EXCEPTIONAL ISOGENIES BETWEEN REDUCTIONS OF PAIRS OF ELLIPTIC CURVES

FRANÇOIS CHARLES

Abstract. Let E and E' be two elliptic curves over a number field. We prove that the reductions of E and E' at a finite place $\mathfrak{p}$ are geometrically isogenous for infinitely many $\mathfrak{p}$, and draw consequences for the existence of supersingular primes. This result is an analogue for distributions of Frobenius traces of known results on the density of Noether-Lefschetz loci in Hodge theory. The proof relies on dynamical properties of the Hecke correspondences on the modular curve.

1. Introduction

The goal of this paper is to prove the following theorem. Say that two elliptic curves over a field k are *geometrically isogenous* if they are isogenous over an algebraic closure of k.

Theorem 1.1. *Let k be a number field, and let E and E' be two elliptic curves over k. Then there exist infinitely many finite places $\mathfrak{p}$ of k such that the reductions $E_\mathfrak{p}$ and $E'_\mathfrak{p}$ of E and E' modulo $\mathfrak{p}$ are geometrically isogenous.*

If k is the function field of a curve over a finite field and E, E' are both non-isotrivial elliptic curves, the analogous result is proved in [CO06, Proposition 7.3] – the situation there is quite different due to the existence of the Frobenius morphism on the base.

Using Faltings' isogeny theorem [Fal83] and the Cebotarev density theorem, it is possible to show that if E and E' are not themselves geometrically isogenous, then – after replacing k by a finite extension – the density of such primes $\mathfrak{p}$ is zero.

The above result is an arithmetic analogue of the following Hodge-theoretic theorem due independently to Green [Voi02, Proposition 17.20] and Oguiso [Ogu03] – see also [BKPSB98]. If H is a Hodge structure of weight 2, let $\rho(H)$ be the *Picard number* of H, that is, the rank of the group of Hodge classes – integral classes of type $(1,1)$ – in H.

Let Δ be the unit disk in $\mathbb{C}$, and let H be a non-trivial variation of Hodge structures of weight 2 over Δ with Hodge number $h^{2,0} = 1$. Let M be the minimal value of the integers $\rho(H_s)$ for s in Δ. Then the Noether-Lefschetz locus

$$NL(H) := \{s \in \Delta,\, \rho(H_s) > M\}$$

is dense in Δ. Note however that $\rho(H_s) = M$ if s is very general in Δ.

In the arithmetic setting, Δ is replaced by a suitable open subset of the spectrum of the ring of integers in a number field k. In that setting, variations of Hodge structures are replaced by representations of the absolute Galois group G_k of k, and the Noether-Lefschetz locus is replaced by the set of primes at which some power of the Frobenius has invariants which do not have a finite orbit under the whole group G_k. Theorem 1.1 then deals with the Galois representation $\mathrm{Hom}(H^1(E_{\overline{k}}, \mathbb{Z}_\ell), H^1(E'_{\overline{k}}, \mathbb{Z}_\ell))$. Indeed, by a theorem of Deuring [Deu41], the reductions of E and E' at a prime $\mathfrak{p}$ are geometrically isogenous if and only if some power of the Frobenius at $\mathfrak{p}$ fixes

Date: September 6, 2017.

a nonzero element of $\mathrm{Hom}(H^1(E_{\overline{k}}, \mathbb{Z}_\ell), H^1(E'_{\overline{k}}, \mathbb{Z}_\ell))$. Since we do not know of an analogue of the Hodge-theoretic argument in this setting, let us offer a different heuristic for Theorem 1.1.

Assume for simplicity that k is the field $\mathbb{Q}$ of rational numbers and that E does not have complex multiplication. Then the Sato-Tate conjecture – now a theorem proved in [CHT08, Tay08, HSBT10, BLGHT11] over totally real fields, see also [BLGG11, BLGGT14] for related developments – predicts that as p varies among the prime numbers, the traces t_p of the Frobenius at p are roughly equidistributed between $-2\sqrt{p}$ and $2\sqrt{p}$. Assume that the same holds for the traces t'_p associated to E', and that E and E' are not geometrically isogenous. Then one might expect – see [Har09] for the case of totally real fields – that the distributions of the t_p and t'_p are independent, so that the probability that t_p is equal to t'_p is of the order of $\frac{1}{\sqrt{p}}$. By Tate's isogeny theorem [Tat66], t_p and t'_p are equal if and only if the reductions of E and E' modulo p are isogenous. Since the sum over all prime numbers p of the $\frac{1}{\sqrt{p}}$ diverges, it might be expected that there exist infinitely many primes p such that the reduction of E and E' modulo p are isogenous.

It seems very difficult to turn the heuristic we just described into a proof. While our proof of Theorem 1.1 can likely be made effective, the lower bounds on the number of $\mathfrak{p}$ satisfying the conclusion is very far from the bounds that could be expected from the discussion above.

The techniques of our paper are much easier than the ones used in the aforementioned proof of the Sato-Tate conjecture. However, we emphasize that Theorem 1.1 does not entail any assumption on the base field nor on the existence of places of multiplicative reduction for E or E'.

Theorem 1.1 has consequences for the reduction modulo different primes of a single elliptic curve.

Corollary 1.2. *Let k be a number field, and let E be an elliptic curve over k. Then at least one of the following statements holds :*

1. *There exist infinitely many places $\mathfrak{p}$ of k such that E has supersingular reduction at $\mathfrak{p}$.*
2. *For any imaginary quadratic number field K, there exist infinitely many places $\mathfrak{p}$ of k such that the reduction of E modulo $\mathfrak{p}$ acquires complex multiplication by K after a finite extension of the ground field.*

Recall that an elliptic curve over a finite field either has complex multiplication by a quadratic imaginary field or is supersingular. A folklore expectation, related to the Lang-Trotter conjecture [LT76], is that both statements of the corollary above should hold unless E has complex multiplication. The existence of infinitely many supersingular primes has been addressed by Elkies [Elk89], who managed to prove that statement (1) is always true when k admits a real place. Very little seems to be known about (2) or the general case of (1).

Our proof of Theorem 1.1 relies on the Arakelov geometry of the moduli space of elliptic curves. The basic strategy is very simple: given a positive integer N, the set of finite places $\mathfrak{p}$ of k such that the reductions $E_\mathfrak{p}$ and $E'_\mathfrak{p}$ of E and E' modulo $\mathfrak{p}$ are related – after some base field extension – by a cyclic isogeny of degree N can be expressed as the image in $\operatorname{Spec}\mathbb{Z}$ of the intersection of an arithmetic curve in $\mathbb{P}^1_\mathbb{Z} \times \mathbb{P}^1_\mathbb{Z}$ with the graph of a Hecke correspondence t_N. We need to show that we can obtain infinitely many places this way as we let N vary.

Instead of the set-theoretic intersection, we can consider the intersection number in the sense of Arakelov geometry. Knowing the height of the modular curves by work of Cohen [Coh84] and Autissier [Aut03] makes it possible to show that the order of magnitude of this intersection number is $N \log N$ – assuming N has few prime factors for simplicity. This reduces the proof of the theorem to bounding the local intersection numbers at all places of k – finite or infinite. This turns out to be, in various forms, a manifestation of the ergodicity of Hecke correspondences as proved in [COU01], though it does not seem to follow directly from it.

As this sketch might suggest, our method of proof is related to the techniques of Gross and Zagier in their celebrated result [GZ86]. Instead of computing intersections of Hecke orbits for Heegner points, we are giving estimates for similar intersection numbers at arbitrary points of the modular curve. Our task is made much simpler technically by the fact that we do not need to prove exact formulas for intersection numbers on modular curves.

As will be apparent in the paper, our proof of Theorem 1.1 should generalize to similar statements regarding to the behavior of Hecke correspondences on Shimura curves.

Section 2 is devoted to setting up notation and proving some basic – and certainly well-known – lemmas. In section 3, we show how Corollary 1.2 can be deduced from the main theorem and reduce the main theorem to local statements. The last two parts of the paper are devoted to the proof of these local statements.

Acknowledgements. This paper has greatly benefited from numerous conversations with Emmanuel Ullmo, whom it is a great pleasure to thank. I would like to thank Ching-Li Chai for pointing out the reference [CO06].

I am especially grateful for a very careful reading of three referees, who went through a rough first version of these papers and helped greatly in improving the exposition and pointing out mistakes. I thank Ananth Shankar and Yunqing Tang for useful correspondence and discussions pointing out inaccuracies, as well as helpful suggestions.

2. Notations and preliminary results

2.1. **Notation.** Let $X(1)$ be the coarse moduli scheme of generalized elliptic curves as defined in [DR73]. It is a smooth arithmetic surface over $\operatorname{Spec}\mathbb{Z}$. The modular invariant j provides an isomorphism

$$j : X(1) \to \mathbb{P}^1_{\mathbb{Z}}.$$

Let $\mathbb{H}$ be the Poincaré half-plane, and let $\overline{\mathbb{H}}$ be the union of $\mathbb{H}$ with the set of cusps $\mathbb{Q} \cup \{\infty\}$. There is a canonical isomorphism between the Riemann surfaces $X(1)_{\mathbb{C}}$ and $\overline{\mathbb{H}}/\Gamma(1)$. We will denote by τ the standard coordinate on $\mathbb{H}$.

Let N be a positive integer, and let $X_0(N)$ be the Deligne-Rapoport compactification of the coarse moduli scheme which parametrizes cyclic isogenies of degree N between elliptic curves. It is a normal arithmetic surface over $\operatorname{Spec}\mathbb{Z}$.

The two tautological maps from $X_0(N)$ to $X(1)$ induce a self-correspondence t_N of $X(1)$. It is called the Hecke correspondence of order N. Define $e_N = N\,\Pi_{p|N}(1+\frac{1}{p})$, where p runs over the prime divisors of N. The Hecke correspondence t_N has bidegree (e_N, e_N).

Let $\mathcal{M}$ be the line bundle of modular forms of weight 12 on $X(1)$. The modular form

$$\Delta(\tau) = (2\pi)^{12} q \Pi_{n\geq 1}(1-q^n),$$

with $q = e^{2i\pi\tau}$ induces a global section of $\mathcal{M}$. It has a zero of order 1 at the cusp $j^{-1}(\infty)$ and does not vanish anywhere else. As a consequence, Δ induces an isomorphism $j^*\mathcal{O}(1) \xrightarrow{\sim} \mathcal{M}$.

If $t \in \mathbb{C}$, the modular form $(t-j)\Delta$ induces a global section of $\mathcal{M}_{\mathbb{C}}$ that has a zero of order 1 at $j^{-1}(t)$ and does not vanish anywhere else. More generally, let Y is an horizontal divisor of relative degree d on $X(1)$ with $Y_{\mathbb{C}} = \sum_i n_i y_i$ and assume that no y_i is a cusp. Then the modular form $\Pi_i[(j(y_i)-j)\Delta]^{n_i}$ is a section of $\mathcal{M}^{\otimes d}$ with divisor Y.

The Petersson metric on modular forms induces a hermitian metric $||.||$ on $\mathcal{M}_{\mathbb{C}}$ such that

$$||\Delta(\tau)|| = |\Delta(\tau)||Im(\tau)|^6,$$

where $|.|$ is the usual complex norm. This metric is L^2_1-singular along the cusp $j^{-1}(\infty)$ – following the terminology of [Bos99, Section 3]. The line bundle $\mathcal{M}$ endowed with the Petersson metric on $\mathcal{M}_{\mathbb{C}}$ is a hermitian line bundle $\overline{\mathcal{M}}$ on $X(1)$.

When working with fields equipped with a non-archimedean valuation such that the residue field has characteristic $p > 0$, we will often use the absolute value $|.|$ such that $|p| = p^{-1}$ and the valuation v such that $v(p) = 1$. We will say that this absolute value (resp. valuation) is *normalized*.

2.2. **Intersection theory on modular curves.** We will use generalized Arakelov intersection theory for arithmetic surfaces as in [Bos99], section 5 of which contains the definitions and notations we are using. We also refer to [Aut03] for the specific case we are considering. The height function with respect to $\overline{\mathcal{M}}$ is denoted by $h_{\overline{\mathcal{M}}}$, and arithmetic degrees are denoted by $\widehat{\deg}$.

The starting point of the proof is the formula giving the height of Hecke correspondences. The following is Theorem 3.2 of [Aut03], and was also proved in [Coh84].

Theorem 2.1. *Let k be a number field with ring of integers $\mathcal{O}_k$. Let Y be a horizontal one-dimensional integral subscheme of $X(1)_{\mathcal{O}_k}$ such that $Y_{\mathbb{C}}$ does not meet $j^{-1}(\infty)$. Let $d = [k(Y) : k]$. Then, as N goes to infinity, we have*

$$h_{\overline{\mathcal{M}}}(t_{N*}Y) \sim 6d[k : \mathbb{Q}]e_N \log(N) \tag{2.1}$$

The estimate above can be rephrased in terms of intersections of divisors on $X(1)_{\mathcal{O}_k}$. Let $\overline{k}$ be an algebraic closure of k. Let $P = \sum_i n_i P_i$ be a zero-cycle on $X(1)_{\mathcal{O}_k}$, where the P_i are closed points. The arithmetic degree of P is defined as

$$\widehat{\deg}(P) = \sum_i n_i \log N(P_i),$$

where $N(P_i)$ is the cardinality of the residue field of P_i. Let Y and Z be two divisors in $X(1)$. The arithmetic degree $\widehat{\deg}(Y.Z)$ is defined as the arithmetic degree of the intersection 0-cycle $Y.Z$.

Finally, let σ be an embedding of k into $\mathbb{C}$. If Z is any purely horizontal divisor on $X(1)_{\mathcal{O}_k}$, write $Z_{\mathbb{C}} = \sum_i n_i Q_i$ with $Q_i \in X(1)(\mathbb{C})$. Assume that $j(Q_i) \neq \infty$ for all i, and let $z_i = j(Q_i) \in \mathbb{C} \subset \mathbb{P}^1(\mathbb{C})$. Let d' be the sum of the n_i. We denote by s^{σ}_Z the global section of $\mathcal{M}_{\mathbb{C}}^{\otimes d'}$ such that

$$s^{\sigma}_Z(\tau) = \Pi_i[(z_i - j(\tau))\Delta(\tau)]^{n_i}.$$

Then the s^{σ}_Z, as σ varies through all embeddings of k into $\mathbb{C}$, extend to a section s_Z of $\mathcal{M}^{\otimes d'}$ over $X(1)_{\mathcal{O}_k}$.

If Y is any purely horizontal divisor on $X(1)$ with $Y_{\mathbb{C}} = \sum_j m_j P_j$, write

$$s^{\sigma}_Z(Y) = \Pi_j s^{\sigma}_Y(P_j)^{m_j}.$$

Let $\sigma_1, \dots, \sigma_{r_1}$ be the real embeddings of k, and let $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$ be the complex embeddings of k. We extend the σ_i to embeddings $\overline{k} \to \mathbb{C}$. As usual, set $\varepsilon_i = 1$ if $1 \leq i \leq r_1$ and $\varepsilon_i = 2$ if $r_1 + 1 \leq i \leq r_1 + r_2$. Using the sections s^{σ}_Z to compute heights with respect to $\mathcal{M}$, Theorem 2.1 gives the following.

Corollary 2.2. *Let Y and Z be two purely horizontal divisors on $X(1)_{\mathcal{O}_k}$ of relative degree d and d' respectively. Assume that Y is effective and irreducible, and that for any positive integer N, the divisors $t_{N*}Y$ and Z do not have any common component. Then, as N goes to infinity, we have*

$$\widehat{\deg}(Z.t_{N*}Y) - \sum_{i=1}^{r_1+r_2} \varepsilon_i \log ||s^{\sigma_i}_Z(t_{N*}Y)|| \sim 6dd'[k : \mathbb{Q}]e_N \log(N).$$

3. Local statements and proof of the main results

In this section, we reduce the proofs of Theorem 1.1 and Corollary 1.2 to local statements which provide estimates for the terms appearing in Corollary 2.2. The proof of these local estimates will be the core of the paper.

Let us briefly explain the motivation for the estimates below. We will prove Theorem 1.1 by showing that, for suitable large N, each individual local term in Corollary 2.2 is negligible before the right-hand-side, which is of the order of $e_N \log(N)$. Let us consider the archimedean term as an example. Let z and y be two complex numbers, that we consider as complex points of $X(1)$. If N is a positive integer, write the *Hecke orbit* of y, $t_{N*}y$, as

$$t_{N*}y = j(\tau_1) + \ldots + j(\tau_{e_N})$$

where the τ_i belong to the Poincaré upper half-plane $\mathbb{H}$. We are interested in comparing the quantity

$$\sum_{i=1}^{e_N} \log(|z - j(\tau_i)|\,||\Delta(\tau_i)||) \tag{3.1}$$

to $e_N \log(N)$ as N goes to infinity.

Equidistribution of Hecke points as proved in [COU01] suggests that the sum above should be compared to the integral

$$e_N \int_{\Gamma\backslash\mathbb{H}} \log(|z - j(\tau)|\,|\Delta(\tau)|\,|\mathrm{Im}(\tau)|^6)\frac{dx\,dy}{y^2}$$

with $\tau = x + iy$ and $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$. It is readily checked that the latter integral converges, which suggests that the sum (3.1) is negligible before $e_N \log(N)$.

The argument above is not correct, as the function we are integrating has a singularity at the point $j^{-1}(z)$. However, what the above computation shows is that the estimate we are interested in amounts to controlling the best approximations of z by points in the Hecke orbit of y.

It might be possible to extend the estimates of our paper so as to study the behavior of the sum (3.1), but we will be content with weaker estimates.

In the following, we write $|t_{N*}y|$ to denote the support of the Hecke orbit of y.

The three propositions below contain the estimates that allow the argument above to go through. The first one deals with the places of bad reduction. From now on, we identify $X(1)$ and $\mathbb{P}^1_{\mathbb{Z}}$ via the j-invariant when convenient – in particular, we see k as a subset of $X(1)(k)$ for any field k.

Proposition 3.1. *Let $|.|$ be a non-archimedean normalized absolute value on $\overline{\mathbb{Q}}$, and let C be the completion of $\overline{\mathbb{Q}}$ with respect to $|.|$. Let y and z be two distinct points of $C \subset X(1)(C)$.*

Assume that $|y| > 1$. Then there exists a positive integer n such that for any positive integer N which is not a perfect square and is prime to n, the following inequality holds :

$$\forall \alpha \in |t_{N*}y|, |z^{-1} - \alpha^{-1}| \geq |z^{-1}|. \tag{3.2}$$

The following result should be seen as a very weak equidistribution result for Hecke correspondences. For archimedean valuations, it follows from [COU01]. For non-archimedean valuations and supersingular reduction, equidistribution has been proved by Fargues (unpublished). For lack of reference, we provide a self-contained argument for our easier result.

Proposition 3.2. *Let $|.|$ be an absolute value on $\overline{\mathbb{Q}}$, which we assume to be normalized in the non-archimedean case, and let C be the completion of $\overline{\mathbb{Q}}$ with respect to $|.|$. Let y and z be two distinct points of $C \subset X(1)(C)$. If the absolute value $|.|$ is not archimedean, assume furthermore that $|y| \leq 1$. Let ε_1 and ε_2 be two positive real numbers.*

There exists a positive constant η such that, letting

$$B_{y,z} = \{N \in \mathbb{N} \setminus (p\mathbb{N}), |\{\alpha \in |t_{N*}y|, |z-\alpha| \leq \eta\}| \geq \varepsilon_1 e_N\},$$

where elements in the Hecke orbit of y are counted with multiplicity, then the upper density of $B_{y,z}$ is at most ε_2, i.e.

$$\limsup_{n\to\infty} \frac{1}{n}|B_{y,z} \cap \{1,\dots,n\}| \leq \varepsilon_2.$$

The last result goes beyond equidistribution. It shows that there cannot exist too many Hecke orbits that contain very good approximations of a given point.

Proposition 3.3. *Let $|.|$ be an absolute value on $\overline{\mathbb{Q}}$, and let C be the completion of $\overline{\mathbb{Q}}$ with respect to $|.|$. Let y and z be two distinct points of $C \subset X(1)(C)$ such that y is not the j-invariant of a CM elliptic curve. If the absolute value $|.|$ is not archimidean, assume that it is normalized and that $|y| \leq 1$.*

Let D be a large enough integer – depending on y, z and the chosen $|.|$, and define

$$S^D_{y,z} = \{N \in \mathbb{N} \setminus (p\mathbb{N}) | \, \exists\, \alpha \in |t_{N*}y|, |\alpha - z| \leq N^{-D}\}.$$

Then

$$\lim_{n\to\infty} \frac{1}{n}|S^D_{y,z} \cap \{1,\dots,n\}| = 0.$$

Remark 3.4. *It is possible to give an explicit bound on D – e.g. $D \geq 20$ suffices in the archimedean case – see Proposition 5.16 and Proposition 5.23.*

The three propositions above will be proved in the next section. We now explain how they imply the main results of the paper.

Proof of Theorem 1.1. We argue by contradiction, and assume that there are only finitely many places $\mathfrak{p}$ of k as in Theorem 1.1. In particular, E and E' are not geometrically isogenous. We can and will assume that E does not have complex multiplication – if both curves have complex multiplication, the theorem is clear as there exist infinitely many primes of supersingular reduction for both E and E' and any two supersingular elliptic curves are geometrically isogenous.

Let S be a finite set of finite places of k containing the places $\mathfrak{p}$ such that the reductions of E and E' modulo $\mathfrak{p}$ are smooth and geometrically isogenous as well as the places of bad reduction for E or E'. Up to enlarging k, we can assume that the only places of bad reduction for E or E' are the places of multiplicative reduction.

Let y (resp. z) be the rational point of $X(1)_k$ corresponding to E (resp. E'). Let Y and Z be the Zariski closures of y and z in $X(1)_{\mathcal{O}_k}$ respectively. Let N be a positive integer. Since E and E' are not geometrically isogenous, Z and $t_{N*}Y$ have no common component. By definition of t_N, the geometric intersection points of Z and $t_{N*}Y$ correspond precisely to the pairs consisting of a finite place $\mathfrak{p}$ of k such that there exists a cyclic isogeny of degree N between $E_{\overline{\kappa}(\mathfrak{p})}$ and $E'_{\overline{\kappa}(\mathfrak{p})}$, where $\overline{\kappa}(\mathfrak{p})$ is an algebraic closure of the residue field of $\mathfrak{p}$.

We use the notations of Corollary 2.2 and get, as N goes to infinity

$$\widehat{\deg}(Z.t_{N*}Y) - \sum_{i=1}^{r_1+r_2} \varepsilon_i \log ||s_Z^{\sigma_i}(t_{N*}Y)|| \sim 6[k:\mathbb{Q}]e_N \log(N).$$

Write $Z.t_{N*}Y = \sum_i n_i P_i$, where the P_i are closed points of $X(1)_{\mathcal{O}_k}$. If $\mathfrak{p}$ is a finite place of k, let us write $\deg_{\mathfrak{p}}(Z.t_{N*}Y)$ for the sum $\sum_i n_i \log N(P_i)$ where P_i runs through the closed points lying over $\mathfrak{p}$. By definition of S, we have $\deg_{\mathfrak{p}}(Z.t_{N*}Y) = 0$ if $\mathfrak{p}$ does not belong to S. As a consequence,

we get, as N goes to infinity

$$\sum_{\mathfrak{p}\in S} \deg_{\mathfrak{p}}(Z.t_{N*}Y) - \sum_{i=1}^{r_1+r_2} \varepsilon_i \log ||s_Z^{\sigma_i}(t_{N*}Y)|| \sim 6[k:\mathbb{Q}]e_N \log(N). \tag{3.3}$$

Given $\mathfrak{p}$ in S, let $|.|_{\mathfrak{p}}$ be the corresponding normalized, non-archimedean absolute value on $\overline{\mathbb{Q}}$. If i is an integer between 1 and $r_1 + r_2$, let $|.|_i$ be an archimedean absolute value on $\overline{\mathbb{Q}}$ extending the absolute value on k defined by the embedding σ_i of k in $\mathbb{C}$. We restrict our attention to those integers N which are prime to the residual characteristic of the $\mathfrak{p} \in S$.

Let $\mathfrak{p}$ be an element of S. We have

$$\deg_{\mathfrak{p}}(Z.t_{N*}Y) = \sum_{\alpha\in|t_{N*}y|} \log \frac{|\alpha - z|_{\mathfrak{p}}}{\mathrm{Max}(1,|\alpha|_{\mathfrak{p}})\mathrm{Max}(1,|z|_{\mathfrak{p}})}.$$

Here $t_{N*}y$ is seen as a set of e_N distinct $\overline{\mathbb{Q}}$-points of $X(1)$ – recall that E does not have complex multiplication.

For any $\alpha \in |t_{N*}y|$, the valuation of y with respect to $\mathfrak{p}$ is negative if and only if the valuation of α is. As a consequence, the above formula specializes to

$$\deg_{\mathfrak{p}}(Z.t_{N*}Y) = \sum_{\alpha\in|t_{N*}y|} \mathrm{Max}(0, -\log|\alpha - z|_{\mathfrak{p}})$$

if the valuation of y is nonnegative, and

$$\deg_{\mathfrak{p}}(Z.t_{N*}Y) = \sum_{\alpha\in|t_{N*}y|} \mathrm{Max}(0, -\log|\alpha^{-1} - z^{-1}|_{\mathfrak{p}})$$

if the valuation of y is negative.

Let A be the finite set consisting of the absolute values $|.|_{\mathfrak{p}}$ for $\mathfrak{p} \in S$ and of the archimedean absolute values $|.|_i$. We apply Propositions 3.1, 3.2 and 3.3 to the absolute values in A simultaneously. Let ε be a positive real number, that we will take to be small enough.

We first apply Proposition 3.1 simultaneously to the set A_{mult} of those non-archimedean absolute values $|.|_a$ in A for which $|y|_a > 1$. We can find an integer n such that if N is any positive integer which is not a square and is prime to n, then

$$\forall \alpha \in |t_{N*}y|, |z^{-1} - \alpha^{-1}|_a \geq |z^{-1}|_a$$

for any non-archimedean absolute value $|.|_a$ in A_{mult}.

We now consider the absolute values $|.|_a$ that are archimedean or satisfy $|y|_a \leq 1$. Applying Proposition 3.2 to those simultaneously, we can find a positive constant η and a set of integers B of upper density at most ε such that for any $|.|_a$ as above, and any positive integer N prime to the residual characteristic of $|.|_a$, we have

$$N \notin B \implies |\{\alpha \in |t_{N*}y|, |z - \alpha|_a \leq \eta\}| \leq \varepsilon e_N.$$

Finally, applying Proposition 3.3, for any D large enough and any of the finitely many absolute values $|.|_a$ in A that are archimedean or non-archimedean and satisfies $|y|_a \leq 1$, we have

$$\limsup_{n\to\infty} \frac{1}{n}|\{1 \leq N \leq n | \forall \alpha \in |t_{N*}y|, \forall a \in A | \alpha - z|_a \geq N^{-D}\}| \geq \frac{1}{2^{|A|}}.$$

The discussion above shows that we can find infinitely many positive integers N satisfying the following three properties:

(i) For any absolute value $|.|_a$ in A_{mult} and any α in t_{N*y}, then

$$|z^{-1} - \alpha^{-1}|_a \geq |z^{-1}|_a;$$

(ii) for any absolute value $|.|_a$ in $A \setminus A_{mult}$, then

$$|\{\alpha \in |t_{N*}y|, |z-\alpha|_a \leq \eta\}| \leq \varepsilon e_N;$$

(iii) for any absolute value $|.|_a$ in $A \setminus A_{mult}$ and any α in $t_{N*}y$, then

$$|\alpha - z|_a \geq N^{-D}.$$

Let us spell out the consequences of these estimates for the intersection numbers we are considering. Let $|.|_a$ be an absolute value in A. If $|.|_a$ is in A_{mult}, then we can write

$$\deg_{\mathfrak{p}}(Z.t_{N*}Y) = \sum_{\alpha \in t_{N*y}} \mathrm{Max}(0, -\log|\alpha^{-1} - z^{-1}|_a) \leq e_N \log|z|. \tag{3.4}$$

If $|.|_a$ is non-archimedean and does not belong to A_{mult}, we have

$$\deg_{\mathfrak{p}}(Z.t_{N*}Y) = \sum_{\alpha \in t_{N*y}} \mathrm{Max}(0, -\log|\alpha - z|_{\mathfrak{p}}) \leq e_N \log(\eta^{-1}) + \varepsilon e_N D \log(N). \tag{3.5}$$

If $|.|_a$ is archimedean, and corresponds to an embedding σ of k in $\mathbb{C}$, choose, for each α in the N-th Hecke orbit of y, an element $\tau_\alpha \in \mathbb{H}$ such that $j(\tau_\alpha) = \sigma(\alpha)$. We have

$$\log||s_Z^\sigma(t_{N*}Y)|| = \sum_{\alpha \in |t_{N*}y|} \log(|\alpha - z|_a||\Delta(\tau_\alpha)||).$$

As the imaginary part of τ_α tends to ∞, the expression $\log(|\alpha - z|_a||\Delta(\tau_\alpha)||)$ tends to ∞ as well. Choose a compact set $K \in \mathbb{C}$ such that $\log(|\alpha - z|_a||\Delta(\tau_\alpha)||) \geq 0$ for any α outside K. Then we have

$$\log||s_Z^\sigma(t_{N*}Y)|| \geq \sum_{\alpha \in |t_{N*}y| \cap K} \log(|\alpha - z|_a||\Delta(\tau_\alpha)||) = \sum_{\alpha \in |t_{N*}y| \cap K} \log(|\alpha - z|_a) + O(e_N).$$

Going back to the above estimates, we find

$$\log||s_Z^\sigma(t_{N*}Y)|| \geq e_N \log||\Delta(\tau)|| - \varepsilon e_N D \log(N)) + (1-\varepsilon) e_N \log(\eta) + O(e_N). \tag{3.6}$$

We now plug in the estimates (3.4), (3.5) and (3.6) in the global degree estimate (3.3) to find – after dividing by e_N, comparing the higher order terms, and noting that the ε_i are either 1 or 2 –

$$6[k:\mathbb{Q}] \leq (|S \setminus A_{mult}| + 2(r_1 + r_2))\varepsilon D. \tag{3.7}$$

Since ε can be chosen arbitrarily small, this is a contradiction. □

Proof of Corollary 1.2. Assume that E has only finitely many places of supersingular reduction. Let K be an imaginary quadratic extension of $\mathbb{Q}$. We need to show that there exist infinitely many places $\mathfrak{p}$ of k such that the reduction of E modulo $\mathfrak{p}$ has complex multiplication by K after some finite extension of the ground field.

Up to enlarging k, we can find an elliptic curve E' defined over k with complex multiplication by K. If $\mathfrak{p}$ is any place of k, then the reduction of E' modulo $\mathfrak{p}$ is either a supersingular elliptic curve or has complex multiplication by K. Since E has only finitely many supersingular reductions, Theorem 1.1 applied to E and E' shows the result. □

4. Basic estimates

The goal of this section is to prove Proposition 3.1 and Proposition 3.2. The – more involved – study of good approximations at the places of good reduction will be dealt with in the next section.

4.1. **Multiplicative reduction.** We prove Proposition 3.1. It is a consequence of the following more precise result, the proof of which is essentially contained in [Sil90, Proposition 2.1].

Proposition 4.1. *Let v be a non-archimedean valuation on $\overline{\mathbb{Q}}$ and let C be the completion of $\overline{\mathbb{Q}}$ at v. Let x be a rational number and write $x = \frac{a}{b}$, where a and b are relatively prime integers. Let E be an elliptic curve over C and assume that $v(j(E))$ is negative. Write $v(j(E)) = \frac{c}{d}$, where c and d are relatively prime integers. Let N be a positive integer such that*

(1) N is not a perfect square ;
(2) N is prime to $abcd$.

Let E' be the quotient of E by a subgroup of order N. Then

$$v(j(E')) \neq x.$$

Proof. Since the valuation of $j(E)$ is negative, E is isomorphic to a Tate curve. Thus, as rigid analytic spaces,

$$E(C) \simeq \frac{C^*}{q^{\mathbb{Z}}}$$

for some $q \in C^*$, with

$$v(q) = -v(j(E)).$$

Let N be any positive integer. Let ξ be a N-th root of q, and let ω be a primitive N-th root of unity. Then the subgroups of E of order N are of the form

$$\frac{\omega^{t\mathbb{Z}}(\omega^s\xi^r)^{\mathbb{Z}}}{q^{\mathbb{Z}}},$$

where r, s and t are positive integers such that $rt = N$ and $s < t$. As in [Sil90, Proposition 2.1], the map $x \mapsto x^r$ induces an isomorphism

$$\frac{C^*}{\omega^{t\mathbb{Z}}(\omega^s\xi^r)^{\mathbb{Z}}} \simeq \frac{C^*}{(\omega^s\xi^r)^{r\mathbb{Z}}} = \frac{C^*}{(\omega^{rs}\xi^{r^2})^{\mathbb{Z}}}$$

so that the valuation of $j(E')$ is

$$v(j(E')) = -v(\omega^{rs}\xi^{r^2}) = -\frac{r^2}{N}v(q) = \frac{r}{t}v(j(E)).$$

Now assume that N satisfies the assumptions of the proposition and that $v(j(E')) = x$. This means that

$$rbc = tad.$$

Since $N = rt$ is prime to $abcd$, this implies $r = t$, which is a contradiction since N is not a square by assumption. □

Proof of Proposition 3.1. Let v be the valuation corresponding to the absolute value $|.|$. Let E be an elliptic curve over C with $j(E) = y$, and let x be the valuation of z. With the notations of Proposition 4.1, let $n = abcd$. Then if N is any positive integer prime to n which is not a perfect square, then Proposition 4.1 shows that any α in $|t_{N*}y|$ satisfies $v(\alpha) \neq x = v(z)$. As a consequence, we have

$$|z^{-1} - \alpha^{-1}| \geq |z^{-1}|.$$

This proves the result. □

4.2. **Equidistribution.** The goal of this section is to prove Proposition 3.2. We use the notations of the proposition. If the absolute value $|.|$ is archimedean, then the result follows from the main theorem of Clozel, Oh and Ullmo [COU01].

We now assume that $|.|$ is non-archimedean. Let p be the residue characteristic. The assumptions on y and z ensure that we can find a complete discrete valuation ring W whose francion field is a subfield of C, and whose residue field is an algebraically closed field of characteristic p, as well as two elliptic curves E and E' over W such that $j(E) = y$ and $j(E') = z$.

Let π be a uniformizing parameter of W. If n is a nonnegative integer, let W_n be the ring $W_n = W/\pi^{n+1}$. Let v be the additive valuation on W such that $v(\pi) = 1$.

Since the valuation of y is nonnegative, so is the valuation of any α in a Hecke orbit of y. If the valuation of z is negative, this implies $|z - \alpha| = |z|$ and the result follows. As a consequence, we can assume that the valuation of z is nonnegative.

Denote by H_n be the group

$$H_n = \mathrm{Hom}_{W_n}(E, E')$$

that consists of morphisms from the reduction of E modulo π^{n+1} to that of E'.

The restriction maps $H_n \to H_{n+1}$ are injective for any $n \geq 0$, see e.g. [Con04, Theorem 2.1]. As a consequence, we consider the sequence $(H_n)_{n\geq 0}$ as a decreasing sequence of subgroups of H_0. Grothendieck's existence theorem implies that the intersection $H = \bigcap_{n\geq 0} H_n$ is equal to the group $\mathrm{Hom}_W(E, E')$ of morphisms defined over W considered as a subgroup of H_0.

Let q be the natural positive-definite quadratic form on H_0 defined by $q(f) = \deg(f)$. Let us state a basic estimate for number of points in lattices.

Lemma 4.2. *Let ε_1 and ε_2 be two positive real numbers. There exists a positive integer n such that the set of integers*

$$B_n = \{N \in \mathbb{N}, |q^{-1}(N) \cap H_n| \geq \varepsilon_1 N\}$$

has upper density at most ε_2.

Proof. General results on the endomorphisms groups of elliptic curves show that the groups H_n are free modules of rank $1, 2$ or 4. If the rank of the H_n is at most 2, let δ be a positive real number such that the balls of radius δ in $H_n \otimes \mathbb{R}$ with respect to q centered at the points of H_n are pairwise disjoint. Write $B(0, R)$ for the open ball of radius R and center 0 in $H_n \otimes \mathbb{R}$, and $A(0, R, R')$ for the open annulus in $H_n \otimes \mathbb{R}$ consisting of the elements $x \in H_n \otimes \mathbb{R}$ such that $R < q(x) < q(R')$. Write v for the euclidean volume in $H_n \otimes \mathbb{R}$. Then

$$v(B(0, \delta)|q^{-1}(N) \cap H_n| \leq v(A(0, \sqrt{N} - \delta, \sqrt{N} + \delta)) = O(\sqrt{N}),$$

so that, for any fixed n, $|q^{-1}(N) \cap H_n| = O(\sqrt{N})$ as N goes to infinity. As a consequence, we can assume that the H_n have rank 4.

The intersection H of the H_n has rank at most 2, as it is equal to the group of morphisms between two elliptic curves over a field of characteristic zero. Since there are only finitely many lattices of bounded index in H_0, the index of H_n in H_0 goes to infinity with n.

Now we have, by the same volume computation as before,

$$|\{h \in H_0 | q(h) \leq N\}| = O(N^2).$$

Furthermore, it is an easy exercise to show that for any positive n, we have

$$\lim_{N\to\infty} \frac{|\{h \in H_0 | q(h) \leq N\}|}{|\{h \in H_n | q(h) \leq N\}|} = [H_0 : H_n].$$

It follows that for any positive real number ε, and any n large enough, the following estimate holds for all N large enough:

$$|\{h \in H_n | q(h) \leq N\}| \leq \varepsilon N^2. \tag{4.1}$$

Fix such an integer n, and let ε_1 and B_n be as in the statement of the lemma. We can write, for any integer N large enough,

$$|\{h \in H_n | q(h) \leq N\}| \geq \sum_{k \in B_n, k \leq N} |\{q^{-1}(k) \cap H_n\}| \geq \sum_{k \in B_n, k \leq N} \varepsilon_1 k \geq \varepsilon_1 \frac{|B_n^N|(|B_n^N|+1)}{2}, \tag{4.2}$$

with $N_n^N = B_n \cap \{1, \ldots, N\}$. The estimates (4.1) and (4.2) show that we can write

$$2\varepsilon N^2 \geq \varepsilon_1 |B_n^N|^2.$$

Choosing ε small enough so that $2\varepsilon \leq \varepsilon_1 \varepsilon_2^2$, the estimate above shows that, for suitable n and for all N large enough, we have $|B_n^N| \leq \varepsilon_2 N$. This proves the result.

□

Proof of Proposition 3.2. We keep the notations above, and choose n as in Lemma 4.2. Let N be an integer prime to p. Then the group scheme $E[N]$ defined as the kernel of multiplication by N is étale over W since N is prime to p. Since the residue field of W is algebraically closed by assumption, $E[N]$ is isomorphic to the constant group $(\mathbb{Z}/N\mathbb{Z})^2$. In other words, the N-torsion points of E are defined over W.

Let α be a point in the Hecke orbit $t_{N*}y$ of y. Since E has no complex multiplication and since $E[N]$ is defined over W, there exists a unique elliptic curve E_α over W with j-invariant α together with a cyclic isogeny $E \to E_\alpha$ of degree N. If n is a positive integer and F an elliptic curve over W, denote by F_n the reduction of F modulo π^{n+1}.

Proposition 2.3 of [GZ85] states the we have the following equality

$$v(\alpha - z) = \sum_{n \geq 0} \frac{|\mathrm{Iso}_n(E_\alpha, E')|}{2},$$

where $\mathrm{Iso}_n(E_\alpha, E_\beta)$ denotes the set of isomorphisms from $E_{\alpha,n}$ to E'_n. Let n be the largest integer such that $E_{\alpha,n}$ and E'_n are isomorphic. Since the group of automorphisms of an elliptic curve over W/π^{n+1} has cardinality at most 24, we have

$$n + 1 \geq \frac{1}{12} v(\alpha - z). \tag{4.3}$$

Choose an isomorphism $E_{\alpha,n} \to E'_n$. The composition

$$E_n \to E_{\alpha,n} \to E'_n$$

is an element $h_\alpha \in q^{-1}(N) \cap H_n$. The isogeny h_α is well-defined up to automorphisms of E'_n, and h_α determines α as the j-invariant of the image of h_α. This shows that for any positive integer n, we have

$$|\{\alpha \in |t_{N*}y|, v(\alpha - z) \geq 12(n+1)\}| \leq |q^{-1}(N) \cap H_n|.$$

Let η be a positive real number such that $|z - \alpha| \leq \eta$ implies $v(z - \alpha) \geq 12(n+1)$ for any α in W. Since for any positive N, $e_N \geq N$, Lemma 4.2 shows that the set

$$B_{y,z} = \{N \in \mathbb{N} \setminus (p\mathbb{N}), |\{\alpha \in |t_{N*}y|, |z - \alpha| \leq \eta\}| \geq \varepsilon_1 e_N\},$$

has upper density at most ε_2. This shows the result. □

5. Bounding the best approximations

The goal of this section is to prove Proposition 3.3. We handle the case of non-archimedean valuations and archimedean valuations separately. The non-archimedean case is proved in Proposition 5.15, and the archimedean case – which reduces to the study of the usual absolute value on $\mathbb{C}$ – is Proposition 5.23.

We need to show that, given two points y and z of $X(1)(C)$, there exist sufficiently many Hecke orbits of y that do not contain elements that are too close to z – with precise estimates to be given below. Our argument is the following: we will show that the only way two different Hecke orbits of y can both contain very good approximations of z is if y is very close to a CM point whose ring of endomorphisms has small discriminant. Since distinct CM points of small discriminant cannot be too close to one another, this will allow us to find Hecke orbits of y that don't contain very good approximations of z.

Before getting to the actual proofs, we record some elementary results. If L is a quadratic lattice, that is, a free abelian group of finite rank endowed with a positive definite, integral valued quadratic form, let $\mathrm{disc}(L)$ denote its discriminant, which is well-defined as an element of $\mathbb{Z}$.

Lemma 5.1. *Let E and E' be two isogenous CM elliptic curves over an algebraically closed field of characteristic zero. Consider $\mathrm{End}(E)$ and $\mathrm{Hom}(E,E')$ as quadratic lattices with respect to the quadratic form $f \mapsto \deg(f)$. Then we have*

$$|\mathrm{disc}(\mathrm{End}(E))| \geq |\mathrm{disc}(\mathrm{Hom}(E,E'))|.$$

Proof. Let $f : E \to E'$ be a cyclic isogeny, and consider the morphism

$$\alpha : \mathrm{Hom}(E,E') \to \mathrm{End}(E), \phi \mapsto \widehat{\phi} \circ f,$$

where $\widehat{\phi} : E' \to E$ is the isogeny dual to ϕ. Then for any $\phi \in \mathrm{Hom}(E,E')$, we have $\deg(\alpha(\phi)) = \deg(f)\deg(\phi)$. In particular, we have

$$|\mathrm{disc}(\alpha(\mathrm{Hom}(E,E')))| = \deg(f)^2 |\mathrm{disc}(\mathrm{Hom}(E,E'))|.$$

If n is a positive integer, let $[n]$ denote multiplication by n on E. Then for $[n]$ to belong to the image of α, it is necessary that the kernel of f be included in the kernel of $[n]$. Since the kernel of $[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ as an abelian group, for $[n]$ to belong to the image of α, the group $(\mathbb{Z}/n\mathbb{Z})^2$ needs to contain an element of order $\deg(f)$. In particular, $\deg(f)$ must divide n and the cokernel of α has cardinality at least $\deg(f)$.

This shows that

$$|\mathrm{disc}(\alpha(\mathrm{Hom}(E,E')))| = |\mathrm{disc}(\mathrm{End}(E))||\mathrm{Coker}(\alpha)|^2 \leq |\mathrm{disc}(\mathrm{End}(E))|\deg(f)^2,$$

which shows the result. □

We record a proof of the following elementary lemma without any regards for the optimality of the constants involved.

Lemma 5.2. *Let L be a rank 2 lattice with positive-definite quadratic form q and discriminant δ. Then for any positive integer n, we have*

$$|\{N \leq n \,|\, \exists\, l \in L,\, q(l) = N\}| \leq 1 + 4\sqrt{2n} + \frac{8n}{\sqrt{\delta}}$$

Proof. By an abuse of notation, we write q for both the quadratic form and the associated bilinear form. Lagrange reduction for rank 2 lattices shows that we can find a basis (e,f) for L such that $2|q(e,f)| \leq q(e) \leq q(f)$. Let a and b two integers. Then

$$q(ae+bf) = a^2q(e) + b^2q(f) + 2abq(e,f) \geq \frac{1}{2}(a^2q(e) + b^2q(f)).$$

In particular, $q(ae+bf) \leq n$ implies $a^2 q(e) \leq 2n$ and $b^2 q(f) \leq 2n$. This implies in particular that the set $\{(a,b) | q(ae+bf) \leq n\}$ has cardinality at most

$$|\{(a,b)|q(ae+bf) \leq n\}| \leq \Big(1 + \frac{2\sqrt{2n}}{\sqrt{q(e)}}\Big)\Big(1 + \frac{2\sqrt{2n}}{\sqrt{q(f)}}\Big) \leq 1 + 4\sqrt{2n} + \frac{8n}{\sqrt{q(e)q(f)}}.$$

The discriminant δ of L is

$$\delta = q(e)q(f) - q(e,f)^2 \leq q(e)q(f).$$

Since of course we have

$$|\{N \leq n | \exists\, l \in L,\, q(l) = N\}| \leq |\{(a,b)|q(ae+bf) \leq n\}|,$$

this finishes the proof. □

Putting the two lemmas above together, we find the following statement.

Proposition 5.3. *Let E and E' be two CM elliptic curves over an algebraically closed field of characteristic zero. Let δ be the discriminant of the lattice* $\mathrm{End}(E)$. *Then, for any positive integer n, we have*

$$|\{N \leq n | \exists\, \phi \in \mathrm{Hom}(E,E'),\, \deg(\phi) = N\} \leq 1 + 4\sqrt{2n} + \frac{8n}{\sqrt{\delta}}.$$

5.1. **The non-archimedean case.** We start with the case where $|.|$ is supposed to be non-archimedean, and let v be an additive valuation associated to $|.|$. Let p be the residual characteristic of v and assume that $|.|$ and v are normalized, so that $|p| = p^{-1}$ and $v(p) = 1$.

We start by discussing some deformation-theoretic results.

Let W be a complete discrete valuation subring of C, with algebraically closed residue field. Let π be a uniformizing parameter of W. If n is a nonnegative integer, let W_n be the ring $W_n = W/\pi^{n+1}$. Let e be the ramification index, so that $v(\pi) = e^{-1}$.

Let E be an elliptic curve over W. We write E_n for the reduction of E modulo π^{n+1}. Let G_n be the group

$$G_n = \mathrm{End}_{W_n}(E).$$

If $n < 0$, we write $G_n = G_0$.

As in section 4.2, we consider the sequence $(G_n)_{n \geq 0}$ as a decreasing sequence of subgroups of G_0. Write q for the positive-definite quadratic form on G_0 defined by $q(f) = \deg(f)$.

Proposition 5.4. *Let n be a nonnegative integer. The multiplication by p maps G_n into G_{n+e}, and the induced map*

$$G_n/G_{n+e} \to G_{n+e}/G_{n+2e}$$

is injective.

Proof. We reproduce an argument in the proof of [Gro86, Proposition 3.3]. Serre-Tate theory and deformation theory of formal groups shows that we have a natural injection

$$G_n/G_{n+e} \hookrightarrow H^2(\widehat{E}, (\pi^{n+1})/(p\pi^{n+1})),$$

where $\widehat{E}$ is the formal completion of E at the origin – see also [**?**, Section 2]. Now since $(p) = (\pi^e)$, multiplication by p induces an isomorphism

$$H^2(\widehat{E}, (\pi^{n+1})/(p\pi^{n+1})) \to H^2(\widehat{E}, (\pi^{n+e+1})/(p\pi^{n+2e+1})).$$

This proves the proposition by considering the commutative diagram

$$\begin{array}{ccc} G_n/G_{n+e} & \hookrightarrow & H^2(\widehat{E},(\pi^{n+1})/(p\pi^{n+1})) \\ \downarrow & & \downarrow \\ G_{n+e}/G_{n+2e} & \hookrightarrow & H^2(\widehat{E},(\pi^{n+e+1})/(p\pi^{n+2e+1})) \end{array}$$

□

While lifting endomorphisms of elliptic curves, we will consider the following property.

Definition 5.5. *Let $\alpha \notin \mathbb{Z}$ be an algebraic integer. We say that α satisfies condition (P) if the index of the ring $\mathbb{Z}[\alpha]$ in its integral closure in $\mathbb{Q}[\alpha]$ is prime to p.*

If ϕ is an endomorphism of an elliptic curve over a scheme, it makes to ask whether ϕ satisfies condition (P).

Lemma 5.6. *Let E_1 and E_2 be two elliptic curves over a field, and let $\phi : E_1 \to E_2$ be an isogeny of degree prime to p. Let α be a self-isogeny of E_1 satisfying condition (P). Then $\phi \circ \alpha \circ \widehat{\phi} : E_2 \to E_2$ satisfies condition (P).*

Proof. We have $\widehat{\phi} \circ \phi = N\mathrm{Id}_{E_1}$ and $\phi \circ \widehat{\phi} = N\mathrm{Id}_{E_2}$. As a consequence, there is an endomorphism of rings

$$\mathrm{End}(E_1) \otimes \mathbb{Z}[1/N] \to \mathrm{End}(E_2) \otimes \mathbb{Z}[1/N], x \mapsto \phi \circ x \circ \frac{1}{N}\widehat{\phi}.$$

In particular, since N is prime to p, if α satisfies condition (P), then $\frac{1}{N}\phi \circ \alpha \circ \widehat{\phi}$ does as well, and so does $\phi \circ \alpha \circ \widehat{\phi}$. □

Lemma 5.7. *Let α be an algebraic integer such that $\mathbb{Q}[\alpha]$ is an imaginary quadratic field. Let d be the discriminant of the characteristic polynomial of α, that is, $d = t^2 - 4N$, where t is the trace of α and N its norm.*

(i) Assume that p is odd. Then α satisfies condition (P) if and only if p^2 does not divide d;
(ii) Assume that $p = 2$. If α satisfies condition (P), then 16 does not divide d.

Proof. Write $d = r^2 d'$, where d' is square free and r is an integer.

If d is congruent to 1 modulo 4, then the ring of integers of $\mathbb{Q}[\alpha]$ has discriminant equals to d'. As a consequence, the index of $\mathbb{Z}[\alpha]$ in this ring of integers is equal to r. Similarly, if d' is congruent to 2 or 3 modulo 4, this index is equal to $r/2$ as the corresponding ring of integers has discriminant $4d'$. This shows the result, since the p-adic valuation of d' is at most 1. □

Lemma 5.8. *Assume that E_0 is supersingular, and let ϕ be an element of $G_n \setminus \mathbb{Z}$ for some nonnegative integer n. Write $N = q(\alpha)$. Then there exists a nonnegative integer k with $p^k \leq N$ and an element $\alpha \in G_{n-ke}$ such that the following holds*

(i) α satisfies condition (P);
(ii) $p^k \alpha \in \mathbb{Z}[\phi]$;
(iii) $q(\alpha) \leq 1 + N$.

Proof. Let $d = p^k d'$ be the index of $\mathbb{Z}[\phi]$ in its integral closure, where d' is prime to p. Since the discriminant of $\mathbb{Z}[\phi]$ is bounded above by N^2, d is bounded above by N, hence $p^k \leq N$.

Since E_0 is supersingular, its ring of endomorphisms G_0 is a maximal order in a quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. In particular, $G_0 \otimes \mathbb{Z}_p$ is the unique maximal order in the quaternion

algebra over $\mathbb{Q}_p$, so that any element of $G_0 \otimes \mathbb{Q}$ with integral norm and trace lies in $G_0 \otimes \mathbb{Z}_p$. Note that for any $\alpha \in G_0$ such that $\mathbb{Z}_p[\phi] \subset \mathbb{Z}_p[\alpha]$, α satisfies condition (P) if and only if

$$[\mathbb{Z}_p[\alpha] : \mathbb{Z}_p[\phi]] = p^k.$$

Let x be a generator of the integral closure of $\mathbb{Z}[\phi]$ in $\mathbb{Q}[\phi] \subset G_0 \otimes \mathbb{Q}$. Then $x \in G_0 \otimes \mathbb{Z}_p$. This means that there exists an integer n, prime to p, such that $\alpha := nx$ belongs to G_0. By construction, we have $\mathbb{Z}_p[\phi] \subset \mathbb{Z}_p[\alpha]$ and α satisfies condition (P), i.e.

$$[\mathbb{Z}_p[\alpha] : \mathbb{Z}_p[\phi]] = p^k.$$

Up to multiplying once again α by an integer prime to p, we may assume that $p^k\alpha$ belongs to $\mathbb{Z}[\phi]$.

For any $\beta \in \mathbb{Z}[\phi]$, we have

$$[\mathbb{Z}_p[\alpha + \beta] : \mathbb{Z}_p[\phi]] = p^k,$$

so that $\alpha + \beta$ satisfies condition (P). As a consequence, we may replace α with $\alpha + \beta$. In particular, we may assume that $\alpha = \lambda + \mu\phi$ with $0 \leq \lambda, \mu \leq 1$, so that $q(\alpha) \leq 1 + N$.

Finally, we know that $\phi \in G_n$ so that $p^k\alpha \in G_n$. Proposition 5.4 shows that $\alpha \in G_{n-ke}$. □

We now state a lifting lemma for endomorphisms satisfying condition (P).

Lemma 5.9. *For some $n \geq 4e$, let $\phi_n : E_n \to E_n$ be an isogeny satisfying condition (P). Then the pair (E_{n-4e}, ϕ_{n-4e}) lifts uniquely to a pair (E_{CM}, ϕ_{CM}) over W.*

Proof. On the tangent space $\mathrm{Lie}(E_n)$, ϕ_n induces multiplication by an element w_n in W/π^{n+1}. As an application of Lubin-Tate theory, it is proved in [GZ85, Proposition 2.7] that condition (P) guarantees[1] that the pair (E_n, ϕ_n) lifts uniquely to a pair (E_{CM}, ϕ_{CM}), where E_{CM} is an elliptic curve over W and $\phi_{CM} : E_{CM} \to E_{CM}$ is a cyclic isogeny of degree N, as soon as the equation

$$X^2 - \mathrm{Tr}(\phi_n)X + q(\phi_n) = 0$$

has a solution w in W that is congruent to w_n modulo π^{n+1}.

Lemma 5.7 shows that the discriminant $\mathrm{Tr}(\phi_n)^2 - 4q(\phi_n)$ is not divisible by p^4. Hensel's lemma as in [Eis95, Theorem 7.3] shows that there exists a solution w in W of the equation above that is congruent to w_n modulo π^{n+1-4e}. The discussion above shows that the pair (E_{n-4e}, ϕ_{n-4e}) lifts uniquely to a pair (E_{CM}, ϕ_{CM}) over W. □

As a consequence of Lemma 5.8, we deduce the following statement.

Proposition 5.10. *Assume that E_0 is supersingular. Let $n \geq 4e$ be an integer, and let $\phi_n : E_n \to E_n$ be an isogeny of degree N which is not in $\mathbb{Z}$. Let k be the largest integer with $p^k \leq N$. Then there exists an isogeny $\alpha : E_{n-ke} \to E_{n-ke}$,satisfying condition (P), such that the pair $(E_{n-(4+k)e}, \alpha_{n-(4+k)e})$ lifts uniquely to a pair (E_{CM}, ϕ_{CM}) over W. Furthermore, we can assume that α has degree at most $1 + N$.*

We give a lower bound for the distance between CM elliptic curves.

Proposition 5.11. *Let M_1 and M_2 be two positive integers. Let E_1 and E_2 be two elliptic curves over W with self-isogenies of degree M_1 and M_2 respectively, both satisfying condition (P). Assume that E_1 and E_2 are not isomorphic, and let n be a nonnegative integer such that $E_{1,n}$ and $E_{2,n}$ are isomorphic over W_n. Then*

$$p^{2n} \leq 4M_1M_2.$$

[1]The assumption in [GZ85] is actually that $\mathbb{Z}[\phi_n]$ is integrally closed in its fraction field. However, one only needs for the proof to go through that the index of $\mathbb{Z}[\phi_n]$ in its integral closure be prime to p.

Proof. Let n be the largest integer such that $E_{1,n}$ and $E_{2,n}$ are isomorphic. We can assume that $n \geq 0$, i.e., that the reductions of E_1 and E_2 modulo π are isomorphic over the field $k = W/\pi$ to the elliptic curve E/k.

If E is a CM elliptic curve, then E_1 and E_2 both are isomorphic over C to the canonical lifting of E as their endomorphisms rings have index prime to p in their algebraic closure – see for instance [Gro86, Section 2]. This is impossible since we assumed that E_1 and E_2 are not isomorphic. As a consequence, we can assume that E is a supersingular elliptic curve, and fix an isomorphism from the reduction of E_1 over W_n to that of E_2.

Let Γ_1 and Γ_2 be the formal $\mathbb{Z}_p$-modules $E_1[p^\infty]$ and $E_2[p^\infty]$ over W. If m is any positive integer, let $\mathrm{End}_m(\Gamma_i)$ be the group of endomorphisms of Γ_i over W_m for $i = 1, 2$. Choose an isomorphism $\gamma : E_{1,n} \to E_{2,n}$. Using γ, we make the identification

$$\mathrm{End}_n(\Gamma_1) = \mathrm{End}_n(\Gamma_2).$$

Now let $\mathcal{O}_i = \mathrm{End}_W(\Gamma_i)$, and let $D = \mathrm{End}_1(\Gamma_1) = \mathrm{End}_1(\Gamma_2)$. As subgroups of D, we have $\mathcal{O}_1 \neq \mathcal{O}_2$, for instance by [Gro86, Proposition 2.1]. Both $\mathcal{O}_1$ and $\mathcal{O}_2$ are saturated in D, and we have $\mathcal{O}_i\left[\frac{1}{p}\right] = \mathbb{Q}_p[\phi_i]$ for $i = 1, 2$. Since $\mathcal{O}_i$ contains the endomorphisms group of E_i, it is integrally closed.

In [Gro86], Gross computes the endomorphisms groups above and shows the equality, for any positive integer m,

$$\mathrm{End}_m(\Gamma_i) = \mathcal{O}_i + p^m D.$$

As a consequence, we have, as subgroups of D,

$$\mathcal{O}_1 + p^n D = \mathcal{O}_2 + p^n D$$

and in particular

$$\mathcal{O}_1/p^n\mathcal{O}_1 = \mathcal{O}_2/p^n\mathcal{O}_2$$

as subgroups of $D/p^n D$.

Since $\mathcal{O}_1$ and $\mathcal{O}_2$ are commutative algebras, the formula above shows that the commutator $[\phi_1, \phi_2]$ belongs to $p^n D$, so that its reduced norm if divisible by p^{2n}. However, since ϕ_2 does not belong to $\mathcal{O}_1$, it does not belong to $\mathcal{O}_1\left[\frac{1}{p}\right]$ since ϕ_2 is integral over $\mathbb{Z}_p$ and $\mathcal{O}_1$ is integrally closed in its fraction field. Since $\mathcal{O}_1\left[\frac{1}{p}\right]$ is its own commutant in the quaternion algebra $D\left[\frac{1}{p}\right]$, this means that the commutator $[\phi_1, \phi_2]$ is not zero. In particular, its reduced norm is at least p^{2n}.

Now by assumption the reduced norm of ϕ_1 (resp. ϕ_2) in D is M_1 (resp. M_2). As a consequence, the reduced norm of $[\phi_1, \phi_2]$ is at most $4M_1M_2$. Finally, we get

$$4M_1M_2 \geq p^{2n}.$$

□

Corollary 5.12. *Let E be an elliptic curve over W, and let n and N be positive integers. Assume that*

$$p^{2n} > 4N^2.$$

Then there exists at most one elliptic curve E_{CM} over W admitting an isogeny of degree at most N satisfying condition (P), and such that $E_n \simeq E_{CM,n}$.

We can now proceed to a proof of Propostion 3.3. Let us fix some notation.

Let y and z be as in Proposition 3.3. We may assume that the valuation of z is nonnegative. The assumptions on y and z ensure that we can find a complete discrete valuation ring W as above, as well as two elliptic curves E and E' over W such that $j(E) = y$ and $j(E') = z$. By assumption, E is not a CM elliptic curve.

Write once again E_n and E'_n for the reductions of E and E' modulo π^{n+1} respectively. Define $H_n = \mathrm{Hom}_{W_n}(E_n, E'_n)$, and consider $(H_n)_{n\geq 0}$ as a decreasing sequence of sublattices of H_0 endowed with quadratic form q given by the degree. Write again $G_n = \mathrm{End}_{W_n}(E_n)$, and write q for the degree quadratic form on G_n as well.

Proposition 5.13. *Assume that E_0 is a CM elliptic curve. For any nonnegative integer n, define*

$$S_n = \{N \geq 0 | \exists \phi \in \mathrm{Hom}_{W_n}(E_n, E'_n), \deg(\phi) = N\}.$$

Then the upper density of S_n tends to zero as n tends to ∞.

Proof. We may assume that E_0 and E'_0 are isogenous, so that E'_0 is CM as well.

By assumption, the lattices H_n all have rank 2. Since the two curves E and E' are not isomorphic, the intersection of the H_n is zero, so that the discriminant of the lattices H_n tends to ∞ with n. Lemma 5.2 allows us to conclude. □

Proposition 5.14. *Assume that E_0 is supersingular. Let N_1 and N_2 be two positive integers, the product of which is not a perfect square. Let n be a nonnegative integer such that there exists $\phi_1, \phi_2 \in H_n$ with $q(\phi_1) = N_1$, $q(\phi_2) = N_2$. Let k be the largest integer such that $p^k \leq N_1 N_2$.*

Then there exists a CM elliptic curve E_{CM}, together with an isogeny satisfying condition (P), of degree at most $1 + N_1 N_2$, such that $E_{CM,n-(4+k)e} \simeq E_{n-(4+k)e}$.

Proof. The composition $\phi = \widehat{\phi_1} \circ \phi_2$ is an element of G_n. We have $q(\phi) = N_1 N_2$. Since it is not a perfect square, ϕ does not belong to $\mathbb{Z}$. By Proposition 5.10 shows the result. □

Putting Proposition 5.14 and Proposition 5.11 together, we obtain the following.

Proposition 5.15. *If D is a positive integer, define*

$$S^D = \{N \in \mathbb{N} \setminus p\mathbb{N} | \exists n \geq 0, p^n \geq N^D \text{ and } \exists \phi \in H_n, q(\phi) = N\}.$$

If $D > 8 + 4e$, then the density of S^D is zero.

Proof. By Proposition 5.13, we may assume that E_0 is supersingular.

Let M be a large enough integer. We may assume that S^D contains at least two integers N_1, N_2 such that $N_1 N_2$ is not a perfect square and $\sqrt{M} \leq N_1, N_2 \leq M$. By definition, we can find $n \geq 0$ such that $p^n \geq M^{D/2}$ and $\phi_1, \phi_2 \in H_n$ with $q(\phi_1) = N_1, q(\phi_2) = N_2$. We can apply Proposition 5.14 and find an elliptic curve $E_C M$ over W such that

(i) E_{CM} admits a self-isogeny α of degree at most M^2, satisfying condition (P);
(ii) $E_{n-(4+k)e} \simeq E_{CM,n-(4+k)e}$,

where k is the largest integer such that $p^k \leq N_1 N_2$.

Note that since $D > 8 + 4e > 4 + 4e$, we have

$$p^{2(n-(4+k)e)} \geq p^{2n}(N_1 N_2)^{-2e} p^{-8e} \geq M^D M^{-8e} p^{-4e} \geq 4M^4$$

for any large enough M, which shows, via Corollary 5.12, that E_{CM} is the only elliptic curve over W satisfying the two conditions above.

We now use the curve E_{CM} to bound the cardinality of $S^D \cap \{\sqrt{M}, \ldots, M\}$. Let N be any element of $S^D \cap \{\sqrt{M}, \ldots, M\}$. By assumption, we can find n with $p^n \geq M^{D/2}$ and $\phi_N : E_n \to E'_n$ of degree N. In particular, we find an isogeny of degree N, which we denote by ϕ_N as well

$$\phi_N : E_{CM,n-(4+k)e} \to E'_{n-(4+k)e}.$$

Let K_0 be the kernel of ϕ_N. Then since N is prime to p, K_0 lifts uniquely to a subgroup K of E_{CM}. Define $E'_{CM} = E_{CM}/K$ and write ψ_N for the quotient map $\psi_N : E_{CM} \to E'_{CM}$. Then we have

(i) E'_{CM} admits a self-isogeny of degree at most M^4, satisfying condition (P);
(ii) $E'_{CM,n-(4+k)e} \simeq E'_{n-(4+k)e}$.

The second point is obvious by construction. For the first, note that

$$\widehat{\psi} \circ \alpha \circ \psi : E'_{CM} \to E'_{CM}$$

is a self-isogeny of E'_{CM} of degree at most $N^2M^2 \leq M^4$. Lemma 5.6 shows that it satisfies condition (P). Since $D > 8 + 4e$, we have once again

$$p^{2(n-(4+k)e)} \geq M^D M^{-8e} p^{-4e} \geq 4M^8,$$

for any large enough M. This shows that E'_{CM} is the only elliptic curve over W satisfying the two conditions above.

We just constructed an injective map

$$S^D \cap \{\sqrt{M}, \dots, M\} \to \mathrm{Hom}(E_{CM}, E'_{CM}), N \mapsto \psi_N$$

such that $q(\psi_N) = N$. Let δ_{CM} be the discriminant of E_{CM}. Proposition 5.3 implies the inequality

$$|S^D \cap \{1, \dots, M\}| \leq 1 + 4\sqrt{2M} + \frac{8M}{\delta_{CM}} + \sqrt{M}. \tag{5.1}$$

The elliptic curve E is not CM, and we proved $E_{n-(4+k)e} \simeq E_{CM,n-(4+k)e}$. Our assumption on D guarantees that $n - (4 + k)e$ tends to infinity with M, E_{CM} takes infinitely many values as n grows. Since there are only finitely many CM elliptic curves over C with bounded discriminant, this shows that δ_{CM} goes to infinity with n. Equation (5.1) allows us to conclude. □

Using (4.3), the previous roposition gives us the following statement, which is a more precise form of the non-archimedean part of Proposition 3.3.

Proposition 5.16. *Define $S^D_{y,z}$ as in Proposition 3.3. If $D > 12 \times (8 + 4e) = 96 + 32e$, then $S^D_{y,z}$ has density* 0.

5.2. **The archimedean case.** We now transpose the results of our preceding question to the archimedean setting, following the same strategy – the reader will compare Proposition 5.14 and Corollary 5.20, as well as Proposition 5.11 and Proposition 5.22. We work over the field of complex numbers, and let $|.|$ be the usual absolute value on $\mathbb{C}$.

We start with two elementary lemmas.

Lemma 5.17. *Let τ be an element of $\mathbb{H}$. Let N be a positive integer, and let a, b, c, d be integers with $ad - bc = N$. Let*

$$f : \mathbb{H} \to \mathbb{H}, z \mapsto \frac{az + b}{cz + d}.$$

Let Ω be a compact subset of $\mathbb{H}$. Then there exists a positive constant c_1 depending only on Ω such that

$$(\tau, f(\tau)) \in \Omega^2 \implies \mathrm{Max}(|a|, |b|, |c|, |d|) \leq c_1\sqrt{N}.$$

Proof. We keep the notations of the statement. Then, for any $\tau \in \mathbb{H}$, we have

$$\mathrm{Im} f(\tau) = \frac{N\mathrm{Im}(\tau)}{|c\tau + d|^2}.$$

As a consequence, the inequality

$$\mathrm{Im}(\tau) \geq \inf_{\tau \in \Omega} \mathrm{Im}(\tau) > 0$$

implies $|c\tau + d| \leq \lambda\sqrt{N}$ for some constant λ depending only on Ω. Since the imaginary part of τ is positive, this implies the required estimate on c, and consequently on d. Furthermore, since

$|c\tau + d| \leq \lambda\sqrt{N}$, we can find a constant μ depending only on Ω such that $|a\tau + b| \leq \mu\sqrt{N}$ as well, which provides the required estimates for a and b as well. □

Lemma 5.18. *Let us keep the notations of the previous lemma and assume $f \neq \mathrm{Id}_{\mathbb{H}}$. Then there exists positive constants ε_2, c_2 depending only on Ω, such that*

$$|\tau - f(\tau)| \leq \frac{\varepsilon_2}{N} \implies \exists\, \tau_0 \in \mathbb{H},\, f(\tau_0) = \tau_0 \text{ and } |\tau - \tau_0| \leq c_2\sqrt{N}|\tau - f(\tau)|.$$

Proof. We leave it to the reader to show that if $c = 0$ and ε_2 is chosen small enough, then there is no $\tau \in \mathbb{H}$ satisfying

$$|\tau - f(\tau)| \leq \frac{\varepsilon_2}{N}.$$

We now assume $c \neq 0$. In that case f has two fixed points in $\mathbb{C}$, τ_0 and τ_0'. We can write

$$|\tau - f(\tau)| = \frac{|c||\tau - \tau_0||\tau - \tau_0'|}{|c\tau + d|}.$$

Lemma 5.17 proves that $|c|$ and $|d|$ are bounded above by $c_1\sqrt{N}$ for some constant c_1 depending only on Ω. It is readily shown that – once again choosing ε_2 to be small enough, the existence of $\tau \in \mathbb{H}$ with

$$|\tau - f(\tau)| \leq \frac{\varepsilon_2}{N}$$

implies that τ_0 and τ_0' are complex conjugates and are not real numbers. We can assume that τ_0 is in $\mathbb{H}$. As a consequence, we have $|\tau - \tau_0'| \geq \mathrm{Im}(\tau)$. Putting these estimates together shows the result. □

Proposition 5.19. *Let y be an element of $\mathbb{C} \subset X(1)(\mathbb{C})$. Then there exist positive constants c_3 and ε_3 such that for any integer $N > 1$ and any $\alpha \in |t_{N*}y|$ such that*

$$|y - \alpha| \leq \frac{\varepsilon_3}{N},$$

there exists a CM elliptic curve E_0 over $\mathbb{C}$ with a cyclic self-isogeny of degree N such that

$$|y - j(E_0)| \leq c_3\sqrt{N}|y - \alpha|.$$

Proof. Let τ be an element of $\mathbb{H}$ with $j(\tau) = y$. Let ε, C be positive real numbers such that for any $z \in \mathbb{C} \subset X(1)(\mathbb{C})$ with $|z - y| \leq \varepsilon$, we can find τ' with $j(\tau') = z$ and

$$C^{-1}|y - z| \geq |\tau - \tau'| \geq C|y - z|.$$

The preimage of $t_{N*}y$ by j exactly the set of elements $\frac{a\tau+b}{c\tau+d} \in \mathbb{H}$, with

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}, \tag{5.2}$$

where α, β and δ are three integers with no common factor and $\alpha\delta = N$, $\alpha \geq 1$, $0 \leq \beta < \delta$.

Let us consider $\alpha \in |t_{N*}y|$ with $|y - \alpha| \leq \varepsilon_2$. We can write $\alpha = j(\frac{a\tau+b}{c\tau+d})$ with a, b, c, d as in (5.2) and $|\tau - \frac{a\tau+b}{c\tau+d}| \leq C^{-1}|y - \alpha|$. Now choose ε_2 as in Lemma 5.18 and assume that $|y - \alpha| \leq C\frac{\varepsilon}{N}$. We can find $\tau_0 \in \mathbb{H}$ such that

$$\tau_0 = \frac{a\tau_0 + b}{c\tau_0 + d} \tag{5.3}$$

and $|\tau - \tau_0| \leq C'\sqrt{N}|y - \alpha|$, where C' is a positive constant depending only on y. Since a, b, c, d are chosen as in (5.2), (5.3) shows that $j(\tau_0)$ is the j-invariant of an elliptic curve E_0 with a cyclic self-isogeny of degree N. Now writing

$$|y - j(E_0)| \leq C^{-1}|\tau - \tau_0| \leq C^{-1}C'\sqrt{N}|y - \alpha|$$

concludes the proof. □

As in the non-archimedean case, we get the following.

Corollary 5.20. *Let y and z be two elements of $\mathbb{C} \subset X(1)(\mathbb{C})$. Then there exist positive constants c_3, ε_3 such that for any two distinct positive integers $N_1, N_2 > 1$, and any $(\alpha, \beta) \in t_{N_1*}y \times t_{N_2*}y$ such that*

$$\max(|\alpha - z|, |\beta - z|) \leq \frac{\varepsilon_3}{N_1 N_2},$$

there exists a CM elliptic curve E_0 over $\mathbb{C}$ with a cyclic self-isogeny of degree at most N_1N_2 such that

$$|y - j(E_0)| \leq c_3 \sqrt{N_1 N_2} |\alpha - \beta|.$$

Proof. Since α belongs to $|t_{N_1*}y|$, y belongs to $|t_{N_1*}\alpha|$. Furthermore, since N_1 and N_2 are distinct, the elements of $|t_{N_1*}\beta|$ are all elements of some $|t_{N*}y|$ for some positive integer N with $1 < N \leq N_1N_2$.

As a consequence of Proposition 5.19, it is enough to show that, if $|\alpha - z$ and $|\beta - z|$ are smaller than a constant depending only on y and z, there exists $\beta' \in |t_{N_1*}\beta|$ such that $|y - \beta'| \leq c_3'|\alpha - \beta|$, where c_3' is a positive constant depending only on y and z.

Since y is the Hecke orbit $t_{N_1*}\alpha$, we can write $y = j(\frac{a\tau_\alpha + b}{c\tau_\alpha + d})$, where τ_α is an element of $\mathbb{H}$ with $j(\tau_\alpha) = \alpha$ and a, b, c, d are as in (5.2) – N being replaced by N_1 of course. Now we can find $\tau_\beta \in \mathbb{H}$ with $j(\tau_\beta) = \beta$ and $|\tau_\alpha - \tau_\beta| \leq C|\alpha - \beta|$ for some positive constant C depending only on z.

Since homographies preserve the hyperbolic distance on $\mathbb{H}$, the hyperbolic distance between y and $\frac{a\tau_\beta + b}{c\tau_\beta + d}$ is equal to that between α and β. Writing $\beta' = j(\frac{a\tau_\beta + b}{c\tau_\beta + d})$ and noting that the hyperbolic distance on $\mathbb{H}$ and the usual distance on $\mathbb{C} \subset X(1)(\mathbb{C})$ are equivalent via j on neighborhoods of τ and $j(\tau) = y$, this shows the inequality

$$|y - \beta'| \leq c_3'|\alpha - \beta|$$

where c_3' depends only on y and z. By construction, β' belongs to $|t_{N_1*}\beta|$, which allows us to conclude. □

Remark 5.21. *While the conclusion of Corollary 5.20 seems not to depend on z, the constants might depend on it.*

The following easy result shows that CM points of $X(1)$ cannot be too close to one another.

Proposition 5.22. *Let Ω be a compact subset of $\mathbb{C} \subset X(1)(\mathbb{C})$. Let $M_1, M_2 > 1$ be two integers, and let E_1, E_2 be two CM elliptic curves over $\mathbb{C}$ with cyclic self-isogenies of degree M_1 and M_2 respectively. Assume that $j(E_1)$ and $j(E_2)$ belong to Ω. If E_1 and E_2 are not isomorphic, then*

$$|j(E_1) - j(E_2)| \geq c_4 (M_1 M_2)^{-1},$$

where c_4 is a positive constant depending only on the compact set Ω.

Proof. As before, and since we are working over a compact set, we only have to prove that if Ω is any compact subset of $\mathbb{H}$, then for any $\tau_1, \tau_2 \in \Omega$ such that $j(\tau_i) = j(E_i)$ for $i = 1, 2$, we have

$$|\tau_1 - \tau_2| \geq C(M_1 M_2)^{-1/2} (\sqrt{M_1} + \sqrt{M_2})^{-1}$$

for some positive constant C depending only on the compact set Ω.

Since E_1 has a cyclic self-isogeny of degree M_1, we have

$$\tau_1 = \frac{\alpha_1 \tau_1 + \beta_1}{\gamma_1 \tau_1 + \delta_1},$$

where the matrix

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z})$$

has determinant M_1 and is not a homothety. In particular, $\gamma_1 \neq 0$. By Lemma 5.17, $|\gamma_1|$ is bounded above by $K_1\sqrt{M_1}$, where the positive constant K_1 only depends on the compact set Ω. Now we can write

$$\tau_1 = \frac{\alpha_1 - \delta_1 + i\sqrt{\Delta_1}}{2\gamma_1},$$

with $\Delta_1 = 4M_1 - (\alpha_1 + \delta_1)^2 \leq 4M_1$. Computing τ_2 the same way, we find

$$|\tau_1 - \tau_2| \geq |\mathrm{Im}(\tau_1) - \mathrm{Im}(\tau_2)| = \Big|\frac{\sqrt{\Delta_1}}{2\gamma_1} - \frac{\sqrt{\Delta_2}}{2\gamma_2}\Big|,$$

where Δ_1, Δ_2 are positive integers bounded above by $4M_1$ and $4M_2$ respectively, and, by Lemma 5.17, γ_1 and γ_2 are integers whose absolute value is bounded above by $c_1\sqrt{M_1}$ and $c_1\sqrt{M_2}$ respectively, for some positive constant c_1 depending only on Ω.

We can write

$$|\tau_1 - \tau_2| \geq \frac{\gamma_2\sqrt{\Delta_1} - \gamma_1\sqrt{\Delta_2}}{2\gamma_1\gamma_2} \geq \frac{1}{2\gamma_1\gamma_2(\gamma_2\sqrt{\Delta_1} + \gamma_1\sqrt{\Delta_2})} \geq (4c_1^4 M_1 M_2)^{-1}.$$

Note indeed that $|\sqrt{a} - \sqrt{b}| \geq \frac{1}{\sqrt{a}+\sqrt{b}}$ for any two distinct positive integers a and b. □

Putting the estimates of Corollary 5.20 and Proposition 5.22 together, we obtain the following statement, analogous to Proposition 5.15.

Proposition 5.23. *Let D be a positive integer and y, z points in $\mathbb{C} \subset X(1)(\mathbb{C})$. Define*

$$S_{y,z}^D = \{N \in \mathbb{N} | \exists\, \alpha \in |t_{N*}y|, |\alpha - z| \leq N^{-D}\}.$$

Assume that y is not the j-invariant of a CM elliptic curve. Then for $D \geq 20$, $S_{y,z}^D$ has density zero.

Proof. Let M be a large enough integer. Fix y and z as above. We can assume that there exists two distinct integers $N_1, N_2 \in S_{y,z}^D$ with $\sqrt{M} \leq N_1, N_2 \leq M$. We get elements $\alpha \in t_{N_1*}y$ and $\beta \in t_{N_2*}y$ with

$$|\alpha - z| \leq N_1^{-D} \leq n^{-D/2},\ |\beta - z| \leq N_2^{-D} \leq M^{-D/2}.$$

In particular, we have $|\alpha - \beta| \leq 2M^{-D/2}$. Since $D/2 > 2$, Corollary 5.20 shows that we can find an elliptic curve E_{CM} with a cyclic self-isogeny of degree at most n^2 such that

$$|y - j(E_{CM})| \leq c_3 M^{1-D/2} \tag{5.4}$$

for some positive constant c_3. Since $1 - D/2 < -4$, Proposition 5.22 shows that E_{CM} is uniquely defined.

We now use the curve E_{CM} to bound the cardinality of $S_{y,z}^D \cap \{1, \ldots, M\}$. Let N be any element of $S_{y,z}^D$ with $\sqrt{M} \leq N \leq M$. By assumption, there exists an element α_N of $|t_{N*}y|$ such that $|\alpha_N - z| \leq M^{-D/2}$. Write $y = j(\tau_y)$. We can find a homography $f : \tau \mapsto \frac{a\tau+b}{c\tau+d}$ such that $\alpha_N = j(f(\tau_y))$ and $ad - bc = N$. Applying Lemma 5.17 with a compact neighborhood of a given preimage τ_z of z by j, we find a constant c_1 such that $|a|, |b|, |c|, |d|$ are bounded above by $c_1\sqrt{n}$.

Using (5.4), we can find an element τ_{CM} of $\mathbb{H}$ such that

$$|\tau_{CM} - \tau_y| \leq C_3 M^{1-D/2}$$

for some positive constant C_3. Let $\tau' = f(\tau_{CM})$ and let E'_{CM} be the corresponding elliptic curve. Then the bound on the coefficients of f guarantees the inequality

$$|j(\tau') - z| \leq K\sqrt{M}M^{1-D/2} = KM^{(3-D)/2}$$

for some positive constant K.

At that point, we copy the end of the proof of Proposition 5.15. By construction, E'_{CM} is a CM elliptic curve with a cyclic isogeny

$$\psi_N : E_{CM} \to E'_{CM}$$

of degree N. Let $\alpha : E_{CM} \to E_{CM}$ be a cyclic self-isogeny of degree at most n^2. We get a self-isogeny

$$\psi_N \circ \alpha \circ \widehat{\psi_N} : E'_{CM} \to E'_{CM}$$

of degree $N^2\deg(\alpha)$. In particular, E'_{CM} admits a cyclic self-isogeny of degree at most M^4. Again, since $(3-D)/2 < -8$, Proposition 5.22 shows that E'_{CM} is determined by this last condition – in particular, it is independent of $N \in S^D_{y,z} \cap \{\sqrt{M}, \dots, M\}$.

We just constructed an injective map

$$S^D_{y,z} \cap \{\sqrt{M}, \dots, M\} \to \mathrm{Hom}(E_{CM}, E'_{CM}), N \mapsto \psi_N$$

such that $q(psi_N) = N$. Let δ_{CM} be the discriminant of E_{CM}. Proposition 5.3 implies the inequality

$$|S^D_{y,z} \cap \{1, \dots, M\}| \leq 1 + 4\sqrt{2M} + \frac{8M}{\delta_{CM}} + \sqrt{M}. \tag{5.5}$$

Since y is not the j-invariant of a CM elliptic curve, the estimate (5.4) and Proposition 5.22 imply that E_{CM} takes infinitely many values as n grows. Since there are only finitely many CM elliptic curves over $\mathbb{C}$ with bounded discriminant, this shows that δ_{CM} goes to infinity with n. Equation (5.5) allows us to conclude. □

References

[Aut03] P. Autissier. Hauteur des correspondances de Hecke. *Bull. Soc. Math. France*, 131(3):421–433, 2003.

[BKPSB98] R. Borcherds, L. Katzarkov, T. Pantev, and N. Shepherd-Barron. Families of K3 surfaces. *J. Algebr. Geom.*, 7:183–193, 1998.

[BLGG11] Thomas Barnet-Lamb, Toby Gee, and David Geraghty. The Sato-Tate conjecture for Hilbert modular forms. *J. Amer. Math. Soc.*, 24(2):411–469, 2011.

[BLGGT14] Thomas Barnet-Lamb, Toby Gee, David Geraghty, and Richard Taylor. Potential automorphy and change of weight. *Ann. of Math. (2)*, 179(2):501–609, 2014.

[BLGHT11] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of Calabi-Yau varieties and potential automorphy II. *Publ. Res. Inst. Math. Sci.*, 47(1):29–98, 2011.

[Bos99] J.-B. Bost. Potential theory and Lefschetz theorems for arithmetic surfaces. *Ann. Scient. Éc. Norm. Sup.*, 32:241–312, 1999.

[CHT08] L. Clozel, M. Harris, and R. Taylor. Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations. *Publ. Math. Inst. Hautes Études Sci.*, (108):1–181, 2008. With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras.

[CO06] C.-L. Chai and F. Oort. Hypersymmetric abelian varieties. *Pure Appl. Math. Q.*, 2(1, Special Issue: In honor of John H. Coates. Part 1):1–27, 2006.

[Coh84] P. Cohen. On the coefficients of the transformation polynomials for the elliptic modular function. *Math. Proc. Cambridge Philos. Soc.*, 95(3):389–402, 1984.

[Con04] B. Conrad. Gross-Zagier revisited. In *Heegner points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 67–163. Cambridge Univ. Press, Cambridge, 2004. With an appendix by W. R. Mann.

[COU01] L. Clozel, H. Oh, and E. Ullmo. Hecke operators and equidistribution of Hecke points. *Invent. Math.*, 144(2):327–351, 2001.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[Eis95] D. Eisenbud. *Commutative algebra, with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[Elk89] N. Elkies. Supersingular primes for elliptic curves over real number fields. *Compositio Mathematica*, 72(2):165–172, 1989.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[Gro86] B. H. Gross. On canonical and quasicanonical liftings. *Invent. Math.*, 84(2):321–326, 1986.

[GZ85] B. H. Gross and D. B. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985.

[GZ86] B. H. Gross and D. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[Har09] Michael Harris. Potential automorphy of odd-dimensional symmetric powers of elliptic curves and applications. In *Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. II*, volume 270 of *Progr. Math.*, pages 1–21. Birkhäuser Boston, Inc., Boston, MA, 2009.

[HSBT10] M. Harris, N. Shepherd-Barron, and R. Taylor. A family of Calabi-Yau varieties and potential automorphy. *Ann. of Math. (2)*, 171(2):779–813, 2010.

[LT76] S. Lang and H. Trotter. *Frobenius distributions in* GL_2*-extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[Ogu03] K. Oguiso. Local families of K3 surfaces and applications. *J. Alg. Geom.*, 12(3):405–433, 2003.

[Sil90] Joseph H. Silverman. Hecke points on modular curves. *Duke Math. J.*, 60(2):401–423, 1990.

[Tat66] J. Tate. Endomorphisms of Abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[Tay08] R. Taylor. Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations. II. *Publ. Math. Inst. Hautes Études Sci.*, (108):183–239, 2008.

[Voi02] C. Voisin. *Théorie de Hodge et géométrie algébrique complexe*, volume 10 of *Cours Spécialisés*. Société Mathématique de France, Paris, 2002.

François Charles, Laboratoire de mathématiques d'Orsay, UMR 8628 du CNRS, Université Paris-Sud, Bâtiment 425, 91405 Orsay cedex, France

E-mail address: francois.charles@math.u-psud.fr