[Silverman, "The arithmetic of elliptic curves"]

3. Elliptic curves and modular forms, I

We now discuss one of the topics closest to the theory of modular forms: elliptic curves. We begin with the basic "analytic / complex" theory, which is very classical and in fact motivated some of the earliest work on modular forms, including their definition.

Definition - An elliptic curve over $\mathbb{C}$ is a quotient $\mathbb{C}/\Lambda$, where $\Lambda \subset \mathbb{C}$ is a lattice (i.e. a discrete subgroup generating $\mathbb{C}$, in practice $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ with ω_1, ω_2 $\mathbb{R}$-linearly independant), viewed as a complex-analytic object.

What does this mean? One can view $\mathbb{C}/\Lambda$ as object of different kinds:

- as a group [but then $\mathbb{C}/\Lambda \simeq \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ for all Λ]
- as a topological space [but $\mathbb{C}/\Lambda$ is homeomorphic to $S^1 \times S^1$ for all Λ]
- as a Riemann surface by considering holomorphic / meromorphic functions on $\mathbb{C}/\Lambda$, which can be defined

as functions $f: \mathbb{C} \to \mathbb{C}$ holomorphic (or meromorphic) and Λ-periodic:

$\forall z \in \mathbb{C}, \forall w \in \Lambda, \ f(z+w) = f(z)$.

(In fact there are only constants if f is assumed holomorphic on $\mathbb{C}$: f is determined by its restriction to a bounded set such as $[0,1]\omega_1 \oplus [0,2]\omega_2$, which is compact, so f is bounded on all of $\mathbb{C}$, so is constant by Liouville's Theorem.)

The point is that from this point of view, there are different elliptic curves. Precisely, one can show that $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic if and only if Λ_1 and Λ_2 are homothetic: There exists $\lambda \in \mathbb{C}^*$ such that $\Lambda_2 = \lambda \Lambda_1$ (in $\mathbb{C}$).

Lemma. The set of isomorphism classes of elliptic curves ($\Leftrightarrow$ lattices in $\mathbb{C}$ modulo homothetes) is in "natural" bijection with $SL_2(\mathbb{Z})\backslash \mathbb{H}$, where $z \in \mathbb{H}$ corresponds to the elliptic curve $\mathbb{C}/(\mathbb{Z} \oplus z\mathbb{Z}) = \Lambda_z$

Thus a modular function ($SL_2(\mathbb{Z})$-invariant function) is "simply" a numerical invariant of elliptic

curves (over $\mathbb{C}$) ; a modular form [for $SL_2(\mathbb{Z})$] of weight k corresponds to a quantity $f(\Lambda)$ which is not quite invariant, but satisfies the rule

$$f(\lambda\Lambda) = \lambda^{-k} f(\Lambda).$$

Proof of the lemma - We can define a map

$$\mathcal{H} \longrightarrow \{\text{lattices } \Lambda \subset \mathbb{C}\}$$

by $$z \longmapsto \Lambda_z.$$

Step 1 - For every lattice $\Lambda \subset \mathbb{C}$, there exists $\lambda \in \mathbb{C}^\times$, $z \in \mathcal{H}$ s.t. $\Lambda = \lambda \Lambda_z$.

Indeed, write $\Lambda = \omega_1 \mathbb{Z} \oplus \omega_2 \mathbb{Z}$ for some ω_1, ω_2 in $\mathbb{C}^\times$, $\mathbb{R}$-linearly independant. In particular $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. Up to replacing ω_1 by $-\omega_1$, which does not change Λ, we can assume that $\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0$. Then

$$\Lambda = \omega_2 (z\mathbb{Z} \oplus \mathbb{Z}) = \omega_2 \Lambda_z$$

with $z = \frac{\omega_1}{\omega_2} \in \mathcal{H}$.

Step 2 - The action of $SL_2(\mathbb{Z})$ on $\mathcal{H}$ corresponds to the action of $SL_2(\mathbb{Z})$ on generators of lattices: $\Lambda = \omega_1 \mathbb{Z} \oplus \omega_2 \mathbb{Z} = g\Lambda$ for any $g \in SL_2(\mathbb{Z})$: for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ($g \in GL_2(\mathbb{R})$ so acts on $\mathbb{C} \simeq \mathbb{R}^2$)

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

gives the same lattice (because $g^{-1} \in SL_2(\mathbb{Z})$), and

$$\frac{\omega_1'}{\omega_2'} = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\frac{\omega_1}{\omega_2} + b}{c\frac{\omega_1}{\omega_2} + d}$$

$$= g \cdot \tau \quad \text{for the } \tau \text{ above.}$$

Finally, observe that a matrix in $GL_2(\mathbb{Z})$ with determinant -1 cannot transform a point in $\mathcal{H}$ to another.

□

Example - ("Arithmetic" Eisenstein series)

Given $\Lambda \subset \mathbb{C}$, define for $k \geq 3$ the sum

$$G_k(\Lambda) = \sum_{x \in \Lambda - \{0\}} \frac{1}{x^k}$$

This converges absolutely, and clearly

$$G_k(\lambda\Lambda) = \sum_{x \in \Lambda - \{0\}} \frac{1}{(\lambda x)^k}$$

$$= \lambda^{-k} G_k(\Lambda)$$

so this "is" a modular form of weight k.

Precisely, it corresponds to the function $\tau \mapsto G_k(\Lambda_\tau)$

$$G_k(\Lambda_\tau) = \sum_{(m,n) \in \mathbb{Z}^2 - \{0\}} \frac{1}{(m\tau + n)^k}$$

$$= \sum_{d \geq 1}' \sum_{(m,n) \in \mathbb{Z}^2 - \{0\}} \frac{1}{(m\tau + n)^k}$$

$$\gcd(m,n) = d$$

$$= \sum_{d \geq 1} \sum_{\substack{(a,b) \in \mathbb{Z}^2 - \{0\} \\ (a,b) = 1}} \frac{1}{d^k (a\tau + b)^k}$$

$$= \zeta(k) \sum_{\substack{(a,b) \in \mathbb{Z}^2 - \{0\} \\ (a,b)=1}} \frac{1}{(az+b)^k}$$

$$= 2\zeta(k) \; E_k(z)$$

using the parameterization of $\overline{N} \backslash SL_2(\mathbb{Z})$ used to compute Fourier expansions of Eisenstein/Poincaré series.

Remark – This perspective on modular forms can be very enlightening. For instance, the Hecke operator $T(n)$, for $n \geq 1$, can be defined by

$$T(n) f(\Lambda) = \sum_{\substack{\Lambda' \subset \Lambda \\ [\Lambda : \Lambda'] = n}} f(\Lambda')$$

(up to normalization). The definition we used is obtained from this by parameterizing sublattices of index n in Λ using explicit bases

$$\begin{cases} \omega_1' = a\omega_1 + b\omega_2 \\ \omega_2' = d\omega_2 \end{cases}, \quad \Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

for $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ of determinant n.

[See Serre, § 5 for the basic theory of Hecke operators in this language.]

The next surprising point is that elliptic curves are algebraic objects.

This results from the structure of spaces of elliptic functions for a given $\Lambda \subset \mathbb{C}$, i.e. of meromorphic

$$f : \mathbb{C} \longrightarrow \mathbb{C}$$

which are Λ-periodic. These basic facts are in fact somewhat similar to those concerning meromorphic modular functions: instead of $SL_2(\mathbb{Z})$ acting on $\mathcal{H}$, we consider Λ ($\simeq \mathbb{Z}^2$) acting on $\mathbb{C}$. In fact, since (i) Λ is abelian (ii) the action has no fixed points (iii) $\mathbb{C}/\Lambda$ is compact; the theory is a bit simpler.

For $f \neq 0$ Λ-periodic meromorphic, one proves first that

$$\begin{cases} \sum_{z \in \mathbb{C}/\Lambda} \operatorname{res}_z(f) = 0 \\ \sum_{z \in \mathbb{C}/\Lambda} \operatorname{ord}_z(f) = 0 \end{cases}$$

by integrating f along the boundary of a "fundamental domain" of $\mathbb{C}/\Lambda$, typically

$$F_\Lambda = \{ z = x\omega_1 + y\omega_2 \mid x, y \in [0,1] \}$$

(but maybe shifted a bit so that f has no zero/pole on the boundary), and then applying this to $\frac{f'}{f}$.

Cor. An elliptic function $f \neq 0$ has ≥ 2 poles [with multiplicity].

Proof. Indeed if there is only one, we would get
then $\operatorname{res}_z f = 0$ so in fact there is none.

□

Def. $\Lambda \subset \mathbb{C}$ lattice

The Weierstrass $\wp$-function of Λ is defined by

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

for $z \notin \Lambda$.

Prop. $\wp_\Lambda$ is Λ-elliptic and has only a double pole with residue 0 at $z \in \Lambda$.

Proof. This is not quite an application of periodicity by averaging: first, one has

$$\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} = O\left(\frac{1}{\lambda^3}\right), \quad z \notin \Lambda$$

so the series converges absolutely locally uniformly to define a $\left\{\begin{matrix}\text{holomorphic} \\ \text{meromorphic}\end{matrix}\right.$ function on $\left\{\begin{matrix}\mathbb{C}-\Lambda \\ \mathbb{C}\end{matrix}\right.$ with a double pole at 0.

Next, differentiating gives

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

which is elliptic by averaging and absolute convergence. Then one checks that $\wp_\Lambda^2(z+\lambda) - \wp_\Lambda^2(z)$ is independent of z, and by putting $z = -\frac{\lambda}{2}$

implies that this constant is 0 for all λ (because $\wp_\Lambda(-z) = \wp_\Lambda(z)$, which is elementary).

□

Prop. (1) Any meromorphic elliptic function is a rational function of $\wp_\Lambda$ and $\wp_\Lambda'$.

(2) $\wp_\Lambda$, $\wp_\Lambda'$ are related by the equation

$$\wp_\Lambda'^2 = 4\wp_\Lambda^3 - 60\, G_4(\Lambda)\,\wp_\Lambda - 140\, G_6(\Lambda)$$

Proof of (2): one checks by direct expansion that

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{k=1}^{+\infty} (2k+1)\, G_{2k+2}\, z^{2k}$$

and then that

$$\wp_\Lambda'^2 - 4\wp_\Lambda^3 + 60\, G_4(\Lambda)\,\wp_\Lambda + 140\, G_6(\Lambda)$$

is a meromorphic elliptic function without pole at $z \in \Lambda$ [the corresponding coefficient of z^{-6}, z^{-4}, z^{-2} cancel out], hence is constant. But the constant term also vanishes.

□

Thus, given Λ, we have a well-defined map

$$\varphi_\Lambda : \mathbb{C}/\Lambda - \{0\} \longrightarrow \{(z,w) \in \mathbb{C}^2 \mid w^2 = 4z^3 - az - b\}$$

with $\begin{cases} a = -60\, G_4(\Lambda), \\ b = -140\, G_6(\Lambda). \end{cases}$

Is this map surjective? What values of a, b can one obtain? The answer is given by the following:

Proposition - (1) φ_Λ is bijective

(2) The polynomial

$$4X^3 - 60\, G_4(\Lambda) X - 140\, G_6(\Lambda)$$

in $\mathbb{C}(X)$ has no multiple root

(3) Conversely, for any a, b in $\mathbb{C}$ with $X^3 + aX + b$ without multiple root, there is a Λ s.th $\begin{cases} a = -60\, G_4(\Lambda) \\ b = -140\, G_6(\Lambda) \end{cases}$

and Λ is unique if one takes isomorphism into account properly.

In other words: elliptic curves, initially defined complex-analytically, turn out to be "the same" as certain "algebraic curves", i.e, solution sets of certain polynomial equations.

This is the beginning of the second part of the theory linking modular forms and elliptic curves.