1 Algebraic correspondences

Let C be a smooth projective curve defined over an algebraic closed field K. Let $\mathrm{Div}(C)$ be the divisor group, that is the free abelian group generated by the points of $C(K)$. Let $D = \sum n_P P$ be a divisor and define $\deg(D) = \sum n_P$. Define

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) \mid \deg D = 0\}.$$

Given $f \in K(C)^*$, let $\mathrm{div}(f) = \sum \mathrm{ord}_P(f)(P)$ and note that $\deg(\mathrm{div}(f)) = 0$. Define $\mathrm{Jac}(C)$ as the quotient of $\mathrm{Div}^0(C)$ by the subgroup of principal divisor, that is the subgroup of divisors of the form $\mathrm{div}(f)$.

Let C be a curve defined over a field K of positive characteristic $p > 0$. Let $q = p^r$. Let $\mathrm{Frob}_q : C \to C^{(q)}$ be the Frobenius of C. Recall that if C is defined by an equation $F(x, y) = 0$, then $\mathrm{Frob}_q(x, y) = (x^q, y^q)$ and $C^{(q)}$ is defined by the equation $F^{(q)}(x, y) = 0$.

Let X, X', Y be three non singular projective curves defined over a field K. An *algebraic correspondence* from X to X' is a pair

$$X \xleftarrow{\alpha} Y \xrightarrow{\beta} X'$$

with α and β finite. Given an algebraic correspondence, we can define a map

$$\beta_* \circ \alpha^* : \mathrm{Div}(X) \to \mathrm{Div}(X')$$

that sends

$$P \to \sum_{Q \in \alpha^{-1}(P)} e_\phi(Q)\beta(Q).$$

One can easily show that this map sends $\mathrm{Div}^0(X)$ to $\mathrm{Div}^0(X')$ and sends principal divisors to principal divisors. Hence, passing through the quotient, we can define a map $J(\beta_* \circ \alpha^*)$ from $\mathrm{Jac}(X)$ to $\mathrm{Jac}(X')$.

Given $f : X \to X$ a morphism, let $Y = \{(x, f(x)) \mid x \in X\}$ be the graph of f. Consider the correspondence

$$X \xleftarrow{\pi_1} Y \xrightarrow{\pi_2} X$$

and so we can define a map

$$J(f) = J(\pi_{2*} \circ \pi_1^*) : \mathrm{Div}(X) \to \mathrm{Div}(X)$$

that sends

$$P \to f(P).$$

In the same way, take the algebraic correspondence

$$X \xleftarrow{\pi_2} Y \xrightarrow{\pi_1} X$$

and so we can define a map

$$J(f)' = J(\pi_{1*} \circ \pi_2^*) : \mathrm{Div}(X) \to \mathrm{Div}(X)$$

that sends

$$P \to \sum_{Q \in f^{-1}(P)} e_f(Q)Q.$$

Note that $J(f)$ and $J(f)'$ are usually defined as f_* and f^*.

Let p be a prime and let C be a non-singular projective curve defined over $\mathbb{F}_p$. So, $C^{(p)} = C$. We can define $J(\mathrm{Frob}_p) : \mathrm{Jac}(C) \to \mathrm{Jac}(C)$ and $J(\mathrm{Frob}_p)' : \mathrm{Jac}(C) \to \mathrm{Jac}(C)$ as above. We will simply denote these maps by Frob_p and Frob'_p.

Theorem 1.1. *Let $N \geq 1$. There exists a polynomial $\Phi_N(X,Y) \in \mathbb{Z}[X,Y]$ with the following property: Let C be the curve defined by $\Phi_N(X,Y) = 0$. Let C^{ns} be the curve obtained by removing the non-singular points of C and there is an embedding C^{ns} in a complete and regular curve $\tilde{C}$. There is an isomorphism $X_0(N) \to \tilde{C}$ (over $\mathbb{C}$). On an open subset, the map sends z to $(j(z), j(Nz))$.*

Proof. See [1, End of Section 7 and before Theorem 10.3] □

On the open subset of $X_0(N)$ of the previous theorem, every point z is associated with a couple $(j(E), j(E'))$ with E and E' two elliptic curves, $j(E) = j(z)$, and an isogeny $\phi : E \to E'$ with kernel a cyclic group of order N.

Let $(p, N) = 1$. We denote by $\overline{X_0(N)}$ the reduction of $\tilde{C}$ modulo p. Since p is coprime with N (we will not prove this, it is difficult!!), we have that $\overline{X_0(N)}$ is non-singular. On an open subset of $\overline{X_0(N)}(\overline{\mathbb{F}}_p)$, the points can be seen as couples $(j(\overline{E}), j(\overline{E'}))$ with $\overline{E}$ and $\overline{E'}$ two elliptic curves defined over $\overline{\mathbb{F}}_p$ with an isogeny of kernel a cyclic group of order N.

Question 1.2. Let p be a prime and N be a positive integer coprime with p. Describe $\mathrm{Frob}_p + \mathrm{Frob}'_p : \mathrm{Jac}(\overline{X_0(N)}) \to \mathrm{Jac}(\overline{X_0(N)})$. In particular, can we find a global (that is, an endomorphism of $\mathrm{Jac}(X_0(N))$) whose reduction modulo p is $\mathrm{Frob}_p + \mathrm{Frob}'_p$?

2 Hecke algebra

Let Γ be a subgroup of $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ of finite index. Let Δ be the set of integer matrices of positive determinant. Given $\alpha \in \Delta$, define $\Gamma^\alpha = \Gamma \cap \alpha^{-1}\Gamma\alpha$. One can easily check that Γ^α has finite index in $\Gamma(1)$. So, $\Gamma = \sqcup \Gamma^\alpha \alpha_i$ for finitely many $\alpha_i \in \Gamma$.

Lemma 2.1. *If $\Gamma = \sqcup_i \Gamma^\alpha \alpha_i$, then $\Gamma\alpha\Gamma = \sqcup_i \Gamma\alpha\alpha_i$.*

Proof. Note that

$$\alpha\Gamma\alpha\Gamma = \sqcup_i \alpha\Gamma\alpha(\Gamma \cap \alpha^{-1}\Gamma\alpha)\alpha_i = \sqcup_i(\alpha\Gamma\alpha\Gamma \cap \alpha\Gamma\alpha)\alpha_i = \sqcup_i \alpha\Gamma\alpha\alpha_i.$$

We conclude by multiplying by α^{-1} on the left. □

Let $\alpha, \beta \in \Delta$ and assume that $\Gamma = \sqcup_i \Gamma^\alpha \alpha_i$ and $\Gamma = \sqcup_j \Gamma^\beta \beta_j$. Then,

$$(\Gamma\alpha\Gamma) \cdot (\Gamma\beta\Gamma) = \Gamma\alpha\Gamma\beta\Gamma = \sqcup_j \Gamma\alpha\Gamma\beta\beta_j = \sqcup_{i,j} \Gamma\alpha\alpha_i\beta\beta_j.$$

Definition 2.2. Let Γ and Δ be as above. Let $H(\Gamma, \Delta)$ be the free abelian group generated by the elements $\{\Gamma\alpha\Gamma \mid \alpha \in \Delta\}$. We want to give to this group a multiplication. Define

$$(\Gamma\alpha\Gamma) \cdot (\Gamma\beta\Gamma) = \sum_{i,j} \Gamma\alpha\alpha_i\beta\beta_j\Gamma.$$

So, $H(\Gamma, \Delta)$ is a $\mathbb{Z}$-module with a compatible multiplication and then it is an algebra. It is called an *Hecke algebra*.

Let Γ be a subgroup of $\Gamma(1)$ of finite index and let α be a matrix with integer coefficients and positive determinant. Let $X(\Gamma) = \Gamma \backslash \mathcal{H}^*$ and $X(\Gamma^\alpha) = \Gamma^\alpha \backslash \mathcal{H}^*$. Since $\Gamma^\alpha < \Gamma$, we can define the map $\pi : \Gamma^\alpha z \to \Gamma z$ from $X(\Gamma^\alpha)$ to $X(\Gamma)$. In the same way, we can define $\pi_\alpha : \Gamma^\alpha z \to \Gamma\alpha z$. So, we have the algebraic correspondence

$$X(\Gamma) \xleftarrow{\pi} X(\Gamma^\alpha) \xrightarrow{\pi_\alpha} X(\Gamma)$$

and we define

$$T(\alpha) = J(\pi_{\alpha*} \circ \pi^*) : \mathrm{Jac}(X(\Gamma)) \to \mathrm{Jac}(X(\Gamma)).$$

If $\Gamma = \sqcup \Gamma^\alpha \alpha_i$, then $\pi^{-1}(\Gamma z) = \{\Gamma^\alpha \alpha_i z\}$. So,

$$T(\alpha)(\Gamma z) = \sum_i \Gamma\alpha\alpha_i z.$$

Remark 2.3. The map $H(\Gamma, \Delta) \to \mathrm{End}(\mathrm{Jac}(X(\Gamma)))$ that sends $\Gamma\alpha\Gamma$ to $T(\alpha)$ is a ring homomorphism.

3 The morphism T(p)

Now, we show an example of an element of $H(\Gamma, \Delta)$, that will be very useful for the next sections.

Example 3.1. Let $\Gamma = \Gamma_0(N)$. Let p be a prime with $(p, N) = 1$. Let $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. So, $\Gamma = \sqcup \Gamma^\alpha \alpha_i$ for some $\alpha_i \in \Gamma$. We want to explicitly write these α_i. Note that

$$\begin{aligned} \alpha^{-1}\Gamma\alpha &= \left\{ \alpha^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha \mid c \equiv 0 \pmod{N} \text{ and } ad - bc = 1 \right\} \\ &= \left\{ \begin{pmatrix} a & bp \\ cp^{-1} & d \end{pmatrix} \mid c \equiv 0 \pmod{N} \text{ and } ad - bc = 1 \right\} \end{aligned}$$

and then

$$\Gamma^\alpha = \left\{ \begin{pmatrix} a & bp \\ c & d \end{pmatrix} \mid c \equiv 0 \pmod N \text{ and } ad - bpc = 1 \right\}.$$

Define $\alpha_i = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$ for $i = 0, 1, \ldots, p-1$. So,

$$\Gamma^\alpha \alpha_i = \left\{ \begin{pmatrix} a & ai + bp \\ c & d + ci \end{pmatrix} \mid c \equiv 0 \pmod N \text{ and } ad - bpc = 1 \right\}.$$

Let $\alpha_p = \begin{pmatrix} p & -x \\ N & y \end{pmatrix}$ with x and y two integers such that $py + xN = 1$. One can easily check that $\Gamma^\alpha \alpha_i \neq \Gamma^\alpha \alpha_j$ if $i \neq j$. We just need to show that $\alpha_j \notin \Gamma^\alpha \alpha_i$ for $i \leq p-1$. If $j \neq p$ and $\alpha_j = \begin{pmatrix} a & ai + bp \\ c & d + ci \end{pmatrix} \in \Gamma^\alpha \alpha_i$, then $a = 1$ and then $i + bp = j$. We find a contradiction looking at the equation modulo p. If $j = p$ and $\alpha_j = \begin{pmatrix} a & ai + bp \\ c & d + ci \end{pmatrix} \in \Gamma^\alpha \alpha_i$, then $a = p$ and this is absurd since the matrix has determinant divisible by p. With similar techniques, we can easily show that

$$\Gamma = \sqcup_{0 \leq i \leq p} \Gamma^\alpha \alpha_i.$$

Lemma 3.2. *Using the notation of the previous example, the matrix* $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ *belongs to* $\Gamma \alpha \alpha_p$.

Proof.

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} yp & x \\ -N & 1 \end{pmatrix} \alpha \alpha_p.$$

□

As before, let $\Gamma = \Gamma_0(N)$ and p be a prime with $(p, N) = 1$. So, $X(\Gamma) = X_0(N)$ and take $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. Define $T(p) = T(\alpha) : \mathrm{Jac}(X_0(N)) \to \mathrm{Jac}(X_0(N))$.

Lemma 3.3. *Let* $(j(E), j(E')) \in X_0(N)$. *Let* $\phi : E \to E'$ *be the isogeny with* $\ker \phi = \mathbb{Z}/N\mathbb{Z}$. *We have*

$$T(p)(j(E), j(E')) = \sum_{i=0}^{p} (j(E/S_i), j(E'/\phi(S_i)))$$

where $\{S_i \mid i = 0, \ldots p\}$ *is the set of subgroups of* E *of order* p.

Proof. Let $\tau \in \mathbb{C}$ be such that $E \cong \mathbb{C}/ < 1, \tau >$. By definition,

$$T(p)(\Gamma z) = \sum_{i=0}^{p} \Gamma \alpha \alpha_i z$$

where α_i are defined in Example 3.1. For $0 \leq i \leq p-1$,

$$\Gamma\alpha\alpha_i\tau = \Gamma \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} \tau = \Gamma \frac{\tau + i}{p}.$$

Let S_i be the subgroup of $\mathbb{C}/ < 1, \tau >$ generated by $(\tau + i)/p$, that is a group of order p. So, the elliptic curve E/S_i is isomorphic to $\mathbb{C}/ < 1, \tau + i/p >$. Hence, $\Gamma\alpha\alpha_i\tau$ can be associated to the couple $(j(E/S_i), j(E'/\phi(S_i)))$. Let S_p be the subgroup of $\mathbb{C}/ < 1, \tau >$ generated by $1/p$, that is a group of order p. By Lemma 3.2, $\Gamma\alpha\alpha_p\tau$ can be associated with the couple $(j(E/S_p), j(E'/\phi(S_p)))$. Note that the subgroups of order p in $\mathbb{Z}/p \times \mathbb{Z}/p$ are $p+1$ and then the set $\{S_i \mid 0 \leq i \leq p\}$ is the set of all the subgroups of $\mathbb{C}/ < 1, \tau >$ of order p. In conclusion

$$T(p)(\tau) = T(p)(j(E), j(E')) = \sum_{i=0}^{p} (j(E/S_i), j(E'/\phi(S_i)))$$

where S_i are the subgroups of order p of E. □

4 The Eichler-Shimura congruence

Lemma 4.1. *Let q be the power of a prime and let E be an elliptic curve defined over $\overline{\mathbb{F}_q}$.*

- *The map $\mathrm{Frob}_q : E \to E^{(q)}$ has degree q and it is purely inseparable. If there is an elliptic curve E' defined over $\overline{\mathbb{F}_q}$, and $\phi : E \to E'$ of degree q and purely inseparable, then E' is isomorphic to $E^{(q)}$.*
- *The multiplication by q has degree q^2.*

Recall that $\overline{\mathbb{Q}_p} \subseteq \mathbb{C}$.

Theorem 4.2. *Let $(p, N) = 1$. Let $\overline{X_0(N)}$ be the reduction modulo p and $\overline{T}(p)$ be the reduction of $T(p)$. Then,*

$$\mathrm{Frob}_p + \mathrm{Frob}'_p = \overline{T}(p).$$

Note that these maps are from $\mathrm{Jac}(\overline{X_0(N)})$ to itself.

Remark 4.3. With $\overline{T(p)}$ we mean the following. Let $\overline{R} \in \mathrm{Jac}(\overline{X_0(N)})(\overline{\mathbb{F}_p})$. Let $R \in \mathrm{Jac}(X_0(N))(\overline{\mathbb{Q}_p})$ be a lift of R. So, $T(p)(R) \in \mathrm{Jac}(X_0(N))(\overline{\mathbb{Q}_p})$ and define $\overline{T}(p)(\overline{R})$ as the reduction modulo p of $T(p)(R)$. During the proof of the theorem we will show that this definition does not depend on the choice of the lift of $\overline{R}$ and then $\overline{T(p)}$ is well-defined.

Proof. Let $\overline{R} \in \overline{X_0(N)}(\overline{\mathbb{F}_p})$. Since we are working with morphisms of abelian varieties, we can focus on points of the form $(j(\overline{E}), j(\overline{E}'))$ as above. Note that $\overline{E}$ and $\overline{E'}$ are defined over $\overline{\mathbb{F}_p}$. Ignoring finitely many points, we can assume that $j(\overline{E}) \notin \mathbb{F}_{p^2}$. If we prove the identity for these points, then we are done. Consider the multiplication by p in $\overline{E}$. This map has degree p^2 and has kernel with cardinality 1 or p.

If it has trivial kernel, then the multiplication by p is purely inseparable and then $\overline{E}$ is isomorphic to $\overline{E}^{(p^2)}$. So, $j(\overline{E})^{p^2} = j(\overline{E}^{(p^2)}) = j(\overline{E})$ and then $j(\overline{E}) \in \mathbb{F}_{p^2}$, contradiction. So, $\ker(p : \overline{E} \to \overline{E})$ has order p.

Let $E \xrightarrow{\phi} E'$ be a lift of $\overline{E} \xrightarrow{\overline{\phi}} \overline{E'}$ to $\overline{\mathbb{Q}_p}$. The reduction map $E[p] \to \overline{E}[p]$ has kernel of order p and let S' be this group. As above, let $\{S_i \mid i = 0, \dots p\}$ be the set of p-subgroups of E. Reordering the indexes, we can assume $S' = S_0$. Consider $\phi_0 : E \to E/S_0$, that is an isogeny with kernel S_0. Let $\phi_0' : E/S_0 \to E$ be the dual of ϕ_0 and $\phi \circ \phi_0 = [p]$. Since $[p]$ has degree p^2 and the reduction modulo p of ϕ_0 and ϕ_0' have degree at most p, we have that reduction modulo p of ϕ_0 has degree p. Moreover, it is purely inseparable (since it has trivial kernel). Hence, $\overline{E/S_0}$ is isomorphic to $\overline{E}^{(p)}$. In the same way, $\overline{E'/\phi(S_0)}$ is isomorphic to $\overline{E'}^{(p)}$. Hence,

$$\mathrm{Frob}(j(\overline{E}), j(\overline{E'})) = (j(\overline{E})^p, j(\overline{E'})^p) = (j(\overline{E}^{(p)}), j(\overline{E'}^{(p)})) = (j(\overline{E/S_0}), j(\overline{E'/\phi(S_0)})).$$

Let $1 \leq i \leq p$. Consider $\phi_i : E \to E/S_i$. This map has degree p and its reduction modulo p is separable since it has kernel of cardinality p. Let ϕ_i' be the dual of ϕ_i and then

$$E \xrightarrow{\phi_i} E/S_i \xrightarrow{\phi_i'} E$$

with $\phi_i \circ \phi_i' = [p]$. So, the reduction $\overline{E/S_i} \xrightarrow{\overline{\phi_i'}} \overline{E}$ has degree p and trivial kernel. As above, $\overline{E}$ is isomorphic to $\overline{(E/S_i)^{(p)}}$. Hence,

$$\mathrm{Frob}_p(j(\overline{E/S_i}), j(\overline{E'/\phi_i(S_i)})) = (j(\overline{E}), j(\overline{E'}))$$

and $(j(\overline{E/S_i}), j(\overline{E'/\phi_i(S_i)})) < \mathrm{Frob}_p'(j(\overline{E}), j(\overline{E'}))$. Therefore,

$$\sum_{1 \leq i \leq p} (j(\overline{E/S_i}), j(\overline{E/\phi_i(S_i)})) < \mathrm{Frob}_p'((j(\overline{E}), j(\overline{E'}))).$$

The divisors of the LHS and of the RHS are both positive and of degree p (since Frob_p has degree p) and then

$$\sum_{1 \leq i \leq p} (j(\overline{E/S_i}), j(\overline{E/\phi_i(S_i)})) = \mathrm{Frob}_p'((j(\overline{E}), j(\overline{E'}))).$$

So,

$$\mathrm{Frob}_p((j(\overline{E}), j(\overline{E'}))) + \mathrm{Frob}_p'((j(\overline{E}), j(\overline{E'}))) = \sum_{0 \leq i \leq p} (j(\overline{E/S_i}), j(\overline{E/\phi_i(S_i)})).$$

By the previous section,

$$T(p)(j(E), j(E')) = \sum_{i=0}^{p} (j(E/S_i), j(E'/\phi_i(S_i)))$$

and so we are done. □

5 Comments on References

For the basic facts, see [2, Section 2 & 3]. For more details on Hecke algebra, see [1, Section 5]. The second part of the note is taken from [1, Section 10].

References

[1] James S. Milne. Modular functions and modular forms (v1.31), 2017. Available at www.jmilne.org/math/.

[2] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.