Introduction to modular forms and elliptic curves

Kenny Li

University of Toronto

5th July 2023

Table of Contents

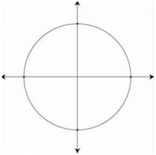
UNIVERSITY OF TORONTO

Definition of Curve

Definition

- In differential geometry, a curve is image of continuously differentiable function $\gamma : [a, b] \to X$ where X is manifold
- **In algebraic geometry, a curve is a zero set of a polynomial of two variables f(x,y)**

- Example: the unit circle $x^2 + y^2 = 1$ can be viewed as $f(x, y) = x^2 + y^2 - 1 = 0$

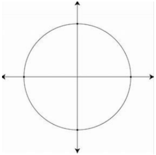


Definition of Curve

Definition

- In differential geometry, a curve is image of continuously differentiable function $\gamma : [a, b] \to X$ where X is manifold
- **In algebraic geometry, a curve is a zero set of a polynomial of two variables f(x,y)**

- Example: the unit circle $x^2 + y^2 = 1$ can be viewed as $f(x, y) = x^2 + y^2 - 1 = 0$



- Remark: Algebraic curve and analytic curve are both rigid while topological curve and differentiable curve are floppy.

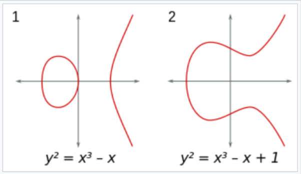
Elliptic curve

Definition

Elliptic curve is a **smooth projective algebraic curve of genus one** with a distinguished point O

In most of the field (e.g. $\mathbb{R}$ or $\mathbb{C}$), the elliptic curves are described by the equation

$$y^2 = x^3 + ax + b$$

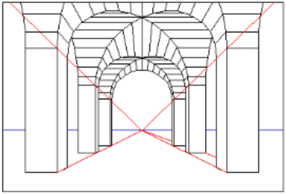


Graphs of curves $y^2 = x^3 - x$ and $y^2 = x^3 - x + 1$

However, these graph just shows part of the elliptic curve

Projective space

- The idea of projective space is to describe the geometry in graphical perspective. To define a projective plane (2D space) , we need a 3D space.

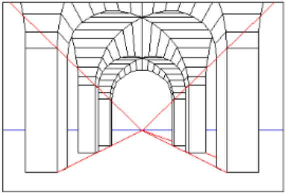


Single point perspective projection.

The vanishing point is called **point at infinity**.

Projective space

- The idea of projective space is to describe the geometry in graphical perspective. To define a projective plane (2D space) , we need a 3D space.



Single point perspective projection.

The vanishing point is called **point at infinity**.

- Mathematically, it is done by taking $p_1 \sim p_2$ if $\exists\lambda \in F, p_2 = \lambda p_1$ that is to consider $p_1 = (x_1, y_1)$ and $\lambda p_1 = (\lambda x_1, \lambda y_1)$ are the very same point

Projective curve

- To define a curve on projective plane, we want to check that p_1 lies on curve if and only if λp_1 lies on the same curve.

Projective curve

- To define a curve on projective plane, we want to check that p_1 lies on curve if and only if λp_1 lies on the same curve.
- Unfortunately, this is **NOT** the case of $y^2 = x^3 + ax + b$.

Projective curve

- To define a curve on projective plane, we want to check that p_1 lies on curve if and only if λp_1 lies on the same curve.
- Unfortunately, this is **NOT** the case of $y^2 = x^3 + ax + b$.
- That is

$$y_1^2 - x_1^3 - ax_1 - b = 0$$

does not implies

$$\lambda^2 y_1^2 - \lambda^3 x_1^3 - \lambda ax_1 - b = 0$$

Projective curve

- To define a curve on projective plane, we want to check that p_1 lies on curve if and only if λp_1 lies on the same curve.
- Unfortunately, this is **NOT** the case of $y^2 = x^3 + ax + b$.
- That is

$$y_1^2 - x_1^3 - ax_1 - b = 0$$

  does not implies

$$\lambda^2 y_1^2 - \lambda^3 x_1^3 - \lambda a x_1 - b = 0$$

- To fix it, we have to consider the **homogeneous** polynomial.
  For $y^2 z = x^3 + axz^2 + bz^3$, the point $P = (x, y, 1)$ correspond to the points $p = (\frac{x}{z}, \frac{y}{z}) = (x, y)$
  Then the point at infinity is just $O = (0, 1, 0)$

Recall

Definition

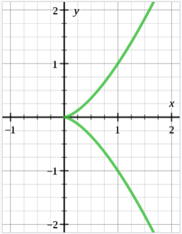
Elliptic curve is a **smooth** projective algebraic curve of **genus one** with a distinguished point O

Smooth curve

- In geometry, smooth means non-singular at everywhere, which means no **cusps** and no **self-intersections** .

Smooth curve

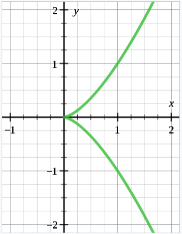
- In geometry, smooth means non-singular at everywhere, which means no **cusps** and no **self-intersections** .
- For algebraic curve described by $f(x, y) = 0$ is non-singular if $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are **not both zero** at that point.
  Example: the curve $y^2 = x^3$ has cusp at 0



A cusp in the semicubical parabola $y^2 = x^3$

Smooth curve

- In geometry, smooth means non-singular at everywhere, which means no **cusps** and no **self-intersections** .
- For algebraic curve described by $f(x, y) = 0$ is non-singular if $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are **not both zero** at that point.
  Example: the curve $y^2 = x^3$ has cusp at 0



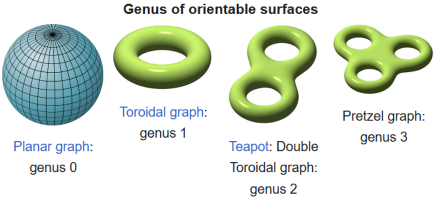
A cusp in the semicubical parabola $y^2 = x^3$

- For elliptic curve $y^2 = x^3 + ax + b$, it is the equivalent to

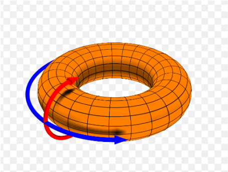
$$\Delta = -16(4a^3 + 27b^2) \neq 0$$

Torus

What do we mean by **genus one**? Intuitively, genus is the number of holes.
Example: **a torus has genus one**.



In fact, an elliptic curve over complex number is a torus.
But then how does elliptic curve be related to ellipse?



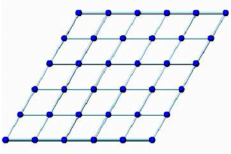
UNIVERSITY OF TORONTO

Complex torus

Definition

A **complex torus** is the set $\mathbb{C}/L$ where $L = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$ is a **lattice** generated by $\omega_1, \omega_2 \in \mathbb{C}$

- Intuitively, a complex torus is formed by gluing opposite sides of the lattice.

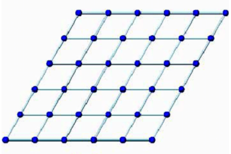


Complex torus

Definition

A **complex torus** is the set $\mathbb{C}/L$ where $L = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$ is a **lattice** generated by $\omega_1, \omega_2 \in \mathbb{C}$

- Intuitively, a complex torus is formed by gluing opposite sides of the lattice.



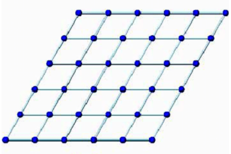
- The idea of taking quotient is similar to $\mathbb{Z}/p\mathbb{Z} = \{0, 1, ..., p-1\}$

Complex torus

Definition

A **complex torus** is the set $\mathbb{C}/L$ where $L = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$ is a **lattice** generated by $\omega_1, \omega_2 \in \mathbb{C}$

- Intuitively, a complex torus is formed by gluing opposite sides of the lattice.



- The idea of taking quotient is similar to $\mathbb{Z}/p\mathbb{Z} = \{0, 1, ..., p-1\}$
- Remark : $\mathbb{C}/L$ can be interpreted as **quotient of the group action** and a **compact Riemann surface** (manifold).

Elliptic function

Definition

An **elliptic function** is a complex differentiable (except some points) such that $\forall \ell \in L$, $f(z+\ell) = f(z)$

- This means the behaviour of the elliptic function repeats in every parallelogram.
  Hence, it can be viewed as a function on complex torus.

Elliptic function

Definition

An **elliptic function** is a complex differentiable (except some points) such that $\forall \ell \in L$, $f(z+\ell) = f(z)$

- This means the behaviour of the elliptic function repeats in every parallelogram.
  Hence, it can be viewed as a function on complex torus.
- It is the inverse of some **elliptic integral** which is generalization of that gives the arc-length of ellipse $\int_0^{2\pi} \sqrt{a^2 \sin^2(\theta) + b^2 \cos^2(\theta)} d\theta$.

Examples

Weierstrass elliptic function is defined as
$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in L - \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right)$

It is the inverse of $u(z) = \int_z^{\infty} \frac{-1}{\sqrt{4s^3 - g_2 s - g_3}} ds$
such that $u(\wp(z)) = z$

UNIVERSITY OF TORONTO

Elliptic curve and torus

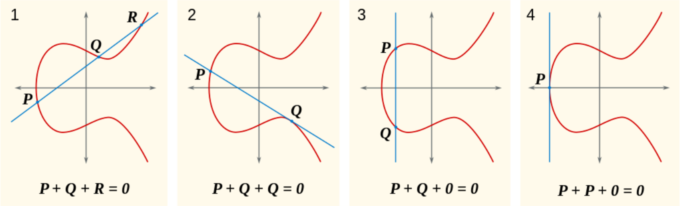
- Weierstrass elliptic function satisfied a differential equation $(\wp'(z))^2 = 4\wp^3(z) - g_2\wp(z) - g_3$

Elliptic curve and torus

- Weierstrass elliptic function satisfied a differential equation $(\wp'(z))^2 = 4\wp^3(z) - g_2\wp(z) - g_3$
- It defines an elliptic curve $y^2 = 4x^3 - g_2x - g_3$ by letting $(x, y) = (\wp(z), \wp'(z))$

Elliptic curve and torus

- Weierstrass elliptic function satisfied a differential equation $(\wp'(z))^2 = 4\wp^3(z) - g_2\wp(z) - g_3$
- It defines an elliptic curve $y^2 = 4x^3 - g_2x - g_3$ by letting $(x, y) = (\wp(z), \wp'(z))$
- More importantly, this map is isomorphic.
  This implies an elliptic curve forms a group isomorphic to complex torus.



The point at infinity O is the group identity.
(It is also isomorphic in terms of Riemann surfaces)

Function of lattice

- But what is g_2 and g_3? It should be something only depends on the lattice but not depends on z.

Function of lattice

- But what is g_2 and g_3? It should be something only depends on the lattice but not depends on z.
- In fact, the construction suggests that $g_2(\lambda\omega_1, \lambda\omega_2) = \lambda^{-4} g_2(\omega_1, \omega_2)$ and $g_3(\lambda\omega_1, \lambda\omega_2) = \lambda^{-6} g_3(\omega_1, \omega_2)$

Function of lattice

- But what is g_2 and g_3? It should be something only depends on the lattice but not depends on z.
- In fact, the construction suggests that $g_2(\lambda\omega_1, \lambda\omega_2) = \lambda^{-4} g_2(\omega_1, \omega_2)$ and $g_3(\lambda\omega_1, \lambda\omega_2) = \lambda^{-6} g_3(\omega_1, \omega_2)$
- These functions are the **modular forms** if we define $\tau = \frac{\omega_2}{\omega_1}$ and $g_2(\tau) = g_2(1, \tau)$.

Examples

The **Eisenstein series** is a modular form defined by
$G_{2k}(z) = \sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \frac{1}{(m+nz)^{2k}}$

Then $g_2 = 60G_4$ and $g_3 = 140G_6$

Function of lattice

- But what is g_2 and g_3? It should be something only depends on the lattice but not depends on z.
- In fact, the construction suggests that $g_2(\lambda\omega_1, \lambda\omega_2) = \lambda^{-4} g_2(\omega_1, \omega_2)$ and $g_3(\lambda\omega_1, \lambda\omega_2) = \lambda^{-6} g_3(\omega_1, \omega_2)$
- These functions are the **modular forms** if we define $\tau = \frac{\omega_2}{\omega_1}$ and $g_2(\tau) = g_2(1, \tau)$.

Examples

The **Eisenstein series** is a modular form defined by $G_{2k}(z) = \sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \frac{1}{(m+nz)^{2k}}$

Then $g_2 = 60G_4$ and $g_3 = 140G_6$

- The theorem about the modular forms implies that $\Delta(z) = (g_2(z))^3 - 27(g_3(z))^2 \neq 0$ except $z = i\infty$

- One may ask when do two elliptic curves $\mathbb{C}/L$ are considered as the same.

Classification of elliptic curve

- One may ask when do two elliptic curves $\mathbb{C}/L$ are considered as the same.
- Intuitively, the lattice L remains the same if you rotates or translate the whole plane or scratch both generators at the same amount .

Classification of elliptic curve

- One may ask when do two elliptic curves $\mathbb{C}/L$ are considered as the same.
- Intuitively, the lattice L remains the same if you rotates or translate the whole plane or scratch both generators at the same amount .
- Mathematically, it is done by the **set of** 2×2 **matrices with integers entries and determinant 1**.

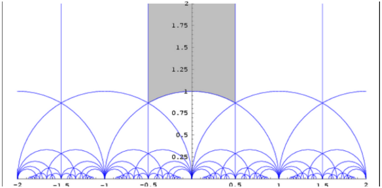
  This means $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} a\tau + b \\ c\tau + d \end{pmatrix} = \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$ should implies τ and τ' defines the same lattice L.

Moduli space

- In geometry, moduli space is the space such that the points classify certain geometric object.
  Example: **circles** can be classified by the **radius**, so the **moduli space** is the **positive real line**.

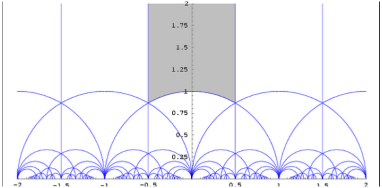
Moduli space

- In geometry, moduli space is the space such that the points classify certain geometric object.
  Example: **circles** can be classified by the **radius**, so the **moduli space** is the **positive real line**.
- Then the **moduli space of elliptic curve** should consists points which cannot be related to other points by those special matrix.



Moduli space

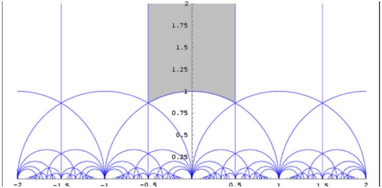
- In geometry, moduli space is the space such that the points classify certain geometric object.
  Example: **circles** can be classified by the **radius**, so the **moduli space** is the **positive real line**.
- Then the **moduli space of elliptic curve** should consists points which cannot be related to other points by those special matrix.



- This means for any point z outside the grey region, there exists a matrix that can brought z inside the grey region.

Moduli space

- In geometry, moduli space is the space such that the points classify certain geometric object.
  Example: **circles** can be classified by the **radius**, so the **moduli space** is the **positive real line**.
- Then the **moduli space of elliptic curve** should consists points which cannot be related to other points by those special matrix.



- This means for any point z outside the grey region,
  there exists a matrix that can brought z inside the grey region.
- It is the **fundamental domain** of the group action of on the upper-half plane by $\gamma(z) = \frac{az+b}{cz+d}$ where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Modular form

Interpretations of modular form

- Modular forms f of weight 2k are the differential forms on the moduli space such that satisfying $f(\gamma(z))d(\gamma(z))^k = f(z)dz^k$
- Modular forms f of weight 2k are the differentiable functions depend on the lattice such that $f(\tau) = g(1,\tau) = \omega_1^{2k} g(\omega_1, \omega_2)$

Examples

- The **j-invariant function** defined by $j(z) = \frac{1728 g_2(z)^3}{g_2(z)^3 - 27 g_3(z)^2}$ satisfied $j(\frac{az+b}{cz+d}) = j(z)$
- The **Eisenstein series** $G_{2k}(z) = \sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \frac{1}{(m+nz)^{2k}}$ satisfied $G_{2k}(\frac{az+b}{cz+d}) = (cz+d)^{2k} G_{2k}(z)$

UNIVERSITY OF TORONTO

Modular form

Definition

Modular form of weight 2k is complex differentiable function such that $f(\gamma(z)) = (cz + d)^{2k} f(z)$ and bounded when $Im(z) \to \infty$

- The condition of being bounded is to ensure that modular form can also be expressed in terms of $q = e^{2\pi iz}$.

Modular form

Definition

Modular form of weight 2k is complex differentiable function such that $f(\gamma(z)) = (cz+d)^{2k} f(z)$ and bounded when $Im(z) \to \infty$

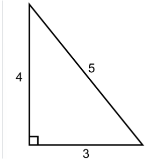
- The condition of being bounded is to ensure that modular form can also be expressed in terms of $q = e^{2\pi iz}$.
- The coefficients are surprisingly informative.

Examples

- $j(z) = q^{-1} + 744 + 196884q + 21493760q^3 + \ldots$ is related to the dimension of representation of monster group which has about $8 \times 10^{53} elements$
- $\frac{G_4(z)}{2\zeta(2k)} = 1 + 240q^2 + 2160q^4 + 6720q^6 + \ldots = 1 + 240\sum_{n=1}^{\infty} \sigma_3(n)q^n$ is related to the optimal sphere packing in 8 dimensional space

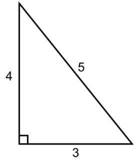
Applications in number theory

- **Congruent number** is a positive integer such that it is the area of a triangle with rational number sides.
  Example: 6 is a congruent number



Congruent number

- **Congruent number** is a positive integer such that it is the area of a triangle with rational number sides.
  Example: 6 is a congruent number

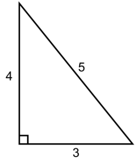


Question

Given a positive integer, can you determine whether it is congruent?

Congruent number

- **Congruent number** is a positive integer such that it is the area of a triangle with rational number sides.
  Example: 6 is a congruent number



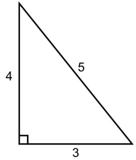
Question

Given a positive integer, can you determine whether it is congruent?

- It was considered by ancient Greeks and Arabs.

Congruent number

- **Congruent number** is a positive integer such that it is the area of a triangle with rational number sides.
  Example: 6 is a congruent number



Question

Given a positive integer, can you determine whether it is congruent?

- It was considered by ancient Greeks and Arabs.
- But is **STILL UNSOLVED NOW** !

UNIVERSITY OF TORONTO

Elliptic curve and congruent number

- n is congruent number if and only if elliptic curve $y^2 = x^3 - n^2x$ has infinitely many rational number points.

Elliptic curve and congruent number

- n is congruent number if and only if elliptic curve $y^2 = x^3 - n^2 x$ has infinitely many rational number points.
- It is closely related to a **US$1,000,000** problem.

Conjecture (Birch and Swinnerton-Dyer)

For r is rank of the group of **elliptic curve over rational number** $E(\mathbb{Q})$ such that it is isomorphic to $E(\mathbb{Q})_{tors} \bigoplus \mathbb{Z}^r$, it is conjectured that the **L function** satisfies

$$L(E, s) = (s-1)^r g(s)$$

where $g(s)$ is complex differentiable and nonzero at $s = 1$.

UNIVERSITY OF TORONTO

Elliptic curve and congruent number

- n is congruent number if and only if elliptic curve $y^2 = x^3 - n^2 x$ has infinitely many rational number points.
- It is closely related to a **US$1,000,000** problem.

Conjecture (Birch and Swinnerton-Dyer)

For r is rank of the group of **elliptic curve over rational number** $E(\mathbb{Q})$ such that it is isomorphic to $E(\mathbb{Q})_{tors} \bigoplus \mathbb{Z}^r$, it is conjectured that the **L function** satisfies

$$L(E, s) = (s-1)^r g(s)$$

where $g(s)$ is complex differentiable and nonzero at $s = 1$.

- If this holds true for elliptic curve $y^2 = x^3 - n^2 x$ then there is an algorithm that can check whether n is congruent or not.

Elliptic curve and congruent number

- n is congruent number if and only if elliptic curve $y^2 = x^3 - n^2 x$ has infinitely many rational number points.
- It is closely related to a **US$1,000,000** problem.

Conjecture (Birch and Swinnerton-Dyer)

For r is rank of the group of **elliptic curve over rational number** $E(\mathbb{Q})$ such that it is isomorphic to $E(\mathbb{Q})_{tors} \bigoplus \mathbb{Z}^r$, it is conjectured that the **L function** satisfies

$$L(E, s) = (s-1)^r g(s)$$

where $g(s)$ is complex differentiable and nonzero at $s = 1$.

- If this holds true for elliptic curve $y^2 = x^3 - n^2 x$ then there is an algorithm that can check whether n is congruent or not.
- But what is L function?

UNIVERSITY OF TORONTO

L functions in number theory

- Prototype: **Riemann zeta function** $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$
  The fact that $\zeta(1 + it) \neq 0$ was used to prove that
  $\#\{\text{prime } \leq x\} \sim \frac{\log(x)}{x}$

L functions in number theory

- Prototype: **Riemann zeta function** $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$
  The fact that $\zeta(1 + it) \neq 0$ was used to prove that $\#\{\text{prime } \leq x\} \sim \frac{\log(x)}{x}$
- First L function: **Dirichlet L function** $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$
  The fact that $L(1, \chi) \neq 0$ was used to prove that there are infinitely many prime of the form $a + nd$ for $gcd(a, d) = 1$

L functions in number theory

- Prototype: **Riemann zeta function** $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$
  The fact that $\zeta(1+it) \neq 0$ was used to prove that $\#\{\text{prime } \leq x\} \sim \frac{\log(x)}{x}$
- First L function: **Dirichlet L function** $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$
  The fact that $L(1,\chi) \neq 0$ was used to prove that there are infinitely many prime of the form $a + nd$ for $gcd(a,d) = 1$
- The idea of L functions is to make $a(n)$ to series $\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$

L functions in number theory

- Prototype: **Riemann zeta function** $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$
  The fact that $\zeta(1+it) \neq 0$ was used to prove that
  $\#\{\text{prime } \leq x\} \sim \frac{\log(x)}{x}$
- First L function: **Dirichlet L function** $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$
  The fact that $L(1,\chi) \neq 0$ was used to prove that there are infinitely many prime of the form $a + nd$ for $gcd(a,d) = 1$
- The idea of L functions is to make $a(n)$ to series $\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$
- In fact, the coefficients of some spacial kind of modular form is associated to L function.

Example

For $\Delta(z) = (g_2(z))^3 - 27(g_3(z))^2 = \sum_{n=1}^{\infty} \tau(n) q^n$,
the series $\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$ is a L function called **Ramanujan L function**

TORONTO

L function of elliptic curve

- The definition of L function of elliptic curves is complicated.

L function of elliptic curve

- The definition of L function of elliptic curves is complicated.
- For $E_n : y^2 = x^3 - n^2x$,

$$L(E_n, s) = \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E_n \backslash \mathbb{F}_p, p^{-s})} = \prod_{p \nmid 2n} \frac{1}{1 - 2a_{E,p}p^{-s} + p^{1-2s}}$$

where $Z(E_n \backslash \mathbb{F}_p, T) = \exp(\sum_{r=1}^{\infty} \frac{N_r}{r}(T)^r)$ and N_r is number of points over $\mathbb{F}_{p^r}$ on the elliptic curve.

L function of elliptic curve

- The definition of L function of elliptic curves is complicated.
- For $E_n : y^2 = x^3 - n^2 x$,

$$L(E_n, s) = \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E_n \backslash \mathbb{F}_p, p^{-s})} = \prod_{p \nmid 2n} \frac{1}{1 - 2a_{E,p}p^{-s} + p^{1-2s}}$$

  where $Z(E_n \backslash \mathbb{F}_p, T) = \exp(\sum_{r=1}^{\infty} \frac{N_r}{r}(T)^r)$ and N_r is number of points over $\mathbb{F}_{p^r}$ on the elliptic curve.
- What if we write it in the form $L(E, s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$?

UNIVERSITY OF TORONTO

- The definition of L function of elliptic curves is complicated.
- For $E_n : y^2 = x^3 - n^2x$,

$$L(E_n, s) = \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E_n \backslash \mathbb{F}_p, p^{-s})} = \prod_{p \nmid 2n} \frac{1}{1 - 2a_{E,p}p^{-s} + p^{1-2s}}$$

where $Z(E_n \backslash \mathbb{F}_p, T) = \exp(\sum_{r=1}^{\infty} \frac{N_r}{r}(T)^r)$ and N_r is number of points over $\mathbb{F}_{p^r}$ on the elliptic curve.

- What if we write it in the form $L(E, s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$?
- Turns out

$$f(E, q) = \sum_{n=1}^{\infty} a(n)q^n$$

is a modular form !

Modular elliptic curve

Modularity theorem

Elliptic curve E over rational number can be obtained by rational map from the **modular curve** $X_0(N)$.

The idea of modular curve is to **classify elliptic curves with extra condition.**

The modular curve $X_0(N)$ is the compactified quotient of upper-half plane by the set of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfying $c \equiv 0 \pmod{N}$.
The associated information about elliptic curve is its **cyclic subgroup of order N**.

Significance of modularity theorem

Fermat's last theorem

$x^n + y^n = z^n$ has no positive integer solution for $n \geq 3$

- It was conjectured by Fermat in 1637.
- The case $n = 3$ was proved by Euler in 1770.
- Some special cases was proved by using algebraic number theory in 19th and early 20th century.
- Suppose $a^p + b^p = c^p$ for positive integer a, b, c and prime $p > 3$, Frey related it to **elliptic curve** $y^2 = x(x - a^p)(x - b^p)$ in 1986.
- Ribet showed that the elliptic curve created by a, b, c is **semistable and not modular** in 1990.
- Wiles proved the **modularity theorem** for the semistable elliptic curve in 1995.
  By **contradiction**, it proved Fermat's last theorem.

Summary

1. Complex elliptic curve is a torus.
2. Its name comes from the relationship with elliptic function.
3. Modular form is function of lattice and form of space classifying elliptic curve.
4. Coefficients of modular form are informative.
5. Elliptic curve itself is related to congruent problem.
6. The connection of elliptic curve and modular form leads to the proof of Fermat's last theorem.

UNIVERSITY OF TORONTO