DETECTING COMPLEX MULTIPLICATION

JEFFREY D. ACHTER

Department of Mathematics
Colorado State University
Fort Collins, CO 80523-1874
`j.achter@colostate.edu`

We give an efficient, deterministic algorithm to decide if two abelian varieties over a number field are isogenous. From this, we derive an algorithm to compute the endomorphism ring of an elliptic curve over a number field.

In this paper, we answer two fundamental decision problems about elliptic curves over number fields. Specifically, we explain how to detect whether two elliptic curves over a number field are isogenous, and how to decide whether an elliptic curve has complex multiplication. These algorithms rely on Lemma 1.2, which actually applies to abelian varieties of any dimension, and Proposition 2.1, respectively.

In each case, we answer a question about a variety over a number field by examining its reduction at finitely many primes. At this level of generality, such a strategy is common in algorithmic number theory. For example, a common method for computing modular polynomials – that is, bivariate polynomials whose roots are j-invariants of elliptic curves related by an isogeny of fixed degree – is to perform the analogous computation over various finite fields, and then to lift the result using the Chinese remainder theorem. In contrast, we will see that to answer the decision problems posed here, one need not ever lift an object to characteristic zero.

The engine driving the machines presented here is Faltings's paper on the Mordell conjecture. Milne observed in *Mathematical Reviews* that Faltings "seems to give an algorithm for deciding when two abelian varieties over a number field are isogenous." In this paper, we further refine the proof of [7, Theorem 5] to the point where it literally yields an efficient algorithm for the isogeny decision problem.

At a crucial stage in that argument, Faltings shows that the isogeny class of X is determined by the action of $\mathrm{Gal}(L/K)$ on $X[\ell](\bar{K})$, where $[L : K]$

2   *J. Achter*

has effectively bounded degree and ramification but is difficult to compute directly. He therefore works with $\widetilde{L}$, the compositum of all possible such extensions of K, a large but still finite extension of K. An appeal to the Chebotarev density theorem guarantees that there is a finite set of primes T of K such that $\{\left[\frac{\mathfrak{p}}{\widetilde{L}/K}\right] : \mathfrak{p} \in T\} = \mathrm{Gal}(\widetilde{L}/K)$. Therefore, X and Y are isogenous if and only if the reductions $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isogenous for each $\mathfrak{p} \in T$.

We derive an algorithm for detecting isogeny by showing that it suffices to use a set of primes $\mathfrak{p}$ with absolute norm smaller than some constant B. Effective Chebotarev-type theorems [3, 8] let us calculate a suitable B solely in terms of the degree and ramification data of L, without requiring recourse to the compositum $\widetilde{L}$.

Subsequently, we show how to use this result to test the hypothesis that an elliptic curve E has complex multiplication by a field F. Briefly, after a finite extension of the base field, there exists an elliptic curve E' with complex multiplication by F. Even without computing E' explicitly, we can use Lemma 1.2 to detect whether E and E' are geometrically isogenous, and thus check whether E has complex multiplication by F.

In the first section, we review literature concerning effective Chebotarev density theorems, and explain how to use ℓ-adic representations to detect isogeny between abelian varieties. The reader may wish to skip Section 1.1 on first reading, and turn directly to Section 1.2.

In the second section, we use these considerations to design algorithms for elliptic curves over number fields. In Section 2.1, we describe an algorithm to determine whether two elliptic curves are isogenous. In Section 2.2, we combine the results of the previous section with new results on complex multiplication to give an algorithm which decides whether a given elliptic curve has complex multiplication.

Several improvements are available to improve the efficiency of these methods. In the interest of streamlining the exposition, these suggestions are gathered as a series of remarks in the final section.

I thank Siman Wong for helpful discussions.

1. Background

As discussed above, the method of this paper is to apply effective Chebotarev bounds to Faltings's proof of the Tate conjecture in order to construct efficient algorithms; we review these results in Sections 1.1 and 1.2, respectively.

1.1. *Effective Chebotarev density theorems*

The Galois group of a finite extension of number fields L/K is generated by the Frobenius elements of primes of L lying over primes $\mathfrak{p}$ of K. We collect here various results from the literature which place upper bounds on the size of the primes necessary in order for their Artin symbols to generate $\mathrm{Gal}(L/K)$. Throughout, we will use (GRH) to highlight bounds which rely on the generalized Riemann hypothesis, and (U) to denote bounds which hold unconditionally.

For an extension of fields L/K, we let $\Delta_{L/K}$ denote the discriminant and $\mathbf{N}_{L/K}$ the norm map. For a prime ideal $\mathfrak{p}$ of K, let $\kappa(\mathfrak{p})$ be the residue field $\mathcal{O}_K/\mathfrak{p}$ and let $p_{\mathfrak{p}}$ be the characteristic of that field.

Let S be a finite set of places of K and N a nonnegative integer. We will express our Chebotarev-type bounds in terms of the following quantities:

$$\Delta^*(K,S,N) := \left|\Delta_{K/\mathbb{Q}}\right|^N (N \cdot \prod_{\mathfrak{p} \in S} p_{\mathfrak{p}}^{1-1/N})^{N \cdot [K:\mathbb{Q}]}$$

$$B_{(\mathrm{LO})}(K,S,N) := 70 \cdot (\log \Delta^*(K,S,N))^2$$

$$B_{(\mathrm{BS})}(K,S,N) := (4 \log \Delta^*(K,S,N) + 2.5N \cdot [K:\mathbb{Q}] + 5)^2$$

$$B_{(\mathrm{GRH})}(K,S,N) := \min\{B_{(\mathrm{LO})}(K,S,N), B_{(\mathrm{BS})}(K,S,N)\}.$$

Let $c_{(\mathrm{U})}$ be the effective constant A_1 of [8], and let

$$B_{(\mathrm{U})}(K,S,N) := \begin{cases} \Delta^*(K,S,N)^{c_{(\mathrm{U})}} & K \supsetneq \mathbb{Q} \\ 2\Delta^*(K,S,N)^{c_{(\mathrm{U})}} & K = \mathbb{Q} \end{cases}.$$

Finally, let

$$\mathcal{T}_{(\mathrm{GRH})}(K,S,N) := \{\mathfrak{p} \subset K : \mathbf{N}_{K/\mathbb{Q}}\mathfrak{p} \leq B_{(\mathrm{GRH})}(K,S,N) \text{ and } \mathfrak{p} \notin S\}$$

$$\mathcal{T}_{(\mathrm{U})}(K,S,N) := \{\mathfrak{p} \subset K : \mathbf{N}_{K/\mathbb{Q}}\mathfrak{p} \leq B_{\bullet}(K,S,N) \text{ and } \mathfrak{p} \notin S\}.$$

Lemma 1.1. *Let K be a finite extension of $\mathbb{Q}$, and let $S \subset K$ be a finite set of prime ideals. Let L/K be a Galois extension with $[L:K] \leq N$ unramified outside S. For any $\sigma \in \mathrm{Gal}(L/K)$, there exists $\mathfrak{p} \in \mathcal{T}_{(\mathrm{U})}(K,S,N)$ and a prime $\mathfrak{q}$ of L dividing $\mathfrak{p}$ such that $\mathrm{Fr}_{\mathfrak{q}} = \sigma$. If the generalized Riemann hypothesis holds, then $\mathfrak{p}$ may be taken in $\mathcal{T}_{(\mathrm{GRH})}(K,S,N)$.*

Proof. The statement combines several different effective Chebotarev density theorems. For a conjugacy class $C \subset \mathrm{Gal}(L/K)$, each gives an effective upper bound for the norm of the smallest prime $\mathfrak{p}$ such that $\left[\frac{\mathfrak{p}}{L/K}\right] = C$,

computed in terms of the absolute discriminant of L. By [15, Proposition 5], $\left|\Delta_{L/\mathbb{Q}}\right| \leq \Delta^*(K, S, N)$; thus, in the sequel, we may replace each occurrence of $\left|\Delta_{L/\mathbb{Q}}\right|$ in [3, 8, 9] with $\Delta^*(K, S, N)$.

By [8, Theorem 1.1], any conjugacy class $C \subset \text{Gal}(L/K)$ occurs as $\left[\frac{\mathfrak{p}}{L/K}\right]$ for some $\mathfrak{p} \in \mathcal{T}_{\text{(U)}}(K, S, N)$. Now suppose that the generalized Riemann hypothesis holds. Lagarias and Odlyzko prove [9] that a bound of the form $B_{\text{(LO)}}$ suffices, and Oesterle shows [15, 2.5] that the constant is at most 70. The bound $B_{\text{(BS)}}$ is obtained by Bach and Sorenson in [3, Theorem 5.1], again under the assumption of the generalized Riemann hypothesis.

Since the Frobenius elements $\text{Fr}_{\mathfrak{q}}$ of all primes lying over a prime $\mathfrak{p}$ of K form the conjugacy class $\left[\frac{\mathfrak{p}}{L/K}\right]$, the result follows. $\qquad\square$

1.2. *Abelian varieties and Galois modules*

Let X/K be an abelian variety, and let ℓ be a rational prime such that X has good reduction at all primes of K lying over ℓ. The ℓ-adic Tate module of X is $T_\ell(X) := \lim_{\overleftarrow{n}} X[\ell^n](\bar{K})$; let $V_\ell(X) := T_\ell(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ be the rational Tate module. Then $T_\ell(X)$ is a $\mathbb{Z}_\ell$-representation of $\text{Gal}(\bar{K}/K)$, while $V_\ell(X)$ is a $\mathbb{Q}_\ell$ representation of $\text{Gal}(\bar{K}/K)$. It has long been known that these representations encode detailed arithmetic information about X.

In fact, Faltings proves the Tate conjecture; the canonical map $\text{End}(X) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \text{End}(T_\ell X)^{\text{Gal}(K)}$ is an isomorphism. Consequently [7, Corollary 2] two abelian varieties are X and Y are isogenous if and only if $V_\ell X$ and $V_\ell Y$ are isomorphic as $\text{Gal}(\bar{K}/K)$-modules.

We denote the reduction of an abelian variety X/K at a prime of good reduction $\mathfrak{p}$ by $X_{\mathfrak{p}}$; it is an abelian variety over $\kappa(\mathfrak{p})$.

The following result was proved by Serre [15, 8.3] in the special case where $\dim X = \dim Y = 1$ and $K = \mathbb{Q}$, but the the absolute constant given there is ineffective.

Lemma 1.2. *Let X and Y be g-dimensional abelian varieties over a number field K. Let S be a set of places of K containing all primes of bad reduction of X and Y, and let ℓ be a rational prime which is relatively prime to each place of S. Let $\nu_g(\ell) = |\text{GL}_{2g}(\mathbb{Z}/\ell)|$. Then X and Y are isogenous if and only if $X_{\mathfrak{p}}$ and $Y_{\mathfrak{p}}$ are isogenous for all $\mathfrak{p} \in \mathcal{T}_{\text{(U)}}(K, S, \nu_g(\ell)^2)$. If the generalized Riemann hypothesis is true, then X and Y are isogenous if and only if $X_{\mathfrak{p}}$ and $Y_{\mathfrak{p}}$ are isogenous for all $\mathfrak{p} \in \mathcal{T}_{\text{(GRH)}}(K, S, \nu_g(\ell)^2)$.*

Proof. Our proof is closely modelled on that of [7, Theorem 5] and [12,

Theorem 23.7]. Let $\mathcal{T} = \mathcal{T}_{(\mathrm{GRH})}(K, S, \nu_g(\ell)^2)$ if the generalized Riemann hypothesis is to be assumed, and let $\mathcal{T} = \mathcal{T}_{(\mathrm{U})}(K, S, \nu_g(\ell)^2)$ otherwise. The key point is that the isogeny class of an abelian variety over a number field is determined by the Galois representation on its rational Tate module. Lemma 1.1 lets us detect the isomorphism class of a Galois representation using only the Frobenius elements over the finite set of primes $\mathcal{T}$.

Let $\rho : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(T_\ell X) \times \mathrm{Aut}(T_\ell Y)$ be the product representation. Since X and Y both have good reduction outside S, $\mathrm{Gal}(\bar{K}/K)$ acts on $T_\ell X \times T_\ell Y$ via some quotient $\mathrm{Gal}(E/K)$ with E unramified outside S. Let R be the subring of $\mathrm{End}(T_\ell X) \times \mathrm{End}(T_\ell Y)$ generated over $\mathbb{Z}_\ell$ by $\{\rho(\sigma) : \sigma \in \mathrm{Gal}(E/K)\}$. We will show that R is in fact generated, again over $\mathbb{Z}_\ell$, by the actions of $\mathrm{Fr}_{\mathfrak{q}}$ for primes $\mathfrak{q}$ of E lying over $\mathfrak{p} \in \mathcal{T}$.

By Nakayama's Lemma, it suffices to prove that these Frobenius elements, acting on $(T_\ell X/\ell) \times (T_\ell Y/\ell) = X[\ell](\bar{K}) \times Y[\ell](\bar{K})$, generate $(R/\ell)^{\times}$. Now, the action of $\mathrm{Gal}(E/K)$ on $X[\ell](\bar{K}) \times Y[\ell](\bar{K})$ factors through $\mathrm{Gal}(L/K)$, where $[L : K]$ is a finite Galois extension of degree at most $\left|\mathrm{Aut}(X[\ell](\bar{K})) \times \mathrm{Aut}(Y[\ell](\bar{K}))\right| = \nu_g(\ell)^2$. By Lemma 1.1, $\{\mathrm{Fr}_{\mathfrak{q}} : \mathfrak{q}|\mathfrak{p} \in \mathcal{T}\} = \mathrm{Gal}(L/K)$. Therefore, $\{\rho(\mathrm{Fr}_{\mathfrak{q}}) : \mathfrak{q}|\mathfrak{p} \in \mathcal{T}\}$ generates R/ℓ over $\mathbb{Z}/\ell$, and this same set generates R over $\mathbb{Z}_\ell$.

If $X_{\mathfrak{p}}$ and $Y_{\mathfrak{p}}$ are isogenous for some prime of good reduction $\mathfrak{p}$, then [20, Theorem 1] $V_\ell X$ and $V_\ell Y$ are isomorphic as $\mathrm{Gal}(\kappa(\mathfrak{p}))$-modules. The hypothesis that $X_{\mathfrak{p}}$ and $Y_{\mathfrak{p}}$ are isogenous for $\mathfrak{p} \in \mathcal{T}$ implies that, for each $\mathrm{Fr}_{\mathfrak{q}}$ with $\mathfrak{q}|\mathfrak{p} \in \mathcal{T}$, $\mathrm{tr}(\mathrm{Fr}_{\mathfrak{q}}|T_\ell X) = \mathrm{tr}(\mathrm{Fr}_{\mathfrak{q}}|T_\ell Y)$. Extending $\mathbb{Z}_\ell$-linearly, we have $\mathrm{tr}(\sigma|T_\ell X) = \mathrm{tr}(\sigma|T_\ell Y)$ for each $\sigma \in \mathrm{Gal}(\bar{K}/K)$, so that [4, §12.1, Proposition 3] $V_\ell X$ and $V_\ell Y$ are isomorphic as $\mathrm{Gal}(\bar{K}/K)$-modules. By the Tate conjecture [7, Corollary 2] X and Y are isogenous. $\qquad\square$

2. Algorithms for elliptic curves

2.1. *Detecting isogenous elliptic curves*

The isogeny class of an elliptic curve E over a finite field κ is uniquely determined by $|E(\kappa)|$. Indeed, by [20, Theorem 1] the isogeny class of E is determined by its characteristic polynomial of Frobenius, which has the form $T^2 - aT + |\kappa|$. Since the number of points on an elliptic curve with such a characteristic polynomial is $|\kappa| + 1 - a$, we see that two elliptic curves over κ are isogenous if and only if they have the same number of points over κ.

Any efficient algorithm for counting points on elliptic curves over finite fields, such as Schoof's method [14] which requires $O(\log^9 |\kappa|)$ bit opera-

tions, therefore yields an efficient method for deciding if two elliptic curves
are isogenous.

More generally, any efficient algorithm for computing the action of
Frobenius on $T_\ell X$ for a class of abelian varieties X, such as Jacobians
of hyperelliptic curves, can decide if two such abelian varieties are isoge-
nous. (Note that, in dimension greater than one, the action of Frobenius is
not uniquely determined by its trace. Data such as the characteristic poly-
nomial of Frobenius, rather than just the trace of Frobenius, is required to
detect the isogeny class of an abelian variety over κ.)

We now turn our attention to number fields. In principle, Faltings's
theorem affords us a choice of methods for determining whether two elliptic
curves E_1 and E_2 over a given number field are isogenous. For instance,
Masser and Wüstholz [11] use transcendence theory to give an explicit upper
bound on the minimal degree of an isogeny between two elliptic curves.
One could then try to enumerate all curves related to E_1 by an isogeny of
given degree [22], and check if E_2 is isomorphic to any of them. One could
also simply try to see if E_1 and E_2 satisfy a modular equation of suitable
degree. Each of these operations carries a nontrivial computational cost
[1]. Moreover, the best known *constant* appearing in such degree bounds
[13, Théorème 1] is larger than 10^{61}; such a method remains of theoretical,
rather than practical, interest.

Alternatively, an efficient algorithm follows from Lemma 1.2. Given
two elliptic curves E_1 and E_2 over a common number field K, compute
the discriminant Δ_i of E_i, and thence the set of primes S_i for which E_i
has bad reduction. If $S_1 \neq S_2$, then E_1 and E_2 are not isogenous [17,
Corollary 2]. Otherwise, choose a rational prime ℓ relatively prime to each
element of $S := S_1 = S_2$. By Lemma 1.2, E_1 and E_2 are isogenous if and
only if $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are isogenous for for each $\mathfrak{p} \in \mathcal{T}(K, S, (\ell^2 - 1)^2(\ell^2 -
\ell)^2)$; this last condition may be checked using point-counting for each $E_{i,\mathfrak{p}}$.
(Again, if a method is available for computing the characteristic polynomial
of Frobenius, then the same method works for detecting isogeny of abelian
varieties of dimension g; one simply computes at all primes with norm less
than $\nu_g(\ell)^2$.)

We remark that exhibiting infinitely many primes $\mathfrak{p}$ for which $E_{1,\mathfrak{p}}$ and
$E_{2,\mathfrak{p}}$ are isogenous does not prove that E_1 and E_2 are isogenous. Indeed,
suppose that E_1 and E_2 have complex multiplication by distinct fields F_1
and F_2, respectively. On one hand, E_1 and E_2 are not isogenous, since
the rational ring of endomorphisms is an isogeny invariant. On the other
hand, we will see below that $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are both supersingular, and

thus isogenous, for all primes $\mathfrak{p}$ of K for which $p_{\mathfrak{p}}$ is inert in each extension $F_i/\mathbb{Q}$.

2.2. *Detecting complex multiplication*

Let E be an elliptic curve over a number field K. The endomorphism ring $\mathrm{End}(E)$ of E is isomorphic either to $\mathbb{Z}$ or to an order $\mathcal{O}$ in a quadratic imaginary field, F. In the latter case, we say that E has complex multiplication by F. (More generally, we will say that an elliptic curve over an arbitrary field has complex multiplication by F if its endomorphism ring contains an order in F.)

Elliptic curves with complex multiplication are prominent in primality testing and cryptography [2] and other aspects of algorithmic number theory [6]. Motivated by this, one might seek an algorithm for determining whether a given elliptic curve E over a number field K has complex multiplication. In [5], the author describes two methods. The first is a probabilistic algorithm which runs in polynomial time in the inputs; the second runs in deterministic polynomial time, but the constants appearing in the analysis of the running time are ineffective. In this section, we use Lemmas 1.1 and 1.2 to give an efficient, effective algorithm to determine whether an elliptic curve has complex multiplication. We start by collecting a body of facts about elliptic curves with complex multiplication. The subsequent algorithm follows naturally from these observations.

Deuring investigated the relationship between the arithmetic of F and the reductions $E_{\mathfrak{p}}$ at primes of K. (For the moment, we ignore primes of bad reduction.) He proved (see [21, Exemple b]) that $E_{\mathfrak{p}}$ is ordinary if and only if $p_{\mathfrak{p}}$, the rational prime lying under $\mathfrak{p}$, splits in F. Invoking the Chebotarev density theorem for F, we see that E has ordinary reduction at half the primes of K, and supersingular reduction at the others.

Conversely, if $\mathrm{End}(E) \cong \mathbb{Z}$, so that E *does not* have complex multiplication, then supersingular primes have density zero [16, IV-13, Exercise 1]. This basic observation leads to a probabilistic method, detailed in [5], for checking whether an elliptic curve has complex multiplication. Broadly speaking, finding may primes of supersingular reduction provides evidence for the hypothesis that E has complex multiplication.

In the sequel, we will use Lemma 1.2 (and the accompanying discussion at the end of Section 2.1) to describe a deterministic algorithm to test whether an elliptic curve E has complex multiplication. By this, we mean that the algorithm is guaranteed to terminate after a finite, explicitly com-

8   *J. Achter*

putable number of operations, and that the output is a verifiable proof that E does (or does not) have complex multiplication.

It is convenient to assume that the elliptic curve of interest has no automorphisms other than $\{\pm 1\}$, and that it has good reduction everywhere. The former condition is equivalent to the assertion that E *does not* have complex multiplication by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, which is easily verified by checking that $j(E) \notin \{0, 1728\}$.

The latter condition holds, possibly after a finite extension of the base field, for an elliptic curve with complex multiplication. (This assertion is equivalent to the result of Weber [18, C.11.2.a] that an elliptic curve with complex multiplication has integral j-invariant.) Concretely, let $\mathcal{N}$ be the product of all primes of bad reduction of E, and let $K_1 = K(\sqrt{\mathcal{N}})$. Suppose that E has complex multiplication by a field whose only roots of unity are 1 and -1. A special case of [17, Theorem 7] shows that E_{K_1} has good reduction at all places of K_1.

Henceforth, we will assume that E/K has everywhere good reduction.

We now show that it is easy to find a prime of ordinary reduction for E, and thereby find a candidate ring of endomorphisms for E.

Lemma 2.1. *Let E/K be an elliptic curve over a number field with complex multiplication and good reduction everywhere. Let S be the set of rational primes ramified in the extension $S/\mathbb{Q}$. Then there exists a prime $\mathfrak{p}$ of K lying over a rational prime p with $p \leq B_{(\mathrm{U})}(\mathbb{Q}, S, 2)$ such that E has good, ordinary reduction at $\mathfrak{p}$. If the generalized Riemann hypothesis is true, then p may be taken less than or equal to $B_{(\mathrm{GRH})}(\mathbb{Q}, S_{\mathbb{Q}}, 2)$.*

Proof. If $\mathrm{End}(E) \otimes \mathbb{Q}$ is isomorphic to a quadratic imaginary field F, then K necessarily contains F [10, Theorem 3.1.1]. In particular, the support of the discriminant of F over $\mathbb{Q}$ is contained in the support of the discriminant of K over $\mathbb{Q}$, so that F is unramified outside S. Moreover, E has ordinary reduction at a prime $\mathfrak{p}$ over the rational prime p if and only if p splits in F. The Chebotarev density theorem (Lemma 1.1) guarantees the existence of such a p with $p \leq B_{(\mathrm{U})}(\mathbb{Q}, S_{\mathbb{Q}}, 2)$. (If the generalized Riemann hypothesis is true, then p may be taken to be at most $B_{(\mathrm{GRH})}(\mathbb{Q}, S_{\mathbb{Q}}, 2)$.) $\square$

Since supersingular primes have density zero for an elliptic curve *without* complex multiplication, it seems unlikely that one would encounter an E/K without a small (in the sense of Lemma 2.1) ordinary prime. Still, if this were to happen, one could then conclude that the elliptic curve had endomorphism ring equal to $\mathbb{Z}$.

Let $\mathfrak{p}$ be a prime of ordinary reduction of E. Then the ring $\mathbb{Z}[\mathrm{Fr}_{\mathfrak{p}}] \subseteq \mathrm{End}(E_{\mathfrak{p}})$ is isomorphic to an order in a quadratic imaginary field F. (To see this, use the result of Deuring [18, Theorem V.3.1], paralleling the result in characteristic zero, that the endomorphism ring of an ordinary elliptic curve is either $\mathbb{Z}$ or an order in a quadratic imaginary field. Moreover, the Frobenius endomorphism cannot have a real conjugate [21, Exemple a], so it must actually generate a quadratic imaginary field.) Moreover, given the number of points on $E_{\mathfrak{p}}$, one can determine the field $F = \mathrm{Frac}\,\mathbb{Z}[\mathrm{Fr}_{\mathfrak{p}}]$. This is a candidate field of (rational) endomorphisms of E, and we show in Proposition 2.1 how to test the hypothesis that E truly does have complex multiplication by F. (At this stage of the calculation, one knows that E has complex multiplication by *some* quadratic imaginary field if and only if it has complex multiplication by F.)

It is known [18, Corollary C.11.1] that there is a finite extension K' of K and an elliptic curve E'/K' with complex multiplication by F. At this point, one could simply compute the j-invariant of E' and check whether $j(E)$ and $j(E')$ are conjugate under $\mathrm{Gal}(\mathbb{Q})$. However, to compute the polynomial over $\mathbb{Q}$ which $j(E')$ satisfies takes time $O(\left|\Delta_{F/\mathbb{Q}}\right|^2 (\log\left|\Delta_{F/\mathbb{Q}}\right|)^2)$ [2] (see also [6, 7.6]).

Now, if one could construct E' efficiently, one could use Lemma 1.2 to test whether E and E' are isogenous, since isogenous elliptic curves have commensurable rings of endomorphisms. Even without knowing E' explicitly, however, we can efficiently test whether the two curves are (geometrically) isogenous.

Proposition 2.1. *Suppose that E/K has good reduction everywhere. Let F be a quadratic imaginary subfield of K whose only roots of unity are -1 and 1, and let $h^*(F) = 2\sqrt{\Delta_{F/\mathbb{Q}}}/\pi$. Then E has complex multiplication by F if and only if for each prime $\mathfrak{p} \in K$ lying over a rational prime p with $\mathbf{N}\mathfrak{p} \leq B_{(\mathrm{U})}(K, \emptyset, h^*(F)\nu_2(2)^2)$, either:*

- *$E_{\mathfrak{p}}$ is supersingular and F is inert or ramified at p, or*
- *$\mathrm{End}(E_{\mathfrak{p}}) \otimes \mathbb{Q} \cong F$, and F is split at p.*

If the generalized Riemann hypothesis is true, then it suffices to consider those primes with norm at most $B_{(\mathrm{GRH})}(K, \emptyset, h^*(F)\nu_2(2)^2)$.

Proof. If the generalized Riemann hypothesis is to be assumed, we write B for $B_{(\mathrm{GRH})}$ and $\mathcal{T}$ for $\mathcal{T}_{(\mathrm{GRH})}$; otherwise, these symbols denote $B_{(\mathrm{U})}$ and $\mathcal{T}_{(\mathrm{U})}$, respectively. Note that the statement is equivalent to the assertion

10   *J. Achter*

that E has complex multiplication by F if and only if the same is true of $E_{\mathfrak{p}}$ for each prime $\mathfrak{p} \in B(K, \emptyset, h^*(F)\nu_2(2)^2)$. Since there is a natural inclusion $\operatorname{End}(E) \hookrightarrow \operatorname{End}(E_{\mathfrak{p}})$ for each prime $\mathfrak{p}$ [10, Theorem 2.3.2], if E has complex multiplication by F then the same is true of $E_{\mathfrak{p}}$ for each prime $\mathfrak{p}$, and in particular for those in $B(K, \emptyset, h^*(F)\nu_2(2)^2)$.

Having secured this, we focus on the converse. There exists an elliptic curve over a field K' with complex multiplication by F if and only if K' contains the Hilbert class field of F [18, Theorem C.11.2]. Moreover, since the only roots of unity in F are $\{\pm 1\}$, we may assume that E' has good reduction everywhere [17, Theorem 9].

Therefore, let K' be the compositum of K and the Hilbert class field of F, and let E'/K' be an elliptic curve with everywhere good reduction and complex multiplication by F. The original elliptic curve E has complex multiplication by F if and only if $E_{K'}$ and E' are isogenous over some finite extension of K'. (An analytic construction, as in [18, C.11], shows that E and E' are isogenous over $\mathbb{C}$; this isogeny must then descend to some finite K'/K [19, Theorem II.2.2].) Equivalently, E has complex multiplication by F if and only if $E_{K'}$ is isogenous to some twist of E'.

Let $N = \nu_2(2)^2$ and suppose that, for all primes $\mathfrak{q} \in \mathcal{T}(K', \emptyset, N)$, $E_{\mathfrak{q}}$ has complex multiplication by F. Then $E_{\mathfrak{q}}$ and $E'_{\mathfrak{q}}$ are isogenous up to a quadratic twist, and there exists a twist E'' of E' such that $E_{\mathfrak{q}}$ and $E''_{\mathfrak{q}}$ are isogenous for all $\mathfrak{q} \in \mathcal{T}(K', \emptyset, N)$. By Lemma 1.2, E and E'' are isogenous, and thus E has complex multiplication by F.

If the prime $\mathfrak{q}$ of K' lies over the prime $\mathfrak{p}$ of K, then $\mathbf{N}_{K'/\mathbb{Q}}(\mathfrak{q}) \leq \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{p})$. In particular, each prime $\mathfrak{q} \in \mathcal{T}(K', \emptyset, N)$ lies over a prime $\mathfrak{p}$ with $\mathbf{N}_{K/\mathbb{Q}}\mathfrak{p} \leq B(K', \emptyset, N)$. Moreover, $E_{\mathfrak{q}}$ is the base change $E_{\mathfrak{p}} \times \kappa(\mathfrak{q})$, and thus $E_{\mathfrak{q}}$ has complex multiplication by F if and only if $E_{\mathfrak{p}}$ does. We have thus shown that E has complex multiplication by F if and only if the same is true for each reduction $E_{\mathfrak{p}}$ with $\mathbf{N}_{K/\mathbb{Q}}\mathfrak{p} \leq B(K', \emptyset, N)$. Now, K' is an unramified extension of K of degree at most $h^*(F)$. Therefore,

$$
\begin{aligned}
\Delta^*(K', \emptyset, N) &= \left|\Delta_{K'/\mathbb{Q}}\right|^N N^{N \cdot [K':\mathbb{Q}]} \\
&= \left|\Delta_{K/\mathbb{Q}}^{[K':K]}\right|^N \cdot N^{N \cdot [K':K] \cdot [K:\mathbb{Q}]} \\
&= \left|\Delta_{K/\mathbb{Q}}\right|^{N \cdot [K':K]} (N^{N \cdot [K':K]})^{[K:\mathbb{Q}]} \\
&\leq \Delta^*(K, \emptyset, h^*(F)N),
\end{aligned}
$$

and the result follows. $\square$

Taken together, the results of this subsection suggest the following algo-

rithm for determining whether an elliptic curve E has complex multiplication. First, check whether $j(E) \in \{0, 1728\}$; if so, the answer is yes; if not, one continues. Second, construct $K(\sqrt{\mathcal{N}})$, and verify that $E/K(\sqrt{\mathcal{N}})$ has good reduction everywhere; if this fails, then [17, Theorem 7] E does not have complex multiplication. Otherwise, replace K with $K(\sqrt{\mathcal{N}})$, and use Lemma 2.1 to find a candidate field F of endomorphisms. Finally, Proposition 2.1 allows us to test efficiently if E/K has complex multiplication by F.

3. Algorithmic considerations

We close with some remarks which may allow more efficient implementation of these algorithms.

Chebotarev density theorem It is sometimes possible to improve the bounds given in Lemma 1.1. In special cases where $[K : \mathbb{Q}]$ and N are both small, [3, Table 1] provides even tighter bounds for the norm of the smallest prime ideal with given Artin symbol.

Moreover, if either the bound $B_{(BS)}$ or $B_{(U)}$ is used, then it suffices to consider those primes $\mathfrak{p}$ of K with norm a rational prime.

Bounds in Lemma 1.2 The term $\nu(g) = |\mathrm{GL}_{2g}(\mathbb{Z}/\ell)|$ arises in the proof of Lemma 1.2 as the size of the automorphism group of $X[\ell]$. If X further comes equipped with a polarization over K of degree prime to ℓ, then the action of $\mathrm{Gal}(\bar{K}/K)$ on $T_\ell X$ commutes with the induced symplectic pairing. Therefore, if one further makes the assumption in Lemma 1.2 that X and Y admit polarizations over K of degree relatively prime to ℓ, then $\nu_g(\ell)$ may be replaced by $\left|\mathrm{GSp}_{2g}(\mathbb{Z}/\ell)\right|$.

Candidate fields of complex multiplication In Section 2.2, we suggested using Lemma 2.1 to find a candidate ring of endomorphisms of E. Alternatively, if $\mathrm{End}_K(E)$ is an order in a quadratic imaginary field then $\mathrm{End}_K(E) \subseteq K$, so that $\mathrm{End}_K(E) \otimes \mathbb{Q}$ is a quadratic imaginary subfield of K. Therefore, one can enumerate each such subfield F_i of K, and apply Proposition 2.1 to each; E has complex multiplication by some field if and only if it has complex multiplication by one of the F_i.

Bounds in Proposition 2.1 The proof of Proposition 2.1 shows that it suffices to consider those primes of K with norm at most, e.g.,

$$70 \cdot (h^*(F) \log \Delta^*(K, \emptyset, \nu_2(2)^2))^2$$

if the Lagarias and Odlyzko bound is to be used; the analogous improvement may be made in each of the other bounds, as well. Moreover, one can replace the (perhaps pessimistic) bound $h^*(F)$ with the actual class number of F; this class number can be computed in time $O(|\Delta_{F/\mathbb{Q}}|^{1/4+\epsilon})$, and even $O(|\Delta_{F/\mathbb{Q}}|^{1/5+\epsilon})$ if the generalized Riemann hypothesis is assumed [6, 5.4]. Finally, if one could verify that the Hilbert class field of F is already contained in K, then one would know (in the notation of the proof) that $K = K'$, and one could replace $h^*(F)$ with 1. However, it is not clear to the author how to verify this condition, short of actually computing the Hilbert class field.

Detecting potential complex multiplication It is not hard to adopt the observations of Section 2.2 to test whether E *potentially* has complex multiplication, in the sense that $\mathrm{End}_{\bar{K}}(E) \otimes \mathbb{Q}$ is a quadratic imaginary field. One needs to replace Lemma 2.1 with an upper bound for the size of a prime of ordinary reduction; as noted there, we expect in practice that it is quite easy to find such a prime. This generates a candidate field F of rational endomorphisms for $E_{\bar{K}}$. One can then apply Proposition 2.1 to check whether $E_{K.F}$ has complex multiplication by F.

References

1. Amod Agashe, Kristin Lauter, and Ramarathnam Venkatesan. Constructing elliptic curves with a known number of points over a prime field. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 1–17. Amer. Math. Soc., Providence, RI, 2004.
2. A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.
3. Eric Bach and Jonathan Sorenson. Explicit bounds for primes in residue classes. *Math. Comp.*, 65(216):1717–1735, 1996.
4. N. Bourbaki. *Éléments de mathématique. 23. Première partie: Les structures fondamentales de l'analyse. Livre II: Algèbre. Chapitre 8: Modules et anneaux semi-simples*. Actualités Sci. Ind. no. 1261. Hermann, Paris, 1958.
5. Denis Charles. Complex multiplication tests for elliptic curves. 2004, math.NT/0409501.
6. Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

7. G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

8. J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54(3):271–296, 1979.

9. J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

10. Serge Lang. *Complex multiplication*, volume 255 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983.

11. D. W. Masser and G. Wüstholz. Estimating isogenies on elliptic curves. *Invent. Math.*, 100(1):1–24, 1990.

12. J.S. Milne. Abelian varieties. 1998, http://www.jmilne.org/math/.

13. Federico Pellarin. Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques. *Acta Arith.*, 100(3):203–243, 2001.

14. René Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

15. Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

16. Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989.

17. Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

18. Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

19. Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

20. John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

21. John Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'apres t. honda). *Seminaire Bourbaki*, 352:95–110, 1968/1969.

22. Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.