(Precise Birch and Swinnerton-Dyer conjecture).

For every elliptic curve E,

$$\text{rank}E(\mathbb{Q}) = \operatorname*{ord}_{s=1} L(E,s) = r$$

and

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q}) \cdot \text{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\text{tor}})^2}$$

for Reg_E is the regulator of E, Ω_E is the real period of E, c_p is the Tamagawa number of E at p.

The Analogy

In fact, we have precise version of BSD.

Conjecture(Precise Birch and Swinnerton-Dyer conjecture).

For every elliptic curve E,

$$\text{rank} E(\mathbb{Q}) = \operatorname*{ord}_{s=1} L(E,s) = r$$

and

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q}) \cdot \text{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\text{tor}})^2}$$

for Reg_E is the regulator of E, Ω_E is the real period of E, c_p is the Tamagawa number of E at p.

Now, let's calculate coeff. of ζ_K at $s = 0$

The Analogy

- $|D_K|^{\frac{s}{2}}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s) = |D_K|^{\frac{1-s}{2}}\Gamma_{\mathbb{R}}(1-s)^{r_1}\Gamma_{\mathbb{C}}(1-s)^{r_2}\zeta_K(1-s)$
- Where $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$, $\Gamma_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s)$

Taking Res at both sides, we can get the following.

The Analogy

- $|D_K|^{\frac{s}{2}}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s) = |D_K|^{\frac{1-s}{2}}\Gamma_{\mathbb{R}}(1-s)^{r_1}\Gamma_{\mathbb{C}}(1-s)^{r_2}\zeta_K(1-s)$
- Where $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$, $\Gamma_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s)$

Taking Res at both sides, we can get the following.

Theorem.

For every number field K,

$$\mathrm{rank}\mathcal{O}_K^{\times} = \operatorname*{ord}_{s=0}\zeta_K(s) = r$$

and

$$\lim_{s\to 0}\frac{\zeta_K(s)}{s^r} = -\frac{h_K\cdot \mathrm{Reg}_K}{w_K} = -\frac{\#Cl(K)\cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^{\times})_{\mathrm{tor}}}$$

The Analogy

- $|D_K|^{\frac{s}{2}}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s) = |D_K|^{\frac{1-s}{2}}\Gamma_{\mathbb{R}}(1-s)^{r_1}\Gamma_{\mathbb{C}}(1-s)^{r_2}\zeta_K(1-s)$
- Where $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$, $\Gamma_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s)$

Taking Res at both sides, we can get the following.

Theorem.

For every number field K,

$$\mathrm{rank}\mathcal{O}_K^{\times} = \operatorname*{ord}_{s=0}\zeta_K(s) = r$$

and

$$\lim_{s\to 0}\frac{\zeta_K(s)}{s^r} = -\frac{h_K\cdot \mathrm{Reg}_K}{w_K} = -\frac{\#Cl(K)\cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^{\times})_{\mathrm{tor}}}$$

Hence we get the real correspondence between EC and NF.

The Analogy

Elliptic Curve : Conjecture(Precise BSD).

For every elliptic curve E, $\mathrm{rank} E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E,s) = r$ and

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q}) \cdot \mathrm{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}$$

for Reg_E is the regulator of E, Ω_E is the real period of E, c_p is the Tamagawa number of E at p.

The Analogy

Elliptic Curve : Conjecture(Precise BSD).

For every elliptic curve E, $\mathrm{rank}E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E,s) = r$ and

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q}) \cdot \mathrm{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}$$

for Reg_E is the regulator of E, Ω_E is the real period of E, c_p is the Tamagawa number of E at p.

Number Field : Theorem.

For every number field K, $\mathrm{rank}\mathcal{O}_K^\times = \mathrm{ord}_{s=0}\, \zeta_K(s) = r$ and

$$\lim_{s\to 0} \frac{\zeta_K(s)}{s^r} = -\frac{\#Cl(K) \cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^\times)_{\mathrm{tor}}}$$

for Reg_E is the regulator of K.

Where does the analogy come from?

The analogy is clear, but ambiguous.

- $\lim_{s \to 0} \frac{\zeta_K(s)}{s^r} = -\frac{\#Cl(K) \cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^\times)_{\mathrm{tor}}}$

Where does the analogy come from?

The analogy is clear, but ambiguous.

- $\lim_{s\to 0} \frac{\zeta_K(s)}{s^r} = -\frac{\#Cl(K)\cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^\times)_{\mathrm{tor}}}$
- $\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Reg}_E\cdot \Omega_E\cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}$

Where does the analogy come from?

The analogy is clear, but ambiguous.

- $\lim_{s\to 0} \frac{\zeta_K(s)}{s^r} = -\frac{\#Cl(K)\cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^\times)_{\mathrm{tor}}}$
- $\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Reg}_E\cdot \Omega_E\cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}$

Some ambiguous points :

Where does the analogy come from?

The analogy is clear, but ambiguous.

- $\lim_{s\to 0} \frac{\zeta_K(s)}{s^r} = -\frac{\#Cl(K)\cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^\times)_{\mathrm{tor}}}$
- $\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}$

Some ambiguous points :

- Where are $\Omega_E, \prod_{p|N} c_p$ gone?

Where does the analogy come from?

The analogy is clear, but ambiguous.

- $\lim_{s\to 0} \frac{\zeta_K(s)}{s^r} = -\frac{\#Cl(K)\cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^\times)_{\mathrm{tor}}}$
- $\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}$

Some ambiguous points :

- Where are $\Omega_E, \prod_{p|N} c_p$ gone?
- Why $\#(\mathcal{O}_K^\times)_{\mathrm{tor}}$ but $(\#E(\mathbb{Q})_{\mathrm{tor}})^2$ in the denominator?

Where does the analogy come from?

The analogy is clear, but ambiguous.

- $\lim_{s\to 0} \frac{\zeta_K(s)}{s^r} = -\frac{\#Cl(K)\cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^\times)_{\mathrm{tor}}}$
- $\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}$

Some ambiguous points :

- Where are $\Omega_E, \prod_{p|N} c_p$ gone?
- Why $\#(\mathcal{O}_K^\times)_{\mathrm{tor}}$ but $(\#E(\mathbb{Q})_{\mathrm{tor}})^2$ in the denominator?
- Why $s = 1$ in EC, but $s = 0$ in NF?

Where does the analogy come from?

The analogy is clear, but ambiguous.

- $\lim_{s\to 0} \frac{\zeta_K(s)}{s^r} = -\frac{\#Cl(K)\cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^\times)_{\mathrm{tor}}}$
- $\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}$

Some ambiguous points :

- Where are $\Omega_E, \prod_{p|N} c_p$ gone?
- Why $\#(\mathcal{O}_K^\times)_{\mathrm{tor}}$ but $(\#E(\mathbb{Q})_{\mathrm{tor}})^2$ in the denominator?
- Why $s = 1$ in EC, but $s = 0$ in NF?
- Where does the minus in NF side come from?

Where does the analogy come from?

The analogy is clear, but ambiguous.

- $\lim_{s\to 0} \frac{\zeta_K(s)}{s^r} = -\frac{\#Cl(K)\cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^\times)_{\mathrm{tor}}}$
- $\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}$

Some ambiguous points :

- Where are $\Omega_E, \prod_{p|N} c_p$ gone?
- Why $\#(\mathcal{O}_K^\times)_{\mathrm{tor}}$ but $(\#E(\mathbb{Q})_{\mathrm{tor}})^2$ in the denominator?
- Why $s = 1$ in EC, but $s = 0$ in NF?
- Where does the minus in NF side come from?
- Why Theorems in NF, but Conjectures in EC?

Where does the analogy come from?

The analogy is clear, but ambiguous.

- $\lim_{s\to 0} \frac{\zeta_K(s)}{s^r} = -\frac{\#Cl(K)\cdot \mathrm{Reg}_K}{\#(\mathcal{O}_K^\times)_{\mathrm{tor}}}$
- $\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}$

Some ambiguous points :

- Where are $\Omega_E, \prod_{p|N} c_p$ gone?
- Why $\#(\mathcal{O}_K^\times)_{\mathrm{tor}}$ but $(\#E(\mathbb{Q})_{\mathrm{tor}})^2$ in the denominator?
- Why $s = 1$ in EC, but $s = 0$ in NF?
- Where does the minus in NF side come from?
- Why Theorems in NF, but Conjectures in EC?

그러게요... As mentioned, we'll not talk about how those come from. Just "throw" the topics.

Overview of the analogy

Why they align?

Overview of the analogy

Why they align?
Big Picture : Scheme

Overview of the analogy

Why they align?
Big Picture : Scheme

- ζ_k is in fact Hasse-Weil L-function for the scheme $\mathrm{Spec}(\mathcal{O}_K)$.

Overview of the analogy

Why they align?
Big Picture : Scheme

- ζ_k is in fact Hasse-Weil L-function for the scheme $\mathrm{Spec}(\mathcal{O}_K)$.

We can generalize Hasse-Weil L-function for

Overview of the analogy

Why they align?
Big Picture : Scheme

- ζ_k is in fact Hasse-Weil L-function for the scheme $\mathrm{Spec}(\mathcal{O}_K)$.

We can generalize Hasse-Weil L-function for

- general curve

Overview of the analogy

Why they align?
Big Picture : Scheme

- ζ_k is in fact Hasse-Weil L-function for the scheme $\mathrm{Spec}(\mathcal{O}_K)$.

We can generalize Hasse-Weil L-function for

- general curve
- algebraic variety

Overview of the analogy

Why they align?
Big Picture : Scheme

- ζ_k is in fact Hasse-Weil L-function for the scheme $\mathrm{Spec}(\mathcal{O}_K)$.

We can generalize Hasse-Weil L-function for

- general curve
- algebraic variety
- scheme(Arithmetic zeta function)

Overview of the analogy

Why they align?
Big Picture : Scheme

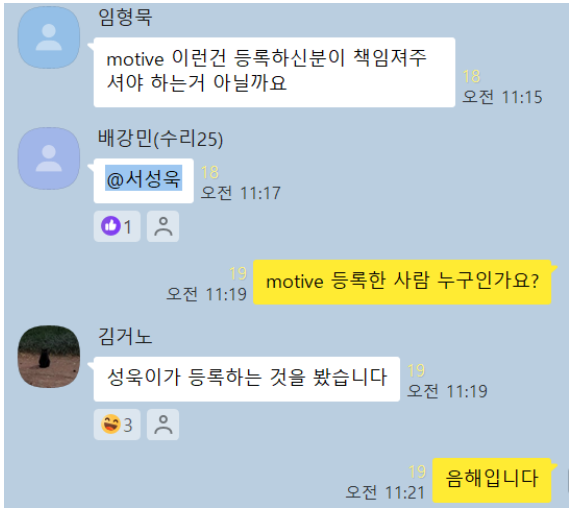
- ζ_k is in fact Hasse-Weil L-function for the scheme $\mathrm{Spec}(\mathcal{O}_K)$.

We can generalize Hasse-Weil L-function for

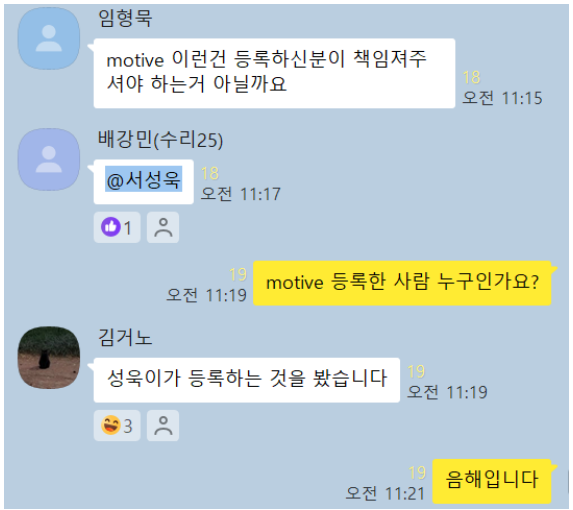
- general curve
- algebraic variety
- scheme(Arithmetic zeta function)

Much Bigger Picture : Motive!

Overview of the analogy

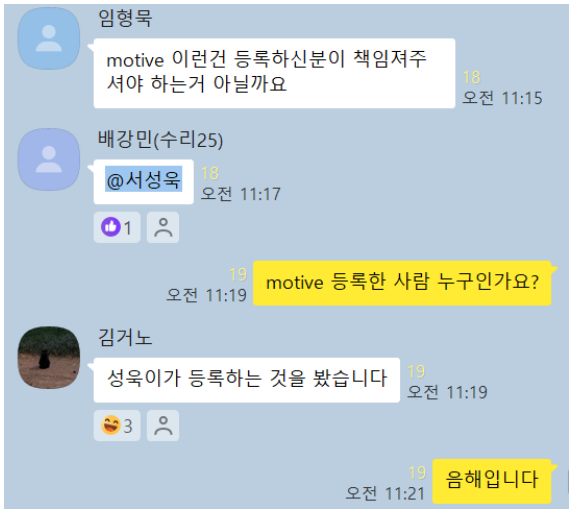


Overview of the analogy



Definition of Motive :

Overview of the analogy



Definition of Motive :

In the formulation of Grothendieck for smooth projective varieties, a motive is a triple (X, p, m), where X is a smooth projective variety, $p : X \vdash X$ is an idempotent correspondence, and m an integer; however, such a triple contains almost no information outside the context of Grothendieck's category of pure motives, where a morphism from (X, p, m) to (Y, q, n) is given by a correspondence of degree $n - m$. A more object-focused approach is taken by Pierre Deligne in *Le Groupe Fondamental de la Droite Projective Moins Trois Points*. In that article, a motive is a "system of realisations" – that is, a tuple

$$\left(M_B, M_{\mathrm{DR}}, M_{\mathbb{A}^f}, M_{\mathrm{cris},p}, \mathrm{comp}_{\mathrm{DR},B}, \mathrm{comp}_{\mathbb{A}^f,B}, \mathrm{comp}_{\mathrm{cris}\,p,\mathrm{DR}}, W, F_\infty, F, \phi, \phi_p\right)$$

consisting of modules

$$M_B, M_{\mathrm{DR}}, M_{\mathbb{A}^f}, M_{\mathrm{cris},p}$$

over the rings

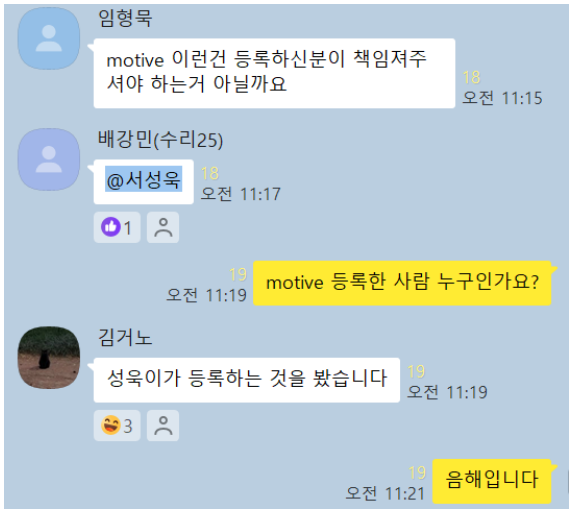
$$\mathbb{Q}, \mathbb{Q}, \mathbb{A}^f, \mathbb{Q}_p,$$

respectively, various comparison isomorphisms

$$\mathrm{comp}_{\mathrm{DR},B}, \mathrm{comp}_{\mathbb{A}^f,B}, \mathrm{comp}_{\mathrm{cris}\,p,\mathrm{DR}}$$

between the obvious base changes of these modules, filtrations W, F, a action ϕ of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ on $M_{\mathbb{A}^f}$, and a "Frobenius" automorphism ϕ_p of $M_{\mathrm{cris},p}$. This data is modeled on the cohomologies of a smooth projective $\mathbb{Q}$-variety and the structures and compatibilities they admit, and gives an idea about what kind of information is contained in a motive.

Overview of the analogy



Definition of Motive :

In the formulation of Grothendieck for smooth projective varieties, a motive is a triple (X, p, m), where X is a smooth projective variety, $p : X \vdash X$ is an idempotent correspondence, and m an integer; however, such a triple contains almost no information outside the context of Grothendieck's category of pure motives, where a morphism from (X, p, m) to (Y, q, n) is given by a correspondence of degree $n - m$. A more object-focused approach is taken by Pierre Deligne in *Le Groupe Fondamental de la Droite Projective Moins Trois Points*. In that article, a motive is a "system of realisations" – that is, a tuple

$$\left(M_B, M_{\mathrm{DR}}, M_{\mathbb{A}^f}, M_{\mathrm{cris},p}, \mathrm{comp}_{\mathrm{DR},B}, \mathrm{comp}_{\mathbb{A}^f,B}, \mathrm{comp}_{\mathrm{cris}\,p,\mathrm{DR}}, W, F_\infty, F, \phi, \phi_p\right)$$

consisting of modules

$$M_B, M_{\mathrm{DR}}, M_{\mathbb{A}^f}, M_{\mathrm{cris},p}$$

over the rings

$$\mathbb{Q}, \mathbb{Q}, \mathbb{A}^f, \mathbb{Q}_p,$$

respectively, various comparison isomorphisms

$$\mathrm{comp}_{\mathrm{DR},B}, \mathrm{comp}_{\mathbb{A}^f,B}, \mathrm{comp}_{\mathrm{cris}\,p,\mathrm{DR}}$$

between the obvious base changes of these modules, filtrations W, F, a action ϕ of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ on $M_{\mathbb{A}^f}$, and a "Frobenius" automorphism ϕ_p of $M_{\mathrm{cris},p}$. This data is modeled on the cohomologies of a smooth projective $\mathbb{Q}$-variety and the structures and compatibilities they admit, and gives an idea about what kind of information is contained in a motive.

...skip.

Big Picture of the analogy

- In short : Motive = Schemes with extra structure... with extra structure

Big Picture of the analogy

- In short : Motive = Schemes with extra structure... with extra structure
- We can also make **L-function** with motive : Motivic L-function $L(s, M)$, which is generalization of both ζ_K and $L(E, s)$.

Big Picture of the analogy

- In short : Motive = Schemes with extra structure... with extra structure
- We can also make **L-function** with motive : Motivic L-function $L(s, M)$, which is generalization of both ζ_K and $L(E, s)$.

Conjecture(Bloch-Kato conjecture for L-functions).

$L(s, M)$ has zero at $s = 0$ with order

$$\operatorname*{ord}_{s=0} L(s, M) = \dim H_1^f(G_K, V^*(1)) - \dim H_0(G_K, V^*(1))$$

and and Taylor coefficient at $s = 0$ is proportional to $Ш \cdot \mathrm{Reg}$.

Big Picture of the analogy

- In short : Motive = Schemes with extra structure... with extra structure
- We can also make **L-function** with motive : Motivic L-function $L(s, M)$, which is generalization of both ζ_K and $L(E, s)$.

Conjecture(Bloch-Kato conjecture for L-functions).

$L(s, M)$ has zero at $s = 0$ with order

$$\operatorname*{ord}_{s=0} L(s, M) = \dim H_1^f(G_K, V^*(1)) - \dim H_0(G_K, V^*(1))$$

and and Taylor coefficient at $s = 0$ is proportional to $Ш \cdot \mathrm{Reg}$.

...where those are about is global Bloch-Kato Selmer group, absolute Galois group, continuous Galois cohomology.

Big Picture of the analogy

- In short : Motive = Schemes with extra structure... with extra structure
- We can also make **L-function** with motive : Motivic L-function $L(s, M)$, which is generalization of both ζ_K and $L(E, s)$.

Conjecture(Bloch-Kato conjecture for L-functions).

$L(s, M)$ has zero at $s = 0$ with order

$$\operatorname*{ord}_{s=0} L(s, M) = \dim H_1^f(G_K, V^*(1)) - \dim H_0(G_K, V^*(1))$$

and and Taylor coefficient at $s = 0$ is proportional to $Ш \cdot \mathrm{Reg}$.

...where those are about is global Bloch-Kato Selmer group, absolute Galois group, continuous Galois cohomology.

- Motivic L-function is one part of **Langlands Program**!
  - More precise : All motivic L is automorphic L.(Like Modularity theorem.)

The End

서울대 수리과학부 25학번 서성욱