Elliptic Curves and Automorphic Forms

Emre Can Sertöz

30.04.14

1 Warmup

Here are a few reminders of the common notions we will be using. Remember we are always working over $\mathbb{C}$. Also, E and E' will be used denote an elliptic curve.

1. A genus 1 non-singular complete curve is not an elliptic curve! Only when such a curve is taken together with a group structure, the pair is called an elliptic curve. Alternatively, one could 'mark' a point on the curve and this will identify a unique group structure on the curve which uses the marked point as identity. Nevertheless, the pair of a genus 1 non-singular complete curve with a point (or a group structure) is denoted by a single letter, a variant of E.

2. A morphisms of elliptic curves are by definition holomorphic maps that are also group homomorphisms. Recall that all holomorphic maps between non-singular complete curves are also algebraic.

3. An isogeny $\phi : E \to E'$ is a morphism of elliptic curves with finite kernel. Note a morphism (between elliptic curves) is either the constant map to the identity or it is an isogeny.

4. A n-isogeny is an isogeny with cyclic kernel of order n.

5. At times it is useful to consider 'enhanced' elliptic curves, that is elliptic curves coupled with additional data; with yet another point or with a subgroup. For instance the curve $Y_1(N) = Y(\Gamma_1(N))$ parametrizes the isomorphism classes of pairs (E, Q) where $Q \in E$ and order of Q is N. Note (E, Q) is isomorphic to (E', Q') if there exists an isomorphism between E and E' mapping Q to Q'. For another instance, the curve $Y_0(N) = Y(\Gamma_0(N))$ parametrizes the isomorphism classes of pairs (E, C) where $C \subset E$ is a cyclic subgroup of order N.

6. Let $[E, Q]$ denote the isomorphism class of (E, Q). Let $E_\tau = \mathbb{C}/\langle \tau, 1\rangle$. One can show 'by-hand' that as sets $Y_1(N) = \{[E_\tau, \frac{1}{N}] \mid \tau \in \mathbb{H}\}$.

7. Given the class $\zeta = [E_\tau, \frac{1}{N}]$ we can find all enhanced curves up to isomorphism that are p-isogenous images of ζ, where p is prime. We denote the set in question by ${}_N I_p(\zeta) = \{[E', Q'] \mid \exists$ a p-isogeny $(E, Q) \to (E', Q')\}$. Then we have the following equality of sets:

$$ {}_N I_p(\zeta) = \{[E_{\frac{\tau+l}{p}}, \frac{1}{N}] \mid l = 0, \ldots, p-1\} \bigcup \{[E_{p\tau}, \frac{p}{N}] \mid \text{if } p \text{ does not divide } N\}\,. $$

   It is a good exercise to prove this last statement. If there is crushing demand, I will outline the argument.

2 Cusp, Modular and Automorphic Forms as sections of line bundles

Recall $\mathrm{GL}_2^+(\mathbb{Q})$ are two-by-two matricies with rational entries and positive determinant. These matricies act on the upper half plane as usual. We let $\mathrm{GL}_2^+(\mathbb{Q})$ act on functions $f : \mathbb{H} \to \mathbb{C}$ from the right. Let $f : \mathbb{H} \to \mathbb{C}$ and $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ then we define the *weight* k operator $[\alpha]$ such that $f[\alpha]_k : \mathbb{H} \to \mathbb{C}$:

$$f[\alpha]_k(\tau) = \det(\alpha)^{k-1}(\alpha_{21}\tau + \alpha_{22})^{-k} f(\alpha \cdot \tau)\,.$$

If we fix k this gives an action of $\mathrm{GL}_2^+(\mathbb{Q})$ on functions from $\mathbb{H}$ to $\mathbb{C}$. Let us call this the *weight* k *action.*

(Nevermind the determinant, mostly we will be working with the standard linear group and hence the determinant will be 1. However, it will be important to consider this general case for the Hecke operators.)

Definition 1. *Let* $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ *be a congruence subgroup. Let* f *be a holomorphic function on* $\mathbb{H}$ *such that*

1. f *is fixed by the weight* k *action of* Γ*, e.g.* $\forall \alpha \in \Gamma \; f = f[\alpha]_k$,
2. $\forall \gamma \in \mathrm{SL}_2(\mathbb{Z}) \; f[\gamma]_k$ *is holomorphic at* $i\infty$.

Then we call f *a* modular form of weight k associated to Γ. *The vector space of all such modular forms is denoted by* $\mathcal{M}_k(\Gamma)$.

A few remarks are in order. If a holomorphic function $g : \mathbb{H} \to \mathbb{C}$ is translation invariant by $h \in \mathbb{Z}_+$, that is if $g(t + h) = g(t)$, then g factors through the quotient

$$q_h : \mathbb{H} \to D^* = \{z \in \mathbb{C} \mid 0 < |z| < 1\} \qquad t \mapsto \exp(\frac{2\pi i t}{h})\,.$$

In other words, there is a holomorphic map $\tilde{g} : D^* \to \mathbb{C}$ such that $g(t) = \tilde{g}(\exp(\frac{2\pi i t}{h}))$. We say g is holomorphic at $i\infty$ if $\tilde{g}$ has a holomorphic extension to the unpunctured disk $D = \{z \in \mathbb{C} \mid |z| < 1\}$. If $h = \min\{l \in \mathbb{Z}_+ \mid \forall z \in \mathbb{H} \quad g(z + l) = g(z)\}$, then the power series expansion of $\tilde{g}$ at the origin will be referred to as the *Fourier series expansion of* g *at* $i\infty$.

The next point to consider is if $f[\gamma]_k$, mentioned in the second condition, is invariant under any translation. To see that it is, note that a congruence group contains by definition the normal subgroup $\Gamma(N) = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$ of $\mathrm{SL}_2(\mathbb{Z})$ for some N. Hence, every conjugate of a congruence subgroup contains $\Gamma(N)$ which in turn contains translations by N. Hence, for any f fixed by the weight k action of Γ we can talk about the Fourier series expansion at $i\infty$ of $f[\gamma]_k$ $\forall \gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Let us cast this definition into a more geometric setting. For this we begin with:

Lemma. *All holomorphic line bundles on the upper half plane are trivial.*

For a proof of this result see Theorem 1 in the Appendix.

Let $p : \mathbb{H} \to Y(\Gamma) = \Gamma\backslash\mathbb{H}$ be the projection map and L a line bundle on $Y(\Gamma)$. By the Lemma above we have an isomorphism $\mathbb{H} \times \mathbb{C} \to p^*L$, fix one and consider the diagram:

$$\begin{array}{ccc} \mathbb{H} \times \mathbb{C} \cong p^*L & \longrightarrow & L \\ \downarrow & & \downarrow \\ \mathbb{H} & \longrightarrow & Y(\Gamma) \end{array}$$

By universal property of the pullback, the action of Γ on the base extends to an action on the pullback bundle and hence on $\mathbb{H} \times \mathbb{C} \to \mathbb{H}$. Note this action does not fix the base, the action on the line bundle followed by the projection will be the standard action on the base. Conversely, if we have a Γ action on the trivial line bundle over $\mathbb{H}$ then the quotient is a line bundle on $Y(\Gamma)$. In fact, this gives a one to one correspondence between the two sets $\{(L, \mu) \mid L \in \mathrm{Pic}(Y(\Gamma)),\ \mu : p^*L \xrightarrow{\sim} \mathbb{H} \times \mathbb{C}\}$ and $\{\Gamma$ actions on $\mathbb{H} \times \mathbb{C} \to \mathbb{H}$ where the action is linear on each fibre$\}$.

Given a Γ action on $\mathbb{H} \times \mathbb{C}$, choose $\alpha \in \Gamma$ and $(\tau, t) \in \mathbb{H} \times \mathbb{C}$. Then $\alpha \cdot (\tau, t) = (\alpha \cdot \tau, j_\alpha(\tau)t)$ for some constant $j_\alpha(\tau) \in \mathbb{C}^*$. Due to the associativity of the group action, this $j : \Gamma \times \mathbb{H} \to \mathbb{C}$ must satisfy the so-called *cocycle condition*,

$$j_{\alpha'\alpha}(\tau) = j_{\alpha'}(\alpha \cdot \tau) j_\alpha(\tau)\,.$$

Conversely any $j : \Gamma \times \mathbb{H} \to \mathbb{C}$ satisfying the cocycle condition will yield an action of Γ on $\mathbb{H} \times \mathbb{C}$. Therefore, the picard group of $Y(\Gamma)$ and the set of cocycles are closely related.

Let $j(\alpha, \tau) = (\alpha_{21}\tau + \alpha_{22})$. Notice that this is a cocycle and so is every power j^k for $k \in \mathbb{Z}$. Let L^k_Γ be the line bundle on $Y(\Gamma)$ corresponding to j^k, that is the quotient of $\mathbb{H} \times \mathbb{C}$ by the Γ action induced by j^k.

Check that $L^2_\Gamma \cong \Omega^1_{Y(\Gamma)}$. Moreover, $L^{2n}_\Gamma \cong \Omega^{\otimes n}_{Y(\Gamma)}$. Observing that $L^k \bigotimes L^m \cong L^{k+m}$ it seems natural to define $\Omega^{\frac{1}{2}}_{Y(\Gamma)} := L^1$. It is important to note that, the cotangent bundles and its powers are mapped back to themselves under any isomorphism of $Y(\Gamma)$, because these objects are natural. In general, sections of the cotangent bundle can be pulled back by any morphism. In particular L^{2k} and its sections can be acted upon by automorphisms of the base curve. In fact, for various Γ, sections of L^k_Γ can be related. Hence, out of all the possible cocycles, these j^k's seem to be the most useful.

Interpreting the line bundle L^{2n} as the nth tensor power of the canonical bundle, $\Omega^{\otimes n}_{Y(\Gamma)}$, allows us to choose a natural extension of the line bundle to the projective curve $X(\Gamma)$, the extension will simply be $\Omega^{\otimes n}_{X(\Gamma)}$. This is a blessing because for arbitrary line bundles on a non-complete curve, there is no unique extension to the completion of the curve.

We observe the following natural bijection:

$$\{f : \mathbb{H} \to \mathbb{C} \mid \text{holomorphic and } \Gamma \text{ invariant under the weight } k \text{ action} \leftrightarrow H^0(L^k_\Gamma)\}\,.$$

The action is roughly given by $f \mapsto f(\,\mathrm{d}z)^{\otimes n}$. This explains what the first condition in Definition 1 really means. We are basically studying holomorphic differential tensor $k/2$-forms on the quotient curve. To interpret the second condition we introduce the following term:

Definition 2. *A* cusp *associated to a congruence subgroup* Γ *is a point in* $X(\Gamma) \setminus Y(\Gamma)$.

The term is misleading since there are no singularities on these curves, hence no cusps! But the fundamental domain in $\mathbb{H}$ corresponding to the group action of Γ in the Poincaré disk model of $\mathbb{H}$

will touch the boundary of the disk at what look like cusps. Those boundary points correspond in a very natural way to the cusps just defined. Hence the name.

Now given sections of $\Omega^{\otimes n}_{Y(\Gamma)}$, we may try to extend them to sections of $\Omega^{\otimes n}_{X(\Gamma)}$. If the sections have essential singularities at the cusps, there is no way to extend them as algebraic sections. However, if the singularities are mild then we can extend them as meromorphic sections of $\Omega^{\otimes n}_{X(\Gamma)}$. This is what the second condition in Definition 1 guarantees. Hence a modular form of weight k extends to a meromorphic section of $\Omega^{\otimes \frac{k}{2}}_{X(\Gamma)}$. Note that the modular form corrsenponds to a section that is holomorphic outside of the cusps, so the singularities may lie only in the set of cusps. In fact, one can identify precisely a divisor $D(k, \Gamma)$ such that there is a natural isomorphism between $\mathcal{M}_k(\Gamma)$ and the global sections of the twisted line bundle $\Omega^{\otimes \frac{k}{2}}_{X(\Gamma)}(D(k, \Gamma))$. Explicit calculations can be found in Chapter 3 of [2].

Definition 3. *The* cusp forms *are modular forms whose Fourier series expansion at the cusps have 0 as the constant term. The vector space of cusp forms of weight k associated to Γ are denoted by $S_k(\Gamma)$.*

It turns out that the cusp forms of weight 2 are precisely the holomorphic 1-forms on the Riemann surface $X(\Gamma)$. That is, there is a natural isomorphism $\mathcal{S}_2(\Gamma) \cong H^0(\Omega_X)$.

We give the following definition for the sake of completeness. We will not use it and there is a version of this definition that looks very much like Definition 1.

Definition 4. *The* automorphic forms of weight k corresponding to Γ *are functions $f : \mathbb{H} \to \mathbb{C}$ that correspond to meromorphic sections of $\Omega^{\otimes \frac{k}{2}}_{X(\Gamma)}$.*

Warning: I am not sure how natural the half tensor powers are and I am not quite sure if our L^k for odd k is invariant under the isomorphisms of the base curve. If you know, let me know and I will add it here. The point of concern is that, any line bundle on a genus g curve which has a 'square-root' will have a total of 2^{2g} distinct square-roots. Why is the one we picked immune to isomorphisms? Or is it immune to begin with?

3 Petersson inner product

Let $f, g \in \mathcal{S}_k(\Gamma)$. The Petersson inner product on the space of cusp forms is defined as:

$$\langle f, g \rangle = \int_{\Gamma \backslash \mathbb{H}} f \cdot \bar{g} \frac{dxdy}{y^{2-k}}$$

For $k = 2$ there is a natural interpretation of this inner product as is described in [4]. However, I don't know how to do something similar for higher k. If you do, please let me know.

4 Appendix

Theorem 1. *All holomorphic line bundles on a contractible complex manifold of dimension one are trivial.*

Proof. There are various generalizations of this fact. However, even non satisfactory generalizations seem to be advanced. So let us be satisfied with this mediocre result.

Let X be the complex manifold of dimension one. Using the exponential sequence and the fact that X is contractible we obtain

$$H^1(\mathcal{O}_X) \cong H^1(\mathcal{O}_X^*) \,.$$

The latter cohomology is isomorphic to the picard group of X. Hence we need only show that $H^1(\mathcal{O}_x)$ is trivial.

But, this follows immediately in the case $\dim X = 1$ and X simply connected by the Poincaré $\bar{\partial}$-Lemma. □

References

[1] Daniel Huybrechts *Complex Geometry, An Introduction.* Springer-Verlag 2005.

[2] Fred Diamond & Jerry Shurman. *First course in modular forms.* Springer-Verlag 2005.

[3] J.S. Milne. *Modular Functions and Modular Forms.* Online script.

[4] H. Darmon, F. Diamond & R. Taylor. *Fermat's Last Theorem.* Online script. May 24 2000.