A mod $p$ variant of the André–Oort conjecture

Bas Edixhoven$^1$ · Rodolphe Richard$^1$

Received: 3 October 2018 / Accepted: 29 November 2018
© The Author(s) 2018

Abstract
We state and prove a variant of the André–Oort conjecture for the product of 2 modular curves in positive characteristic, assuming GRH for quadratic fields.

Keywords
Elliptic curves · Complex multiplication · Positive characteristic

Mathematics Subject Classification 11G15 · 14G35 · 14K22

1 Introduction

The André–Oort conjecture says that, for $\Sigma$ any set of special points in a Shimura variety $S$, the irreducible components of the Zariski closure of $\Sigma$ are special subvarieties. See [8,15] for the current state of affairs around this conjecture. In the simplest non-trivial case of this conjecture the Shimura variety $S$ is $\mathbb{C}^2$, the product of two copies of the $j$-line, hence the coarse moduli space for pairs of complex elliptic curves. The irreducible special curves in $\mathbb{C}^2$ are, apart from the fibres of the two projections, the images of the modular curves $Y_0(n)$ ($n \geq 1$), and consist of the pairs $(j(E), j(E/\langle P \rangle))$ with $E$ a complex elliptic curve and $P \in E$ of order $n$. In this case, the conjecture was proved in [1], and, conditionally on the generalised Riemann hypothesis (GRH) for quadratic fields, in [4]. In this article we state a variant in positive characteristic, and prove it under GRH for quadratic fields.

Definition 1.1 For a point $x$ in a scheme $X$ we let $\kappa(x) = \mathcal{O}_{X,x}/m_x$ be its residue field, and we denote $\iota_x : \text{Spec}(\kappa(x)) \to X$ the induced $\kappa(x)$-point of $X$. So we may view $\iota_x$ as an element of $X(\kappa(x))$, the set of $\kappa(x)$-valued points of $X$. For $X = \mathbb{A}^2$, we have $X(\kappa(x)) = \kappa(x)^2$.

By CM-point in $\mathbb{A}^2_{\mathbb{Q}}$ we mean a closed point $s$ of the affine plane over $\mathbb{Q}$, such that both coordinates of $\iota_s \in \kappa(s)^2$ are $j$-invariants of CM elliptic curves.

By CM-point in $\mathbb{A}^2_{\mathbb{Z}}$ we mean the closure in $\mathbb{A}^2_{\mathbb{Z}}$ of a CM-point in $\mathbb{A}^2_{\mathbb{Q}}$. We view such a CM-point $[s]$ as a closed subset, or as a reduced closed subscheme. For any prime number $p$ we then denote by $[s]_{\mathbb{F}_p}$ the reduced fibre over $p$ and call it the reduction of $s$ at $p$.

$^1$ Universiteit Leiden, Leiden, The Netherlands

Published online: 17 December 2018
Theorem 1.2 Assume the generalised Riemann hypothesis for quadratic fields. Let $p$ be a prime number. Let $\Sigma$ be a set of finite closed subsets $s$ of $\mathbb{A}^1_{\mathbb{Z}}$ that are reductions of CM-points in $\mathbb{A}^2_{\mathbb{F}_p}$. Let $Z$ be the Zariski closure of the union of all $s$ in $\Sigma$. Then every irreducible component of dimension 1 of $Z$ is special: a fibre of one of the 2 projections, or an irreducible component of the image in $\mathbb{A}^2_{\mathbb{F}_p}$ of some $Y_0(n)_{\mathbb{F}_p}$ with $n \in \mathbb{Z}_{\geq 1}$.

Remark 1.3 If $K_1, \ldots, K_r$ are quadratic subfields of $\mathbb{Q}$, then GRH holds for their compositum $K$ if and only if it holds for each quadratic subfield of $K$ (the zeta function of $K$ is the product of the Riemann zeta-function and the $L$-functions of the quadratic subfields of $K$).

2 Some facts on CM elliptic curves

We will need some results on CM elliptic curves and their reduction mod $p$. For more detail see [4, Sect. 2], and references therein.

For $E$ over $\overline{\mathbb{Q}}$ an elliptic curve with CM, $\text{End}(E)$ is an order in an imaginary quadratic field $K$, hence isomorphic to $\mathcal{O}_K, f = \mathbb{Z} + f \mathcal{O}_K$, with $\mathcal{O}_K$ the ring of integers in $K$, and $f \in \mathbb{Z}_{\geq 1}$, unique, called the conductor.

For $K \subset \overline{\mathbb{Q}}$ imaginary quadratic and $f \geq 1$, we let $S_{K, f}$ be the set of isomorphism classes of $(E, \alpha)$, where $E$ is an elliptic curve over $\overline{\mathbb{Q}}$ and $\alpha: \mathcal{O}_K, f \rightarrow \text{End}(E)$ is an isomorphism, such that the action of $\text{End}(E)$ on the tangent space of $E$ at 0 induces the given embedding $K \rightarrow \overline{\mathbb{Q}}$. The group $\text{Pic}(\mathcal{O}_K, f)$ acts on $S_{K, f}$, making it a torsor. This action commutes with the action of $G_K := \text{Gal}(\overline{\mathbb{Q}}/K)$, giving a group morphism $G_K \rightarrow \text{Pic}(\mathcal{O}_K, f)$ through which $G_K$ acts on $S_{K, f}$.

This map is surjective, unramified outside $f$, and the Frobenius element at a maximal ideal $m$ of $\mathcal{O}_K$ outside $f$ is the class $[m^{-1}]$ in $\text{Pic}(\mathcal{O}_K, f)$.

For $f' \geq 1$ dividing $f$, the inclusion $\mathcal{O}_K, f \rightarrow \mathcal{O}_K, f'$ induces compatible surjective maps of groups $\text{Pic}(\mathcal{O}_K, f) \rightarrow \text{Pic}(\mathcal{O}_K, f')$ and of torsors $S_{K, f} \rightarrow S_{K, f'}$: $(E, \alpha)$ is mapped to $O_{K, f'} \otimes_{\mathcal{O}_K, f} E$ with its $O_{K, f'}$-action. In terms of complex lattices: $O_{K, f'} \otimes_{\mathcal{O}_K, f} \mathbb{C}/\Lambda = \mathbb{C}/O_{K, f'} \Lambda$.

For $p$ a prime number, and $f'$ the prime to $p$ part of $f$, the map $S_{K, f} \rightarrow S_{K, f'}$ is the quotient by the inertia subgroup at any of the maximal ideals $m$ of $\mathcal{O}_K$ containing $p$ (to show this, use the adelic description of ramification in class field theory).

Elliptic curves with CM over $\overline{\mathbb{Q}}$ extend uniquely over $\overline{\mathbb{Z}}$ (the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$), and their endomorphisms as well.

For $K$ and $f$ as above we define $j_{K, f}$ to be the image of $j(E): \text{Spec}(\overline{\mathbb{Z}}) \rightarrow \mathbb{A}^1_{\overline{\mathbb{Q}}}$, where $E$ is an elliptic curve over $\overline{\mathbb{Q}}$ with $\text{End}(E)$ isomorphic to $O_{K, f}$; this does not depend on the choice of $E$. Then $j_{K, f}$ is an irreducible closed subset of $\mathbb{A}^1_{\overline{\mathbb{Z}}}$. We equip it with its reduced induced scheme structure. Then it is finite over $\mathbb{Z}$ of degree $\#\text{Pic}(\mathcal{O}_K, f)$, and in fact $j_{K, f}(\overline{\mathbb{Z}})$ is in bijection with $S_{K, f}$ and hence is a $\text{Pic}(\mathcal{O}_K, f)$-torsor (here we use that $K$ has a given embedding into $\overline{\mathbb{Q}}$). For $p$ prime, we let $j_{K, f, \mathbb{F}_p}$ be the fibre of $j_{K, f}$ over $\mathbb{F}_p$.

Let $p$ be a prime number, and $K$ and $f$ as above. If $p$ is not split in $\mathcal{O}_K$ then $j_{K, f, \mathbb{F}_p}$ consists of supersingular points, and $j_{K, f}$ can be highly singular above $p$ (by lack of supersingular targets). If $p$ is split in $\mathcal{O}_K$ then $j_{K, f, \mathbb{F}_p}$ consists of ordinary points, and the corresponding elliptic curves over $\mathbb{F}_p$ have endomorphism ring isomorphic to $O_{K, f'}$, where $f'$ is the prime to $p$ part of $f$, and then $j_{K, f', \mathbb{F}_p} = (j_{K, f, \mathbb{F}_p})_{\text{red}}$, and for each morphism of rings $\overline{\mathbb{Z}} \rightarrow \mathbb{F}_p$ the map $j_{K, f'}(\overline{\mathbb{Z}}) \rightarrow j_{K, f'}(\mathbb{F}_p)$ is a bijection and it makes $j_{K, f', \mathbb{F}_p}(\mathbb{F}_p)$ into a $\text{Pic}(O_{K, f'})$-torsor. Note that every ordinary point $x$ in $\mathbb{F}_p$ belongs to exactly one $j_{K, f'}(\mathbb{F}_p)$.
3 Some facts about pairs of CM elliptic curves

Let \( s \) be a CM-point in \( \mathbb{A}^2_\mathbb{Q} \) as in Definition 1.1. Then \( s(\mathbb{Q}) \) is a \( G_\mathbb{Q} \)-orbit. Let \( (x_1, x_2) \) be in \( s(\mathbb{Q}) \). Then \( x_1 \) is in \( j_{K_1, f_1}(\mathbb{Q}) \) for a unique imaginary quadratic subfield \( K_1 \) of \( \mathbb{Q} \), and similarly for \( x_2 \), and \( G_{K_1, K_2} \) acts through \( \text{Pic}(O_{K_1, f_1}) \times \text{Pic}(O_{K_2, f_2}) \), and \( s(\mathbb{Q}) \) decomposes into at most 4 orbits under \( G_{K_1, K_2} \).

Let \( p \) be a prime. Let \( s \) be a finite closed subset of \( \mathbb{A}^2_{\mathbb{F}_p} \) that is the reduction at \( p \) of a CM-point in \( \mathbb{A}^2_\mathbb{Z} \) (see Definition 1.1). Then \( s(\mathbb{F}_p) \) is a finite subset of \( \mathbb{F}_p \times \mathbb{F}_p \) that is stable under \( G_{\mathbb{F}_p} := \text{Gal}(\mathbb{F}_p/\mathbb{F}_p) \). For each of the 2 projections, the image of \( s(\mathbb{F}_p) \) consists entirely of ordinary points or entirely of supersingular points (this follows from the facts recalled in Sect. 2). If for all \( (x_1, x_2) \) in \( s(\mathbb{F}_p) \) both \( x_1 \) and \( x_2 \) are ordinary, then the \( x_1 \) form a \( \text{Pic}(O_{K_1, f_1}) \)-orbit, and the \( x_2 \) form a \( \text{Pic}(O_{K_2, f_2}) \)-orbit, with \( f_1 \) and \( f_2 \) prime to \( p \).

4 Images under suitable Hecke correspondences

For \( \ell \) a prime number, \( T_\ell \) denotes the correspondence on the \( j \)-line, over any field not of characteristic \( \ell \), sending an elliptic curve \( E \) over an algebraically closed field \( k \) to the sum of its \( \ell + 1 \) quotients by the subgroups of \( E(k) \) of order \( \ell \). Similarly, \( T_\ell \times T_\ell \) is the correspondence on the \( j \)-line times itself that sends a pair of elliptic curves \( (E_1, E_2) \) to the sum of all \( (E_1/C_1, E_2/C_2) \) with \( C_1 \) and \( C_2 \) subgroups of order \( \ell \).

**Theorem 4.1** Assumptions as in Theorem 1.2, and assume that all irreducible components of \( Z \) are of dimension 1, and are not a fibre of any of the \( 2 \) projections. There are infinitely many prime numbers \( \ell \) such that \( Z \cap (T_\ell \times T_\ell)Z \) is of dimension 1.

**Proof** There are only finitely many points \( (x_1, x_2) \) in \( Z(\mathbb{F}_p) \) such that \( x_1 \) or \( x_2 \) is not ordinary. Therefore we can replace \( \Sigma \) by its subset of \( s \)’s whose images under both projections are ordinary.

At this point we combine the arguments of [5] with reduction modulo \( p \). Let \( d_1 \) and \( d_2 \) be the degrees of the projections from \( Z \) to \( \mathbb{A}^2_{\mathbb{F}_p} \).

For \( s \) in \( \Sigma \) and \( (x_1, x_2) \) in \( s(\mathbb{F}_p) \), let \( O_{1,s} \) and \( O_{2,s} \) be the endomorphism rings of the elliptic curves \( E_1 \) and \( E_2 \) over \( \mathbb{F}_p \) corresponding to \( x_1 \) and \( x_2 \).

We claim that for all but finitely many \( s \) there is a prime number \( \ell \) such that \( \ell \) is split in both \( O_{1,s} \) and \( O_{2,s} \), and \( \#s(\mathbb{F}_p) > 2d_1d_2(\ell + 1)^2 \), and \( \ell > \log(\#s(\mathbb{F}_p)) \). This claim follows, as in the proof of [5, Lemma 7.1], from the (conditional) effective Chebotarev theorem of Lagarias and Odlyzko [9] as stated in Theorem 4 of [12], and Siegel’s theorem on class numbers of imaginary quadratic fields [14] and [10, Chap. XVI].

Now let \( s \), \( (x_1, x_2) \) and \( \ell \) be as in the claim above. Let \( \varphi : \overline{\mathbb{Z}} \to \overline{\mathbb{F}_p} \) be a morphism of rings. Then there are unique embeddings of \( O_{1,s} \) and \( O_{2,s} \) into \( \overline{\mathbb{Z}} \) that composed with \( \varphi \) give the actions on the tangent spaces at 0 of \( E_1 \) and \( E_2 \). Let \( m \) be a maximal ideal of index \( \ell \) in \( O_{1,s}O_{2,s} \subseteq \overline{\mathbb{Z}} \), and \( m_1 \) and \( m_2 \) the intersections of \( m \) with \( O_{1,s} \) and \( O_{2,s} \). By the facts recalled at the end of Sect. 2, there are canonical \( \tilde{x}_1 \) and \( \tilde{x}_2 \) in \( \overline{\mathbb{Z}} \) lifting \( E_1 \) and \( E_2 \) to \( \tilde{E}_1 \) and \( \tilde{E}_2 \), with \( \text{End}(\tilde{E}_1) = \text{End}(E_1) \) and \( \text{End}(\tilde{E}_2) = \text{End}(E_2) \). Let \( \sigma \) be a Frobenius element in \( G_{K_1, K_2} \) at \( m \). Then \( \tilde{E}_1 = [m_1]^{-1}[m_1]\tilde{E}_1 \) shows that \( \tilde{E}_1 \) is \( \ell \)-isogenous to \( [m_1]\tilde{E}_1 \) which is the conjugate of \( \tilde{E}_1 \) by \( \sigma^{-1} \), and similarly for \( \tilde{E}_2 \). Then \( ([m_1]E_1, [m_2]E_2) \) is the reduction of \( \sigma^{-1}(\tilde{E}_1, \tilde{E}_2) \), hence in \( s(\mathbb{F}_p) \). So \( (x_1, x_2) \) is in \( (T_\ell \times T_\ell)([m_1]E_1, [m_2]E_2) \). So \( (x_1, x_2) \) is both in \( s(\mathbb{F}_p) \) and in \( (T_\ell \times T_\ell)(s(\mathbb{F}_p)) \). We conclude that \( s(\mathbb{F}_p) \) is contained in \( Z(\mathbb{F}_p) \cap (T_\ell \times T_\ell)Z(\mathbb{F}_p) \).
Now the degrees of the projections from \((T_\ell \times T_\ell)Z\) to \(\mathbb{A}^1_p\), are \((\ell + 1)^2d_1\) and \((\ell + 1)^2d_2\), so the intersection number (in \((\mathbb{P}^1 \times \mathbb{P}^1)_\ell\)) of \(Z\) and \((T_\ell \times T_\ell)\) is \(2d_1d_2(\ell + 1)^2\). But the intersection contains \(s(\mathbb{P}^1_\ell)\), which has more points than this intersection number, so the intersection is not of dimension 0.

\[\square\]

5 Goursat’s lemma and Zarhin’s theorem

Here we deviate from the topological approach in [4,5].

**Theorem 5.1** Let \(C\) be an irreducible reduced closed curve in \(\mathbb{A}^2_p\), not a fibre of one of the 2 projections, such that there are infinitely many prime numbers \(\ell\) for which \((T_\ell \times T_\ell)(C)\) is reducible. Then there is an \(n \in \mathbb{Z}_{\geq 0}\) such that \(C\) is the image of an irreducible component of \(Y_0(n)_{\mathbb{P}^1_p}\) in \(\mathbb{A}^2_p\).

**Proof** Let \(K\) denote the function field of \(C\), and let \(E_1\) and \(E_2\) be elliptic curves over \(K\) with \(j\)-invariants the projections \(\pi_1\) and \(\pi_2\), viewed as functions on \(C\); these \(E_1\) and \(E_2\) are unique up to quadratic twist. We must prove that \(E_1\) is isogeneous to a twist of \(E_2\).

Let \(K \to K_{\text{sep}}\) be a separable closure and let \(G := \text{Gal}(K_{\text{sep}}/K)\). For \(\ell \neq p\) a prime number, let \(V_{\ell, 1} := E_1(K_{\text{sep}})[\ell]\) and \(V_{\ell, 2} := E_2(K_{\text{sep}})[\ell]\) and let \(G_\ell\) be the image of \(G\) in \(GL(V_{\ell, 1}) \times GL(V_{\ell, 2})\), with projections \(G_{\ell, 1}\) and \(G_{\ell, 2}\). Because of the Weil pairing, \(G\) acts on \(\text{det}(V_{\ell, 1})\) and \(\text{det}(V_{\ell, 2})\) by the cyclotomic character \(\chi_\ell:\ G \to [\mathbb{F}_\ell^\times = \text{Aut}(\mu_\ell(K_{\text{sep}}))].\)

For all but finitely many \(\ell\), \(G_{\ell, 1}\) contains \(\text{SL}(V_{\ell, 1})\) and similarly for \(E_2\) (this follows, as in [2], from the fact that for \(n\) prime to \(p\) the geometric fibres of the modular curve over \(\mathbb{Z}[\zeta_n, 1/n]\) parametrising elliptic curves with symplectic basis of the \(n\)-torsion are irreducible [6, Theorem 3] and [7, Corollary 10.9.2]). Let \(q\) be the number of elements of the algebraic closure of \(\mathbb{F}_p\) in \(K\). Then, for all but finitely many \(\ell\), \(G_{\ell, 1}\) is the subgroup of elements of \(\text{SL}(V_{\ell, 1})\), whose determinant is a power of \(q\), and similarly for \(G_{\ell, 2}\). Let \(L\) be the set of prime numbers \(\ell \neq 2\) for which \(G_{\ell, 1}\) and \(G_{\ell, 2}\) are as in the previous sentence, and such that \((T_\ell \times T_\ell)(C)\) is reducible. Then \(L\) is infinite.

Let \(\ell\) be in \(L\). Let \(N_{\ell, 1} := \ker(G_\ell \to G_{\ell, 2})\) and \(N_{\ell, 2} := \ker(G_\ell \to G_{\ell, 1})\). Then \(N_{\ell, i}\) is a normal subgroup of \(G_{\ell, i} \cap \text{SL}(V_{\ell, i})\), and \(G_\ell\) is the inverse image of the graph of an isomorphism \(G_{\ell, 1}/N_{\ell, 1} \to G_{\ell, 2}/N_{\ell, 2}\). The only normal subgroups of \(\text{SL}(\mathbb{F}_\ell)\) are the trivial subgroups and the center \([\pm 1]\), with different number of elements. As \#\(G_{\ell, 1}\) = \#\(G_{\ell, 2}\), we have \#\(N_{\ell, 1}\) = \#\(N_{\ell, 2}\), and so there are 3 cases.

If \(N_{\ell, 1} = \text{SL}(V_{\ell, 1})\), then \(G_\ell\) contains \(\text{SL}(V_{\ell, 1}) \times \text{SL}(V_{\ell, 2})\), contradicting the reducibility of \((T_\ell \times T_\ell)(C)\). Hence \(N_{\ell, 1}\) is \([\pm 1]\) or \([1]\), and \(G_\ell\) gives us an isomorphism \(\varphi_\ell: G_{\ell, 1}/[\pm 1] \to G_{\ell, 2}/[\pm 1]\). As all automorphisms of \(\text{SL}(\mathbb{F}_\ell)/[\pm 1]\) are induced by \(\text{GL}(\mathbb{F}_\ell)\) ([11]), or [16, Sect. 3.3.4]), there is an isomorphism \(\gamma: V_{\ell, 1} \to V_{\ell, 2}\) of \(\mathbb{F}_\ell\)-vector spaces (not necessarily \(G\)-equivariant) that induces the restriction \(\varphi_\ell\) from \(\text{SL}(V_{\ell, 1})/[\pm 1]\) to \(\text{SL}(V_{\ell, 2})/[\pm 1]\). Let \(\alpha_\ell\) be the automorphism of \(G_{\ell, 1}/[\pm 1]\) obtained as the composition of first \(\varphi_\ell\), and then \(G_{\ell, 2}/[\pm 1] \to G_{\ell, 1}/[\pm 1]\), \(g \mapsto \gamma^{-1}g\gamma\). Consider the short exact sequence

\[\{1\} \to \text{SL}(V_{\ell, 1})/[\pm 1] \to G_{\ell, 1}/[\pm 1] \to \langle g \rangle \to \{1\}.\]

Then \(\alpha_\ell\) induces the identity on \(\text{SL}(V_{\ell, 1})/[\pm 1]\) and on \(\langle g \rangle\). Lemma 5.3 gives us that \(\alpha_\ell\) is the identity. Hence \(\varphi_\ell\) is the morphism \(G_{\ell, 1}/[\pm 1] \to G_{\ell, 2}/[\pm 1]\), \(g \mapsto \gamma g \gamma^{-1}\). If \(N_{\ell, 1} = \{1\}\) then \(G_\ell\) is \(G_{\ell, 1}/[\pm 1] \to G_{\ell, 2}/[\pm 1]\), \(g \mapsto \gamma g \gamma^{-1}\). If \(N_{\ell, 1} = \{\pm 1\}\) then \(G_\ell\) is \(G_{\ell, 1}/\gamma : \{(\pm g \gamma) \gamma^{-1} : g \in G_{\ell, 1}\}\). This means that \(\gamma : V_{\ell, 1}/[\pm 1] \to V_{\ell, 2}/[\pm 1]\) is \(G\)-equivariant. Even better, writing, for \(g\) in \(G\), \(\gamma(gv) = \varepsilon_\ell(g)g(\gamma(v))\) with \(\varepsilon_\ell(g) \in \{\pm 1\}\),
Let $U \subset C$ be the open subscheme where $C$ is regular and where $E_1$ and $E_2$ have good reduction. Then for all $\ell$ in $L$, and all closed $x$ in $U$, $\varepsilon_\ell$ is unramified at $x$. As $U$ is a smooth curve over a finite field, there are only finitely many characters $\varepsilon : G \to \{ \pm 1 \}$ unramified on $U$, if $p \neq 2$ (this uses Kummer theory). For $p = 2$, one has to be more careful; we argue as follows. There are infinitely many characters $\varepsilon : G \to \{ \pm 1 \}$ unramified on $U$, but only finitely many with bounded conductor on the projective smooth curve $C$ with function field $K$. Let $K' \subset K^{\text{sep}}$ be the extension cut out by $V_{3,1} \times V_{3,2}$, and let $\overline{C}' \to \overline{C}$ be the corresponding cover. Then both $E_1$ and $E_2$ have semistable reduction over $\overline{C}'$ by [3, Corollary 5.18]. The Galois criterion for semi-stability in [13, Example IX, Proposition 3.5] tells us that all $\varepsilon_\ell$ become unramified on $\overline{C}'$. This shows that also for $p = 2$ there are only finitely many distinct $\varepsilon_\ell$. The conclusion is that, for general $p$, there are only finitely many distinct $\varepsilon_\ell$, and therefore we can assume (by shrinking $L$ to an infinite subset) that they are all equal to some $\varepsilon$. Then we replace $E_2$ by its twist by $\varepsilon$, and then $\varepsilon_\ell$ are trivial.

Now Zarhin’s result [17, Corollary 2.7] tells us that there is a non-zero morphism $\alpha : E_1 \to E_2$. \hfill $\square$

**Remark 5.2** Up to sign, there is a unique isogeny $\alpha : E_1 \to E_2$ of minimal degree $n$. Then $C$ is an irreducible component of the image of $Y_0(n)_{\mathbb{F}_p}$. We write $n = p^k m$ with $m$ prime to $p$. Then $C$ is the image of the image of $Y_0(m)_{\mathbb{F}_p}$ by the $p^k$-Frobenius map on the first or on the second coordinate, and $C$ is also an irreducible component of the images of all $Y_0(p^{2l} n)$ with $i \in \mathbb{Z}_{\geq 0}$.

**Lemma 5.3** Let $G$ be a group, $N$ a normal subgroup of $G$ and $Q$ the quotient. Let $\alpha$ be an automorphism of $G$ inducing the identity on $N$ and on $Q$, and suppose that $G$ acts trivially by conjugation on the center of $N$, and that there is no non-trivial morphism from $Q$ to the center of $N$. Then $\alpha$ is the identity on $G$.

**Proof** We write, for all $g \in G$:

$$\alpha(g) = g \beta(g), \quad \text{with } \beta \text{ a map (of sets!) from } G \text{ to itself.}$$

As $\alpha$ induces the identity on $Q$, $\beta$ takes values in $N$. As $\alpha$ is the identity on $N$, we have $\beta(n) = 1$ for all $n \in N$. For all $g_1$ and $g_2$ in $G$ we have:

$$g_1 g_2 \beta(g_1 g_2) = \alpha(g_1 g_2) = \alpha(g_1) \alpha(g_2) = g_1 \beta(g_1) g_2 \beta(g_2),$$

and therefore

$$\beta(g_1 g_2) = g_2^{-1} \beta(g_1) g_2 \beta(g_2).$$

For $g_1$ in $N$, this gives that for all $g_2$ in $G$, $\beta(g_1 g_2) = \beta(g_2)$. Hence $\beta$ factors through $\overline{\beta} : Q \to N : \beta(g) = \overline{\beta}(g)$. Now, for $g_1$ in $G$ and $g_2$ in $N$, we have

$$\overline{\beta}(g_1) = \overline{\beta}(g_1 g_2) = g_2^{-1} \overline{\beta}(g_1) g_2.$$
6 Proof of the main theorem

We are now ready to prove Theorem 1.2.

If \( Z = \mathbb{A}^2_{\mathbb{F}_p} \) or is finite, then \( Z \) has no irreducible components of dimension 1. Now assume that \( Z \) has dimension 1. We write \( Z = V \cup H \cup F \cup Z' \) with \( V \) the union in \( Z \) of fibers of the 1st projection \( \text{pr}_1 \), \( H \) the union in \( Z \) of fibers of \( \text{pr}_2 \), and \( F \) the set of isolated points in \( Z \), and \( Z' \) the union of the remaining irreducible components of \( Z \). Let \( B_1 \) be the image of \( V \cup U \) under \( \text{pr}_1 \), and \( B_2 \) the image of \( H \cup U \) under \( \text{pr}_2 \).

Let \( s \) be in \( \Sigma \) such that \( \text{pr}_1(s) \) meets \( B_1 \). Then either \( \text{pr}_1(s) (\overline{\mathbb{F}_p}) \) consists of supersingular points, or it consists of ordinary points with the same endomorphism ring as an ordinary \((\text{pr}_1 \text{ and } \text{pr}_2 \text{, and the intersection of this union with } Z) \) point in \( Z \). Hence for such a \( \text{pr}_1(s) \) there are only finitely many possibilities. Similarly for the \( \text{pr}_2(s) \). It follows that the \( s \) in \( \Sigma \) such that \( \text{pr}_1(s) \) disjoint from \( B_1 \) and \( \text{pr}_2(s) \) disjoint from \( B_2 \) are contained in \( Z' \). Let \( \Sigma' \) be the set of these \( s \). The \( s \) in \( \Sigma - \Sigma' \) lie on a finite union of fibres of \( \text{pr}_1 \) and \( \text{pr}_2 \), and the intersection of this union with \( Z' \) is finite. Therefore the union of the \( s \) in \( \Sigma' \) is dense in \( Z' \). We replace \( Z \) by \( Z' \), and \( \Sigma \) by \( \Sigma' \). Then all irreducible components of \( Z \) are of dimension 1 and are not a fibre of \( \text{pr}_1 \) or \( \text{pr}_2 \). Let \( d_i \) \((i \in \{1, 2\})\) be the degree of \( \text{pr}_i \) restricted to \( Z \).

There are only finitely many points \((x_1, x_2)\) in \( Z(\overline{\mathbb{F}_p}) \) such that \( x_1 \) or \( x_2 \) is not ordinary. Therefore we can replace \( \Sigma \) by its subset of \( s \)'s whose image under both projections is ordinary.

Theorem 4.1 gives us an infinite set \( L \) of primes \( \ell \) such that \( Z \cap (T_\ell \times T_\ell) Z \) is of dimension 1. Let \((Z_i)_{i \in I}\) be the set of irreducible components of \( Z \). Then for each \( \ell \) in \( L \) there are \( i \) and \( j \) in \( I \) such that \( Z_i \) is in \( (T_\ell \times T_\ell) Z_j \). If moreover \( \ell > 12d_1 \) then \( (T_\ell \times T_\ell) Z_j \) is reducible, because if not, then \( (T_\ell \times T_\ell) Z_j \) equals \( Z_i \) (as closed subsets of \( \mathbb{A}^2_{\mathbb{F}_p} \)), but for any ordinary \((x, y)\) in \( Z_j(\overline{\mathbb{F}_p}) \), \( T_\ell(x, y) \) consists of at least \((\ell + 1)/12 > d_1 \) distinct points.

There is a \( j_0 \in I \) such that for infinitely many \( \ell \in L \), \( (T_\ell \times T_\ell) Z_{j_0} \) is reducible. Theorem 5.1 then tells us that there is an \( n \geq 1 \) such that \( Z_{j_0} \) is the image in \( \mathbb{A}^2_{\mathbb{F}_p} \) of an irreducible component of \( Y_0(n)_{\overline{\mathbb{F}_p}} \). We let \( T(n) \) be the reduced closed subscheme of \( \mathbb{A}^2_{\mathbb{F}_p} \) whose geometric points correspond to pairs \((E_1, E_2)\) of elliptic curves that admit a morphism \( \varphi : E_1 \to E_2 \) of degree \( n \). Let \( J \) be the set of \( j \in I \) such that \( Z_j \) is an irreducible component of \( T(n)_{\overline{\mathbb{F}_p}} \), let \( Z(n) \) be their union, and let \( Z' \) be the union of the \( Z_i \) with \( i \notin J \).

We claim that any \( s \) in \( \Sigma \) that meets \( T(n)_{\overline{\mathbb{F}_p}} \) is contained in \( T(n)_{\overline{\mathbb{F}_p}} \). So let \((j(E_1), j(E_2))\) be in \( s(\overline{\mathbb{F}_p}) \), and \( \varphi : E_1 \to E_2 \) be of degree \( n \). Let \( \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p} \) be a morphism of rings, and \( \tilde{\varphi} : \tilde{E}_1 \to \tilde{E}_2 \) the canonical lift over \( \overline{\mathbb{F}_p} \). Then \( \tilde{\varphi} \) is of degree \( n \), and so are all its conjugates by \( G_\mathbb{Q} \), and so \( s(\overline{\mathbb{F}_p}) \), consisting of all reductions of these conjugates, lies in \( T(n)(\overline{\mathbb{F}_p}) \).

As \( T(n)_{\overline{\mathbb{F}_p}} \cap Z' \) is finite, the set \( \Sigma' \) of \( s \) in \( \Sigma \) that do not meet \( T(n)_{\overline{\mathbb{F}_p}} \) is dense in \( Z' \) and our proof is finished by induction on the number of irreducible components of \( Z \).

Remark 6.1 We think that Theorem 1.2 remains true if \( E \subset \overline{\mathbb{Q}} \) is a finite extension of \( \mathbb{Q} \) and we work with \( \mathbb{A}^2_{\overline{\mathbb{Q}}} \) and consider reductions of \( G_E \)-orbits of CM-points in \( \mathbb{A}^2(\overline{\mathbb{Q}}) \). However, the case \( E = \mathbb{Q} \) has a special feature: up to fibres of the projections, the \( Z \) are invariant under switching the coordinates. This comes from the dihedral nature of the Galois action. As soon as \( E \) contains an imaginary quadratic field, there are \( \Sigma \) such that \( Z \) consists of one irreducible component of \( Y_0(p)_{\overline{\mathbb{F}_p}} \).
A mod $p$ variant of the André–Oort conjecture

References

1. André, Y.: Finitude des couples d’invariants modulaires singuliers sur une courbe algébrique plane non modulaire. J. Reine Angew. Math. 505, 203–208 (1998)
2. Cojocaru, A.C., Hall, C.: Uniform results for Serre’s theorem for elliptic curves. Int. Math. Res. Not. 50, 3065–3080 (2005). https://doi.org/10.1155/IMRN.2005.3065
3. Deschamps, M.: Réduction semi-stable. Séminaire sur les pinceaux de courbes de genre au moins deux. Astérisque 86, 1–34 (1981)
4. Edixhoven, B.: Special points on the product of two modular curves. Compos. Math. 114(3), 315–328 (1998). https://doi.org/10.1023/A:1000539721162
5. Edixhoven, B.: Special points on products of modular curves. Duke Math. J. 126(2), 325–348 (2005). https://doi.org/10.1215/S0012-7094-04-12624-7
6. Igusa, J.-I.: Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves. Am. J. Math. 81, 453–476 (1959). https://doi.org/10.2307/2372751
7. Katz, N.M., Mazur, B.: Arithmetic moduli of elliptic curves. In: Annals of Mathematics Studies, vol. 108. Princeton University Press, Princeton (1985)
8. Klingler, B., Ullmo, E., Yafaev, A.: Bi-algebraic geometry and the André–Oort conjecture. In: Algebraic Geometry: Salt Lake City 2015, 319–359, Proc. Sympos. Pure Math., 97.2. Amer. Math. Soc., Providence (2018). https://webusers.imj-prg.fr/~bruno.klingler/papiers/Survey2.pdf
9. Lagarias, J.C., Odlyzko, A.M.: Effective versions of the Chebotarev density theorem. In: Algebraic Number Fields: L-Functions and Galois properties (Proc. Sympos., Univ. Durham, Durham), pp. 409–464 (1975)
10. Lang, S.: Algebraic number theory. In: Graduate Texts in Mathematics, vol. 110, 2nd edn. Springer, New York (1994). https://link.springer.com/book/10.1007
11. Schreier, O., van der Waerden, B.L.: Die Automorphismen der projektiven Gruppen. Abh. Math. Sem. Univ. Hamburg 6, 303–322 (1928). https://doi.org/10.1007/BF02940620
12. Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. Inst. Hautes Études Sci. Publ. Math. 54, 323–401 (1981). http://archive.numdam.org/article/PMIHES_1981__54__123_0.pdf
13. SGA 7.1: Groupes de monodromie en géométrie algébrique. I. Séminaire de Géométrie Algébrique du Bois–Marie 1967–1969 (SGA 7 I). Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D.S. Rim. Lecture Notes in Mathematics, vol. 288. Springer, Berlin (1972)
14. Siegel, C.L.: Über die Classenzahl quadratischer Zahlkörper. Acta Arith. 1(1), 83–86 (1935). http://eudml.org/doc/205054
15. Tsimerman, J.: The André–Oort conjecture for $A_g$. Ann. Math. (2) 187(2), 379–390 (2018)
16. Wilson, R.A.: The Finite Simple Groups. Graduate Texts in Mathematics, vol. 251. Springer, London (2009). https://doi.org/10.1007/978-1-84800-988-2
17. Zarhin, Y.: Abelian varieties over fields of finite characteristic. Cent. Eur. J. Math. 12(5), 659–674 (2014). https://doi.org/10.2478/s11533-013-0370-1

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.