

Modular Forms, Elliptic curves and Modular curves

Armand Perrin, Samy, Damian

May 7, 2025

Part I

The Modularity Theorem

The modularity theorem was first partially proven by Andrew Wiles in 1995 (before known as the Taniyama-Shimura conjecture) and led to a proof of Fermat's Last theorem (1637). The proof was then completed in 2001, showing a strong connexion between two kind of objects : modular forms and elliptic curves. In this part we will introduce some notions in order to understand the statement of the modularity theorem :

Theorem (Modularity Theorem) All elliptic curves over \mathbb{Q} are modular.

1 Riemann surfaces

A Riemann surface is a connected one-dimensional complex manifold, in this section we will specify what it means.

Definition 1.1 A n -manifold \mathcal{M} is a Hausdorff topological space locally homeomorphic to \mathbb{R}^n . This means that for every point $p \in \mathcal{M}$ there exists an open neighborhood U of p and an homeomorphism $\varphi : U \rightarrow \mathbb{R}^n$ to an open subset of \mathbb{R}^n . (U, φ) is called a chart.

Definition 1.2 Given two charts (U, φ) and (V, ψ) of an n -manifold \mathcal{M} with $U \cap V \neq \emptyset$ the map $\varphi \circ \psi^{-1} : \psi(U \cap V) \subset \mathbb{R}^n \rightarrow \varphi(U \cap V) \subset \mathbb{R}^n$ is called a transition map.

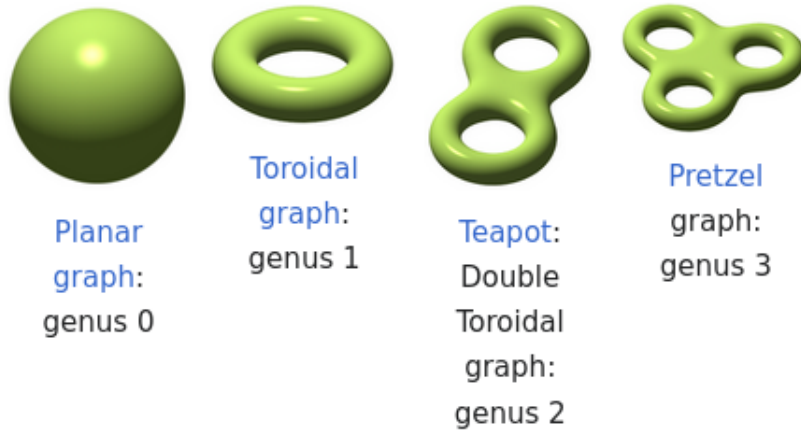
We want to extend theses notions to the complex numbers therefore we can replace \mathbb{R}^n by \mathbb{C}^n in the two previous definitions to define a complex n -manifold. A real n -manifold is said to be \mathcal{C}^k if it's transition maps are all \mathcal{C}^k similarly we will consider the complex 1-manifolds whose transition maps are not only smooth but also holomorphic, wich is a much more stronger constraint.

Definition 1.3 A Riemann surface is a connected complex 1-manifold whose transitions maps are holomorphic.

Definition 1.4 A map $f : \mathcal{M}_1 \rightarrow \mathcal{M}_2$ between two Riemann surfaces is said to be holomorphic if for each charts $(U, \varphi), (V, \psi)$ of $\mathcal{M}_1, \mathcal{M}_2$ respectively, the complex function $\psi \circ f \circ \varphi^{-1}$ is holomorphic over $\varphi(U \cap f^{-1}(V))$.

Definition 1.5 (Unformal)

Intuitively the genus of a Riemann surface is the number of its holes as a multiple torus.



More formally the genus of X can be defined as half the dimension of $H_1(X, \mathbb{C})$, the first singular homology group.

Theorem 1.6 (Classification of compact Riemann surfaces)

Two compact Riemann surfaces are homeomorphic to each other if and only if they have the same genus.

2 Lattices and complex tori

Definition 2.1 A **lattice** is a subset of \mathbb{C} of the form $\omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ with $\{\omega_1, \omega_2\}$ a \mathbb{R} -basis of \mathbb{C} .

This is equivalent to $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. We can suppose that $\frac{\omega_1}{\omega_2} \in \mathcal{H}$ for convenience.

Definition 2.2 We say that two lattices Λ and Λ' are isomorphic if there exists an $m \in \mathbb{C}$ such that $m\Lambda = \Lambda'$.

Proposition 2.3 Every lattice $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ is isomorphic to $\mathbb{Z} \oplus \tau\mathbb{Z}$ for some $\tau \in \mathcal{H}$.

Proof : $\omega_1 \neq 0$ so we can consider the isomorphic lattice $(\frac{1}{\omega_1})\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ with $\tau = \frac{\omega_2}{\omega_1}$, if $\tau \notin \mathcal{H}$ then $-\tau \in \mathcal{H}$ and $\mathbb{Z} \oplus -\tau\mathbb{Z} = \mathbb{Z} \oplus \tau\mathbb{Z}$.

Proposition 2.4 Two lattices $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ and $\Lambda' = \mathbb{Z} \oplus \tau'\mathbb{Z}$ are isomorphic if and only if $\tau' = \gamma \cdot \tau$ for some $\gamma \in SL_2(\mathbb{Z})$.

Definition 2.5 The complex tori associated to a lattice Λ is the abelian quotient group \mathbb{C}/Λ .

Proposition 2.6 The quotient topology over \mathbb{C}/Λ makes it a Riemann surface.

Definition 2.7 An **isomorphism** of complex tori $\varphi : \mathbb{C}/\Lambda \rightarrow \mathbb{C}/\Lambda'$ is a holomorphic group isomorphism. \mathbb{C}/Λ and \mathbb{C}/Λ' are then said to be isomorphic.

Theorem 2.8 Two complex tori \mathbb{C}/Λ and \mathbb{C}/Λ' are isomorphic if and only if Λ and Λ' are isomorphic.

Remark: The map $\Psi : \Lambda \mapsto \mathbb{C}/\Lambda$ is a bijection from the set of lattices to the set of complex tori that preserves isomorphism. Therefore, the categories of lattices up to isomorphism and complex tori up to isomorphism are equivalent.

3 Complex tori and elliptic curves

Definition 3.1 Given a sub-field \mathbb{K} of \mathbb{C} , an **elliptic curve** over \mathbb{K} is the set of points $(x, y) \in \mathbb{K}^2$ such that

$$y^2 = 4x^3 - ax - b$$

for some $(a, b) \in \mathbb{K}^2$ such that $a^3 - 27b^2 \neq 0$.

Remark: The condition $a^3 - 27b^2 \neq 0$ correspond to the curve being smooth.

Definition 3.2 An isogeny of elliptic curves is a map between two elliptic curves such that $\phi(x, y) = (R_1(x, y), R_2(x, y))$ with R_1 and R_2 two rational functions and that is also a group morphism. And an isogeny that is also a group isomorphism is called an isomorphism of elliptic curves.

Proposition 3.3 If there is an isogeny ϕ from E_1 to E_2 then there is an isogeny $\psi : E_1 \rightarrow E_2$ called the dual isogeny, and we say that E_1 and E_2 are isogenous. This defines an equivalence relation.

Remark: It can be shown that every curve that is the zero set of a polynomial of the form :

$$y^2z - (ax^3 + bx^2z + cxz^2 + dz^3)$$

is isogenous (if we adapt the previous definition) to a curve of the form

$$y^2z - (x^3 + bxz^2 + cz^3)$$

whose solutions of the form $(x, y, 1)$ satisfies the equation :

$$y^2 = x^3 + bx + c$$

Definition 3.4 Given a complex lattice Λ , the Weierstrass function \wp is defined by :

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

Proposition 3.5 \wp and \wp' are Λ -periodic.

Theorem 3.6 The Weierstrass function satisfies the differential equation :

$$\wp'^2 = 4\wp^3 - g_2(\Lambda)\wp - g_3(\Lambda)$$

for two complex numbers $g_2(\Lambda)$ and $g_3(\Lambda)$.

Proof : For z close to 0 we have :

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

We can change summation order as the series converges absolutely

$$\begin{aligned} &= \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) z^n \sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\omega^2} \frac{1}{\omega^n} \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) z^n G_{n+2} \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2} z^{2n} \quad \text{since } \forall n \geq 1 \quad G_{2n+1} = 0 \end{aligned}$$

Theredore we can compute :

$$\begin{aligned}\wp'(z) &= -\frac{2}{z^3} + \sum_{n=1}^{\infty} (2n+1)2nG_{2n+2}z^{2n-1} \\ \wp'(z)^2 &= \frac{4}{z^6} - \frac{4}{z^3} \sum_{n=1}^{\infty} (2n+1)2nG_{2n+2}z^{2n-1} + \left(\sum_{n=1}^{\infty} (2n+1)2nG_{2n+2}z^{2n-1} \right)^2 \\ &= \frac{4}{z^6} - \frac{24G_4}{z^2} + h(z) \quad \text{with } h \text{ holomorphic on a neighborhood of } 0\end{aligned}$$

On the other hand :

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + 3G_4z^2 + O(z^4) \\ \wp(z)^3 &= \frac{1}{z^6} + \frac{9G_4z^2}{z^4} + O(1) \\ 4\wp(z)^3 &= \frac{4}{z^6} + \frac{36G_4}{z^2} + g(z) \quad \text{with } g \text{ holomorphic on a neighborhood of } 0\end{aligned}$$

Then we obtain that $\wp' - 4\wp^3 + 60G_4\wp$ is holomorphic on a neighborhood of 0. But by Λ -periodicity this function is holomorphic on \mathbb{C} . By continuity and Λ -periodicity it is also bounded on \mathbb{C} and therefore constant. Let's denote $-g_3$ this constant (one can show with similar calculations that $g_3 = 140G_6$). We have then :

$$\wp'^2 = 4\wp^3 - g_2(\Lambda)\wp - g_3(\Lambda)$$

Theorem 3.7 The map :

$$z + \Lambda \rightarrow (\wp(z), \wp'(z))$$

is a bijection from nonzero points of \mathbb{C}/Λ to the elliptic curve associated to the equation

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

Definition-Proposition 3.8 (Group law) Given an elliptic curve E , \mathbb{C}/Λ its associated complex tori and two points $U, V \in E$. There exists two points $u, v \in \mathbb{C}/\Lambda$ such that $U = (\wp(u), \wp'(u))$ and $V = (\wp(v), \wp'(v))$. Let's consider the line of \mathbb{C}^2 going through U and V if $U \neq V$ and the tangent line to E at U if $U = V$. This gives us an line equation of the form

$$ax + by + c = 0$$

Lets consider the function f over \mathbb{C}/Λ such that:

$$f(z) = a\wp(z) + b\wp'(z) + c$$

We observe that f has zeros at points u, v . If $b \neq 0$ then f has exactly one other zero w and it is such that $u + v + w + \Lambda = 0 + \Lambda$. If $b = 0$ then $u + v + \Lambda = 0 + \Lambda$ then let $w = 0$ and again $u + v + w + \Lambda = 0 + \Lambda$. Lets define a point O "at infinity" to make notations coherent we denote $(\wp(0), \wp'(0)) := O$. Thus we define the group law on $E \cup \{O\}$ by :

$$U + V := (\wp(-u - v), \wp'(-u - v))$$

This makes the map : $\begin{cases} \mathbb{C}/\Lambda & \longrightarrow & E \cup \{O\} \\ z + \Lambda & \longmapsto & (\wp(z), \wp'(z)) \end{cases}$ a group isomorphism.

Theorem 3.9 Let E_Λ and $E_{\Lambda'}$ be some elliptic curves associated to the lattices Λ and Λ' respectively, then the following statements are equivalent :

- i) E_Λ and $E_{\Lambda'}$ are isomorphic
- ii) \mathbb{C}/Λ and \mathbb{C}/Λ' are isomorphic.
- iii) Λ and Λ' are isomorphic.

This theorem reduces the problem of parametrization of elliptic curves up to isomorphism to the much simpler problem of parametrization of lattices up to isomorphism. In what follows we will identify those 3 categories as the same mathematical objects.

4 Modular curves

In this section we are looking for a moduli spaces (i.e a space that parametrize) of elliptic curves up to isogeny.

Definition 4.1 Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$, we define the modular curve associated to Γ by $Y(\Gamma) := \{\Gamma\tau, \tau \in \mathcal{H}\}$, i.e the set of orbits of the action of Γ on \mathcal{H} . We also denote $Y_0(N)$ for $Y(\Gamma_0(N))$ and $Y_1(N)$ for $Y(\Gamma_1(N))$.

Proposition Each point of $Y(SL_2(\mathbb{Z}))$ correspond to a unique elliptic curve isomorphism class.

Proof : Points $\tau, \tau' \in \mathbb{C}$ are in the same orbit iff $\tau' = \gamma \cdot \tau$ for some $\gamma \in SL_2(\mathbb{Z})$. This is equivalent by proposition 2.4 to $\mathbb{Z} \oplus \tau\mathbb{Z}$ and $\mathbb{Z} \oplus \tau'\mathbb{Z}$ being isomorphic.

This last proposition says that $Y(SL_2(\mathbb{Z}))$ is a moduli space of elliptic curves up to isomorphism, we will now answer the question : what classes of elliptic curves does the modular curves $Y_0(N)$ and $Y_1(N)$ represent ?

Definition We call a pair (E, p) a pointed elliptic curve if E is an elliptic curve and p is a N -torsion point on E (seen as an abelian quotient group \mathbb{C}/Λ). And we say that two pointed elliptic curves (E, p) and (E', p') are isomorphic if there is an isomorphism $\phi : E \rightarrow E'$ such that $\phi(p) = p'$.

Definition We call a pair (E, C) an enhanced elliptic curve if E is an elliptic curve and C is a cyclic subgroup of E of order N . And we say that two enhanced elliptic curves (E, C) and (E', C') are isomorphic if there is an isomorphism $\phi : E \rightarrow E'$ such that $\phi(C) = C'$.

Theorem (Moduli spaces $Y_1(N)$ and $Y_0(N)$)

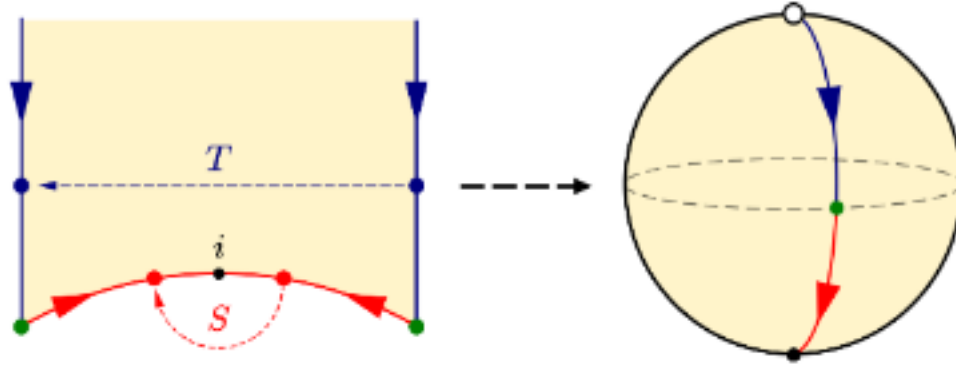
- Each point of $Y_1(N)$ correspond to a unique pointed elliptic curve isomorphism class.
- Each point of $Y_0(N)$ correspond to a unique enhanced elliptic curve isomorphism class.

It follows from Chow's theorem and the Rieman-Roch theorem that compact Riemann surfaces are complex algebraic curves, this and Theorem 1.6 gives us motivation to make $Y(\Gamma)$ a compact Rieman surface.

Definition The fundamental domain $\mathcal{D} \subset \mathcal{H}$ of the modular form $Y(\Gamma)$ is a region that contains exactly one point from each orbit of Γ action except some possible duplication on the edge.

Proposition The region $\mathcal{D} = \{\tau \in \mathcal{H} \mid |\tau| \geq 1 \text{ and } |Re(\tau)| \leq 1/2\}$ is a fundamental domain for $Y(SL_2(\mathbb{Z}))$.

After identification of duplicate points on the edge we see that $Y(SL_2(\mathbb{Z})) \simeq SL_2(\mathbb{Z}) \backslash \mathcal{D}$ is a punctured sphere.



Proposition $Y(SL_2(\mathbb{Z}))$ can be made a Riemann surface and compactified into $X(1)$ by adding a point at infinity.

Proposition Similarly for any congruence subgroup Γ , $Y(\Gamma)$ can be made a Riemann surface and compactified into $X(\Gamma)$ by adding a finite number of points. We will denote $X(\Gamma_0(N))$ as $X_0(N)$ for any integer N .

Definition A complex elliptic curve E is said to be **modular** if there exists an integer N such that there is a surjection holomorphic map φ from the modular curve $X_0(N)$ to E as Riemann surfaces. φ is called a modular parametrization of E .

TODO congruence subgroup, ex ref [1] G_2 $g_2(\Lambda)$ Eisenstein series genus...

References

- [1] PETER ZHOU. *THE MODULARITY THEOREM*. URL: <https://math.uchicago.edu/~may/REU2023/REUPapers/Zhou,Peter.pdf>.