MATH 470: Elliptic curves over $\mathbb{C}$ and Uniformization theorem

Frédéric Cai

27-01-2025

We will present the underlying connection between the geometric objects of *elliptic curves*, the algebraic curves defined by *Weierstrass equations* and *lattices* in $\mathbb{C}$, with the help of Weierstrass theory and the Uniformaization Theorem. There will be a few black boxes when we will get too close to algebraic geometry, especially when divisors and Riemann-Roch theorem are required. This presentation is largely based by chapter 6 of Silverman's *Arithmetic of Elliptic Curves*.

1 Elliptic Curves and Weierstrass Equations

Recall the previous definitions.

Definition 1.1. A *Weierstrass equation* in $\mathbb{C}$ can be written in the form

$$y^2 = x^3 + Ax + B. \tag{1.2}$$

We define the following quantities

$$\Delta = -16(4A^3 + 27B^2),$$
$$j = 1728(4A)^3/\Delta.$$

Then a (cubic) curve $\mathcal{C}$ defined by a Weierstrass equation is the locus of the above Equation (1.2) homogenized and viewed in $\mathbb{P}^2$.

Lemma 1.3. *a) If $\mathcal{C}$ and $\mathcal{C}'$ are two curves defined by a Weierstrass equation, then $\mathcal{C} \simeq \mathcal{C}'$ (as algebraic curves) if and only if their associated j value are the same i.e. $j(\mathcal{C}) = j(\mathcal{C}')$. Thus, this quantity is called the j-invariant.*

b) For any $j_0 \in \mathbb{C}$, there exists a curve defined by a Weierstrass equation whose j-invariant is j_0

Proof. Brute force calculations, but worth the try. See Silverman's Proposition III.1.4. □

We consider the definition of *smooth* or *non-singular* for an algebraic curve as having at all its points, at least one of its first partial derivative is non vanishing. We get the following result.

Lemma 1.4. *Let $\mathcal{C}$ be a curve defined by a Weierstrass equation. Then $\mathcal{C}$ is smooth if and only if its associated Δ is non zero.*

Proof. Suppose $\Delta \neq 0$. Since we are in $\mathbb{P}^2$, we will first see that the curve $\mathcal{C}$ with $\{f(x,y) = y^2 - x^3 - Ax - B = 0\}$ is not singular at the point at infinity $\mathcal{O} = [0:1:0]$. Homogenizing the equation,

$$F(X,Y,Z) = Y^2Z - X^3 - AXZ^2 - BZ^3,$$

we wee that

$$\frac{\partial F}{\partial z}(0) = 1 \neq 0,$$

hence $\mathcal{O}$ is not a singular point.
Wlog, suppose $\mathcal{C}$ is singular at $(0,0)$, which can be done since one can check that Δ is translation invariant. This implies

$$B = f(0,0) = 0, \quad A = \frac{\partial f}{\partial x}(0,0) = 0.$$

Then, the curve the equation $f(x,y) = y^2 - x^3 = 0$ has $\Delta = 0$, contradicting. $\mathcal{C}$ is smooth.

For the converse direction, we first observe that

$$\frac{\partial f}{\partial x} = -2x^2 - A, \quad \frac{\partial f}{\partial y} = 2y.$$

Then $\mathcal{C}$ is singular if and only if there is a point $(x_0, y_0) \in \mathcal{C}$ such that $2y_0 = -2x_0^2 - A = 0$. This means that there is a point $(x_0, 0)$ that would be a double root of the degree 3 polynomial $y_0^2 = 0 = x_0^3 + Ax_0 + B$, which is the case if and only if the discrimant of this polynomial $= -4A^3 - 27B^2 = -\Delta/16$ is 0. Hence, $\mathcal{C}$ non-singular implies $\Delta \neq 0$. ☐

We give the geometric definition of an elliptic curve.

Definition 1.5. An *elliptic curve* E over $\mathbb{C}$ $(E/\mathbb{C})$ is a non-singular algebraic curve of genus 1 with an identified point $\mathcal{O} \in E$

Our main idea in this section is that every elliptic curve can be written as a plane cubic, and conversely, every smooth Weierstrass plane cubic curve is an elliptic curve.

Theorem 1.6. *Let E be an elliptic curve over $\mathbb{C}$*

a) *There exists functions $x, y \in \mathbb{C}(E)$ the function field* ($\mathbb{C}(E)$*can be seen as rational functions on the curve*) *called Weierstrass coordinates such that the map*

$$\phi : E \longrightarrow \mathbb{P}^2 = [x : y : 1]$$

gives an isomorphism of $E/\mathbb{C}$ onto a curve defined by a Weierestrass equation, with $\mathcal{O} \longmapsto [0 : 1 : 0]$ satisfied.

b) *Conversely, every smooth cubic curve $\mathcal{C}$ given by a Weierstrass equation is an elliptic curve over $\mathbb{C}$ with base point $\mathcal{O} = [0, 1, 0]$.*

Proof. It requires a fair bit of algebraic geometry so we will black box it. The idea of b) is to use Riemann-Roch to see that $\mathcal{C}$ has genus 1. See Silverman's Proposition III.3.1. ☐

Hence, we have the bijection of sets

$$\{\text{Ellipitic curves } E\ \} \overset{\sim}{\longleftrightarrow} \left\{ \begin{array}{c} \text{Smooth curves } \mathcal{C} \text{ defined by} \\ \text{a Weierestrass equation } y^2 = x^3 + Ax + B \end{array} \right\},$$

where the $\mathcal{O} \in E$ point will alway correspond to the $[0 : 1 : 0]$ point. For our sake, we will take the right side as an equivalent definition of elliptic curves.

2 Lattices and Uniformization Theorem

We define a *lattice* to be $\Lambda \subset \mathbb{C}$ with $\Lambda = \{\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2\}$ such that $\omega_2/\omega_1 \in \mathcal{H}$.
Let $g_2 = g_2(\Lambda)$ and $g_3 = (\Lambda)$, and $\wp(z) = \wp(\Lambda, z)$ the Weierestrass $\wp$-function.

Lemma 2.1. *Let Λ a lattice. We define a curve $E/\mathbb{C}$ by $E : y^2 = 4x^3 - g_2(\Lambda) - g_3(\Lambda) \subset \mathbb{P}^2$. Then, the map*

$$\mathbb{C}/\Lambda \overset{\sim}{\longrightarrow} E,$$

$$z \longmapsto [\wp(z) : \wp'(z) : 1]$$

is an complex analytic and group isomorphism (*it is actually a complex Lie group isomorphism*).

Proof. We ommit it once again. We state the following facts that are used :vw

1) The equation $f(x) = 4x^3 - g_2 x - g_3$ has distinct roots, thus $\Delta(\Lambda) = g_2^3 - 27g_3^3 \neq 0$,

2) We have relation $\wp'^2 = 4\wp^3 - g_2\wp - g_3$ (that we proved in the previous weeks),

3) The map ϕ send $0 + \Lambda$ to $[0 : 1 : 0]$. The idea is that using rescaling $[\wp(z) : \wp'(z) : 1]\tilde{[}\frac{1}{z^2} : \frac{1}{z^3} : 1] = [z^3 : 1 : z^2]$, evaluated at $z = 0$ gives $[0 : 1 : 0]$.

See Silverman"s Proposition VI.3.6. □

Remark. The curve $E : y^2 = 4x^3 - g_2x - g_3$ is an ellipitic curve following fact 1) above. A change of variable will give the standard form we had earlier.

Maps in lattices are related to maps in elliptic curves.

Lemma 2.2. *Let Λ_1, Λ_2 lattices in $\mathbb{C}$.*

a) There is a bijection between

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \tilde{\longrightarrow} \left\{ \begin{array}{c} \textit{Holomorphic maps} \\ \varphi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \textit{with } \varphi(0) = 0 \end{array} \right\}$$

$$\alpha \longmapsto \varphi_\alpha, \quad \varphi_\alpha : z \mapsto \alpha z (\mathrm{mod} \Lambda_2).$$

b) Let E_1, E_2 elliptic curves defined as in Lemma 2.1. Then

$$\{\textit{Isogenies } E_1 \to E_2\} \tilde{\longrightarrow} \left\{ \begin{array}{c} \textit{Holomorphic maps} \\ \varphi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \textit{with } \varphi(0) = 0 \end{array} \right\}$$

$$\alpha \longmapsto \varphi_\alpha, \quad \varphi_\alpha : z \mapsto \alpha z (\mathrm{mod} \Lambda_2).$$

Proof. First part was Proved by Ludovic, using covering space. Also, see Silverman's Theorem VI.4.1 for the two parts. □

It follows immediately.

Corollary 2.3. *As defined as above, $E_1 \simeq E_2$ if and only if Λ_1 and Λ_2 are homothetic, i.e. $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}^*$.*

We know find a way to relate all elliptic curves with lattices. The following Theorem and Corollary are called the *Uniformisation theorem*.

Theorem 2.4. *For any $A, B \in \mathbb{C}$, $4A^3 - 27B^2 \neq 0$, there exists a unique lattice $\Lambda \in \mathbb{C}$ such that $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$*

Proof. Ludovic proved this result in his previous presentation. Also, see Proposition 1.4.3 of Diamond and Shurman. □

Corollary 2.5. *Let $E/\mathbb{C}$ be an elliptic curve. Then, there exists a unique lattice up to homotethy $\Lambda \in \mathbb{C}$ such that we have the isomorphism*

$$\phi : \mathbb{C}/\Lambda \tilde{\longrightarrow} E,$$

$$z \longmapsto [\wp(z) : \wp'(z) : 1].$$

Proof. Existence comes from using Theorem 2.4 on the Weierestrass equation (Equation (1.2)) corresponding to the elliptic curve (Theorem 1.6), then applying Lemma 2.1.
Uniqueness up to homotethy follows Corollary 2.3. □

To recap, we have showed that there is an isomorphism between the complex torus of some lattice and some ellipitc curves E_Λ, and that by the Uniformisation Theorem, that every elliptic curve is uniquely isomorphic to such elliptic curves E_Λ. We also get a correspondance between maps on those two objects, which actually gives us an equivalence of categories. Thus,

$$\left\{ \text{ Elliptic curves } \right\}_{/\simeq} \xleftrightarrow{\text{by Theorem 1.6}} \left\{ \begin{matrix} \text{Smooth curve defined} \\ \text{by Weierestrass} \\ \text{equations} \end{matrix} \right\}_{/\simeq} \xleftrightarrow[\text{by Theorem 1.6}]{\text{by Theorem 2.4, and Corollary 2.5}} \left\{ \begin{matrix} \text{Lattices} \\ \Lambda \subset \mathbb{C} \end{matrix} \right\}_{/\text{homothety}}$$

3 Construction of Lattices from Elliptic Curves

Our goal now is to construct a lattice from an elliptic curve, and that it will be the inverse of the map from Theorem 1.6, $phi : E \longrightarrow \mathbb{C}/\Lambda$.
We first define a useful object.

Definition 3.1. Let $\mathcal{C}$ be a smooth algebraic curve over $\mathbb{C}$. Then, $\Omega_\mathcal{C}$ is the *space of differentials* for the curve $\mathcal{C}$. It is a $\mathbb{C}(\mathcal{C})$-vector space ($\mathbb{C}(\mathcal{C})$ is the function field on $\mathcal{C}$, "rational functions on $\mathcal{C}$"), and is generated by symbols df, for $f \in \mathbb{C}(\mathcal{C})$ with the properties :

1) $d(x+y) = dx + dy$, $x, y \in \mathbb{C}(\mathcal{C})$
2) $d(xy) = xdy + ydx$, $x, y \in \mathbb{C}(\mathcal{C})$
3) da, $a \in \mathbb{C}$.

Remark. For a a non constant map of curves $\varphi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$, we get a natural map $\varphi^* : \mathbb{C}(\mathcal{C}_1) \longrightarrow \mathbb{C}(\mathcal{C}_2)$ which induces a pullback on the differentials

$$\Omega_{\mathcal{C}_2} \longrightarrow \Omega_{\mathcal{C}_1}$$
$$\varphi^*(\sum f_i dx_i) = \sum \varphi^*(f_i) d(\varphi^*(x_i))$$

Lemma 3.2. *Let $\mathcal{C}$ be a smooth algebraic curve over $\mathbb{C}$. The space of differentials over $\mathcal{C}$, $\Omega_\mathcal{C}$, is a 1-dimensional vector space over $\mathbb{C}(\mathcal{C})$.*

Proof. The idea is to look at the smooth curve (1-dimensional) in some *local coordinate* t at each point p. Then any function can be written in terms of this local coordinate $f(t)\mathbb{C}(t)$ around p. All differentials will then be of the form

$$d(f(t)) = f'(t)dt.$$

See Silverman's Proposition II.4.2. □

For the curve $E : y^2 = x^3 + Ax + B$, we get the differential $\omega = \frac{dx}{y}$, which we consider to be "nice enough", it is *regular*. The space of regular differentials of a curve is finite dimensional over $\mathbb{C}$. It is easier to see through the isomorphism

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E,$$
$$z \longmapsto [\wp(z) : \wp'(z) : 1],$$

that this choice is not totally arbitrary. We pullback the diffrential

$$\phi^*(\frac{dx}{y}) = \frac{d(\wp(z))}{\wp'(z)} = \frac{\wp'(z)}{\wp(z)} dz = dz.$$

Lemma 3.3. *Let $P \in E$, and τ_P be the translation map from E to itself : $X \longmapsto P + X$. Then the pullback of the differential $\omega = \frac{dx}{y}$ is $\tau_P^* \omega = \omega$, i.e. ω is translation invariant. Thus, this differential is called the invariant differential.*

Proof. Once again it is easier to see it through the torus, as $d(z+a) = dz$ for $a \in \mathbb{C}$. See Silverman's Proposition II.5.1. □

Now, we might look at how the integral on the elliptic curve with this differential works. Let's hypothetize a map

$$\begin{aligned} E/\mathbb{C} &\rightsquigarrow \mathbb{C} \\ P &\longmapsto \int_{\mathcal{O}}^{\mathbb{P}} \omega. \end{aligned}$$

Then, this map is not well-defined up to the $\mathrm{H}_1(E, \mathbb{Z}) = \mathbb{Z} \times \mathbb{Z}$ as there are multiple paths from $\mathcal{O}$ to P. The integral on non contractible paths on the torus are not well defined. However, integrating over the two closed paths generating the homology group, α and β, makes sense. Those numbers are called the *periods* of E :

$$\omega_1 = \int_\alpha \omega \quad \text{and} \quad \omega_2 = \int_\beta \omega.$$

Thus, any path from $\mathcal{O}$ to P is differ by a path homotopic to $n_1\alpha + n_2\beta$, for some integers $n_1, n_2 \in \mathbb{Z}$.
To see that the integral on two homotopic paths are the same, let γ_1, γ_2 homotopic paths from $\mathcal{O}$ to P. The concatenation $\gamma_2^{-1} \circ \gamma_1$ gives a closed region U on the torus. Then with the help of Stokes' Theorem,

$$\begin{aligned} \int_{\gamma_1} \omega - \int_{\gamma_2} \omega &= \int_{\gamma_2^{-1} \circ \gamma_1} \omega \\ &= \int_{\partial U} \omega = \int_U d\omega = 0, \end{aligned}$$

using $d\omega = 0$ (since ω is regular, so holomorphic).
Thus, considering the set $\Lambda = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}$, the following map is well defined,

$$\begin{aligned} F : E &\longrightarrow \mathbb{C}/\Lambda \\ P &\longmapsto \int_{\mathcal{O}}^{P} \omega \pmod{\Lambda}. \end{aligned}$$

The map F is a group homomorphism, since with translation invariant of ω,

$$\int_{\mathcal{O}}^{P+Q} \omega = \int_{\mathcal{O}}^{P} + \int_{P}^{P+Q} \omega = \int_{\mathcal{O}}^{P} \omega + \int_{\mathcal{O}}^{Q} \tau_P^* \omega = \int_{\mathcal{O}}^{P} \omega + \int_{\mathcal{O}}^{Q} \omega \pmod{\Lambda}.$$

In order to make Λ a lattice, we need to check that ω_1 and ω_2 are $\mathbb{R}$-linearly independent.

Lemma 3.4. *Let $E/\mathbb{C}$ an elliptic curve.*

a) Let α, β be a basis for $\mathrm{H}_1(E, \mathbb{Z})$. Then the periods $\omega_1 = \int_\alpha \omega$, and $\omega_2 = \int_\beta \omega$ are $\mathbb{R}$-linearly independent.

b) Let $\Lambda \subset \mathbb{C}$ be the lattice generetad by ω_1, ω_2. Then

$$\begin{aligned} F : E &\longrightarrow \mathbb{C}/\Lambda \\ P &\longmapsto \int_{\mathcal{O}}^{P} \omega \pmod{\Lambda} \end{aligned}$$

is an isomorphism.

Proof. a) We know it exists a lattice Λ_1 such that the map

$$\begin{aligned} \phi_1 : \mathbb{C}/\Lambda_1 &\longrightarrow 7E, \\ z &\longmapsto [\wp(z) : \wp'(z) : 1] \end{aligned}$$

is an isomorphism. Then $\phi_1^{-1} \circ \alpha$ and $\phi_1^{-1} \circ \beta$ form a basis for $\mathrm{H}_1(\mathbb{C}/\Lambda_1, \mathbb{Z})$, and actually $\mathrm{H}_1(\mathbb{C}/\Lambda_1, \mathbb{Z}) \simeq \Lambda_1$ (via $\gamma \mapsto \int_\gamma dz$). As mentionned earlier, the differential $\omega = \frac{dx}{y}$ pulls-back to $\phi_1^*(\frac{dx}{y}) = dz$ on $\mathbb{C}/\Lambda_1$). Then the periods

$$\omega_1 = \int_\alpha \omega = \int_{\phi_1^{-1} \circ \alpha} dz \quad \text{and} \quad \omega_2 = \int_\beta \omega = \int_{\phi_1^{-1} \circ \beta} dz$$

form a basis for Λ_1, thus are $\mathbb{R}$-linearly independent. Hence, the lattice Λ_1 corresponding to E is precisely the above $\Lambda = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}$, and that the map from the uniformization theorem $\phi = \phi_1$.

b) From just above, we get that the map

$$F \circ \phi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda$$
$$F \circ \phi(z) = \int_0^{\wp(z),\wp'(z)} \frac{dx}{y}$$

Since $F^*(dz) = \frac{dx}{y}$ and $\phi^*(\frac{dx}{y}) = dz$, then $(F \circ \phi)^*(dz) = dz$. Using Lemma 2.2, the map $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ has the form $\psi_\alpha(z) = \alpha z$, $\alpha \in \mathbb{C}^*$, but since $\psi_\alpha^*(dz) = \alpha dz$, we see that $(F \circ \phi)(z) = z$, the identity map. Since ϕ is an isomorphism, $F = \phi^{-1}$ is an isomorphism as well, and the inverse map !

□

Corollary 3.5. *The above map F is the inverse of ϕ.*

Thus, we get that the set of elliptic curves, attached with a precise invariant differential (E, ω) is isomorphic to set of lattices $\mathfrak{L}$ (thus not up to homotethy),

$$\{(E, \omega)\} \stackrel{\sim}{\longleftrightarrow} \mathfrak{L}.$$

4 Modular Forms on Lattices

We give a quick word on modular forms. There is a definition of modular fomrs on elliptic curves, which implies one on lattices, and this actually helps motivate how the analytic definiiton on the upper half plane is made.

Recall. We had from a previous week,

$$\mathfrak{L}/\mathbb{C}^* \simeq \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}.$$

We get the following definition, which actually come from a more abstract one on (E, ω).

Definition 4.1. A *weak modular form over $\mathbb{C}$ of weight k* is a function from the set of lattices $f : \mathfrak{L} \longrightarrow \mathbb{C}$ such that $f(\lambda\Lambda) = \lambda^{-k} f(\Lambda)$ for all $\lambda \in \mathbb{C}^*$, and all $\Lambda \in \mathfrak{L}$.

Using above *Recall*, we can redefine it in such way

$$f(\tau) := f(\Lambda_\tau) = f(\tau\mathbb{Z} \oplus \mathbb{Z}).$$

Then for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we get

$$\begin{aligned} f(\gamma\tau) &= f((\gamma\tau)\mathbb{Z} \oplus Z) = f((c\tau + d)^{-1}((a\tau + b)\mathbb{Z} \oplus (c\tau + d)\mathbb{Z})) \\ &= (c\tau + d)^{-k} f((a\tau + b)\mathbb{Z} \oplus (c\tau + d)\mathbb{Z})) = (c\tau + d)^k f(\tau). \end{aligned}$$

Thus, we get the familiar analytic definition of modular forms. We will dive more in depth on such modular forms in the following meetings.