Elliptic Curves and the Special Values of L-functions

ICTS, 2021

Introduction to Elliptic Curves: Lecture 3

Anupam Saikia

Department of Mathematics,
Indian Institute of Technology Guwahati

Sections

Sections

The Riemann Zeta Function: a typical example

- We are familiar with the zeta series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad s \in \mathbb{C}.$$

- The series converges for all complex numbers s with $Re(s) > 1$ giving us the the Riemann zeta function.
- The Riemann zeta function $\zeta(s)$ has analytic continuation to all of $\mathbb{C}$, except for a simple pole of residue 1 at $s = 1$.
- The Riemann zeta function also satisfies a functional equation, relating its values at s and $1 - s$.
- The Riemnann zeta function can be expressed as a Euler product

$$\zeta(s) = \prod_p \frac{1}{(1 - p^{-s})}, \qquad Re(s) > 1.$$

The Riemann Zeta Function: a typical example

- We are familiar with the zeta series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad s \in \mathbb{C}.$$

- The series converges for all complex numbers s with $Re(s) > 1$ giving us the the Riemann zeta function.
- The Riemann zeta function $\zeta(s)$ has analytic continuation to all of $\mathbb{C}$, except for a simple pole of residue 1 at $s = 1$.
- The Riemann zeta function also satisfies a functional equation, relating its values at s and $1 - s$.
- The Riemnann zeta function can be expressed as a Euler product

$$\zeta(s) = \prod_{p} \frac{1}{(1 - p^{-s})}, \qquad Re(s) > 1.$$

The Riemann Zeta Function: a typical example

- We are familiar with the zeta series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad s \in \mathbb{C}.$$

- The series converges for all complex numbers s with $Re(s) > 1$ giving us the the Riemann zeta function.
- The Riemann zeta function $\zeta(s)$ has analytic continuation to all of $\mathbb{C}$, except for a simple pole of residue 1 at $s = 1$.
- The Riemann zeta function also satisfies a functional equation, relating its values at s and $1-s$.
- The Riemnann zeta function can be expressed as a Euler product

$$\zeta(s) = \prod_{p} \frac{1}{(1-p^{-s})}, \qquad Re(s) > 1.$$

The Riemann Zeta Function: a typical example

- We are familiar with the zeta series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad s \in \mathbb{C}.$$

- The series converges for all complex numbers s with $Re(s) > 1$ giving us the the Riemann zeta function.
- The Riemann zeta function $\zeta(s)$ has analytic continuation to all of $\mathbb{C}$, except for a simple pole of residue 1 at $s = 1$.
- The Riemann zeta function also satisfies a functional equation, relating its values at s and $1 - s$.
- The Riemnann zeta function can be expressed as a Euler product

$$\zeta(s) = \prod_{p} \frac{1}{(1 - p^{-s})}, \qquad Re(s) > 1.$$

The Riemann Zeta Function: a typical example

- We are familiar with the zeta series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad s \in \mathbb{C}.$$

- The series converges for all complex numbers s with $Re(s) > 1$ giving us the the Riemann zeta function.
- The Riemann zeta function $\zeta(s)$ has analytic continuation to all of $\mathbb{C}$, except for a simple pole of residue 1 at $s = 1$.
- The Riemann zeta function also satisfies a functional equation, relating its values at s and $1 - s$.
- The Riemnann zeta function can be expressed as a Euler product

$$\zeta(s) = \prod_{p} \frac{1}{(1 - p^{-s})}, \qquad Re(s) > 1.$$

Arithmetic Significance of Values of $\zeta(s)$

The values of the Riemann zeta function at at even positive integers are related to Bernoulli numbers, and have interesting arithmetic interpretations in terms of ideal class groups of cyclotomic fields. We have

$$\zeta(2n) = (-1)^{n+1} \frac{(2\pi)^{2n} B_{2n}}{2(2n)!}, \qquad n \in \mathbb{N},$$

where B_k denotes the k-th Bernoulli number defined by

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Let A denote the p-Sylow subgroup of the class group of the cyclotomic field $\mathbb{Q}(\zeta_p)$ for an odd prime p, and $A^{(i)}$ denote χ^i component of A where χ is the cyclotomic character.

Herbrand's Theorem: If $p \mid \#A^{(i)}$, then $p \mid B_{p-i}$ for $3 \leq i \leq p-2$, i odd.
Ribet's Theorem: The converse also holds.

Lichtenbaum's conjecture gives arithmetic interpretation for values of $\zeta(s)$ at odd negative integers.

Arithmetic Significance of Values of $\zeta(s)$

The values of the Riemann zeta function at at even positive integers are related to Bernoulli numbers, and have interesting arithmetic interpretations in terms of ideal class groups of cyclotomic fields. We have

$$\zeta(2n) = (-1)^{n+1}\frac{(2\pi)^{2n}B_{2n}}{2(2n)!}, \qquad n \in \mathbb{N},$$

where B_k denotes the k-th Bernoulli number defined by

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Let A denote the p-Sylow subgroup of the class group of the cyclotomic field $\mathbb{Q}(\zeta_p)$ for an odd prime p, and $A^{(i)}$ denote χ^i component of A where χ is the cyclotomic character.

Herbrand's Theorem: If $p \mid \#A^{(i)}$, then $p \mid B_{p-i}$ for $3 \le i \le p-2$, i odd.
Ribet's Theorem: The converse also holds.

Lichtenbaum's conjecture gives arithmetic interpretation for values of $\zeta(s)$ at odd negative integers.

Arithmetic Significance of Values of $\zeta(s)$

The values of the Riemann zeta function at at even positive integers are related to Bernoulli numbers, and have interesting arithmetic interpretations in terms of ideal class groups of cyclotomic fields. We have

$$\zeta(2n) = (-1)^{n+1}\frac{(2\pi)^{2n}B_{2n}}{2(2n)!}, \qquad n \in \mathbb{N},$$

where B_k denotes the k-th Bernoulli number defined by

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Let A denote the p-Sylow subgroup of the class group of the cyclotomic field $\mathbb{Q}(\zeta_p)$ for an odd prime p, and $A^{(i)}$ denote χ^i component of A where χ is the cyclotomic character.

Herbrand's Theorem: If $p \mid \#A^{(i)}$, then $p \mid B_{p-i}$ for $3 \leq i \leq p-2$, i odd.
Ribet's Theorem: The converse also holds.

Lichtenbaum's conjecture gives arithmetic interpretation for values of $\zeta(s)$ at odd negative integers.

Arithmetic Significance of Values of $\zeta(s)$

The values of the Riemann zeta function at at even positive integers are related to Bernoulli numbers, and have interesting arithmetic interpretations in terms of ideal class groups of cyclotomic fields. We have

$$\zeta(2n) = (-1)^{n+1}\frac{(2\pi)^{2n}B_{2n}}{2(2n)!}, \qquad n \in \mathbb{N},$$

where B_k denotes the k-th Bernoulli number defined by

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Let A denote the p-Sylow subgroup of the class group of the cyclotomic field $\mathbb{Q}(\zeta_p)$ for an odd prime p, and $A^{(i)}$ denote χ^i component of A where χ is the cyclotomic character.

Herbrand's Theorem: If $p \mid \#A^{(i)}$, then $p \mid B_{p-i}$ for $3 \leq i \leq p-2$, i odd.
Ribet's Theorem: The converse also holds.

Lichtenbaum's conjecture gives arithmetic interpretation for values of $\zeta(s)$ at odd negative integers.

Arithmetic Significance of Values of $\zeta(s)$

The values of the Riemann zeta function at at even positive integers are related to Bernoulli numbers, and have interesting arithmetic interpretations in terms of ideal class groups of cyclotomic fields. We have

$$\zeta(2n) = (-1)^{n+1}\frac{(2\pi)^{2n}B_{2n}}{2(2n)!}, \qquad n \in \mathbb{N},$$

where B_k denotes the k-th Bernoulli number defined by

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Let A denote the p-Sylow subgroup of the class group of the cyclotomic field $\mathbb{Q}(\zeta_p)$ for an odd prime p, and $A^{(i)}$ denote χ^i component of A where χ is the cyclotomic character.

Herbrand's Theorem: If $p \mid \#A^{(i)}$, then $p \mid B_{p-i}$ for $3 \leq i \leq p-2$, i odd.

Ribet's Theorem: The converse also holds.

Lichtenbaum's conjecture gives arithmetic interpretation for values of $\zeta(s)$ at odd negative integers.

Arithmetic Significance of Values of $\zeta(s)$

The values of the Riemann zeta function at at even positive integers are related to Bernoulli numbers, and have interesting arithmetic interpretations in terms of ideal class groups of cyclotomic fields. We have

$$\zeta(2n) = (-1)^{n+1}\frac{(2\pi)^{2n}B_{2n}}{2(2n)!}, \qquad n \in \mathbb{N},$$

where B_k denotes the k-th Bernoulli number defined by

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Let A denote the p-Sylow subgroup of the class group of the cyclotomic field $\mathbb{Q}(\zeta_p)$ for an odd prime p, and $A^{(i)}$ denote χ^i component of A where χ is the cyclotomic character.

Herbrand's Theorem: If $p \mid \#A^{(i)}$, then $p \mid B_{p-i}$ for $3 \le i \le p-2$, i odd.
Ribet's Theorem: The converse also holds.

Lichtenbaum's conjecture gives arithmetic interpretation for values of $\zeta(s)$ at odd negative integers.

Arithmetic Significance of Values of $\zeta(s)$

The values of the Riemann zeta function at at even positive integers are related to Bernoulli numbers, and have interesting arithmetic interpretations in terms of ideal class groups of cyclotomic fields. We have

$$\zeta(2n) = (-1)^{n+1} \frac{(2\pi)^{2n} B_{2n}}{2(2n)!}, \qquad n \in \mathbb{N},$$

where B_k denotes the k-th Bernoulli number defined by

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Let A denote the p-Sylow subgroup of the class group of the cyclotomic field $\mathbb{Q}(\zeta_p)$ for an odd prime p, and $A^{(i)}$ denote χ^i component of A where χ is the cyclotomic character.

Herbrand's Theorem: If $p \mid \#A^{(i)}$, then $p \mid B_{p-i}$ for $3 \leq i \leq p-2$, i odd.
Ribet's Theorem: The converse also holds.

Lichtenbaum's conjecture gives arithmetic interpretation for values of $\zeta(s)$ at odd negative integers.

The Dedekind Zeta Function of a Number Field

- Let K be a finite extension of $\mathbb{Q}$, and $\mathcal{O}_K$ be its ring of integers. For any non-zero ideal $\mathfrak{a}$, let $N\mathfrak{a}$ denote the cardinality of the quotient $\mathcal{O}_K/\mathfrak{a}$.

- The Dedekind zeta function of K is defined by the infinite series
$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s}, \qquad s \in \mathbb{C}, \quad Re(s) > 1.$$

- Since $\mathcal{O}_K$ is a Dedekind domain, every non-zero ideal $\mathfrak{a}$ can be expressed uniquely as a finite product of prime ideals $\mathfrak{p}$, giving an Euler product
$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1-(N\mathfrak{p})^{-s}}, \qquad Re(s) > 1.$$

- The Dedekind zeta function too has a meromorphic continuation to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, Dirichlet's class number formula.

The Dedekind Zeta Function of a Number Field

- Let K be a finite extension of $\mathbb{Q}$, and $\mathcal{O}_K$ be its ring of integers. For any non-zero ideal $\mathfrak{a}$, let $N\mathfrak{a}$ denote the cardinality of the quotient $\mathcal{O}_K/\mathfrak{a}$.
- The Dedekind zeta function of K is defined by the infinite series
$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s}, \qquad s \in \mathbb{C}, \;\; Re(s) > 1.$$
- Since $\mathcal{O}_K$ is a Dedekind domain, every non-zero ideal $\mathfrak{a}$ can be expressed uniquely as a finite product of prime ideals $\mathfrak{p}$, giving an Euler product
$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1-(N\mathfrak{p})^{-s}}, \qquad Re(s) > 1.$$
- The Dedekind zeta function too has a meromorphic continuation to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, Dirichlet's class number formula.

The Dedekind Zeta Function of a Number Field

- Let K be a finite extension of $\mathbb{Q}$, and $\mathcal{O}_K$ be its ring of integers. For any non-zero ideal $\mathfrak{a}$, let $N\mathfrak{a}$ denote the cardinality of the quotient $\mathcal{O}_K/\mathfrak{a}$.
- The Dedekind zeta function of K is defined by the infinite series
$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s}, \qquad s \in \mathbb{C}, \quad Re(s) > 1.$$
- Since $\mathcal{O}_K$ is a Dedekind domain, every non-zero ideal $\mathfrak{a}$ can be expressed uniquely as a finite product of prime ideals $\mathfrak{p}$, giving an Euler product
$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1-(N\mathfrak{p})^{-s}}, \qquad Re(s) > 1.$$
- The Dedekind zeta function too has a meromorphic continuation to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, Dirichlet's class number formula.

The Dedekind Zeta Function of a Number Field

- Let K be a finite extension of $\mathbb{Q}$, and $\mathcal{O}_K$ be its ring of integers. For any non-zero ideal $\mathfrak{a}$, let $N\mathfrak{a}$ denote the cardinality of the quotient $\mathcal{O}_K/\mathfrak{a}$.

- The Dedekind zeta function of K is defined by the infinite series
$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s}, \qquad s \in \mathbb{C}, \quad Re(s) > 1.$$

- Since $\mathcal{O}_K$ is a Dedekind domain, every non-zero ideal $\mathfrak{a}$ can be expressed uniquely as a finite product of prime ideals $\mathfrak{p}$, giving an Euler product
$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1-(N\mathfrak{p})^{-s}}, \qquad Re(s) > 1.$$

- The Dedekind zeta function too has a meromorphic continuation to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, Dirichlet's class number formula.

The Dedekind Zeta Function of a Number Field

- Let K be a finite extension of $\mathbb{Q}$, and $\mathcal{O}_K$ be its ring of integers. For any non-zero ideal $\mathfrak{a}$, let $N\mathfrak{a}$ denote the cardinality of the quotient $\mathcal{O}_K/\mathfrak{a}$.
- The Dedekind zeta function of K is defined by the infinite series
$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s}, \qquad s \in \mathbb{C}, \;\; Re(s) > 1.$$
- Since $\mathcal{O}_K$ is a Dedekind domain, every non-zero ideal $\mathfrak{a}$ can be expressed uniquely as a finite product of prime ideals $\mathfrak{p}$, giving an Euler product
$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1-(N\mathfrak{p})^{-s}}, \qquad Re(s) > 1.$$
- The Dedekind zeta function too has a meromorphic continuation to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, Dirichlet's class number formula.

Dirichlet L-functions: another example

- A Dirichlet character χ is a group homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}, \qquad \chi(ab) = \chi(a)\chi(b).$$

χ can also be thought of as a function on $\mathbb{Z}$ by defining

$$\chi(n) = \begin{cases} \chi(n \text{ mod } N) & \text{if } (n, N) = 1 \\ \chi(n) = 0 & \text{if } (n, N) \neq 1 \end{cases}$$

- For any Dirichlet character χ, one can construct the Dirichlet L-series

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad Re(s) > 1.$$

- The Dirichlet L-series can be expressed as a Euler product, can be meromorphically continued to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, non-vanishing of $L(1, \chi)$ for non-trivial χ leads to Dirichlet's theorem on primes in arithmetic progression.

Dirichlet L-functions: another example

- A Dirichlet character χ is a group homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}, \qquad \chi(ab) = \chi(a)\chi(b).$$

χ can also be thought of as a function on $\mathbb{Z}$ by defining

$$\chi(n) = \begin{cases} \chi(n \text{ mod } N) & \text{if } (n, N) = 1 \\ \chi(n) = 0 & \text{if } (n, N) \neq 1 \end{cases}$$

- For any Dirichlet character χ, one can construct the Dirichlet L-series

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad Re(s) > 1.$$

- The Dirichlet L-series can be expressed as a Euler product, can be meromorphically continued to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, non-vanishing of $L(1, \chi)$ for non-trivial χ leads to Dirichlet's theorem on primes in arithmetic progression.

Dirichlet L-functions: another example

- A Dirichlet character χ is a group homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}, \qquad \chi(ab) = \chi(a)\chi(b).$$

χ can also be thought of as a function on $\mathbb{Z}$ by defining

$$\chi(n) = \begin{cases} \chi(n \text{ mod } N) & \text{if } (n, N) = 1 \\ \chi(n) = 0 & \text{if } (n, N) \neq 1 \end{cases}$$

- For any Dirichlet character χ, one can construct the Dirichlet L-series

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad Re(s) > 1.$$

- The Dirichlet L-series can be expressed as a Euler product, can be meromorphically continued to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, non-vanishing of $L(1, \chi)$ for non-trivial χ leads to Dirichlet's theorem on primes in arithmetic progression.

Dirichlet L-functions: another example

- A Dirichlet character χ is a group homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}, \qquad \chi(ab) = \chi(a)\chi(b).$$

χ can also be thought of as a function on $\mathbb{Z}$ by defining

$$\chi(n) = \begin{cases} \chi(n \text{ mod } N) & \text{if } (n, N) = 1 \\ \chi(n) = 0 & \text{if } (n, N) \neq 1 \end{cases}$$

- For any Dirichlet character χ, one can construct the Dirichlet L-series

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad Re(s) > 1.$$

- The Dirichlet L-series can be expressed as a Euler product, can be meromorphically continued to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, non-vanishing of $L(1, \chi)$ for non-trivial χ leads to Dirichlet's theorem on primes in arithmetic progression.

Dirichlet L-functions: another example

- A Dirichlet character χ is a group homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}, \qquad \chi(ab) = \chi(a)\chi(b).$$

χ can also be thought of as a function on $\mathbb{Z}$ by defining

$$\chi(n) = \begin{cases} \chi(n \text{ mod } N) & \text{if } (n, N) = 1 \\ \chi(n) = 0 & \text{if } (n, N) \neq 1 \end{cases}$$

- For any Dirichlet character χ, one can construct the Dirichlet L-series

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad Re(s) > 1.$$

- The Dirichlet L-series can be expressed as a Euler product, can be meromorphically continued to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, non-vanishing of $L(1, \chi)$ for non-trivial χ leads to Dirichlet's theorem on primes in arithmetic progression.

Dirichlet L-functions: another example

- A Dirichlet character χ is a group homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}, \qquad \chi(ab) = \chi(a)\chi(b).$$

χ can also be thought of as a function on $\mathbb{Z}$ by defining

$$\chi(n) = \begin{cases} \chi(n \text{ mod } N) & \text{if } (n, N) = 1 \\ \chi(n) = 0 & \text{if } (n, N) \neq 1 \end{cases}$$

- For any Dirichlet character χ, one can construct the Dirichlet L-series

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad Re(s) > 1.$$

- The Dirichlet L-series can be expressed as a Euler product, can be meromorphically continued to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, non-vanishing of $L(1, \chi)$ for non-trivial χ leads to Dirichlet's theorem on primes in arithmetic progression.

Dirichlet L-functions: another example

- A Dirichlet character χ is a group homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}, \qquad \chi(ab) = \chi(a)\chi(b).$$

χ can also be thought of as a function on $\mathbb{Z}$ by defining

$$\chi(n) = \begin{cases} \chi(n \text{ mod } N) & \text{if } (n, N) = 1 \\ \chi(n) = 0 \quad \text{if } (n, N) \neq 1 \end{cases}$$

- For any Dirichlet character χ, one can construct the Dirichlet L-series

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad Re(s) > 1.$$

- The Dirichlet L-series can be expressed as a Euler product, can be meromorphically continued to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, non-vanishing of $L(1, \chi)$ for non-trivial χ leads to Dirichlet's theorem on primes in arithmetic progression.

Dirichlet L-functions: another example

- A Dirichlet character χ is a group homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}, \qquad \chi(ab) = \chi(a)\chi(b).$$

χ can also be thought of as a function on $\mathbb{Z}$ by defining

$$\chi(n) = \begin{cases} \chi(n \text{ mod } N) & \text{if } (n, N) = 1 \\ \chi(n) = 0 \quad \text{if } (n, N) \neq 1 \end{cases}$$

- For any Dirichlet character χ, one can construct the Dirichlet L-series

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad Re(s) > 1.$$

- The Dirichlet L-series can be expressed as a Euler product, can be meromorphically continued to the whole complex plane, satisfies a functional equation, and its values at integers have arithmetic significance. For example, non-vanishing of $L(1, \chi)$ for non-trivial χ leads to Dirichlet's theorem on primes in arithmetic progression.

The L-function of an Elliptic Curve

- The L-function of an elliptic curve $E/\mathbb{Q}$ can be defined as a Euler product that converges on one half of the complex plane, i.e.,

$$L(E,s) := \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C}, \qquad Re(s) > \frac{3}{2}.$$

- For each rational prime p, the local L-factor $L_p(E,s)$ is such that it contains arithmetic information about the curve at the prime p.

- In order to motivate the definition of the local factor, we first discuss the notion of zeta function of a projective variety over a finite field.

- It is natural to expect meromorphic/analytic continuation of $L(E,s)$ to the whole complex plane, a functional equation and most importantly, interpretation of the value of the function at integers (most crucially as it turns out, at $s = 1$.)

The L-function of an Elliptic Curve

- The L-function of an elliptic curve $E/\mathbb{Q}$ can be defined as a Euler product that converges on one half of the complex plane, i.e.,

$$L(E,s) := \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C}, \qquad Re(s) > \frac{3}{2}.$$

- For each rational prime p, the local L-factor $L_p(E,s)$ is such that it contains arithmetic information about the curve at the prime p.

- In order to motivate the definition of the local factor, we first discuss the notion of zeta function of a projective variety over a finite field.

- It is natural to expect meromorphic/analytic continuation of $L(E,s)$ to the whole complex plane, a functional equation and most importantly, interpretation of the value of the function at integers (most crucially as it turns out, at $s = 1$.)

The L-function of an Elliptic Curve

- The L-function of an elliptic curve $E/\mathbb{Q}$ can be defined as a Euler product that converges on one half of the complex plane, i.e.,

$$L(E,s) := \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C}, \qquad Re(s) > \frac{3}{2}.$$

- For each rational prime p, the local L-factor $L_p(E,s)$ is such that it contains arithmetic information about the curve at the prime p.

- In order to motivate the definition of the local factor, we first discuss the notion of zeta function of a projective variety over a finite field.

- It is natural to expect meromorphic/analytic continuation of $L(E,s)$ to the whole complex plane, a functional equation and most importantly, interpretation of the value of the function at integers (most crucially as it turns out, at $s = 1$.)

The L-function of an Elliptic Curve

- The L-function of an elliptic curve $E/\mathbb{Q}$ can be defined as a Euler product that converges on one half of the complex plane, i.e.,

$$L(E,s) := \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C}, \qquad Re(s) > \frac{3}{2}.$$

- For each rational prime p, the local L-factor $L_p(E,s)$ is such that it contains arithmetic information about the curve at the prime p.

- In order to motivate the definition of the local factor, we first discuss the notion of zeta function of a projective variety over a finite field.

- It is natural to expect meromorphic/analytic continuation of $L(E,s)$ to the whole complex plane, a functional equation and most importantly, interpretation of the value of the function at integers (most crucially as it turns out, at $s = 1$.)

The L-function of an Elliptic Curve

- The L-function of an elliptic curve $E/\mathbb{Q}$ can be defined as a Euler product that converges on one half of the complex plane, i.e.,

$$L(E,s) := \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C}, \qquad Re(s) > \frac{3}{2}.$$

- For each rational prime p, the local L-factor $L_p(E,s)$ is such that it contains arithmetic information about the curve at the prime p.

- In order to motivate the definition of the local factor, we first discuss the notion of zeta function of a projective variety over a finite field.

- It is natural to expect meromorphic/analytic continuation of $L(E,s)$ to the whole complex plane, a functional equation and most importantly, interpretation of the value of the function at integers (most crucially as it turns out, at $s = 1$.)

The L-function of an Elliptic Curve

- The L-function of an elliptic curve $E/\mathbb{Q}$ can be defined as a Euler product that converges on one half of the complex plane, i.e.,

$$L(E,s) := \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C}, \qquad Re(s) > \frac{3}{2}.$$

- For each rational prime p, the local L-factor $L_p(E,s)$ is such that it contains arithmetic information about the curve at the prime p.

- In order to motivate the definition of the local factor, we first discuss the notion of zeta function of a projective variety over a finite field.

- It is natural to expect meromorphic/analytic continuation of $L(E,s)$ to the whole complex plane, a functional equation and most importantly, interpretation of the value of the function at integers (most crucially as it turns out, at $s = 1$.)

The L-function of an Elliptic Curve

- The L-function of an elliptic curve $E/\mathbb{Q}$ can be defined as a Euler product that converges on one half of the complex plane, i.e.,

$$L(E,s) := \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C}, \qquad Re(s) > \frac{3}{2}.$$

- For each rational prime p, the local L-factor $L_p(E,s)$ is such that it contains arithmetic information about the curve at the prime p.

- In order to motivate the definition of the local factor, we first discuss the notion of zeta function of a projective variety over a finite field.

- It is natural to expect meromorphic/analytic continuation of $L(E,s)$ to the whole complex plane, a functional equation and most importantly, interpretation of the value of the function at integers (most crucially as it turns out, at $s = 1$.)

Sections

Sections

The Zeta Function of a Projective Variety $V/\mathbb{F}_q$

- Let V be a projective variety defined over the finite field $\mathbb{F}_q$ of $q = p^f$ elements, where p is a prime. Let $\mathbb{F}_{q^n}$ be the unique extension of $\mathbb{F}_q$ of degree n, so $\#\mathbb{F}_{q^n} = q^n$.

- The zeta function of $V/\mathbb{F}_q$ is defined as the power series

$$Z(V/\mathbb{F}_q, T) := \exp\left(\sum_{n=1}^{\infty}(\#V(\mathbb{F}_{q^n})\frac{T^n}{n}\right).$$

- For example, with $V = \mathbb{P}^N$, we have

$$\#V(\mathbb{F}_{q^n}) = \frac{q^{n(N+1)} - 1}{q^n - 1} = \sum_{i=0}^{N} q^{ni}$$

$$\implies \log Z(V/\mathbb{F}_q, T) = \sum_{n=1}^{\infty}\left(\sum_{i=0}^{N} q^{ni}\right)\frac{T^n}{n} = \sum_{i=0}^{N} -\log(1 - q^i T)$$

$$\implies Z(V/\mathbb{F}_q, T) = \frac{1}{(1-T)(1-qT)\dots(1-q^N T)}.$$

The Zeta Function of a Projective Variety $V/\mathbb{F}_q$

- Let V be a projective variety defined over the finite field $\mathbb{F}_q$ of $q = p^f$ elements, where p is a prime. Let $\mathbb{F}_{q^n}$ be the unique extension of $\mathbb{F}_q$ of degree n, so $\#\mathbb{F}_{q^n} = q^n$.
- The zeta function of $V/\mathbb{F}_q$ is defined as the power series

$$Z(V/\mathbb{F}_q, T) := \exp\Big(\sum_{n=1}^{\infty}(\#V(\mathbb{F}_{q^n})\frac{T^n}{n}\Big).$$

- For example, with $V = \mathbb{P}^N$, we have

$$\#V(\mathbb{F}_{q^n}) = \frac{q^{n(N+1)}-1}{q^n-1} = \sum_{i=0}^{N} q^{ni}$$

$$\implies \log Z(V/\mathbb{F}_q, T) = \sum_{n=1}^{\infty}\Big(\sum_{i=0}^{N} q^{ni}\Big)\frac{T^n}{n} = \sum_{i=0}^{N} -\log(1-q^iT)$$

$$\implies Z(V/\mathbb{F}_q, T) = \frac{1}{(1-T)(1-qT)\ldots(1-q^NT)}.$$

The Zeta Function of a Projective Variety $V/\mathbb{F}_q$

- Let V be a projective variety defined over the finite field $\mathbb{F}_q$ of $q = p^f$ elements, where p is a prime. Let $\mathbb{F}_{q^n}$ be the unique extension of $\mathbb{F}_q$ of degree n, so $\#\mathbb{F}_{q^n} = q^n$.
- The zeta function of $V/\mathbb{F}_q$ is defined as the power series

$$Z(V/\mathbb{F}_q, T) := \exp\Big(\sum_{n=1}^{\infty}(\#V(\mathbb{F}_{q^n})\frac{T^n}{n}\Big).$$

- For example, with $V = \mathbb{P}^N$, we have

$$\#V(\mathbb{F}_{q^n}) = \frac{q^{n(N+1)} - 1}{q^n - 1} = \sum_{i=0}^{N} q^{ni}$$

$$\implies \log Z(V/\mathbb{F}_q, T) = \sum_{n=1}^{\infty}\Big(\sum_{i=0}^{N} q^{ni}\Big)\frac{T^n}{n} = \sum_{i=0}^{N} -\log(1 - q^i T)$$

$$\implies Z(V/\mathbb{F}_q, T) = \frac{1}{(1-T)(1-qT)\dots(1-q^N T)}.$$

The Zeta Function of a Projective Variety $V/\mathbb{F}_q$

- Let V be a projective variety defined over the finite field $\mathbb{F}_q$ of $q = p^f$ elements, where p is a prime. Let $\mathbb{F}_{q^n}$ be the unique extension of $\mathbb{F}_q$ of degree n, so $\#\mathbb{F}_{q^n} = q^n$.

- The zeta function of $V/\mathbb{F}_q$ is defined as the power series

$$Z(V/\mathbb{F}_q, T) := \exp\left(\sum_{n=1}^{\infty} (\#V(\mathbb{F}_{q^n}))\frac{T^n}{n}\right).$$

- For example, with $V = \mathbb{P}^N$, we have

$$\#V(\mathbb{F}_{q^n}) = \frac{q^{n(N+1)} - 1}{q^n - 1} = \sum_{i=0}^{N} q^{ni}$$

$$\implies \log Z(V/\mathbb{F}_q, T) = \sum_{n=1}^{\infty}\left(\sum_{i=0}^{N} q^{ni}\right)\frac{T^n}{n} = \sum_{i=0}^{N} -\log(1 - q^i T)$$

$$\implies Z(V/\mathbb{F}_q, T) = \frac{1}{(1-T)(1-qT)\dots(1-q^N T)}.$$

The Weil Conjectures

The Weil Conjectures (1949) predict the behaviour of the zeta function for any smooth projective variety $V/\mathbb{F}_q$ of dimension N as follows:

- Rationality: $Z(V/\mathbb{F}_q, T) \in \mathbb{Q}(T)$.
- Functional Equation: there is an integer ϵ such that

$$Z(V/\mathbb{F}_q, 1/q^N T) = \pm q^{N\epsilon/2} T^\epsilon Z(V/\mathbb{F}_q, T).$$

- Riemann Hypothesis: The zeta function factors as

$$Z(V/\mathbb{F}_q, T) = \frac{P_1(T)\dots P_{2N-1}(T)}{P_0(T)\dots P_{2N}(T)}, \qquad P_i(T) \in \mathbb{Z}[T],$$

with $P_0(T) = 1 - T$, $P_{2N}(T) = 1 - q^N T$, and for each $0 \le i \le 2N$, the polynomials $P_i(T)$ factors over $\mathbb{C}$ as

$$P_i(T) = \prod_{j=1}^{b_i}(1 - \alpha_{ij}T), \qquad |\alpha_{ij}| = q^{\frac{1}{2}}.$$

The Weil Conjectures

The Weil Conjectures (1949) predict the behaviour of the zeta function for any smooth projective variety $V/\mathbb{F}_q$ of dimension N as follows:

- Rationality: $Z(V/\mathbb{F}_q, T) \in \mathbb{Q}(T)$.
- Functional Equation: there is an integer ϵ such that

$$Z(V/\mathbb{F}_q,\, 1/q^N T) = \pm q^{N\epsilon/2} T^{\epsilon} Z(V/\mathbb{F}_q, T).$$

- Riemann Hypothesis: The zeta function factors as

$$Z(V/\mathbb{F}_q, T) = \frac{P_1(T) \ldots P_{2N-1}(T)}{P_0(T) \ldots P_{2N}(T)}, \qquad P_i(T) \in \mathbb{Z}[T],$$

with $P_0(T) = 1 - T$, $P_{2N}(T) = 1 - q^N T$, and for each $0 \leq i \leq 2N$, the polynomials $P_i(T)$ factors over $\mathbb{C}$ as

$$P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T), \qquad |\alpha_{ij}| = q^{\frac{i}{2}}.$$

The Weil Conjectures

The Weil Conjectures (1949) predict the behaviour of the zeta function for any smooth projective variety $V/\mathbb{F}_q$ of dimension N as follows:

- Rationality: $Z(V/\mathbb{F}_q, T) \in \mathbb{Q}(T)$.
- Functional Equation: there is an integer ϵ such that

$$Z(V/\mathbb{F}_q,\, 1/q^N T) = \pm q^{N\epsilon/2} T^{\epsilon} Z(V/\mathbb{F}_q, T).$$

- Riemann Hypothesis: The zeta function factors as

$$Z(V/\mathbb{F}_q, T) = \frac{P_1(T)\ldots P_{2N-1}(T)}{P_0(T)\ldots P_{2N}(T)}, \qquad P_i(T) \in \mathbb{Z}[T],$$

with $P_0(T) = 1 - T$, $P_{2N}(T) = 1 - q^N T$, and for each $0 \leq i \leq 2N$, the polynomials $P_i(T)$ factors over $\mathbb{C}$ as

$$P_i(T) = \prod_{j=1}^{b_i}(1 - \alpha_{ij}T), \qquad |\alpha_{ij}| = q^{\frac{i}{2}}.$$

The Weil Conjectures

The Weil Conjectures (1949) predict the behaviour of the zeta function for any smooth projective variety $V/\mathbb{F}_q$ of dimension N as follows:

- Rationality: $Z(V/\mathbb{F}_q, T) \in \mathbb{Q}(T)$.
- Functional Equation: there is an integer ϵ such that

$$Z(V/\mathbb{F}_q,\, 1/q^N T) = \pm q^{N\epsilon/2} T^{\epsilon} Z(V/\mathbb{F}_q, T).$$

- Riemann Hypothesis: The zeta function factors as

$$Z(V/\mathbb{F}_q, T) = \frac{P_1(T)\dots P_{2N-1}(T)}{P_0(T)\dots P_{2N}(T)}, \qquad P_i(T) \in \mathbb{Z}[T],$$

with $P_0(T) = 1 - T$, $P_{2N}(T) = 1 - q^N T$, and for each $0 \leq i \leq 2N$, the polynomials $P_i(T)$ factors over $\mathbb{C}$ as

$$P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T), \qquad |\alpha_{ij}| = q^{\frac{1}{2}}.$$

The Weil Conjectures

The Weil Conjectures (1949) predict the behaviour of the zeta function for any smooth projective variety $V/\mathbb{F}_q$ of dimension N as follows:

- Rationality: $Z(V/\mathbb{F}_q, T) \in \mathbb{Q}(T)$.
- Functional Equation: there is an integer ϵ such that

$$Z(V/\mathbb{F}_q,\, 1/q^N T) = \pm q^{N\epsilon/2} T^{\epsilon} Z(V/\mathbb{F}_q, T).$$

- Riemann Hypothesis: The zeta function factors as

$$Z(V/\mathbb{F}_q, T) = \frac{P_1(T) \dots P_{2N-1}(T)}{P_0(T) \dots P_{2N}(T)}, \qquad P_i(T) \in \mathbb{Z}[T],$$

  with $P_0(T) = 1 - T$, $P_{2N}(T) = 1 - q^N T$, and for each $0 \leq i \leq 2N$, the polynomials $P_i(T)$ factors over $\mathbb{C}$ as

$$P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T), \qquad |\alpha_{ij}| = q^{\frac{1}{2}}.$$

The Zeta Function for an Elliptic Curve over $\mathbb{F}_q$

- The conjectures were proved by Weil for curves and abelian varieties. The rationality in general was proved by Dwork. Later, Deligne proved the Riemann hypothesis for projective varieties.

- By Weil Conjectures, the zeta function of an elliptic curve $E/\mathbb{F}_q$ can be written as

$$Z(E/\mathbb{F}_q, T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)},$$

where $\alpha,\ \beta \in \mathbb{C}$ and $\alpha\beta = q$.

- By Weil conjectures, we further have

$$|\alpha| = |\beta| = \sqrt{q},$$

The last statement implies that the zeroes of $Z(E/\mathbb{F}_q, q^{-s})$ lies on the line $Re(s) = \frac{1}{2}$, when we introduce the complex variable s by substituting $T = q^{-s}$.

The Zeta Function for an Elliptic Curve over $\mathbb{F}_q$

- The conjectures were proved by Weil for curves and abelian varieties. The rationality in general was proved by Dwork. Later, Deligne proved the Riemann hypothesis for projective varieties.
- By Weil Conjectures, the zeta function of an elliptic curve $E/\mathbb{F}_q$ can be written as

$$Z(E/\mathbb{F}_q, T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)},$$

  where $\alpha,\ \beta \in \mathbb{C}$ and $\alpha\beta = q$.
- By Weil conjectures, we further have

$$|\alpha| = |\beta| = \sqrt{q},$$

  The last statement implies that the zeroes of $Z(E/\mathbb{F}_q, q^{-s})$ lies on the line $Re(s) = \frac{1}{2}$, when we introduce the complex variable s by substituting $T = q^{-s}$.

The Zeta Function for an Elliptic Curve over $\mathbb{F}_q$

- The conjectures were proved by Weil for curves and abelian varieties. The rationality in general was proved by Dwork. Later, Deligne proved the Riemann hypothesis for projective varieties.
- By Weil Conjectures, the zeta function of an elliptic curve $E/\mathbb{F}_q$ can be written as

$$Z(E/\mathbb{F}_q, T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)},$$

where $\alpha,\ \beta \in \mathbb{C}$ and $\alpha\beta = q$.

- By Weil conjectures, we further have

$$|\alpha| = |\beta| = \sqrt{q},$$

The last statement implies that the zeroes of $Z(E/\mathbb{F}_q, q^{-s})$ lies on the line $Re(s) = \frac{1}{2}$, when we introduce the complex variable s by substituting $T = q^{-s}$.

The Zeta Function for an Elliptic Curve over $\mathbb{F}_q$

- The conjectures were proved by Weil for curves and abelian varieties. The rationality in general was proved by Dwork. Later, Deligne proved the Riemann hypothesis for projective varieties.
- By Weil Conjectures, the zeta function of an elliptic curve $E/\mathbb{F}_q$ can be written as

$$Z(E/\mathbb{F}_q, T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)},$$

where $\alpha,\ \beta \in \mathbb{C}$ and $\alpha\beta = q$.

- By Weil conjectures, we further have

$$|\alpha| = |\beta| = \sqrt{q},$$

The last statement implies that the zeroes of $Z(E/\mathbb{F}_q, q^{-s})$ lies on the line $Re(s) = \frac{1}{2}$, when we introduce the complex variable s by substituting $T = q^{-s}$.

The Zeta Function for an Elliptic Curve over $\mathbb{F}_q$

- The conjectures were proved by Weil for curves and abelian varieties. The rationality in general was proved by Dwork. Later, Deligne proved the Riemann hypothesis for projective varieties.

- By Weil Conjectures, the zeta function of an elliptic curve $E/\mathbb{F}_q$ can be written as

$$Z(E/\mathbb{F}_q, T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)},$$

  where $\alpha, \ \beta \in \mathbb{C}$ and $\alpha\beta = q$.

- By Weil conjectures, we further have

$$|\alpha| = |\beta| = \sqrt{q},$$

The last statement implies that the zeroes of $Z(E/\mathbb{F}_q, q^{-s})$ lies on the line $Re(s) = \frac{1}{2}$, when we introduce the complex variable s by substituting $T = q^{-s}$.

The Zeta Function for an Elliptic Curve over $\mathbb{F}_q$

- The conjectures were proved by Weil for curves and abelian varieties. The rationality in general was proved by Dwork. Later, Deligne proved the Riemann hypothesis for projective varieties.
- By Weil Conjectures, the zeta function of an elliptic curve $E/\mathbb{F}_q$ can be written as

$$Z(E/\mathbb{F}_q, T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)},$$

where $\alpha,\ \beta \in \mathbb{C}$ and $\alpha\beta = q$.

- By Weil conjectures, we further have

$$|\alpha| = |\beta| = \sqrt{q},$$

The last statement implies that the zeroes of $Z(E/\mathbb{F}_q, q^{-s})$ lies on the line $Re(s) = \frac{1}{2}$, when we introduce the complex variable s by substituting $T = q^{-s}$.

The Euler Factor at p

$$Z(E/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}\right) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

$$\implies \#E(\mathbb{F}_q) = \frac{d}{dT} \log Z(E/\mathbb{F}_q, T)\Big|_{T=0}$$

$$= \left(\frac{-\alpha}{1-\alpha T} + \frac{-\beta}{1-\beta T} - \frac{-1}{1-T} - \frac{-q}{1-qT}\right)\Big|_{T=0}$$

$$\implies \#E(\mathbb{F}_q) = 1 + q - (\alpha + \beta).$$

- We frequently use the notation (*for the 'error term'*)

$$a_q = \alpha + \beta = 1 + q - \#E(\mathbb{F}_q) \qquad (|a_q| \le 2\sqrt{q} \text{ [Hasse bound]}).$$

- In forming the L-function of $E/\mathbb{Q}$, we take the Euler factor at a prime p from the numerator of the zeta function of $E/\mathbb{F}_p$, i.e.,

$$L_p(E, s) = (1 - \alpha p^{-s})(1 - \beta p^{-s}) = 1 - a_p p^{-s} + p^{1-2s}$$

except for a finitely many 'bad primes' (to be discussed next).

The Euler Factor at p

$$Z(E/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}\right) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

$$\implies \#E(\mathbb{F}_q) = \frac{d}{dT}\log Z(E/\mathbb{F}_q, T)\Big|_{T=0}$$

$$= \left(\frac{-\alpha}{1-\alpha T} + \frac{-\beta}{1-\beta T} - \frac{-1}{1-T} - \frac{-q}{1-qT}\right)\Big|_{T=0}$$

$$\implies \#E(\mathbb{F}_q) = 1 + q - (\alpha+\beta).$$

- We frequently use the notation (*for the 'error term'*)

  $a_q = \alpha + \beta = 1 + q - \#E(\mathbb{F}_q) \qquad (|a_q| \le 2\sqrt{q}$ [Hasse bound]).

- In forming the L-function of $E/\mathbb{Q}$, we take the Euler factor at a prime p from the numerator of the zeta function of $E/\mathbb{F}_p$, i.e.,

  $$L_p(E,s) = (1-\alpha p^{-s})(1-\beta p^{-s}) = 1 - a_p p^{-s} + p^{1-2s}$$

  except for a finitely many 'bad primes' (to be discussed next).

The Euler Factor at p

$$Z(E/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}\right) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

$$\implies \#E(\mathbb{F}_q) = \frac{d}{dT}\log Z(E/\mathbb{F}_q, T)\Big|_{T=0}$$

$$= \left(\frac{-\alpha}{1-\alpha T} + \frac{-\beta}{1-\beta T} - \frac{-1}{1-T} - \frac{-q}{1-qT}\right)\Big|_{T=0}$$

$$\implies \#E(\mathbb{F}_q) = 1 + q - (\alpha + \beta).$$

- We frequently use the notation (*for the 'error term'*)

  $$a_q = \alpha + \beta = 1 + q - \#E(\mathbb{F}_q) \qquad (|a_q| \leq 2\sqrt{q} \text{ [Hasse bound]}).$$

- In forming the L-function of $E/\mathbb{Q}$, we take the Euler factor at a prime p from the numerator of the zeta function of $E/\mathbb{F}_p$, i.e.,

  $$L_p(E, s) = (1 - \alpha p^{-s})(1 - \beta p^{-s}) = 1 - a_p p^{-s} + p^{1-2s}$$

  except for a finitely many 'bad primes' (to be discussed next).

The Euler Factor at p

$$Z(E/\mathbb{F}_q, T) = \exp\Big(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}\Big) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

$$\implies \#E(\mathbb{F}_q) = \frac{d}{dT}\log Z(E/\mathbb{F}_q, T)\Big|_{T=0}$$

$$= \Big(\frac{-\alpha}{1-\alpha T} + \frac{-\beta}{1-\beta T} - \frac{-1}{1-T} - \frac{-q}{1-qT}\Big)\Big|_{T=0}$$

$$\implies \#E(\mathbb{F}_q) = 1 + q - (\alpha+\beta).$$

- We frequently use the notation (*for the 'error term'*)

  $$a_q = \alpha + \beta = 1 + q - \#E(\mathbb{F}_q) \qquad (|a_q| \leq 2\sqrt{q} \ \text{[Hasse bound]}).$$

- In forming the L-function of $E/\mathbb{Q}$, we take the Euler factor at a prime p from the numerator of the zeta function of $E/\mathbb{F}_p$, i.e.,

  $$L_p(E, s) = (1-\alpha p^{-s})(1-\beta p^{-s}) = 1 - a_p p^{-s} + p^{1-2s}$$

  except for a finitely many 'bad primes' (to be discussed next).

The Euler Factor at p

$$Z(E/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}\right) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

$$\implies \#E(\mathbb{F}_q) = \frac{d}{dT}\log Z(E/\mathbb{F}_q, T)\Big|_{T=0}$$

$$= \left(\frac{-\alpha}{1-\alpha T} + \frac{-\beta}{1-\beta T} - \frac{-1}{1-T} - \frac{-q}{1-qT}\right)\Big|_{T=0}$$

$$\implies \#E(\mathbb{F}_q) = 1 + q - (\alpha+\beta).$$

- We frequently use the notation (*for the 'error term'*)

  $$a_q = \alpha + \beta = 1 + q - \#E(\mathbb{F}_q) \qquad (|a_q| \le 2\sqrt{q}\ \text{[Hasse bound]}).$$

- In forming the L-function of $E/\mathbb{Q}$, we take the Euler factor at a prime p from the numerator of the zeta function of $E/\mathbb{F}_p$, i.e.,

  $$L_p(E,s) = (1-\alpha p^{-s})(1-\beta p^{-s}) = 1 - a_p p^{-s} + p^{1-2s}$$

  except for a finitely many 'bad primes' (to be discussed next).

Bad Primes

- For simplicity, take an elliptic curve E over $\mathbb{Q}$ given by

$$f(x, y) = y^2 - (x^3 + ax + b), \quad a,\ b\ \in\ \mathbb{Z}.$$

- By reducing modulo a prime p, we obtain a curve $\tilde{E}$ over $\mathbb{F}_p$ as

$$\bar{f}(x, y) = y^2 - (x^3 + \bar{a}x + \bar{b}), \qquad \bar{a},\ \bar{b} \in \mathbb{F}_p.$$

- If $p \nmid (4a^3 + 27b^2)$ and $p \neq 2$, $\tilde{E}$ is an elliptic curve over $\mathbb{F}_p$. Then p is called a good prime. There are only finitely many bad primes.

- If $\tilde{E}$ has a singular point $S = (x_0, y_0)$, then the Taylor series expansion of $\bar{f}(x, y)$ at S has the form

$$\bar{f}(x, y) - \bar{f}(x_0, y_0) = [(y - y_0)^2 + l(x - x_0)(y - y_0) + m(x - x_0)^2] - (x - x_0)^3.$$

- We denote the non-singular points on $\tilde{E}$ by $\tilde{E}_{ns}$, which still has a group structure. If p is a good prime, $\tilde{E}_{ns} := \tilde{E}$.

Bad Primes

- For simplicity, take an elliptic curve E over $\mathbb{Q}$ given by

$$f(x, y) = y^2 - (x^3 + ax + b), \quad a,\ b\ \in\ \mathbb{Z}.$$

- By reducing modulo a prime p, we obtain a curve $\tilde{E}$ over $\mathbb{F}_p$ as

$$\bar{f}(x, y) = y^2 - (x^3 + \bar{a}x + \bar{b}), \qquad \bar{a},\ \bar{b} \in \mathbb{F}_p.$$

- If $p \nmid (4a^3 + 27b^2)$ and $p \neq 2$, $\tilde{E}$ is an elliptic curve over $\mathbb{F}_p$. Then p is called a good prime. There are only finitely many bad primes.

- If $\tilde{E}$ has a singular point $S = (x_0, y_0)$, then the Taylor series expansion of $\bar{f}(x, y)$ at S has the form

$$\bar{f}(x, y) - \bar{f}(x_0, y_0) = [(y - y_0)^2 + l(x - x_0)(y - y_0) + m(x - x_0)^2] - (x - x_0)^3.$$

- We denote the non-singular points on $\tilde{E}$ by $\tilde{E}_{ns}$, which still has a group structure. If p is a good prime, $\tilde{E}_{ns} := \tilde{E}$.

Bad Primes

- For simplicity, take an elliptic curve E over $\mathbb{Q}$ given by

$$f(x,y) = y^2 - (x^3 + ax + b), \quad a,\ b \in \mathbb{Z}.$$

- By reducing modulo a prime p, we obtain a curve $\tilde{E}$ over $\mathbb{F}_p$ as

$$\bar{f}(x,y) = y^2 - (x^3 + \bar{a}x + \bar{b}), \quad \bar{a},\ \bar{b} \in \mathbb{F}_p.$$

- If $p \nmid (4a^3 + 27b^2)$ and $p \neq 2$, $\tilde{E}$ is an elliptic curve over $\mathbb{F}_p$. Then p is called a good prime. There are only finitely many bad primes.

- If $\tilde{E}$ has a singular point $S = (x_0, y_0)$, then the Taylor series expansion of $\bar{f}(x,y)$ at S has the form

$$\bar{f}(x,y) - \bar{f}(x_0,y_0) = [(y-y_0)^2 + l(x-x_0)(y-y_0) + m(x-x_0)^2] - (x-x_0)^3.$$

- We denote the non-singular points on $\tilde{E}$ by $\tilde{E}_{ns}$, which still has a group structure. If p is a good prime, $\tilde{E}_{ns} := \tilde{E}$.

Bad Primes

- For simplicity, take an elliptic curve E over $\mathbb{Q}$ given by

$$f(x,y) = y^2 - (x^3 + ax + b), \quad a,\ b\ \in\ \mathbb{Z}.$$

- By reducing modulo a prime p, we obtain a curve $\tilde{E}$ over $\mathbb{F}_p$ as

$$\bar{f}(x,y) = y^2 - (x^3 + \bar{a}x + \bar{b}), \qquad \bar{a},\ \bar{b} \in \mathbb{F}_p.$$

- If $p \nmid (4a^3 + 27b^2)$ and $p \neq 2$, $\tilde{E}$ is an elliptic curve over $\mathbb{F}_p$. Then p is called a good prime. There are only finitely many bad primes.

- If $\tilde{E}$ has a singular point $S = (x_0, y_0)$, then the Taylor series expansion of $\bar{f}(x,y)$ at S has the form

$$\bar{f}(x,y) - \bar{f}(x_0,y_0) = [(y-y_0)^2 + l(x-x_0)(y-y_0) + m(x-x_0)^2] - (x-x_0)^3.$$

- We denote the non-singular points on $\tilde{E}$ by $\tilde{E}_{ns}$, which still has a group structure. If p is a good prime, $\tilde{E}_{ns} := \tilde{E}$.

Bad Primes

- For simplicity, take an elliptic curve E over $\mathbb{Q}$ given by

$$f(x,y) = y^2 - (x^3 + ax + b), \quad a,\ b\ \in\ \mathbb{Z}.$$

- By reducing modulo a prime p, we obtain a curve $\tilde{E}$ over $\mathbb{F}_p$ as

$$\bar{f}(x,y) = y^2 - (x^3 + \bar{a}x + \bar{b}), \qquad \bar{a},\ \bar{b} \in \mathbb{F}_p.$$

- If $p \nmid (4a^3 + 27b^2)$ and $p \neq 2$, $\tilde{E}$ is an elliptic curve over $\mathbb{F}_p$. Then p is called a good prime. There are only finitely many bad primes.

- If $\tilde{E}$ has a singular point $S = (x_0, y_0)$, then the Taylor series expansion of $\bar{f}(x,y)$ at S has the form

$$\bar{f}(x,y) - \bar{f}(x_0,y_0) = [(y-y_0)^2 + l(x-x_0)(y-y_0) + m(x-x_0)^2] - (x-x_0)^3.$$

- We denote the non-singular points on $\tilde{E}$ by $\tilde{E}_{ns}$, which still has a group structure. If p is a good prime, $\tilde{E}_{ns} := \tilde{E}$.

Bad Primes

- For simplicity, take an elliptic curve E over $\mathbb{Q}$ given by

$$f(x,y) = y^2 - (x^3 + ax + b), \quad a,\ b\ \in\ \mathbb{Z}.$$

- By reducing modulo a prime p, we obtain a curve $\tilde{E}$ over $\mathbb{F}_p$ as

$$\bar{f}(x,y) = y^2 - (x^3 + \bar{a}x + \bar{b}), \qquad \bar{a},\ \bar{b} \in \mathbb{F}_p.$$

- If $p \nmid (4a^3 + 27b^2)$ and $p \neq 2$, $\tilde{E}$ is an elliptic curve over $\mathbb{F}_p$. Then p is called a good prime. There are only finitely many bad primes.

- If $\tilde{E}$ has a singular point $S = (x_0, y_0)$, then the Taylor series expansion of $\bar{f}(x,y)$ at S has the form

$$\bar{f}(x,y) - \bar{f}(x_0,y_0) = [(y-y_0)^2 + l(x-x_0)(y-y_0) + m(x-x_0)^2] - (x-x_0)^3.$$

- We denote the non-singular points on $\tilde{E}$ by $\tilde{E}_{ns}$, which still has a group structure. If p is a good prime, $\tilde{E}_{ns} := \tilde{E}$.

Bad Primes

- For simplicity, take an elliptic curve E over $\mathbb{Q}$ given by

$$f(x,y) = y^2 - (x^3 + ax + b), \quad a,\ b\ \in\ \mathbb{Z}.$$

- By reducing modulo a prime p, we obtain a curve $\tilde{E}$ over $\mathbb{F}_p$ as

$$\bar{f}(x,y) = y^2 - (x^3 + \bar{a}x + \bar{b}), \qquad \bar{a},\ \bar{b} \in \mathbb{F}_p.$$

- If $p \nmid (4a^3 + 27b^2)$ and $p \neq 2$, $\tilde{E}$ is an elliptic curve over $\mathbb{F}_p$. Then p is called a good prime. There are only finitely many bad primes.

- If $\tilde{E}$ has a singular point $S = (x_0, y_0)$, then the Taylor series expansion of $\bar{f}(x,y)$ at S has the form

$$\bar{f}(x,y) - \bar{f}(x_0,y_0) = [(y-y_0)^2 + l(x-x_0)(y-y_0) + m(x-x_0)^2] - (x-x_0)^3.$$

- We denote the non-singular points on $\tilde{E}$ by $\tilde{E}_{ns}$, which still has a group structure. If p is a good prime, $\tilde{E}_{ns} := \tilde{E}$.

Bad Primes

- For simplicity, take an elliptic curve E over $\mathbb{Q}$ given by

  $$f(x,y) = y^2 - (x^3 + ax + b), \quad a,\ b\ \in\ \mathbb{Z}.$$

- By reducing modulo a prime p, we obtain a curve $\tilde{E}$ over $\mathbb{F}_p$ as

  $$\bar{f}(x,y) = y^2 - (x^3 + \bar{a}x + \bar{b}), \qquad \bar{a},\ \bar{b} \in \mathbb{F}_p.$$

- If $p \nmid (4a^3 + 27b^2)$ and $p \neq 2$, $\tilde{E}$ is an elliptic curve over $\mathbb{F}_p$. Then p is called a good prime. There are only finitely many bad primes.

- If $\tilde{E}$ has a singular point $S = (x_0, y_0)$, then the Taylor series expansion of $\bar{f}(x,y)$ at S has the form

  $$\bar{f}(x,y) - \bar{f}(x_0,y_0) = [(y-y_0)^2 + l(x-x_0)(y-y_0) + m(x-x_0)^2] - (x-x_0)^3.$$

- We denote the non-singular points on $\tilde{E}$ by $\tilde{E}_{ns}$, which still has a group structure. If p is a good prime, $\tilde{E}_{ns} := \tilde{E}$.

Types of Reduction

- If the quadratic $z^2 + lz + m$ in the Taylor expansion has a repeated root, we say that E has additive reduction at p. The singular point S is called a cusp in this case. One cas show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^+, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_p$ itself, we say that E has split multiplicative reduction at p. The singular point S is called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p - 1.$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_{p^2}$ (but not in $\mathbb{F}_{p^2}$ itself), we say that E has non-split multiplicative reduction at p. The singular point S is again called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \{\alpha \in \mathbb{F}_{p^2}^\times \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha) = 1\}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p + 1.$$

Types of Reduction

- If the quadratic $z^2 + lz + m$ in the Taylor expansion has a repeated root, we say that E has additive reduction at p. The singular point S is called a cusp in this case. One cas show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^{+}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_p$ itself, we say that E has split multiplicative reduction at p. The singular point S is called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^{\times}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p - 1.$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_{p^2}$ (but not in $\mathbb{F}_{p^2}$ itself), we say that E has non-split multiplicative reduction at p. The singular point S is again called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \{\alpha \in \mathbb{F}_{p^2}^{\times} \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha) = 1\}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p + 1.$$

Types of Reduction

- If the quadratic $z^2 + lz + m$ in the Taylor expansion has a repeated root, we say that E has additive reduction at p. The singular point S is called a cusp in this case. One cas show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^+, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_p$ itself, we say that E has split multiplicative reduction at p. The singular point S is called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p - 1.$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_{p^2}$ (but not in $\mathbb{F}_{p^2}$ itself), we say that E has non-split multiplicative reduction at p. The singular point S is again called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \{\alpha \in \mathbb{F}_{p^2}^\times \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha) = 1\}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p + 1.$$

Types of Reduction

- If the quadratic $z^2 + lz + m$ in the Taylor expansion has a repeated root, we say that E has additive reduction at p. The singular point S is called a cusp in this case. One cas show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^{+}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_p$ itself, we say that E has split multiplicative reduction at p. The singular point S is called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^{\times}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p - 1.$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_{p^2}$ (but not in $\mathbb{F}_{p^2}$ itself), we say that E has non-split multiplicative reduction at p. The singular point S is again called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \{\alpha \in \mathbb{F}_{p^2}^{\times} \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha) = 1\}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p + 1.$$

Types of Reduction

- If the quadratic $z^2 + lz + m$ in the Taylor expansion has a repeated root, we say that E has additive reduction at p. The singular point S is called a cusp in this case. One cas show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^+, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_p$ itself, we say that E has split multiplicative reduction at p. The singular point S is called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p - 1.$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_{p^2}$ (but not in $\mathbb{F}_{p^2}$ itself), we say that E has non-split multiplicative reduction at p. The singular point S is again called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \{\alpha \in \mathbb{F}_{p^2}^\times \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha) = 1\}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p + 1.$$

Types of Reduction

- If the quadratic $z^2 + lz + m$ in the Taylor expansion has a repeated root, we say that E has additive reduction at p. The singular point S is called a cusp in this case. One cas show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^+, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_p$ itself, we say that E has split multiplicative reduction at p. The singular point S is called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p - 1.$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_{p^2}$ (but not in $\mathbb{F}_{p^2}$ itself), we say that E has non-split multiplicative reduction at p. The singular point S is again called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \{\alpha \in \mathbb{F}_{p^2}^\times \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha) = 1\}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p + 1.$$

Types of Reduction

- If the quadratic $z^2 + lz + m$ in the Taylor expansion has a repeated root, we say that E has additive reduction at p. The singular point S is called a cusp in this case. One cas show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^+, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_p$ itself, we say that E has split multiplicative reduction at p. The singular point S is called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p - 1.$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_{p^2}$ (but not in $\mathbb{F}_{p^2}$ itself), we say that E has non-split multiplicative reduction at p. The singular point S is again called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \{\alpha \in \mathbb{F}_{p^2}^\times \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha) = 1\}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p + 1.$$

Types of Reduction

- If the quadratic $z^2 + lz + m$ in the Taylor expansion has a repeated root, we say that E has additive reduction at p. The singular point S is called a cusp in this case. One cas show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^+, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_p$ itself, we say that E has split multiplicative reduction at p. The singular point S is called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p - 1.$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_{p^2}$ (but not in $\mathbb{F}_{p^2}$ itself), we say that E has non-split multiplicative reduction at p. The singular point S is again called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \{\alpha \in \mathbb{F}_{p^2}^\times \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha) = 1\}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p + 1.$$

Types of Reduction

- If the quadratic $z^2 + lz + m$ in the Taylor expansion has a repeated root, we say that E has additive reduction at p. The singular point S is called a cusp in this case. One cas show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^+, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_p$ itself, we say that E has split multiplicative reduction at p. The singular point S is called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \mathbb{F}_p^\times, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p - 1.$$

- If the quadratic $z^2 + lz + m$ has two distinct roots in $\mathbb{F}_{p^2}$ (but not in $\mathbb{F}_{p^2}$ itself), we say that E has non-split multiplicative reduction at p. The singular point S is again called a node. One can show that

$$\tilde{E}_{ns}(\mathbb{F}_p) \simeq \{\alpha \in \mathbb{F}_{p^2}^\times \mid N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha) = 1\}, \qquad \#\tilde{E}_{ns}(\mathbb{F}_p) = p + 1.$$

Local L-Factors

- If p is a prime of bad reduction, the local L-factor at p is taken as

$$L_p(E,s) = \begin{cases} 1 - p^{-s} & \text{if } E \text{ has split multiplicative reduction at } p \\ 1 + p^{-s} & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 1 & \text{if } E \text{ has additive reduction at } p \end{cases}$$

- Let $N_p = \#\tilde{E}_{ns}(\mathbb{F}_p)$. Putting $s = 1$, we find that for any prime p of bad reduction

$$L_p(E,1) = \frac{N_p}{p}.$$

- Observe that even when E has good reduction at p, we have

$$L_p(E,1) = 1 - a_p p^{-1} + p^{1-2} = \frac{1 + p - a_p}{p} = \frac{\#\tilde{E}(\mathbb{F}_p)}{p} = \frac{N_p}{p}.$$

Local L-Factors

- If p is a prime of bad reduction, the local L-factor at p is taken as

$$L_p(E,s) = \begin{cases} 1 - p^{-s} & \text{if } E \text{ has split multiplicative reduction at } p \\ 1 + p^{-s} & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 1 & \text{if } E \text{ has additive reduction at } p \end{cases}$$

- Let $N_p = \#\tilde{E}_{ns}(\mathbb{F}_p)$. Putting $s = 1$, we find that for any prime p of bad reduction

$$L_p(E,1) = \frac{N_p}{p}.$$

- Observe that even when E has good reduction at p, we have

$$L_p(E,1) = 1 - a_p p^{-1} + p^{1-2} = \frac{1 + p - a_p}{p} = \frac{\#\tilde{E}(\mathbb{F}_p)}{p} = \frac{N_p}{p}.$$

Local L-Factors

- If p is a prime of bad reduction, the local L-factor at p is taken as

$$L_p(E,s) = \begin{cases} 1 - p^{-s} & \text{if } E \text{ has split multiplicative reduction at } p \\ 1 + p^{-s} & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 1 & \text{if } E \text{ has additive reduction at } p \end{cases}$$

- Let $N_p = \#\tilde{E}_{ns}(\mathbb{F}_p)$. Putting $s = 1$, we find that for any prime p of bad reduction

$$L_p(E,1) = \frac{N_p}{p}.$$

- Observe that even when E has good reduction at p, we have

$$L_p(E,1) = 1 - a_p p^{-1} + p^{1-2} = \frac{1 + p - a_p}{p} = \frac{\#\tilde{E}(\mathbb{F}_p)}{p} = \frac{N_p}{p}.$$

Local L-Factors

- If p is a prime of bad reduction, the local L-factor at p is taken as

$$L_p(E,s) = \begin{cases} 1 - p^{-s} & \text{if } E \text{ has split multiplicative reduction at } p \\ 1 + p^{-s} & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 1 & \text{if } E \text{ has additive reduction at } p \end{cases}$$

- Let $N_p = \#\tilde{E}_{ns}(\mathbb{F}_p)$. Putting $s = 1$, we find that for any prime p of bad reduction

$$L_p(E,1) = \frac{N_p}{p}.$$

- Observe that even when E has good reduction at p, we have

$$L_p(E,1) = 1 - a_p p^{-1} + p^{1-2} = \frac{1 + p - a_p}{p} = \frac{\#\tilde{E}(\mathbb{F}_p)}{p} = \frac{N_p}{p}.$$

The Hasse-Weil L-Function $L(E,s)$

- The Hasse-Weil Function of $E/\mathbb{Q}$ is defined by the Euler product

$$L(E,s) := \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C}$$
$$= \prod_{p\ \ good} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p\ \ bad} \frac{1}{L_p(E,s)}$$
$$= \prod_{p\ \ good} \frac{1}{(1-\alpha(p)p^{-s})(1-\beta(p)p^{-s})} \prod_{p\ \ bad} \frac{1}{L_p(E,s)},$$

- As $|\alpha(p)| = |\beta(p)| = \sqrt{p}$, the Euler product in $L(E,s)$ converges for $Re(s) > 3/2$.

- Hasse conjectured analytic continuation of $L(E,s)$ to $\mathbb{C}$.

- It was also expected that $L(E,s)$ also satisfies a functional equation relating $L(E,s)$ with $L(E,2-s)$.

- For an elliptic curve E over a number field K, $L(E/K,s)$ can be defined in a similar way.

The Hasse-Weil L-Function $L(E,s)$

- The Hasse-Weil Function of $E/\mathbb{Q}$ is defined by the Euler product

$$\begin{aligned} L(E,s) &:= \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C} \\ &= \prod_{p \ good} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p \ bad} \frac{1}{L_p(E,s)} \\ &= \prod_{p \ good} \frac{1}{(1-\alpha(p)p^{-s})(1-\beta(p)p^{-s})} \prod_{p \ bad} \frac{1}{L_p(E,s)}, \end{aligned}$$

- As $|\alpha(p)| = |\beta(p)| = \sqrt{p}$, the Euler product in $L(E,s)$ converges for $Re(s) > 3/2$.
- Hasse conjectured analytic continuation of $L(E,s)$ to $\mathbb{C}$.
- It was also expected that $L(E,s)$ also satisfies a functional equation relating $L(E,s)$ with $L(E,2-s)$.
- For an elliptic curve E over a number field K, $L(E/K,s)$ can be defined in a similar way.

The Hasse-Weil L-Function $L(E,s)$

- The Hasse-Weil Function of $E/\mathbb{Q}$ is defined by the Euler product

$$L(E,s) := \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C}$$

$$= \prod_{p \ \ good} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p \ \ bad} \frac{1}{L_p(E,s)}$$

$$= \prod_{p \ \ good} \frac{1}{(1-\alpha(p)p^{-s})(1-\beta(p)p^{-s})} \prod_{p \ \ bad} \frac{1}{L_p(E,s)},$$

- As $|\alpha(p)| = |\beta(p)| = \sqrt{p}$, the Euler product in $L(E,s)$ converges for $Re(s) > 3/2$.
- Hasse conjectured analytic continuation of $L(E,s)$ to $\mathbb{C}$.
- It was also expected that $L(E,s)$ also satisfies a functional equation relating $L(E,s)$ with $L(E,2-s)$.
- For an elliptic curve E over a number field K, $L(E/K,s)$ can be defined in a similar way.

The Hasse-Weil L-Function $L(E, s)$

- The Hasse-Weil Function of $E/\mathbb{Q}$ is defined by the Euler product

$$\begin{aligned} L(E,s) &:= \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C} \\ &= \prod_{p \ \ good} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p \ \ bad} \frac{1}{L_p(E,s)} \\ &= \prod_{p \ \ good} \frac{1}{(1-\alpha(p)p^{-s})(1-\beta(p)p^{-s})} \prod_{p \ \ bad} \frac{1}{L_p(E,s)}, \end{aligned}$$

- As $|\alpha(p)| = |\beta(p)| = \sqrt{p}$, the Euler product in $L(E, s)$ converges for $Re(s) > 3/2$.
- Hasse conjectured analytic continuation of $L(E, s)$ to $\mathbb{C}$.
- It was also expected that $L(E, s)$ also satisfies a functional equation relating $L(E, s)$ with $L(E, 2 - s)$.
- For an elliptic curve E over a number field K, $L(E/K, s)$ can be defined in a similar way.

The Hasse-Weil L-Function $L(E,s)$

- The Hasse-Weil Function of $E/\mathbb{Q}$ is defined by the Euler product

$$\begin{aligned} L(E,s) &:= \prod_p L_p(E,s)^{-1}, \qquad s \in \mathbb{C} \\ &= \prod_{p \ good} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p \ bad} \frac{1}{L_p(E,s)} \\ &= \prod_{p \ good} \frac{1}{(1-\alpha(p)p^{-s})(1-\beta(p)p^{-s})} \prod_{p \ bad} \frac{1}{L_p(E,s)}, \end{aligned}$$

- As $|\alpha(p)| = |\beta(p)| = \sqrt{p}$, the Euler product in $L(E,s)$ converges for $Re(s) > 3/2$.
- Hasse conjectured analytic continuation of $L(E,s)$ to $\mathbb{C}$.
- It was also expected that $L(E,s)$ also satisfies a functional equation relating $L(E,s)$ with $L(E,2-s)$.
- For an elliptic curve E over a number field K, $L(E/K,s)$ can be defined in a similar way.

Functional Equation

- The conductor N_E of an elliptic curve $E/\mathbb{Q}$ is an integer divisible only by primes of bad reduction. The conductor is defined as

$$N_E := \prod_{p \text{ bad}} p^{f_p},$$

where $f_p = \begin{cases} 1 \text{ if } E \text{ has multiplicative reduction at } p \\ 2 \text{ if } E \text{ has additive reduction at } p \neq 2, 3. \end{cases}$

  The value of f_p at primes 2 and 3 is more involved, which is beyond the scope of discussion here.

- Theorem: Let $\Lambda(E, s) = N_E^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E, s)$. Then $\Lambda(E, s)$ has analytic continuation to the whole complex plane and satisfies a functional equation

$$\Lambda(E, s) = w_E \Lambda(E, 2 - s), \qquad w_E = \pm 1.$$

  w_E is called the sign of the functional equation. It determines whether the order of vanishing of $L(E, s)$ at $s = 1$ is even or odd.

Functional Equation

- The conductor N_E of an elliptic curve $E/\mathbb{Q}$ is an integer divisible only by primes of bad reduction. The conductor is defined as

$$N_E := \prod_{p \text{ bad}} p^{f_p},$$

where $f_p = \begin{cases} 1 \text{ if } E \text{ has multiplicative reduction at } p \\ 2 \text{ if } E \text{ has additive reduction at } p \neq 2,3. \end{cases}$

The value of f_p at primes 2 and 3 is more involved, which is beyond the scope of discussion here.

- Theorem: Let $\Lambda(E,s) = N_E^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E,s)$. Then $\Lambda(E,s)$ has analytic continuation to the whole complex plane and satisfies a functional equation

$$\Lambda(E,s) = w_E \Lambda(E,2-s), \qquad w_E = \pm 1.$$

w_E is called the sign of the functional equation. It determines whether the order of vanishing of $L(E,s)$ at $s=1$ is even or odd.

Functional Equation

- The conductor N_E of an elliptic curve $E/\mathbb{Q}$ is an integer divisible only by primes of bad reduction. The conductor is defined as

$$N_E := \prod_{p \text{ bad}} p^{f_p},$$

$$\text{where } f_p = \begin{cases} 1 \text{ if } E \text{ has multiplicative reduction at } p \\ 2 \text{ if } E \text{ has additive reduction at } p \neq 2, 3. \end{cases}$$

The value of f_p at primes 2 and 3 is more involved, which is beyond the scope of discussion here.

- Theorem: Let $\Lambda(E,s) = N_E^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E,s)$. Then $\Lambda(E,s)$ has analytic continuation to the whole complex plane and satisfies a functional equation

$$\Lambda(E,s) = w_E \Lambda(E, 2-s), \qquad w_E = \pm 1.$$

w_E is called the sign of the functional equation. It determines whether the order of vanishing of $L(E,s)$ at $s = 1$ is even or odd.

Functional Equation

- The conductor N_E of an elliptic curve $E/\mathbb{Q}$ is an integer divisible only by primes of bad reduction. The conductor is defined as

$$N_E := \prod_{p \text{ bad}} p^{f_p},$$

$$\text{where } f_p = \begin{cases} 1 \text{ if } E \text{ has multiplicative reduction at } p \\ 2 \text{ if } E \text{ has additive reduction at } p \neq 2, 3. \end{cases}$$

The value of f_p at primes 2 and 3 is more involved, which is beyond the scope of discussion here.

- Theorem: Let $\Lambda(E, s) = N_E^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E, s)$. Then $\Lambda(E, s)$ has analytic continuation to the whole complex plane and satisfies a functional equation

$$\Lambda(E, s) = w_E \Lambda(E, 2 - s), \qquad w_E = \pm 1.$$

w_E is called the sign of the functional equation. It determines whether the order of vanishing of $L(E, s)$ at $s = 1$ is even or odd.

Functional Equation

- The conductor N_E of an elliptic curve $E/\mathbb{Q}$ is an integer divisible only by primes of bad reduction. The conductor is defined as

$$N_E := \prod_{p \text{ bad}} p^{f_p},$$

$$\text{where } f_p = \begin{cases} 1 \text{ if } E \text{ has multiplicative reduction at } p \\ 2 \text{ if } E \text{ has additive reduction at } p \neq 2, 3. \end{cases}$$

The value of f_p at primes 2 and 3 is more involved, which is beyond the scope of discussion here.

- Theorem: Let $\Lambda(E,s) = N_E^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E,s)$. Then $\Lambda(E,s)$ has analytic continuation to the whole complex plane and satisfies a functional equation

$$\Lambda(E,s) = w_E \Lambda(E, 2-s), \qquad w_E = \pm 1.$$

w_E is called the sign of the functional equation. It determines whether the order of vanishing of $L(E,s)$ at $s=1$ is even or odd.

Shimura-Taniyama Conjecture

- Let $L(E, s) = \sum_n a_n n^{-s}$. The modularity conjecture of Shimura-Taniyama predicted that

$$f(z) = \sum_n a_n e^{2\pi i n z}, \quad z \in \mathbb{C}, \quad Im(z) > 0$$

is a modular form of level N_E, i.e.,

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z), \quad \forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N_E).$$

- An equivalent formulation of Shimura-Taniyama Conjecture: Let $E/\mathbb{Q}$ be an elliptic curve. Then there exists a surjective morphism of curves over $\mathbb{Q}$ from the modular curve $X_0(N)$ to the elliptic curve E,

$$X_0(N) \longrightarrow E.$$

Shimura-Taniyama Conjecture

- Let $L(E,s) = \sum_n a_n n^{-s}$. The modularity conjecture of Shimura-Taniyama predicted that

$$f(z) = \sum_n a_n e^{2\pi i n z}, \quad z \in \mathbb{C}, \quad Im(z) > 0$$

is a modular form of level N_E, i.e.,

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z), \quad \forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N_E).$$

- An equivalent formulation of Shimura-Taniyama Conjecture: Let $E/\mathbb{Q}$ be an elliptic curve. Then there exists a surjective morphism of curves over $\mathbb{Q}$ from the modular curve $X_0(N)$ to the elliptic curve E,

$$X_0(N) \longrightarrow E.$$

Shimura-Taniyama Conjecture

- Let $L(E, s) = \sum_n a_n n^{-s}$. The modularity conjecture of Shimura-Taniyama predicted that

$$f(z) = \sum_n a_n e^{2\pi i n z}, \quad z \in \mathbb{C}, \quad Im(z) > 0$$

is a modular form of level N_E, i.e.,

$$f\Big(\frac{az+b}{cz+d}\Big) = (cz+d)^2 f(z), \quad \forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N_E).$$

- An equivalent formulation of Shimura-Taniyama Conjecture: Let $E/\mathbb{Q}$ be an elliptic curve. Then there exists a surjective morphism of curves over $\mathbb{Q}$ from the modular curve $X_0(N)$ to the elliptic curve E,

$$X_0(N) \longrightarrow E.$$

Consequence of Modularity of $E/\mathbb{Q}$

- Frey conjectured (1982) and Ribet (1986) proved the following.
  If $a^p + b^p = c^p$ for a prime $p > 3$, then the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ will violate the modularity conjecture.
- Wiles (with help of Taylor) showed that if $E/\mathbb{Q}$ has either good or multiplicative reduction at all primes p, then $E/\mathbb{Q}$ is modular. As a consequence, Fermat's Last Theorem followed.
- Breuil, Conrad, Diamond and Taylor proved the modularity conjecture for all $E/\mathbb{Q}$. As a consequence, analytic continuation and functional equation of $L(E,s)$ followed for $E/\mathbb{Q}$.
- The analytic continuation and functional equation of $L(E/K,s)$ for any elliptic curve over a general number field K is not yet resolved. For real quadratic and totally real cubic number fields, a modularity result has been obtained by work of Siksek et al which implies analytic continuation for E/K. For elliptic curves with complex multiplication, analytic continuation of $L(E/K,s)$ is known for any number field K.

Consequence of Modularity of $E/\mathbb{Q}$

- Frey conjectured (1982) and Ribet (1986) proved the following.

  If $a^p + b^p = c^p$ for a prime $p > 3$, then the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ will violate the modularity conjecture.

- Wiles (with help of Taylor) showed that if $E/\mathbb{Q}$ has either good or multiplicative reduction at all primes p, then $E/\mathbb{Q}$ is modular. As a consequence, Fermat's Last Theorem followed.

- Breuil, Conrad, Diamond and Taylor proved the modularity conjecture for all $E/\mathbb{Q}$. As a consequence, analytic continuation and functional equation of $L(E, s)$ followed for $E/\mathbb{Q}$.

- The analytic continuation and functional equation of $L(E/K, s)$ for any elliptic curve over a general number field K is not yet resolved. For real quadratic and totally real cubic number fields, a modularity result has been obtained by work of Siksek et al which implies analytic continuation for E/K. For elliptic curves with complex multiplication, analytic continuation of $L(E/K, s)$ is known for any number field K.

Consequence of Modularity of $E/\mathbb{Q}$

- Frey conjectured (1982) and Ribet (1986) proved the following.

  If $a^p + b^p = c^p$ for a prime $p > 3$, then the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ will violate the modularity conjecture.

- Wiles (with help of Taylor) showed that if $E/\mathbb{Q}$ has either good or multiplicative reduction at all primes p, then $E/\mathbb{Q}$ is modular. As a consequence, Fermat's Last Theorem followed.

- Breuil, Conrad, Diamond and Taylor proved the modularity conjecture for all $E/\mathbb{Q}$. As a consequence, analytic continuation and functional equation of $L(E, s)$ followed for $E/\mathbb{Q}$.

- The analytic continuation and functional equation of $L(E/K, s)$ for any elliptic curve over a general number field K is not yet resolved. For real quadratic and totally real cubic number fields, a modularity result has been obtained by work of Siksek et al which implies analytic continuation for E/K. For elliptic curves with complex multiplication, analytic continuation of $L(E/K, s)$ is known for any number field K.

Consequence of Modularity of $E/\mathbb{Q}$

- Frey conjectured (1982) and Ribet (1986) proved the following.

  If $a^p + b^p = c^p$ for a prime $p > 3$, then the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ will violate the modularity conjecture.
- Wiles (with help of Taylor) showed that if $E/\mathbb{Q}$ has either good or multiplicative reduction at all primes p, then $E/\mathbb{Q}$ is modular. As a consequence, Fermat's Last Theorem followed.
- Breuil, Conrad, Diamond and Taylor proved the modularity conjecture for all $E/\mathbb{Q}$. As a consequence, analytic continuation and functional equation of $L(E, s)$ followed for $E/\mathbb{Q}$.
- The analytic continuation and functional equation of $L(E/K, s)$ for any elliptic curve over a general number field K is not yet resolved. For real quadratic and totally real cubic number fields, a modularity result has been obtained by work of Siksek et al which implies analytic continuation for E/K. For elliptic curves with complex multiplication, analytic continuation of $L(E/K, s)$ is known for any number field K.

Consequence of Modularity of $E/\mathbb{Q}$

- Frey conjectured (1982) and Ribet (1986) proved the following.

  If $a^p + b^p = c^p$ for a prime $p > 3$, then the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ will violate the modularity conjecture.
- Wiles (with help of Taylor) showed that if $E/\mathbb{Q}$ has either good or multiplicative reduction at all primes p, then $E/\mathbb{Q}$ is modular. As a consequence, Fermat's Last Theorem followed.
- Breuil, Conrad, Diamond and Taylor proved the modularity conjecture for all $E/\mathbb{Q}$. As a consequence, analytic continuation and functional equation of $L(E, s)$ followed for $E/\mathbb{Q}$.
- The analytic continuation and functional equation of $L(E/K, s)$ for any elliptic curve over a general number field K is not yet resolved. For real quadratic and totally real cubic number fields, a modularity result has been obtained by work of Siksek et al which implies analytic continuation for E/K. For elliptic curves with complex multiplication, analytic continuation of $L(E/K, s)$ is known for any number field K.

Consequence of Modularity of $E/\mathbb{Q}$

- Frey conjectured (1982) and Ribet (1986) proved the following.

  If $a^p + b^p = c^p$ for a prime $p > 3$, then the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ will violate the modularity conjecture.
- Wiles (with help of Taylor) showed that if $E/\mathbb{Q}$ has either good or multiplicative reduction at all primes p, then $E/\mathbb{Q}$ is modular. As a consequence, Fermat's Last Theorem followed.
- Breuil, Conrad, Diamond and Taylor proved the modularity conjecture for all $E/\mathbb{Q}$. As a consequence, analytic continuation and functional equation of $L(E, s)$ followed for $E/\mathbb{Q}$.
- The analytic continuation and functional equation of $L(E/K, s)$ for any elliptic curve over a general number field K is not yet resolved. For real quadratic and totally real cubic number fields, a modularity result has been obtained by work of Siksek et al which implies analytic continuation for E/K. For elliptic curves with complex multiplication, analytic continuation of $L(E/K, s)$ is known for any number field K.

Consequence of Modularity of $E/\mathbb{Q}$

- Frey conjectured (1982) and Ribet (1986) proved the following.

  If $a^p + b^p = c^p$ for a prime $p > 3$, then the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ will violate the modularity conjecture.

- Wiles (with help of Taylor) showed that if $E/\mathbb{Q}$ has either good or multiplicative reduction at all primes p, then $E/\mathbb{Q}$ is modular. As a consequence, Fermat's Last Theorem followed.

- Breuil, Conrad, Diamond and Taylor proved the modularity conjecture for all $E/\mathbb{Q}$. As a consequence, analytic continuation and functional equation of $L(E, s)$ followed for $E/\mathbb{Q}$.

- The analytic continuation and functional equation of $L(E/K, s)$ for any elliptic curve over a general number field K is not yet resolved. For real quadratic and totally real cubic number fields, a modularity result has been obtained by work of Siksek et al which implies analytic continuation for E/K. For elliptic curves with complex multiplication, analytic continuation of $L(E/K, s)$ is known for any number field K.

Consequence of Modularity of $E/\mathbb{Q}$

- Frey conjectured (1982) and Ribet (1986) proved the following.

  If $a^p + b^p = c^p$ for a prime $p > 3$, then the elliptic curve $y^2 = x(x - a^p)(x + b^p)$ will violate the modularity conjecture.
- Wiles (with help of Taylor) showed that if $E/\mathbb{Q}$ has either good or multiplicative reduction at all primes p, then $E/\mathbb{Q}$ is modular. As a consequence, Fermat's Last Theorem followed.
- Breuil, Conrad, Diamond and Taylor proved the modularity conjecture for all $E/\mathbb{Q}$. As a consequence, analytic continuation and functional equation of $L(E, s)$ followed for $E/\mathbb{Q}$.
- The analytic continuation and functional equation of $L(E/K, s)$ for any elliptic curve over a general number field K is not yet resolved. For real quadratic and totally real cubic number fields, a modularity result has been obtained by work of Siksek et al which implies analytic continuation for E/K. For elliptic curves with complex multiplication, analytic continuation of $L(E/K, s)$ is known for any number field K.

Deuring's Result for Elliptic Curves with CM

- An elliptic curve E over a number field K is said to have complex multiplication (CM) if it has additional endomorphisms apart from multiplication by an integer, i.e., E has CM if $End(E) > \mathbb{Z}$. If E has CM, then $End(E)$ must be an order in an imaginary quadratic field F. For example, the elliptic curve $y^2 = x^3 - n^2x$ has CM by $\mathbb{Z}[i]$, where i acts via $[i](x, y) = (-x, iy)$).

- If E/K has complex multiplication, then one has a Grossencharacter ψ from the idele group of K to $F^\times$, essentially by mapping the uniformizer at a good prime v to the element in F that corresponds to the Frobenius endomorphism at v.

- One can show that

$$L(E/K, s) = L(\psi, s)L(\overline{\psi}, s).$$

The analytic continuation and functional equation for $L(E, s)$ follows from the analogues for $L(\psi, s)$, which has been well-known.

Deuring's Result for Elliptic Curves with CM

- An elliptic curve E over a number field K is said to have complex multiplication (CM) if it has additional endomorphisms apart from multiplication by an integer, i.e., E has CM if $End(E) > \mathbb{Z}$. If E has CM, then $End(E)$ must be an order in an imaginary quadratic field F. For example, the elliptic curve $y^2 = x^3 - n^2 x$ has CM by $\mathbb{Z}[i]$, where i acts via $[i](x, y) = (-x, iy)$).

- If E/K has complex multiplication, then one has a Grossencharacter ψ from the idele group of K to $F^\times$, essentially by mapping the uniformizer at a good prime v to the element in F that corresponds to the Frobenius endomorphism at v.

- One can show that

$$L(E/K, s) = L(\psi, s)L(\overline{\psi}, s).$$

The analytic continuation and functional equation for $L(E, s)$ follows from the analogues for $L(\psi, s)$, which has been well-known.

Deuring's Result for Elliptic Curves with CM

- An elliptic curve E over a number field K is said to have complex multiplication (CM) if it has additional endomorphisms apart from multiplication by an integer, i.e., E has CM if $End(E) > \mathbb{Z}$. If E has CM, then $End(E)$ must be an order in an imaginary quadratic field F. For example, the elliptic curve $y^2 = x^3 - n^2x$ has CM by $\mathbb{Z}[i]$, where i acts via $[i](x, y) = (-x, iy)$).

- If E/K has complex multiplication, then one has a Grossencharacter ψ from the idele group of K to $F^\times$, essentially by mapping the uniformizer at a good prime v to the element in F that corresponds to the Frobenius endomorphism at v.

- One can show that

$$L(E/K, s) = L(\psi, s)L(\overline{\psi}, s).$$

The analytic continuation and functional equation for $L(E, s)$ follows from the analogues for $L(\psi, s)$, which has been well-known.

Deuring's Result for Elliptic Curves with CM

- An elliptic curve E over a number field K is said to have complex multiplication (CM) if it has additional endomorphisms apart from multiplication by an integer, i.e., E has CM if $End(E) > \mathbb{Z}$. If E has CM, then $End(E)$ must be an order in an imaginary quadratic field F. For example, the elliptic curve $y^2 = x^3 - n^2 x$ has CM by $\mathbb{Z}[i]$, where i acts via $[i](x, y) = (-x, iy)$).
- If E/K has complex multiplication, then one has a Grossencharacter ψ from the idele group of K to $F^\times$, essentially by mapping the uniformizer at a good prime v to the element in F that corresponds to the Frobenius endomorphism at v.
- One can show that

$$L(E/K, s) = L(\psi, s)L(\overline{\psi}, s).$$

The analytic continuation and functional equation for $L(E, s)$ follows from the analogues for $L(\psi, s)$, which has been well-known.

Deuring's Result for Elliptic Curves with CM

- An elliptic curve E over a number field K is said to have complex multiplication (CM) if it has additional endomorphisms apart from multiplication by an integer, i.e., E has CM if $End(E) > \mathbb{Z}$. If E has CM, then $End(E)$ must be an order in an imaginary quadratic field F. For example, the elliptic curve $y^2 = x^3 - n^2 x$ has CM by $\mathbb{Z}[i]$, where i acts via $[i](x, y) = (-x, iy)$).
- If E/K has complex multiplication, then one has a Grossencharacter ψ from the idele group of K to $F^\times$, essentially by mapping the uniformizer at a good prime v to the element in F that corresponds to the Frobenius endomorphism at v.
- One can show that

$$L(E/K, s) = L(\psi, s)L(\overline{\psi}, s).$$

The analytic continuation and functional equation for $L(E, s)$ follows from the analogues for $L(\psi, s)$, which has been well-known.

Deuring's Result for Elliptic Curves with CM

- An elliptic curve E over a number field K is said to have complex multiplication (CM) if it has additional endomorphisms apart from multiplication by an integer, i.e., E has CM if $End(E) > \mathbb{Z}$. If E has CM, then $End(E)$ must be an order in an imaginary quadratic field F. For example, the elliptic curve $y^2 = x^3 - n^2x$ has CM by $\mathbb{Z}[i]$, where i acts via $[i](x, y) = (-x, iy)$).
- If E/K has complex multiplication, then one has a Grossencharacter ψ from the idele group of K to $F^\times$, essentially by mapping the uniformizer at a good prime v to the element in F that corresponds to the Frobenius endomorphism at v.
- One can show that

$$L(E/K, s) = L(\psi, s)L(\overline{\psi}, s).$$

The analytic continuation and functional equation for $L(E, s)$ follows from the analogues for $L(\psi, s)$, which has been well-known.

Deuring's Result for Elliptic Curves with CM

- An elliptic curve E over a number field K is said to have complex multiplication (CM) if it has additional endomorphisms apart from multiplication by an integer, i.e., E has CM if $End(E) > \mathbb{Z}$. If E has CM, then $End(E)$ must be an order in an imaginary quadratic field F. For example, the elliptic curve $y^2 = x^3 - n^2 x$ has CM by $\mathbb{Z}[i]$, where i acts via $[i](x, y) = (-x, iy)$).
- If E/K has complex multiplication, then one has a Grossencharacter ψ from the idele group of K to $F^\times$, essentially by mapping the uniformizer at a good prime v to the element in F that corresponds to the Frobenius endomorphism at v.
- One can show that

$$L(E/K, s) = L(\psi, s)L(\overline{\psi}, s).$$

  The analytic continuation and functional equation for $L(E, s)$ follows from the analogues for $L(\psi, s)$, which has been well-known.

Sections

Sections

The Birch and Swinnerton-Dyer Conjecture

- The BSD Conjecture connects the algebraic behaviour of an elliptic curve to its analytic behaviour.
- Roughly speaking, the BSD conjecture predicts that $E(\mathbb{Q})$ is infinite if and only if $L(E,1)=0$. But the BSD conjecture is much more precise than that.
- The first part of the conjecture states that the rank of $E(\mathbb{Q})$ is equal to the order of the vanishing of the $L(E,s)$ at $s=1$.
- It is remarkable to note that when the conjecture first appeared in 1965, it was not even known whether $L(E,s)$ is well-defined at $s=1$. $L(E,s)$ was well-defined only for $Re(s)>\frac{3}{2}$ and its analytic continuation was still a conjecture at that stage.

The Birch and Swinnerton-Dyer Conjecture

- The BSD Conjecture connects the algebraic behaviour of an elliptic curve to its analytic behaviour.
- Roughly speaking, the BSD conjecture predicts that $E(\mathbb{Q})$ is infinite if and only if $L(E,1)=0$. But the BSD conjecture is much more precise than that.
- The first part of the conjecture states that the rank of $E(\mathbb{Q})$ is equal to the order of the vanishing of the $L(E,s)$ at $s=1$.
- It is remarkable to note that when the conjecture first appeared in 1965, it was not even known whether $L(E,s)$ is well-defined at $s=1$. $L(E,s)$ was well-defined only for $Re(s)>\frac{3}{2}$ and its analytic continuation was still a conjecture at that stage.

The Birch and Swinnerton-Dyer Conjecture

- The BSD Conjecture connects the algebraic behaviour of an elliptic curve to its analytic behaviour.
- Roughly speaking, the BSD conjecture predicts that $E(\mathbb{Q})$ is infinite if and only if $L(E, 1) = 0$. But the BSD conjecture is much more precise than that.
- The first part of the conjecture states that the rank of $E(\mathbb{Q})$ is equal to the order of the vanishing of the $L(E, s)$ at $s = 1$.
- It is remarkable to note that when the conjecture first appeared in 1965, it was not even known whether $L(E, s)$ is well-defined at $s = 1$. $L(E, s)$ was well-defined only for $Re(s) > \frac{3}{2}$ and its analytic continuation was still a conjecture at that stage.

The Birch and Swinnerton-Dyer Conjecture

- The BSD Conjecture connects the algebraic behaviour of an elliptic curve to its analytic behaviour.
- Roughly speaking, the BSD conjecture predicts that $E(\mathbb{Q})$ is infinite if and only if $L(E, 1) = 0$. But the BSD conjecture is much more precise than that.
- The first part of the conjecture states that the rank of $E(\mathbb{Q})$ is equal to the order of the vanishing of the $L(E, s)$ at $s = 1$.
- It is remarkable to note that when the conjecture first appeared in 1965, it was not even known whether $L(E, s)$ is well-defined at $s = 1$. $L(E, s)$ was well-defined only for $Re(s) > \frac{3}{2}$ and its analytic continuation was still a conjecture at that stage.

The Birch and Swinnerton-Dyer Conjecture

- The BSD Conjecture connects the algebraic behaviour of an elliptic curve to its analytic behaviour.
- Roughly speaking, the BSD conjecture predicts that $E(\mathbb{Q})$ is infinite if and only if $L(E, 1) = 0$. But the BSD conjecture is much more precise than that.
- The first part of the conjecture states that the rank of $E(\mathbb{Q})$ is equal to the order of the vanishing of the $L(E, s)$ at $s = 1$.
- It is remarkable to note that when the conjecture first appeared in 1965, it was not even known whether $L(E, s)$ is well-defined at $s = 1$. $L(E, s)$ was well-defined only for $Re(s) > \frac{3}{2}$ and its analytic continuation was still a conjecture at that stage.

The Birch and Swinnerton-Dyer Conjecture

- The BSD Conjecture connects the algebraic behaviour of an elliptic curve to its analytic behaviour.
- Roughly speaking, the BSD conjecture predicts that $E(\mathbb{Q})$ is infinite if and only if $L(E, 1) = 0$. But the BSD conjecture is much more precise than that.
- The first part of the conjecture states that the rank of $E(\mathbb{Q})$ is equal to the order of the vanishing of the $L(E, s)$ at $s = 1$.
- It is remarkable to note that when the conjecture first appeared in 1965, it was not even known whether $L(E, s)$ is well-defined at $s = 1$. $L(E, s)$ was well-defined only for $Re(s) > \frac{3}{2}$ and its analytic continuation was still a conjecture at that stage.

The Taylor Series for $L(E, s)$

- As $L(E, s)$ has analytic continuation to all of $\mathbb{C}$ (conjecturally in 1965), it has Taylor series expansion around $s = 1$:

$$L(E, s) = a_k(s-1)^k + a_{k+1}(s-1)^{k+1} + \dots \qquad k \in \mathbb{Z}_{\geq 0}.$$

The *analytic rank* of $E/\mathbb{Q}$ is defined as $r_{an}(E) = k$, in other words it is the order of vanishing of $L(E, s)$ at $s = 1$.

- The first part of the BSD Conjecture predicts that the algebraic rank of $E(\mathbb{Q})$ equals the analytic rank.

The second part of the conjecture relates the first non-zero coefficient a_k of the Taylor series expansion of $L(E, s)$ explicitly to arithmetic invariants associated with E.

The Taylor Series for $L(E, s)$

- As $L(E, s)$ has analytic continuation to all of $\mathbb{C}$ (conjecturally in 1965), it has Taylor series expansion around $s = 1$:

$$L(E, s) = a_k(s-1)^k + a_{k+1}(s-1)^{k+1} + \ldots \qquad k \in \mathbb{Z}_{\geq 0}.$$

The *analytic rank* of $E/\mathbb{Q}$ is defined as $r_{an}(E) = k$, in other words it is the order of vanishing of $L(E, s)$ at $s = 1$.

- The first part of the BSD Conjecture predicts that the algebraic rank of $E(\mathbb{Q})$ equals the analytic rank.

The second part of the conjecture relates the first non-zero coefficient a_k of the Taylor series expansion of $L(E, s)$ explicitly to arithmetic invariants associated with E.

The Taylor Series for $L(E, s)$

- As $L(E, s)$ has analytic continuation to all of $\mathbb{C}$ (conjecturally in 1965), it has Taylor series expansion around $s = 1$:

  $$L(E, s) = a_k(s-1)^k + a_{k+1}(s-1)^{k+1} + \ldots \qquad k \in \mathbb{Z}_{\geq 0}.$$

  The *analytic rank* of $E/\mathbb{Q}$ is defined as $r_{an}(E) = k$, in other words it is the order of vanishing of $L(E, s)$ at $s = 1$.

- The first part of the BSD Conjecture predicts that the algebraic rank of $E(\mathbb{Q})$ equals the analytic rank.

  The second part of the conjecture relates the first non-zero coefficient a_k of the Taylor series expansion of $L(E, s)$ explicitly to arithmetic invariants associated with E.

The Taylor Series for $L(E, s)$

L-functions

The Hasse-Weil L-function of an Elliptic Curve

The BSD Conjecture

- As $L(E, s)$ has analytic continuation to all of $\mathbb{C}$ (conjecturally in 1965), it has Taylor series expansion around $s = 1$:

$$L(E, s) = a_k(s-1)^k + a_{k+1}(s-1)^{k+1} + \ldots \qquad k \in \mathbb{Z}_{\geq 0}.$$

The *analytic rank* of $E/\mathbb{Q}$ is defined as $r_{an}(E) = k$, in other words it is the order of vanishing of $L(E, s)$ at $s = 1$.

- The first part of the BSD Conjecture predicts that the algebraic rank of $E(\mathbb{Q})$ equals the analytic rank.

The second part of the conjecture relates the first non-zero coefficient a_k of the Taylor series expansion of $L(E, s)$ explicitly to arithmetic invariants associated with E.

The Taylor Series for $L(E, s)$

- As $L(E, s)$ has analytic continuation to all of $\mathbb{C}$ (conjecturally in 1965), it has Taylor series expansion around $s = 1$:

$$L(E,s) = a_k(s-1)^k \; + \; a_{k+1}(s-1)^{k+1} \; + \; \dots \qquad k \in \mathbb{Z}_{\geq 0}.$$

  The *analytic rank* of $E/\mathbb{Q}$ is defined as $r_{an}(E) = k$, in other words it is the order of vanishing of $L(E, s)$ at $s = 1$.

- The first part of the BSD Conjecture predicts that the algebraic rank of $E(\mathbb{Q})$ equals the analytic rank.

  The second part of the conjecture relates the first non-zero coefficient a_k of the Taylor series expansion of $L(E, s)$ explicitly to arithmetic invariants associated with E.

The Taylor Series for $L(E, s)$

- As $L(E, s)$ has analytic continuation to all of $\mathbb{C}$ (conjecturally in 1965), it has Taylor series expansion around $s = 1$:

  $$L(E, s) = a_k(s-1)^k + a_{k+1}(s-1)^{k+1} + \ldots \qquad k \in \mathbb{Z}_{\geq 0}.$$

  The *analytic rank* of $E/\mathbb{Q}$ is defined as $r_{an}(E) = k$, in other words it is the order of vanishing of $L(E, s)$ at $s = 1$.

- The first part of the BSD Conjecture predicts that the algebraic rank of $E(\mathbb{Q})$ equals the analytic rank.

  The second part of the conjecture relates the first non-zero coefficient a_k of the Taylor series expansion of $L(E, s)$ explicitly to arithmetic invariants associated with E.

The Taylor Series for $L(E, s)$

- As $L(E, s)$ has analytic continuation to all of $\mathbb{C}$ (conjecturally in 1965), it has Taylor series expansion around $s = 1$:

$$L(E, s) = a_k(s-1)^k + a_{k+1}(s-1)^{k+1} + \dots \qquad k \in \mathbb{Z}_{\geq 0}.$$

  The *analytic rank* of $E/\mathbb{Q}$ is defined as $r_{an}(E) = k$, in other words it is the order of vanishing of $L(E, s)$ at $s = 1$.

- The first part of the BSD Conjecture predicts that the algebraic rank of $E(\mathbb{Q})$ equals the analytic rank.

  The second part of the conjecture relates the first non-zero coefficient a_k of the Taylor series expansion of $L(E, s)$ explicitly to arithmetic invariants associated with E.

A Heuristic Argument

- If we put $s = 1$ in the Euler product for $L(E, s)$,

$$L(E,1) = \prod_p \frac{1}{1 - a_p p^{-1} + p^{-1}} = \prod_p \frac{p}{p + 1 - a_p} = \prod_p \frac{p}{\#\tilde{E}_{ns}(\mathbb{F}_p)}.$$

- If p is a good prime, $|\, p + 1 - \#\tilde{E}(\mathbb{F}_p) \,| = |\, a_p \,| \leq \; 2\sqrt{p}$.

$$\therefore p + 1 - 2\sqrt{p} \;\leq\; \#\tilde{E}(\mathbb{F}_p) \;\leq\; p + 1 + 2\sqrt{p}.$$

- If $E(\mathbb{Q})$ is infinite, $\#\tilde{E}(\mathbb{F}_p)$ should be closer to $p + 1 + 2\sqrt{p}$ than to $p + 1 - 2\sqrt{p}$ for most of good primes p.
- Then, the infinite product $\prod_p \frac{p}{(p+2\sqrt{p})}$ can be expected to be 0.
- Conversely, if $L(E, 1) = 0$, then the terms in the infinite product should have large denominator, i.e., $\tilde{E}(\mathbb{F}_p)$ should be large for most good primes p. Therefore $E(\mathbb{Q})$ should be very large too. ('Hasse principle', or 'local to global principle').

A Heuristic Argument

- If we put $s = 1$ in the Euler product for $L(E, s)$,

$$L(E,1) = \prod_p \frac{1}{1 - a_p p^{-1} + p^{-1}} = \prod_p \frac{p}{p+1-a_p} = \prod_p \frac{p}{\#\tilde{E}_{ns}(\mathbb{F}_p)}.$$

- If p is a good prime, $|\, p + 1 - \#\tilde{E}(\mathbb{F}_p)\, | = |\, a_p \,| \le 2\sqrt{p}$.

$$\therefore p + 1 - 2\sqrt{p} \le \#\tilde{E}(\mathbb{F}_p) \le p + 1 + 2\sqrt{p}.$$

- If $E(\mathbb{Q})$ is infinite, $\#\tilde{E}(\mathbb{F}_p)$ should be closer to $p + 1 + 2\sqrt{p}$ than to $p + 1 - 2\sqrt{p}$ for most of good primes p.
- Then, the infinite product $\prod_p \frac{p}{(p+2\sqrt{p})}$ can be expected to be 0.
- Conversely, if $L(E, 1) = 0$, then the terms in the infinite product should have large denominator, i.e., $\tilde{E}(\mathbb{F}_p)$ should be large for most good primes p. Therefore $E(\mathbb{Q})$ should be very large too. ('Hasse principle', or 'local to global principle').

A Heuristic Argument

- If we put $s = 1$ in the Euler product for $L(E, s)$,

$$L(E,1) = \prod_p \frac{1}{1 - a_p p^{-1} + p^{-1}} = \prod_p \frac{p}{p+1-a_p} = \prod_p \frac{p}{\#\tilde{E}_{ns}(\mathbb{F}_p)}.$$

- If p is a good prime, $|\, p + 1 - \#\tilde{E}(\mathbb{F}_p) \,| = |\, a_p \,| \leq 2\sqrt{p}$.

$$\therefore p + 1 - 2\sqrt{p} \leq \#\tilde{E}(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

- If $E(\mathbb{Q})$ is infinite, $\#\tilde{E}(\mathbb{F}_p)$ should be closer to $p + 1 + 2\sqrt{p}$ than to $p + 1 - 2\sqrt{p}$ for most of good primes p.
- Then, the infinite product $\prod_p \frac{p}{(p+2\sqrt{p})}$ can be expected to be 0.
- Conversely, if $L(E, 1) = 0$, then the terms in the infinite product should have large denominator, i.e., $\tilde{E}(\mathbb{F}_p)$ should be large for most good primes p. Therefore $E(\mathbb{Q})$ should be very large too. ('Hasse principle', or 'local to global principle').

A Heuristic Argument

- If we put $s = 1$ in the Euler product for $L(E, s)$,

$$L(E,1) = \prod_p \frac{1}{1 - a_p p^{-1} + p^{-1}} = \prod_p \frac{p}{p + 1 - a_p} = \prod_p \frac{p}{\#\tilde{E}_{ns}(\mathbb{F}_p)}.$$

- If p is a good prime, $|\ p + 1 - \#\tilde{E}(\mathbb{F}_p)\ | = |\ a_p\ | \leq\ 2\sqrt{p}$.

$$\therefore p + 1 - 2\sqrt{p}\ \leq\ \#\tilde{E}(\mathbb{F}_p)\ \leq\ p + 1 + 2\sqrt{p}.$$

- If $E(\mathbb{Q})$ is infinite, $\#\tilde{E}(\mathbb{F}_p)$ should be closer to $p + 1 + 2\sqrt{p}$ than to $p + 1 - 2\sqrt{p}$ for most of good primes p.
- Then, the infinite product $\prod_p \frac{p}{(p+2\sqrt{p})}$ can be expected to be 0.
- Conversely, if $L(E, 1) = 0$, then the terms in the infinite product should have large denominator, i.e., $\tilde{E}(\mathbb{F}_p)$ should be large for most good primes p. Therefore $E(\mathbb{Q})$ should be very large too. ('Hasse principle', or 'local to global principle').

A Heuristic Argument

- If we put $s = 1$ in the Euler product for $L(E, s)$,

$$L(E,1) = \prod_p \frac{1}{1 - a_p p^{-1} + p^{-1}} = \prod_p \frac{p}{p + 1 - a_p} = \prod_p \frac{p}{\#\tilde{E}_{ns}(\mathbb{F}_p)}.$$

- If p is a good prime, $|\ p + 1 - \#\tilde{E}(\mathbb{F}_p)\ | = |\ a_p\ | \leq\ 2\sqrt{p}$.

$$\therefore p + 1 - 2\sqrt{p}\ \leq\ \#\tilde{E}(\mathbb{F}_p)\ \leq\ p + 1 + 2\sqrt{p}.$$

- If $E(\mathbb{Q})$ is infinite, $\#\tilde{E}(\mathbb{F}_p)$ should be closer to $p + 1 + 2\sqrt{p}$ than to $p + 1 - 2\sqrt{p}$ for most of good primes p.
- Then, the infinite product $\prod_p \frac{p}{(p+2\sqrt{p})}$ can be expected to be 0.
- Conversely, if $L(E, 1) = 0$, then the terms in the infinite product should have large denominator, i.e., $\tilde{E}(\mathbb{F}_p)$ should be large for most good primes p. Therefore $E(\mathbb{Q})$ should be very large too. ('Hasse principle', or 'local to global principle').

A Heuristic Argument

- If we put $s = 1$ in the Euler product for $L(E, s)$,

$$L(E,1) = \prod_p \frac{1}{1 - a_p p^{-1} + p^{-1}} = \prod_p \frac{p}{p + 1 - a_p} = \prod_p \frac{p}{\#\tilde{E}_{ns}(\mathbb{F}_p)}.$$

- If p is a good prime, $|\, p + 1 - \#\tilde{E}(\mathbb{F}_p) \,| = |\, a_p \,| \leq 2\sqrt{p}$.

$$\therefore p + 1 - 2\sqrt{p} \leq \#\tilde{E}(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

- If $E(\mathbb{Q})$ is infinite, $\#\tilde{E}(\mathbb{F}_p)$ should be closer to $p + 1 + 2\sqrt{p}$ than to $p + 1 - 2\sqrt{p}$ for most of good primes p.
- Then, the infinite product $\prod_p \frac{p}{(p+2\sqrt{p})}$ can be expected to be 0.
- Conversely, if $L(E, 1) = 0$, then the terms in the infinite product should have large denominator, i.e., $\tilde{E}(\mathbb{F}_p)$ should be large for most good primes p. Therefore $E(\mathbb{Q})$ should be very large too. ('Hasse principle', or 'local to global principle').

The Second Part of the Conjecture

- The second part of the BSD Conjecture predicts that the first non-vanishing coefficient of the Taylor series for $L(E, s)$ can be expressed as

$$\lim_{s \to 1} \frac{L(E,s)}{(s-1)^k} = \frac{\#(\text{Ш}(E) \Omega_E R_E \prod_p c_p}{(\#E(\mathbb{Q})_{tor})^2}.$$

- Ω_E is called the real period of E. It is the value of an integral of the invariant differential associated with E ($\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y+a_1x+a_3}$).

- The c_ps are known as the local Tamagawa numbers. For each prime p, c_p is defined as

$$c_p = \# \frac{E(\mathbb{Q}_p)}{E_0(\mathbb{Q}_p)},$$

where $E_0(\mathbb{Q}_p)$ denotes the set of points of non-singular reduction on $E(\mathbb{Q}_p)$. Here $\mathbb{Q}_p$ denotes the p-adic completion of $\mathbb{Q}$. Note that $c_p \neq 1$ only at the finitely many bad primes.

The Second Part of the Conjecture

- The second part of the BSD Conjecture predicts that the first non-vanishing coefficient of the Taylor series for $L(E, s)$ can be expressed as

$$\lim_{s \to 1} \frac{L(E,s)}{(s-1)^k} = \frac{\#(Ш(E)\Omega_E R_E \prod_p c_p}{(\#E(\mathbb{Q})_{tor})^2}.$$

- Ω_E is called the real period of E. It is the value of an integral of the invariant differential associated with E ($\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y+a_1x+a_3}$).

- The c_ps are known as the local Tamagawa numbers. For each prime p, c_p is defined as

$$c_p = \# \frac{E(\mathbb{Q}_p)}{E_0(\mathbb{Q}_p)},$$

where $E_0(\mathbb{Q}_p)$ denotes the set of points of non-singular reduction on $E(\mathbb{Q}_p)$. Here $\mathbb{Q}_p$ denotes the p-adic completion of $\mathbb{Q}$. Note that $c_p \neq 1$ only at the finitely many bad primes.

The Second Part of the Conjecture

- The second part of the BSD Conjecture predicts that the first non-vanishing coefficient of the Taylor series for $L(E,s)$ can be expressed as

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^k} = \frac{\#(Ш(E)\Omega_E R_E \prod_p c_p}{(\#E(\mathbb{Q})_{tor})^2}.$$

- Ω_E is called the real period of E. It is the value of an integral of the invariant differential associated with E $(\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y+a_1x+a_3})$.

- The c_ps are known as the local Tamagawa numbers. For each prime p, c_p is defined as

$$c_p = \#\frac{E(\mathbb{Q}_p)}{E_0(\mathbb{Q}_p)},$$

where $E_0(\mathbb{Q}_p)$ denotes the set of points of non-singular reduction on $E(\mathbb{Q}_p)$. Here $\mathbb{Q}_p$ denotes the p-adic completion of $\mathbb{Q}$. Note that $c_p \neq 1$ only at the finitely many bad primes.

The Second Part of the Conjecture

- The second part of the BSD Conjecture predicts that the first non-vanishing coefficient of the Taylor series for $L(E,s)$ can be expressed as

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^k}=\frac{\#(Ш(E)\Omega_E R_E\prod_p c_p}{(\#E(\mathbb{Q})_{tor})^2}.$$

- Ω_E is called the real period of E. It is the value of an integral of the invariant differential associated with E ($\Omega_E=\int_{E(\mathbb{R})}\frac{dx}{2y+a_1x+a_3}$).

- The c_ps are known as the local Tamagawa numbers. For each prime p, c_p is defined as

$$c_p=\#\frac{E(\mathbb{Q}_p)}{E_0(\mathbb{Q}_p)},$$

where $E_0(\mathbb{Q}_p)$ denotes the set of points of non-singular reduction on $E(\mathbb{Q}_p)$. Here $\mathbb{Q}_p$ denotes the p-adic completion of $\mathbb{Q}$. Note that $c_p\neq 1$ only at the finitely many bad primes.

The Second Part of the Conjecture

- The second part of the BSD Conjecture predicts that the first non-vanishing coefficient of the Taylor series for $L(E,s)$ can be expressed as

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^k}=\frac{\#(Ш(E)\Omega_E R_E\prod_p c_p}{(\#E(\mathbb{Q})_{tor})^2}.$$

- Ω_E is called the real period of E. It is the value of an integral of the invariant differential associated with E ($\Omega_E=\int_{E(\mathbb{R})}\frac{dx}{2y+a_1x+a_3}$).
- The c_ps are known as the local Tamagawa numbers. For each prime p, c_p is defined as

$$c_p=\#\frac{E(\mathbb{Q}_p)}{E_0(\mathbb{Q}_p)},$$

where $E_0(\mathbb{Q}_p)$ denotes the set of points of non-singular reduction on $E(\mathbb{Q}_p)$. Here $\mathbb{Q}_p$ denotes the p-adic completion of $\mathbb{Q}$. Note that $c_p\neq 1$ only at the finitely many bad primes.

The Second Part of the Conjecture

- The second part of the BSD Conjecture predicts that the first non-vanishing coefficient of the Taylor series for $L(E, s)$ can be expressed as

$$\lim_{s \to 1} \frac{L(E, s)}{(s-1)^k} = \frac{\#(\text{Ш}(E)\Omega_E R_E \prod_p c_p}{(\#E(\mathbb{Q})_{tor})^2}.$$

- Ω_E is called the real period of E. It is the value of an integral of the invariant differential associated with E ($\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y+a_1x+a_3}$).

- The c_ps are known as the local Tamagawa numbers. For each prime p, c_p is defined as

$$c_p = \#\frac{E(\mathbb{Q}_p)}{E_0(\mathbb{Q}_p)},$$

where $E_0(\mathbb{Q}_p)$ denotes the set of points of non-singular reduction on $E(\mathbb{Q}_p)$. Here $\mathbb{Q}_p$ denotes the p-adic completion of $\mathbb{Q}$. Note that $c_p \neq 1$ only at the finitely many bad primes.

The Second Part of the Conjecture

- The second part of the BSD Conjecture predicts that the first non-vanishing coefficient of the Taylor series for $L(E, s)$ can be expressed as

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^k} = \frac{\#(Ш(E)\Omega_E R_E \prod_p c_p}{(\#E(\mathbb{Q})_{tor})^2}.$$

- Ω_E is called the real period of E. It is the value of an integral of the invariant differential associated with E ($\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y+a_1x+a_3}$).

- The c_ps are known as the local Tamagawa numbers. For each prime p, c_p is defined as

$$c_p = \# \frac{E(\mathbb{Q}_p)}{E_0(\mathbb{Q}_p)},$$

where $E_0(\mathbb{Q}_p)$ denotes the set of points of non-singular reduction on $E(\mathbb{Q}_p)$. Here $\mathbb{Q}_p$ denotes the p-adic completion of $\mathbb{Q}$. Note that $c_p \neq 1$ only at the finitely many bad primes.

The Second Part of the Conjecture

- The second part of the BSD Conjecture predicts that the first non-vanishing coefficient of the Taylor series for $L(E,s)$ can be expressed as

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^k}=\frac{\#(\text{Ш}(E)\Omega_E R_E\prod_p c_p}{(\#E(\mathbb{Q})_{tor})^2}.$$

- Ω_E is called the real period of E. It is the value of an integral of the invariant differential associated with E ($\Omega_E=\int_{E(\mathbb{R})}\frac{dx}{2y+a_1x+a_3}$).

- The c_ps are known as the local Tamagawa numbers. For each prime p, c_p is defined as

$$c_p=\#\frac{E(\mathbb{Q}_p)}{E_0(\mathbb{Q}_p)},$$

where $E_0(\mathbb{Q}_p)$ denotes the set of points of non-singular reduction on $E(\mathbb{Q}_p)$. Here $\mathbb{Q}_p$ denotes the p-adic completion of $\mathbb{Q}$. Note that $c_p\neq 1$ only at the finitely many bad primes.

The Regulator and the Shafarevich-Tate Group

- R_E is the regulator of the elliptic curve.
- Here, $Ш(E/\mathbb{Q})$ is the mysterious Shafarevich-Tate group which is not yet proven to be finite.
- Roughly speaking, the Shafarevich-Tate group measures the failure of ‘local-to-global principle’ for curves isomorphic to E over $\mathbb{C}$.
- Showing the finiteness of the Shafarevich-Tate group itself is a very hard problem.
- Cassels has shown that if $Ш(E/\mathbb{Q})$ is finite, then its order must be a perfect square.

The Regulator and the Shafarevich-Tate Group

- R_E is the regulator of the elliptic curve.
- Here, $Ш(E/\mathbb{Q})$ is the mysterious Shafarevich-Tate group which is not yet proven to be finite.
- Roughly speaking, the Shafarevich-Tate group measures the failure of 'local-to-global principle' for curves isomorphic to E over $\mathbb{C}$.
- Showing the finiteness of the Shafarevich-Tate group itself is a very hard problem.
- Cassels has shown that if $Ш(E/\mathbb{Q})$ is finite, then its order must be a perfect square.

The Regulator and the Shafarevich-Tate Group

- R_E is the regulator of the elliptic curve.
- Here, $Ш(E/\mathbb{Q})$ is the mysterious Shafarevich-Tate group which is not yet proven to be finite.
- Roughly speaking, the Shafarevich-Tate group measures the failure of 'local-to-global principle' for curves isomorphic to E over $\mathbb{C}$.
- Showing the finiteness of the Shafarevich-Tate group itself is a very hard problem.
- Cassels has shown that if $Ш(E/\mathbb{Q})$ is finite, then its order must be a perfect square.

The Regulator and the Shafarevich-Tate Group

- R_E is the regulator of the elliptic curve.
- Here, $Ш(E/\mathbb{Q})$ is the mysterious Shafarevich-Tate group which is not yet proven to be finite.
- Roughly speaking, the Shafarevich-Tate group measures the failure of ‘local-to-global principle’ for curves isomorphic to E over $\mathbb{C}$.
- Showing the finiteness of the Shafarevich-Tate group itself is a very hard problem.
- Cassels has shown that if $Ш(E/\mathbb{Q})$ is finite, then its order must be a perfect square.

The Regulator and the Shafarevich-Tate Group

- R_E is the regulator of the elliptic curve.
- Here, $Ш(E/\mathbb{Q})$ is the mysterious Shafarevich-Tate group which is not yet proven to be finite.
- Roughly speaking, the Shafarevich-Tate group measures the failure of 'local-to-global principle' for curves isomorphic to E over $\mathbb{C}$.
- Showing the finiteness of the Shafarevich-Tate group itself is a very hard problem.
- Cassels has shown that if $Ш(E/\mathbb{Q})$ is finite, then its order must be a perfect square.

Progress on the BSD Conjecture

- Coates-Wiles (1977): Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. If $E(\mathbb{Q})$ is infinite, then $L(E,1)=0$.

  They showed that if there is a point of infinite order in $E(\mathbb{Q})$, then there are infinitely many prime ideals in K which divide $L(E,1)$ (after factoring out a suitable transcendental element).

- Gross-Zagier (1986): If $L(E,1)=0$ then there exists a point $P\in E(\mathbb{Q})$ such that $L'(E,1)=\alpha\Omega_E\langle P,P\rangle$, where α is a non-zero rational number. In particular, $ord_{s=1}L(E,s)=1 \implies r_E(\mathbb{Q})\geq 1$. Here, the pairing is given by

$$\langle\ ,\ \rangle : E(\overline{\mathbb{Q}})\times E(\overline{\mathbb{Q}})\longrightarrow \mathbb{R}$$

$$\langle P,Q\rangle=\frac{1}{2}\Big[\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q)\Big].$$

  (See Theorem 5 in the article by Coates in the reference for more details)

Progress on the BSD Conjecture

- Coates-Wiles (1977): Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. If $E(\mathbb{Q})$ is infinite, then $L(E,1)=0$.

  They showed that if there is a point of infinite order in $E(\mathbb{Q})$, then there are infinitely many prime ideals in K which divide $L(E,1)$ (after factoring out a suitable transcendental element).

- Gross-Zagier (1986): If $L(E,1)=0$ then there exists a point $P\in E(\mathbb{Q})$ such that $L'(E,1)=\alpha\Omega_E\langle P,P\rangle$, where α is a non-zero rational number. In particular, $ord_{s=1}L(E,s)=1 \implies r_E(\mathbb{Q})\geq 1$. Here, the pairing is given by

$$\langle\ ,\ \rangle\ :\ E(\overline{\mathbb{Q}})\times E(\overline{\mathbb{Q}})\longrightarrow\mathbb{R}$$

$$\langle P,Q\rangle=\frac{1}{2}\Big[\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q)\Big].$$

  (See Theorem 5 in the article by Coates in the reference for more details)

Progress on the BSD Conjecture

- Coates-Wiles (1977): Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. If $E(\mathbb{Q})$ is infinite, then $L(E,1) = 0$.

  They showed that if there is a point of infinite order in $E(\mathbb{Q})$, then there are infinitely many prime ideals in K which divide $L(E,1)$ (after factoring out a suitable transcendental element).

- Gross-Zagier (1986): If $L(E,1) = 0$ then there exists a point $P \in E(\mathbb{Q})$ such that $L'(E,1) = \alpha \Omega_E \langle P, P \rangle$, where α is a non-zero rational number. In particular, $ord_{s=1} L(E,s) = 1 \implies r_E(\mathbb{Q}) \geq 1$. Here, the pairing is given by

$$\langle\ ,\ \rangle : E(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R}$$

$$\langle P, Q \rangle = \frac{1}{2}\left[\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right].$$

  (See Theorem 5 in the article by Coates in the reference for more details)

Progress on the BSD Conjecture

- Coates-Wiles (1977): Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. If $E(\mathbb{Q})$ is infinite, then $L(E, 1) = 0$.

  They showed that if there is a point of infinite order in $E(\mathbb{Q})$, then there are infinitely many prime ideals in K which divide $L(E, 1)$ (after factoring out a suitable transcendental element).

- Gross-Zagier (1986): If $L(E, 1) = 0$ then there exists a point $P \in E(\mathbb{Q})$ such that $L'(E, 1) = \alpha \Omega_E \langle P, P \rangle$, where α is a non-zero rational number. In particular, $ord_{s=1} L(E, s) = 1 \implies r_E(\mathbb{Q}) \geq 1$.
  Here, the pairing is given by

$$\langle \ , \ \rangle : E(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R}$$

$$\langle P, Q \rangle = \frac{1}{2} \Big[\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q) \Big].$$

  (See Theorem 5 in the article by Coates in the reference for more details)

Progress on the BSD Conjecture

- Coates-Wiles (1977): Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. If $E(\mathbb{Q})$ is infinite, then $L(E,1) = 0$.

  They showed that if there is a point of infinite order in $E(\mathbb{Q})$, then there are infinitely many prime ideals in K which divide $L(E,1)$ (after factoring out a suitable transcendental element).

- Gross-Zagier (1986): If $L(E,1) = 0$ then there exists a point $P \in E(\mathbb{Q})$ such that $L'(E,1) = \alpha \Omega_E \langle P, P \rangle$, where α is a non-zero rational number. In particular, $ord_{s=1} L(E,s) = 1 \implies r_E(\mathbb{Q}) \geq 1$. Here, the pairing is given by

$$\langle \ , \ \rangle \ : \ E(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R}$$

$$\langle P, Q \rangle = \frac{1}{2} \Big[\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \Big].$$

  (See Theorem 5 in the article by Coates in the reference for more details)

Progress on the BSD Conjecture

- Kolyvagin (1989) together with work of Gross-Zagier: For any elliptic curve $E/\mathbb{Q}$,

  $$r_{an}(E) := ord_{s=1} L(E,s) \leq 1 \implies r_E(\mathbb{Q}) = r_{an}(E).$$

  and $\text{Ш}(E/\mathbb{Q})$ is finite.

- Bhargava et al: Nearly 66 % of elliptic curves over $\mathbb{Q}$ satisfy the BSD Conjecture.

- Parity Conjecture: $ord_{s=1} L(E,s) \equiv r_E(\mathbb{Q})$ (mod 2).

Progress on the BSD Conjecture

- Kolyvagin (1989) together with work of Gross-Zagier: For any elliptic curve $E/\mathbb{Q}$,

$$r_{an}(E) := ord_{s=1} L(E, s) \leq 1 \implies r_E(\mathbb{Q}) = r_{an}(E).$$

and $Ш(E/\mathbb{Q})$ is finite.

- Bhargava et al: Nearly 66 % of elliptic curves over $\mathbb{Q}$ satisfy the BSD Conjecture.

- Parity Conjecture: $ord_{s=1} L(E, s) \equiv r_E(\mathbb{Q}) \pmod 2$.

Progress on the BSD Conjecture

- Kolyvagin (1989) together with work of Gross-Zagier: For any elliptic curve $E/\mathbb{Q}$,

  $$r_{an}(E) := ord_{s=1}L(E,s) \leq 1 \implies r_E(\mathbb{Q}) = r_{an}(E).$$

  and $\text{Ш}(E/\mathbb{Q})$ is finite.

- Bhargava et al: Nearly 66 % of elliptic curves over $\mathbb{Q}$ satisfy the BSD Conjecture.

- Parity Conjecture: $ord_{s=1}L(E,s) \equiv r_E(\mathbb{Q})$ (mod 2).

Progress on the BSD Conjecture

- Kolyvagin (1989) together with work of Gross-Zagier: For any elliptic curve $E/\mathbb{Q}$,

  $$r_{an}(E) := ord_{s=1}L(E,s) \leq 1 \implies r_E(\mathbb{Q}) = r_{an}(E).$$

  and $\text{Ш}(E/\mathbb{Q})$ is finite.

- Bhargava et al: Nearly 66 % of elliptic curves over $\mathbb{Q}$ satisfy the BSD Conjecture.

- Parity Conjecture: $ord_{s=1}L(E,s) \equiv r_E(\mathbb{Q}) \pmod 2$.

Progress on the BSD Conjecture

- Kolyvagin (1989) together with work of Gross-Zagier: For any elliptic curve $E/\mathbb{Q}$,

  $$r_{an}(E) := ord_{s=1}L(E, s) \leq 1 \implies r_E(\mathbb{Q}) = r_{an}(E).$$

  and $Ш(E/\mathbb{Q})$ is finite.

- Bhargava et al: Nearly 66 % of elliptic curves over $\mathbb{Q}$ satisfy the BSD Conjecture.

- Parity Conjecture: $ord_{s=1}L(E, s) \equiv r_E(\mathbb{Q}) \pmod{2}$.

Additional References

- *Notes on elliptic curves II.*, B. Birch and P. Swinnerton-Dyer, Crelle 218 (1965) 79–108.
- *The Work of Gross and Zagier on Heegner points and the derivative of L-Series*, J. Coates, Asterisque No. 133-134 (1986), 5772.
- *Elliptic Curves*, D. Husemoller, Graduate Text in Mathematics, Springer, 2004.
- *Elliptic Curves*, J. S. Milne.

THANK YOU