HORIZONTAL ISOGENY THEOREMS[*]

by

Gerhard Frey, Essen University

and

Moshe Jarden, Tel Aviv University

Directory: \Works\Paper75

20 June, 2001

[*] Research partially supported by the Minkowski Center for Geometry at Tel Aviv University founded by the Minerva Foundation

Introduction

One of the results of Tate's celebrated article from 1966 on endomorphisms of abelian varieties over finite fields [Tat] was the isogeny theorem: Let A and A' be abelian varieties over a finite field K. If $l \neq \mathrm{char}(K)$ and $\rho_{A,l^\infty} \sim \rho_{A',l^\infty}$, then $A \sim_K A'$ (see below for notation). Zarhin generalized the isogeny theorem to the case where K is finitely generated over $\mathbb{F}_p$ and $p \neq 2$. The case $p = 2$ was treated by Mori. Finally, one of the outcomes of Faltings' solution of Mordell's conjecture in 1983 was the isogeny theorem for fields which are finitely generated over $\mathbb{Q}$. As a result, we know now that the isogeny theorem holds over each finitely generated field K.

One may view ρ_{A,l^∞} as the limit of the representations $\rho_{A,l^i}\colon \mathrm{Gal}(K) \to \mathrm{Aut}(A_{l^i})$. It is therefore appropriate to rename the isogeny theorem as the **vertical isogeny theorem**. A result of Zarhin implies a **horizontal isogeny theorem** for abelian varieties: If the representations $\rho_{A,l}$ and $\rho_{A',l}$ of $\mathrm{Gal}(K)$ are equivalent for infinitely many prime numbers l, then $A \sim_K A'$.

Our main interest in this work is elliptic curves over a finitely generated field K. If E and E' are elliptic curves over K and $\rho_{E,l} \sim \rho_{E',l}$ for some l, then $\mathrm{Ker}(\rho_{E,l}) = \mathrm{Ker}(\rho_{E',l})$. Hence, $K(E_l) = K(E'_l)$. Of course, the latter condition does not imply the former one, because $\mathrm{Gal}(K(E_l)/K)$ may have outer automorphisms.

One may relax the latter condition to $[K(E_l, E'_l) : K(E_l) \cap K(E'_l)] \leq c$ for all l in a large set Λ of prime numbers and for some constant $c \geq 1$ which is independent of l and look for an isogeny between E and E'.

Of course, one can not hope for an isogeny over K. For example, let E and E' be elliptic curves over K which are not K-isogenous but become K'-isomorphic for some finite separable extension K' of K. Then $K'(E_l) = K'(E'_l)$ and hence $[K(E_l, E'_l) : K(E_l) \cap K(E'_l)] \leq [K' : K]$ for all l.

So, it makes more sense to ask about an isogeny after some field extension. It follows from results of Serre [Ser, Lemma 9 and Théorème 7] that if K is a number field, then the existence of c and an infinite set Λ as above implies $E \sim_{\tilde{K}} E'$. Here $\tilde{K}$ denotes the algebraic closure of K. We generalize Serre's results:

Theorem A (The strong isogeny theorem for elliptic curves): *Let E and E' be elliptic* *curves over a finitely generated field K. Suppose there exist $c \geq 1$ and a set Λ of prime numbers such that $[K(E_l, E'_l) : K(E_l) \cap K(E'_l)] \leq c$ for each $l \in \Lambda$. Then $E' \sim_{\tilde{K}} E$ in each of the following three cases:*

(a) Λ *is infinite and E has no CM;*

(b) Λ *is infinite, E has CM, and* $\mathrm{char}(K) = 0$*;*

(c) Λ *has Dirichlet density* $> \frac{3}{4}$*, E has CM, and* $\mathrm{char}(K) > 0$.

The basic idea in the case where E has no CM is as in Serre's proof. Let $N_l = K(E_l, E'_l)$ and $M_l = K(E_l) \cap K(E'_l)$. First we realize that if $[N_l : M_l] \leq c$ for infinitely many l, then also E' has no complex multiplication. Then we use that $\mathrm{Gal}(N_l/K(\zeta_l)) \cong \mathrm{SL}(2, \mathbb{F}_l)$ if l is large to find a quadratic character ε_l: $\mathrm{Gal}(K) \to \pm 1$ with $\rho_{E',l} \sim \varepsilon_l \otimes \rho_{E,l}$.

In the case that K is a number field, Serre proves that the ε_l are unramified outside a finite set of prime divisors of K. Hence, Λ has an infinite subset Λ_0 such that $\varepsilon_l = \varepsilon$ is independent of l for all $l \in \Lambda_0$. Let K' be the fixed field of $\mathrm{Ker}(\varepsilon)$. Then the restrictions of $\rho_{E',l}$ and $\rho_{E,l}$ to $\mathrm{Gal}(K')$ are equivalent. It follows from the horizontal isogeny theorem that $E \sim_{K'} E$.

We reduce the case where K is a function field of one variable over a number field to the case of number fields by good reduction. In the case where K is a function field of one variable over a finite field, two additional ingredients appear: Tate curves and Hilbert class fields.

The proof of Theorem A for a finite field K is completely different. Under the assumption of (c), we first find a finite extension K' of K and a subset Λ' of Λ of Dirichlet density larger than $\frac{3}{4}$ with $K'(E_l) = K'(E'_l)$ for all $l \in \Lambda'$. If E and E' are not $\tilde{K}$-isogenous, then $\mathbb{Q}$ has distinct imaginary quadratic extensions L and L' with $L \subseteq \mathrm{End}_{\tilde{K}}(E) \otimes \mathbb{Q}$ and $L' \subseteq \mathrm{End}_{\tilde{K}}(E') \otimes \mathbb{Q}$. Then we find an infinite subset Λ'' of Λ' such that each l in Λ'' is prime in L' but decomposes in L. With the aid of these l we construct infinitely many non isomorphic elliptic curves over K' all of which are K'-isogenous to E'. This contradiction proves that $E \sim_{\tilde{K}} E'$.

The condition "Λ has Dirichlet density $> \frac{3}{4}$" in Theorem A(c) can not be relaxed to "Λ is infinite". This follows from an improved version of a result of Heath-Brown concerning primitive roots modulo p. This result was communicated to the authors by

R. Murty. We do not know whether Theorem A(c) holds under the condition "Λ has positive Dirichlet density".

Convention and Notation

For a field K we let K_s be its separable closure, $\tilde{K}$ its algebraic closure, and $\mathrm{Gal}(K) = \mathrm{Gal}(K_s/K)$ its absolute Galois group. If $\mathrm{char}(K) \nmid n$, then ζ_n denotes a primitive root of unity of order n. We say that K is **finitely generated** if K is finitely generated over its prime field.

Let A, A' be abelian varieties over K and L a field extension of K. We write $A \sim_L A'$ if the varieties $A \times_K L$ and $A' \times_K L$ (which are defined over L) are isogenous. In this case we also say that A and A' are **L-isogenous**. Suppose now that K_0 is a subfield of K. We say that A is **defined** over K_0 if there exists an abelian variety A_0 over K_0 with $A \cong A_0 \times_{K_0} K$.

Let A_l, $T_l(A)$, and V_l be the subgroup of l-torsion points of A, its l-Tate-module, and $T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, respectively. Here and through the whole work we use l for a prime number. Denote the torsion subgroup of A by A_{tor}.

Further, we use $\rho_{A,l}$ and ρ_{A,l^∞} to denote the l-ic (also known as "mod l") and l-adic representations of $\mathrm{Gal}(K)$ defined by the action of $\mathrm{Gal}(K)$ on $A_l(\tilde{K})$ and $T_l(A)$, respectively. We will tacitly assume that bases for $A_l(\tilde{K})$ and $T_l(A)$ have been chosen and consider $\rho_{A,l}$ and ρ_{A,l^∞} as homomorphisms of $\mathrm{Gal}(K)$ into $\mathrm{GL}(n, \mathbb{F}_l)$ and $\mathrm{GL}(n, \mathbb{Z}_l)$, respectively, for an appropriate n.

For l-ic representations ρ: $\mathrm{Gal}(K) \to \mathrm{GL}(n, \mathbb{F}_l)$ and ρ': $\mathrm{Gal}(K) \to \mathrm{GL}(n', \mathbb{F}_l)$ we write $\rho \sim \rho'$ if ρ and ρ' are **equivalent**. That is, $n = n'$ and there exists $g \in \mathrm{GL}(n, \mathbb{F}_l)$ with $g^{-1}\rho(\sigma)g = \rho'(\sigma)$ for all $\sigma \in \mathrm{Gal}(K)$. Similarly we write $\rho \sim \rho'$ for l-adic representations ρ: $\mathrm{Gal}(K) \to \mathrm{GL}(n, \mathbb{Q}_l)$ and ρ': $\mathrm{Gal}(K) \to \mathrm{GL}(n', \mathbb{Q}_l)$ if $n = n'$ and there is $g \in \mathrm{GL}(n, \mathbb{Q}_l)$ with $g^{-1}\rho(\sigma)g = \rho'(\sigma)$ for all $\sigma \in \mathrm{Gal}(K)$.

Let E be an elliptic curve over a field K. We write $\mathrm{End}_{\tilde{K}}(E)$ for $\mathrm{End}(E \times_K \tilde{K})$. We say that E has CM if $\mathrm{End}_{\tilde{K}}(E)$ properly contains $\mathbb{Z}$.

Acknowledgement: We are indebted to Wulf-Dieter Geyer for help in case when K is finite and to Aharon Razon for a critical reading of the manuscript.

1. Isogeny theorems for abelian varieties

We start with an observation about the effect of an isogeny between two abelian varieties over a field K on the l-adic and l-ic representations of $\mathrm{Gal}(K)$ associated with these varieties.

LEMMA 1.1: *Let λ: $A \to A'$ be an isogeny of abelian varieties over a field K. Then the following holds:*

(a) $\rho_{A,l^\infty} \sim \rho_{A',l^\infty}$ *for each* $l \neq \mathrm{char}(K)$.

(b) $\mathrm{trace}(\rho_{A,l}(\sigma)) = \mathrm{trace}(\rho_{A',l}(\sigma))$ *for each* $l \neq \mathrm{char}(K)$ *and every* $\sigma \in \mathrm{Gal}(K)$.

(c) $\rho_{A,l} \sim \rho_{A',l}$ *for each* $l \neq \mathrm{char}(K)$ *which does not divide* $|\mathrm{Ker}(\lambda)|$.

Proof of (a): Suppose $l \neq \mathrm{char}(K)$. By definition, $\lambda(A(\tilde{K})) = A'(\tilde{K})$ and $\mathrm{Ker}(\lambda)$ is finite. So, $\dim(A)$ and $\dim(A')$ are the same number d.

By [Mum, p. 64], $T_l(A)$ (resp. $T_l(A')$) is a free $\mathbb{Z}_l$-module of rank $2d$. As $\mathrm{Ker}(\lambda)$ is finite, λ induces an embedding of $\mathbb{Z}_l$-modules, $T_l(\lambda)$: $T_l(A) \to T_l(A')$. So, $\mathrm{Coker}(T_l(\lambda))$ is finite. Tensoring with $\mathbb{Q}_l$ gives an isomorphism $V_l(\lambda)$: $V_l(A) \to V_l(A')$ of finite dimensional $\mathbb{Q}_l$-vector spaces. Since the isomorphism commutes with the action of $\mathrm{Gal}(K)$, we have $\rho_{A,l^\infty} \sim \rho_{A',l^\infty}$.

Proof of (b): By (a), $\mathrm{trace}(\rho_{A,l^\infty}(\sigma)) = \mathrm{trace}(\rho_{A',l^\infty}(\sigma))$. Reduction modulo l gives $\mathrm{trace}(\rho_{A,l}(\sigma)) = \mathrm{trace}(\rho_{A',l}(\sigma))$.

Proof of (c): For each $l \neq \mathrm{char}(K)$, restriction to A_l gives a homomorphism λ_l: $A_l(\tilde{K}) \to A'_l(\tilde{K})$ of $\mathbb{F}_l$-vectors spaces of dimension $2d$ which commutes with the action of $\mathrm{Gal}(K)$. If in addition $l \nmid |\mathrm{Ker}(\lambda)|$, then λ_l is injective and therefore bijective. Conclude that $\rho_{A,l} \sim \rho_{A',l}$. ∎

The isogeny theorems go in the other direction. Under suitable assumptions on the representations attached to A and A', they assert that A and A' are isogenous. The basic results of this sort are due to Tate, Zarhin, Faltings, and Mori.

PROPOSITION 1.2: *Let K be a finitely generated field, A and A' abelian varieties over K, and $l \neq \mathrm{char}(K)$. Then:*

(a) *Semi-simplicity: $V_l(A)$ is a semi-simple* $\mathrm{Gal}(K)$*-module.*

(b) *Tate's conjecture: The natural map* $\mathrm{Hom}_K(A,A')\otimes\mathbb{Z}_l \to \mathrm{Hom}_{\mathrm{Gal}(K)}(T_l(A),T_l(A'))$ *is an isomorphism.*

(c) *Vertical isogeny theorem for abelian varieties: If the l-adic representations ρ_{A,l^∞} and ρ_{A',l^∞} of* $\mathrm{Gal}(K)$ *are equivalent, then $A \sim_K A'$.*

Proof: The case where K is a finite field is due to Tate [Tat, essentially Thm. 1]. This has been generalized to arbitrary finitely generated extensions of $\mathbb{F}_p$ by Zarhin for $p \neq 2$ and by Mori-Zarhin [MoB, p. 244–245, Thm. 2.5] for $p = 2$.

In the case where K is a finitely generated extension of $\mathbb{Q}$, the proposition is due to Faltings [FaW, p. 204, Thm. 1(b) and p. 118 "Proof of 1.3, (ii) $\Longrightarrow$ (i)"]. ∎

Here is an l-ic analog to Proposition 1.2(a),(b):

Proposition 1.3 (Zarhin): *Let A and A' be abelian varieties over a finitely generated field K. Then for almost all l the* $\mathrm{Gal}(K)$*-module A_l is semisimple and the canonical homomorphism*

$$\varphi_l\colon \mathrm{Hom}_K(A,A')\otimes\mathbb{F}_l \to \mathrm{Hom}_{\mathrm{Gal}(K)}(A_l,A'_l)$$

is an isomorphism. Here φ_l maps each K-homomorphism $\eta\colon A \to A'$ onto its restriction to A_l.

Proof: Zarhin proves the theorem in [Zar1, Thm. 1.1] when $\mathrm{char}(K) \neq 0, 2$ and in [Zar2, Cor. 5.4.5] when $\mathrm{char}(K) = 0$. Using a latter result of Mori [MoB, p. 244, Cor. 2.4], the above proofs work also in characteristic 2. ∎

Proposition 1.4 (Horizontal isogeny theorem for abelian varieties): *Let A and A' be abelian varieties over a finitely generated field K. Suppose $\rho_{A,l} \sim \rho_{A',l}$ for infinitely many l. Then A and A' are K-isogenous.*

Proof: It is possible to reduce the horizontal isogeny theorem to the vertical isogeny theorem. However, following an oral communication with Zarhin, we prefer to show how the horizontal isogeny theorem follows from Proposition 1.3.

Let l be a prime number $\neq \mathrm{char}(K)$ such that $\rho_{A,l} \sim \rho_{A',l}$ and the homomorphism φ_l of Proposition 1.3 is an isomorphism. In particular there exists a $\mathrm{Gal}(K)$-isomorphism $h\colon A_l \to A'_l$. Lift h over φ_l to a K-homomorphism $\eta\colon A \to A'$ and let H be the

$\tilde{K}$-connected component of the identity of $\mathrm{Ker}(\eta)$. Then $H_l \leq \mathrm{Ker}(h)$ and therefore $\dim(H) = \frac{1}{2}\dim_{\mathbb{F}_l}(H_l(\tilde{K})) = 0$. Thus, $\mathrm{Ker}(\eta)$ is finite.

In addition, $\dim(A) = \frac{1}{2}\dim_{\mathbb{F}_l}(A_l(\tilde{K})) = \frac{1}{2}\dim_{\mathbb{F}_l}(A'_l(\tilde{K})) = \dim(A')$. Conclude that η is an isogeny. ▮

2. Pairs of elliptic curves without CM

The group $\mathrm{GL}(2,\mathbb{F}_l)$ appears often as the image of $\mathrm{Gal}(K)$ under $\rho_{E,l}$ where E is an elliptic curve over K without CM. A few facts about this group turn out to be useful in the investigation of isogenies of E.

FACT 2.1: *Let $l \geq 3$ be a prime number.*

(a) $\mathrm{SL}(2,\mathbb{F}_l)$ *is generated by all elementary matrices with determinant* 1 *(also called* **transvections***) [Hup, p. 179, Hilfsatz 6.6]. These matrices have the form* $\left(\begin{smallmatrix}1 & \beta\\ 0 & 1\end{smallmatrix}\right)$ *or* $\left(\begin{smallmatrix}1 & 0\\ \gamma & 1\end{smallmatrix}\right)$. *So,* $\mathrm{SL}(2,\mathbb{F}_l)$ *is actually generated by the matrices* $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$. *The order of these matrices is l.*

(b) *The centralizer of* $\mathrm{SL}(2,\mathbb{F}_l)$ *in* $\mathrm{GL}(2,\mathbb{F}_l)$ *consists of all scalar matrices. So, it can be identified with* $\mathbb{F}_l^\times$. *The center of* $\mathrm{SL}(2,\mathbb{F}_l)$ *is the group* $\pm 1 = \left\{\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)\right\}$. *Moreover,* $\mathrm{SL}(2,\mathbb{F}_l)\cdot\mathbb{F}_l^\times$ *is the unique subgroup of index* 2 *of* $\mathrm{GL}(2,\mathbb{F}_l)$ *that contains* $\mathrm{SL}(2,\mathbb{F}_l)$.

(c) *If $l \geq 5$, then* $\mathrm{PSL}(2,\mathbb{F}_l) = \mathrm{SL}(2,\mathbb{F}_l)/\pm 1$ *is a nonabelian simple group [Hup, p. 182, Satz 6.13].*

(d) $|\mathrm{GL}(2,\mathbb{F}_l)| = (l^2-1)(l^2-l)$ *and* $|\mathrm{SL}(2,\mathbb{F}_l)| = l(l^2-1)$ *[Hup, p. 178, Hilfsatz 6.2].*

(e) *Every automorphism of* $\mathrm{PSL}(2,\mathbb{F}_l)$ *or of* $\mathrm{PGL}(2,\mathbb{F}_l)$ *comes from conjugation with an element of* $\mathrm{GL}(2,\mathbb{F}_l)$. *This is a result of Hua. See [Die, §§IV1, IV3, IV6].*

LEMMA 2.2: *For a prime number $l \geq 5$ the only proper nontrivial normal subgroup of* $\mathrm{SL}(2,\mathbb{F}_l)$ *is* ± 1.

Proof: Denote $\mathrm{SL}(2,\mathbb{F}_l)$ by S. Suppose $N \triangleleft S$ and $N \neq 1, \pm 1, S$. By Fact 2.1(c), $\pm 1 \cdot N = S$. Hence $(S : N) \leq 2$. Thus, each $a \in S$ satisfies $a^2 \in N$. If $\mathrm{ord}(a) = l$, this implies $a \in N$. In particular, $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$ are in N. Since these matrices generate S (Fact 2.1(a)), we conclude that $N = S$. ∎

PROPOSITION 2.3: *Let E be an elliptic curve over a finitely generated field K. Suppose E has no CM. Then, for almost all l*

(1a) $\rho_{E,l}(\mathrm{Gal}(K)) \geq \mathrm{SL}(2,\mathbb{F}_l)$,

(1b) $\mathrm{Gal}(K(E_l)/K(\zeta_l)) \cong \mathrm{SL}(2,\mathbb{F}_l)$, *and*

(1c) *if* $\mathrm{char}(K) = 0$, *then* $\rho_{E,l}(\mathrm{Gal}(K)) = \mathrm{GL}(2, \mathbb{F}_l)$.

Proof: For each l, the properties of the lth Weil pairing [Sil1, p. 96, Prop. 8.1] imply that $\zeta_l \in K(E_l)$. Moreover, $\zeta_l^\sigma = \zeta_l^{\det(\rho_{A,l}(\sigma))}$ for each $\sigma \in \mathrm{Gal}(K)$. Hence, $\rho_{E,l}(\mathrm{Gal}(K(\zeta_l))) = \mathrm{SL}(2, \mathbb{F}_l) \cap \rho_{E,l}(\mathrm{Gal}(K))$. So, (1b) follows from (1a). Statement (1c) follows from (1b) because $[K(\zeta_l) : K] = l - 1$ for almost all l. We reduce the proof of (1a) to three cases which appear in the literature.

Reduction step A: *If K' is a finite extension of K and (1a) holds for K', then it also holds for K.* This follows from the inclusion $\rho_{E,l}(\mathrm{Gal}(K')) \le \rho_{E,l}(\mathrm{Gal}(K))$.

Reduction step B: *If L is a finite separable extension of K and (1a) holds for K, then it also holds for L.* Indeed, by Reduction step A, we may replace L by the Galois closure of L/K, if necessary, to assume that L/K is Galois.

Next observe that for $l \neq \mathrm{char}(K)$ the field $K(E_l) \cap L(\zeta_l)$ is a Galois extension of $K(\zeta_l)$ of degree at most $[L : K]$. So, almost all l satisfy $l \ge 5$, $\mathrm{Gal}(K(E_l)/K(\zeta_l)) \cong \mathrm{SL}(2, \mathbb{F}_l)$, $[K(E_l) : K(E_l) \cap L(\zeta_l)] > 2$, and $|\mathrm{SL}(2, \mathbb{F}_l)| > [L : K]$. Since the only nontrivial normal subgroups of $\mathrm{SL}(2, \mathbb{F}_l)$ are itself and ± 1 (Lemma 2.2), we must have $K(E_l) \cap L(\zeta_l) = K(\zeta_l)$. Hence, $\mathrm{Gal}(L(E_l)/L(\zeta_l)) \cong \mathrm{SL}(2, \mathbb{F}_l)$.

Reduction step C: *If L is a purely inseparable extension of K or $L = K(t)$ with t transcendental over K and if (1a) holds for K, then it also holds for L.* Indeed, in both cases, if $l \neq \mathrm{char}(K)$, then $K(E_l)$ is a Galois extension of K and therefore linearly disjoint from L over K.

Conclusion of the proof: Let K_0 be the prime field of K. By [Sil1, p. 50, Prop. 1.4], there exists an elliptic curve E' with $j(E') = j(E) = j$ which is defined over $K_0(j)$ and becomes isomorphic to E over a finite extension of K. Hence, if (1a) holds for E' over $K_0(j)$, then, by the reduction steps, it is true also for E over K.

We may therefore assume that $K = K_0(j)$. Since E has no CM, $K_0(j)$ is an infinite field [Sil1, p. 137, Thm. 3.1(b)]. There are therefore three cases.

Either K is a number field. Then (1a) follows from [Ser, p. 260].

Or, j is transcendental over $\mathbb{Q}$. Then, by a classical result of Weber [Lan2, p. 68], $\rho_{E,n}(\mathrm{Gal}(K)) = \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ for each positive integer n. So, (1a) holds.

Or, j is transcendental over $\mathbb{F}_p$. By a theorem of Igusa [Igu, pp. 469-470], for each $l \neq p$ we have $\rho_{E,l}(\mathrm{Gal}(K)) = \{A \in \mathrm{GL}(2,\mathbb{F}_l) \mid \det(A) \in \langle p \rangle\}$, where $\langle p \rangle$ denotes the subgroup of $\mathbb{F}_l^\times$ generated by p. In particular, $\mathrm{SL}(2,\mathbb{F}_l) \leq \rho_{E,l}(\mathrm{Gal}(K))$ and therefore (1a) holds. ∎

Remark 2.4: Pairs of elliptic curves. Consider elliptic curves E and E' over a field K with $\mathrm{Gal}(K(E_l)/K(\zeta_l)) \cong \mathrm{Gal}(K(E'_l)/K(\zeta_l)) \cong \mathrm{SL}(2,\mathbb{F}_l)$ for all large l. Let $N_l = K(E_l, E'_l)$ and $M_l = K(E_l) \cap K(E'_l)$. Then $\mathrm{Gal}(K(E_l)/M_l)$ is isomorphic to a normal subgroup of $\mathrm{SL}(2,\mathbb{F}_l)$. Hence by Lemma 2.2, $M_l = K(\zeta_l)$, $[K(E_l) : M_l] = 2$, or $M_l = K(E_l)$. In the first case $[K(E_l) : M_l] = |\mathrm{SL}(2,\mathbb{F}_l)| = [K(E'_l) : M_l]$. In the second case, $[K(E_l) : M_l] = 2 = [K(E'_l) : M_l]$. In the third case $K(E_l) = K(E'_l)$. It follows that if $[N_l : K(E_l)] \leq c$ for some constant c and for all l in an infinite set Λ, then for all large $l \in \Lambda$ either $K(E_l) = K(E'_l)$ or $[N_l : K(E_l)] = [N_l : K(E'_l)] = 2$ and $[N_l : M_l] = 4$. We prove in this case that E and E' are isogenous over $\tilde{K}$. ∎

LEMMA 2.5: *Let E and E' be elliptic curves over a field K. Consider a prime number $l \geq 5$ with $l \neq \mathrm{char}(K)$,*

(a) $\mathrm{Gal}(K(E_l)/K(\zeta_l)) \cong \mathrm{Gal}(K(E'_l)/K(\zeta_l)) \cong \mathrm{SL}(2,\mathbb{F}_l)$, *and*

(b) $[K(E_l, E'_l) : K(E_l)] \leq 2$.

Then there exists a quadratic character ε_l: $\mathrm{Gal}(K) \to \pm 1$ such that $\rho_{E',l} \sim \varepsilon_l \otimes \rho_{E,l}$.

Proof: The representation $\rho_{E,l}$ (resp. $\rho_{E',l}$) induces an isomorphism of $\mathrm{Gal}(K(E_l)/K)$ (resp. $\mathrm{Gal}(K(E'_l)/K)$) onto a subgroup H (resp., H') of $\mathrm{GL}(2,\mathbb{F}_l)$ containing $\mathrm{SL}(2,\mathbb{F}_l)$. By (a), $|H| = |H'|$. Since $\mathrm{GL}(2,\mathbb{F}_l)/\mathrm{SL}(2,\mathbb{F}_l) \cong \mathbb{F}_l^\times$ is a cyclic group, $H = H'$.

Let π_l: $\mathrm{GL}(2,\mathbb{F}_l) \to \mathrm{PGL}(2,\mathbb{F}_l)$ be the canonical map whose kernel is the group of all scalar matrices, which we identify with $\mathbb{F}_l^\times$. Let $\bar{\rho}_{E,l} = \pi_l \circ \rho_{E,l}$ and $\bar{\rho}_{E',l} = \pi_l \circ \rho_{E',l}$, and $\bar{H} = \pi_l(H)$. Denote the fixed field of $\mathrm{Ker}(\bar{\rho}_{E,l})$ (resp. $\mathrm{Ker}(\bar{\rho}_{E',l})$) in K_s by L_l (resp. L'_l). Thus, L_l (resp. L'_l) is the fixed field in $K(E_l)$ (resp. $K(E'_l)$) of the center of $\mathrm{Gal}(K(E_l)/K)$ (resp., $\mathrm{Gal}(K(E'_l)/K)$). We claim $L_l = L'_l$.

This is clear if $K(E_l) = K(E'_l)$. Suppose $K(E_l) \neq K(E'_l)$ and let $M_l = K(E_l) \cap K(E'_l)$. Then $[K(E_l) : M_l] = [K(E'_l) : M_l] = 2$ and both $\rho_{E,l}$ and $\rho_{E',l}$ map $\mathrm{Gal}(M_l)$

onto the unique subgroup ±1 of $\mathrm{SL}(2,\mathbb{F}_l)$ of order 2. Then $L_l \cap K(\zeta_l)$ is the unique quadratic subfield K' of $K(\zeta_l)/K$ and $L_l \cdot K(\zeta_l) = M_l$ (Fact 2.1(b)). As $\mathrm{Gal}(M_l/K(\zeta_l))$ is isomorphic to the simple nonabelian group $\mathrm{PSL}(2,\mathbb{F}_l)$ (Fact 2.1(c)), L_l is uniquely determined by those conditions. As L'_l satisfies the same conditions, it coincides with L_l. Thus, in all cases, $\mathrm{Ker}(\bar\rho_{E,l}) = \mathrm{Ker}(\bar\rho_{E',l})$. It follows that $\bar\rho_{E',l} = \bar\alpha_l \circ \bar\rho_{E,l}$ for some $\bar\alpha_l \in \mathrm{Aut}(\bar H)$.

Since $(\mathrm{PGL}(2,\mathbb{F}_l) : \mathrm{PSL}(2,\mathbb{F}_l)) = 2$, we have $\bar H = \mathrm{PSL}(2,\mathbb{F}_l)$ or $\bar H = \mathrm{PGL}(2,\mathbb{F}_l)$. By Fact 2.1(e) there exists $g \in \mathrm{GL}(2,\mathbb{F}_l)$ such that $\pi_l(\rho_{E',l}(\sigma)) = \pi_l(\rho_{E,l}(\sigma)^g)$ for all $\sigma \in \mathrm{Gal}(K)$. Hence, there exists a function $\varepsilon_l\colon \mathrm{Gal}(K) \to \mathbb{F}_l^\times$ such that $\rho_{E',l}(\sigma) = \varepsilon_l(\sigma)\rho_{E,l}(\sigma)^g$ for all $\sigma \in \mathrm{Gal}(K)$. So, ε_l is a homomorphism. Also, $\det(\rho_{E',l}(\sigma)) = \varepsilon_l(\sigma)^2 \det(\rho_{E,l}(\sigma))$. By the properties of the Weil pairing

$$\zeta_l^{\det(\rho_{E,l}(\sigma))} = \zeta_l^\sigma = \zeta_l^{\det(\rho_{E',l}(\sigma))} = \zeta_l^{\varepsilon_l(\sigma)^2 \det(\rho_{E,l}(\sigma))}.$$

Conclude that $\varepsilon_l(\sigma)^2 = 1$ for each $\sigma \in \mathrm{Gal}(K)$. ∎

Lemma 2.6: *Let K be a function field of one variable over a perfect field K_0 of characteristic $\neq 2$. Consider elliptic curves E and E' over K. Let Λ be an infinite set of prime numbers. For each $l \in \Lambda$ let d_l be an element of K such that $K(\sqrt{d_l}) \subseteq K(E_l, E'_l)$. Then K has a quadratic extension K', Λ has an infinite subset Λ_0, and for each $l \in \Lambda_0$ there exists $b_l \in K_0$ such that $K'(\sqrt{b_l}) = K'(\sqrt{d_l})$.*

Proof: For each prime divisor $\mathfrak{p}$ of K/K_0 denote the corresponding normalized valuation by $v_\mathfrak{p}$. Denote the set of all prime divisors $\mathfrak{p}$ of K/K_0 such that E or E' have bad reduction at $\mathfrak{p}$ by Π'. Let Π be the complement set. If $\mathfrak{p} \in \Pi$ and $l \neq \mathrm{char}(K)$, then $v_\mathfrak{p}(l) = 0$. Hence, by Néron-Ogg-Shafarevich, $\mathfrak{p}$ is unramified in $K(E_l, E'_l)$ [Sil1, p. 184, Thm. 7.1] and therefore also in $K(\sqrt{d_l})$. So, $2|v_\mathfrak{p}(d_l)$.

It follows that $\mathrm{div}(d_l) = \mathfrak{a}_l + 2\mathfrak{b}_l$, where the divisor $\mathfrak{a}_l$ of K/K_0 is a linear combination of elements of Π' with coefficients in the set $\{0,1\}$. As Π' is finite, there are only finitely many possibilities for $\mathfrak{a}_l$. Thus, Λ has an infinite subset Λ_1 and K/K_0 has a divisor $\mathfrak{a}$ such that $\mathrm{div}(d_l) = \mathfrak{a} + 2\mathfrak{b}_l$ for each $l \in \Lambda_1$. Choose $l_1 \in \Lambda_1$ to get $\mathrm{div}(d_{l_1}^{-1} d_l) = 2(\mathfrak{b}_l - \mathfrak{b}_{l_1})$ for all $l \in \Lambda_1$.

The divisors $\mathfrak{b}_l - \mathfrak{b}_{l_1}$ correspond modulo principal divisors of K/K_0 to points of $J_2(\tilde{K}_0)$, where J is the Jacobian of K/K_0. As $J_2(\tilde{K}_0)$ is a finite group, K/K_0 has a divisor $\mathfrak{b}$ and Λ_1 has an infinite subset Λ_2 such that for each $l \in \Lambda_2$ there exists $c_l \in K^\times$ with $\mathfrak{b}_l - \mathfrak{b}_{l_1} = \mathfrak{b} + \mathrm{div}(c_l)$.

It follows that for each $l \in \Lambda_2$ we have $\mathrm{div}(d_{l_1}^{-1} d_l) = 2\mathfrak{b} + \mathrm{div}(c_l^2)$. Choose $l_2 \in \Lambda_2$ to get $\mathrm{div}(d_l d_{l_2}^{-1}) = \mathrm{div}(c_l^2 c_{l_2}^{-2})$. Hence, there exists $b_l \in K_0$ with $d_l = b_l c_l^2 c_{l_2}^{-2} d_{l_2}$. The field $K' = K(\sqrt{d_{l_2}})$ and $\Lambda_0 = \Lambda_2$ satisfy the requirements of the lemma ∎

LEMMA 2.7: *Let K be a finitely generated field. Let E and E' be elliptic curves over K. Suppose that there exists an infinite set Λ of prime numbers and a constant c such that*

$$[K(E_l, E_l') : K(E_l)] \le c \tag{2}$$

for each $l \in \Lambda$. Then j_E and $j_{E'}$ are algebraically dependent over the prime field of K.

Proof: Denote the prime field of K by K_0. Let $j = j_E$ and $j' = j_{E'}$. K has a finite separable extension L such that E (resp. E') is isomorphic over L to an elliptic curve E_1 (resp. E_1') such that E_1 (resp. E_1') is already defined over $K_0(j)$ (resp. $K_0(j')$). Condition (2) for K, E, E' implies the same condition for L, E_1, E_1'. Hence, we may replace K, E, E' by L, E_1, E_1', if necessary, to assume that E (resp. E') is already defined over $K_0(j)$ (resp. $K_0(j')$). Let K_1 be the algebraic closure of $K_0(j, j')$ in K. In particular, $K_1(E_l, E_l') \cap K = K_1$ and therefore $[K_1(E_l, E_l') : K_1(E_l)] = [K(E_l, E_l') : K(E_l)] \le c$ for each $l \in \Lambda$. We may therefore replace K by K_1, if necessary, to assume that K is a finite extension of $K_0(j, j')$. Enlarging c, if necessary, we may even assume that $K = K_0(j, j')$.

Assume that j and j' are algebraically independent over K_0. In particular, each of them is transcendental over K_0 and therefore has no CM. Suppose without loss that $\mathrm{char}(K) \notin \Lambda$. Then, for each $l \in \Lambda$, $K_0(j, E_l)$ (resp. $K_0(j', E_l')$) is a regular extension of $K_0(\zeta_l)$ [Igu, p. 468, Thm. 1]. Hence, $K_0(j, E_l)$ and $K_0(j', E_l')$ are linearly disjoint over $K_0(\zeta_l)$ [FrJ, Lemma 9.9].

$$\begin{tikzcd}
K_0(j,E_l) \arrow[r, dash] \arrow[d, dash] & K(E_l) \arrow[r, dash] \arrow[d, dash] & K(E_l,E_l') \arrow[d, dash] \\
K_0(\zeta_l,j) \arrow[r, dash] \arrow[d, dash] & K(\zeta_l) \arrow[r, dash] \arrow[d, dash] & K(E_l') \arrow[d, dash] \\
K_0(\zeta_l) \arrow[r, dash] & K_0(\zeta_l,j') \arrow[r, dash] & K_0(j',E_l')
\end{tikzcd}$$

Hence, by Proposition 2.3,

$$\mathrm{Gal}(K(E_l,E_l')/K(E_l)) \cong \mathrm{Gal}(K_0(j',E_l')/K_0(\zeta_l,j')) \cong \mathrm{SL}(2,\mathbb{F}_l)$$

for all large l. Conclude from Fact 2.1(d) that $[K(E_l,E_l') : K(E_l)] = l(l^2-1)$. This contradicts (2) and proves our claim. ∎

Proposition 2.8: *Let K be a finitely generated field, E and E' elliptic curves over K without CM, and $c > 0$. Suppose $[K(E_l,E_l') : K(E_l)] \le c$ for infinitely many l. Then E is $\tilde{K}$-isogenous to E'.*

Proof: By Remark 2.4, $[K(E_l,E_l') : K(E_l)] \le 2$ for infinitely many l. For each l let $N_l = K(E_l,E_l')$. By assumption and by Proposition 2.3 there exists an infinite set Λ of prime numbers such that for each $l \in \Lambda$ the following conditions hold:

(3a) $l \ge 5$ and $l \ne \mathrm{char}(K)$.

(3b) $\mathrm{Gal}(K(E_l)/K(\zeta_l)) \cong \mathrm{Gal}(K(E_l')/K(\zeta_l)) \cong \mathrm{SL}(2,\mathbb{F}_l)$.

(3c) $[N_l : K(E_l)] \le 2$.

For each $l \in \Lambda$, Lemma 2.5 gives a quadratic character ε_l: $\mathrm{Gal}(K) \to \pm 1$ with

$$\rho_{E',l} \sim \varepsilon_l \otimes \rho_{E,l}. \tag{4}$$

In particular, $\varepsilon_l(\sigma) = 1$ for each $\sigma \in \mathrm{Gal}(N_l)$. Denote the fixed field in K_s of $\mathrm{Ker}(\varepsilon_l)$ by K_l. Then K_l is an extension of K of degree at most 2 which is contained in N_l. Moreover, $\rho_{E,l}|_{\mathrm{Gal}(K_l)} \sim \rho_{E',l}|_{\mathrm{Gal}(K_l)}$. Suppose we prove there are only finitely many possibilities for K_l. Then there will be a quadratic extension K' of K and an infinite subset Λ_0 of Λ such that $K_l = K'$ for each $l \in \Lambda_0$. By the horizontal isogeny theorem (Proposition 1.4), E will be K'-isogenous to E'.

Let therefore K_0 be the prime field of K. By Lemma 2.7, j_E and $j_{E'}$ are algebraically dependent over K_0. Moreover, the first paragraph of the proof of Lemma 2.7 allows us to assume that K is a finite extension of $K_0(j_E, j_{E'})$. There are therefore three cases to consider.

Case A: *K is a number field.* At the end of [Ser, Proof of Lemma 8] Serre proves that if v is a valuation of K which is unramified over $\mathbb{Q}$ and both E and E' have good reduction at v, then v is unramified in K_l. Hence, there are only finitely many possibilities for K_l [Sil1, p. 194, Prop. 1.6].

Case B: *j_E and $j_{E'}$ are transcendental over $\mathbb{Q}$.* Then K is a function field of one variable over a number field F. By Lemma 2.6, K has a quadratic extension K', Λ has an infinite subset Λ_0 and for each $l \in \Lambda_0$ there exists $d_l \in F$ with $K'K_l = K'(\sqrt{d_l})$. Replace K by K' and F by its algebraic closure in K', if necessary, to assume that $K_l = K(\sqrt{d_l})$. Choose a prime divisor $\mathfrak{p}$ of K/F at which both E and E' have good reduction and none of the reduced curves $\bar{E}_\mathfrak{p}$ and $\bar{E}'_\mathfrak{p}$ has CM. (E.g., choose $\mathfrak{p}$ such that the reductions of j_E and $j_{E'}$ modulo $\mathfrak{p}$ are not algebraic integers.) Omit finitely many elements of Λ to assume that Conditions (3a) and (3b) hold also for $\bar{E}_\mathfrak{p}$ and $\bar{E}'_\mathfrak{p}$ over F. Then so does (3c). By Néron-Ogg-Shafarevich we may reduce (4) to

$$\rho_{\bar{E}'_\mathfrak{p},l} \sim \bar{\epsilon}_l \otimes \rho_{\bar{E}_\mathfrak{p},l}, \tag{5}$$

where $\bar{\epsilon}_l$ is a quadratic character of $\mathrm{Gal}(\bar{K})$ with $\bar{K}$ being the residue field of K at $\mathfrak{p}$. Extending $\mathfrak{p}$ to a prime divisor of $\tilde{K}$ with the same name, we find that the residue field of K_l is $\bar{K}(\sqrt{d_l})$. Moreover, by (5), the latter field is the fixed field in $\bar{K}_s$ of $\bar{\epsilon}_l$. As in Case A, there are only finitely many possibilities for $\bar{K}(\sqrt{d_l})$. Hence, there are only finitely many possibilities for $K\bar{K}(\sqrt{d_l})$. So, there are only finitely many possibilities for K_l.

Case C: *j_E and $j_{E'}$ are transcendental over $\mathbb{F}_p$ with $p = \mathrm{char}(K)$.* Then K is a function field of one variable over $\mathbb{F}_{p^m}$ for some $m \in \mathbb{N}$. Replace K by a finite extension, if necessary, to assume that each prime divisor $\mathfrak{p}$ of K satisfies the following condition:

(6a) If E has bad reduction at $\mathfrak{p}$, then the reduction is not potentially good.

(6b) If E' has bad reduction at $\mathfrak{p}$, then the reduction is not potentially good.

Let $l \in \Lambda$. By (3a), $l \neq \mathrm{char}(K)$ and $l \neq 2$. Consider a prime divisor $\mathfrak{p}$ of K. Let $\hat{K}_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$. Denote the index of ramification of $\mathfrak{p}$ in $K(E_l)$ by e. If $e > 1$, then by Néron-Ogg-Shafarevich and since $l \neq \mathrm{char}(K)$, E has bad reduction at $\mathfrak{p}$. By (6a), the reduction is not potentially good. Hence, j_E is not $\mathfrak{p}$-integral [Sil1, p. 181, Prop. 5.5]. Let q be the period that corresponds to j_E [Lan2, p. 201]. Let $E^{(\mathfrak{p})}$ be the Tate-curve over $\hat{K}_{\mathfrak{p}}$ with period q and absolute invariant j_E. Then E is isomorphic to $E^{(\mathfrak{p})}$ over a quadratic extension of $\hat{K}_{\mathfrak{p}}$. Use Krasner's lemma to replace K by a finite extension, if necessary, such that E is already isomorphic to $E^{(\mathfrak{p})}$ over $\hat{K}_{\mathfrak{p}}$. (As E has bad reduction at only finitely many prime divisors of K, we may make the above finite extension independent of $\mathfrak{p}$.) By [Lan2, p. 203, Thm. 3], $\hat{K}_{\mathfrak{p}}(E_l) = \hat{K}_{\mathfrak{p}}(\zeta_l, q^{1/l})$. But $\hat{K}_{\mathfrak{p}}(\zeta_l)/K$ is an unramified extension. Hence, $e = l$. So, in each case e divides l. Similarly, the index of ramification of $\mathfrak{p}$ in $K(E'_l)$ divides l.

Let $M_l = K(E_l) \cap K(E'_l)$. By (3) and Remark 2.4, $[K(E_l) : M_l] \leq 2$ and $[K(E'_l) : M_l] \leq 2$. Hence, each extension $\mathfrak{P}$ of $\mathfrak{p}$ to M_l is unramified both in $K(E_l)$ and in $K(E'_l)$. So, $\mathfrak{P}$ is unramified in N_l. It follows that the ramification index of $\mathfrak{p}$ in N_l divides l. In particular, $\mathfrak{p}$ is unramified in K_l.

We have therefore proved that K_l is an unramified quadratic extension of K. As such, it is contained in the Hilbert class field of K. The latter is a finite extension of K [CaF, p. 356]. Hence, K_l has only finitely many possibilities. ∎

Using remark 2.4 we may reformulate Proposition 2.8 in a way that generalizes [Ser, Lemme 9].

Corollary 2.9: *Let K be a finitely generated field. Let E and E' be elliptic curves over K without CM. If E is not $\tilde{K}$-isogenous to E', then $K(E_l) \cap K(E'_l) = K(\zeta_l)$ for all but finitely many l.*

3. Elliptic curves with CM in characteristic 0

Let E and E' be elliptic curves over a number field K. Suppose one of the curves has CM. Suppose further there is $c > 0$ with $[K(E_l, E'_l) : K(E_l)] \leq c$ for infinitely many l. It is possible to prove then that $K(E_{\rm tor}) \cap K(E'_{\rm tor})$ is an infinite extension of $K_{\rm cycl}$ (the field obtained from K by adjoining all roots of unity). By [Ser, Thm. 7], $E \sim_{\tilde{K}} E'$.

There are few ways to prove the latter result directly. We present one of them here.

LEMMA 3.1: *Let F be a number field, L an abelian extension of $\mathbb{Q}$ which contains F, and l a prime number. Suppose l is unramified in F and tamely ramified in L. Suppose further L/F is unramified outside the primes which lie over l. Then there is $c > 0$ which depends on F but not on l such that $[L : \mathbb{Q}] \leq cl$.*

Proof: By Kronecker-Weber, $L \subseteq \mathbb{Q}(\zeta_m)$ for some positive integer m. Let I be the inertia group of l in $\mathrm{Gal}(L/\mathbb{Q})$. Denote the fixed field of I in L by L_0. Then $[L : L_0]$ is relatively prime to l and divides the ramification index of l in $\mathbb{Q}(\zeta_m)$. The latter divides $(l-1)l^r$ for some positive integer r. Hence, $[L : L_0] | (l-1)$. Also, L_0/F is an abelian unramified extension. So, $[L_0 : F]$ is at most the class number h_F of F. Conclude: $[L : \mathbb{Q}] \leq [F : \mathbb{Q}] h_F (l-1)$. ∎

For each prime number l let a_l and b_l be real numbers. We use the notation "$a_l \ll b_l$" to indicate the existence of $c > 0$ such that $a_l \leq c b_l$ for all l.

LEMMA 3.2: *Let F_1, F_2 be distinct quadratic extensions of $\mathbb{Q}$. For $i = 1, 2$ and each prime number l denote the maximal abelian extension of F_i which is unramified outside l and tamely ramified over l by $F_{i,l}$. Then $[F_{1,l} \cap F_{2,l} : \mathbb{Q}] \ll l$.*

Proof: Write $F_i = \mathbb{Q}(\sqrt{d_i})$ with d_i a square free integer. Let H_i be the Hilbert class field of F_i, that is, the maximal unramified extension of F_i, $i = 1, 2$. Put $F = F_1 F_2$, $L_l = F_{1,l} F_2 \cap F_1 F_{2,l}$, and $H = H_1 \cap H_2$. Then H_i, H, $F_{i,l}$, and L_l are Galois extensions of $\mathbb{Q}$.

CLAIM A: *$F_1 \not\subseteq H_2$ or $F_2 \not\subseteq H_1$.* Otherwise $F \subseteq H$. Hence F is unramified over both F_1 and F_2. Denote the third quadratic extension of $\mathbb{Q}$ which is contained in F by F_0.

For each prime divisor $\mathfrak{p}$ of F which ramifies over $\mathbb{Q}$ put $F_\mathfrak{p}$ for the inertia field of $\mathfrak{p}$ over $\mathbb{Q}$. Then $\mathfrak{p}$ is totally ramified over $F_\mathfrak{p}$. Hence, $F_\mathfrak{p} = F_0$. So, $\mathfrak{p}|_{F_0}$ is unramified over $\mathbb{Q}$. It follows, $F_0/\mathbb{Q}$ is an unramified quadratic extension. This contradiction proves our claim.

Assume for example $F_2 \not\subseteq H_1$.

Claim B: *There is at most one l with $F_2 \subseteq F_{1,l}$.* Indeed, let l, l' be distinct prime numbers. Then $F_{1,l} \cap F_{1,l'}$ is an unramified abelian extension of F_1. So, $F_{1,l} \cap F_{2,l} \subseteq H_1$. Conclude from $F_2 \not\subseteq H_1$ that either $F_2 \not\subseteq F_{1,l}$ or $F_2 \not\subseteq F_{1,l'}$.

Claim C: *$[L_l : \mathbb{Q}] \ll l$.* Indeed let l be a prime number with $F_2 \not\subseteq F_{1,l}$. Put $L_{1,l} = F_{1,l} \cap L_l$ and consider the following diagram of fields

$$\begin{tikzcd}
F_{1,l} \arrow[r, dash] \arrow[d, dash] & F_{1,l}F_2 \arrow[d, dash] & \\
L_{1,l} \arrow[r, dash] \arrow[d, dash] & L_l \arrow[r, dash] \arrow[d, dash] & F_1F_{2,l} \arrow[dd, dash] \\
F_1 \arrow[r, dash] \arrow[d, dash] & F \arrow[d, dash] & \\
\mathbb{Q} \arrow[r, dash] & F_2 \arrow[r, dash] & F_{2,l}
\end{tikzcd}$$

In particular, $L_{1,l}$ is a Galois extension of $\mathbb{Q}$. By assumption, $F_{1,l} \cap F_2 = \mathbb{Q}$. Hence, $L_{1,l} \cap F_2 = \mathbb{Q}$. Also, $[L_l : L_{1,l}] = [F_{1,l}F_2 : F_{1,l}] = [F_2 : \mathbb{Q}] = 2$. Hence, $L_{1,l}F_2 = L_l$. It follows, $\mathrm{Gal}(L_{1,l}/\mathbb{Q}) \cong \mathrm{Gal}(L_l/F_2)$. In addition, $F_1F_{2,l} = FF_{2,l}$ is an abelian extension of F_2. Hence, L_l/F_2 is abelian. Therefore, $L_{1,l}/\mathbb{Q}$ is abelian.

By assumption, $L_{1,l}/F_1$ is unramified outside l and tamely ramified over l. So, Lemma 3.1 gives $c > 0$, independent of l, with $[L_{1,l} : \mathbb{Q}] \leq cl$. Then, $[F_{1,l} \cap F_{2,l} : \mathbb{Q}] \leq [L_l : \mathbb{Q}] \leq cl$, as desired. ∎

Lemma 3.3: *Let E be an elliptic curve with CM over a field K of characteristic* 0. *Let F be the CM-field of E.*

(a) *If $l \nmid 2 \cdot \mathrm{discriminant}(\mathrm{End}(E))$, then $l \nmid [K(E_l) : K]$. If in addition $F \subseteq K$, then $\mathrm{Gal}(K(E_l)/K)$ is abelian.*

(b) *$l^2 \ll [K(E_l) : K] \ll l^2$ as $l \to \infty$.*

Proof: End(E) is isomorphic to an order S of F. Let $K' = KF$. Consider l as in (a). Then $|(S/lS)^\times|$ is $(l-1)^2$ or l^2-1 [GeJ, §4.1]. Moreover, $\mathrm{Gal}(K'(E_l)/K')$ is isomorphic to a subgroup of $(S/lS)^\times$ of index at most 6 [GeJ, §4.2 and Prop. 4.2]. As $[K' : K] \leq 2$, this proves both (a) and (b). ∎

When an elliptic curve E is defined over a field K of characteristic 0 by a Weierstrass equation we denote the Weber function on finite points (x, y) of $E(\tilde{K})$ by h. It is a constant times x (or x^2 or x^3) [GeJ, p. 277].

LEMMA 3.4: *For $i = 1, 2$ let E_i be an elliptic curve over a field of characteristic* 0*. Suppose that E_i has CM. Denote the CM-field of E_i by F_i. Suppose that E_i is defined over $F(j_{E_i})$ and that* End(E_i) *is the ring of integers of F_i. Let $F_{i,l} = F_i(j_{E_i}, h(E_{i,l}))$. Suppose that $F_1 \neq F_2$. Then $[F_{1,l}F_{2,l} : F_{1,l}] \gg l$*

Proof: By definition, $F_i = \mathbb{Q}(\sqrt{-d_i})$, where d_i is a square free positive integer. Denote the set of all prime numbers l that do not divide $2d_1d_2$ by Λ. Let from now on l range over the elements of Λ. Then the following statements are true for $i = 1, 2$:

(1a) $F_{i,l}$ is the maximal abelian extension of F_i unramified outside l.

(1b) $F_{i,l}$ is a Galois extension of $\mathbb{Q}$.

(1c) l is tamely ramified in $F_{i,l}$.

(1d) $l^2 \ll [F_{i,l} : F_i] \ll l^2$.

Indeed, $F_{i,l}$ is the ray class field of F_i with conductor l [Lan2, p. 126, Thm. 2]. So (1a) holds [Neu, p. 100, Cor. 7.6]. Condition (1b) follows from (1a). Next note that $F_i(j_{E_i})$ is the maximal abelian unramified extension of F_i [Lan2, p. 23]. By Lemma 3.3(a), $l \nmid [F_i(j_{E_i}, E_{i,l}) : F_i(j_{E_i})]$. Hence, l is tamely ramified in $F_i(j_{E_i}, E_{i,l})$ and therefore also in $F_{i,l}$. This proves (1c). Finally, Observe that $[F_i(j_{E_i}) : F_i]$ does not depend on l while $[F_i(j_{E_i}, E_{i,l}) : F_i(j_{E_i}, h(E_{i,l})] \leq 6$ [GeJ, Prop. 4.2]. So, (1d) is a consequence of Lemma 3.3(b).

Finally, by (1) and Lemma 3.2, $[F_{1,l}F_{2,l} : F_{1,l}] = [F_{2,l} : F_{1,l} \cap F_{2,l}] = \frac{[F_{2,l}:\mathbb{Q}]}{[F_{1,l}\cap F_{2,l}:\mathbb{Q}]} \gg l$, as contended. ∎

THEOREM 3.5: *Let E_1 and E_2 be elliptic curves over a finitely generated field K. Suppose at least one of the elements j_E or $j_{E'}$ does not belong to a finite field. Suppose* *also there exists c with $[K(E_{1,l}, E_{2,l}) : K(E_{1,l})] \leq c$ for infinitely many l. Then E_1 has CM if and only if E_2 has CM. Moreover, $E \sim_{\tilde{K}} E'$.*

Proof: By Lemma 2.7 none of the elements j_E and $j_{E'}$ belongs to a finite field. Therefore, if $\mathrm{char}(K) \neq 0$, then neither E nor E' has CM. So, by Proposition 2.8, $E \sim_{\tilde{K}} E'$.

Assume therefore $\mathrm{char}(K) = 0$. The case were neither E nor E' has CM is covered by Proposition 2.8. So, assume at least one of the curves has CM. Extend K, if necessary, to assume that K contains the CM-field of that curve. Let $M_l = K(E_l) \cap K(E'_l)$. Then either $K(E_l)/K$ or $K(E'_l)/K$ is an abelian extension [GeJ, (4) on p. 277]. In both cases $M_l/K(\zeta_l)$ is abelian. If the other curve had no CM, we might choose $l \geq 5$ with $\mathrm{Gal}(M_l/K(\zeta_l)) \cong \mathrm{PSL}(2, \mathbb{F}_l)$ (Proposition 2.3). Conclude that this can not happen. So, both curves have CM.

Suppose both E_1 and E_2 have CM. For $i = 1, 2$ let F_i be the CM-field of E_i. Replace E_i by an isomorphic curve, if necessary, to assume that E_i is defined over $\mathbb{Q}(j_{E_i})$ [Sil1, p. 50, Prop. 1.4(c)]. Then there exists c' such that

$$(2) \qquad [F_1F_2(j_{E_1}, j_{E_2}, E_{1,l}, E_{2,l}) : F_1(j_{E_1}, E_{1,l})] \leq c' \text{ for infinitely many } l.$$

Next take an elliptic curve E'_i over $\mathbb{Q}(j_{E_i})$ such that $\mathrm{End}(E'_i)$ is isomorphic to the ring of integers of F_i [Shi, p. 104, Prop. 4.8]. Then E'_i is $\tilde{\mathbb{Q}}$-isogenous to E_i [Shi, p. 105, Prop. 4.9]. In particular, E'_i is isomorphic to E_i over a finite extension of $\mathbb{Q}$. Hence, (2) remains valid for E'_1, E'_2 instead of for E_1, E_2. We may therefore replace E_i by E'_i, if necessary, to assume that $\mathrm{End}(E_i)$ is isomorphic to the ring of integers of F_i, $i = 1, 2$. By [GeJ, Prop. 4.2], $[F_i(j_{E_1}, E_{i,l}) : F_i(j_{E_i}, h(E_{i,l})] \leq 6$. Hence, there exists c'' such that

$$[F_1F_2(j_{E_1}, j_{E_2}, h(E_{1,l}), h(E_{2,l})) : F_1(j_{E_1}, h(E_{1,l}))] \leq c'' \text{ for infinitely many } l.$$

Hence, by Lemma 3.4, $F_1 = F_2$. Conclude from [Shi, p. 105, Prop. 4.9] that $E_1 \sim_{\tilde{K}} E_2$. ∎

4. Elliptic curves over finite fields

Let E and E' be elliptic curves over a finite field K such that

(1) $[K(E_l, E'_l) : K(E_l) \cap K(E'_l)] \leq c$ for some constant c and for all l in a set Λ of prime numbers.

Since $\mathrm{Gal}(K(E_l, E'_l)/K)$ is a cyclic group, Condition (1) gives us less information than in all other cases. We have therefore to assume much more about Λ than just being infinite in order to deduce that $E \sim_{\tilde{K}} E'$. For example, if the Dirichlet density of Λ is greater than $\frac{3}{4}$, then $E \sim_{\tilde{K}} E'$.

We start with the introduction of the notion of 'Dirichlet set' and 'ε-density'. For relatively prime integers a and n let $\Lambda_{a,n}$ be the set of all prime numbers l with $l \equiv a \mod n$. Let Λ be a set of prime numbers. If Λ has a Dirichlet density, we denote it by $\delta(\Lambda)$. Dirichlet's theorem says that $\delta(\Lambda_{a,n}) = \frac{1}{\varphi(n)}$, where $\varphi(n)$ is Euler's totient function [Lan1, p. 167, Example]. We call Λ a **Dirichlet set** if Λ differs from a finite union of sets of the form $\Lambda_{a,n}$ by a finite set. Thus, each infinite Dirichlet set has a positive Dirichlet density. The collection of all Dirichlet sets is a Boolean algebra, i.e., it is closed under unions, intersections, and taking complements. Indeed, let $n_1, \ldots, n_r$ be positive integers and $a_1, \ldots, a_r$ be integers with $\gcd(a_i, n_i) = 1$, $i = 1, \ldots, r$. Put $n = \mathrm{lcm}(n_1, \ldots, n_r)$. Let P_i be the finite set of all prime numbers $p \equiv a_i \mod n_i$ with $p|n$. Then there exist b_{ij} relatively prime to n with $\Lambda_{a_i,n_i} = P_i \cup \bigcup_j \Lambda_{b_{ij},n}$. Hence, the intersection of the Λ_{a_i,n_i} is again a Dirichlet set.

Let ε be a real number. We say that Λ is **ε-dense** if $\Lambda \cap \Lambda'$ is an infinite set for each Dirichlet set Λ' with Dirichlet density at least $1-\varepsilon$. If $\varepsilon' < \varepsilon$ and Λ is ε-dense, then Λ is also ε'-dense. If Λ is ε-dense for each $\varepsilon < 1$, then, by Dirichlet's theorem, $\Lambda \cap \Lambda'$ is infinite for each infinite Dirichlet set Λ'. If $\delta(\Lambda) > \varepsilon$, then Λ is ε-dense. However, there is a set Λ which is ε-dense for each $\varepsilon < 1$ but $\delta(\Lambda) = 0$. For example, order the sets $\Lambda_{a,n}$ in a sequence $\Lambda_1, \Lambda_2, \Lambda_3, \ldots$. Then choose $p_n \in \Lambda_n$ with $p_n > 2p_{n-1}$. Let $\Lambda = \{p_1, p_2, p_3, \ldots\}$. Since for each i there exists $j > i$ such that $\Lambda_i \supseteq \Lambda_j$, the set Λ has the desired properties.

Note that if Λ is ε-dense and Λ_0 is a Dirichlet set with $\delta(\Lambda_0) \leq \gamma$, then $\Lambda \smallsetminus \Lambda_0$ is $(\varepsilon - \gamma)$-dense. Indeed, let Λ' be a Dirichlet set with $\delta(\Lambda') \geq 1 - \varepsilon + \gamma$. Then

$\delta(\Lambda' \smallsetminus \Lambda_0) \geq 1 - \varepsilon$. Hence, $(\Lambda \smallsetminus \Lambda_0) \cap \Lambda' = \Lambda \cap (\Lambda' \smallsetminus \Lambda_0)$ is an infinite set.

Suppose L is a number field with a ring of integers O_L and l is a prime number. We say that l **is prime in** L if lO_L is a prime ideal of O_L. Similarly, we say that l **decomposes into** k **distinct primes in** L if lO_L decomposes into k distinct prime ideals in O_L.

LEMMA 4.1: *Let L and L' be distinct quadratic extensions of $\mathbb{Q}$. Let Λ be a $\frac{3}{4}$-dense set of prime numbers. Then Λ contains infinitely many l which are prime in L' but decompose into two distinct primes in L or Λ contains infinitely many l which are prime in L but decompose into two distinct primes in L'.*

Proof: Denote the discriminant of L (resp. L') by d (resp. d'). Let Δ_1 (resp. Δ_{-1}) be the set of all l such that $l \nmid 2d$ and $\left(\frac{d}{l}\right) = 1$ (resp. $l \nmid 2d$ and $\left(\frac{d}{l}\right) = -1$). If $l \in \Delta_1$, then l decomposes into two distinct primes in L; if $l \in \Delta_{-1}$, then l is prime in L [BoS, p. 236, Thm. 1]. Similarly we define Δ'_1 and Δ'_{-1} with respect to d'.

The quadratic reciprocity law implies that $\Delta_1 \cap \Delta'_{-1}$ is a union of sets of the form $\Lambda_{a,4dd'}$ where a ranges over $\frac{1}{4}$ of all possible values. So, $\delta(\Delta_1 \cap \Delta'_{-1}) = \frac{1}{4}$. Since Λ is $\frac{3}{4}$-dense, $\Lambda \cap (\Delta_1 \cap \Delta'_{-1})$ is an infinite set. ∎

Recall that either $\mathrm{End}_{\tilde{K}}(E) \otimes \mathbb{Q}$ is an imaginary quadratic extension of $\mathbb{Q}$ or $\mathrm{End}_{\tilde{K}}(E) \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$. In the former case one says that E is **ordinary** (or also **singular**), in the latter case one says that E is **supersingular**.

Remark 4.2: Norm of an ideal in $\mathrm{End}_{\tilde{K}}(E)$. Consider $\alpha \in \mathrm{End}_{\tilde{K}}(E) \smallsetminus \mathbb{Z}$ and let $\hat{\alpha}$ be the dual endomorphism. Then $N(\alpha) = \alpha\hat{\alpha} = \deg(\alpha) \in \mathbb{Z}$ [Sil1, p. 86]. Hence, $T(\alpha) = \alpha + \hat{\alpha} = 1 + N(\alpha) - N(\alpha - 1) \in \mathbb{Z}$. So, α and $\hat{\alpha}$ are the roots of the equation $X^2 - T(\alpha)X + N\alpha = 0$ with coefficients in $\mathbb{Z}$. Thus, $L = \mathbb{Q}(\alpha)$ is a quadratic subfield of $\mathrm{End}_{\tilde{K}}(E) \otimes \mathbb{Q}$. It follows that $N\alpha = \mathrm{norm}_{L/\mathbb{Q}}\alpha$ and $T\alpha = \mathrm{trace}_{L/\mathbb{Q}}(\alpha)$. So, $f_\alpha(X) = X^2 - T(\alpha)X + N\alpha$ is the characteristic polynomial of α, viewed as a linear operator of L over $\mathbb{Q}$.

For each l, α may be viewed as an endomorphism α_l of the $\mathbb{Q}_l$-vector space $V_l(E)$. If $l \neq \mathrm{char}(K)$, then $\det(\alpha_l) = \deg(\alpha) = N\alpha$ and $\mathrm{trace}(\alpha_l) = 1 + \deg(\alpha) - \deg(1 - \alpha) =$

$T\alpha$ [Sil1, p. 134, Prop. 2.3]. Hence, the characteristic polynomial of α_l coincides with $f_\alpha(X)$.

Let now $S = L \cap \mathrm{End}_{\tilde{K}}(E)$. Then S is an order of L. For each ideal $\mathfrak{a}$ of S we define $\mathrm{Ker}(\mathfrak{a}) = \bigcap_{\alpha\in\mathfrak{a}} \mathrm{Ker}(\alpha)$. Since $\mathrm{Ker}(\alpha)$ is a finite subgroup of $E(\tilde{K})$ in case $\alpha \neq 0$, also $\mathrm{Ker}(\mathfrak{a})$ is a finite subgroup of $E(\tilde{K})$ if $\mathfrak{a} \neq 0$. Next we define $N\mathfrak{a}$ to be the ideal of $\mathbb{Z}$ generated by all $N\alpha$ with $\alpha \in \mathfrak{a}$. In particular, $N(\alpha S) = \alpha\hat{\alpha}\mathbb{Z}$. If, in addition, $\mathrm{char}(K) \nmid \deg(\alpha)$, then $\deg(\alpha) = |\mathrm{Ker}(\alpha)|$ [Sil1, p. 76] and therefore $N(\alpha S) = |\mathrm{Ker}(\alpha)|\mathbb{Z}$.

Claim: *If $\mathfrak{a}$ is relatively prime to* $\mathrm{char}(K)$ *and to the conductor of S, then* $|\mathrm{Ker}(\mathfrak{a})|\mathbb{Z} = N\mathfrak{a} = (S : \mathfrak{a})\mathbb{Z}$. To this end recall that the **conductor** of S is a positive integer c such that $S = \mathbb{Z} + cO$, where $O = O_L$. Since $\mathfrak{a} + cO = S$, we have $O = S + \mathfrak{a}O$. By [Lan2, p. 92, Thm. 4], $\mathfrak{a}O \cap S = \mathfrak{a}$. Hence, $(S : \mathfrak{a}) = (O : \mathfrak{a}O)$.

The norm of an ideal of O is the ideal of $\mathbb{Z}$ defined by the norm of its elements [Jan, p. 35]. Every $x \in \mathfrak{a}O$ can be written as $x = \sum_{i=1}^m a_i x_i$ with $a_i \in \mathfrak{a}$ and $x_i \in O$. Then $cx = \sum_{i=1}^m a_i \cdot cx_i = a \in \mathfrak{a}$. Hence, $c^2 Nx = Na \in N\mathfrak{a}$. As c is relatively prime to $\mathfrak{a}$, it is also relatively prime to $N\mathfrak{a}$. It follows that $Nx \in N\mathfrak{a}$. Conclude that $N\mathfrak{a} = N(\mathfrak{a}O)$. By [Jan, p. 37, Prop. 8.6], $N\mathfrak{a} = (O : \mathfrak{a}O)\mathbb{Z} = (S : \mathfrak{a})\mathbb{Z}$.

In order to prove that $|\mathrm{Ker}(\mathfrak{a})|\mathbb{Z} = N\mathfrak{a}$ it suffices to prove for each l the equality $|\mathrm{Ker}(\mathfrak{a}) \cap E_{l^\infty}|\mathbb{Z}_{(l)} = N\mathfrak{a}_{(l)}$. Here $E_{l^\infty} = \bigcup_{i=1}^\infty E_{l^i}$. The subscript (l) means localization with respect to the multiplicative set $\mathbb{Z} \smallsetminus l\mathbb{Z}$.

First suppose $l|c$. Then l is relatively prime to $\mathfrak{a}$. Hence, $\mathrm{Ker}(\mathfrak{a}) \cap E_{l^\infty} = 0$ and therefore $|\mathrm{Ker}(\mathfrak{a}) \cap E_{l^\infty}|\mathbb{Z}_{(l)} = \mathbb{Z}_{(l)} = N\mathfrak{a}_{(l)}$. Suppose therefore that $l \nmid c$. Then $S_{(l)} = O_{(l)}$. As $O_{(l)}$ is a Dedekind domain with finitely many prime ideals (at most 2), it is principal [Lan1, p. 21]. Thus, there exists $\alpha \in O$ with $\mathfrak{a}_{(l)} = \alpha S_{(l)}$. Also, if $l \nmid m$, then multiplication by m gives an automorphism of E_{l^∞}. Hence, each element of $S_{(l)}$ is an endomorphism of E_{l^∞}. So,

$$\mathrm{Ker}(\mathfrak{a}) \cap E_{l^\infty} = \mathrm{Ker}(\mathfrak{a}_{(l)}|_{E_{l^\infty}}) = \mathrm{Ker}(\alpha|_{E_{l^\infty}}).$$

Hence, $|\mathrm{Ker}(\mathfrak{a}) \cap E_{l^\infty}|\mathbb{Z}_{(l)} = |\mathrm{Ker}(\alpha|_{E_{l^\infty}})|\mathbb{Z}_{(l)} = |\mathrm{Ker}(\alpha)|\mathbb{Z}_{(l)} = N\alpha \cdot \mathbb{Z}_{(l)} = N\mathfrak{a}_{(l)}$, as desired. ∎

Here is a criterion for the existence of an isogeny of elliptic curves over finite fields which is similar to the one for elliptic curves with CM over number fields.

LEMMA 4.3: *Let E and E' be elliptic curves over a finite field K. Suppose that* $\mathrm{End}_{\tilde{K}}(E)\otimes\mathbb{Q}$ *and* $\mathrm{End}_{\tilde{K}}(E')\otimes\mathbb{Q}$ *have a common quadratic subfield L. Then $E\sim_{\tilde{K}}E'$. In particular, all supersingular elliptic curves are isogenous over $\tilde{K}$.*

Proof: Let $p=\mathrm{char}(K)$. If E is ordinary, then p decomposes in L into two distinct primes [Lan2, p. 175, Thm. 5]. If E' is supersingular, then $\mathrm{End}_{\tilde{K}}(E')\otimes\mathbb{Q}$ ramifies in p [Lan2, p. 178, Remark proceeding Theorem 8]. This implies that $\mathrm{End}_{\tilde{K}}(E')\otimes\mathbb{Q}_p$ is a division algebra (See also [Wei, p. 202]). As $L\otimes\mathbb{Q}_p$ is a commutative subalgebra of $\mathrm{End}_{\tilde{K}}(E')\otimes\mathbb{Q}_p$, it is a field. So, there is only one prime of L over p. [CaF, p. 57, Thm.]. Hence, either both curves are ordinary or both of them are supersingular. In the first case $\mathrm{End}_{\tilde{K}}(E)\otimes\mathbb{Q}=L=\mathrm{End}_{\tilde{K}}(E')\otimes\mathbb{Q}$. In the second case both $\mathrm{End}_{\tilde{K}}(E)\otimes\mathbb{Q}$ and $\mathrm{End}_{\tilde{K}}(E')\otimes\mathbb{Q}$ are the unique quaternion algebra $\mathbb{Q}_{\infty,p}$ which ramifies exactly at p and ∞ [Deu, p. 220]. Conclude from [Mum, p. 259, Cor.] that $E\sim_{\tilde{K}}E'$. ∎

Denote the group of upper triangular matrices in $\mathrm{GL}(2,\mathbb{F}_l)$ by $T(2,\mathbb{F}_l)$.

LEMMA 4.4: *Let H be a cyclic subgroup of* $\mathrm{GL}(2,\mathbb{F}_l)$. *Then H is conjugate to a subgroup of $T(2,\mathbb{F}_l)$ if and only if $|H|$ divides $(l-1)l$.*

Proof: Each $a=\left(\begin{smallmatrix}\alpha&\beta\\0&\gamma\end{smallmatrix}\right)\in T(2,\mathbb{F}_l)$ satisfies $a^{(l-1)l}=1$. So, the condition is necessary.

Suppose therefore that $|H|$ divides $(l-1)l$. Let h be a generator of H. Let α and α' be the eigenvalues of h. If $\alpha\in\mathbb{F}_l$, then $\beta\in\mathbb{F}_l$ and h is conjugate to an upper triangular matrix.

So, assume $\alpha\notin\mathbb{F}_l$. Then $\alpha\in\mathbb{F}_{l^2}$, α' is the conjugate of α over $\mathbb{F}_l$, and $\alpha\neq\alpha'$. It follows that h is conjugate in $\mathrm{GL}(2,\mathbb{F}_{l^2})$ to the diagonal matrix $\left(\begin{smallmatrix}\alpha&0\\0&\alpha'\end{smallmatrix}\right)$. Since $h^{(l-1)l}=1$, also $\alpha^{(l-1)l}=1$. But as the order of α divides l^2-1, it is relatively prime to l. Hence, $\alpha^{l-1}=1$ and therefore $\alpha\in\mathbb{F}_l$. This contradiction proves that H is conjugate to a subgroup of $T(2,\mathbb{F}_l)$. ∎

PROPOSITION 4.5: *Let E and E' be elliptic curves over a finite field K. Let Λ be a $\frac{3}{4}$-dense set of prime numbers. Suppose $K(E_l)=K(E'_l)$ for each $l\in\Lambda$. Then $E\sim_{\tilde{K}}E'$.*

Proof: Both $\mathrm{End}_{\tilde{K}}(E)$ and $\mathrm{End}_{\tilde{K}}(E')$ are finitely generated over $\mathbb{Z}$ [Sil1, p. 94, Cor. 7.5]. So, we may replace K by a finite extension, if necessary, to assume that all endomorphisms of both E and E' are defined over K.

If both E and E' are supersingular, then $E \sim_{\tilde{K}} E'$ (Lemma 4.3). So, assume for example E' is ordinary. Then $L' = \mathbb{Q} \otimes \mathrm{End}(E')$ is a quadratic field but $\mathbb{Q} \otimes \mathrm{End}(E)$ is either a quadratic field or a quaternion algebra. In each case choose a quadratic subfield L of $\mathbb{Q} \otimes \mathrm{End}(E)$.

Assume $E \not\sim_{\tilde{K}} E'$. By Lemma 4.3, $L \neq L'$. So, Lemma 4.1 gives an infinite subset Λ_0 of Λ such that each $l \in \Lambda_0$ is prime in L' but decomposes into two distinct primes in L.

Put $S = \mathrm{End}_{\tilde{K}}(E) \cap L$ and $S' = \mathrm{End}_{\tilde{K}}(E')$. Remove finitely many elements from Λ_0, if necessary, to assume that each $l \in \Lambda_0$ is relatively prime to the conductors of S and S' and that $l \neq \mathrm{char}(K)$.

We break up the rest of the proof into three parts and draw a contradiction.

Part A: *Constructions of isogenies of E.* Consider an $l \in \Lambda_0$. Let $lS = \mathfrak{l}\bar{\mathfrak{l}}$ be the decomposition of l into two distinct irreducible ideals of S. By Remark 4.2, $|\mathrm{Ker}(\mathfrak{l})|\mathbb{Z} = N\mathfrak{l} = l\mathbb{Z}$. Hence, $\mathrm{Ker}(\mathfrak{l})$ is a subgroup of $E(\tilde{K})$ of order l. Since the action of $\mathrm{Gal}(K)$ and $\mathrm{End}_{\tilde{K}}(E)$ commute, $\mathrm{Gal}(K)$ leaves $\mathrm{Ker}(\mathfrak{l})$ invariant. Hence, E has an isogeny λ with $\mathrm{Ker}(\lambda) = \mathrm{Ker}(\mathfrak{l})$ which is defined over K and has degree l. In particular, $\mathrm{Ker}(\lambda)$ is cyclic.

Choose a generator $\mathbf{p}$ of $\mathrm{Ker}(\lambda)$ and another point $\mathbf{q}$ of $E_l(\tilde{K})$ such that $\mathbf{p}, \mathbf{q}$ form a basis for $E_l(\tilde{K})$ over $\mathbb{F}_l$. For each $\sigma \in \mathrm{Gal}(K)$ there exists $a \in \mathbb{F}_l$ such that $\sigma\mathbf{p} = a\mathbf{p}$. Hence, $\rho_{E,l}(\mathrm{Gal}(K))$ is a subgroup of $T(2, \mathbb{F}_l)$. As K is finite, $\rho_{E,l}(\mathrm{Gal}(K)) \cong \mathrm{Gal}(K(E_l)/K)$ is cyclic. Hence, by Lemma 4.4, $|\rho_{E,l}(\mathrm{Gal}(K))|$ divides $(l-1)l$.

Part B: *Cyclic isogenies of E'.* By assumption, $|\rho_{E',K}(\mathrm{Gal}(K))| = [K(E'_l) : K] = [K(E_l) : K] = |\rho_{E,l}(\mathrm{Gal}(K))|$. Hence, by Part A and since K is finite, $\rho_{E',l}(\mathrm{Gal}(K))$ is a cyclic subgroup of $\mathrm{GL}(2, \mathbb{F}_l)$ whose order divides $(l-1)l$. Hence, by Lemma 4.4, $\rho_{E',l}(\mathrm{Gal}(K))$ is conjugate to a subgroup of $T(2, \mathbb{F}_l)$. Thus, $E'_l(\tilde{K})$ has an $\mathbb{F}_l$-basis $\mathbf{p}', \mathbf{q}'$ such that $\mathrm{Gal}(K)$ leaves the subgroup that $\mathbf{p}'$ generates invariant. It follows that this subgroup is the kernel of a K-isogeny λ' of E' of degree l.

PART C: *Infinitely many non-isomorphic curves over K.* List the elements of Λ_0 as $l_1, l_2, l_3, \ldots$. For each i Part B gives a K-isogeny λ_i' of E' of degree l_i. For each positive integer n, $C_n = \sum_{i=1}^n \mathrm{Ker}(\lambda_i')$ is a cyclic subgroup of $E'(\tilde{K})$ of order $l_1 l_2 \cdots l_n$ which $\mathrm{Gal}(K)$ leaves invariant. Hence, $D^{(n)} = E'/C_n$ is an elliptic curve which is K-isogenous to E'. We prove that if $m < n$, then $D^{(m)} \ncong D^{(n)}$. This will give infinitely many elliptic curves over K which are mutually non isomorphic over $\tilde{K}$. Since K is finite, this will produce the desired contradiction.

Indeed, since $D^{(m)} \sim_K E'$, we have $\mathrm{End}_{\tilde{K}}(D^{(m)}) \otimes \mathbb{Q} = \mathrm{End}_{\tilde{K}}(E') \otimes \mathbb{Q} = L'$. Also, there is a K-isogeny μ: $D^{(m)} \to D^{(n)}$ of degree $d = l_{m+1} l_{m+2} \cdots l_n$. If $D^{(m)}$ were isomorphic to $D^{(n)}$ over $\tilde{K}$, then μ would be a $\tilde{K}$-endomorphism of $D^{(m)}$ and therefore would belong to L'. Hence, $d = \deg(\mu) = N_{L'/\mathbb{Q}}(\mu)$ (Remark 4.2). Then $\mu O_{L'}$ would decompose into prime ideals of $O_{L'}$ which lie over the prime numbers l_i, $i = m+1 \ldots, n$. But, by construction, $l_i O_{L'}$ is a prime ideal of $O_{L'}$ and $N_{L'/\mathbb{Q}}(l_i O_{L'}) = l_i^2 \mathbb{Z}$. It would follow that $l_i^2 | d$, $i = m+1, \ldots, n$, which is a contradiction. ∎

LEMMA 4.6: *Let E and E' be elliptic curves over a finite field K, Λ a set of prime numbers, $\varepsilon > 0$, and $c \geq 1$. Suppose for each $l \in \Lambda$*

$$[K(E_l, E_l') : K(E_l) \cap K(E_l')] \leq c.$$

Then there exists a Dirichlet set of prime numbers Λ_0 with $\delta(\Lambda_0) < \varepsilon$ and there exists a finite extension K' of K such that $K'(E_l) = K'(E_l')$ for each $l \in \Lambda \smallsetminus \Lambda_0$.

Proof: Let $N_l = K(E_l, E_l')$ and $M_l = K(E_l) \cap K(E_l')$. For each positive integer m let Λ_m be the set of all l such that $l \leq c$ or $l \equiv \pm 1 \mod q^m$ for some prime number $q \leq c$. By Dirichlet's theorem,

$$\delta(\Lambda_m) \leq \sum_{q \leq c} \frac{2}{(q-1)q^{m-1}} \longrightarrow 0, \quad \text{as} \quad m \to \infty.$$

Choose m large enough such that $\delta(\Lambda_m) < \varepsilon$ and let $\Lambda_0 = \Lambda_m$.

For each prime number $q \leq c$ let v_q be the normalized q-adic valuation of $\mathbb{Q}$. Let $k = \max\big(v_q([N_l : M_l]) \mid q \leq c,\ l \in \Lambda\big)$. Then let K' be the unique extension of K of degree $\prod_{q \leq c} q^{3m+k}$. Let $N_l' = K'(E_l, E_l')$ and $M_l' = M_l K'$.

Consider now $l \in \Lambda \smallsetminus \Lambda_0$ and a prime number $q \le c$. Then

$$[M_l' : M_l] = \frac{[K' : K]}{\gcd\bigl([M_l : K], [K' : K]\bigr)}. \tag{3}$$

Since $l \notin \Lambda_0$, we have $l > c \ge q$ and $l \not\equiv \pm 1 \mod q^m$. Therefore $v_q(l) = 0$ and $v_q(l \mp 1) \le m$. Since $[M_l : K] | [K(E_l) : K] | (l-1)^2 l(l+1)$ (Fact 2.1(d)), we have

$$v_q([M_l : K]) \le v_q\bigl((l-1)^2 l(l+1)\bigr) = 2v_q(l-1) + v_q(l+1) \le 3m. \tag{4}$$

Hence, by (3) and (4),

$$\begin{aligned} v_q\bigl([M_l' : M_l]\bigr) &= 3m + k - \min\Bigl(v_q\bigl([M_l : K]\bigr), 3m + k\Bigr) \\ &\ge 3m + k - v_q([M_l : K]) \ge k \ge v_q\bigl([N_l : M_l]\bigr). \end{aligned}$$

By assumption, each prime divisor of $[N_l : M_l]$ is at most c. It follows that $[N_l : M_l]$ divides $[M_l' : M_l]$. Hence, since $K(E_l)$ is a finite field, $N_l \subseteq M_l'$ and therefore $M_l' = N_l'$. Conclude: $K'(E_l) = K'(E_l')$, as desired. ▮

Theorem 4.7: *Let E and E' be elliptic curves over a finitely generated field K. Suppose j_E or $j_{E'}$ belong to a finite field. Let $c \ge 1$ and let Λ be a set of prime numbers such that $[K(E_l, E_l') : K(E_l) \cap K(E_l')] \le c$ for each $l \in \Lambda$. Further suppose there exists $\varepsilon > 0$ such that Λ is $(\frac{3}{4} + \varepsilon)$-dense. Then $E \sim_{\tilde{K}} E'$. In particular, this holds if $\delta(\Lambda) > \frac{3}{4}$.*

Proof: By Lemma 2.7, both j_E and $j_{E'}$ belong to a finite field. We may therefore assume that K is finite. Lemma 4.6 gives a subset Λ' of Λ and a finite extension K' of K such that Λ' is $\frac{3}{4}$-dense and $K'(E_l) = K'(E_l')$ for each $l \in \Lambda'$. Conclude from Proposition 4.5 that $E \sim_{\tilde{K}} E'$. ▮

Remark 4.8: On the impossibility to improve Theorem 4.7. We prove that, in contrast to the case where j_E does not belong to a finite field, the condition on Λ in Theorem 4.7 can not be weakened to "Λ is infinite".

For each prime number q let Λ_q (resp. Λ_q') be the set of all $l \ne q$ such that q is a primitive root modulo l (resp. and $l \equiv 1 \mod 4$). A well known conjecture of Artin says that Λ_q has positive density [Art, pp. viii-x]. Lenstra [Len, Thm. 8.3] proves under the generalized Riemann hypothesis that Λ_q' has positive density if $q \equiv 1 \mod 4$.

Heath-Brown [HBr, Cor. 2] proves that, with the exception of two prime numbers, each Λ_q is infinite. Ram Murty (private communication) informed the authors that Heath-Brown's proof can be adapted to prove that Λ'_q is infinite. In Example 4.10 below we use Murty's remark to find a finite field K, elliptic curves E and E' over K which are not $\tilde{K}$-isogenous, and an infinite set Λ of prime numbers such that $[K(E_l, E'_l) : K(E_l) \cap K(E'_l)]$ is bounded when l ranges on Λ.

We could also use Lenstra's result to prove the existence of K, E, E', and Λ as above. But this would depend on the truth of the generalized Riemann Hypothesis. ∎

Lemma 4.9: *Let $p \equiv 1 \mod 4$ be a prime number, Δ an infinite set of prime numbers each of which is congruent to 1 modulo 4, and n a positive integer. Then Δ has an infinite subset Λ and there exist positive integers $d_1, \ldots, d_n$ such that the following conditions hold:*

(4a) *$d_1, \ldots, d_n$ are square-free and mutually relatively prime.*

(4b) *$p \nmid d_1 \cdots d_n$ and $l \nmid d_1 \cdots d_n$ for all $l \in \Lambda$.*

(4c) *$\left(\frac{-d_i}{p}\right) = 1$ and $\left(\frac{-d_i}{l}\right) = 1$ for $i = 1, \ldots, n$ and each $l \in \Lambda$.*

Proof: Induction on n reduces the proof of the lemma to the case where $n = 1$. To prove this case let Π be the set of all prime numbers which do not belong to $\Delta \cup \{2, p\}$. Make Δ smaller, if necessary, to assume that Π is infinite. Choose distinct large elements q_1 and q_2 in Π. By assumption, $\left(\frac{-1}{l}\right) = 1$ for each $l \in \Delta$. Hence, for each $l \in \Delta$ we have $\left(\frac{-q_1}{l}\right) = 1$, or $\left(\frac{-q_2}{l}\right) = 1$, or $\left(\frac{-q_1 q_2}{l}\right) = 1$. One of the possibilities occurs infinitely often. In other words, there is c in $\{q_1, q_2, q_1 q_2\}$ and there is an infinite subset Δ_1 of Δ such that $\left(\frac{-c}{l}\right) = 1$ for each $l \in \Delta_1$.

Apply the same procedure to find a positive integer c' and an infinite subset Λ of Δ_1 with $p \nmid cc'$, $\gcd(c, c') = 1$, and $\left(\frac{-c'}{l}\right) = 1$ for each $l \in \Lambda$. If $\left(\frac{c}{p}\right) = 1$, let $d = c$. If $\left(\frac{c'}{p}\right) = 1$, let $d = c'$. If $\left(\frac{c}{p}\right) = -1$ and $\left(\frac{c'}{p}\right) = -1$, let $d = cc'$. Now use that $p \equiv 1 \mod 4$ and $l \equiv 1 \mod 4$ for each $l \in \Lambda$ to conclude that $\left(\frac{-d}{p}\right) = 1$ and $\left(\frac{-d}{l}\right) = 1$ for each $l \in \Lambda$. ∎

Example 4.10: *Use Remark 4.8 to choose a prime number $p \equiv 1 \mod 4$ for which* *the set of all $l \equiv 1 \mod 4$ such that p is a primitive root modulo l is infinite. Denote this set by Δ. Let Λ be the infinite subset and d_1, d_2 positive integers which satisfy Condition 4 with $n = 2$. Then $\mathbb{F}_p$ has a finite extension $\bar{K}$, there exist ordinary elliptic curves $\bar{E}$ and $\bar{E}'$ over $\bar{K}$ which are not $\tilde{\mathbb{F}}_p$-isogenous, and there exists $c > 0$ such that $[\bar{K}(\bar{E}_l, \bar{E}'_l) : \bar{K}(\bar{E}_l) \cap \bar{K}(\bar{E}'_l)] \leq c$ for each $l \in \Lambda$.*

Proof: Choose elliptic curves E and E' over $\tilde{\mathbb{Q}}$ such that $\mathrm{End}(E)$ is isomorphic to the ring of integers of $\mathbb{Q}(\sqrt{-d_1})$ and $\mathrm{End}(E')$ is isomorphic to the ring of integers of $\mathbb{Q}(\sqrt{-d_2})$ [Sil2, p. 99]. By Serre-Tate we may choose a finite Galois extension K of $\mathbb{Q}$ which contains $\mathbb{Q}(\sqrt{-d_1}, \sqrt{-d_2})$ such that both E and E' have good reduction at each prime divisor $\mathfrak{p}$ of K which lies over p [Sil2, p. 149].

Choose such a $\mathfrak{p}$ and denote reduction modulo $\mathfrak{p}$ by a bar. In particular, $\bar{E}$ and $\bar{E}'$ are elliptic curves over $\bar{K}$. The latter is a finite extension of $\mathbb{F}_p$. By (4c), p decomposes in $\mathbb{Q}(\sqrt{-d_1})$ into two distinct primes. Hence, by [Lan2, p. 182, Thm. 12], $\mathrm{End}(\bar{E}) = \mathrm{End}(E)$. In particular, $\bar{E}$ is ordinary [Lan2, p. 177, Thm. 7]. Similarly, $\bar{E}'$ is an ordinary elliptic curve over $\bar{K}$ and $\mathrm{End}(\bar{E}') \cong \mathrm{End}(E')$. In particular, $\mathrm{End}(\bar{E}) \otimes \mathbb{Q}$ and $\mathrm{End}(\bar{E}') \otimes \mathbb{Q}$ are distinct imaginary quadratic extensions of $\mathbb{Q}$. Hence, $\bar{E} \not\sim_{\tilde{\mathbb{F}}_p} \bar{E}'$.

By (4c), for each $l \in \Lambda$, $\mathrm{Gal}(K(E_l)/K)$ is isomorphic to a subgroup of $\mathbb{Z}/(l-1)\mathbb{Z} \oplus \mathbb{Z}/(l-1)\mathbb{Z}$ [GeJ, p. 276, (3) and (4)]. By good reduction, $\mathrm{Gal}(\bar{K}(\bar{E}_l)/\bar{K})$ is isomorphic to a subgroup of $\mathrm{Gal}(K(E_l)/K)$. On the other hand $\mathrm{Gal}(\bar{K}(\bar{E}_l)/\bar{K})$ is cyclic. Hence, $\bar{K}(\bar{E}_l)$ is contained in the unique extension $\bar{K}_{l-1}$ of $\bar{K}$ of degree $l-1$. In addition, $\bar{K}(\zeta_l) \subseteq \bar{K}(\bar{E}_l)$. Similarly, $\bar{K}(\zeta_l) \subseteq \bar{K}(\bar{E}'_l) \subseteq \bar{K}_{l-1}$. Since $\mathrm{ord}_l p = l-1$, we have $[\mathbb{F}_p(\zeta_l) : \mathbb{F}_p] = l-1$. Hence,

$$[\bar{K}(\bar{E}_l, \bar{E}'_l) : K(\bar{E}_l) \cap K(\bar{E}'_l)] \leq [\bar{K}_{l-1} : \bar{K}(\zeta_l)] = \frac{l-1}{[\bar{K}(\zeta_l) : \bar{K}]} = \frac{[\mathbb{F}_p(\zeta_l) : \mathbb{F}_p]}{[\bar{K}(\zeta_l) : \bar{K}]} \leq [\bar{K} : \mathbb{F}_p].$$

This completes the proof of our claim. ∎

PROBLEM 4.11: *Do there exist a finite field K, elliptic curves E and E' over K which are not $\tilde{K}$-isogenous, a constant c, and a set of prime numbers Λ with positive Dirichlet density such that $[K(E_l, E'_l) : K(E_l) \cap K(E'_l)] \leq c$ for each $l \in \Lambda$?*

References

[Art] E. Artin, *Collected Papers,* Addision Wesely, Reading, 1965.

[BoS] Z. I. Borevich and I. R. Shafarevich, *Number Theory,* Academic Press, New York, 1966.

[CaF] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory,* Academic Press, London, 1967.

[Deu] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **14** (1941), 197–272.

[Die] J. Dieudonné, *La géométrie des groupes classiques,* Ergebnisse der Mathematik und ihrer Grenzgebiete, neue Folge **5**, Springer 1963.

[FaW] G. Faltings and G. Wüstholz et al., *Rational Points,* Seminar Bonn/Wuppertal 1983/84, Vieweg, Braunschweig, 1984.

[FrJ] M.D. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986.

[GeJ] W.-D. Geyer and M. Jarden, *Torsion points of elliptic curves over large algebraic extensions of finitely generated fields,* Israel Journal of Mathematics **31** (1978), 157–197.

[HBr] D. R. Heath-Brown, *Artin's conjecture for primitive roots,* Quarterly Journal of Mathematics, Oxford (2) **37** (1986), 27–38.

[Hup] B. Huppert, *Endliche Gruppen I,* Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen **134**, Springer, Berlin, 1967.

[Igu] J. I. Igusa, *Fibre systems of Jacobian varieties (III. Fibre systems of elliptic curves),* American Journal of Mathematics **81** (1959), 454–475.

[Jan] G.J. Janusz, *Algebraic Number Fields,* Academic Press, New York, 1973.

[Lan1] S. Lang, *Algebraic Number Theory,* Addison-Wesley, Reading, 1970.

[Lan2] S. Lang, *Elliptic Functions,* Addison-Wesley, Reading, 1973.

[Len] H. W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields,* Inventiones mathematicae **42** (1977), 201-224.

[MoB] L. Moret-Bailly, *Pinceaux de variétés abéliennes,* Astérisque **129** (1985).

[Mum] D. Mumford, *Abelian Varieties,* Oxford University Press, London, 1974.

[Shi] G. Shimura, *Introduction to the Aritmetic Theory of Automorphic Functions,* Iwanami Shoten, Publishers and Princeton University Press, 1971.

[Ser] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques,* Inventiones mathematicae **15** (1972), 259–331.

[Sil1] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Graduate texts in Mathematics **106**, Springer, New York, 1986.

[Sil2] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves,* Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994.

[Tat] J. Tate, *Endomorphisms of Abelian varieties over finite fields,* Inventiones mathematicae **2** (1966), 134–144.

[Wei] A. Weil, *Basic Number Theory,* Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen **144**, Springer-Verlag, Berlin, 1967.

[Zar1] Y. G. Zarhin, *Endomorphisms of abelian varieties and points of finite order in characteristic p,* Mathemtical Notes **21** (1977), 415–419.

[Zar2] Y. G. Zarhin, *A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction,* Inventiones mathematicae **79** (1985), 309–321.