The Modularity Theorem for Jacobians

Kendra Plante

One of the most important developments in number theory in recent times was the discovery of how to associate certain elliptic curves to certain modular forms. More specifically, there is a correspondence between elliptic curves over $\mathbb{Q}$ and weight 2 eigenforms. This is known as the *modularity theorem*. In this paper, we will build up the necessary background to understand the statement of the theorem. Furthermore, we will describe one direction of this correspondence, i.e. how an elliptic curve arises given a normalized weight 2 newform. In doing so, we will also develop a more refined notion of modularity via the language of Jacobians.

1 Preliminary Notions

We will begin with some basic definitions. The idea of a modular form is a function with "nice" symmetry properties. The relevant notion of symmetry is captured in a certain class of subgroups of $SL_2(\mathbb{Z})$ called *congruence subgroups.*

Definition 1. *The principle congruence subgroup $\Gamma(N)$ of level N is*

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

Definition 2. *A subgroup of $SL_2(\mathbb{Z})$ is called a congruence subgroup of level N if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$.*

There are many examples of congruence subgroups, but for our purposes, it suffices to focus on one,

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

These congruence subgroups act on the upper half plane by left multiplication. We then consider the orbit space of this action.

Definition 3. *The modular curve $X(\Gamma)$ of level N with respect to Γ is*

$$X(\Gamma) = \Gamma/\mathcal{H}^*, \qquad \mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$$

In the important special case when, $\Gamma = \Gamma_0(N)$, we use the notation $X_0(N) = X(\Gamma_0(N))$.

We'll take a moment to unpack this definition and understand the geometry. Consider $X(\Gamma)$ as a topological space with the quotient topology induced by $\pi : \mathcal{H}^* \to X(\Gamma)$. Since Γ is finite index in $SL_2(\mathbb{Z})$ for any congruence subgroup Γ, its action on $\mathcal{H}$ is properly discontinuous. This ensures that $X(\Gamma)$ is Hausdorff as a topological space. We can then define charts on $X(\Gamma)$ that make it into a Riemann surface. The addition of the rational points and the point at infinity, in the definition of $\mathcal{H}^*$, serve the purpose of compactification.

Proposition 1. *$X(\Gamma)$ has the structure of a compact Riemann surface.*

From here, we have enough background to state the first version of the modularity theorem, in terms of holomorphic maps of Riemann surfaces.

Theorem 1. *Let E be a complex elliptic curve with $j(E) \in \mathbb{Q}$. Then for some positive integer N, there exists a surjective holomorphic function of compact Riemann surfaces*

$$X_0(N) \to E$$

This is a powerful result, but it does not elucidate where the elliptic curve comes from, nor how modular forms fit into the picture. For these purposes, we will need to build up more material.

2 Modular Forms

Let $f : \mathcal{H} \to \mathbb{C}$ be a meromorphic function on the upper half plane. For some $k \in \mathbb{Z}$ and some congruence subgroup Γ, define the weight k operator $[\gamma]_k$ by

$$(f[\gamma]_k)(\tau) = (c\tau + d)^{-k} f(\gamma(\tau))$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $\tau \in \mathcal{H}$. If f is invariant under this operator, i.e. $f[\gamma]_k = f$ for all $\gamma \in \Gamma$, then we say that f is *weakly modular of weight k with respect to* Γ.

One can show that a weakly modular holomorphic function has a Fourier expansion on the punctured disc $D/\{0\}$, $D = \{z \in \mathbb{C} : |z| < 1\}$, given by

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n q_h^n$$

for $q_h = e^{2\pi i \tau / h}$. Suppose we can extend f holomorphically to the full disc D. Then we say f is *holomorphic at* ∞, and we conclude that the Fourier expansion of f reduces to

$$f(\tau) = \sum_{n=0}^{\infty} a_n q_h^n$$

We call this the q expansion of f. We are now able to define what we mean by a modular form with respect to a congruence subgroup.

Definition 4. *Let $f : \mathcal{H} \to \mathbb{C}$. Suppose Γ is a congruence subgroup and $k \in \mathbb{Z}$. Then we call f a modular form of weight k with respect to Γ if*

1. *f is holomorphic*
2. *f is weakly modular of weight k with respect to Γ*
3. *$f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$.*

In this paper, however, we will be especially concerned with a very important subclass of modular forms, called cusp forms.

Definition 5. *If $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight k with respect to Γ, and $a_0 = 0$ in the q expansion of $f[\alpha]_k$ for all $\alpha \in SL_2(\mathbb{Z})$, then we call f a cusp form of weight k with respect to Γ.*

We let $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$ respectively denote the set of modular forms and cusp forms of weight k with respect to Γ.

We now illustrate an important connection between modular forms and modular curves. Let $\Omega^1_{\text{hol}}(X(\Gamma))$ denote the complex vector space of degree 1 holomorphic differentials on $X(\Gamma)$. Then we have the following equivalence.

Proposition 2. *Let Γ be a congruence subgroup. Then we have an isomorphism of complex vector spaces*

$$\begin{aligned} \omega : S_2(\Gamma) &\to \Omega^1_{\text{hol}}(X(\Gamma)) \\ f &\mapsto (\omega_j) \end{aligned}$$

where (ω_j) pulls back to $f(\tau)d\tau \in \Omega^1_{\text{hol}}(\mathcal{H})$.

This is a special case of a much more general correspondence between automorphic forms (the meremorphic analogue of a modular form) and differentials on modular curves, but for the purposes of this paper, the above is sufficient.

Now, for a general Riemann surface X, consider the dual space $\Omega^1_{\text{hol}}(X)^\wedge = \hom_{\mathbb{C}}(\Omega^1_{\text{hol}}(X), \mathbb{C})$. We know from analysis that functionals of this type are given by integrals against the differential. Furthermore, complex analysis allows us to represent these integrals very neatly.

If X has genus g, then it is conformally equivalent to a sphere with g handles. The integral of a differential on X along any curve can thus be broken up into $2g$ integrals, half of them integrating around latitudinal loops on X, and the other half integrating around longitudinal loops on X. We thus conclude

$$\Omega^1_{\text{hol}}(X)^\wedge = \bigoplus_{j=1}^{2g} \mathbb{R} \int_{X_j}$$

With this perspective, it is natural to consider the subgroup given by the first homology of X, i.e.

$$H_1(X, \mathbb{Z}) = \bigoplus_{j=1}^{2g} \mathbb{Z} \int_{X_j}$$

Forming the quotient gives us the object we call the Jacobian.

Definition 6. *The Jacobian of X is the quotient group*

$$\operatorname{Jac}(X) = \Omega^1_{\text{hol}}(X)^\wedge / H_1(X, \mathbb{Z})$$

The Jacobian is more than a group. It naturally has the structure of a g dimensional complex torus

$$\operatorname{Jac}(X) \cong \mathbb{C}^g / \Lambda_g$$

If X has positive genus $g > 0$, then it naturally embeds in its Jacobian as

$$X \to \operatorname{Jac}(X), \qquad x \mapsto \int_{x_0}^{x}$$

In the special case when X is an elliptic curve, $X = E$, this embedding is actually an isomorphism, i.e. $E \cong J(E)$ for every elliptic curve E.

Now, suppose we have a map $h : X \to Y$ Riemann surfaces. We can lift this to the level of Jacobians. Define the *forward map*

$$h_J : \operatorname{Jac}(X) \to \operatorname{Jac}(Y), \qquad h_J[\phi] = [\phi \circ h^*]$$

where h^* is the pullback of h. The forward map acts as a change of variables on the integral

$$h_J \left(\sum_x n_x \int_{x_0}^{x} \right) = \sum_x n_x \int_{h(x_0)}^{h(x)}$$

Returning to modularity, this allows us to lift the map from the modularity theorem to the level of Jacobians, and in doing so, we derive a new version of modularity.

Theorem 2. *Let E be a complex elliptic curve with $j(E) \in \mathbb{Q}$. Then for some positive integer N, there exists a surjective holomorphic homomorphism of complex tori*

$$J_0(N) \to E$$

.

Proof. Let $h : X_0(N) \to E$ be the map from the modularity theorem. Then we get

$$h_J : J_0(N) = \mathrm{Jac}(X_0(N)) \to \mathrm{Jac}(E) \cong E$$

It suffices now to show that h_J is surjective whenever h is, but we omit this. □

Note that, via the correspondence between weight 2 cusp forms and differentials on the modular curve, we think of an element of the Jacobian as a coset of functionals on $\mathcal{S}_2(\Gamma_0(N))$. We would like to refine this perspective so that we can associate to the elliptic curve one specific modular form. Something else we may observe is that $j_0(N)$ is a high dimensional complex torus, whereas E is a 1 dimensional complex torus. We therefore might suspect that by decomposing $J_0(N)$ into smaller pieces somehow, we can isolate the piece from which E arises, heuristically speaking.

Doing this effectively amounts to a certain eigenspace decomposition. In order to understand this, we must define a certain class of operators on the vector space $S_2(\Gamma_0(N))$.

Suppose n is relatively prime to N. Then let $\langle n\rangle : \mathcal{M}_k(\Gamma_0(N)) \to \mathcal{M}_k(\Gamma_0(N))$ be given by $\langle n\rangle f = f[\alpha]_k$, for any $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ with $d = n \mod n$. If d is not relatively prime to n, then we define $\langle d\rangle$ to be trivial.

Now suppose p is prime. Then let $T_p : \mathcal{M}_k(\Gamma_0(N)) \to \mathcal{M}_k(\Gamma_0(N))$ be given by

$$T_p f = f \left[\Gamma_0(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_0(N)\right]_k$$

Define $T_1 = 1$. For prime powers p^r, define T_{p^r} inductively as

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}}$$

Finally, for all $n \in \mathbb{Z}^+$, define T_n by

$$T_n = \prod_i T_{p_i^{r_i}}$$

The collection of all operators so defined, $\{\langle n\rangle, T_n\}$ are known as the *Hecke operators*. They form a $\mathbb{Z}$-algebra, known as the *Hecke algebra*

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[\{\langle n\rangle, T_n : n \in \mathbb{Z}^+\}]$$

One can show that these operators all commute with each other. Therefore, they can be simultaneously diagonalized, and hence the Hecke algebra has eigenvectors. Since these eigenvectors are also forms, we call them *eigenforms*. Note that since $\mathcal{S}_k(\Gamma)$ is a subspace of $\mathcal{M}_k(\Gamma)$, all of the above applies all the same to spaces of cusp forms.

Now, recall that we have

$$\begin{aligned}\mathrm{Jac}(X(\Gamma)) &= \Omega^1_{\mathrm{hol}}(X(\Gamma))^\wedge / H_1(X(\Gamma), \mathbb{Z}) \\ &\cong \mathcal{S}_2(\Gamma)^\wedge / H_1(X(\Gamma), \mathbb{Z})\end{aligned}$$

Considering the Hecke operators which act on $\mathcal{S}_2(\Gamma)$, we might expect that we can lift them to an action on the Jacobian $\mathrm{Jac}(X(\Gamma))$. Indeed, we can

$$T : J_0(N) \to J_0(N), \quad [\phi] \mapsto [\phi \circ T], \quad \phi \in \mathcal{S}_2(\Gamma_0(N))^\wedge$$

for any Hecke operator T.

Now, suppose an eigenform $f \in \mathcal{S}_2(\Gamma_0(M_f))$ is given, for some level M_f which depends on f. We can consider the subset of the Hecke algebra on which f vanishes.

$$I_f = \{T \in \mathbb{T}_{\mathbb{Z}} : Tf = 0\}$$

Since $\mathbb{T}_{\mathbb{Z}}$ acts on $J_0(M_f)$, the subgroup $I_f J_0(M_f)$ makes sense. We are thus lead to consider the quotient.

Definition 7. *For $f \in \mathcal{S}_2(\Gamma_0(M_f))$, define the Abelian variety associated to f to be*

$$A_f = J_0(M_f)/I_f J_0(M_f)$$

To better understand what structure this object has, define

$$V_f = \mathrm{span}(f) \subset \mathcal{S}_2(\Gamma_0(M_f))$$

$$\Lambda_f = H_1(X_0(M_f), \mathbb{Z})\big|_{V_f}$$

We can then show that forming the quotient $V_f^\wedge/\Lambda_f$ gives us the same result.

Proposition 3. *When f is an eigenform over $\mathbb{Q}$, we have an isomorphism*

$$A_f \to V_f^\wedge/\Lambda_f, \quad [\phi] + I_f J_0(M_f) \mapsto \phi|_{V_f} + \Lambda_f$$

The RHS has the structure of a 1-dimensional complex torus, hence so does A_f. The idea now is that, up to isogeny, these 1-dimesional complex tori together make up the full Jacobian $J_0(N)$. More precisely, we call a holomorphic homomorphism $f : A \to B$ of complex tori an *isogeny* if f is surjective and has finite kernel. Thus, it differs from a holomorphic isomorphism only in that it might have a nontrivial finite kernel. We can now state the decomposition formally.

Theorem 3. *The Jacobian associated to $\Gamma_0(N)$ is isogenous to a direct sum of Abelian varieties associated to eigenforms*

$$J_0(N) \to \bigoplus_f A_f^{m_f}$$

We are now able to state the main theorem. Factor $J_0(N) \to E$ through the isogeny $J_0(N) \to \bigoplus_f A_f^{m_f}$ and restrict to $A_f \to E$, and we obtain our final version of modularity.

Theorem 4. *Let E be a complex elliptic curve with $j(E) \in \mathbb{Q}$. Then for some positive integer N and some eigenform $f \in \mathcal{S}_2(\Gamma_0(N))$, there exists a surjective holomorphic homomorphism of complex tori*

$$A_f \to E$$

We have thus successfully associated to a particular eigenform f an elliptic curve E, namely as an image of the Abelian variet A_f associated to f.

References

[1] Fred Diamond, Jerry Shurman, *A First Course in Modular Forms.* Springer, 2005.