THE CHARACTERISTIC POLYNOMIAL OF FROBENIUS AND THE ISOGENY CLASS OF AN ELLIPTIC CURVE

DENIS CHARLES

1. Introduction

In an important paper in 1966 [Tat66], Tate proved his famous isogeny theorem for abelian varieties over finite fields. This is a special case of a conjecture that he had made a few years earlier in 1963 which appears in [Tat65]. One important consequence of the isogeny theorem is that two abelian varieties over a finite field k are k-isogenous iff they have the same characteristic polynomial of the Frobenius over this field. In this article we prove this corollary directly when the abelian varieties in question are elliptic curves.

I am delighted to thank Professor John Tate for an e-mailed response to a question that led to me think about this. I would like to thank Nigel Boston and Eric Bach for helpful discussions.

2. The Proof

Theorem 2.1. *Let E_1 and E_2 be two elliptic curves over a finite field k. Then E_1 is k-isogenous to E_2 iff the characteristic polynomial of the Frobenius π of k as an endomorphism of E_1 is the same as that on E_2.*

Proof : The easier direction is when there is an isogeny $\phi : E_1 \to E_2$ defined over k. Let $\pi^2 - t\pi + q = 0$ be the characteristic polynomial of $\phi \in \mathrm{End}(E_1)$ and $q = \#k$. Then π commutes with ϕ since ϕ is defined over k. Furthermore, the multiplication by m maps commute with ϕ as ϕ is a homomorphism of abelian groups. Let P be a point on E_1, then on the one hand

$$\phi\big((\pi^2 - t\pi + q)P\big) = \phi(\mathscr{O}_{E_1}) = \mathscr{O}_{E_2}$$

while on the other hand

$$\phi\big((\pi^2 - t\pi + q)P\big) = \pi^2\phi(P) - t\pi\phi(P) + q\phi(P).$$

Since isogenies are surjective the above implies that $\pi^2 - t\pi + q = 0$ in $\mathrm{End}(E_2)$. Thus the characteristic polynomials of Frobenius on both the curves are the same.

Now for the more difficult direction. We are given that two elliptic curves E_1 and E_2 such that the characteristic polynomial of Frobenius is the same on both the curves. We have to cook up a k-isogeny between the curves. We split the discussion into two cases depending on whether the elliptic curves are supersingular or not.

Date: 28 October, 2004.

First we discuss the case when E_1 and (hence also) E_2 are supersingular. All isomorphism classes of elliptic curves in any isogeny class can be obtained by composing prime degree isogenies, and the graph of supersingular elliptic curves and prime degree isogenies as edges is connected (for a proof of this see Mestre). This means that starting from E_1 and composing k-rational 2-isogenies (since supersingular elliptic curves always have a k-rational 2-torsion point) we will reach E_2.

Assume that E_1 and E_2 are not supersingular and that their characteristic polynomial of Frobenius are the same. We apply Deuring's lifting theorem to obtain elliptic curves $\tilde{E}_1$ and $\tilde{E}_2$ over a number field K, with the additional property that $\mathrm{End}(E_1) \cong \mathrm{End}(\tilde{E}_1)$ and $\mathrm{End}(E_2) \cong \mathrm{End}(\tilde{E}_2)$. Since the curves are not supersingular their endomorphism rings are orders in some imaginary quadratic fields L_1 and L_2. Our assumption that the Frobenius satisifies the same polynomial in both rings gives us that:

$$\mathrm{End}(E_1) \supseteq \mathbb{Z}[\pi] \subseteq \mathrm{End}(E_2).$$

Thus the two quadratic orders share a common suborder, this means that

$$K_1 = K_2 = \mathbb{Q}(\sqrt{-D})$$

for some positive integer D or in more revealing terms

$$\mathrm{End}(E_1) \otimes \mathbb{Q} \cong \mathrm{End}(E_2) \otimes \mathbb{Q}.$$

Since we are dealing with curves with Complex Multiplication over $\mathbb{C}$ we have the following easy criterion to determine when they are isogenous.

Let $L_1 = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be the lattice associated to $\tilde{E}_1$ and $L_2 = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'$ be the lattice associated to $\tilde{E}_2$ such that $z = \frac{\omega_1}{\omega_2} \in \mathfrak{H}$ and $z' = \frac{\omega_1'}{\omega_2'} \in \mathfrak{H}$. If E_1 and E_2 have CM then $\mathbb{Q}(z) = \mathrm{End}(E_1) \otimes \mathbb{Q}$ and $\mathbb{Q}(z') = \mathrm{End}(E_2) \otimes \mathbb{Q}$ and furthermore, they are isogenous iff there is a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$$

such that $\frac{az+b}{cz+d} = z'$, where $\mathrm{GL}_2^+(\mathbb{Q})$ is the group of invertible matrices over $\mathbb{Q}$ with positive determinant.

Given this criterion and that $\mathbb{Q}(z) = \mathbb{Q}(z')$ one can readily verify that $\tilde{E}_1$ and $\tilde{E}_2$ are isogenous. All that remains to be shown is that the reduction of this isogeny is defined over k. Let $\phi : \tilde{E}_1 \to \tilde{E}_2$ be an isogeny. In terms of lattices, this isogeny is represented by a complex number α such that $\alpha L_1 \subseteq L_2$. Let ϖ be the complex number representing the (lift of the) Frobenius endomorphism on both the curves, and suppose $z \in \mathbb{C}/L_1$ be in the kernel of ϕ. This means that $\alpha z \in L_2$. Now consider $\alpha\varpi z = \varpi\alpha z = \varpi\omega$ for some $\omega \in L_2$, but ϖ is an endomorphism of L_2 so $\varpi\omega$ lies in L_2 also. In other words, the Kernel of ϕ is stabilized by the lift of the Frobenius. The reduction of the isogeny modulo the prime ideal lying above char k of norm q is an isogeny from E_1 to E_2 whose kernel is stabilized by the Frobenius of k. Thus this isogeny is defined over k. $\square$

References

[Tat65] Tate, John; *Algebraic Cycles and Poles of Zeta Functions*, in Arithmetical Algebraic Geometry, ed. Schilling, O. F. G., Harper & Row, 1965.

[Tat66] Tate, John; *Endomorphisms of abelian varieties over finite fields*, Invent. Math., **2**, 134-144, 1966.

Department of Computer Sciences, University of Wisconsin-Madison
E-mail address: cdx@cs.wisc.edu