23MAC260 Elliptic Curves: Week 9

Last updated: April 4, 2024

Last week we discussed

- holomorphic and meromorphic functions
- lattices in the complex plane and doubly-periodic functions
- the Weierstrass $\wp$-function

This week we will use the Weierstrass $\wp$-function to understand the "shape" of complex elliptic curves.

1 Eisenstein series and the $\wp$-function

We start with a definition.

Definition 1.1. *Let L be a lattice in the complex plane, and $k \geq 3$ an integer. The* **Eisenstein series of weight k associated to L** *is defined as*

$$G_k(L) = \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^k}$$

Remarks:

- If $k \leq 2$, then the series above doesn't converge; hence our restriction to $k \geq 3$ in the definition.
- If k is odd then the terms in the sum corresponding to ω and $-\omega$ cancel, so $G_k(L) = 0$.

Sometimes we will just write G_k instead of $G_k(L)$.

In general for a given lattice L it is hard (or impossible) to give a simple formula for $G_k(L)$. But here's one example where we can:

Example: Let $L = \mathbb{Z} \oplus \mathbb{Z} \cdot i$, meaning the lattice spanned by the numbers 1 and i. So

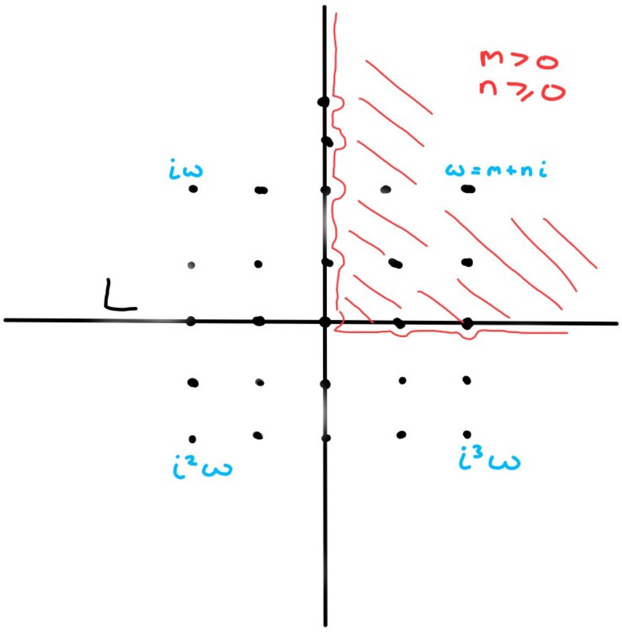
$$L = \{m + n\,i \mid m,\, n \in \mathbb{Z}\}$$

and therefore the Eisenstein series $G_k(L)$ is given by the formula

$$G_k(L) = \sum_{\substack{m,\, n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m + n\,i)^k}.$$

We claim that $G_6(L) = 0$.

To see this, consider the following picture showing the lattice L:



The key point to notice is that every element $\omega' \in L$ is of the form $\omega' = i^k \omega$ for some $\omega = m + ni$ with $m > 0$, $n \geq 0$ and $k = 0, 1, 2$ or 3. So we have

$$\begin{aligned} G_6(L) &= \sum_{\omega \neq 0} \frac{1}{\omega^6} \\ &= \sum_{m > 0, n \geq 0} \left(\frac{1}{(m + ni)^6} + \frac{1}{(i(m + ni))^6)} + \frac{1}{(i^2(m + ni))^6} + \frac{1}{(i^3(m + ni))^6} \right). \end{aligned}$$

But we have $i^6 = -1$ and $i^{12} = 1$ and $i^{18} = -1$, so for each m, n these 4 terms sum to 0, so we end up with $G_6(L) = 0$.

Eisenstein series and the $\wp$-function

Recall the definition of the Weierstrass $\wp$-function:

$$\wp_L(z) = \frac{1}{z^2} + \sum_{\omega \in L,\, \omega \neq 0} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

The significance of the Eisenstein series for us is that they appear as coefficients in the Laurent expansion of the Weierstrass $\wp$-function:

Theorem 1.2. *The Laurent expansion of $\wp_L(z)$ about 0 is given by*

$$\begin{aligned}\wp_L(z) &= \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}\,z^{2k} \\ &= z^{-2} + 3G_4z^2 + 5G_6z^4 + \cdots\end{aligned}$$

Corollary 1.3. *The Laurent expansion of the derivative $\wp_L'(z)$ about 0 is given by*

$$\wp_L'(z) = -2z^{-3} + 6G_4z + 20G_6z^3 + \cdots$$

Proof of Theorem. For $|z| < |\omega|$ we can write

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-(\frac{z}{\omega}))^2} - 1\right) = \frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^n}.$$

So if $|z| < \min\{|\omega| : \omega \in L, \omega \neq 0\}$ we have

$$\begin{aligned}\wp_L(z) &= \frac{1}{z^2} + \sum_{\omega\in L,\omega\neq 0}\frac{1}{\omega^2}\left(\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^n}\right) \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)\left(\sum_{\omega\in L,\omega\neq 0}\frac{1}{\omega^{n+2}}\right)z^n \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)G_{n+2}z^n\end{aligned}$$

and using the fact that $G_k = 0$ for k odd, we get the claimed result. □

The differential equation

We can put these expansions together to see that the Weierstrass $\wp$-function satisfies a differential equation.

Theorem 1.4. *Let L be a lattice in the complex plane, and $\wp_L(z)$ the associated Weierstrass $\wp$-function. Then we have*

$$\wp_L'(z)^2 = 4\wp_L(z)^3 - 60G_4\wp_L(z) - 140G_6.$$

Proof. We use the Laurent expansions for $\wp_L(z)$ and $\wp_L'(z)$ from Theorem 1.2 and Corollary 1.3. We calculate

$$\begin{aligned}\wp_L'(z)^2 &= 4z^{-6} - 24G_4z^{-2} - 80G_6 + \cdots \\ \wp_L(z)^3 &= z^{-6} + 9G_4z^{-2} + 15G_6 + \cdots \\ \text{which gives}\quad \wp_L'(z)^2 - 4\wp_L(z)^3 &= -60G_4z^{-2} - 140G_6 + \cdots\end{aligned}$$

Using the expansion for $\wp_L(z)$ again we get

$$\wp_L'(z)^2 - 4\wp_L(z)^3 + 60G_4\wp_L(z) = -140G_6 + \sum_{k=2}^{\infty} a_k z^k \quad \text{(for some } a_k \in \mathbb{C}) \qquad (*)$$

The left-hand side of $(*)$ is doubly-periodic with respect to L, with poles possibly at points of L. But the right-hand side has no negative powers of z, so it is holomorphic at $z = 0$, hence by periodicity holomorphic at all $\omega \in L$. We saw in Week 8 that a holomorphic doubly-periodic function is constant, and putting $z = 0$ on the right-hand side of $(*)$ we see that the constant value equals $-140G_6$. So we get

$$\wp_L'(z)^2 - 4\wp_L(z)^3 + 60G_4\wp_L(z) = -140G_6$$

as required. □

Theorem 1.4 is the key ingredient in connecting the Weierstrass $\wp$-function to elliptic curves. To make this more clear, let E_L denote the elliptic curve defined by the following equation:

$$E_L \;:\; y^2 = 4x^3 - 60G_4x - 140G_6$$

where G_4 and G_6 are the Eisenstein series associated to L. Then we have

Corollary 1.5. *Define a map*

$$\begin{aligned} \phi : \mathbb{C} &\to \mathbb{P}^2 \\ z &\mapsto \begin{cases} [\wp_L(z), \wp_L'(z), 1] & \textit{if } z \in \mathbb{C} \setminus L \\ [0, 1, 0] & \textit{if } z \in L \end{cases} \end{aligned}$$

Then the image $\phi(\mathbb{C})$ is contained in the elliptic curve E_L.

Proof. If $P \in \phi(\mathbb{C})$ then either $P = [0, 1, 0] = O$, the point at infinity, which is in E_L, or else $P = (x, y)$ with

$$x = \wp_L(z), \quad y = \wp_L'(z).$$

But then Theorem 1.4 shows that

$$y^2 = 4x^3 - 60G_4x - 140G_6$$

so $(x, y) \in E_L$ as claimed. □

2 The Equivalence Theorem

We have seen that the Weierstrass $\wp$-function maps the complex plane to an elliptic curve in $\mathbb{P}^2$. Now we give a more precise result, called the **Equivalence Theorem**. We state in in two parts, starting with:

Theorem 2.1 (Equivalence Theorem, Part 1). *Let* L *be a lattice in the complex plane. Then the map*

$$\begin{aligned} \phi : \mathbb{C} &\to \mathbb{P}^2 \\ z &\mapsto \begin{cases} [\wp_L(z), \wp'_L(z), 1] & \text{if } z \in \mathbb{C} \setminus L \\ [0, 1, 0] & \text{if } z \in L \end{cases} \end{aligned}$$

induces an isomorphism of groups

$$\mathbb{C}/L \cong E_L$$

where $\mathbb{C}/L$ *denotes the quotient of the group* $\mathbb{C}$ *by the subgroup* L*, and* E_L *denotes the elliptic curve defined by the equation*

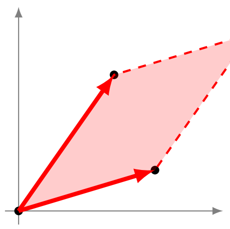
$$y^2 = 4x^3 - 60G_4x - 140G_6.$$

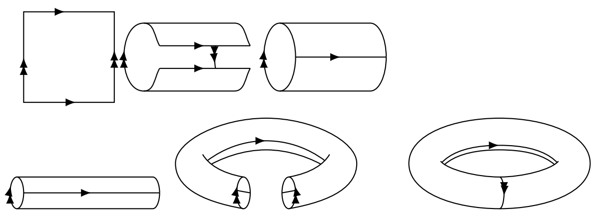
Part 1 says that the quotient of $\mathbb{C}$ by a lattice is isomorphic to an elliptic curve. But the converse is also true:

Theorem 2.2 (Equivalence Theorem, Part 2). *Let* $E \subset \mathbb{P}^2_{\mathbb{C}}$ *be an elliptic curve over the complex numbers. Then there exists a lattice* L *and an isomorphism of groups*

$$\mathbb{C}/L \cong E.$$

Parts 1 and 2 of the Equivalence Theorem together say that elliptic curves over the complex number are the "same thing" as quotients $\mathbb{C}/L$ of the complex numbers by a lattice.





These pictures[1] illustrate the geometry of the Equivalence Theorem: we can think of an elliptic curve as the space we get by "glueing" the opposite sides of the fundamental parallelogram, and the pictures show that this gives us a **torus**.

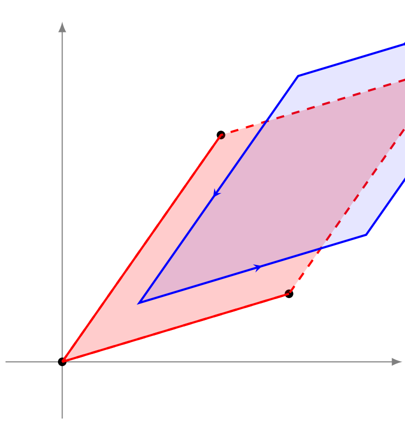
Now let's turn to sketching the proof of Part 1 of the Equivalence Theorem. More details can be found in Silverman, *The Arithmetic of Elliptic Curves*, Proposition 3.6 p.165.

Recall from last week:

[1] created by Andrew Stacey; taken from `https://tex.stackexchange.com/a/18246`

Theorem 2.3 (Residue Theorem)**.** *Let* f *be a meromorphic function. Let* γ *be a simple closed curve in* $\mathbb{C}$ *that does not pass through any pole of* f*, and let* $z_1, \dots, z_n$ *be the poles of* f *inside* γ*. Then*

$$\int_\gamma f(z)\,dz = 2\pi i \sum_{k=1}^{n} \operatorname{Res}(f, z_k).$$



We will apply this to a curve γ as in the picture, obtained by shifting the boundary of Π a bit to avoid points of L.

Key fact: If $f(z)$ is any doubly-periodic function with respect to L, then $\int_\gamma f(z)\,dz = 0$ because the contributions from opposite sides of the parallelogram cancel out.

Using this we can prove:

Lemma 2.4. *If* f *is any doubly-periodic function with respect to* L*, then*

1. $\sum_{w \in \Pi} \operatorname{Res}(f, w) = 0$.
2. $\sum_{w \in \Pi} \operatorname{ord}(f, w) = 0$.
3. $\sum_{w \in \Pi} \operatorname{ord}(f, w) \cdot w \in L$.

Sketch of proof. Part 1 follows by applying the Key Fact above to the function $f(z)$: the integral is zero, and so the sum of the resides of f must be zero too.

To deduce Part 2, now apply the Key Fact to the function $f'(z)/f(z)$, which is doubly-periodic with respect to L since f is. Problem Sheet 8 Question 2 shows that the reside of $f'(z)/f(z)$ at a point is exactly the order of f at that point, which proves the claim.

The proof of Part 3 can be found in the reference given above. □

Corollary 2.5 (to Statement 2 of Lemma)**.** *For any doubly-periodic function with respect to* L*, the numbers of zeroes and poles (counted with multiplicities) inside* Π *must be equal.*

Now we can move on to prove Part 1 of the Equivalence Theorem. Recall this said that the map

$$\begin{aligned} \phi : \mathbb{C} &\to \mathbb{P}^2 \\ z &\mapsto \begin{cases} [\wp_L(z), \wp_L'(z), 1] & \text{if } z \in \mathbb{C} \setminus L \\ [0, 1, 0] & \text{if } z \in L \end{cases} \end{aligned}$$

induces an isomorphism of groups

$$\mathbb{C}/L \cong E_L$$

- **Surjectivity:** first we prove that $\phi : \mathbb{C} \to E_L$ is **surjective**, which implies that $\mathbb{C}/L \to E_L$ is surjective also.

  To see this, let (x, y) be a point on E_L, and consider the function $\wp_L(z) - x$. This has a double pole at any point of L, so according to the Corollary it must have a zero inside Π too, say at $z = a$. Then since $\phi(a) \in E_L$ we know that $\phi(a) = (x, y)$ or $(x, -y)$, since these are the only points on the curve with first coordinate equal to x. In the first case we are done. In the second case, we replace a by $-a$: then

  $$\begin{aligned} \phi(-a) &= (\wp(-a), \wp'(-a)) \\ &= (\wp(a), -\wp'(a)) \\ &= (x, y) \end{aligned}$$

  since $\wp$ is even and $\wp'$ is odd. In either case we get a point in Π which maps to the point (x, y), so ϕ is surjective.

- **Injectivity:** To prove that ϕ induces an injective function $\mathbb{C}/L \to \mathbb{P}^2$, suppose $\phi(z_1) = \phi(z_2)$. We need to prove that $[z_1] = [z_2]$ in $\mathbb{C}/L$, meaning that $z_1 = z_2$ modulo L.

  Consider the doubly-periodic function $\wp(z) - \wp(z_1)$: this has zeroes at z_1, $-z_1$, and z_2. Again it has a double pole at a point of L, so it has exactly 2 zeroes (counted with multiplicity) inside Π. Hence these 3 values can't all be distinct modulo L.

  If $2z_1 \notin L$ then z_1 and $-z_1$ are distinct modulo L, so this means $z_2 = \pm z_1$ modulo L. But $\wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm\wp'(z_1)$ so in fact we must have $z_2 = z_1$ modulo L. Similarly if $2z_1 \in L$ we can show the function $\wp(z) - \wp(z_1)$ has a double zero at z_1 and is zero at z_2, so again we must have $z_2 = z_1$ modulo L.

- **Homomorphism:** Finally we say something about why ϕ is a group homomorphism. To see this, we need to prove that for any z_1 and z_2 we have

  $$\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2) \qquad (*)$$

  where the sum on the right-hand side is the sum of points on E_L.

To see this, we observe that since $\phi(0) = O$ by definition, the identity in $\mathbb{C}/L$ maps to the identity in E_L. So instead of $(*)$ we can prove the equivalent statement that if $z_1 + z_2 + z_3 = 0$ in $\mathbb{C}/L$, then $\phi(z_1) + \phi(z_2) + \phi(z_3) = O$ in E_L: in other words the points $\phi(z_1)$, $\phi(z_2)$, $\phi(z_3)$ lie on a line.

For simplicity assume that all 3 points are distinct and none of them equals O. Then they have homogeneous coordinates $[x_i, y_i, 1]$ for $i = 1, 2, 3$, where $x_i = \wp(z_i)$, $y_i = \wp'(z_i)$.

Now to prove that they lie on a line, it is equivalent to show that the following matrix has determinant zero when we set $z = z_3$:

$$\begin{pmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ 1 & \wp(z) & \wp'(z) \end{pmatrix}$$

This determinant is a doubly-periodic function of the form

$$F(z) = A + B\wp(z) + C\wp'(z)$$

where $C = x_1 - x_2$ which is nonzero by assumption. So $F(z)$ has a single pole of order 3 at each lattice point, and hence has 3 zeros inside Π by Corollary 2.5. Two of these zeroes are located at z_1 and z_2. By Part 3 of Lemma 2.4 if the third zero is ζ we have

$$z_1 + z_2 + \zeta \in L$$

hence $\zeta = -z_1 - z_2 = z_3 \bmod L$. Since F is doubly-periodic, we get $F(z_3) = F(\zeta) = 0$ as required. $\square$