HONDA-TATE THEOREM FOR ELLIPTIC CURVES

MIHRAN PAPIKIAN

1. Introduction

These are the notes from a reading seminar for graduate students that I organised at Penn State during the 2011-12 academic year.

Tate's isogeny theorem over finite fields, and the related Honda-Tate theorem, are important results in arithmetic geometry. The original papers by Tate [4], [5] prove these theorems for general abelian varieties, so, even if one is primarily interested in the case of elliptic curves, understanding the proofs requires some knowledge of the theory of abelian varieties. The goal of the seminar was to review some of the material in [1] and [2] necessary for understanding the statements of Tate isogeny theorem and Honda-Tate theorem for elliptic curves, and then to prove these theorems using only tools from the theory of elliptic curves.

2. Statement of Honda-Tate theorem for abelian varieties

Unless otherwise is indicated k will be a field of characteristic p with $q = p^a$ elements. Given a simple abelian variety A defined over k, we have the Frobenius endomorphism $\pi_A \in \mathrm{End}_k(A)$ relative to k. The ring $\mathrm{End}_k(A)$ is an order in the finite dimensional division algebra $\mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. Hence π_A can be considered as an algebraic integer. It is known that the absolute value $|\phi(\pi_A)|$ is equal to $q^{1/2}$ for any embedding $\phi : \mathbb{Q}(\pi_A) \to \mathbb{C}$.

Definition 2.1. A *q-Weil number* is an algebraic integer π such that $|\phi(\pi)| = q^{1/2}$ for any embedding $\phi : \mathbb{Q}(\pi) \to \mathbb{C}$. We say that two such numbers are conjugate if they are conjugate over $\mathbb{Q}$, i.e., there exists an isomorphism $\mathbb{Q}(\pi_1) \to \mathbb{Q}(\pi_2)$ which maps π_1 to π_2.

Theorem 2.2 (Honda-Tate). *Assume A is a simple abelian variety over k, and let*

$$F = \mathbb{Q}(\pi_A) \subset D = \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

1. *The map $A \to \pi_A$ gives a bijection between the k-isogeny classes of simple abelian varieties over k and the conjugacy classes of q-Weil numbers.*
2. *D is a division algebra with center F. The algebra D does not split at any real place of F, splits at every finite place prime to p, and its invariant at a place $\mathfrak{p}$ over p is given by the formula*

$$\mathrm{inv}_{\mathfrak{p}}(D) \equiv \frac{\mathrm{ord}_{\mathfrak{p}}(\pi_A)}{\mathrm{ord}_{\mathfrak{p}}(q)}[F_{\mathfrak{p}} : \mathbb{Q}_p] = \mathrm{ord}_{\mathfrak{p}}(\pi_A)\frac{f_{\mathfrak{p}}}{a} \pmod{\mathbb{Z}},$$

Date: May 13, 2012.

where $F_{\mathfrak{p}}$ is the completion of F at $\mathfrak{p}$ and $f_{\mathfrak{p}}$ is the degree of residue field extension at $\mathfrak{p}$.

(3) $2\dim(A) = [D:F]^{\frac{1}{2}}[F:\mathbb{Q}]$.

Remark 2.3. Note that Part (2) of the theorem implies that up to isomorphism D is uniquely determined by π_A, i.e., the Frobenius endomorphism determines the whole endomorphism algebra.

3. Tate isogeny theorem for elliptic curves

Denote $G = \mathrm{Gal}(\bar{k}/k)$. Let E_1 and E_2 be two elliptic curves over k. It is easy to see that the natural map

$$\mathrm{Hom}_k(E_1, E_2) \to \mathrm{Hom}_G(T_\ell(E_1), T_\ell(E_2))$$

is injective. In fact, by Theorem III.7.4 in [1], this map remains injective after tensoring the left hand side with $\mathbb{Z}_\ell$:

$$\mathrm{Hom}_k(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_G(T_\ell(E_1), T_\ell(E_2)). \tag{3.1}$$

Remark 3.1. The injectivity of (3.1) is not an automatic consequence of the flatness of $\mathbb{Z}_\ell$ over $\mathbb{Z}$, since the right hand side is considered as a $\mathbb{Z}_\ell$-module (its rank as a $\mathbb{Z}$-module is infinite). In fact, it is easy to construct an injective $\mathbb{Z}$-module homomorphism $\mathbb{Z}^n \to \mathbb{Z}_\ell$ for any $n \geq 2$ (just map the generators of $\mathbb{Z}^n$ to $\mathbb{Z}$-linearly independent elements in $\mathbb{Z}_\ell$), which clearly cannot remain injective after tensoring $\mathbb{Z}^n$ with $\mathbb{Z}_\ell$.

Lemma 3.2. *The cokernel of (3.1) is torsion-free.*

Proof. This is implicit in the proof of Theorem III.7.4 in [1]. More precisely, suppose $\phi \in \mathrm{Hom}_k(E_1, E_2) \otimes \mathbb{Z}_\ell$ is such that $\phi_\ell = \ell\varphi_\ell$ for some $\varphi_\ell \in \mathrm{Hom}_G(T_\ell(E_1), T_\ell(E_2))$. Let $M \subset \mathrm{End}_k(E_1, E_2)$ be some finitely generated subgroup with the property that $\phi \in M \otimes \mathbb{Z}_\ell$. Then M^{div} is finitely generated and free. Let

$$\psi_1, \dots, \psi_t \in \mathrm{Hom}_k(E_1, E_2)$$

be a basis for M^{div}, and write

$$\phi = \alpha_1\psi_1 + \cdots + \alpha_t\psi_t \quad \text{with} \quad \alpha_1, \dots, \alpha_t \in \mathbb{Z}_\ell.$$

Let $a_1, \dots, a_t \in \mathbb{Z}$ be such that $\alpha_i \equiv a_i \pmod{\ell}$. The assumption $\phi_\ell = \ell\varphi_\ell$ implies that the isogeny

$$\psi = [a_1] \circ \psi_1 + \cdots + [a_t] \circ \psi_t$$

annihilates $E_1[\ell]$. This then implies that ℓ must divide all a_i, and thus also all α_i. But that implies φ_ℓ is in the image of (3.1). □

The previous lemma shows that to prove that (3.1) is an isomorphism it is enough to prove that

$$\mathrm{Hom}_k(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \to \mathrm{Hom}_G(V_\ell(E_1), V_\ell(E_2)) \tag{3.2}$$

is an isomorphism, where $V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

Theorem 3.3. *The map (3.2) is an isomorphism.*

Proof. First, assume $\mathrm{Hom}_k(E_1, E_2) \neq 0$, i.e., the elliptic curves in question are isogenous over k. The existence of an isogeny implies that the dimension of $\mathrm{Hom}_k(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ as a vector space over $\mathbb{Q}_\ell$ is equal to the dimension of $\mathrm{End}_k(E_1) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. Similarly for $\mathrm{Hom}_G(V_\ell(E_1), V_\ell(E_2))$. Thus, it is enough to prove that

$$\dim_{\mathbb{Q}_\ell}(\mathrm{End}_k(E) \otimes \mathbb{Q}_\ell) \geq \dim_{\mathbb{Q}_\ell}(\mathrm{End}_G(V_\ell(E)).$$

Let π be the Frobenius endomorphism of E. Let $F = \mathbb{Q}(\pi)$ and $D = \mathrm{End}_k(E) \otimes \mathbb{Q}$. The Frobenius satisfies the quadratic equation (see Theorem V.2.3.1 in [1])

$$x^2 - tx + q = 0,$$

where $t = \mathrm{Tr}(\pi_\ell) = q + 1 - \#E(\mathbb{F}_q)$. The field F is in the center of the division algebra D. In particular, π is semi-simple, so its image π_ℓ is also semi-simple as an element of $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(E))$.

If $[F : \mathbb{Q}] = 2$, then $\dim D \otimes \mathbb{Q}_\ell \geq 2$ and π_ℓ is not a scalar. On the other hand, since G is topologically generated by the Frobenius automorphism, $\mathrm{End}_G(V_\ell(E))$ is the centralizer of $\mathbb{Q}_\ell(\pi_\ell)$ in $\mathrm{End}(V_\ell(E)) \cong \mathbb{M}_2(\mathbb{Q}_\ell)$. Obviously this centralizer has dimension at least 2, as it contains $\mathbb{Q}_\ell(\pi_\ell)$. But the dimension of a centralizer of a division algebra in the matrix algebra $\mathbb{M}_2$ is a divisor of 4, thus the centralizer has dimension either 2 or 4. The latter case is not possible, since otherwise $\mathbb{Q}_\ell(\pi_\ell)$ is in the center of $\mathbb{M}_2(\mathbb{Q}_\ell)$, which would imply that π_ℓ is a scalar.

Now suppose $F = \mathbb{Q}$, i.e., $\pi \in \mathbb{Z}$. This implies $\hat{\pi} = \pi$ and $\pi^2 = [q]$. In particular, $\hat{\pi}$ is not separable and a is even. Moreover, $\mathrm{End}_k(E) = \mathrm{End}_{\bar{k}}(E)$ since an endomorphism is defined over k if and only if it commutes with π. We conclude that E is supersingular and $\dim D \otimes \mathbb{Q}_\ell = 4 = \dim \mathrm{End}(V_\ell(E)) \geq \dim \mathrm{End}_G(V_\ell(E))$, cf. [1, Thm. 3.1].

It remains to show that $\mathrm{Hom}_k(E_1, E_2) \neq 0$ when $\mathrm{Hom}_G(V_\ell(E_1), V_\ell(E_2)) \neq 0$. It is enough to prove this after passing to an arbitrary finite extension k' of k. Indeed, if

$$\mathrm{Hom}_{k'}(E_1, E_2) \otimes \mathbb{Q}_\ell \cong \mathrm{Hom}_{G'}(V_\ell(E_1), V_\ell(E_2)),$$

then the isomorphism over k results by taking $\mathrm{Gal}(k'/k)$-invariants of both sides. Using Propositions 4.1 and 4.2, we see that we can assume that either both E_1 and E_2 are ordinary and all isogenies between them are defined over k, or that both E_1 and E_2 are supersingular with all their endomorphisms and all isogenies between them defined over k. Since π_ℓ is semi-simple, the existence of non-trivial homomorphism $V_\ell(E_1) \to V_\ell(E_2)$ of G-modules is equivalent to π_ℓ having the same characteristic polynomial as a linear operator acting on $V_\ell(E_1)$ and $V_\ell(E_2)$. Let π_i be the Frobenius endomorphism of E_i, $i = 1, 2$, and $F_i = \mathbb{Q}(\pi_i)$. We see that the existence of non-trivial homomorphism $V_\ell(E_1) \to V_\ell(E_2)$ implies $F_1 \cong F_2$. Identify these fields and denote it by F.

Suppose E_1 and E_2 are ordinary. Then $[F : \mathbb{Q}] = 2$. By Deuring's Lifting Theorem (Theorem 14, page 184 [3]) there exist elliptic curves $\tilde{E}_1$ and $\tilde{E}_2$ defined over a number field K, having CM by F, and reducing to E_1 and E_2 modulo a prime $\mathfrak{P}$ lying above p. On the other hand, two elliptic curves over $\mathbb{C}$ having CM by the same imaginary quadratic field are isogenous. Indeed, the lattices of such curves are in F, hence can be scaled into one another by multiplication by an appropriate complex number (see Theorem VI.4.1 in [1]). Thus, there is an isogeny $\alpha : \tilde{E}_1 \to \tilde{E}_2$ defined over a finite extension of K. The existence of Néron models [2] implies that modulo $\mathfrak{P}$ we get an isogeny $\bar{\alpha} : E_1 \to E_2$, which by assumption is defined over k.

Now suppose E_1 and E_2 are supersingular. Then $F = \mathbb{Q}$ and the endomorphism algebras of both curves is the quaternion algebra D ramified at p and ∞. Let L be any field which splits D. Such L is imaginary quadratic and p does not split in L. By Deuring's Lifting Theorem there exist elliptic curves $\tilde{E}_1$ and $\tilde{E}_2$ defined over a number field K, having CM by L, and reducing to E_1 and E_2 modulo a prime $\mathfrak{P}$ lying above p. Now repeat the earlier argument. □

Remark 3.4. Tate's original approach [4] reduces the proof of the isomorphism (3.1) to the case of endomorphisms (of abelian varieties) by considering the k-endomorphisms of the surface $E_1 \times E_2$.

Corollary 3.5. *If $[F : \mathbb{Q}] = 2$, then $D = \mathbb{Q}(\pi)$. If $F = \mathbb{Q}$, then a is even and D is a quaternion algebra. In particular, a supersingular curve defined over k with a odd cannot have all its endomorphisms defined over k.*

Corollary 3.6. *The following are equivalent:*

(1) *E_1 and E_2 are isogenous over k.*
(2) *$V_\ell(E_1) \cong V_\ell(E_2)$ as G-modules.*
(3) *$V_\ell(E_1) \cong V_\ell(E_2)$ as $\mathbb{Q}_\ell[\pi_\ell]$-modules.*
(4) *The characteristic polynomial of π_ℓ acting on $V_\ell(E_1)$ is the same as the characteristic polynomial of π_ℓ acting on $V_\ell(E_2)$.*
(5) $\mathrm{Tr}(\pi_\ell|V_\ell(E_1)) = \mathrm{Tr}(\pi_\ell|V_\ell(E_2))$.
(6) $\#E_1(k) = \#E_2(k)$.

Proof. (1)⇔(2) is a consequence of Tate's isomorphism. (2)⇔(3) because G is topologically generated by π. (3)⇔(4) because π_ℓ is semi-simple. (4)⇔(5) because the characteristic polynomial is $x^2 - \mathrm{Tr}(\pi_\ell)x + q$. (5)⇔(6) because $\#E(k) = q + 1 - \mathrm{Tr}(\pi_\ell)$. □

4. Honda-Tate theorem for elliptic curves

Corollary 3.6 implies that to each k-isogeny class of elliptic curves we can associated a well-defined integer $\mathrm{Tr}(\pi_\ell)$ of absolute value $\leq 2\sqrt{q}$, and the resulting map

$$\mathrm{HT} : \{k\text{-isogeny classes of elliptic curves}\} \to \{\text{integers in } [-2\sqrt{q}, 2\sqrt{q}]\}$$

is injective. Note that $\mathrm{Tr}(\pi_\ell)$ uniquely determines the Galois conjugacy class of the q-Weil number of E, hence this injectivity is part of the Honda-Tate theorem 2.2. The problem now is to determine the image of HT. We need some preliminary results.

Proposition 4.1. *E is supersingular if and only if $\pi^n \in \mathbb{Q}$ for some $n \geq 1$.*

Proof. E is supersingular if and only if $\bar{D} := \mathrm{End}_{\bar{k}}(E) \otimes \mathbb{Q}$ is a quaternion algebra; see Theorem V.3.1 in [1]. Let $k' = \mathbb{F}_{q^n}$ be an extension of k where all endomorphism of E are defined. The Frobenius of E over k' is π^n. If $\pi^n \in \mathbb{Q}$, then $\bar{D}$ is a quaternion algebra by Corollary 3.5.

Conversely, suppose $\bar{D}$ is a quaternion algebra. The center of $\bar{D}$ is $\mathbb{Q}$. On the other hand, π^n is in the center of $\bar{D}$. □

Proposition 4.2. *The following are equivalent:*

1. *E is ordinary.*
2. *$F = D$ and p splits in F.*
3. *$t = \mathrm{Tr}(\pi_\ell)$ is coprime to p.*

Proof. By Proposition 4.1, if $F = \mathbb{Q}$ then E is supersingular. Hence, if E is ordinary, then F is imaginary quadratic over $\mathbb{Q}$, cf. Theorem III.9.3 in [1]. In the proof of Theorem V.3.1 in [1], it is shown that D embeds into $\mathrm{End}(V_p(E)) = \mathbb{Q}_p$. Therefore, D is commutative and must be equal to F. Also, since we can realize F as a subfield of $\mathbb{Q}_p$, the prime p must split in F. This proves (1)⇒(2).

Next, suppose p splits as $\mathfrak{p}\mathfrak{p}'$. We have $\mathrm{Nr}(\pi) = q$, so $(\pi) = \mathfrak{p}^m\mathfrak{p}'^n$ with $m + n = a$. But if both n and m are positive, then $\pi = [p] \circ \phi$ for some endomorphism ϕ. Since π is purely inseparable, $[p]$ also must be purely inseparable. This implies that E is supersingular, so $\pi^b \in \mathbb{Q}$ for some b. Then $m = n$, and $(\pi) = (p^{a/2})$. This is a contradiction to p being split in $F = \mathbb{Q}(\pi)$. Hence after permuting $\mathfrak{p}$ and $\mathfrak{p}'$, we can assume $(\pi) = \mathfrak{p}^a$. Since $t = \pi + \bar{\pi}$, neither $\mathfrak{p}$ nor $\mathfrak{p}'$ divide t, so p cannot divide t. This proves (2)⇒(3). Also, clearly no power of π can be in $\mathbb{Q}$ if $(\pi) = \mathfrak{p}^a$. Therefore, (2)⇒(1).

Finally, assume t is coprime to p. Since F is generated by the roots of $x^2 - tx + q$, which decomposes into a product of coprime factors modulo p, the prime p splits in F. Hence (3)⇒(2). □

Corollary 4.3. *If a is even and $\pi = \pm p^{a/2}$, then E is supersingular, $F = \mathbb{Q}$ and D is a quaternion algebra. Moreover, $D = \bar{D}$. Otherwise, $F = D$ is imaginary quadratic over $\mathbb{Q}$ with the following possibilities.*

1. *If p splits in F, $(p) = \mathfrak{p}\mathfrak{p}'$, then $(\pi) = \mathfrak{p}^a$ and E is ordinary with all endomorphisms defined over k.*
2. *If p ramifies, $(p) = \mathfrak{p}^2$, then $(\pi) = \mathfrak{p}^a$ and E is supersingular with not all endomorphisms defined over k.*
3. *If p remains inert, $(p) = \mathfrak{p}$, then a is even, $(\pi) = \mathfrak{p}^{a/2}$ and E is supersingular with not all endomorphisms defined over k.*

The splitting behaviour of p in F in terms of t is given by the following elementary lemma [6, p. 537]:

Lemma 4.4. *In $F = \mathbb{Q}(\sqrt{t^2 - 4q})$:*

1. *p ramifies if*
   - (i) *$t = 0$ and a is odd;*
   - (ii) *$t = 0$, a is even, and $p = 2$;*
   - (iii) *$t = \pm\sqrt{q}$, a is even, and $p = 3$;*
   - (iv) *$t = \pm p^{\frac{a+1}{2}}$, a is odd, and $p = 2$ or 3.*

(2) *p stays prime if*
   (i) *$t=0$, a is even, and $p \equiv 3 \pmod 4$;*
   (ii) *$t=\pm\sqrt{q}$, a is even, and $p \equiv 2 \pmod 3$.*

(3) *p splits in all other cases.*

Example 4.5. Not all integers in $[-2\sqrt{q}, 2\sqrt{q}]$ are necessarily in the image of HT. As an example, let $q=8$. Then the range of HT is $[-5,5]$. Suppose there is an elliptic curve with $t=2$. By Lemma 4.4, 2 splits in F. Hence E must be ordinary. On the other hand, t is not coprime to p, which leads to a contradiction.

It is interesting to note that π satisfying $x^2-2x+8=0$ is an 8-Weil number. What happens in fact is that $(\pi)=\mathfrak{p}^2\mathfrak{p}'$, where $(2)=\mathfrak{p}\mathfrak{p}'$. By Theorem 2.2, D is a division algebra with center F whose invariants are $2/3$ and $1/3$ at $\mathfrak{p}$ and $\mathfrak{p}'$, respectively, and 0 everywhere else. Thus, the dimension of D over F is 9, which implies that $\dim(A)=3$, i.e., π is a Weil number of a 3-fold.

Example 4.6. Let $q=p^2$ and $p \equiv 1 \pmod 3$. Let $t=\pm p$. The prime p splits in $F=\mathbb{Q}(\sqrt{-3})$. On the other hand, t is not coprime to p, so there is no elliptic curve with Frobenius trace t. The corresponding q-Weil number is ζp, where ζ is a root of unity. By Theorem 2.2, D is a division algebra with center F whose invariants are $1/2$ and $1/2$ at $\mathfrak{p}$ and $\mathfrak{p}'$, respectively, and 0 everywhere else. Thus, the dimension of D over F is 4, which implies that $\dim(A)=2$. This abelian variety is supersingular, since $\pi^n \in \mathbb{Q}$ for any n such that $\zeta^n=1$. This means that A is simple over k, but is not absolutely simple: it becomes isogenous to a direct product of two supersingular elliptic curves over the degree n extension of k.

Example 4.7. Let $q=p^a$ with $a \geq 3$ odd. Let $t=\pm p^b$ with $1 \leq b < a/2$. Then F is imaginary quadratic where p splits. We must have $(\pi)=\mathfrak{p}^n(\mathfrak{p}')^m$ with $n,m \geq 1$ and $n+m=a$. The invariants of D, as a division algebra with center F, are n/a and m/a at $\mathfrak{p}$ and $\mathfrak{p}'$, respectively, and zero everywhere else. If n or m is coprime to a, then D has dimension a^2 over F, so $\dim(A)=a$.

Theorem 4.8 (Honda-Tate theorem)**.** *The image of* HT *consists of the following values:*

(1) *t coprime to p;*
(2) *If a is even: $t=\pm 2\sqrt{q}$;*
(3) *If a is even and $p \not\equiv 1 \pmod 3$: $t=\pm\sqrt{q}$;*
(4) *If a is odd and $p=2$ or 3: $t=\pm p^{\frac{a+1}{2}}$;*
(5) *If either a is odd, or a is even and $p \not\equiv 1 \pmod 4$: $t=0$.*

The first of these are not supersingular; the second are and have all their endomorphisms defined over k; the rest are but do not have all their endomorphisms defined over k.

Remark 4.9. Let d be the degree of the extension of k over which all endomorphisms of E are defined. In case (3), $d=3$. In case (5), $d=2$. In case (4), if $p=2$ then $d=4$, if $p=3$ then $d=6$. To see this, note that d is the minimal power for which $\pi^d \in \mathbb{Q}$. The corresponding q-Weil numbers π are explicitly given at the bottom of page 537 of [6].

Remark 4.10. Assume a is even. Then $\pi = \pm p^{a/2}$ are q-Weil numbers corresponding to supersingular elliptic curves with all endomorphisms defined over k. (The corresponding $t = \pm 2p^{a/2}$.) The k-isogeny classes corresponding to π and $-\pi$ are distinct. When we make a quadratic extension these two fall together: any two supersingular curves are isogenous over a quadratic extension of a field where all their endomorphisms are defined. But the extension which identifies these two classes creates also a new isogeny class; there are two classes at each stage, even though any two fixed curves eventually become isogenous.

5. Proof of Theorem 4.8

We give two different proofs. The first one uses results from the theory of abelian varieties.

Definition 5.1. Let π be a q-Weil number. We say that π is *elliptic* if $[F:\mathbb{Q}] \leq 2$ and there is only one finite place of F where π has positive valuation. We say that π is *effective* is π is a conjugate of the Frobenius π_A of some simple abelian variety over k.

It is clear that if π is elliptic (resp. effective) q-Weil number, then π^N is also elliptic (resp. effective) q^N-Weil number for any integer $N \geq 1$. It is not true in general that if π^N is elliptic then π is elliptic (see Example 4.6).

Lemma 5.2. *If π^N is effective, then π is effective.*

Proof. This is Lemme 1 on page 100 in Tate's exposé [5], which is proven using methods from the theory of abelian varieties (restriction of scalars construction). □

Lemma 5.3. *If π is effective and elliptic, then A is an elliptic curve.*

Proof. If $F = \mathbb{Q}$, then $\mathrm{ord}_p(\pi)/a = 1/2$. In this case, by Part (2) of Theorem 2.2, $\dim_{\mathbb{Q}}(D) = 4$ and by Part (3) of the same theorem, $\dim(A) = 1$. Now assume $[F:\mathbb{Q}] = 2$. Let $\mathfrak{p}$ be the place of F where $\mathrm{ord}_{\mathfrak{p}}(\pi) \neq 0$. If p splits or ramifies in F, then $\mathrm{ord}_{\mathfrak{p}}(\pi)/a = 1$. If p remains inert, then $f_{\mathfrak{p}}\mathrm{ord}_{\mathfrak{p}}(\pi)/a = 1$. In either case, $\mathrm{inv}_{\mathfrak{p}}(D) = 0$, as well as at all other finite places of F, so $D = F$. Again by Part (3) of Theorem 2.2, $\dim(A) = 1$. □

Lemma 5.4. *Let π be a q-Weil number and π_0 be a q_0-Weil number. Assume both are elliptic, q and q_0 are powers of the same prime and $\mathbb{Q}(\pi) = \mathbb{Q}(\pi_0)$. Assume moreover that* $\mathrm{ord}_{\mathfrak{p}}(\pi) \neq 0$ *if and only if* $\mathrm{ord}_{\mathfrak{p}}(\pi_0) \neq 0$. *Then there exist N and N_0 such that $\pi^N = \pi_0^{N_0}$.*

Proof. There is a unique finite place in F where π and π_0 have non-zero valuations. This place is over p. Hence we can choose n and n_0 such that $\mathrm{ord}_v(\pi^n) = \mathrm{ord}_v(\pi_0^{n_0})$ for all non-archimedean places of F. This implies that $\pi^n/\pi_0^{n_0}$ is a unit in F. Since F is either $\mathbb{Q}$ or imaginary quadratic, the only units are roots of unity. Therefore, for some m we have $(\pi^n/\pi_0^{n_0})^m = 1$. □

Proposition 5.5. *The values listed in parts (2)-(5) of Theorem 4.8 are in the image of* HT.

Proof. These values correspond to q-Weil numbers which are elliptic, and moreover, $\pi^N \in \mathbb{Q}$ for an appropriate $\mathbb{Q}$. Thus, using Lemmas 5.2-5.4 and Proposition 4.1, it is enough to show that in characteristic p there is at least one supersingular elliptic curve. This follows from Theorem V.4.1 in [1]. □

Proposition 5.6. *The values in part (1) of Theorem 4.8 are in the image of* HT*.*

Proof. Let π be the q-Weil number corresponding to t. Then p splits in F and π is elliptic (since t is coprime to p). Let $\mathfrak{p}$ be the place over p such that $\mathrm{ord}_{\mathfrak{p}}(\pi) \neq 0$.

Let $\mathcal{O}$ be the ring of integers of F. Consider $E = \mathbb{C}/\mathcal{O}$. This is an elliptic curve over $\mathbb{C}$ such that $\mathrm{End}(E) \otimes \mathbb{Q} = F$. Since E is CM, it can be defined over a finite extension H of F, and has potentially good reduction at any finite place of H. Thus, after possibly extending H, we can assume that E has everywhere good reduction. Let $\mathfrak{P}$ be a prime of H over $\mathfrak{p}$. Let $\bar{E}$ be the reduction of E modulo $\mathfrak{P}$. Proposition II.4.4 in [2] implies that $\mathrm{End}(\bar{E}) \otimes \mathbb{Q} = F$. The Frobenius π_0 of $\bar{E}$ is a q_0-Weil number, where q_0 is the cardinality of the residue field at $\mathfrak{P}$. Clearly q_0 is a power of p. After possibly replacing π by its conjugate, we can also assume that $\mathrm{ord}_{\mathfrak{p}}(\pi_0) \neq 0$. Now the conditions of Lemma 5.4 are satisfied. Since $\pi_0^{N_0}$ is obviously effective, π^N is effective and thus π is effective. Since π is also elliptic, we are done. □

Before giving the alternative proof of Theorem 4.8, we point out an important subtlety. If E and E' are isogenous curves over k, then their Weil numbers are Galois conjugate, so the fields $\mathbb{Q}(\pi) \cong \mathbb{Q}(\pi')$ are isomorphic. It is not true though that if $\mathbb{Q}(\pi) \cong \mathbb{Q}(\pi')$ then E is isogenous to E' over k. This is easy to see: take $\pm t$ in the image of HT. Since $t^2 - 4q = (-t)^2 - 4q$, the field F is the same but the curves are not isogenous. As a more complicated example, take $q = 7$, $t = 4$ and $t' = 5$. Both of these values are in the image of HT since they are coprime to p. On the other hand, $4^2 - 28 = -12 = -4 \cdot 3$ and $5^2 - 28 = -3$, so $F = \mathbb{Q}(\sqrt{-12}) \cong \mathbb{Q}(\sqrt{-3})$.

Lemma 5.7. *If $\mathbb{Q}(\pi) \cong \mathbb{Q}(\pi')$, then E and E' are isogenous over a finite degree extension of k. The degree of this extension is ≤ 6.*

Proof. After replacing π' by its conjugate, we can assume that both q-Weil numbers π and π' have non-zero valuations at the place $\mathfrak{p}$ of F. Since by Corollary 4.3 the valuations of both π and π' at $\mathfrak{p}$ are the same, $\zeta = \pi/\pi'$ is a unit in F. Since F is imaginary quadratic, ζ is a root of unity, and it is well-know that ζ is either 1, 2, 3, 4 or 6-th root of unity. If $\zeta^n = 1$, then $\pi^n = (\pi')^n$. Thus, E and E' are isogenous over degree n extension of k. □

Lemma 5.8. *Let k be a field and E an elliptic curve over k. Suppose* $\mathrm{End}_k(E)$ *contains an order $\mathcal{O}$ in an imaginary quadratic field with ring of integers $\mathcal{O}'$. Then E is isogenous over k to an elliptic curve E' such that $\mathcal{O}' \subseteq$* $\mathrm{End}_k(E')$*.*

Proof. Let $\mathfrak{c} := \{\alpha \in \mathcal{O}' \mid \alpha\mathcal{O}' \subseteq \mathcal{O}\}$. It is easy to see that $\mathfrak{c}$ is a non-zero ideal of $\mathcal{O}'$ and $\mathfrak{c} \subseteq \mathcal{O}$. The group scheme $E[\mathfrak{c}] = \cap_{\alpha\in\mathfrak{c}} E[\alpha]$ is defined over k, so there is an isogeny $\varphi : E \to E'$ over k with kernel $E[\mathfrak{c}]$; cf. Proposition 4.12 and Exercise 3.13 (e) in [1]. Fix some $c \in \mathfrak{c}$ and let $a \in \mathcal{O}'$ be arbitrary. Since ac and c are in $\mathcal{O}$, there is an isogeny $\phi_1 : E \to E$ with kernel $E[ac]$ and an isogeny $\phi_2 : E \to E$ with kernel $E[c]$. Consider the compositions $\varphi\phi_1 : E \to E'$ and $\varphi\phi_2 : E \to E'$. Since

$$\ker(\varphi\phi_2) = E[c\mathfrak{c}] \subseteq E[ac\mathfrak{c}] = \ker(\varphi\phi_1)$$

there is an isogeny $\tilde{a} : E' \to E'$ such that $\varphi \circ ac = \tilde{a} \circ \varphi \circ c$. The isogeny $\tilde{a}$ corresponds to the action of a on E'. This shows that $\mathcal{O}' \subseteq \mathrm{End}_k(E')$. □

Remark 5.9. Let $\mathcal{O}$ and $\mathcal{O}'$ be as in the previous lemma. It is not hard to show that there is an integer $n > 0$ such that $\mathcal{O} = \mathbb{Z} + n\mathcal{O}'$; see Exercise 3.20 in [1]. This implies that $\mathfrak{c}$, as an ideal of $\mathcal{O}'$, is generated by n. However, this does not mean that $E[\mathfrak{c}] = E[n]$ because $\mathfrak{c}$, as an ideal of $\mathcal{O}$, is not principal. For example, if $\mathcal{O}'$ is the ring of Gaussian integers $\mathbb{Z} + i\mathbb{Z}$ and $\mathcal{O} = \mathbb{Z} + 2i\mathbb{Z}$, then $\mathfrak{c}$ is generated by 2 and $2i$. It is easy to see that this ideal is not principal in $\mathcal{O}$.

Proposition 5.10. *Let π and π' be elliptic q-Weil numbers. If π is effective and $\mathbb{Q}(\pi) \cong \mathbb{Q}(\pi')$, then π' is also effective.*

Proof. By replacing π' by its conjugate, we can assume that π and π' have non-zero valuation at the same place $\mathfrak{p}$ of F. The relation of $\mathfrak{p}$ and the ideals (π) and (π') are given by Corollary 4.3. Hence $\zeta = \pi/\pi'$ is a root of unity. Let E be an elliptic curve over k with Weil number π, so that $F \subset \mathrm{End}_k(E) \otimes \mathbb{Q}$. If $\zeta = \pm 1$, then clearly $\zeta \in \mathrm{Aut}_k(E)$. If ζ is a root of unity of order > 2, then $\mathrm{End}_k(E)$ contains an order $\mathcal{O}$ in the imaginary quadratic field F, but it is not necessarily true[1] that $\zeta \in \mathrm{End}_k(E)$. On the other hand, thanks to Lemma 5.8, after possibly replacing E by a k-isogenous curve, we can assume that $\mathrm{End}_k(E)$ contains the ring of integers of F so that again $\zeta \in \mathrm{Aut}_k(E)$. Finally, by Lemma 6.2, a twist of E will have q-Weil number π'. □

The previous proposition reduces the proof of Theorem 4.8 to showing that for any elliptic π there exists an elliptic curve E over k such that $\mathbb{Q}(\pi_E) \cong \mathbb{Q}(\pi)$. First, we prove another supplementary lemma.

Lemma 5.11. *Let E be an elliptic curve defined over a local field K of characteristic zero. Assume the j-invariant of E is integral. Then there exists a totally ramified extension L/K such that E has good reduction over L.*

Proof. Since $j(E)$ is integral, E has potential good reduction by Proposition VII.5.5 in [1]. Let K'/K be a finite extension such that E has good reduction over K'. We can assume that K'/K is Galois. Consider the natural surjective homomorphism $\mathrm{Gal}(K'/K) \to \mathrm{Gal}(k'/k)$, where k' and k are the residue fields of K' and K, respectively. This homomorphism splits since we have a lifting to $\mathrm{Gal}(K'/K)$ of a generator of the cyclic group $\mathrm{Gal}(k'/k)$. Fix such a splitting $\mathrm{Gal}(k'/k) \to \mathrm{Gal}(K'/K)$, and let W be the image. The field $L = (K')^W$ is totally ramified over K. We claim that E has good reduction over L. Indeed, since K'/L is unramified the reduction type of E over K' is the same as the reduction type of E over L; see [1, Prop. VII.5.4]. □

Proposition 5.12. *Let π be an elliptic q-Weil number. Let $F = \mathbb{Q}(\pi)$. There exists an elliptic curve E over k such that $\mathbb{Q}(\pi_E) \cong F$.*

Proof. Suppose $F = \mathbb{Q}$. Then a is even and π is equal to either $p^{a/2}$ or $-p^{a/2}$. It is known that there is a supersingular elliptic curve E defined over $\mathbb{F}_p$. If $p \geq 3$, then we can assume $\#E(\mathbb{F}_p) = p + 1$; see Example V.4.5 and Exercise V.5.10 in [1]. If $p = 2$, the curve given by

[1] This was pointed out to me by Jiangwei Xue.

the equation $E : y^2 + y = x^3$ is supersingular and $\#E(\mathbb{F}_2) = 3$. The Weil number of E over $\mathbb{F}_p$ is $\pi_E = \pm\sqrt{-p}$. Over k, the Weil number of E is $\pi_E^a = (-p)^{a/2}$, so $\mathbb{Q}(\pi_E^a) = F$, as was required to show.

Now suppose F is imaginary quadratic and p splits in F. Let $\mathfrak{p}$ be the place where π has positive valuation. By Corollary 4.3, $\mathfrak{p}^a = (\pi)$, so the order of $\mathfrak{p}$ in the class group of F divides a. Let $\mathcal{O}_F$ be the ring of integers of F. Let $\widetilde{E} = \mathbb{C}/\mathcal{O}_F$. This curve has CM by F. It is known that $\widetilde{E}$ can be defined over the Hilbert Class Field H of F, and that its j-invariant is an algebraic integer. Moreover, by [3, p. 136] all endomorphism of $\widetilde{E}$ are defined over H, so $\mathrm{End}_H(\widetilde{E}) \otimes \mathbb{Q} = F$. Let $\mathfrak{P}$ be a prime of H over $\mathfrak{p}$. By class field theory, the degree of residue field extension $[\mathcal{O}_H/\mathfrak{P} : \mathcal{O}_F/\mathfrak{p}]$ is the order of $\mathfrak{p}$ in the class group, so it divides a. Since $\mathcal{O}_F/\mathfrak{p} = \mathbb{F}_p$, we conclude that $\mathcal{O}_H/\mathfrak{P}$ is a subfield of k. Consider $\widetilde{E}$ over the completion $H_{\mathfrak{P}}$. In principle, $\widetilde{E}$ need not have good reduction over $H_{\mathfrak{P}}$, but by Lemma 5.11, we can pass to a finite totally ramified extension L of $H_{\mathfrak{P}}$ where $\widetilde{E}$ has good reduction. This does not affect the residue field. Therefore, without loss of generality, assume $\widetilde{E}$ has good reduction modulo $\mathfrak{P}$. The reduction E of $\widetilde{E}$ modulo $\mathfrak{P}$ is defined over k and contains F in its algebra of endomorphism; see [3, pp. 120-121]. Since p splits in F, E is ordinary and $F = \mathbb{Q}(\pi_E)$.

Now suppose F is imaginary quadratic but p does not split. Then Corollary 4.3 and the previous construction produce a curve E over k which contains F as a subfield of its endomorphism algebra D. Suppose $D \neq F$. Then the Frobenius π' of E is in $\mathbb{Q}$. It is a q-Weil number, which, when considered as an element of F, has positive valuation only at $\mathfrak{p}$. Thus $\zeta = \pi/\pi'$ is a root of 1. Using the argument in the proof of Proposition 5.10, we can assume $\zeta \in \mathrm{Aut}_k(E)$. By Lemma 6.2, a twist of E has q-Weil number π. □

6. Twists of elliptic curves

Let K be an arbitrary perfect field. An elliptic curve E' defined over K is a *twist* of E if E' is isomorphic to E over $\bar{K}$ (but not necessarily over K). Since the j-invariant of an elliptic curve characterizes the $\bar{K}$-isomorphism class of E, the curve E' is a twist of E if and only if $j(E') = j(E)$. Let $\phi : E' \to E$ be an isomorphism defined over $\bar{K}$. Let $\sigma \in \mathrm{Gal}(\bar{K}/K) =: G$. Then $\phi^\sigma\phi^{-1}$ is an automorphism of E. The map $\xi : G \to \mathrm{Aut}(E)$ given by $\sigma \mapsto \xi_\sigma = \phi^\sigma\phi^{-1}$ measures the failure of ϕ to be defined over K. This map is 1-cocycle, and in fact the twists of E are in bijection with $H^1(G, \mathrm{Aut}(E))$; see Theorem X.2.2 in [1].

Example 6.1. If $j(E) \neq 0, 1728$ then $\mathrm{Aut}(E) = \mathrm{Aut}_K(E) = \mathbb{Z}/2\mathbb{Z}$, where the unique nontrivial automorphism is the negation: $P \mapsto -P$. In this case, $H^1(G, \mathrm{Aut}(E)) = \mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z})$, and the only twists are the quadratic twists. If the characteristic of K is not 2, then $\mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z}) \cong K^\times/(K^\times)^2$. Suppose E is given by the equation $y^2 = f(x)$, and let $d \in K^\times$ be square-free. We obtain a homomorphism $\chi_d : G \to \mathbb{Z}/2\mathbb{Z}$ by $\sigma \mapsto \sigma(\sqrt{d})/\sqrt{d}$. Multiplication by $\chi_d(\sigma)$ is an automorphism of E. The corresponding quadratic twist E_d of E is the elliptic curve defined by the equation $dy^2 = f(x)$. This twist can also be characterized as the elliptic curve E' whose set of $\bar{K}$ points as a G-module is the set $E(\bar{K})$ with a "twisted" Galois action where σ sends P to $\chi_d(\sigma)\sigma(P)$, i.e.,

$$\sigma \circ (x, y) = (\sigma x, \chi_d(\sigma)\sigma y).$$

We are particularly interested in twists by automorphisms defined over K; these correspond to the elements of $H^1(G, \mathrm{Aut}_K(E))$. Since the action of Galois on $\mathrm{Aut}_K(E)$ is trivial,

$$H^1(G, \mathrm{Aut}_K(E)) \cong \mathrm{Hom}(G, \mathrm{Aut}_K(E)).$$

Let $\chi : G \to \mathrm{Aut}_K(E)$ be a homomorphism. The corresponding twist E_χ of E is uniquely characterized by the property that the set $E_\chi(\bar{K})$ as a G-module is $E(\bar{K})$ with a "twisted" Galois action:

$$\sigma \circ P = \chi(\sigma) \circ \sigma(P),$$

where $P \in E(\bar{K})$, $\sigma(P)$ indicates the action of G on $E(\bar{K})$ and $\chi(\sigma) \circ Q$ is the image of $Q \in E(\bar{K})$ under the action of automorphism $\chi(\sigma)$.

Now assume $K = k$ is a finite field. Then G is topologically generated by the Frobenius, so any continuous homomorphism $G \to \mathrm{Aut}_k(E)$ is uniquely determined by the image of Frob_q. It is known that an automorphism of E has order $1, 2, 3, 4$, or 6. Let $\zeta \in \mathrm{Aut}_k(E)$. Denote the twist corresponding to $\chi(\mathrm{Frob}_q) = \zeta$ by E_ζ. The Frobenius Frob_q acts on $E_\zeta(\bar{k})$ (identified with $E(\bar{k})$) by

$$\mathrm{Frob}_q \circ (x, y) = \zeta \circ (x^q, y^q).$$

Denote the linear transformation induced by the Frobenius on $V_\ell(E_\zeta)$ by $\pi_{\ell,\zeta}$. From previous discussion, if we identify $V_\ell(E_\zeta) = V_\ell(E)$, then $\pi_{\ell,\zeta}$ action on $V_\ell(E_\zeta)$ corresponds to the action of $\pi_\ell\zeta_\ell$ on $V_\ell(E)$. Since π_ℓ and ζ_ℓ are semisimple commuting operators, they can be simultaneously diagonalized (over $\overline{\mathbb{Q}}_\ell$). Now ζ_ℓ has as its characteristic polynomial one of the following

$$(x-1)^2, \quad (x+1)^2, \quad x^2+1, \quad x^2+x+1, \quad x^2-x+1$$

depending on its order being $1, 2, 4, 3$, or 6. Fix a root i of $x^2 + 1$, and ρ of $x^2 + x + 1$.

Lemma 6.2. *Let π be a q-Weil number corresponding to E.*

(1) *$-\pi$ is a q-Weil number for E_ζ if ζ has order* 2.
(2) *$i\pi$ is a q-Weil number for E_ζ or $E_{\zeta^{-1}}$ if ζ has order* 4.
(3) *$\rho\pi$ is a q-Weil number for E_ζ or $E_{\zeta^{-1}}$ if ζ has order* 3.

Proof. The linear operator π_ℓ has eigenvalues $\{\pi, \bar{\pi}\}$, and ζ_ℓ has eigenvalues $\{\zeta, \zeta^{-1}\}$. It is easy to see that the eigenvalues of $\pi_\ell\zeta_\ell$ are either $\{\zeta\pi, \zeta^{-1}\bar{\pi}\}$ or $\{\zeta^{-1}\pi, \zeta\bar{\pi}\}$. □

Remark 6.3. Suppose $p \neq 2$. Let E be an elliptic curve over k given by the equation $y^2 = f(x)$. Fix a non-square $\eta \in k$. The quadratic twist E' of E (up to k-isomorphism) is given by $\eta y^2 = f(x)$. We have

$$\#E(k) + \#E'(k) = 2q + 2.$$

To see this one can argue as follows. The k-rational points at infinity of E and E' contribute 2 to the sum $\#E(k) + \#E'(k)$. Suppose $x_0 \in k$ is such that $f(x_0) = 0$. Then the point $(0, x_0)$ belongs to both $E(k)$ and $E'(k)$, so contributes 2 to the sum of their orders. Now consider $x_0 \in k$ such that $f(x_0) \neq 0$. Then either $f(x_0)$ is a square in k and we get 2 k-rational points on E, or $f(x_0)$ is a non-square. In the second case, $\eta^{-1}f(x_0)$ is a square, and we get 2 k-rational points on E'. Thus, each x_0 which is not a zero of $f(x)$ contributes exactly 2 to the sum $\#E(k) + \#E'(k)$.

Let t and t' be the traces of the Frobenius of E and E'. Since $t = q + 1 - \#E(k)$, the previous lemma implies that $t + t' = 0$. But the roots of $x^2 - tx + q$ are the negatives of the roots of $x^2 + tx + q$. Hence the q-Weil number of E is the negative of the q-Weil number of E'. This gives an alternative direct proof of Part (1) of Lemma 6.2.

Example 6.4. Assume $k = \mathbb{F}_2$. By Theorem 4.8, $t = 0, \pm 2$ are in the image of HT, and these values are exactly the values corresponding to supersingular elliptic curves. Consider the following elliptic curves over $\mathbb{F}_2$:

$$\begin{aligned} E_1 &: y^2 + y = x^3 \\ E_2 &: y^2 + y = x^3 + x^2 \\ E_3 &: y^2 + y = x^3 + x^2 + 1. \end{aligned}$$

It is easy to check that $\#E_1(k) = 3$, $\#E_2(k) = 5$, $\#E_3(k) = 1$. Hence the corresponding trace t is $0, -2, 2$, respectively. Also, as one easily checks, all three curves have j-invariant 0, so they are twists of each other. In fact, up to $\bar{k}$-isomorphism, there is a unique supersingular elliptic curve in characteristic 2; see Exercise V.5.9 in [1].

References

[1] J. Silverman, *The arithmetic of elliptic curves*, GTM 106.

[2] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, GTM 151.

[3] S. Lang, *Elliptic functions*, GTM 112.

[4] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Inventiones Mathematicae **2** (1966), 134–144.

[5] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki, Exposé 352 (1968/69).

[6] W. Waterhouse, *Abelian varieties over finite fields*, Annales scientifiques de l'École Normale Supérieure **2** (1969), 521–560.