ELLIPTIC FUNCTIONS, ELLIPTIC CURVES, AND MODULAR FORMS

YOUNG JIN KIM

Contents

1. Introduction

Elliptic curves often encode lots of interesting properties and contain information to interesting problems. For example,

Example 1.1. Are there three consecutive integers whose product is a perfect square?

The answer would bring us to trying to solve the equation

$$y^2 = x(x+1)(x+2)$$

where $x, y \in \mathbb{Z}, y \neq 0$ and this equation is an elliptic curve!

Moreover, elliptic curves have applications- elliptic curve cryptography is premise of modern cryptography and most famously, elliptic curves were used to solve *Fermat's Last Theorem.*

Because elliptic curves have so interesting, let's try to study them and classify them.

2. Singly-Periodic Functions

Note that everything we do will be in the complex plane unless specified otherwise.

Definition 2.1 (Singly-Periodic)**.** A function f on $\mathbb{C}$ is **singly-periodic** with period ω if for $\omega \neq 0$, we have that

$$f(z+w) = f(z) \qquad \text{for all } z \in \mathbb{C}.$$

Examples

- $e^z = e^{x+yi} = e^x e^{yi}$ has period $2\pi i$
- $\sin z$ and $\cos z$ has period 2π.

We will only consider "nice" functions, to us meaning differentiable, (actually holomorphic or meromorphic) and if ω is a period, then by successive iterations, we get that

$$f(z+nw) = f(z) \qquad \text{for all } z \in \mathbb{C}, n \in \mathbb{Z}$$

That is, we have that f is *invariant* under translation by the group $\mathbb{Z} \cdot w \subseteq \mathbb{C}$.

3. Elliptic Functions

Singly periodic functions are nice but uninteresting. So what if we try to have a nice function with **two periods?**

Definition 3.1 (Doubly-periodic)**.** A function $f : C \longrightarrow \mathbb{C}$ is **doubly-periodic** if there exists $\omega_1, \omega_2 \in \mathbb{C}$ with $\omega_1, \omega_2 \in \mathbb{C}^\times$ such that

$$f(z+\omega_1) = f(z) \text{ and } f(z+\omega_2) = f(z) \qquad \text{for all } z \in \mathbb{C}$$

where ω_1, ω_2 are linearly independent over $\mathbb{R}$.

Iterating the periodicity condition yields

$$f(z+n\omega_1+m\omega_2) = f(z) \qquad \text{for all } z \in \mathbb{C}, n, m \in \mathbb{Z}.$$

Since we are looking for such periodic functions, which are also "nice", it would be natural for us to treat ω_1, ω_2 as vectors and consider their $\mathbb{Z}$-span (the span generated by them).

Definition 3.2 (Lattice)**.** A **lattice** Λ is a subset of $\mathbb{C}$ of the form

$$\Lambda = \mathbb{Z} \cdot \omega_1 + \mathbb{Z} \cdot \omega_2 = \text{Span}\{\omega_1, \omega_2\}$$

where ω_1, ω_2 are linearly independent over $\mathbb{R}$. We say ω_1 and ω_2 are the basis elements that generate Λ. Note that this is actually module over $\mathbb{Z}$.

Associated to the lattice Λ is the **fundamental parallelogram** with respect to the basis ω_1 and ω_2

$$\mathcal{P} = \mathcal{P}(\omega_1, \omega_2) = \{t_1\omega_1 + t_2\omega_2 : 0 \leq t_1, t_2 \leq 1\}.$$

This is both convenient and important because f is completely determined by its behaviour on $\mathcal{P}$ by periodicity. Thus, we get a tiling of $\mathbb{C}$ which are all translates of $\mathcal{P}$ (see Figure 1).

Suppose we have $z, w \in \mathbb{C}$ such that $z - \omega = \lambda \in \Lambda$, then we get that

$$f(z) = f(z-\lambda) = f(z-z+w) = f(w)$$

and so it is natural for us to group everything into an equivalence class. The equivalence class of $z \in \mathbb{C}$ is the set of the form

$$[z] = \{\omega \in \mathbb{C} : w - z \in \Lambda\} = z + \Lambda.$$

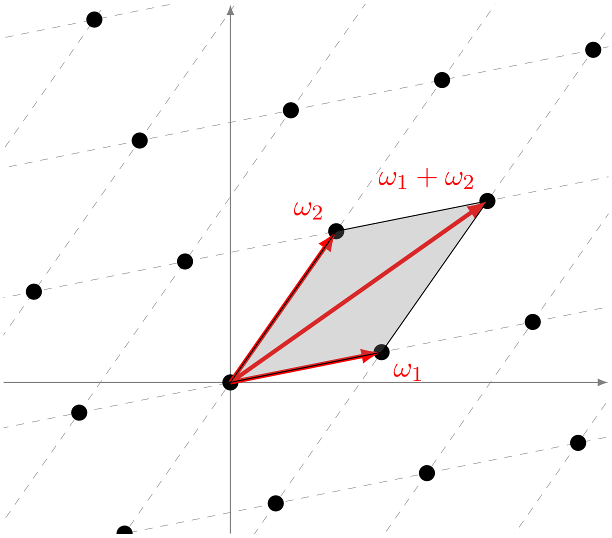


Figure 1. A lattice $\Lambda \subseteq \mathbb{C}$ and its fundamental parallelogram $\mathcal{P}$.

For an analogy, consider $\mathbb{Z}/n\mathbb{Z}$, and in here, we say $x = y$ if and only if $x - y = kn$ for some $k \in \mathbb{Z}$ and so when we work with $\mathbb{Z}/n\mathbb{Z}$, we work with the equivalence classes.

The same story holds here. We have the quotient of the complex plane by the lattice $\mathbb{C}/\Lambda$, which is the set of all equivalence classes with respect to the relation

$$z - w = \lambda \in \Lambda.$$

Just as we had addition on $\mathbb{Z}/n\mathbb{Z}$, we can define addition on $\mathbb{C}/\Lambda$, which it inherits from $\mathbb{C}$, as

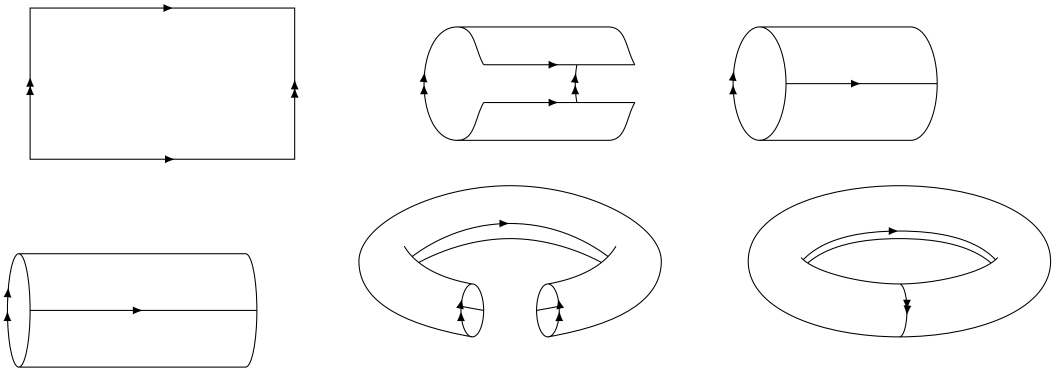
$$[z] + [w] = [z + w]$$
$$z + \Lambda + w + \Lambda = (z + w) + \Lambda$$

and since $+$ is commutative, we say $\mathbb{C}/\Lambda$ is an abelian group.

Since every point in $\mathbb{C}/\Lambda$ has a representative in $\mathcal{P}$, we get that

$$z \equiv w \iff z = w \text{ or } \ z = w + \lambda$$

where the latter is only true if z and w live on the boundary on opposite sides.



This gives us that $\mathcal{P}$ is actually a torus!! Thus, every doubly-periodic function lives on the surface of the complex torus.

Remark: Since for all $z \in \mathbb{C}$, there exists an $\omega \in \Lambda$ such that $z - \omega \in \mathcal{F}$, every value of f is taken in Λ and since $\mathcal{P}$ is compact, if f is continuous everywhere on $\mathcal{P}$, then f is bounded and so by **Liouville's Theorem**, f will be constant.

3.1. Weierstrauss $\wp$ Functions

So this brings us to the question:

Are there any non-constant doubly-periodic functions?

The answer is **yes**, but this is not easy. So here's an example given. Consider the function

$$\wp(z) = \begin{cases} \dfrac{1}{z^2} + \displaystyle\sum_{w \in \Lambda \backslash \{0\}} \left(\dfrac{1}{(z-w)^2} - \dfrac{1}{w^2} \right) & \text{if } z \notin \Lambda \\ \\ \infty & \text{if } z \in \Lambda \end{cases}$$

The correction term $1/\omega^2$ in the sum makes the sum converge to about z/ω^3 and so this converges absolutely and uniformly on compact sets away from Λ but this isn't necessarily obvious that $\wp$ has period Λ.

It's derivative,

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$$

is a bit nicer in that it is convergent and clearly has period Λ.

Proof. It follows that the difference $\wp(z+\omega) - \wp(z)$ has derivative $\wp'(z+\omega) - \wp'(z) = 0$. Since $\wp'(z)$ is periodic, we get that there exists a constant c such that

$$\wp(z+\omega) = \wp(\omega) + c \qquad \text{for all } z \in \mathbb{C}.$$

Since we can inspect that $\wp$ is an even function, we get that the $\wp(-z) = \wp(z)$ and so if we set $z = -\dfrac{\omega}{2}$, we see that

$$c = \wp(-\frac{\omega}{2} + \omega) - \wp(\frac{\omega}{2}) = 0$$

and so $\wp$ is periodic. □

Some interesting things about these guys are that they satisfy the relation

$$\left(\wp'(z)\right)^2 = 4\left(\wp(z)\right)^3 - g_2(\Lambda) \cdot \wp(z) - g_3(\Lambda)$$

where

$$g_2(\Lambda) = 60 \sum_{\omega \in \Lambda \backslash \{0\}} \frac{1}{\omega^4} \qquad \text{and} \qquad g_3(\Lambda) = 140 \sum_{\omega \in \Lambda \backslash \{0\}} \frac{1}{\omega^6}$$

(the $g_2(\Lambda)$ and $g_3(\Lambda)$ terms are the 4^{th} and 6^{th} coefficients in the lattice Eisenstein series.)

4. Elliptic Curves

Let $E := \{(x, y) : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)\}$.

The relation above tells us that the mapping $z \longmapsto \big(\wp(z), \wp'(z)\big)$ takes non-lattice points of $\mathbb{C}$ to E.

So for an analogy, just as we have *sine* and *cosine* (its derivative) map $\mathbb{R} \to S^1$, we have the Weierstrass $\wp$ function and its derivative map $\mathbb{C} \to E$. That is, we have

$$\begin{tikzcd}
\mathbb{R} \arrow[r] \arrow[d] & S^1 \\
\mathbb{R}/2\pi\mathbb{Z} \arrow[ur] &
\end{tikzcd}
\qquad
\begin{tikzcd}
x \arrow[r] \arrow[d] & (\sin x, \cos x) \\
x + 2\pi\mathbb{Z} \arrow[ur] &
\end{tikzcd}$$

$$\begin{tikzcd}
\mathbb{C} \arrow[r] \arrow[d] & E \\
\mathbb{C}/\Lambda \arrow[ur] &
\end{tikzcd}
\qquad
\begin{tikzcd}
z \arrow[r] \arrow[d] & \big(\wp(z), \wp'(z)\big) \\
z + \Lambda \arrow[ur] &
\end{tikzcd}$$

and since we have $\mathbb{R}/2\pi\mathbb{Z}$ is a bijection to S^1, we have a bijection between the torus $\mathbb{C}/\Lambda$ and E, the elliptic curve.

Moreover, we get that the structure is preserved between the complex torus and the elliptic curve and so using the structure on the torus, we can try to learn more about the structure of the elliptic curve.

5. Modular Forms

Now, just as we have grouped the equivalent elements in $\mathbb{C}$ to their equivalence classes to form $\mathbb{C}/\Lambda$ and showed that this is an elliptic curve, we want to do the same thing with the complex tori and elliptic curves.

So to begin, we need to clarify when two lattices are the same.

We can perform a change of basis, that is, if we have $\{\omega_1, \omega_2\}$ and $\{\omega_1', \omega_2'\}$ as another basis, we can set

$$\begin{aligned} \omega_1' &= a\omega_1 + b\omega_2 \\ \omega_2' &= c\omega_1 + d\omega_2 \qquad\qquad \text{where } a, b, c, d \in \mathbb{Z} \end{aligned}$$

and so we get that

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \begin{bmatrix} a\omega_1 + b\omega_2 \\ c\omega_1 + d\omega_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

and so we see that $a, b, c, d \in \mathbb{Z}$ and moreover, since we should be able to reverse this change of basis, we would get that the determinant and $1/(\det) \in \mathbb{Z}$ and so $ad - bc = \pm 1$. However, if $ad - bc = -1$, we can move the multiply the matrix by -1 and change the sign of the vectors ω_1 and ω_2 and so we can assume without loss of generality that the determinant is 1.

So considering the set

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

we get a specific case of the special linear group known as the **modular group**.

Moreover, we can normalize the basis elements ω_1 and ω_2. That is, if ω_1, ω_2 are the basis of Λ, then we can take $\tau = \omega_1/\omega_2$ and take without loss of generality that $\tau \in \mathcal{H}$.

To start the process of classifying all complex tori, we start by considering a function F such that

$$F(\alpha \cdot \Lambda) = \alpha^{-k} \cdot F(\Lambda)$$

and we call F a **homogeneous function of degree $-k$.**

Example of homogeneity

Recall that we have the coefficients of the Eisenstein series in the $\wp$ function where

$$g_2(\Lambda) = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4} \qquad \text{and} \qquad g_3(\Lambda) = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$$

and so it follows that since

$$\sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(\alpha\omega)^{2k}} = \alpha^{-2k} \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^{2k}}$$

that $g_2(\Lambda)$ will be of degree -4 and g_3 is of degree -6.

Combining the ideas of homogeneity and change of basis, and since functions should be independent of the choice of basis, we get that if

$$f(z) = F(\mathbb{Z} \cdot z + \mathbb{Z} \cdot 1)$$

then there exists $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ such that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} z \\ 1 \end{bmatrix} = \begin{bmatrix} az+b \\ cz+d \end{bmatrix}$$

and so this gives us that

$$\begin{aligned} \implies f(z) &= F(\mathbb{Z} \cdot z + \mathbb{Z} \cdot 1) = F(\mathbb{Z} \cdot (az+b) + \mathbb{Z} \cdot (cz+d)) \\ &= F\left((cz+d)\left[\mathbb{Z} \cdot \left(\frac{az+b}{cz+d}\right) + \mathbb{Z} \cdot 1\right]\right) \\ &= (cz+d)^{-k} F(\mathbb{Z} \cdot \left(\frac{az+b}{cz+d}\right) + \mathbb{Z} \cdot 1) \\ &= (cz+d)^{-k} f(\frac{az+b}{cz+d}) \\ &= (cz+d)^{-k} f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}(z)\right) \end{aligned}$$

where the last equality holds due to the fact that we have that the modular group acts on the upper half plane via fractional linear transformations. Multiplying both sides by $(cz+d)^k$ gives us

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}(z)\right) = (cz+d)^k f(z)$$

and this gives us the powerful function known as a *modular form.*

Definition 5.1 (Modular form)**.** A holomorphic function $f : \mathcal{H} \to \hat{\mathbb{C}}$, where $\hat{\mathbb{C}}$ is the Riemann sphere, is a **modular form of (weakly) weight** k if

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}(z)\right) = (cz+d)^k\, f(z) \qquad \text{for } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$$

Interestingly, we get a few properties from this. That is, $f(z+1) = f(z)$ and this gives us that *any modular form of odd weight is zero.*

Moreover, since f is period 1, it possesses a Fourier expansion,

$$f(z) = \sum_{n=0}^{\infty} a_n q^n, \qquad q := e^{2\pi i z}$$

and if we have that $a_0 = 0$, then we call f a **cusp form**.

Examples of Cusp Forms

Recall that

$$g_2(\Lambda) = \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^4} \text{ and } g_3(\Lambda) = \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^6}$$

we define the **modular discriminant** as

$$\Delta : \mathcal{H} \longrightarrow \mathbb{C}, \qquad \Delta(\Lambda) = \big(g_2(\Lambda)\big)^3 - 27\,\big(g_3(\Lambda)\big)^2$$

and Δ is a modular form of weight 12 and has $a_0 = 0$ and $a_1 = (2\pi)^{12}$ in its Fourier expansion.

Since $\Delta(\Lambda) \neq 0$, (the only zero of Δ is at the point of ∞), which is a nontrivial result), we can define the function

$$j : \mathcal{H} \longrightarrow \mathbb{C} \qquad j(\Lambda) = 1728\frac{(g_2(\Lambda))^3}{\Delta(\Lambda)}$$

which is called the **modular discriminant**, and it is the absolute invariant, as we do have

$$\Delta(\alpha\cdot\Lambda) = \alpha^{-12}\Delta(\Lambda)$$
$$j(\alpha\cdot\Lambda) = j(\Lambda)$$

and after using a lot of complex analytic tools, we will get that

$$j : \mathcal{H} \longrightarrow \mathbb{C}$$

induces a mapping

$$\hat{j} : \mathcal{H}/(SL_2(\mathbb{Z})) \longrightarrow \mathbb{C}$$

where $\mathcal{H}/(SL_2(\mathbb{Z}))$ is the set of all equivalence classes of the lattices such that the diagram

$$\begin{tikzcd}
\mathcal{H} \arrow[r] \arrow[d] & \mathbb{C} \\
\mathcal{H}/(SL_2(\mathbb{Z})) \arrow[ur] &
\end{tikzcd}$$

commutes and $\hat{j}$ is actually the bijection between these equivalence classes and $\mathbb{C}$. That is, we have for all $z \in \mathbb{C}$, there is exactly one equivalence class of lattices having $j(\Lambda) = z$ and so we have classified all isomorphism classes of complex elliptic curves.

References

[1] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*, Springer, New York 2005

[2] Eberhard Freitag, Rolf Busam *Complex Analysis*, Springer, Berlin, Germany, second Edition, 2009