INTEGRAL TATE MODULES AND SPLITTING OF PRIMES IN TORSION FIELDS OF ELLIPTIC CURVES

TOMMASO GIORGIO CENTELEGHE

ABSTRACT. Let E be an elliptic curve over a finite field k, and ℓ a prime number different from the characteristic of k. In this paper we consider the problem of finding the structure of the Tate module $T_\ell(E)$ as an integral Galois representations of k. We indicate an explicit procedure to solve this problem starting from the characteristic polynomial $f_E(x)$ and the j-invariant j_E of E. Hilbert Class Polynomials of imaginary quadratic orders play here an important role. We give a global application to the study of prime-splitting in torsion fields of elliptic curves over number fields.

1. Introduction

Let k be a finite field of characteristic p and cardinality q, $\bar{k}$ a fixed algebraic closure of k, and G_k the corresponding absolute Galois group. Let E be an elliptic curve over k, $\pi_E : E \to E$ the Frobenius isogeny relative to k, and a_E the "error term" $q + 1 - |E(k)|$. For a prime $\ell \neq p$, it is well known that the isogeny invariant of E given by the *rational* ℓ-adic Tate module $V_\ell(E) = T_\ell(E) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ is a semi-simple Galois representation of k. Thus its isomorphism class is determined by the characteristic polynomial

$$f_E(x) = x^2 - a_E x + q$$

of the arithmetic Frobenius $\mathrm{Frob}_k \in G_k$, which also uniquely identifies the k-isogeny class of E (see [12], Théorème 1). On the other hand, the *integral* representation given by $T_\ell(E)$ is not an isogeny invariant, and finding its Galois structure requires, in general, a refinement of the information carried by $f_E(x)$ alone.

In [2], Duke and Tóth study the problem of finding $T_\ell(E)$ from a slightly different perspective. Their main result roughly says that in order to determine $T_\ell(E)$ in the crucial case where $\mathrm{End}_k(E) \otimes \mathbf{Q}$ is an imaginary quadratic field, it suffices to know $f_E(x)$ and the order $\mathrm{End}_k(E)$. More precisely, out of $f_E(x)$ and the *index*

$$b_E = [\mathrm{End}_k(E) : \mathbf{Z}[\pi_E]] \in \mathbf{Z}_{>0} \cup \{\infty\},$$

they construct an explicit two-by-two matrix with integral entries that gives the action of Frob_k on $T_\ell(E)$ in a suitable $\mathbf{Z}_\ell$-basis, for any $\ell \neq p$.

In this paper we go one step further and explain how, in almost all cases, the index b_E can be recovered from the j-invariant j_E of E and from $f_E(x)$

using a procedure involving a family of polynomials $\{\mathcal{P}_D(x)\}_{D\in\mathbf{Z}_{\leq 0}}$ associated to singular moduli of elliptic curves (see (1)). Furthermore, we offer an alternative proof of the result of Duke and Tóth which avoids Deuring's Lifting Lemma. Instead, it relies on the observation that, when b_E is finite, $T_\ell(E)$ is free of rank one over $\mathrm{End}_k(E)\otimes\mathbf{Z}_\ell$ (see § 2). This freeness is a special instance of a more general fact on abelian varieties with complex multiplication by a Gorenstein ring (see [8], Remark in § 4). For this reason, the variant we give is suitable for generalizations of [2] to the higher dimensional setting of abelian varieties of GL_2-type.

Lastly, we remark that the method we use to find b_E from $f_E(x)$ and j_E has been known for long time when E is ordinary as a consequence of Deuring's Lifting Lemma. However, the observation that it remains valid in the supersingular case depends on the nature of the ring $\mathrm{End}_k(E)$ when E does not have all of its endomorphisms defined over k, and may contain some novelty (see § 2).

Before stating the main result of this paper we need some definitions and another piece of notation.

Definition 1. We say that the elliptic curve E over k is *special* if $p\equiv 3 \pmod 4$, the degree $[k:\mathbf{F}_p]$ is odd, $a_E=0$, and $j_E=1728\in k$.

Let $D\in\mathbf{Z}$ be a negative discriminant, i.e., $D<0$ and $D\equiv 0$ or $1 \pmod 4$, and denote by $\mathcal{O}_D$ the imaginary quadratic order of discriminant D, viewed inside the field $\mathbf{C}$ of complex numbers. Let

$$\mathcal{P}_D(x)=\prod_{\mathcal{O}_D\subset\mathrm{End}(\mathbf{C}/\mathfrak{a})}(x-j_{\mathbf{C}/\mathfrak{a}}) \tag{1}$$

be the separable, monic polynomial in $\mathbf{C}[x]$ whose roots are all the j-invariants of complex elliptic curves $\mathbf{C}/\mathfrak{a}$ whose endomorphism rings contain the order $\mathcal{O}_D$. For any given D these values of j are algebraic integers which are permuted by the absolute Galois group of $\mathbf{Q}$, and so $\mathcal{P}_D(x)\in\mathbf{Z}[x]$ (see [3], § 11). Moreover two such j-invariants $j_{\mathbf{C}/\mathfrak{a}}$ and $j_{\mathbf{C}/\mathfrak{a}'}$ lie in the same $G_{\mathbf{Q}}$-orbit if and only if $\mathrm{End}_{\mathbf{C}}(\mathbf{C}/\mathfrak{a})=\mathrm{End}_{\mathbf{C}}(\mathbf{C}/\mathfrak{a}')$. The irreducible factors of $\mathcal{P}_D(x)$ are usually called Hilbert Class Polynomials of the corresponding imaginary quadratic orders.

Extend the definition of $\mathcal{P}_D(x)$ to all $D\leq 0$ by setting $\mathcal{P}_0(x)=0$ and $\mathcal{P}_D(x)=1$ for all negative D with $D\equiv 2$ or $3 \pmod 4$. Denote by Δ_E the discriminant a_E^2-4q of $f_E(x)$, and by $\bar{g}(x)\in\mathbf{F}_p[x]$ the reduction modulo p of any given polynomial $g(x)\in\mathbf{Z}[x]$. Our main result says:

Theorem 2. *Let E be an elliptic curve over k. Define*

$$\beta_E=\sup_{h>0}\{h : h^2|\Delta_E \ \text{ and } \ \bar{\mathcal{P}}_{\Delta_E/h^2}(j_E)=0\},$$

and

$$\sigma_E = \begin{cases} \begin{pmatrix} \dfrac{a_E\beta_E - \Delta_E}{2\beta_E} & \dfrac{\Delta_E(\beta_E^2 - \Delta_E)}{4\beta_E^3} \\ \beta_E & \dfrac{a_E\beta_E + \Delta_E}{2\beta_E} \end{pmatrix} & \text{if } \Delta_E < 0, \\ \\ \begin{pmatrix} a_E/2 & 0 \\ 0 & a_E/2 \end{pmatrix} & \text{if } \Delta_E = 0. \end{cases}$$

The matrix σ_E has integral entries and, for any prime $\ell \neq p$, describes the action of Frob_k *on $T_\ell(E)$, with respect to a suitable $\mathbf{Z}_\ell$-basis, provided that ℓ be odd if E is special. Furthermore, $b_E = \beta_E$ if E is not special, and $b_E = \beta_E/2$ or β_E otherwise.*

If E is special and $\ell = 2$ then b_E is either p^m or $2p^m$, where $[k : \mathbf{F}_p] = 2m + 1$. For completeness, the two corresponding possibilities for the action of Frob_k on $T_2(E)$ are given in § 3. Together with Panagiotis Tsaknias we implemented a Magma package which computes σ_E from E (see [1]).

An immediate consequence of the theorem is that if N is a positive integer not divisible by p then $\sigma_E \pmod N$ describes the action of Frob_k on the N-th torsion subgroup $E[N](\bar{k})$ of E. Compared to [2], Theorem 2 has the extra feature of indicating a way to construct σ_E from the basic invariants $f_E(x)$ and j_E.

From Theorem 2 we deduce the following global application. Let K be a number field, and $\mathcal{E}$ an elliptic curve over K with j-invariant $j_{\mathcal{E}}$. If $\mathfrak{p}$ is a finite prime of K with residue field $k_{\mathfrak{p}}$ at which $\mathcal{E}$ has good reduction $\mathcal{E}_{\mathfrak{p}}$, denote by $a_{\mathfrak{p}}$ the error term $|k_{\mathfrak{p}}| + 1 - |\mathcal{E}_{\mathfrak{p}}(k_{\mathfrak{p}})|$, and by $\Delta_{\mathfrak{p}}$ the discriminant $a_{\mathfrak{p}}^2 - 4|k_{\mathfrak{p}}|$ of the characteristic polynomial $f_{\mathcal{E}_{\mathfrak{p}}}(x)$ of $\mathcal{E}_{\mathfrak{p}}$. If N is a positive integer, let $K(\mathcal{E}[N])/K$ be the extension of K obtained by "joining the coordinates" of the N-torsion points of $\mathcal{E}$ (see § 4 for more details).

Theorem 3. *Let N be a positive integer, and $\mathfrak{p}$ a finite prime of K not dividing N and at which $\mathcal{E}$ has good reduction. If $N = 2$, assume furthermore that $\mathcal{E}_{\mathfrak{p}}$ is not special. The prime $\mathfrak{p}$ splits completely in $K(\mathcal{E}[N])/K$ if and only if the following conditions hold:*

(1) $N^2 | \Delta_{\mathfrak{p}}$ and $\mathcal{P}_{\Delta_{\mathfrak{p}}/N^2}(j_{\mathcal{E}}) \equiv 0 \pmod{\mathfrak{p}}$;

(2) $a_{\mathfrak{p}} \equiv 2 + \frac{\Delta_{\mathfrak{p}}}{N} \pmod{N^*}$;

where $N^* = N$ if N is odd and $N^* = 2N$ if N is even.

Theorem 3 gives an idea of how a reciprocity law in a non-abelian context may appear. It emphasizes the role that the family of polynomials $\{\mathcal{P}_{\mathcal{D}}(x)\}_{D \leq 0}$ play in the study of prime-splitting in torsion field of elliptic curves over number fields. More generally, Theorem 2 can be used to describe the conjugacy class of $\rho_{\mathcal{E}[N]}(\mathrm{Frob}_{\mathfrak{p}})$ in $\mathrm{Aut}(\mathcal{E}[N]) \simeq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, where $\mathrm{Frob}_{\mathfrak{p}}$ is a Frobenius element at $\mathfrak{p}$.

The paper is structured as follows: in § 2 we explain how to compute b_E from $f_E(x)$ and j_E, in § 3 we give a proof of the main result, and § 4 contains the details of the global application given by Theorem 3. We will retain throughout the notation established so far.

2. The Index b_E

In this section we describe a method for finding the index b_E from $f_E(x)$ and j_E using the family of polynomials $\mathcal{P}_D(x)$. The proof differs in the ordinary and supersingular cases, even though the statement is uniform (see Proposition 5).

We clarify our terminology on complex multiplication of elliptic curves, which follows [4]. If $\bar{\kappa}$ is an algebraic closure of a field κ then we say that an elliptic curve A over κ *has complex multiplication by an imaginary quadratic order* $\mathcal{O}$ (abbreviated CM by $\mathcal{O}$) if there exists an injection

$$\iota : \mathcal{O} \hookrightarrow \mathrm{End}_{\bar{\kappa}}(A \times_\kappa \bar{\kappa})$$

which is maximal, in the sense that it cannot be extended to a strictly larger imaginary quadratic order $\mathcal{O}' \supsetneq \mathcal{O}$.

We observe that an elliptic curve E over a finite field k has CM by $\mathrm{End}_k(E)$ when this ring is an imaginary quadratic order. The reason is that if k'/k is any field extension, then the natural inclusion

$$\mathrm{End}_k(E) \hookrightarrow \mathrm{End}_{k'}(E \times_k k') \tag{2}$$

has torsion free cokernel (see [8], § 4). Furthermore, if E is ordinary then $\mathrm{End}_k(E)$ is an imaginary quadratic order and the map (2) is an isomorphism for all k'/k. Hence any ordinary E has CM *only* by $\mathrm{End}_k(E)$.

Proposition 4. *Let D be a negative discriminant. The j-invariant j_E of E is a root of the reduction of $\mathcal{P}_D(x)$ modulo p if and only if E has CM by an imaginary quadratic order $\mathcal{O}$ containing $\mathcal{O}_D$.*

The proposition is well-known to experts, therefore we omit its proof. We shall only say that the "only if" part follows from the properties of good reduction of CM elliptic curves in characteristic zero (see [8], § 5), and the "if" part is a consequence of Deuring's Lifting Lemma (see [5], § 15.5 Theorem 14).

Consider now the quantity

$$\beta_E = \sup_{h>0}\{h : h^2|\Delta_E \ \text{ and } \ \bar{\mathcal{P}}_{\Delta_E/h^2}(j_E) = 0\}$$

introduced in Theorem 2. The main proposition of the section is:

Proposition 5. *If E is not special then $b_E = \beta_E$. If E is special, then $\beta_E = 2p^m$ and $b_E = \beta_E$ or $\beta_E/2$, where $[k : \mathbf{F}_p] = 2m + 1$.*

Proof. We shall distinguish three cases

(1) E is ordinary;
(2) E is supersingular and $\mathrm{End}_k(E) \otimes \mathbf{Q}$ is an imaginary quadratic field;
(3) E is supersingular and $\mathrm{End}_k(E) \otimes \mathbf{Q}$ is the definite quaternion algebra over $\mathbf{Q}$ of discriminant p.

Case (2) is the only case where E acquires new endomorphisms over a suitable (typically quadratic) finite extension k' of k, and we will refer to it as the *unstable supersingular* case. Case (3) occurs if and only if b_E is infinite or, equivalently, $\Delta_E = 0$; in this situation the proposition is trivial and we will continue assuming b_E finite.

The Frobenius isogeny π_E generates a subring of $\mathrm{End}_k(E)$ of discriminant Δ_E and gives rise to an inclusion

$$\iota : \mathcal{O}_{\Delta_E} \longrightarrow \mathrm{End}_k(E).$$

Clearly b_E is the largest $h > 0$ such that two conditions hold:

- there exists a quadratic order $\mathcal{O} \supset \mathcal{O}_{\Delta_E}$ with $[\mathcal{O} : \mathcal{O}_{\Delta_E}] = h$;
- ι extends to an inclusion $\iota' : \mathcal{O} \hookrightarrow \mathrm{End}_k(E)$.

Given this, case (1) follows immediately from Proposition 4, since an ordinary elliptic curve E has complex multiplication only by $\mathrm{End}_k(E)$.

We are therefore left with the unstable supersingular case. We proceed with a case-by-case computation of both b_E and β_E. The polynomials $f_E(x)$ arising in case (2) are characterized by the conditions $\Delta_E < 0$ *and* p does not split completely in $\mathbf{Q}(\sqrt{\Delta_E})$ (see [13], § 4.1 or [12], Théorème 1). All possibilities are listed in the following table, where $r = [k : \mathbf{F}_p]$.

Table 1. Unstable supersingular Weil polynomials over k.

$f_E(x)$	p	r	Δ_E	b_E
$x^2 + p^{2m+1}$	-	$2m+1$	$-4p^{2m+1}$	p^m or $2p^m$
$x^2 + p^{2m}$	$\not\equiv 1 \bmod 4$	$2m$	$-4p^{2m}$	p^m
$x^2 \pm p^m x + p^{2m}$	$\not\equiv 1 \bmod 3$	$2m$	$-3p^{2m}$	p^m
$x^2 \pm p^{m+1} x + p^{2m+1}$	2 or 3	$2m+1$	$-(4-p)p^{2m+1}$	p^m

The values of the index b_E appearing in the last column of the table are readily computed from the corresponding Δ_E, taking into account that $\mathrm{End}_k(E)$ is maximal locally at p (see [13], Theorem 4.2). The point is that, except for the case where $p \equiv 3 \pmod 4$, $r = 2m+1$ is odd, and $f_E(x) = x^2 + p^{2m+1}$, the order $\mathbf{Z}[\pi_E]$ is maximal at every prime $\ell \neq p$, and thus $\mathrm{End}_k(E)$ is the maximal order, from which the equality $b_E = p^m$ follows.

On the other hand, if $p \equiv 3 \pmod 4$ and $f_E(x) = x^2 + p^{2m+1}$, then b_E is either $2p^m$ or p^m, according to whether $\mathrm{End}_k(E)$ is maximal or sits in the maximal order with index 2, respectively. Since both cases do arise for suitable E ([13], Theorem 4.2), b_E is not constant on the k-isogeny class defined by $f_E(x)$ and cannot be determined from $f_E(x)$ alone.

We now turn to the study of β_E. Since E has Complex Multiplication by $\mathrm{End}_k(E)$, Proposition 4 implies that

$$\beta_E \geq b_E.$$

Moreover, if $\mathrm{End}_k(E)$ is the maximal order, then β_E cannot be larger than b_E (for Δ_E/h^2 is not a discriminant if $h > b_E$), and $\beta_E = b_E$ follows. We are therefore left with showing that $\beta_E = b_E$ when $\mathrm{End}_k(E)$ is not maximal and E is not special. Notice that in this case $\mathrm{End}_k(E)$ has discriminant $-4p$, and $p \equiv 3 \pmod 4$. By Proposition 4, it is enough to show that:

Lemma 6. *Let $p \equiv 3 \pmod 4$, assume that $r = 2m+1$ is odd, and let E be an elliptic curve over k with $f_E(x) = x^2 + p^{2m+1}$. If $j_E \neq 1728$, then E has CM by $\mathcal{O}_{-p}$ or $\mathcal{O}_{-4p}$ but not by both these rings. In the first case $b_E = 2p^m$, in the second one $b_E = p^m$.*

Proof. Choose a square root $\sqrt{-p}$ of $-p$ inside the imaginary quadratic field $\mathcal{O}_{-p} \otimes \mathbf{Q}$, and identify $\mathbf{Z}[\pi_E]$ with an order of $\mathcal{O}_{-p} \otimes \mathbf{Q}$ via the map sending π_E to $\sqrt{-p}^{2m+1}$. By the maximality of $\mathrm{End}_k(E)$ at p already mentioned, the inclusion $\mathbf{Z}[\pi_E] \subset \mathrm{End}_k(E)$ extends to an embedding $\tau : \mathcal{O}_{-4p} \hookrightarrow \mathrm{End}_k(E)$, sending $\sqrt{-p}^{2m+1}$ to π_E. If τ further extends to an embedding of the maximal order $\mathcal{O}_{-p}$, then $b_E = 2p^m$ and E has CM by $\mathcal{O}_{-p}$, otherwise $b_E = p^m$ and E has CM by $\mathcal{O}_{-4p}$.

To prove the lemma, we need to show that if $j_E \neq 1728$ then it is not possible to find two inclusions

$$\iota_1 : \mathcal{O}_{-p} \longhookrightarrow \mathrm{End}_{\bar{k}}(E \times_k \bar{k}) \quad \text{and} \quad \iota_2 : \mathcal{O}_{-4p} \longhookrightarrow \mathrm{End}_{\bar{k}}(E \times_k \bar{k})$$

which are both maximal, in the sense of the definition of complex multiplication given at the beginning of the section. Since 1728 is the only supersingular invariant when $p = 3$, we may and will continue the proof assuming $p > 3$.

We will argue in two steps: first we show that the existence of a maximal embedding

$$\iota : \mathcal{O} \longhookrightarrow \mathrm{End}_{\bar{k}}(E \times_k \bar{k}),$$

where $\mathcal{O} = \mathcal{O}_{-p}$ or $\mathcal{O}_{-4p}$, ensures the existence of a k-form E_θ of E which is k-isogenous to E and for which $\mathrm{End}_k(E_\theta) \simeq \mathcal{O}$. Next, using that $j_E \neq 1728$, we show that the ring of k-endomorphisms of any k-form of E is isomorphic to $\mathrm{End}_k(E)$.

Before carrying out this plan, we make a digression on the study k-forms of E (see [10] for more details). The absolute Galois group G_k acts in a natural way on the left of the group $\mathrm{Aut}_{\bar{k}}(E \times_k \bar{k})$. A 1-cocycle θ of this action defines an elliptic curve E_θ over k and an isomorphism

$$\varphi_\theta : E_\theta \times_k \bar{k} \xrightarrow{\sim} E \times_k \bar{k}$$

such that, if $\sigma \in G_k$ is the arithmetic Frobenius of k, the isogeny π_{E_θ} corresponds to $\theta(\sigma)\pi_E$ under the identification

$$\mathrm{End}_{\bar{k}}(E_\theta \times_k \bar{k}) \simeq \mathrm{End}_{\bar{k}}(E \times_k \bar{k})$$

induced by φ_θ. In particular, extension of scalars identifies $\mathrm{End}_k(E_\theta)$ with the subring of $\mathrm{End}_{\bar{k}}(E \times_k \bar{k})$ given by the centralizer of $\theta(\sigma)\pi_E$. This construction induces a bijection

$$H^1(G_k, \mathrm{Aut}_{\bar{k}}(E \times_k \bar{k})) \xrightarrow{\sim} \{k\text{-forms of } E\}_{/\sim}.$$

Since $\pi_E^2 = -p^{2m+1}$, the curve E acquires all of its geometric endomorphisms over the degree 2 extension of k inside $\bar{k}$, therefore the Galois action of G_k on $\operatorname{End}_{\bar{k}}(E \times_k \bar{k})$, which is non-trivial, becomes trivial when restricted to its index 2 subgroup. The group $\operatorname{Aut}_{\bar{k}}(E \times_k \bar{k})$ is cyclic of order 2, 4, or 6, because $p > 3$. It follows that $\sigma \in G_k$ acts on $\operatorname{Aut}_{\bar{k}}(E \times_k \bar{k})$ by inversion, and it is easy to see that evaluation of cocycles at σ induces an isomorphism

$$H^1(G_k, \operatorname{Aut}_{\bar{k}}(E \times_k \bar{k})) \xrightarrow{\sim} \operatorname{Aut}_{\bar{k}}(E \times_k \bar{k}) / \operatorname{Aut}_{\bar{k}}(E \times_k \bar{k})^2,$$

in particular $H^1(G_k, \operatorname{Aut}_{\bar{k}}(E \times_k \bar{k}))$ has order two.

Let now $\mathcal{O}$ be either $\mathcal{O}_{-p}$ or $\mathcal{O}_{-4p}$ and let $\iota : \mathcal{O} \hookrightarrow \operatorname{End}_{\bar{k}}(E \times_k \bar{k})$ be a maximal embedding. The unique ideal I_p of $\operatorname{End}_{\bar{k}}(E \times_k \bar{k})$ of reduced norm p is principal and generated by $\iota(\sqrt{-p})$. Since the reduced norm of π_E is p^{2m+1}, there exists a unit $u \in \operatorname{Aut}_{\bar{k}}(E \times_k \bar{k})$ such that

$$\iota(\sqrt{-p}^{2m+1}) = u\pi_E.$$

If θ is the 1-cocycle of G_k valued in $\operatorname{Aut}_{\bar{k}}(E \times_k \bar{k})$ satisfying $\theta(\sigma) = u$, the construction described above leads to a k-form E_θ of E and an isomorphism $\varphi_\theta : E_\theta \times_k \bar{k} \xrightarrow{\sim} E \times_k \bar{k}$ such that π_{E_θ} corresponds to $u\pi_E$ and the ring $\operatorname{End}_k(E_\theta)$ corresponds to $\iota(\mathcal{O})$, the centralizer of $u\pi_E$ in $\operatorname{End}_{\bar{k}}(E \times_k \bar{k})$. Therefore

$$\operatorname{End}_k(E_\theta) \simeq \mathcal{O},$$

and the first step of our program is complete.

To prove the second step, observe that the assumption $j_E \neq 1728$ is equivalent to require that $-1 \in \operatorname{Aut}_{\bar{k}}(E \times_k \bar{k})$ not be a square. Therefore the 1-cocycle sending σ to -1 on the one hand describes the only non-trivial k-form of E, on the other hand it defines an elliptic curve over k whose ring of k-endomorphisms is isomorphic to $\operatorname{End}_k(E)$, since the centralizer of $-\pi_E$ is the same as that of π_E. We conclude that if $j_E \neq 1728$ the two non-isomorphic k-forms of E have isomorphic k-endomorphism rings. This completes the proof of the lemma. □

To complete the proof of Proposition 5 we are only left with showing that if E is special then $\beta_E = 2p^m$. Equivalently, we need to show that any special E has CM by $\mathcal{O}_{-p}$. This was observed by Elkies in [4], where he considered the elliptic curve over $\mathbf{F}_p$ given by $y^2 = x^3 - x$. □

We make the final remark that if E is special, then the value of b_E cannot be determined from the sole knowledge of $f_E(x)$ and j_E. One can show that $b_E = 2p^m$ if the two-torsion $E[2]$ of E is all defined over k, and $b_E = p^m$ otherwise, where $[k : \mathbf{F}_p] = 2m + 1$.

3. Proof of Theorem 2

After explaining in § 2 how to find the index b_E from $f_E(x)$ and j_E, we are now ready to prove the main theorem of the paper.

We begin by pointing out the basic fact that the action of Frob_k on $T_\ell(E)$ is the *same* as that induced by π_E via functoriality of T_ℓ. Next, we observe that the theorem is trivial if E is supersingular with all of its geometric endomorphisms defined over k. In fact in this case $\Delta_E = 0$ and π_E is equal to multiplication by the integer $a_E/2$.

We continue assuming $\Delta_E < 0$, i.e., b_E finite, and prove a lemma on the natural action of $\mathrm{End}_k(E) \otimes \mathbf{Z}_\ell$ on $T_\ell(E)$.

Lemma 7. *Assume that the index b_E is finite. For any prime $\ell \neq p$, the Tate module $T_\ell(E)$ of E is free of rank one over* $\mathrm{End}_k(E) \otimes \mathbf{Z}_\ell$.

Proof. Functoriality of T_ℓ induces an isomorphism

$$r_\ell : \mathrm{End}_k(E) \otimes \mathbf{Z}_\ell \xrightarrow{\sim} \mathrm{End}_{\mathbf{Z}_\ell[G_k]}(T_\ell(E)). \tag{3}$$

This follows, for example, from a celebrated theorem of Tate on abelian varieties over finite fields (see [11]).[1]

The ring $\mathrm{End}_k(E) \otimes \mathbf{Z}_\ell$ is a free $\mathbf{Z}_\ell$-module of rank two, and admits a $\mathbf{Z}_\ell$-basis of the form $(1, \pi')$, for some $\pi' \in \mathrm{End}_k(E) \otimes \mathbf{Z}_\ell$. Since r_ℓ is an isomorphism, $(1, r_\ell(\pi'))$ is a $\mathbf{Z}_\ell$-basis of $\mathrm{End}_{\mathbf{Z}_\ell[G_k]}(T_\ell(A))$. We deduce that for any $s \in \mathbf{Z}_\ell$ the element

$$r_\ell(\pi') - s \cdot 1$$

is not divisible by ℓ in $\mathrm{End}_{\mathbf{Z}_\ell[G_k]}(T_\ell(E))$. Equivalently, the reduction modulo ℓ of $r_\ell(\pi')$ is an endomorphism of $T_\ell(E)/\ell T_\ell(E)$ which is not given by multiplication by a scalar in $\mathbf{Z}/\ell\mathbf{Z}$. This is to say that there exists $t \in T_\ell(E) - \ell T_\ell(E)$ such that

$$r_\ell(\pi') \cdot t \;\notin\; \mathbf{Z}_\ell \cdot t + \ell T_\ell(E).$$

By Nakayama's Lemma we have that the pair $(t, r_\ell(\pi') \cdot t)$ is a $\mathbf{Z}_\ell$-basis $T_\ell(E)$, since the mod ℓ reductions of its components generate $T_\ell(E)/\ell T_\ell(E)$. It follows that

$$\mathrm{End}_k(E) \otimes \mathbf{Z}_\ell \ni a \longmapsto r_\ell(a) \cdot t \in T_\ell(E) \tag{4}$$

is an isomorphism of $\mathrm{End}_k(E) \otimes \mathbf{Z}_\ell$-modules, which shows that $T_\ell(E)$ is free of rank one over $\mathrm{End}_k(E) \otimes \mathbf{Z}_\ell$. □

Let $\sqrt{\Delta_E} \in \mathrm{End}_k(E)$ be the square root of Δ_E given by $2\pi_E - a_E$. It is elementary to check that

$$\pi'_E = (\Delta_E + b_E\sqrt{\Delta_E})/2b_E^2$$

belongs to $\mathrm{End}_k(E)$ and the pair $\mathcal{B}_{\mathbf{Z}} = (1, \pi'_E)$ is a $\mathbf{Z}$-basis of $\mathrm{End}_k(E)$. Furthermore, multiplication by π_E on $\mathrm{End}_k(E)$ is given in the coordinates induced by $\mathcal{B}_{\mathbf{Z}}$ by the matrix

[1] The injectivity of r_ℓ follows from a general fact on abelian varieties (see [6], § 19, Theorem 3). Its surjectivity is easy and can be proved directly without invoking Tate's theorem.

$$\sigma'_E = \begin{pmatrix} \dfrac{a_E b_E - \Delta_E}{2b_E} & \dfrac{\Delta_E(b_E^2 - \Delta_E)}{4b_E^3} \\ b_E & \dfrac{a_E b_E + \Delta_E}{2b_E} \end{pmatrix}.$$

The same matrix a *fortiori* describes multiplication by $\pi_E \otimes 1$ on $\mathrm{End}_k(E) \otimes \mathbf{Z}_\ell$, with respect to the $\mathbf{Z}_\ell$-basis deduced from $\mathcal{B}_{\mathbf{Z}}$. Since, by Lemma 7, $T_\ell(E)$ is free of rank one over $\mathrm{End}_k(E) \otimes \mathbf{Z}_\ell$, we conclude that σ'_E describes the multiplication action of π_E on $T_\ell(E)$ as well, in the $\mathbf{Z}_\ell$-coordinates of a suitable basis. This completes the proof of Theorem 2 when E is not special, for $\sigma'_E = \sigma_E$ by Proposition 5, and also gives an alternative proof of the main result of [2].

If E is special then $b_E = p^m$ or $2p^m$ where $[k : \mathbf{F}_p] = 2m + 1$ (see Proposition 5), and the matrix σ'_E is given by

(5)
$$m_1 = \begin{pmatrix} 2p^{m+1} & -p^{m+1}(4p+1) \\ p^m & -2p^{m+1} \end{pmatrix} \text{ or } m_2 = \begin{pmatrix} p^{m+1} & -p^{m+1}(p+1)/2 \\ 2p^m & -p^{m+1} \end{pmatrix},$$

respectively. Moreover, $\beta_E = 2p^m$ and hence $\sigma_E = m_2$. The matrix equality

$$\begin{pmatrix} 1 & p \\ 0 & 2 \end{pmatrix} m_1 \begin{pmatrix} 1 & p \\ 0 & 2 \end{pmatrix}^{-1} = m_2$$

shows that m_1 and m_2 define the same $\mathrm{GL}_2(\mathbf{Z}_\ell)$-conjugacy class for any odd prime ℓ. This suffices to complete the proof of Theorem 2.

4. A Global Application

Let K be a number field, $\bar{K}$ an algebraic closure of it, and G_K the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ of K. If $\mathfrak{p}$ is a finite prime of K, denote by $k_\mathfrak{p}$ its residue field, by p its residual characteristic, by $K_\mathfrak{p}$ the corresponding completion of K, and by $G_{K_\mathfrak{p}}$ the decomposition group of G_K at $\mathfrak{p}$ with respect to the choice of a prime $\bar{\mathfrak{p}}$ of $\bar{K}$ lying above $\mathfrak{p}$. Denote moreover by $\bar{k}_\mathfrak{p}$ the algebraic closure of $k_\mathfrak{p}$ given by the residue field of $\bar{\mathfrak{p}}$, and by $G_{k_\mathfrak{p}}$ the Galois group $\mathrm{Gal}(\bar{k}_\mathfrak{p}/k_\mathfrak{p})$.

Let $\mathcal{E}$ be an elliptic curve over K with j-invariant $j_\mathcal{E}$. If $\mathfrak{p}$ is a finite prime of K at which $\mathcal{E}$ has good reduction $\mathcal{E}_\mathfrak{p}$, denote by $a_\mathfrak{p}$ the error term $|k_\mathfrak{p}| + 1 - |\mathcal{E}_\mathfrak{p}(k_\mathfrak{p})|$, and by $\Delta_\mathfrak{p}$ the discriminant $a_\mathfrak{p}^2 - 4|k_\mathfrak{p}|$. If N is an integer ≥ 1, the N-th torsion subgroup $\mathcal{E}[N]$ is a finite group scheme over K of rank N^2 whose group of L-valued points, for any K-algebra L, is given by $\mathcal{E}[N](L) = \mathrm{Hom}(\mathbf{Z}/N\mathbf{Z}, \mathcal{E}(L))$. We will identify $\mathcal{E}[N]$ with $\mathcal{E}[N](\bar{K})$, an abelian group isomorphic to $(\mathbf{Z}/N\mathbf{Z})^2$ equipped with a continuous action of G_K. By Galois Theory, the kernel of the representation

$$\rho_{\mathcal{E}[N]} : G_K \longrightarrow \mathrm{Aut}(\mathcal{E}[N]) \simeq \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$$

defines a Galois extension $K(\mathcal{E}[N])/K$, known as the N-th torsion field of $\mathcal{E}$, with Galois group isomorphic to $\mathrm{Im}(\rho_{\mathcal{E}[N]})$. As is well known, $\rho_{\mathcal{E}[N]}$ is unramified at every finite prime $\mathfrak{p}$ of K not dividing N and at which $\mathcal{E}$ has good reduction. More precisely, for any N not divisible by p, the reduction map induces an identification

$$\mathcal{E}[N](\bar{K}) = \mathcal{E}_{\mathfrak{p}}[N](\bar{k}_{\mathfrak{p}}) \tag{6}$$

which is equivariant with respect to the Galois actions of $G_{K_{\mathfrak{p}}}$ and $G_{k_{\mathfrak{p}}}$ (see [8], Lemma 2). Theorem 2 can then be applied to describe the conjugacy class of

$$\rho_{\mathcal{E}[N]}(\mathrm{Frob}_{\mathfrak{p}})$$

in $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ in terms of the trace $a_{\mathfrak{p}}$, the size of $k_{\mathfrak{p}}$, and the j-invariant $j_{\mathcal{E}_{\mathfrak{p}}}$, provided that N satisfies the usual constraint of being odd if $\mathfrak{p}$ is one of the finitely many primes of K such that $\mathcal{E}_{\mathfrak{p}}$ is special. Notice that our local method will not say anything about the $\mathrm{Im}(\rho_{\mathcal{E}[N]})$-conjugacy class of $\rho_{\mathcal{E}[N]}(\mathrm{Frob}_{\mathfrak{p}})$. However, if E has no complex multiplication then a celebrated result of Serre says that $\mathrm{Im}(\rho_{\mathcal{E}[N]}) = \mathrm{Aut}(\mathcal{E}[N])$ for all N relatively prime to some positive constant N_E (see [7]).

In Theorem 3, we only made explicit the necessary and sufficient condition for $\rho_{\mathcal{E}[N]}(\mathrm{Frob}_{\mathfrak{p}})$ to act as the identity on $\mathcal{E}[N]$ or, equivalently, for $\mathfrak{p}$ to split completely in the N-th torsion field of $\mathcal{E}$.

proof of Theorem 3. The theorem is trivial if $\Delta_{\mathfrak{p}} = 0$, therefore we continue assuming $\Delta_p < 0$ and first treat the case where $\mathcal{E}_{\mathfrak{p}}$ is not special. The integral matrix associated to $\mathcal{E}_{\mathfrak{p}}$ by Theorem 2 is

$$\sigma_{\mathfrak{p}} = \begin{pmatrix} \dfrac{a_{\mathfrak{p}}\beta_{\mathfrak{p}} - \Delta_{\mathfrak{p}}}{2\beta_{\mathfrak{p}}} & \dfrac{\Delta_{\mathfrak{p}}(\beta_{\mathfrak{p}}^2 - \Delta_{\mathfrak{p}})}{4\beta_{\mathfrak{p}}^3} \\ \beta_{\mathfrak{p}} & \dfrac{a_{\mathfrak{p}}\beta_{\mathfrak{p}} + \Delta_{\mathfrak{p}}}{2\beta_{\mathfrak{p}}} \end{pmatrix},$$

where $\beta_{\mathfrak{p}}$ is equal to

$$\sup_{h>0}\{h : h^2 \mid \Delta_{\mathfrak{p}} \text{ and } \mathcal{P}_{\Delta_{\mathfrak{p}}/h^2}(j_{\mathcal{E}}) \equiv 0 \pmod{\mathfrak{p}}\},$$

which is an integer since $\Delta_{\mathfrak{p}} \neq 0$. Moreover, the ratio Δ_p/β_p^2 is necessarily a negative discriminant, since $\mathcal{P}_D(x)$ is defined as the constant polynomial 1 for all negative integers $D \equiv 2$ or $3 \pmod 4$.

By Theorem 2, if N is an integer not divisible by p, the prime $\mathfrak{p}$ splits completely in $K(\mathcal{E}[N])/K$ if and only if

$$\sigma_{\mathfrak{p}} \equiv \mathrm{Id}_2 \pmod{N}, \tag{7}$$

where Id_2 is the two-by-two identity matrix. Our task is verifying that (7) is equivalent to have conditions (1) and (2) of Theorem 3 both satisfied.

We begin by observing that $\sigma_{\mathfrak{p}}$ is a scalar matrix if and only if condition (1) holds, which is to say

$$\sigma_{\mathfrak{p}} \text{ is a scalar matrix} \iff N \mid b_{\mathfrak{p}}. \tag{8}$$

The "only if" direction of (8) is clear, and to see the "if" part it is enough to observe that the upper right entry of $\sigma_{\mathfrak{p}}$ is divisible by $\beta_{\mathfrak{p}}$, since the ratio $\Delta_{\mathfrak{p}}/\beta_{\mathfrak{p}}^2$ is a negative discriminant, and that the difference of the diagonal entries

$$\frac{a_{\mathfrak{p}}\beta_p - \Delta_{\mathfrak{p}}}{2\beta_p} - \frac{a_{\mathfrak{p}}\beta_{\mathfrak{p}} + \Delta_{\mathfrak{p}}}{2\beta_{\mathfrak{p}}} = -\frac{\Delta_p}{\beta_p}$$

is also divisible by β_p.

To complete the proof in the non-special case it suffices to observe the elementary fact that if N divides β_p then

$$\frac{a_{\mathfrak{p}}\beta_{\mathfrak{p}} + \Delta_{\mathfrak{p}}}{2\beta_{\mathfrak{p}}} \equiv 1 \pmod{N} \iff a_{\mathfrak{p}} \equiv 2 + \frac{\Delta_{\mathfrak{p}}}{\beta_{\mathfrak{p}}} \pmod{N^*},$$

where $N^* = N$ if N is odd and $N^* = 2N$ otherwise.

Assume now that $\mathcal{E}_{\mathfrak{p}}$ is special, and let N be an integer > 2 and not divisible by p. The Frobenius $\rho_{\mathcal{E}[N]}(\mathrm{Frob}_{\mathfrak{p}})$ is described by one of the two matrices in (5), where m is such that $2m+1 = [k_{\mathfrak{p}} : \mathbf{F}_p]$. However, both these matrices are not congruent to the identity modulo N, hence $\mathfrak{p}$ does not split in $K(\mathcal{E}[N])/K$. On the other hand, condition (1) of the theorem is not satisfied, since N^2 does not divide $\Delta_{\mathfrak{p}} = -4p^{2m+1}$, and the proof is complete. □

Finally, notice that in the special case where $N = \ell$ is prime, Theorem 3 gives a criterion for deciding whether or not $\mathrm{Frob}_{\mathfrak{p}}$ acts on $\mathcal{E}[\ell]$ in a semisimple fashion in the critical case when $\ell | \Delta_{\mathfrak{p}}$, i.e., when such an action has only one eigenvalue. This problem has been emphasized in [9].

Acknowledgments

It is a pleasure to thank Gebhard Böckle for all the time spent together discussing this work and related topics. I thank Löic Merel for several discussions we had, which motivated my interest in the questions considered in this paper. I thank Andrew Snowden and Jared Weinstein for their comments on an earlier version of the manuscript that helped me improve the exposition. The first version of this work was completed in June 2013 while I was visiting UCLA. I want to thank Chandrashekhar Khare for his kind invitation there.

References

[1] T. Centeleghe and P. Tsaknias, Integral Frobenius, *Magma package available at* http://math.uni.lu/∼tsaknias/sfware.html

[2] W. Duke and Á. Tóth, The splitting of primes in division fields of elliptic curves, *Experiment. Math.* **11**(4) (2002) 555–565.

[3] D. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication.* John Wiley & Sons, Inc., New York (1989).

[4] N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over **Q**, *Invent. math.* **89** (1987) 561–567.

[5] S. Lang, *Elliptic functions.* Second edition. Graduate Texts in Mathematics, **112**. Springer-Verlag, New-York (1987).

[6] D. Mumford, *Abelian varieties.* Second edition. Tata Institute of Fundamental Research, Bombay (1974).

[7] J.-P. Serre, Propriétés galoisiennes des point d'ordre fini des courbes elliptiques, *Invent. math.* **15** (1972) 259–331.

[8] J.-P. Serre and J. Tate, Good reduction of abelian varieties, *Annals of Math.* **88**(3) (1968) 492–517.

[9] G. Shimura, A reciprocity law in non–solvable extensions, *J. Reine Angew. Math.* **221** (1966) 209–220.

[10] J. H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, **106**. Spinger-Verlag, New York (1986).

[11] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. math.* **2** (1966) 134–144.

[12] J. Tate, Classes d'isogénie des variétés abéliennes sur un corps fini, *Sém. Bourbaki* 21e année, 1968/69, no 352.

[13] W.C. Waterhouse, Abelian varieties over finite fields, *Ann. scient. Éc. Norm. Sup.*, 4^e série, t. 2 (1969) 521–560.

IWR, Universität Heidelberg, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany

E-mail address: tommaso.centeleghe@iwr.uni-heidelberg.de

URL: http://www.iwr.uni-heidelberg.de/groups/arith-geom/centeleghe/