The Shimura–Taniyama formula

Let us start by considering a very concrete, simple question. Let $E/\mathbf{F}_p$ be the elliptic curve given by equation $y^2 = x^3 - x$, and suppose $p \equiv 1 \mod 4$. Then E has an action of $\mathbf{Z}[i]$ given by $[i](x, y) = (-x, iy)$. The p-power Frobenius morphism is central in the endomorphism algebra, so it is given by some element $\pi \in \mathbf{Z}[i]$. We also know it has degree p.

If we write $(p) = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathbf{Z}[i]$, then does π belong to $\mathfrak{p}_1$ or $\mathfrak{p}_2$? In this case we have an easy way of being able to tell. Since $\mathbf{Z}[i]$ acts on E, it also acts on the 1-dimensional $\mathbf{F}_p$-vector space $H^0(E, \Omega^1_E)$; let $\mathfrak{p}$ be the kernel of this action. Consider the invariant differential $\omega = dx/y$. Then for any $\alpha \in \mathbf{Z}[i]$, we have $[\alpha]^*\omega = \alpha\omega$. Since Frobenius is inseparable, we see that $\pi\omega = 0$, so $\pi \in \mathfrak{p}$.

The Shimura–Taniyama formula answers the analogous question for abelian varieties of dimension g_0 with an action by a CM extension of a totally real field of degree g_0. In this note we will discuss p-divisible groups with CM and prove the Shimura–Taniyama formula. We will include unramifiedness hypotheses for simplicity of exposition, but they can be removed.

1 p-divisible groups with complex multiplication

1.1 p-divisible groups with action by a local field

Let F and K be finite unramified extensions of $\mathbf{Q}_p$. Let Γ be a p-divisible group over $\mathcal{O}_F$ of dimension d and height $h = [K : \mathbf{Q}_p]$ with an action by $\mathcal{O}_K$. Let k denote the residue field of $\mathcal{O}_F$ and put $q = p^r = \#k$. Let

$$\lambda = \lambda(\Gamma) \coloneqq \frac{d}{h}$$

denote the slope of Γ. Also let $W \coloneqq W(\overline{\mathbf{F}}_p)$ and $L \coloneqq W[\frac{1}{p}]$.

Proposition 1.1. *Suppose $\pi \in \mathcal{O}_K$ lifts the q-power Frobenius action on Γ_k, where k is the residue field of F. Then we have*

$$\lambda = \frac{\operatorname{ord}_p \pi}{r}.$$

Proof. We need to show that π^h and q^d differ by a unit multiple in $\mathcal{O}_K$. Consider the connected-étale sequence

$$0 \longrightarrow \Gamma^0 \longrightarrow \Gamma \longrightarrow \Gamma^{\text{ét}} \longrightarrow 0.$$

We note that the Tate module $T_p\Gamma$ is free of rank 1 as a module over $\mathcal{O}_K$, so Γ is either connected or étale.

If Γ is étale, then $d = 0$ and the Frobenius map is an isomorphism, so $\pi \in \mathcal{O}_K^\times$ as desired.

If Γ is connected, then by Tate's theorem we know that Γ is a formal Lie group and thus is of the form $\operatorname{Spf} \mathcal{O}_F[\![X_1, \dots, X_d]\!]$. Since π lifts the Frobenius on $\Gamma_k \cong \operatorname{Spf} k[\![X_1, \dots, X_d]\!]$ which has degree q^d, we see that $\deg \pi = q^d$. On the other hand, $\deg p = p^h$ so $\deg q = q^h$. We conclude that π^h and q^d have the same degree as endomorphisms of Γ, and hence the same absolute value as elements of $\mathcal{O}_K$. $\square$

Consider the covariant Dieudonné module $D \coloneqq \mathbf{D}(\Gamma_k)$, and let $\varphi : D \to D$ denote the σ^{-1}-linear endomorphism associated to the Dieudonné module, where $\sigma : F \to F$ is the

Frobenius morphism. Now D is a free module of rank 1 over $\mathcal{O}_K \otimes_{\mathbf{Z}_p} \mathcal{O}_F$. We have an isomorphism of $\mathcal{O}_K$-modules

$$D \otimes_{\mathcal{O}_F} \mathcal{O}_L \cong \prod_{\phi \in \mathrm{Hom}(K, \mathbf{C}_p)} \mathcal{O}_L$$

where $\alpha \in \mathcal{O}_K$ acts on the ϕ'th copy of $\mathcal{O}_L$ by $\phi(\alpha)$. We write φ_L for the associated endomorphism of $D \otimes_{\mathcal{O}_F} \mathcal{O}_L$ given by $\varphi \otimes \sigma^{-1}$. Since φ commutes with the action of $\mathcal{O}_K$, we see that

$$\varphi_L = t(1 \otimes \sigma^{-1})$$

where $t = (t_\phi) \in \prod_\phi \mathcal{O}_L$. Since we know that $pD \subset \varphi D$, we conclude that $\mathrm{ord}_p\, t_\phi \leq 1$ for all ϕ. Let $\mathrm{Hom}(K, \mathbf{C}_p; \Gamma)$ denote the subset of ϕ for which $\mathrm{ord}_p\, t_\phi = 1$ We then see that

$$d = \dim_k D/\varphi D = \#\,\mathrm{Hom}(K, \mathbf{C}_p; \Gamma)$$

so we have arrived at:

Proposition 1.2. *With setup as above, we have*

$$\lambda = \frac{\#\,\mathrm{Hom}(K, \mathbf{C}_p; \Gamma)}{\#\,\mathrm{Hom}(K, \mathbf{C}_p)}.$$

1.2 p-divisible groups with action by a global field

Let F, k, q as before, but now consider a number field K unramified at p, and a p-divisible group $\mathcal{G}$ over $\mathcal{O}_F$ of dimension d and height $h = [K : \mathbf{Q}]$, with an action of $\mathcal{O}_K$.

Observe $T_p\mathcal{G}$ is a free module of rank 1 over $\mathcal{O}_K \otimes \mathbf{Z}_p = \prod_{\mathfrak{p}|p} \mathcal{O}_{K_\mathfrak{p}}$. Then we see that $\mathcal{G}$ is isogenous to a product

$$\prod_{\mathfrak{p}|p} G_\mathfrak{p}$$

where $G_\mathfrak{p}$ is a p-divisible group over $\mathcal{O}_F$ of height $[K_\mathfrak{p} : \mathbf{Q}_p]$ with an action by $\mathcal{O}_{K_\mathfrak{p}}$. Using the local results of the previous section, we obtain:

Proposition 1.3. *Suppose $\pi \in \mathcal{O}_K$ lifts the Frobenius action on $\mathcal{G}_k$. For each $\mathfrak{p} \mid p$ (in $\mathcal{O}_K$) we have*

$$\frac{\mathrm{ord}_\mathfrak{p}\, \pi}{r} = \frac{\#\,\mathrm{Hom}(K_\mathfrak{p}, \mathbf{C}_p; G_\mathfrak{p})}{\#\,\mathrm{Hom}(K_\mathfrak{p}, \mathbf{C}_p)}.$$

2 Abelian varieties with complex multiplication

2.1 CM types

Let K^+ denote a totally real number field and K/K^+ a CM extension. Let $g_0 = [K^+ : \mathbf{Q}]$. Let $\mathrm{Hom}(K, \mathbf{C})$ denote the set of field embeddings of K into $\mathbf{C}$. For each $\phi^+ \in \mathrm{Hom}(K^+, \mathbf{C})$ there is a conjugate pair of embeddings $\phi, \overline{\phi} \in \mathrm{Hom}(K, \mathbf{C})$ extending ϕ^+.

Definition 2.1. A subset $\Phi \in \mathrm{Hom}(K, \mathbf{C})$ of cardinality g_0 is a *CM type* for K if for every $\phi^+ \in \mathrm{Hom}(K^+, \mathbf{C})$ there is a $\phi \in \Phi$ extending ϕ^+.

A CM-type is clearly equivalent to specifying the discrete measure on $\mathrm{Hom}(K, \mathbf{C})$ given by $\mu(S) = \#(S \cap \Phi)$.

Essentially, a CM type is a choice of one element of the conjugate pair of embeddings of K above each embedding of K^+.

2.2 CM type of an abelian variety

The key point is that the abelian variety $A/\mathbf{C}$ with an action of $\mathcal{O}_K$ canonically determines a CM type for K as follows. Since we have an embedding $\mathcal{O}_K \hookrightarrow \mathrm{End}\, A$, we obtain a linear action of $\mathcal{O}_K$ on $\mathrm{Lie}\, A$.

Via the exponential map there is an exact sequence

$$0 \longrightarrow \Lambda \longrightarrow \mathrm{Lie}\, A \longrightarrow A \longrightarrow 0$$

where Λ is a free $\mathbf{Z}$-module of rank $2g_0$. Then Λ is a flat $\mathcal{O}_K$-module of rank 1, so $\mathrm{Lie}\, A = \Lambda_{\mathbf{R}}$ is a flat module of rank 1 over

$$\mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{R} = \prod_{\phi^+ \in \mathrm{Hom}(K^+, \mathbf{C})} \mathbf{C}_{\phi^+}$$

where $\mathbf{C}_{\phi^+}$ is $\mathbf{C}$ with $\mathcal{O}_{K^+}$-algebra action determined by ϕ.

Also $\mathrm{Lie}\, A$ is a module over the ring

$$\mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{C} \cong \prod_{\phi \in \mathrm{Hom}(K, \mathbf{C})} \mathbf{C}_\phi.$$

The map of $\mathcal{O}_{K^+}$-algebras $\Lambda_{\mathbf{R}} \to \mathrm{Lie}\, A$ then produces a choice $\phi \in \mathrm{Hom}(K, \mathbf{C})$ above each $\phi^+ \in \mathrm{Hom}(K^+, \mathbf{C})$, i.e. a CM type for K. We let Φ_A denote this CM type. In particular as an $\mathcal{O}_K$-algebra we have

$$\mathrm{Lie}\, A \cong \prod_{\phi \in \Phi_A} \mathbf{C}_\phi.$$

By choosing an embedding $\iota : \mathbf{C} \hookrightarrow \mathbf{C}_p$ we obtain a bijection $\mathrm{Hom}(K, \mathbf{C}) \simeq \mathrm{Hom}(K, \mathbf{C}_p)$. Any field embedding $\phi : K \hookrightarrow \mathbf{C}_p$ extends to a $\mathbf{Q}_p$-linear map $\phi_{\mathbf{Q}_p} : K \otimes \mathbf{Q}_p \to \mathbf{C}_p$. We have

$$K \otimes \mathbf{Q}_p = \prod_{\mathfrak{p}|p} K_{\mathfrak{p}}$$

and thus we have a bijection

$$\mathrm{Hom}(K, \mathbf{C}) \simeq \bigsqcup_{\mathfrak{p}|p} \mathrm{Hom}_{\mathrm{cts}}(K_{\mathfrak{p}}, \mathbf{C}_p).$$

Definition 2.2. We will denote by $S_{\mathfrak{p}}$ the subset of $\mathrm{Hom}(K, \mathbf{C})$ corresponding to $\mathrm{Hom}_{\mathrm{cts}}(K_{\mathfrak{p}}, \mathbf{C}_p)$.

We note that $\#S_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbf{Q}_p]$.

2.3 CM abelian varieties over a number field

Let $F \subseteq \mathbf{C}$ denote a number field unramified at p, given as a subfield of $\mathbf{C}$. Upon choosing an embedding $\iota : \mathbf{C} \to \mathbf{C}_p$, we determine a prime ideal $\mathfrak{q}$ of $\mathcal{O}_F$ above p. We let k denote the residue field at $\mathfrak{q}$, of cardinality $q = p^r$.

We let A denote an abelian variety over F of dimension g_0 with an action by $\mathcal{O}_K$. We suppose that A has a model $\mathcal{A}/\mathcal{O}_{F_\mathfrak{q}}$. Let $\Gamma = \mathcal{A}[p^\infty]$ its p-divisible group. As in §1, we obtain a decomposition of Γ (up to isogeny) of the form $\prod_{\mathfrak{p}|p} \Gamma_\mathfrak{p}$.

Proposition 2.3. *We have $\# \operatorname{Hom}(K_\mathfrak{p}, \mathbf{C}_p; \Gamma_\mathfrak{p}) = \mu_A(S_\mathfrak{p})$.*

Proof. Let $D = \mathbf{D}(\Gamma_k)$ denote the covariant Dieudonné module and let D_L denote its (semi-linear) base change to L. Then we have $\mathcal{O}_K$-equivariant maps

$$D_L/pD_L \twoheadrightarrow D_L/\varphi D_L \cong \operatorname{Lie} \mathcal{A}_k \otimes_{\mathbf{Z}} \mathcal{O}_L \cong \prod_{\phi \in \Phi_A} \mathcal{O}_L/p\mathcal{O}_L$$

Consequently, in the notation of §1.1, we see that $t_\phi \in p\mathcal{O}_L$ for $\phi \in \Phi_A$. It follows that $\phi \in \operatorname{Hom}(K_\mathfrak{p}, \mathbf{C}_p)$ belongs to $\operatorname{Hom}(K_\mathfrak{p}, \mathbf{C}_p; \Gamma_\mathfrak{p})$ if and only if $\phi \in \Phi_A$. □

Let $\pi \in \operatorname{End}(\mathcal{A}_k)$ denote the q-power Frobenius map. Then π is central in $\operatorname{End}(\mathcal{A}_k)$ and so can be viewed as an element of $\mathcal{O}_K$. The Shimura–Taniyama formula determines the factorization of (π) as an ideal of $\mathcal{O}_K$.

Theorem 2.4 (Shimura–Taniyama)**.** *For each prime $\mathfrak{p}$ of $\mathcal{O}_K$ above p, we have*

$$\frac{\operatorname{ord}_\mathfrak{p} \pi}{r} = \frac{\mu_A(S_\mathfrak{p})}{\# S_\mathfrak{p}}.$$

Proof. Combine Proposition 1.3 and Proposition 2.3. □

3 Example: elliptic curves

Let E be an elliptic curve defined over F with good reduction at $\mathfrak{q}$, and suppose it has CM by $\mathcal{O}_K$ for an imaginary quadratic field $K/\mathbf{Q}$. Then $\operatorname{Lie} E_\mathbf{C} \cong \mathbf{C}$ so the action of $\mathcal{O}_K$ on E determines an embedding $\phi : K \hookrightarrow \mathbf{C}$. This ϕ is the data of the CM type for K associated to E.

We have two cases; either p is inert in K or it splits. If p is inert there is a unique prime $\mathfrak{p}$ above p (of norm p^2) and we must have $a_\mathfrak{p} = r/2$ simply for reasons of degree. This proves the S–T formula in this case since $\# S_\mathfrak{p} = 2$ and $\#(\Phi \cap S_\mathfrak{p}) = 1$.

If p splits the situation is slightly more interesting. In this case we can write $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ (these factors are conjugate to each other). Without loss of generality we'll suppose that $\phi \in S_{\mathfrak{p}_1}$, i.e. $K \overset{\phi}{\hookrightarrow} \mathbf{C} \hookrightarrow \mathbf{C}_p$ factors through $K \hookrightarrow K_{\mathfrak{p}_1} \cong \mathbf{Q}_p$. Via the embedding of F into $\mathbf{C}_p$ we then have a map $\mathcal{O}_K \to \operatorname{End} \operatorname{Lie} \mathcal{E}_{\overline{\mathbf{F}}_p}$ whose kernel is $\mathfrak{p}_1$. On the other hand the p-power Frobenius morphism is inseparable and so acts by 0 on $\operatorname{Lie} \mathcal{E}_{\overline{\mathbf{F}}_p}$. It follows that $\pi \in \mathfrak{p}_1^r$ and $a_{\mathfrak{p}_1} = r$, $a_{\mathfrak{p}_2} = 0$. This also agrees with the S–T formula since $\# S_{\mathfrak{p}_1} = \#(\Phi \cap S_{\mathfrak{p}_1}) = 1$.

References

[1] B. Conrad. Shimura–Taniyama formula.
http://math.stanford.edu/∼conrad/vigregroup/vigre04/stformula.pdf.

[2] A. Genestier and B.C. Ngô. Lectures on shimura varieties.