

Elliptic Curves

An **Elliptic Curve** over a field K is a curve of the form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where the a_i 's are constants. If $\text{char}K \neq 2$ or 3 we can write this as:

$$y^2 = x^3 + Ax + B$$

Elliptic Curve as a Group

An elliptic curve is a group. There are many ways to define the group structure, such as the chord-tangent method. For elliptic curves over \mathbb{C} we will use \wp -functions:

Let H be $\{z \in \mathbb{C} : \text{Im}z > 0\}$ (The Upper Half Plane).

Let ω_1 and ω_2 be non-zero complex numbers with $\frac{\omega_2}{\omega_1}$ in the upper half plane. Then the set

$$\Lambda := \{n\omega_1 + m\omega_2 : n, m \in \mathbb{Z}\} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$$

is called a **lattice**, and it is an additive subgroup of \mathbb{C} .

The group \mathbb{C}/Λ is a compact Riemann surface of genus 1

Elliptic Functions

An **elliptic function** (doubly periodic function) is a meromorphic function f such that $f(z + \omega_1) = f(z) = f(z + \omega_2)$ for all z in \mathbb{C} . An elliptic function is completely determined by the values in its fundamental parallelogram:

$$\{a\omega_1 + b\omega_2 : 0 \leq a \leq 1, 0 \leq b \leq 1\}$$

Using this fact together with Liouville's Theorem we can show that the only holomorphic elliptic functions are constants.

Also by integrating $f(z)$ along the boundary of the fundamental parallelogram we can show that if it is non-constant, $f(z)$ has more than one pole in the parallelogram (counting multiplicity).

The Weierstrass \wp -Function

The Weierstrass \wp -function for a lattice Λ is

$$\wp(z) = \frac{1}{z^2} + \sum_{l \in \Lambda, l \neq 0} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$

$\wp(z)$ has a pole of order 2 at each lattice point and is holomorphic everywhere else. $\wp'(z)$ has a pole of order 3 at each lattice point and is holomorphic everywhere else.

$\wp(z)$ satisfies a certain differential equation:

$$(\wp'(z))^2 = 4\wp^3(z) + g_2\wp(z) + g_3$$

for constants g_2 and g_3 which depend on Λ . Let $x = \wp(z)$, $y = \wp'(z)$. Then the map $z \mapsto (\wp(z), \wp'(z))$ is a bijection between \mathbb{C}/Λ and the elliptic curve $E : y^2 = 4x^3 + g_2x + g_3$ (considered projectively).

Elliptic Functions

The elliptic functions for a lattice are exactly the rational functions of $\wp(z)$ and $\wp'(z)$.

1-1 correspondence: Lattices \leftrightarrow Elliptic Curves

Each lattice specifies a \wp -function which in turn satisfies a differential equation that specifies an elliptic curve. On the other hand, each elliptic curve (over \mathbb{C}) is parameterized by the \wp -function and its derivative for some lattice.

The group law on \mathbb{C}/Λ extends to a group law on E . The identity element, call it O , is the point at infinity (that is: $(0 : 1 : 0)$ if E is considered projectively). E is homeomorphic and isomorphic to \mathbb{C}/Λ and is a compact genus 1 Riemann surface.

The group also has the property that if $x_1, x_2, y_1,$ and y_2 are in some subfield F of \mathbb{C} then so is $(x_1, y_1) + (x_2, y_2)$.

Torsion Points

For an abelian group G and a positive integer n , the set of n -torsion points is $\{g \in G : n \cdot g = 0\}$.

For an elliptic curve E over \mathbb{C} and a positive integer n there are n^2 n -torsion points, corresponding to the n -torsion points of \mathbb{C}/Λ .

The subgroup of torsion points with rational coordinates is much smaller: in fact it is always finite. For example, the curve $y^2 + y = x^3 - x^2 - 10x - 20$ has exactly five rational torsion points, and they form a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

The Modular Group: $SL_2(\mathbb{Z})$

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}$$

$SL_2(\mathbb{Z})$ acts on the upper half plane in the following way:

$$\text{If } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ then } \gamma z = \frac{az+b}{cz+d}$$

$SL_2(\mathbb{Z})$ is generated by two elements:

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ corresponding to } z \mapsto \frac{-1}{z}$$

and

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ corresponding to } z \mapsto z + 1$$

Fundamental Domain

Define an equivalence relation by saying two points $a, b \in H$ are equivalent if $a = \gamma b$ for some $\gamma \in SL_2(\mathbb{Z})$

The set $\{z \in H : -\frac{1}{2} \leq \operatorname{Re}z \leq \frac{1}{2} \text{ and } |z| \geq 1\}$ is called the **fundamental domain** of $SL_2(\mathbb{Z})$. Every point on the upper half plane is equivalent to exactly one point on the fundamental domain (Or maybe more than one boundary point)

The edges match up and we can “wrap up” the fundamental domain into a compact Riemann surface (compactifying to add the cusp at infinity). This is called the **modular curve** of $SL_2(\mathbb{Z})$.

Subgroups

For positive integers N define subgroups of $SL_2(\mathbb{Z})$ by:

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma^1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \pmod{N} \right\}$$

For each N , $\Gamma(N) \subset \Gamma^1(N) \subset \Gamma^0(N) \subset SL_2(\mathbb{Z})$.

A subgroup of $SL_2(\mathbb{Z})$ is called a **congruence group** if it contains $\Gamma(N)$ for some N , Otherwise it is called **noncongruence**.

Subgroups

For a subgroup Γ of $SL_2(\mathbb{Z})$ we say $a, b \in H$ are Γ -equivalent if $a = \gamma b$ for some γ in Γ .

As we did with $SL_2(\mathbb{Z})$, we can find a fundamental domain for this equivalence relation and wrap it up as a compact Riemann surface.

Note that the action $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$ is also a permutation on the set $\mathbb{Q} \cup \{\infty\}$. The **cusps** of Γ are the orbits of this action. $SL_2(\mathbb{Z})$ has only one cusp: The point at ∞ .

Examples: $\Gamma(2)$, $\Gamma^0(11)$

Modular Functions

A **modular function** for $\Gamma \leq SL_2(\mathbb{Z})$ is a function f meromorphic in the upper half plane such that $f(\gamma z) = f(z)$ for every $\gamma \in \Gamma$ and f is meromorphic at the cusps.

Γ contains $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ for some positive integer N , so f must satisfy $f(z) = f(z + N)$ for all $z \in H$. Thus f is periodic and can be written as a Fourier series:

$$f(z) = \sum_{i=n}^{\infty} a_i q^i$$

for some $n \in \mathbb{Z}$ where $q = e^{2\pi iz/N}$

If Γ is a congruence subgroup then the denominators of the coefficients in the Fourier series of f are a bounded set.

Functions on a Modular Curve

Recall: The meromorphic functions on the extended complex plane (\mathbb{C} compactified with a point at infinity) are exactly the rational functions: $\mathbb{C}(z)$.

For $SL_2(\mathbb{Z})$ the meromorphic functions are generated by the j -function:

$$j(z) := q^{-1} + 744 + 196884q + 21493760q^2 + \dots$$

where $q = e^{2\pi iz}$. $j(z)$ is a bijective map from the fundamental domain of $SL_2(\mathbb{Z})$ to \mathbb{C} , and it has a single pole of order 1 at ∞ . The meromorphic functions of $SL_2(\mathbb{Z})$ are exactly $\mathbb{C}(j(z))$.

$\Gamma(2)$ has a modular function λ which generates the modular functions of $\Gamma(2)$

Functions on Genus 1 Curves

What about genus 1 curves?

In the elliptic curve case, the doubly periodic functions are exactly the rational functions of $\wp(z)$ and $\wp'(z)$ for a lattice Λ . So the meromorphic functions on the elliptic curve corresponding to Λ are just the rational functions of $\wp(z)$ and $\wp'(z)$ (considered as functions on the elliptic curve).

Similarly, for $\Gamma^0(11)$, a genus 1 subgroup, there will be two functions x and y that together generate the meromorphic functions.

Genus 1 Subgroups

We are interested in genus 1 subgroups of $SL_2(\mathbb{Z})$. If Γ is genus 1 it is finitely generated with two kinds of generators:

- γ_i where each γ_i is a generator of the stabilizer of a cusp or an elliptic point
- A and B generators of the homology.

Then:

$$\Gamma = \langle \gamma_1, \dots, \gamma_n, A, B : \gamma_1 \dots \gamma_n A B A^{-1} B^{-1} = 1 \rangle$$

Homomorphisms

Consider a homomorphism $\phi : \Gamma \rightarrow H$ where H is a finite abelian group. ϕ gives rise to two homomorphisms ϕ_1 and ϕ_2 such that:

- $\phi_1(A) = 1, \phi_1(B) = 1, \phi_1(\gamma_i) = \phi(\gamma_i)$
- $\phi_2(A) = \phi(A), \phi_2(B) = \phi(B), \phi_2(\gamma_i) = 1.$

We are interested in the second kind, so assume that $\phi(\gamma_i) = 1$ for all i .

Let $G = \ker(\phi)$. G is called a **character group of the second kind**.

A Result:

If $\phi : \Gamma^0(N) \rightarrow H$ is a homomorphism such that $\phi(\gamma_i) = 1$ for all i , H is abelian, and $\Gamma := \ker \phi$ does not contain $\Gamma^1(N)$ then Γ is noncongruence.

The Group $\Gamma^0(11)$

$$\text{Recall: } \Gamma^0(11) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \pmod{11} \right\}$$

$\Gamma^0(11)$ is a genus 1 group with no elliptic points. Its field of functions is generated by two functions:

- x with an order 2 pole at ∞ and no other poles
- y with an order 3 pole at ∞ and no other poles

These functions can be shown to satisfy a certain relation:

$$E : y^2 + y = x^3 - x^2 - 10x - 20$$

An elliptic curve!

The Curve $y^2 + y = x^3 - x^2 - 10x - 20$

This elliptic curve considered over \mathbb{Q} has a torsion group of order 5 generated by $P := [5, 5]$:

$$2P = [16, -61]$$

$$3P = [16, 60]$$

$$4P = [5, -6]$$

$$5P = O$$

Over \mathbb{C} it's 5-torsion subgroup is isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, and is generated by $P := [5, 5]$ and $Q := [-\frac{1}{2} + \frac{11}{10}\sqrt{5}, \frac{11}{10}\sqrt{-25 - 2\sqrt{5}}]$

Deriving x and y

From the theory of elliptic curves $\frac{dx}{2y+1}$ is a non-vanishing holomorphic differential, and from the theory of modular forms we know the space of cusp forms of $\Gamma^0(11)$ is one-dimensional and consists of all multiples of $\eta(11z)^2\eta(z)^2$, where

$$\eta(z) = q^{1/24} \prod_{n \geq 1} (1 - q^n)$$

and $q = e^{2\pi iz}$. So we have

$$\frac{dx}{2y+1} = c \cdot \eta(11z)^2\eta(z)^2 dz$$

and combining this with the equation of the elliptic curve we can solve for a Fourier series of x and y

Fourier series of x and y

$$x = q^{-2} + 2q^{-1} + 4 + 5q + 8q^2 + q^3 + 7q^4 - 11q^5 + \dots$$

$$y = q^{-3} + 3q^{-2} + 7q^{-1} + 12 + 17q + 26q^2 + 19q^3 + \dots$$

where $q = e^{2\pi iz/11}$

The map $z \mapsto (x(z), y(z))$ gives a bijection between the modular curve $X^0(11)$ and the elliptic curve E , so we can think of x and y as functions on E .

We want to construct a function on E which has a single pole of order 5 at the identity and a zero of order 5 at the 5-torsion point P . This function is found to be:

$$f_P = xy - 4x^2 + 30x - 4y - 55$$

Function Fields of Character Groups

Take the fifth root of f_P and get a function with poles of order 1 at each lattice point. This means $\sqrt[5]{f_P}$ is not an elliptic function for the original lattice, but is for a larger lattice.

If F is the field of functions for $X^0(11)$ then $F(f_p)$ is the field of functions for one of the character groups of $\Gamma^0(11)$ of index 5.

$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ has 6 subgroups of order 5, and generators for them are $P, Q, Q + P, Q + 2P, Q + 3P, Q + 4P$.

There are 6 character groups of $\Gamma^0(11)$ of index 5. The field of functions of the other five come from applying this same process to the other torsion points: $F(\sqrt[5]{f_Q}), F(\sqrt[5]{f_{Q+P}})$, etc.

Series

$$f_P = q^{-5} + q^{-4} - 3q^{-3} + 13q^{-2} + 20q^{-1} + \dots$$

$$f_{Q+P} = q^{-5} + q^{-4} + \frac{23 + \sqrt{5} + i(3 + \sqrt{5})\sqrt{25 + 2\sqrt{5}}}{4}q^{-3} + \dots$$

$$f_{Q+2P} = q^{-5} + q^{-4} + \frac{99 - 33\sqrt{5} + i(23 + 3\sqrt{5})\sqrt{25 + 2\sqrt{5}}}{44}q^{-3} + \dots$$

$$f_{Q+3P} = q^{-5} + q^{-4} + \frac{99 - 33\sqrt{5} - i(23 + 3\sqrt{5})\sqrt{25 + 2\sqrt{5}}}{44}q^{-3} + \dots$$

$$f_{Q+4P} = q^{-5} + q^{-4} + \frac{23 + \sqrt{5} - i(3 + \sqrt{5})\sqrt{25 + 2\sqrt{5}}}{4}q^{-3} + \dots$$

The series corresponding to Q is more complicated. The fifth root of each of the above series has unbounded denominators, hence they correspond to noncongruence subgroups. The final series corresponds to $\Gamma^1(11)$.