LECTURES ON SHIMURA CURVES 1: ENDOMORPHISMS OF ELLIPTIC CURVES

PETE L. CLARK

0.1. **Endomorphisms of elliptic curves.** Recall that a homomorphism of complex elliptic curves is just a holomorphic map $E_1 \to E_2$ which preserves the origin. (It turns out that this condition is enough to force it to be a homomorphism of groups in the usual sense; why?) An **isogeny** of elliptic curves is a homomorphism whose kernel is a finite subgroup of E_1. In fact the kernel of a homomorphism of Lie groups is a closed Lie subgroup, so in this case is either finite or all of E_1, so an isogeny of elliptic curves is the same as a nonzero homomorphism. An **endomorphism** of E is an isogeny from E to E.

Of course, these definitions make sense over an arbitrary algebraically closed field, just by replacing both "Lie" and "holomorphic" by "algebraic." In fact the definitions *make sense* over an arbitary field k provided we interpret "subgroup" as "subgroup scheme," but this is a bit glib: especially in positive characteristic, a group scheme is a more subtle concept than an algebraic group, and the differences from the classical ($k = \mathbb{C}$) case are not merely linguistic.

1. Complex elliptic curves

1.1. **Rational and complex representations.** The fact that every complex elliptic curve admits a uniformization $\mathbb{C}/\Lambda$ is very helpful in analyzing the endomorphism ring. Indeed, an endomorphism of E is given by a $\mathbb{C}$-linear map α – i.e., multiplication by some nonzero complex number – such that $\alpha(\Lambda) \subset \Lambda$. Clearly, for any integer n we can take $\alpha = n$, and these are all distinct endomorphisms. That is, every elliptic curve admits $\mathbb{Z}$ as a subring of endomorphisms.

Choosing an isomorphism $\Lambda \cong \mathbb{Z}^2$, we get a faithful representation

$$\rho_{\mathbb{Z}} : \mathrm{End}(E) \to M_2(\mathbb{Z}),$$

the so-called **rational representation**. (We shall also write $\rho_{\mathbb{Q}}$ for the composition of $\rho_{\mathbb{Z}}$ with the embedding $M_2(\mathbb{Z}) \to M_2(\mathbb{Q})$.) Thus the endomorphism ring is a subring of $M_2(\mathbb{Z})$, so is a free abelian group of rank at most 4. On the other hand, we saw that passing to the tangent space gives another representation

$$\rho_{\mathbb{C}} : \mathrm{End}(E) \to \mathbb{C},$$

the **complex representation**.

It is natural to look for some simple algebraic relationship between $\rho_{\mathbb{Q}}$ and $\rho_{\mathbb{C}}$. To do this, let us actually compute with matrices. Take the complex number 1 as a basis for $\mathbb{C}$, let $(u_1,\ u_2)$ be a basis for Λ, and let U be the column vector $[u_1\ u_2]^t$. Let φ be a nonzero endomorphism of E. Then we have the equation

$$U\rho_{\mathbb{C}}(\varphi) = \rho_{\mathbb{Q}}(\varphi)U,$$

and also, applying complex conjugation, the equation

$$\overline{U}\overline{\rho_{\mathbb{C}}(\varphi)} = \rho_{\mathbb{Q}}(\varphi)\overline{U}.$$

Hence we have the matrix equation

$$\begin{bmatrix} \rho_{\mathbb{C}}(\varphi) & 0 \\ 0 & \overline{\rho_{\mathbb{C}}(\varphi)} \end{bmatrix} \left[\ U \mid \ \ \overline{U}\ \right] = \left[\ U \mid \ \ \overline{U}\ \right] \rho_{\mathbb{Q}}(\varphi).$$

The matrix $[U\ |\overline{U}]$ is easily seen to be nonsingular (check this: it expresses the fact that z_1 and z_2 are $\mathbb{R}$-linearly independent), so we have shown that

$$\rho_{\mathbb{Q}} = \rho_{\mathbb{C}} \oplus \overline{\rho_{\mathbb{C}}}. \tag{1}$$

Remark: As we shall see later, this discussion carries over verbatim to higher-dimensional complex tori $\mathbb{C}^n/\Lambda$ (where $\Lambda \cong \mathbb{Z}^{2n}$ is a discrete subgroup).

1.2. **The endomorphism ring.** The above analysis gives us enough information to determine the endomorphism ring:

Theorem 1. *Let E be a complex elliptic curve. Then* $\mathrm{End}(E)$ *is either* $\mathbb{Z}$ *or isomorphic to an order in an imaginary quadratic field. Conversely, all such rings arise.*

Proof: Because $\rho_{\mathbb{Z}}$ is faithful, $\mathrm{End}(E) \hookrightarrow M_2(\mathbb{Z})$ is a free abelian group of rank at most 4. Moreover, for any $\varphi \in \mathrm{End}(E)$, the characteristic polynomial of $\rho_{\mathbb{Z}}(\varphi)$ is a (monic) quadratic polynomial with $\mathbb{Z}$-coefficients, so the subring $\mathbb{Z}[\varphi]$, if not isomorphic to $\mathbb{Z}$, is an order in a quadratic field. Moreover, equation (1) shows that for all $\varphi \in \mathrm{End}(E)$,

$$\varphi \cdot \overline{\varphi} = \det(\rho_{\mathbb{Q}}(\varphi)) \in \mathbb{Z},$$

from which it follows that $\mathbb{Q}[\varphi] = \mathbb{Z}[\varphi] \otimes \mathbb{Q}$ cannot be a real quadratic field. Consider now $\mathrm{End}^0(E) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$; it is a $\mathbb{Q}$-algebra of dimension d, where $1 \leq d \leq 4$. Moreover, it is a division algebra: indeed, we have just shown that every nonscalar element lies in an imaginary quadratic field, so this is clear. Finally, $\mathrm{End}^0(E)$ is commutative, since the complex representation embeds it into $\mathbb{C}$. Putting all this together, we conclude that $\mathrm{End}^0(E)$ is isomorphic to $\mathbb{Q}$ or to an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-m})$.[1]

Definition: In case $\mathrm{End}^0(E) \cong K$ (and not $\mathbb{Q}$), we say that E has **complex multiplication**.

We now turn to the more subtle issue of the endomorphism *ring*. $\mathrm{End}(E)$ is necessarily $\mathbb{Z}$ when $\mathrm{End}^0(E) = \mathbb{Q}$ and otherwise ia an order in some imaginary quadratic field K. Let us recall what this means:

Definition: Let L be a finite-dimensional $\mathbb{Q}$-algebra, with $[L : \mathbb{Q}] = d$, say. An **order** in L is a subring $\mathcal{O}$ of L which as an abelian group is isomorphic to $\mathbb{Z}^d$.

[1] For the remainder of this lecture K shall always denote an imaginary quadratic field.

(Equivalently, $\mathcal{O}$ is finitely generated as a $\mathbb{Z}$-module and is such that the natural map $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} \to L$ is an isomorphism.) An order is **maximal** if it is not properly contained in another order; it is not hard to see that maximal orders always exist (e.g. use Zorn's Lemma). If L is a number field, then the unique maximal order is $\mathcal{O}_L$, the ring of integers in L. If L is non-commutative, there can be more than one maximal order, even up to conjugacy.

Exercise 1.1: The orders of quadratic fields have a very simple structure: if $\mathcal{O}_F = \mathbb{Z}.1 + \mathbb{Z}.\theta$, where $\theta = \sqrt{m}$ if $m \equiv 2,\ 3 \mod 4$ or $\theta = \frac{1+\sqrt{m}}{2}$ if $m \equiv 1 \mod 4$, then for every positive integer f, we get an order $\mathcal{O}_f = \mathbb{Z}.1 + f\mathbb{Z}.\theta$ of index f in the maximal order $\mathcal{O}_F$, and these are all the possible orders. (Prove it!)

We can now show the converse direction of Theorem 1: let $\mathcal{O}_f$ be an order in an imaginary quadratic field K. Then just by viewing K as a subfield of $\mathbb{C}$, we realize $\mathcal{O}_f$ as a rank 2 lattice, so $E = \mathbb{C}/\mathcal{O}_f$ is almost tautologically an elliptic curve which admits $\mathcal{O}_f$ as a ring of endomorphisms.[2]

This completes the proof of Theorem 1, except for the distressing technicality that we have not yet exhibited any elliptic curves *without* complex multiplication. This state of affairs is remedied in the exercises.

Exercise 1.2: Let $E = \mathbb{C}/\Lambda$ be an elliptic curve with endomorphism ring $\mathcal{O}_f$.
a) Show that the complex representation equips Λ with the structure of an $\mathcal{O}_f$-module.
b)* Show that the resulting $\mathcal{O}_f$-module structure is rank one projective, or in other words that Λ is a fractional $\mathcal{O}_f$-ideal.
c)* Conversely, let $\mathfrak{a}$ be a fractional $\mathcal{O}_f$-ideal. Explain how $\mathfrak{a}$ can be viewed as a lattice in $\mathbb{C}$, so that $\mathbb{C}/\mathfrak{a}$ is an elliptic curve with complex multiplication by $\mathcal{O}_f$. Is $\mathrm{End}(\mathbb{C}/\mathfrak{a})$ isomorphic to $\mathfrak{a}$ as an $\mathcal{O}_f$-module?
d) Show that if $\mathfrak{a}$ and $\mathfrak{b}$ are in the same ideal class, the elliptic curves $E/\mathfrak{a}$ and $E/\mathfrak{b}$ are isomorphic.
e) Conclude that the set of isomorphism classes of elliptic curves with endomorphism ring $\mathcal{O}_f$ is finite.

Exercise 1.3: a) Show that there exists a complex elliptic curve *without* complex multiplication.
b)* Show that there exists an elliptic curve with $j(E) \in \mathbb{Q}$ without complex multiplication.

Exercise 1.4: a) Let E be a CM elliptic curve. Show that $j(E)$ is an algebraic number.
b) Show that any two CM elliptic curves with the same endomorphism algebra are isogenous. (Note that this is certainly not the case for non-CM elliptic curves.)
c) Conclude that any CM elliptic curve E has the virtue of being isogenous to each

[2] What is not tautologous, but is easy enough to check in this case, is that the endomorphism ring of $\mathbb{C}/\mathcal{O}_f$ is precisely $\mathcal{O}_f$ and not some larger order. In general, the issue of exactly which order in a $\mathbb{Q}$-algebra one has is a very delicate one, which is why we often discuss the endomorphism *algebra* instead of the endomorphism ring.

of its Galois conjugates E^σ. Most non-CM elliptic curves do not have this property. The ones that do are called (confusingly enough) $\mathbb{Q}$-curves, and they have an important role to play in 21st century number theory.

Exercise 1.5*: It follows from the facts recalled in the last section (and the primitive element theorem!) that every number field F arises as $\mathbb{Q}(j(E))$ for some complex elliptic curve E. What can be said about the number fields which are generated by j-invariants of CM elliptic curves? E.g., does one get all number fields this way?

In case this seems too vague, the answer to the section question is "no" for at least three (qualitatively different) reasons:
a) The extension $F/\mathbb{Q}$ need not be Galois, but there are some strong restrictions on the Galois group of its Galois closure. What are they?
b) There is a nontrivial restriction on $F \otimes \mathbb{R}$, i.e., on the Archimedean places of F. What is it?
c) There is a restriction on the number of fields F of any given degree over $\mathbb{Q}$ which can arise. Why?
As far as I know, there may be other restrictions. Do you know any?

Finally, the following result in the theory of complex multiplication lies a bit too deep for us to discuss now (later we will see how to prove a vast generalization, given the right technology), but seems important to record.

Theorem 2. *Let E be a CM elliptic curve. Then $j(E)$ is an algebraic integer.*

Proof: See [ECII, § II.6].

Remark: It is not hard to see that this theorem is equivalent to the statement that a CM elliptic curve has potentially good reduction at every finite place.

1.3. **Recalled facts about elliptic curves.** In order to analyze the endomorphism rings of elliptic curves over more general fields, we need to have some basic facts at our disposal, all of which can be found in early chapters of [ECI]. In the following, let $E_{/k}$ be an elliptic curve over an algebraically closed field k.

An isogeny $\varphi : E_1 \rightarrow E_2$ induces (and is equivalent to) an embedding of function fields $\varphi^* : k(E_2) \hookrightarrow k(E_1)$. The index $[k(E_1) : \varphi^*(k(E_2))]$ is finite and called the **degree** of φ. Equivalently, the kernel $H = \ker(\varphi)$ of φ is a finite flat subgroup scheme of E, and its order (in the scheme-theoretic sense!) is equal to the degree of φ.

Proposition 3. *Given any isogeny $\varphi : E_1 \rightarrow E_2$, there exists an isogeny $\varphi^\vee : E_2 \rightarrow E_1$, called the* ***dual isogeny****, which is characterized by*

$$\varphi^\vee \circ \varphi = [\deg(\varphi)].$$

Proposition 4. *For any positive integer n, the multiplication by n map $[n] : E \rightarrow E$ is an isogeny of degree n^2. This map is separable if k has characteristic zero, or if k has characteristic $p > 0$ and $(n,p) = 1$; otherwise it is inseparable.*

Recall that any finite field extension $F_1 \subset F_2$ "factors" as $F_1 \subset F \subset F_2$ where F/F_1 is separable and F_2/F is purely inseparable[3]. One speaks of the **separable**

[3] In french, *radiciel.*

degree $[F : F_1]$ and the **inseparable degree** $[F_2 : F]$.

Suppose F is the function field of an algebraic curve defined over an algebraically closed field of positive characteristic p. Then for every $q = p^a$, there is a unique purely inseparable field extension of degree q, namely the extension $F^{\frac{1}{q}}/F$ given by the Frobenius map $\pi_q : f \mapsto f^{\frac{1}{q}}$.

So every inseparable isogeny of elliptic curves in characteristic p factors through the Frobenius isogeny $\pi_p : E \to E^p$. In particular $[p]$ factors through π_p at least once. (The question of whether it factors through twice – i.e., whether it is purely inseparable, is highly relevant to the classification of endomorphism rings that we are about to give.)

Proposition 5. *Let $\varphi : E_1 \to E_2$ be a degree d isogeny of elliptic curves over k, and let $P \in E_2(k)$ be any point. Then the cardinality of $\{Q \in E_1(k) \mid \varphi(Q) = P\}$ is equal to the separable degree of φ; in particular it is at most d, with equality if and only if φ is separable.*

Corollary 6. *If $E_{/k}$ is an elliptic curve, and n is a positive integer not divisible by the characteristic of k, then $E(k)[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. However, if k has characteristic $p > 0$, then $\#E(k)[p] \leq p$.*

1.4. **The case of positive characteristic.**

Theorem 1 is false for elliptic curves defined over (algebraically closed) fields k of positive characteristic. However, one can still get a classification result by modifying the above argument in several places. Let us recall how this goes.

We no longer have the representation $\rho_{\mathbb{Z}}$, so it is less clear that $\mathrm{End}(E)$ is a free $\mathbb{Z}$-module of rank at most 4, but this is still true. To see this, note first that $\mathrm{End}(E)$ is a torsionfree $\mathbb{Z}$-module – this is equivalent to the fact that $E(k)$ is not N-torsion for any fixed N, which is easily checked using Weierstrass equations. Then, as a replacement for the rational representation we have, for any ℓ not equal to the characteristic of k, the ℓ-adic representation

$$\rho_\ell : \mathrm{End}(E) \to \mathrm{End}(T_\ell(E)),$$

where $T_\ell(E) = \lim_{\leftarrow} E[\ell^n]$ is the ℓ-adic Tate module. By Corollary 6, for ℓ different from p, $T_\ell \cong \mathbb{Z}_\ell^2$, so ρ_ℓ amounts to a homomorphism $\mathrm{End}(E) \to M_2(\mathbb{Z}_\ell)$.

Exercise 1.6: Show that ρ_ℓ is faithful. (Hint: The torsion points of ℓ-power order, being infinite in number, are Zariski-dense in $E(k)$.)

What we really need is the following stronger result.

Theorem 7. *Let E_1, E_2 be two elliptic curves defined over an algebraically closed field k. Then the natural map*

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(E_1), T_\ell(E_2)$$

is injective.

Proof: See [ECI, Theorem III.7.2].

It follows that every nonscalar element of $\mathrm{End}(E)$ can be viewed as a quadratic integer. To see that it is necessarily an imaginary quadratic integer we can use the dual isogeny: if $\varphi : E_1 \to E_2$, there exists $\varphi^\vee : E_2 \to E_1$ satisfying, among other things, that $\varphi^\vee \cdot \varphi$ is multiplication by the degree of φ. When $E_1 = E_2$, this means that $\mathrm{End}(E)$ is equipped with an involution $\alpha \mapsto \alpha^*$ which is positive: the quadratic form $\alpha \mapsto \alpha\alpha^*$ takes values in $\mathbb{Z}^{\geq 0}$. But real quadratic fields do not have such involutions, so every nonscalar element must again generate an element in an imaginary quadratic field. This again shows that $\mathrm{End}_0(E)$ is a division algebra over $\mathbb{Q}$.[4]

If it is not an imaginary quadratic field, it is a four-dimensional division algebra $D/\mathbb{Q}$ which is "locally quadratic": in other words, it is a quaternion algebra.

Let us pause to recall the classification of quaternion algebras over local and global fields: if K is a p-adic field (i.e., a finite extension of $\mathbb{Q}_p$) then there are exactly two quaternion algebras over K: the matrix algebra $M_2(K)$ (called "split") and a unique division quaternion algebra. If K is a number field, and B, B' are two quaternion algebras defined over K, then $B \cong B'$ if and only if for all places v of K,

$$B_v = B \otimes_K K_v \cong B' \otimes_K K_v = B'_v.$$

One says that B is *split* at v if $B_v \cong M_2(K_v)$; otherwise it is said to be *ramified.* Furthermore, one knows that the number of ramified places is finite and *even*, and finally that given any finite set S of places of K of even cardinality there does exist a quaternion algebra B ramified exactly at the places of S.

Exercise 1.7: Take $K = \mathbb{Q}$. A quaternion algebra over $\mathbb{Q}$ is said to be *indefinite* or *definite* according to whether it is split or not at the place ∞. Show that B is indefinite if and only if it contains a real quadratic subfield.

Definition: An elliptic curve over a field of positive characteristic is called **supersingular** if its endomorphism algebra is a quaternion algebra, and called **ordinary** if it is not supersingular.

Proposition 8. *The endomorphism algebra B of a supersingular elliptic curve is the (unique) quaternion algebra over $\mathbb{Q}$ ramified at p and at ∞.*

Proof: By Exercise 7, B is ramified at ∞. Take now any $\ell \neq p$. Tensoring the ℓ-adic representation with $\mathbb{Q}$ we get a representation

$$\rho_\ell : B_\ell = B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to M_2(\mathbb{Q}_\ell).$$

By Theorem 6, this is an injection of one 4-dimensional $\mathbb{Q}_\ell$-algebra into another, i.e., it is an isomorphism, which means precisely that B is split at ℓ. It follows from

[4] This argument is not quite correct, but I kept it here because it was said this way in class. It shows that $\mathrm{End}^0(E)$ cannot be a real quadratic field, but does not quite show that it cannot contain a real quadratic field, because how do we know that such a subfield is stabilized by the involution? This is not hard to fix: once we agree that $\mathrm{End}^0(E)$, if not an imaginary quadratic field, must be a division quaternion algebra over $\mathbb{Q}$, we now apply the positivity argument to conclude that it is a definite quaternion algebra. By the way, this makes the terminology more clear, since the map $\alpha \in B \mapsto \alpha\alpha' \in \mathbb{Q}$ is a quadratic form.

the structure of global quaternion algebras that B must be ramified at p, completing the proof.

Problem 1.1: Is there a direct, elementary argument showing that B is ramified at p? (The only proof I can think of involves Dieudonné modules.)

Theorem 9. *For an elliptic curve E over a field of characteristic p, the following are equivalent:*
a) E is supersingular.
b) $E(k)[p] = 0$.
c) $[p]$ is purely inseparable.

Proof: The equivalence of b) and c) follows easily from Proposition 5 above. Namely, we know that $E[p](k)$ is equal to the separable degree of the inseparable degree p^2 morphism $[p]$, so it is either 1 or p according to whether $[p]$ is purely inseparable or not. Clearly when $E(k)[p] = 0$ we have $T_p(E) = \varprojlim E[p^n] = 0$; an easy inductive argument gives that if $E(k)[p] = \mathbb{Z}/p\mathbb{Z}$, $T_p(E) \cong \mathbb{Z}_p$ in the latter case.

Exercise 1.8: If $T_p(E) \cong \mathbb{Z}_p$, then the p-adic representation

$$\rho_p : \mathrm{End}(E) \to \mathrm{End}(V_p) \cong \mathbb{Q}_p$$

is faithful. In particular, $\mathrm{End}(E)$ is commutative.

From the above exercise we conclude b) $\implies$ a). The proof of the converse is harder (and more interesting). We begin with the following

Lemma 10. *If E/k is supersingular, then $j(E) \in \mathbb{F}_{p^2}$.*

Exercise 1.9: Prove it! (Hint: Since $[p]$ is purely inseparable, it is, up to an isomorphism, equal to π_{p^2}.)

Exercise 1.10: Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves. Then φ induces and isomorphism of endomorphism *algebras* $\mathrm{End}^0(E_1) \to \mathrm{End}^0(E_2)$. (Hint: use the dual isogeny.)

From these two exercises we derive the startling fact that if E is supersingular, there are up to isomorphism only finitely many elliptic curves isogenous to it. It is an important fact that the isogeny class of any nonsupersingular elliptic curve is infinite: let us see why this is the case.

Observe that if E is not supersingular, there are infinitely many primes ℓ (not equal to the characteristic of k) such that E does not have an endomorphism of degree ℓ. If $\mathrm{End}(E) = \mathbb{Z}$ this is true for all primes, since $\deg([n]) = n^2$. Otherwise $\mathrm{End}(E)$ is contained in the ring of integers of some quadratic field K, and for $\alpha \in \mathrm{End}(E)$, $\deg(\alpha) = \alpha\overline{\alpha}$, i.e., the norm of α. So if p is nonsplit in K then it is not the norm of a prime ideal of $\mathrm{End}(E)$ (let alone a principal prime ideal). In fact, if ℓ_1 and ℓ_2 are any two nonsplit primes (of which there are certainly infinitely many) in K, then neither is there an isogeny of degree $\ell_1\ell_2$. So let H_1 and H_2 be cyclic subgroups of E of orders ℓ_1 and ℓ_2, respectively. Then $E_1 := E/H_1$ and $E_2 := E/H_2$ are isogenous to E but not isomorphic to it. In fact they are not isomorphic to each other. To see this, for $i = 1,\ 2$ write φ for the isogeny $E \to E/H_i$.

If $\iota : E_1 \to E_2$ were an isomorphism, then

$$\varphi_2^\vee \circ \iota \circ \varphi_1 : E \to E$$

would be an endomorphism of E of degree $\ell_1 \ell_2$, which we just saw does not exist! Therefore we have exhibited infinitely many pairwise nonisomorphic elliptic curves in the isogeny class of E, so E is not supersingular. This completes the proof of Theorem 9.

Problem 1.2: Let E be an elliptic curve. Define a graph $\mathcal{G}(E)$ whose vertices correspond to isomorphism classes of elliptic curves which are isogenous to E. We say that two vertices are adjacent if the corresponding elliptic curves are isogenous via an isogeny of prime degree. What can be said about the structure of this graph?

The following simple result will be useful for us:

Proposition 11. *Let E be an elliptic curve defined over a field of positive characteristic p with $\operatorname{End}^0(E) = K$ an imaginary quadratic field. Then the prime p splits in K.*

Proof: By the above, $T_p(E) \cong \mathbb{Z}_p$, so tensoring the p-adic representation with $\mathbb{Z}_p$ gives a map

$$K_p = K \otimes \mathbb{Q}_p \to \mathbb{Q}_p.$$

Now this is a unital homomorphism of $\mathbb{Q}_p$-algebras which is not injective, so K_p had better not be a field. In other words, p splits in K.

Theorem 12. *Let E be an elliptic curve defined over a field of characteristic $p > 0$. Then $\operatorname{End}(E) = \mathbb{Z}$ if and only if $j(E)$ is transcendental over $\mathbb{F}_p$.*

Proof: Suppose that $j(E)$ is algebraic, so that E can be defined over a finite field $\mathbb{F}_q$. Then the Frobenius map π_q gives an endomorphism ϖ of E. Note that this morphism has degree q, so if q is an odd power of p it is certainly not equal to $[n]$ for any n (as the degree of $[n]$ is n^2). But if $\varpi = [\sqrt{q}]$ then $[p]$ is purely inseparable, so E is supersingular.

Now suppose that $j(E)$ is transcendental. Then E is a *generic* elliptic curve in characteristic p; in other words, every elliptic curve is obtained by specializing the value of $j(E)$. If then the endomorphism algebra of E strictly contained $\mathbb{Q}$, it would mean that there was a common CM field contained in the endomorphism algebra of every elliptic curve in characteristic p. But we will see later that every imaginary quadratic field in which p splits arises as the endomorphism algebra of an elliptic curve in characteristic p, so the intersection of all the possible characteristic p endomorphism algebras is $\mathbb{Q}$.

Notice that we still do not know which elliptic curves defined over finite fields are ordinary (and with what CM orders) and which are supersingular (or indeed, that any supersingular elliptic curves exist at all.) An approach to this is given in Silverman's first book. Here we will take an approach which follows more closely the classical (and brilliant) work of Deuring. The basic tool will be reduction of CM elliptic curves from characteristic 0. Note that if E/K is an elliptic curve over a complete, discretely valued field given by a Weierstrass equation with coefficients in the valuation ring $\mathcal{O}_K$ and whose discriminant is a unit, then we can literally reduce the coefficients of the equation modulo the maximal ideal (π) of $\mathcal{O}_K$ to get an elliptic curve over the residue field k. (What makes this a little subtle is that the discriminant depends upon the choice of a Weierstrass equation, so that one equation may make this reduction possible while another does not. One says the elliptic curve has good reduction if some Weierstrass equation works. In general, the valuation of the discriminant is well-defined modulo 12, so in many cases one can see from a given Weierstrass equation that the reduction will be bad.)

As mentioned above, it is in fact the case that CM elliptic curves always have potentially good reduction: in other words, if E/K is a CM elliptic curve over a p-adic field, there exists a finite field extension L/K such that E/L has good reduction. In fact, this extension can be taken to be totally ramified, so that one always ends up with an elliptic curve defined over the residue field of k. In particular, given a CM elliptic curve $E\mathbb{Q}$, one can assign an elliptic curve over $\mathbb{F}_p$, defined up to moduli simply by the condition that the j-invariant is the reduction mod p of the j-invariant of E.

Another general fact is that upon good reduction of an elliptic curve, $E/K \mapsto \tilde{E}/k$, we get an injection

$$\mathrm{End}(E) \to \mathrm{End}(\tilde{E})$$

of endomorphism rings.[5]

Now a very interesting question arises: take a CM elliptic curve E defined over a number field K and v a finite place of K. What is the endomorphism algebra of the reduction of E modulo v?

Proposition 13. *(Deuring) If E/K is a CM elliptic curve and v is a place of v, then the reduction $\tilde{E}/k$ of E is supersingular if and only if p is inert or ramified in K.*

Exercise 1.11: Prove it.

Corollary 14. *For every prime p, there exists at least one supersingular elliptic curve.*

Exercise 1.12: Prove it.

Remark: The number of supersingular elliptic curves in characteristic p is approximately $\frac{p}{12}$. There is an exact formula, but instead of giving it here it seems more illuminating to remark that this number is precisely one more than the genus of the modular curve $X_0(p)$.

Note that we have not yet addressed the endomorphism *rings* in characteristic p. Things here get a bit complicated and we will just state the results:

Theorem 15. *(Deuring) a) Any elliptic curve defined over $\overline{\mathbb{F}_p}$ arises as the good reduction of a CM elliptic curve defined over an unramified extension of $\mathbb{Q}_p$.*
b) If E is an elliptic curve over a field of characteristic p with endomorphism algebra

[5] Classical proofs of this sort of statement are rather unpleasant: they appear in the work of Shimura, couched in the language of Weil-style algebraic geometry, a language which has very few native speakers. Nowadays, this reduction theorem is best seen as a consequence of the functoriality of the Néron model, which we will not discuss at this time.

an imaginary quadratic field K, then End(E) *is an order of conductor prime to p. Conversely, all such orders occur.*
c) Let E/F be an elliptic curve over a number field, whose endomorphism ring is an imaginary quadratic order of conductor $f = p \cdot n$ in a quadratic field K. If p splits in K, the endomorphism ring of $\tilde{E}/k$ is the quadratic order of conductor n in K. If p does not split in K, End(E) *is a maximal order in the quaternion algebra B split at p and ∞.*

Proof: The classical reference is [**?**], which unfortunately seems never to have been translated into English (or French). Anglophones can find a nice discussion in [**?**].

An important problem: Let E/K be an elliptic curve over a number field without CM. Again, for all but finitely many primes of K we have a well-defined reduction over a finite field. What can be said about the endomorphism algebras of these reductions? It follows from Serre's open image theorem that the set of primes for which the reduction is supersingular has density zero, and also that infinitely many different CM fields arise. Elkies has shown that whenever K has a real place, every elliptic curve has infinitely many primes of supersingular reduction, and recent work of David Jao has extended this to certain elliptic curves over imaginary quadratic fields. This is really a question about the distribution of the Frobenius eigenvalues a_p, and there is a conjectured distribution due to Lang and Trotter. One can also ask other questions about the mod p reductions (e.g., when is the reduced group of $\mathbb{F}_q$-rational points cyclic?); this is an active area of research.

1.5. **The case of an arbitrary field.**

Let $E_{/k}$ be an elliptic curve defined over an arbitrary field of characteristic zero. Note well that by an endomorphism of E, one generally means an endomorphism of E defined over $\overline{k}$, an algebraic closure of k. We will use End(E) to mean this. It is of course the case that the endomorphisms φ of E which are defined over k itself form a subring of End(E), which we shall denote $\text{End}_k(E)$. As we shall see, the containment $\text{End}_k(E) \subset \text{End}(E)$ can be proper.

The classification of End(E) (note: over the algebraic closure!) turns out to be exactly the same as the case $k = \mathbb{C}$ done above. There are at least two strategies for showing this: we can either adapt the above purely algebraic approach, or we can try to directly *deduce* the result for an arbitrary field of characteristic zero from the case of $k = \mathbb{C}$ which we proved above using analytic methods.

Given the machinery we have already introduced, the algebraic approach is quite straightforward:

Exercise 1.13: Let E/k be an elliptic curve defined over a field of characteristic zero. Show that End(E) is either $\mathbb{Z}$ or an order in an imaginary quadratic field (equivalently, $\text{End}^0(E)$ is $\mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{-m})$).

Suppose next that k is a subfield of $\mathbb{C}$, with algebraic closure $\overline{k}$. We would like to show that $\text{End}(E) = \text{End}(E/\overline{k})$ is in fact equal to $\text{End}(E/\mathbb{C})$. This is obviously the case if $\text{End}(E/\mathbb{C}) = \mathbb{Z}$. Otherwise $E/\mathbb{C}$ has CM by an order in an imaginary quadratic field K, and we are done by the following result:

Proposition 16. *Let E be an elliptic curve defined over a subfield k of $\mathbb{C}$, such that $E/\mathbb{C}$ has complex multiplication by $\mathcal{O} \subset K$. Then every endomorphism of $E/\mathbb{C}$ is defined over the composite field kK.*

Sketch Proof:[6] The complex representation $\rho_{\mathbb{C}}$ allows us to see the endomorphism ring on the tangent space (or better yet, on the cotangent space, because invariant differentials are algebraic objects). It is thus not hard to check that if σ is any automorphism of the complex numbers and $\alpha \in \mathrm{End}(E)$, then the action of α on the (co)tangent space of E^{σ} is as α^{σ}. The result follows immediately from this, since over the field kK, $E^{\sigma} \cong E$ and $\alpha^{\sigma} = \alpha$.

Exercise 1.14: Suppose that $E_{/k}$ is an elliptic curve with CM by (an order in) the field K, with $k \subset \mathbb{C}$.
a) $\mathrm{End}_k(E)$ acts on the cotangent space $\Omega^1_{E/k}$, giving a representation (the k-rational representation)

$$\rho_k : \mathrm{End}_k(E) \to M_1(k) \cong k.$$

Show that this representation is faithful. (When $k = \mathbb{C}$, this is the dual of the complex representation we defined above.)
b) Use this to give another proof that for a CM elliptic curve with $\mathrm{End}^0(k) = K$, $\mathrm{End}(E) = \mathrm{End}_k(E) \implies \mathrm{K} \subset k$.
c) Suppose that E is a CM elliptic curve defined over $\mathbb{R}$. Give a topological proof that $\mathrm{End}_{\mathbb{R}}(E) = \mathbb{Z}$. (Hint: consider the action of complex conjugation on the singular cohomology group $H^1(E(\mathbb{R}), \mathbb{Q})$.)

Finally, if k is not actually a subfield of $\mathbb{C}$, then our elliptic curve $E_{/k}$ is actually defined over a small subfield of k. Indeed, taking a Weierstrass equation $y^2 = x^3 + Ax + B$ shows E is defined over $\mathbb{Q}(A, B)$ (so a field of transcendence degree at most 2); in fact, though, we know that E can be defined over $\mathbb{Q}(j(E))$, a field of transcendence degree at most 1. Thus certainly E can be defined over $\mathbb{C}$, and the preceding discussion shows that its endomorphisms can be defined over k (in the non-CM case) or over kK in the CM case.

However, there is one problem: how do we know that if k is some crazy field containing $\mathbb{C}$, then E does not acquire *more* endomorphisms over k? To see that this is not too farfetched for us to worry about, consider the group of of algebraic maps from $E_{/k}$ to $E_{/k}$ (not necessarily preserving the origin). Aside from the homomorphisms, there is always translation by any point $P \in E(k)$, and if k is algebraically closed then the natural map $E(k) \to \mathbb{P}^1(k)$ given by $P \mapsto x(P)$ is surjective. Thus, if k has larger cardinality then the continuum, so does the group of automorphisms of E as an algebraic curve!

In fact it follows from what we have done already that an elliptic curve will never have a larger endomorphism ring over any field of characteristic zero than it does over the complex numbers: the only endomorphism rings possible over any field of characteristic zero are $\mathbb{Z}$ and orders in imaginary quadratic fields, and in the latter case we know that all the endomorphisms can be defined over a number field. In other words, we know the following result:

[6] For more details, see [ECII, II.2.2]

Proposition 17. *Let E be an elliptic curve defined over an arbitrary field k. Suppose $k \subset K$ and $\varphi \in \mathrm{End}_K(E)$ is an endomorphism defined over the larger field K. Then there exists an intermediate field $k \subset l \subset K$, with l/k finite, such that φ can be defined over l.*

Problem 1.3: Give a proof of this proposition that generalizes to higher-dimensional abelian varieties.

1.6. **An application to CM elliptic curves.** The previous results suggest an algorithm to determine whether an elliptic curve defined over a number field has complex multiplication. We outline it here; it would be nice if someone was interested enough to try to implement it.

The basic principle is the above (unproved, but never mind!) observation that given an elliptic curve defined over a number field, the characteristic zero endomorphism ring injects into all the endomorphism rings of the reductions mod $\mathfrak{p}$ (for defined for all but finitely many primes of K), and that one should use these positive characteristic "clues" to determine the endomorphism ring in characteristic zero.

If $j(E)$ is not an algebraic integer, E does not have CM. (This rules out "most" elliptic curves already.)

For a sequence of small primes $\mathfrak{p}$ not dividing the discriminant of a Weierstrass equation for E, one can compute at least the endomorphism algebra of the reduction of E modulo $\mathfrak{p}$ by counting points: E is supersingular if and only if $a_q = q+1-\#\tilde{E}(\mathbb{F}_q)$ is $\equiv 1 \pmod{p}$. Assuming we are not in the supersingular case, the endomorphism algebra is the imaginary quadratic field generated by the roots of $x^2 - a_q x + q$. The endomorphism ring may be a little bit harder to compute, but at least one gets an upper bound on the conductor by considering the order generated by the Frobenius root, i.e., $\mathcal{O} = \mathbb{Z}[x]/(x^2 - a_q x + q)$.

In practice, if E does not have CM, then most of the primes will be primes of ordinary reduction (it follows from a famous theorem of Serre that the set of supersingular primes has density zero), whereas if E has CM, we have seen that half of the primes will have ordinary reduction. Thus, one will quickly develop a *guess* at whether or not E has CM. The trick is to prove the guess.

One works on the following two tasks at the same time:

Task 1: Keep track of a list of the imaginary quadratic fields arising as endomorphism algebras of mod $\mathfrak{p}$ reductions. If one ever gets two distinct imaginary quadratic fields, then one knows the original elliptic curve does not have CM.

Task 2: If, say, of the first 100 primes 98 give ordinary reduction with always the same quadratic field, we suspect the elliptic curve really does have CM and need to find its j-invariant. However, keeping track of the endomorphism rings of the reductions (and using Deuring's Theorem), one will eventually learn exactly what quadratic order the elliptic curve has CM by. But once one guesses this, one applies the modular function j to the imaginary generator $\tau = f\theta$ of the quadratic order. One can compute this approximately but rapidly to very high precision, and using class field theory one can identify a finite list of number fields in which $j(\tau)$ must be an algebraic integer – namely $j(\tau)$ lies in a field of degree equal to the class number of the order and ramified at most at the primes dividing the discriminant of the imaginary quadratic field K; there are only finitely many such number fields.

Thus after a finite computation one gets the j-invariant of the order, and one just has to check whether the j-invariant of our original curve is a Galois conjugate of it.

Exercise 1.15*: Show that is is actually an algorithm: i.e., we will eventually succeed at either Task 1 or Task 2.

Problem 1.4: Actually implement this algorithm: i.e., write a computer program which, given an irreducible polynomial $P[x] \in \mathbb{Q}[x]$, determines whether a root of this polynomial corresponds to a CM j-invariant. Alternately, give a better algorithm to do the same thing.

References

[ECI] J. Silverman, *The Arithmetic of Elliptic Curves, Springer GTM 106.*

[ECII] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer GTM 151.