Galois action on torsion points of elliptic curves*

Alexandru-Anton Popa

March 10, 2000

The Characteristic Polynomial of the Frobenius. The main tool in computing the characteristic polynomials of Galois actions on torsion points is the Weil pairing. If E is an elliptic curve over an arbitrary field K, and m is an integer relatively prime to char(K), then there is a pairing

$$e_m : E[m] \times E[m] \longrightarrow \mu_m = \ m^{th} \text{ roots of unity in } K$$

having the following properties:
i. It is bilinear in both variables;
ii. It is alternating: $e_m(T,T) = 1$;
iii. It is nondegenerate: if $e_m(S,T) = 1$ for all $S \in E[m]$, then $T = O$;
iv. It is Galois invariant: $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$;
v. If $\phi : E_1 \to E_2$ is an isogeny with dual $\widehat{\phi} : E_2 \to E_1$, and $S \in E_1[m], T \in E_2[m]$ then:

$$e_m(S, \widehat{\phi}(T)) = e_m(\phi(S), T).$$

To illustrate the use of the Weil pairing, we prove the following:

Lemma 1 *Let E be an elliptic curve over a field K, let $\phi : E \to E$ be an isogeny, and let p be a prime integer not equal to the characteristic of K. Then the determinant of ϕ viewed as a linear transformation on $E[p] \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ satisfies:*

$$\det(\phi) \equiv \deg(\phi) \bmod p$$

Proof: Let v_1, v_2 be a basis of $E[p]$ and let

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$$

be the matrix of ϕ with respect to this basis. Using the Weil pairing $e_p : E[p] \to E[p]$ we compute $e_p(\phi(v_1), \phi(v_2))$ in two ways:

$$e_p(\phi(v_1), \phi(v_2)) = e_p(av_1 + cv_2, bv_1 + dv_2) = e_p(v_1, v_2)^{ad-bc}$$

*Reference: [AEC] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986

On the other hand, using the fact that $\phi\widehat{\phi} = \widehat{\phi}\phi = [deg(\phi)]$ where $\widehat{\phi}$ is the dual isogeny, we can write:

$$e_p(\phi(v_1), \phi(v_2)) = e_p(v_1, \widehat{\phi}\phi v_2) = e_p(v_1, v_2)^{\deg \phi}$$

But $e_p(v_1, v_2) \neq 1$ because the Weil pairing is nondegenerate, and the two expressions above show that $\det(\phi) \equiv \deg(\phi) \bmod p$. $\surd$

Now let E be an elliptic curve over a number field K, and let L be a Galois extension of K containing $E[p]$, where p is a fixed prime. Let λ be an unramified prime of K and let $\sigma \in \mathrm{Gal}(L/K)$ be the Frobenius substitution corresponding to a prime $\mathfrak{L}$ of L above λ. We assume that E has good reduction over the local field K_λ, and that the characteristic of the residue field of K_λ is $l \neq p$. We use lemma 1 to compute the characteristic polynomial of σ acting on $E[p]$:

Proposition 1 *With the above hypothesis, the characteristic polynomial of the Frobenius substitution σ acting on $E[p]$ is $x^2 - a_\lambda x + q$, where q is the the order of the residue field k of K_λ, and $a_\lambda = 1 + q - \#\widetilde{E}(k)$.*

Proof: Fixing an embedding $\bar{K} \subset \bar{K}_\lambda$, we view σ as an element of $\mathrm{Gal}(L_\mathfrak{L}/K_\lambda)$. Since E has good reduction over K_λ and $E[p] \subset L_\mathfrak{L}$, the reduction map gives an injection

$$E[p] \hookrightarrow \widetilde{E}(k')$$

where k' is the residue fields of $L_\mathfrak{L}$. Since the reduction of σ is the q^{th} power Frobenius automorphism σ_q of k'/k, it follows that the characteristic polynomial of σ acting on $E[p]$ is the same as the characteristic polynomial of σ_q acting on $\widetilde{E}[p]$. The later is easier to compute since $\sigma_q : \widetilde{E} \to \widetilde{E}$ is an isogeny of degree q.

Indeed, lemma 1 immediately gives us:

$$\det(\sigma_q) \equiv q \bmod p.$$

To find the trace of σ_q we use the formula $\mathrm{Tr}(A) = 1 + \det(A) - \det(I - A)$, which holds for every 2 by 2 matrix A. We have to compute $\det(I - \sigma_q)$. Using again the lemma, we find that $\det(I - \sigma_q) \equiv \deg(I - \sigma_q) \bmod p$. But the isogeny $I - \sigma_q$ is separable [AEC Ch. III, Cor. 5.5], therefore $\deg(I - \sigma_q) = \#\ker(I - \sigma_q)$ [AEC, Ch. III, Th. 4.10]. Finally

$$\#\ker(I - \sigma_q) = \#\{P \in \widetilde{E} : \sigma_q(P) = P\} = \#\widetilde{E}(k)$$

where for the last equality we use the fact that σ_q is the topological generator of $\mathrm{Gal}(\bar{k}/k)$. It follows that

$$\mathrm{Tr}(\sigma_q) = 1 + q - \#\widetilde{E}(k) = a_\lambda.$$

Hence the characteristic polinomyal of σ_q is $x^2 - a_\lambda x + q \in (\mathbb{Z}/p\mathbb{Z})[x]$, which is also the characteristic polynomial of σ as observed above.

The characteristic polynomial of complex conjugation. Let E be an elliptic curve over $\mathbb{Q}$. Fixing an embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$, it makes sense to talk about the action of the complex conjugation τ on $E[p]$, for a prime p. Assuming $p > 2$ we show that the characteristic polynomial of τ is $x^2 - 1$. Indeed, it is enough to show that the minimal polynomial is not $x + 1$ or $x - 1$.

Assuming by contradiction either of these holds, we see that for any $P_1, P_2 \in E[P]$

$$e_p(P_1, P_2)^\tau = e_p(P_1^\tau, P_2^\tau) = e_p(\pm P_1, \pm P_2) = e_p(P_1, P_2)$$

because $e_p(P_1, P_2) = e_p(-P_1. - P_2)$. It follows that $e_p(P_1, P_2) = 1$, which contradicts the nondegeneracy of the Weil pairing.

Therefore the characteristic polynomial of τ is $x^2 - 1$ as desired.

Application to our objects of interest. First we recall the setting. Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and let K be an imaginary quadratic extension of $\mathbb{Q}$ of discriminant $-D$, in which all the prime factors of N are split. Let p be an odd prime and n an odd square free integer coprime to NDp.

Let $L = K(E[p])$, which is a Galois extension of $\mathbb{Q}$. Note that the extension $K(E[p])/K$ is unramified outside the primes of K not dividing pN:[1]if λ is a prime of K, not dividing pN, then E has good reduction over the local field K_λ, the completion of K at λ. Fixing an embedding $\bar{K} \hookrightarrow \bar{K}_\lambda$, it is enough to show that the extension of local fields $K_\lambda(E[p])/K_\lambda$ is unramified. But since the reduced curve $\widetilde{E}/k$ is nonsingular, the reduction map gives an injection $E[p] \hookrightarrow \widetilde{E}(k')$, where k', k are the residue fields of $K_\lambda(E[p])$, K_λ respectively. This shows that the inertia group of $K_\lambda(E[p])/K_\lambda$ fixes all the elements of $E[p]$, as it fixes their images in $\widetilde{E}(k')$. So the inertia group is trivial, that is $K_\lambda(E[p])/K_\lambda$ is unramified, that is λ is unramified in L/K.

Let l be a prime factor of n. It follows that l is unramified in $L = K(E[p])$. We further assume that the conjugacy class $\mathrm{Frob}(l) \subset \mathrm{Gal}(L/\mathbb{Q})$ contains the complex conjugation τ. By Cebotarev's density theorem there are an infinite number of primes l with this property.

The assumption on $\mathrm{Frob}(l)$ implies that the prime l is inert in K (it is unramified and the residue field extension has degree 2); denote by λ its prime factor and by F_l, F_λ the corresponding residue fields. Note that the residue field of L at a prime above λ is again F_λ.

By the computation in the first section, the characteristic polynomial of $\mathrm{Frob}(l)$ acting on $E[p]$ is $x^2 - a_l x + l$, where $a_l = l + 1 - \#\widetilde{E}(F_l)$. From the equality of the characteristic polynomials of $\mathrm{Frob}(l)$ and τ for the extension $\mathbb{Q}(E[p])/\mathbb{Q}$, it follows that

$$l + 1 \equiv a_l \equiv 0 \bmod p.$$

Looking now at the extension $L/\mathbb{Q}$, note that $\tau \in \mathrm{Frob}(l)$ implies that the reduction $\tilde{\tau}$ of τ modulo a prime $\mathfrak{L}$ of L above l is well-defined; moreover $\tilde{\tau} = \sigma_l$, the l-power Frobenius automorphism. Denoting by $\widetilde{E}(F_\lambda)^\pm$ the ± 1 eigenspaces of $\tilde{\tau} = \sigma_l$ acting on $\widetilde{E}(F_\lambda)$, we can compute their orders as follows:

$$\begin{aligned}
\#\widetilde{E}(F_\lambda)^+ &= \#\{P \in \widetilde{E}(F_\lambda) : P^{\sigma_l} = P\} = \#\widetilde{E}(F_l) = l + 1 - a_l \\
\#\widetilde{E}(F_\lambda)^- &= \#\{P \in \widetilde{E}(F_\lambda) : P^{\sigma_l + 1} = O\} = \#\ker(1 + \sigma_l) = \deg(1 + \sigma_l) = \\
&\equiv \det(1 + \sigma_l) \equiv 1 + \mathrm{Tr}(\sigma_l) + \det(\sigma_l) \equiv 1 + a_l + l \bmod p
\end{aligned}$$

(we have used the fact that $1 + \sigma_l$ is separable together with Lemma 1). Since both $l + 1 \pm a_l$ are divisible by p and $\#\widetilde{E}(F_\lambda)^\pm \neq 0$, it follows that $\widetilde{E}[p]^\pm \simeq \mathbb{Z}/p\mathbb{Z}$ (the p-torsion of $\widetilde{E}$ is contained in $\widetilde{E}(F_\lambda)$ because of the injectivity of the reduction map $E[p] \hookrightarrow \widetilde{E}(F_\lambda)$).

[1] Another way of saying this: if E is an elliptic curve with good reduction over a local field F, then the $G_{\bar{F}/F}$ module $E[m]$ is unramified for all m relatively prime to the characteristic of the residue field of F [AEC, Ch. 7, Prop. 4.1].