INDEPENDENCE OF POINTS ON ELLIPTIC CURVES ARISING FROM SPECIAL POINTS ON MODULAR AND SHIMURA CURVES, I: GLOBAL RESULTS

ALEXANDRU BUIUM AND BJORN POONEN

to Ken Ribet on his 60^{th} birthday

Abstract. Given a correspondence between a modular curve S and an elliptic curve A, we prove that the intersection of any finite-rank subgroup of A with the set of points on A corresponding to CM-points on S is finite. We prove also a version in which S is replaced by a Shimura curve and A is replaced by a higher-dimensional abelian variety.

This article has been published in *Duke Math. J.* **147** (2009), no. 1, 181–191.

1. Introduction

1.1. **CM-points mapping into a finite rank subgroup.** Let $N \in \mathbf{Z}$ satisfy $N > 3$. Let $X_1(N)$ over $\overline{\mathbf{Q}}$ be the complete modular curve attached to the group $\Gamma_1(N)$. If $Y_1(N) \subset X_1(N)$ is the non-cuspidal locus then $Y_1(N)(\overline{\mathbf{Q}})$ is in bijection with the set of isomorphism classes of pairs (E, α) where E is an elliptic curve over $\overline{\mathbf{Q}}$ and $\alpha\colon \mathbf{Z}/N\mathbf{Z} \hookrightarrow E(\overline{\mathbf{Q}})$ is an injection. A CM-*point* on the curve $X_1(N)$ is a point in $Y_1(N)(\overline{\mathbf{Q}})$ represented by a pair (E, α) such that E has complex multiplication, i.e., $\mathrm{End}(E) \neq \mathbf{Z}$. Let $\mathrm{CM} \subset X_1(N)(\overline{\mathbf{Q}})$ be the set of CM-points. Say that an abelian group Γ is of *finite rank* if $\dim_{\mathbf{Q}}(\Gamma \otimes_{\mathbf{Z}} \mathbf{Q}) < \infty$. We prove that the images of CM-points in any elliptic curve A are mostly independent in $A(\overline{\mathbf{Q}})$:

Theorem 1.1. *Let A be an elliptic curve over $\overline{\mathbf{Q}}$. Let $\Phi\colon X_1(N) \to A$ be a non-constant morphism. Let $\Gamma \leq A(\overline{\mathbf{Q}})$ be a finite rank subgroup. Then $\Phi(\mathrm{CM}) \cap \Gamma$ is finite.*

In fact, we extend Theorem 1.1 in various directions. First, we can replace the morphism Φ by a *correspondence* between $X_1(N)$ and A. Second, we can replace A by a higher-dimensional abelian variety. Third, we can "fatten" Γ in the style of [20] by replacing Γ by $\Gamma + B_\epsilon$ where B_ϵ is a set of points of small Néron-Tate height. Fourth, we can prove variants where $X_1(N)$ is replaced by a Shimura curve. For all of these, see Section 2.

1.2. **Previous work.** Most previous work on problems related to this paper concerned Heegner points, which are certain special points in $\Phi(\mathrm{CM})$ for a morphism $\Phi\colon X_1(N) \to A$. The study of the linear dependences among Heegner points (and their traces) plays an important role in work on the Birch and Swinnerton-Dyer conjecture, especially in the breakthroughs by Gross-Zagier [10] and Kolyvagin [13]. See [7] for an exposition of this circle of ideas. See also [18, 24, 6] for more recent advances, especially in relation to Mazur's conjectures

Date: October 5, 2008.

2000 *Mathematics Subject Classification.* 11G18, 14G20.

Key words and phrases. modular curve, Shimura curve, CM point.

in [14]. In particular, [18] proved that there are only finitely many torsion Heegner points on any elliptic curve over $\mathbf{Q}$. Along slightly different lines it was recently proved in [21] that if $Q_1, \ldots, Q_s$ are Heegner points associated to distinct quadratic imaginary fields and if the odd parts of the class numbers of these fields are sufficiently large then $Q_1, \ldots, Q_s$ are linearly independent. Recall that, by the classical theory of complex multiplication, the set of all points in CM defined over a given number field is finite; this, together with the Hermite-Minkowski theorem, implies that $\Phi(\mathrm{CM}) \cap \Gamma$ is finite for any finitely generated $\Gamma \leq A(\overline{\mathbf{Q}})$. In contrast, our finiteness results allow Γ to have points of unbounded degree (by Northcott's theorem, this is always the case if Γ contains an infinite set of bounded height, for instance an infinite set of torsion points).

Pink has formulated and proved some results toward a conjecture combining the Mordell-Lang and André-Oort conjectures [19]. Our Theorem 2.1 may also be seen as combining the Mordell-Lang conjecture with the André-Oort conjecture (the latter appears only in a trivial case, however, since we consider only 1-dimensional Shimura varieties). But as far as we can tell, Pink's conjecture, even if fully proved, would not imply any of our results: his conjecture concerns subvarieties of mixed Shimura varieties such as the universal family of abelian varieties over some Shimura variety, whereas our Theorem 2.1 concerns subvarieties of the product of a Shimura curve (a modular curve) with an abelian variety where the abelian variety is not required to bear any relationship to the Shimura curve.

Finally we mention [22, Theorem 1.1], which gives an estimate for the average height of the points in the image of a Hecke correspondence T_m applied to a point of a modular curve; see also [1] for a stronger version of this result. The estimate grows with m, so at least one of the points in the image must be non-torsion; if moreover these points are Galois conjugates (as is true for large prime m if they are not CM, as pointed out in the proof of [22, Corollary 0.3]), then all are non-torsion.

1.3. **Structure of the paper.** Section 2 states all our variants of Theorem 1.1, and Section 3 proves them. We use methods quite different from those used in the papers mentioned in Section 1.2: our proofs rely on the fact that the limit measure promised by equidistribution results for Galois orbits in abelian varieties is incompatible with the limit measure in equidistribution results for modular curves and Shimura curves.

1.4. **The sequel to this paper.** In [4], we prove "local" versions of these results, in which $\overline{\mathbf{Q}}$ is replaced by the completion of the maximal unramified extension of the ring $\mathbf{Z}_p$ of p-adic integers, and CM is replaced by the subset CL of canonical lift points. Although these substitutions would appear to give a weaker statement, there are also several advantages:

(1) We obtain effective bounds for the size of the intersection.
(2) The results remain valid for certain Γ of infinite rank.
(3) The method applies also to prove results where CM is replaced by a (partial) isogeny class of points in the modular or Shimura curve.

The proofs in [4] use arguments very different from those in this paper: they involve the theory of arithmetic differential equations in the sense of [3].

Acknowledgments. While writing this paper the authors were partially supported by NSF grants: the first author by DMS-0552314, and the second author by DMS-0301280 and DMS-0841321. We are indebted to M. Christ, M. Kim, J. H. Silverman, P. Vojta, and

J. F. Voloch for their remarks and suggestions. We thank also W. Duke, P. Michel, and S. Zhang for discussing equidistribution of CM-points. Finally we thank the referees for several helpful comments.

2. Variants

2.1. **Modular curves and higher-dimensional abelian varieties.** By *variety*, we mean a separated scheme of finite type over a field. By a *coset* in an abelian variety A over an algebraically closed field, we mean a translate of an abelian subvariety of A.

Theorem 2.1. *Let $S = X_1(N)$ over $\overline{\mathbf{Q}}$ for some $N \geq 1$. Let A be an abelian variety over $\overline{\mathbf{Q}}$. Let X be a closed irreducible subvariety of $S \times A$. Let $\Gamma \leq A(\overline{\mathbf{Q}})$ be a finite-rank subgroup. If $X(\overline{\mathbf{Q}}) \cap (\mathrm{CM} \times \Gamma)$ is Zariski dense in X, then $X = S' \times A'$ where S' is a subvariety of S and A' is a coset in A.*

If in Theorem 2.1 we drop the assumption that $X(\overline{\mathbf{Q}}) \cap (\mathrm{CM} \times \Gamma)$ is Zariski dense in X, we can apply Theorem 2.1 to the irreducible components of the Zariski closure of $X(\overline{\mathbf{Q}}) \cap (\mathrm{CM} \times \Gamma)$ to deduce the following equivalent form of Theorem 2.1.

Theorem 2.2. *Let S, A, Γ be as in Theorem 2.1. Let X be a closed subvariety of $S \times A$. Then the intersection $X(\overline{\mathbf{Q}}) \cap (\mathrm{CM} \times \Gamma)$ is contained in a subvariety $Z \subsetneq X$ that is a finite union of products $S' \times A'$ where each S' is a subvariety of S and each A' is a coset in A.*

We can actually strengthen Theorem 2.1, as [20] strengthened the Mordell-Lang conjecture, by fattening Γ as follows. Let $h\colon A(\overline{\mathbf{Q}}) \to \mathbf{R}_{\geq 0}$ be a canonical height function attached to some symmetric ample line bundle on A. For $\Gamma \leq A(\overline{\mathbf{Q}})$ and $\epsilon \geq 0$, let

$$\Gamma_\epsilon := \{\, \gamma + a \mid \gamma \in \Gamma, a \in A(\overline{\mathbf{Q}}), h(a) \leq \epsilon \,\}.$$

Theorem 2.3. *Assume that S, A, X, Γ are as in Theorem 2.1. If $X(\overline{\mathbf{Q}}) \cap (\mathrm{CM} \times \Gamma_\epsilon)$ is Zariski dense in X for every $\epsilon > 0$, then $X = S' \times A'$ where S' is a subvariety of S and A' is a coset in A.*

Just as Theorem 2.1 implied Theorem 2.2, Theorem 2.3 implies the following more general (but equivalent) version of itself:

Theorem 2.4. *Assume that S, A, Γ are as in Theorem 2.3. Let X be a closed subvariety of $S \times A$ defined over $\overline{\mathbf{Q}}$. Then for some $\epsilon > 0$, the intersection $X(\overline{\mathbf{Q}}) \cap (\mathrm{CM} \times \Gamma_\epsilon)$ is contained in a subvariety $Z \subsetneq X$ that is a finite union of products $S' \times A'$ where each S' is a subvariety of S and each A' is a coset in A.*

2.2. **Shimura curves.** Let D be a non-split indefinite quaternion algebra over $\mathbf{Q}$. Fix a maximal order $\mathcal{O}_D$ once and for all. Let $X^D(\mathcal{U})$ be the Shimura curve attached to the pair $(D, \mathcal{U})$, where $\mathcal{U}$ is a sufficiently small compact subgroup of $(\mathcal{O}_D \otimes (\varprojlim \mathbf{Z}/m\mathbf{Z}))^\times$ such that $X^D(\mathcal{U})$ is connected: see [5, 27]. A *fake elliptic curve*[1] is a pair (E, i) consisting of an abelian surface E over $\overline{\mathbf{Q}}$ and an embedding $i\colon \mathcal{O}_D \to \mathrm{End}(E)$. The set $X^D(\mathcal{U})(\overline{\mathbf{Q}})$ is in bijection with the set of isomorphism classes of fake elliptic curves equipped with a level $\mathcal{U}$ structure in the sense of [5, 27].

The classification of endomorphism algebras [16, p. 202] shows that for any fake elliptic curve (E, i), the algebra $(\mathrm{End}\, E) \otimes \mathbf{Q}$ is isomorphic to either D or $D \otimes \mathcal{K} \simeq M_2(\mathcal{K})$ for some

[1] In the literature this is sometimes called a "false elliptic curve".

imaginary quadratic field $\mathcal{K}$ embeddable in D. In the latter case, (E, i) is called *CM*; then E is isogenous to the square of an elliptic curve with CM by an order in $\mathcal{K}$. A *CM-point* of $S(\overline{\mathbf{Q}})$ is a point whose associated (E, i) is CM. Let $\mathrm{CM} \subset S(\overline{\mathbf{Q}})$ be the set of CM-points on S.

Theorem 2.5. *Let $S = X^D(\mathcal{U})$ over $\overline{\mathbf{Q}}$, let A be an abelian variety over $\overline{\mathbf{Q}}$, and let $\Phi\colon S \to A$ be a morphism. Let $\Gamma \leq A(\overline{\mathbf{Q}})$ be a finite-rank subgroup. Then $\Phi(\mathrm{CM}) \cap \Gamma$ is finite.*

Finally, we can again fatten Γ:

Theorem 2.6. *In the notation of Theorem 2.5, there exists $\epsilon > 0$ such that $\Phi(\mathrm{CM}) \cap \Gamma_\epsilon$ is finite.*

Theorems 2.3 and 2.6 imply Theorem 1.1 and all the other results in this section, so we focus on them.

3. Proofs

We begin with Theorem 2.3; for its proof we need some measure-theoretic prerequisites.

Lemma 3.1. *Let S be a smooth projective curve over $\mathbf{C}$. Let X be a (possibly singular) closed N-dimensional subvariety of $\mathbf{P}^n_{\mathbf{C}}$. Let $\pi\colon X \to S$ be a morphism. Let $s \in S(\mathbf{C})$. Equip $S(\mathbf{C})$ and $\mathbf{P}^n(\mathbf{C})$ with real analytic Riemannian metrics. Let B_r be the open disk in S with center s and radius r, and let $B'_r = B_r - \{s\}$. Then there exists $\delta > 0$ such that the N-dimensional volume of $\pi^{-1}(B'_r)$ with respect to the metric on $\mathbf{P}^n(\mathbf{C})$ is $O(r^\delta)$ as $r \to 0$.*

Proof. Irreducible components of X having dimension less than N have zero N-dimensional volume, so we may reduce to the case in which X is irreducible of dimension N.

Define $\Delta := \{z \in \mathbf{C} : |z| < 1\}$ and $\blacktriangle := \{z \in \mathbf{C} : |z| \leq 1/2\}$. Let $g_{\mathbf{P}}$ and g_S be the given metrics on $\mathbf{P}^n(\mathbf{C})$ and $S(\mathbf{C})$. Let μ be Lebesgue measure on $\mathbf{C}^N$. Fix a holomorphic chart $\iota_S\colon \Delta \to S(\mathbf{C})$ mapping 0 to s.

We may assume that $\dim \pi^{-1}(s) < N$. By work of Hironaka, there exists a desingularization $p\colon Y \to X$ (see [12, Corollary 3.22]) and we may assume that the fiber of the map $f := \pi \circ p\colon Y \to S$ above s is a simple normal crossing divisor (see [12, Theorem 3.21]). Then for each $y \in f^{-1}(s)$, there exists a holomorphic chart $\iota_Y\colon \Delta^N \to Y(\mathbf{C})$ mapping 0 to y such that f is given with respect to ι_Y and ι_S by

$$h\colon \Delta^N \to \Delta$$
$$z = (z_1, \ldots, z_N) \mapsto u(z) z_1^{e_1} \cdots z_N^{e_N}$$

for some nonvanishing holomorphic function $u\colon \Delta^N \to \mathbf{C}$ and $e_i \in \mathbf{Z}_{\geq 0}$. By compactness, there exist $\varepsilon > 0$ and finitely many ι_Y such that the sets $\iota_Y(\blacktriangle^N)$ cover $f^{-1}(B_\varepsilon)$.

Since $\blacktriangle$ is compact, $(\iota_S^* g_S)|_{\blacktriangle}$ is bounded above and below by positive constants times the standard metric. Similarly, the pullback of $g_{\mathbf{P}}$ to $\blacktriangle^N$ is bounded above in terms of the standard metric. Thus we reduce to showing that for each ι_Y, there exists $\delta > 0$ such that

$$\mu\left(\{z \in \blacktriangle^N : |h(z)| < r\}\right) = O(r^\delta)$$

as $r \to 0$.

Let $u_{\min} := \inf\{|u(z)| : z \in \blacktriangle^N\} > 0$. We may assume that $r < u_{\min}$. Fix $E > \sum e_i$. Let $\rho := (r/u_{\min})^{1/E} < 1$. If $|z_i| \geq \rho$ for all i, then $|h(z)| \geq u_{\min} \rho^E = r$. Thus

$$\{z \in \blacktriangle^N : |h(z)| < r\} \subseteq \{z \in \blacktriangle^N : |z_i| < \rho \text{ for some } i\}.$$

The volume of the latter is $O(\rho^2) = O(r^{2/E})$ as $r \to 0$. $\square$

Lemma 3.2. *Let Y, H be varieties over $\mathbf{C}$, with Y proper. Let X be a closed subvariety of $Y \times H$. Let (h_i) be a sequence in $H(\mathbf{C})$ converging to h_∞. For $i \leq \infty$, let X_i be the fiber of $X \to H$ above h_i. View X_i as a subvariety of Y. Then any open neighborhood N of $X_\infty(\mathbf{C})$ in the complex topology contains $X_i(\mathbf{C})$ for all sufficiently large i.*

Proof. The open set $((Y \times H) - X)(\mathbf{C}) \cup (N \times H(\mathbf{C}))$ contains $Y(\mathbf{C}) \times \{h_\infty\}$, so it contains also $Y(\mathbf{C}) \times U$ for some open neighborhood U of h_∞ in H, by the "tube lemma for compact spaces" (Lemma 5.8 on p. 169 of [17]). For large i, we have $h_i \in U$, and then $X_i(\mathbf{C}) \subseteq N$. $\square$

From now on, we assume that $S = X_1(N)$ as in Theorem 2.3. Let $\mathcal{H} := \{\tau \in \mathbf{C} : \operatorname{Im} \tau > 0\}$, and let $\mathcal{H}^* := \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$, so $S(\mathbf{C}) = \Gamma_1(N) \backslash \mathcal{H}^*$. Let $\infty_S \in S(\mathbf{C})$ be the image of the cusp $\infty \in \mathbf{P}^1(\mathbf{Q}) \subset \mathcal{H}^*$. Choose a real analytic Riemannian metric on $S(\mathbf{C})$. Define B_r to be the open disk in $S(\mathbf{C})$ with center ∞_S and radius r with respect to the metric. Let $\mu_{\mathcal{H}}$ be the probability measure on $S(\mathbf{C})$ whose pullback to $\mathcal{H}$ equals a multiple of the hyperbolic measure $\frac{dx\,dy}{y^2}$.

We next show that $\mu_{\mathcal{H}}$ blows up relative to the Riemannian metric near the cusp ∞_S. (The Riemannian volume of B_r is only $O(r^2)$ as $r \to 0$.)

Lemma 3.3. *There exists $u > 0$ such that for all sufficiently small $r > 0$, we have $\mu_{\mathcal{H}}(B_r) > u/\log(1/r)$.*

Proof. Let τ be the usual parameter on $\mathcal{H}$. Then $q := e^{2\pi i \tau}$ is an analytic uniformizer at $\infty_S \in S(\mathbf{C})$ (defined on some neighborhood of ∞_S) because the subgroup of $\Gamma_1(N) \subseteq \mathrm{PSL}_2(\mathbf{Z})$ stabilizing $\infty \in \mathcal{H}^*$ is generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. So there exists $c > 0$ such that for all sufficiently small r, in the fundamental domain in $\mathcal{H}$, the part corresponding to B_r contains the part where $|q| < cr$. The inequality $|q| < cr$ is equivalent to $\operatorname{Im}(\tau) > \frac{1}{2\pi} \log(1/(cr))$, so $\mu_{\mathcal{H}}(B_r)$ is at least a constant times $1/\log(1/(cr))$ for sufficiently small r. If u is small enough, this exceeds $u/\log(1/r)$ for all sufficiently small r. $\square$

We will need also an equidistribution result for CM points. The first such equidistribution result was proved in [8], and this has been generalized in several directions by several authors: see Section 5.4 of the survey paper [15], for instance. The version we use is a special case of a result in [28].

Lemma 3.4. *Let k be a finite extension of $\mathbf{Q}$. Fix an embedding $\overline{k} \hookrightarrow \mathbf{C}$. Let S be a modular curve $X_1(N)$ or a Shimura curve $X^D(\mathcal{U})$ over $\overline{k}$. Let (x_i) be an infinite sequence of distinct* CM*-points in $S(\overline{k})$. The uniform probability measure on the* $\mathrm{Gal}(\overline{k}/k)$*-orbit of x_i converges weakly as $i \to \infty$ to the measure $\mu_{\mathcal{H}}$ on $S(\mathbf{C})$.*

Proof. This follows from Corollary 3.3 of [28]. Namely, we choose $\delta < 1/2$ as on p. 3663 of [28], choose $\epsilon > 0$ so that $\delta/2 + 1/4 + \epsilon < 1/2$, and define the "CM-suborbit" $O(x_i)$ as the $\mathrm{Gal}(\overline{k}/k)$-orbit of x_i. The hypothesis of Corollary 3.3 of [28] is satisfied, by the Brauer-Siegel theorem (see the first remark following Corollary 3.3 of [28]). $\square$

Proof of Theorem 2.3. Let A' be the image of $X \to A$. By Corollary 9 of [20] (also proved partially independently as Theorem 1.2 of [26]) applied to $A' \subseteq A$, we have that A' is a coset. We may translate to assume that A' is an abelian subvariety, and hence reduce to the case

where $X \to A$ is surjective. We may assume also that $X \to S$ is surjective, since $\dim S = 1$. We want $X = S \times A$. Suppose not. Then $X \to A$ is generically finite, say of degree d.

The group Γ is contained in the division hull of a finitely generated group Γ_0. Choose a number field $k \subset \overline{\mathbf{Q}}$ such that A, S, X are all defined over k and $\Gamma_0 \leq A(k)$.

Since $X(\overline{\mathbf{Q}}) \cap (\mathrm{CM} \times \Gamma_\epsilon)$ is Zariski dense in X for every $\epsilon > 0$, and since X has only countably many subvarieties, we may choose a generic infinite sequence of points $x_i = (s_i, a_i) \in X(\overline{\mathbf{Q}})$ with $s_i \in \mathrm{CM}$ and $a_i \in \Gamma_{\epsilon_i}$ where $\epsilon_i \to 0$. ("Generic" means that each proper subvariety of X contains at most finitely many x_i.) In particular, each s_i appears only finitely often. Since class numbers of imaginary quadratic fields tend to infinity, we have $[k(s_i) : k] \to \infty$. So $[k(x_i) : k] \to \infty$. For all but finitely many i, the a_i lie in the open locus above which the fibers of $X \to A$ have size d, and then $[k(x_i) : k] \leq d[k(a_i) : k]$. Thus $[k(a_i) : k] \to \infty$.

The a_i form a sequence of almost division points relative to k in the sense of [26]. By passing to a subsequence we may assume that they have a coherent limit $(C, b + T)$ in the sense of [26], where C is an abelian subvariety of A, and $b \in A(\mathbf{C})/C(\mathbf{C})$, and T is a finite set of torsion points of A/C. Since $[k(a_i) : k] \to \infty$, we have $\dim C > 0$ by definition of coherent limit. By replacing X by its image under $S \times A \xrightarrow{(\mathrm{id},\phi)} S \times \tilde{A}$ for a suitable isogeny $\phi\colon A \to \tilde{A}$, we may reduce to the case where $T = \{0\}$ and $A \simeq B \times C$ for some abelian subvariety B of A. Identify A/C with B. Write $a_i = (b_i, c_i)$ with $b_i \in B(\overline{\mathbf{Q}})$ and $c_i \in C(\overline{\mathbf{Q}})$. By definition of T, we have $b_i \in B(k)$. By Theorem 1.1 of [26], the uniform probability measure on the orbit $\mathrm{Gal}(\overline{k}/k)a_i$ (supported on $\{b_i\} \times C(\mathbf{C})$) converges weakly as $i \to \infty$ to the $C(\mathbf{C})$-invariant probability measure on $\{b\} \times C(\mathbf{C})$. So the uniform probability measure on $\mathrm{Gal}(\overline{k}/k)c_i$ converges to Haar measure μ_C on $C(\mathbf{C})$.

For each i, let X_{b_i} be the fiber of the projection $X \to B$ above b_i, viewed as a subvariety of $S \times C$. Since the b_i are generic in B, we may pass to a subsequence to assume that the X_{b_i} have the same Hilbert polynomial (with respect to some embedding $S \times C \hookrightarrow \mathbf{P}^N$) and that the corresponding points of the Hilbert scheme H converge in the complex topology; let $X_{b_\infty} \subseteq S \times C$ be the closed subscheme corresponding to the limit. We have $\dim X_{b_i} < \dim(S \times C)$ for all finite i (and hence also for $i = \infty$), since otherwise by genericity of the b_i, we would have $X = S \times B \times C = S \times A$.

Let $\pi_C\colon S \times B \times C \to C$ be the projection. Also, for $i \leq \infty$, let $\pi_{S,i}\colon X_{b_i} \to S$ be the projection.

Choose a real analytic Riemannian metric on $C(\mathbf{C})$ whose associated volume form equals μ_C. Let $g = \dim C$. Let $B'_r = B_r - \{\infty\}$. By Lemma 3.3, there exists $u > 0$ such that $\mu_{\mathcal{H}}(B'_r) = \mu_{\mathcal{H}}(B_r) > u/\log(1/r)$ for all sufficiently small r. On the other hand, Lemma 3.1 implies that for some $\delta > 0$, the g-dimensional volume of $\pi_{S,\infty}^{-1}(B'_r)$ is $O(r^\delta)$ as $r \to 0$. Let $L_r := \pi_C(\pi_{S,\infty}^{-1}(B'_r))$. Projection onto C can only decrease g-dimensional volume, so $\mu_C(L_r) = O(r^\delta)$. Thus we may fix $r > 0$ such that $\mu_{\mathcal{H}}(B'_r) > \mu_C(L_r)$. Let $L = L_r$. Fix a compact annulus $K \subseteq B'_r$ large enough so that $\mu_{\mathcal{H}}(K) > \mu_C(L)$.

For a compact subset M' of a metric space M, let $N_\rho M'$ be the set of points in M whose distance to M' is less than ρ. Fix $\rho > 0$ such that $N_\rho K \subseteq B'_r$. By Lemma 3.2 with $Y = S \times C$, with H the Hilbert scheme, and X the universal family in $Y \times H$, we have $X_{b_i}(\mathbf{C}) \subseteq N_\rho X_{b_\infty}(\mathbf{C})$ after discarding finitely many i. In particular, every point of $\pi_{S,i}^{-1}(K)$ is within ρ of a point of $X_{b_\infty}(\mathbf{C})$. The S-projections of the points of $X_{b_\infty}(\mathbf{C})$ so used are

then within ρ of K, so

$$\pi_{S,i}^{-1}(K) \subseteq \pi_{S,\infty}^{-1}(N_\rho K) \subseteq \pi_{S,\infty}^{-1}(B'_r).$$

Projecting to C, we obtain

$$\pi_C(\pi_{S,i}^{-1}(K)) \subseteq L. \tag{3.5}$$

Now as $i \to \infty$, the fraction of points of $\mathrm{Gal}(\overline{k}/k)x_i$ whose S-projection lies in K tends to $\mu_{\mathcal{H}}(K)$ by Lemma 3.4, and the fraction of points of $\mathrm{Gal}(\overline{k}/k)x_i$ whose C-projection lies in L tends to $\mu_C(L)$. But (3.5) implies that the first set of points is contained in the second set of points, so $\mu_{\mathcal{H}}(K) \leq \mu_C(L)$, contradicting the choice of K. □

For the proof of Theorem 2.6, we will need the following:

Lemma 3.6. *Let $\Phi\colon S \to A$ be a morphism from a Shimura curve to an elliptic curve A over $\mathbf{C}$. Let $\mu_{\mathcal{H}}$ be the hyperbolic probability measure on $S(\mathbf{C})$. Let μ_A be the Haar probability measure on $A(\mathbf{C})$. Then $\Phi_*\mu_{\mathcal{H}} \neq \mu_A$.*

Proof. By replacing S with a finite cover, we may assume that $\mathcal{H} \to S(\mathbf{C})$ is unramified. The universal cover of $A(\mathbf{C})$ is not biholomorphic to $\mathcal{H}$, so the composition $\mathcal{H} \to S(\mathbf{C}) \to A(\mathbf{C})$ cannot be unramified. Hence Φ is ramified. Pick $s \in S(\mathbf{C})$ at which the ramification index e is > 1. Let $a = \Phi(s)$. Choose a Riemannian metric on $A(\mathbf{C})$ inducing the Haar probability measure μ_A. Let B_r be the disk of radius r centered at a. With respect to suitable uniformizing parameters, Φ near s is equivalent to $z \mapsto z^e$, so there exists $c > 0$ such that $\mu_{\mathcal{H}}(\Phi^{-1}(B_r)) > c\mu_A(B_r)^{1/e}$ for all sufficiently small r. In particular, for sufficiently small r, we have $(\Phi_*\mu_{\mathcal{H}})(B_r) = \mu_{\mathcal{H}}(\Phi^{-1}(B_r)) > \mu_A(B_r)$. □

Proof of Theorem 2.6. As in the first three sentences of the proof of Theorem 2.3, we may use Corollary 9 of [20] to reduce to the case that Φ is surjective. If $A = 0$, there is nothing to show, so we may assume that A is an elliptic curve.

Choose a number field $k \subset \overline{\mathbf{Q}}$ such that A, S, X are all defined over k and Γ is contained in the division hull of $A(k)$.

If the conclusion fails, then there is an infinite sequence (s_i) in CM with $\Phi(s_i) \in \Gamma_{\epsilon_i}$ for some $\epsilon_i \to 0$. Let $a_i = \Phi(s_i)$. By Lemma 3.4, the uniform probability measure on $\mathrm{Gal}(\overline{k}/k)s_i$ converges weakly to $\mu_{\mathcal{H}}$ on $S(\mathbf{C})$. It follows that the uniform probability measure on $\mathrm{Gal}(\overline{k}/k)a_i$ converges weakly to $\Phi_*\mu_{\mathcal{H}}$ on $A(\mathbf{C})$.

On the other hand, (a_i) is a sequence of almost division points. By the previous paragraph, $[k(s_i) : k] \to \infty$, so $[k(a_i) : k] \to \infty$. Passing to a subsequence, we may assume that (a_i) has a coherent limit, which can only be $(A, \{0\})$, since $[k(a_i) : k] \to \infty$. By Theorem 1.1 of [26], the uniform probability measure on $\mathrm{Gal}(\overline{k}/k)a_i$ converges weakly to the Haar measure μ_A on $A(\mathbf{C})$.

The previous two paragraphs imply that $\Phi_*\mu_{\mathcal{H}} = \mu_A$, contradicting Lemma 3.6. □

References

1. Autissier, P.: Hauteur des correspondances de Hecke, Bull. Soc. Math. France **131** (2003), no. 3, 421–433.
2. Breuil C., Conrad B., Diamond F., Taylor R.: On the modularity of elliptic curves over **Q**: wild 3-adic exercises, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.
3. Buium, A.: Arithmetic Differential Equations. Math. Surveys and Monographs **118**, AMS (2005).
4. Buium, A., Poonen, B.: Independence of points on elliptic curves arising from special points on modular and Shimura curves, II: local results, preprint.

5. Buzzard, K.: Integral models of certain Shimura curves, Duke Math J. **87** (1997), no. 3, 591–612.
6. Cornut, C.: Mazur's conjecture on higher Heegner points, Invent. Math. **148** (2002), 495–523.
7. Darmon, H.: Rational points on modular elliptic curves. CBMS No. 101, AMS (2004).
8. Duke, W.: Hyperbolic distribution problems and half-integral weight Maass forms, Invent. Math. **92** (1988), 73–90.
9. Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (1983), 349–366.
10. Gross B., Zagier D.: Heegner points and derivatives of L-series, Invent. Math. **84** (1986), no. 2, 225–320.
11. Gross B., Kohnen W., Zagier D.: Heegner points and derivatives of L-series II, Math. Ann. **278** (1987), nos. 1–4, 497–562.
12. Kollár, J: Lectures on resolution of singularities, Annals of Math. Studies **166**, Princeton University Press, 2007.
13. Kolyvagin, V. A.: Finiteness of $E(\mathbf{Q})$ and $SH(E, \mathbf{Q})$ for a subclass of Weil elliptic curves, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540.
14. Mazur, B.: Modular curves and arithmetic, Proc. ICM, Warsaw, 1983, PWN (1984), 185–211.
15. Michel, P. and Venkatesh, A.: Equidistribution, L-functions and ergodic theory: on some problems of Yu. V. Linnik, preprint (2006), available at `http://cims.nyu.edu/~venkatesh/research/linnik.pdf`
16. Mumford, D.: Abelian varieties, Oxford University Press, 1970.
17. Munkres, J.: Topology: a first course, Prentice-Hall, 1975.
18. Nekovář, J. and Schappacher, N.: On the asymptotic behaviour of Heegner points, Turkish J. Math. **23** (1999), 549–556.
19. Pink, R.: A combination of the conjectures of Mordell-Lang and André-Oort, pp. 251–282. In: Geometric methods in algebra and number theory, Progr. Math. **235**, Birkhäuser, 2005.
20. Poonen, B.: Mordell-Lang plus Bogomolov, Invent. Math. **137** (1999), 413–425.
21. Rosen, M., and Silverman, J. H.: On the independence of Heegner points associated to distinct imaginary fields, arXiv.math.NT/0508259v2, 15 August 2005, to appear in J. Number Theory.
22. Silverman, J. H.: Hecke points on modular curves, Duke Math. J. **60** (1990), 401–423.
23. Taylor R., Wiles A.: Ring-theoretic properties of certain Hecke algebras, Annals of Math. (2) **141** (1995), no. 3, 553–572.
24. Vatsal V.: Uniform distribution of Heegner points, Invent. Math. **148** (2002), 1–48.
25. Wiles, A.: Modular elliptic curves and Fermat's Last Theorem, Annals of Math. (2) **141** (1995), no. 3, 443–551.
26. Zhang, S.: Distribution of almost division points, Duke Math. J. **103** (2000), 39–46.
27. Zhang, S.: Heights of Heegner points on Shimura curves, Annals of Math. (2) **153** (2001), 27–147.
28. Zhang, S.: Equidistribution of CM-points on quaternion Shimura varieties, Int. Math. Res. Not. **2005**, no. 59, 3657–3689.

University of New Mexico, Albuquerque, NM 87131
E-mail address: `buium@math.unm.edu`
URL: `http://math.unm.edu/~buium`

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
Current address: Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
E-mail address: `poonen@math.mit.edu`
URL: `http://math.mit.edu/~poonen`