Forum of Mathematics, Sigma (2018), Vol. 6, e13, 17 pages
doi:10.1017/fms.2018.15

UNLIKELY INTERSECTIONS IN FINITE CHARACTERISTIC

ANANTH N. SHANKAR[1] and JACOB TSIMERMAN[2]

[1] Department of Mathematics, MIT, Cambridge, MA, USA;
email: ananth.shnkr@gmail.com

[2] Department of Mathematics, University of Toronto, Toronto, ON, Canada;
email: jacobt@math.toronto.edu

Received 17 October 2017; accepted 29 June 2018

Abstract

We present a heuristic argument based on Honda–Tate theory against many conjectures in 'unlikely intersections' over the algebraic closure of a finite field; notably, we conjecture that every abelian variety of dimension 4 is isogenous to a Jacobian. Using methods of additive combinatorics, we answer a related question of Chai and Oort where the ambient Shimura variety is a power of the modular curve.

1. Introduction

In [1], Chai and Oort ask the following (folklore) question: *For every algebraically closed field k and $g \geqslant 4$, does there exist an abelian variety A over k which is not isogenous to the Jacobian of a stable curve*. It is natural to interpret this question by looking at the moduli space $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g: let $\tau_g \subset \mathcal{A}_g$ be the Torelli locus of Jacobians of stable curves, and $T_n\tau_g$ be the locus of abelian varieties with a degree n isogeny to the Torelli locus. Then an equivalent formulation of the conjecture is the statement that there exists a k-point of $\mathcal{A}_g$ outside the countable union of these proper subvarieties. In other words,

$$\bigcup_n T_n\tau_g(k) \neq \mathcal{A}_g(k).$$

In this form, it becomes natural to replace τ_g by any proper subvariety and retain the statement of the conjecture. Using this interpretation, it becomes a

simple matter to verify the conjecture for uncountable fields k, and even those with sufficiently large ($\geqslant (g^2+g)/2$) transcendence degree over their prime field. However, the cases of $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}}_p$ prove substantially more difficult. The characteristic-0 case was settled by the second-named author in [14], using a strategy of Chai and Oort outlined in [1] relying on the Andre–Oort conjecture about CM points in subvarieties. (Now a theorem for $\mathcal{A}_g$ [15].) Though an analogous strategy cannot work over $\overline{\mathbb{F}}_p$ as every point is a CM point, the prevailing opinion seems to be that the answer to the question should nevertheless be 'yes'. In this paper, we present a heuristic probabilistic argument for deciding such conjectures, and conjecture based on this heuristic the answer should be 'no' over $\overline{\mathbb{F}}_p$ for $g = 4$.

1.1. Plan for the rest of the paper. In Section 2, we present our heuristic, and lay out our main conjectures. In Section 3 we discuss sizes of isogeny classes of principally polarized abelian varieties. We detail some conjectures about sizes of isogeny classes over finite fields and present some partial results. In Section 4, we provide evidence for our conjectures by providing an explicit hypersurface in $X(1)^{270}$ which we prove intersects every isogeny class. Our proof relies heavily on results in additive combinatorics.

2. The heuristic

2.1. Honda–Tate theory. In this section we describe our heuristic. We first restrict to the setting of ordinary abelian varieties: Let $V \subset \mathcal{A}_g$ be a d-dimensional subvariety defined over $\mathbb{F}_q$, which intersects the ordinary Newton stratum. Our idea is to count the number of ordinary $\mathbb{F}_{q^n}$-isogeny classes weighted by their size, that show up in $\mathcal{A}_g(\mathbb{F}_{q^n})$ for large n. By the Honda–Tate theorem, isogeny classes are in bijection with certain type of q^n-Weil numbers. One can count these rather easily by looking at Weil-polynomials and arrive at an answer of roughly $q^{n((g^2+g)/4)}$ (see [3, Theorems 1.1,1.2]). (Remember our dimension g is fixed and the finite field $\mathbb{F}_{q^n}$ is growing; otherwise this would be quite thorny!) As such, one would expect the size of each ordinary isogeny class to also be roughly $q^{n((g^2+g)/4)}$, to account for the $q^{n((g^2+g)/2)}$ points in $\mathcal{A}_g(\mathbb{F}_{q^n})$.

We have a natural map from $V(\mathbb{F}_{q^n})$ to isogeny classes of Abelian varieties and the underlying assumption we make for our heuristic is to treat this as a random map. Now, $V(\mathbb{F}_{q^n})$ has roughly q^{nd} points, which leads us to a natural conjecture.

There is a caveat to be had: if V is contained in the mod-p reduction of a characteristic-0 proper Shimura subvariety S of $\mathcal{A}_g$, then there will be isogeny classes of Weyl CM points on $\mathcal{A}_g$ that cannot intersect S, nor will their mod-p reduction intersect V. We rule this out by insisting that for a prime ℓ not

dividing q, the ℓ-adic monodromy of V is Zariski dense in the symplectic group GSp_{2g}. Thus, our conjecture is:

CONJECTURE 2.1 (The ordinary stratum). *Let $V \subset \mathcal{A}_g$ be an irreducible subvariety of dimension d, whose ℓ-adic monodromy is Zariski dense in* GSp_{2g}. *If $d \geqslant (g^2+g)/4 = (\dim \mathcal{A}_g)/2$, then for each ordinary abelian variety A over $\overline{\mathbb{F}}_p$, there exist infinitely many points in $V(\overline{\mathbb{F}}_p)$ corresponding to abelian varieties which are isogenous to A. If, on the other hand, V does not satisfy either the monodromy condition or the dimension condition, then there exists an abelian variety A over $\overline{\mathbb{F}}_p$ such that no points in $V(\overline{\mathbb{F}}_p)$ correspond to abelian varieties which are isogenous to A.*

2.2. Nonordinary Newton strata. We now deal with the other Newton strata. To that end, let A be a principally polarized abelian variety, let W be its Newton polygon, and let $N(W)$ be the open Newton stratum of $\mathcal{A}_g$ consisting of all abelian varieties whose Newton polygon is W. By work of Oort (see [8, Section 5]), every Newton stratum decomposes into an almost product of what he terms as 'Central leaves' and 'Isogeny leaves'.

The central leaf through A consists of all abelian varieties in $N(W)$ whose p-divisible group is isomorphic to $A[p^\infty]$. The isogeny leaf through A is a maximal irreducible subscheme of $\mathcal{A}_g$, consisting of all abelian varieties A' in $N(W)$ with the property that A' is isogenous to A through an isogeny with the kernel being an extension of α_p group schemes. The dimensions of the central leaves and isogeny leaves through A depend solely on the Newton polygon of A. Using the computations in [9, Section 5], we prove below that the number of Weil q^n-numbers with Newton polygon W is of size $O(q^{n(c/2)})$, where c is the dimension of the central leaf associated to A (one may show it is within a constant of $q^{n(c/2)}$).

There is a beautiful formula [9, Section 5.2] which equates the dimension c of the central leaf of a newton stratum to a lattice-point count. To summarize: one simply draws the Newton polygon N, which starts at $(0,0)$ and ends at $(2g,g)$. Let N^* be the polygon made by taking the slopes of N in the reverse order, so that N^* is concave down. Then consider the region S defined by those points which are above or on N, strictly below N^*, and $x \leqslant g$. Then c is equal to the number of integer points in S.

EXAMPLE. Consider the case of 5-dimensional abelian varieties, and the newton polygon $(0, 1/3, 1/2, 2/3, 1)$. The characteristic polynomial of Frobenius of an abelian variety over $\mathbb{F}_q$ with the above newton polygon will have the form:

$$f(x) = x^{10} + a_1x^9 + a_2x^8 + a_3x^7 + a_4x^6 + a_5x^5 + qa_4x^4 + q^2a_3x^3 + q^3a_2x^2 + q^4a_1x + q^5,$$

where $a_i \in \mathbb{Z}$, and has absolute value bounded by $q^{i/2}$. Further, the condition on the newton polygon implies that $(a_1, p) = 1$, $q^{1/3}|a_2$, $q^{2/3}|a_3$ and $q|a_4$ and $q^{3/2}|a_5$. Therefore, the Archimedean and p-adic conditions allow us to estimate the number of such polynomials. Indeed, a_1 has $O(q^{1/2})$ choices, a_2, a_3, a_4 (the coefficients which correspond to the slope $1/3$) have

$$O\left(\frac{q \cdot q^{3/2} \cdot q^2}{q^{1/3} \cdot q^{2/3} \cdot q}\right) = O(q^{5/2})$$

choices in total, and a_5 has $O(q^{5/2}/q^{3/2}) = O(q)$ choices. This gives a total of $O(q^4)$ points. Moreover, by following Oort's procedure described above we see $c = 8$, as desired.

We now give the general result:

LEMMA 2.2. *The number of Weil q^n-numbers with Newton polygon W is of size $O(q^{n(c/2)})$, where c is the dimension of the central leaf associated to A.*

Proof. For $1 \leqslant i \leqslant g$, the divisibility condition on a_i is that $p^{m_i} \parallel a_i$, where (i, m_i) is the point on W with $x = i$. Moreover, $|a_i| \leqslant q^{i/2}$, so there are at most $O(q^{i/2-m_i})$ choices for a_i. Thus there are at most $O(q^{\sum_i i/2-m_i})$ such Weil numbers. We thus have to show that $\sum_i i/2 - m_i = \#S(\mathbb{Z})$. This is part of the statement of [9, Lemma 5.3] (the first and third quantities in his chain of equalities), which completes the proof. □

Suppose that $V \subset \mathcal{A}_g$ is a d-dimensional subvariety that intersects $N(W)$. Then the assumption we make for our heuristic is to treat the map from $V(\mathbb{F}_{q^n})$ to the set of Weil q^n-numbers with Newton polygon W as a random map, but we consider the dimension of the projection of $V \cap N(W)$ onto a central leaf instead of the dimension of $V \cap N(W)$. We impose this condition because we wish to rule out the case of $V \cap N(W)$ being a positive dimensional fibration over a subvariety over the central leaf. Analogous to Conjecture 2.1, our expectation is:

CONJECTURE 2.3 (Arbitrary Newton strata). *Suppose that $W \subset \mathcal{A}_g$ is a closed subvariety as above, and let d be the dimension of the projection of* $\dim V \cap N(W)$ *onto a central leaf. If $d > c/2$, and the ℓ-adic monodromy of $V \cap N(W)$ is Zariski dense in* GSp_{2g}*, then for each abelian variety A over $\overline{\mathbb{F}}_p$ with Newton polygon W, there exist infinitely many points in $V(\overline{\mathbb{F}}_p)$ corresponding to abelian varieties which are isogenous to A. If, on the other hand, either V does not satisfy the monodromy condition or $d < c/2$, then there exists an abelian variety A over*

$\overline{\mathbb{F}}_p$ with Newton polygon W such that no points in $V(\overline{\mathbb{F}}_p)$ correspond to abelian varieties which are isogenous to A.

REMARK. In the case of $d = c/2$ and maximal ℓ-adic monodromy, our heuristic suggests that $V(\overline{\mathbb{F}}_p)$ should contain every isogeny class with newton polygon W. However, the numbers suggest that this happens extremely rarely, so we are not confident enough to include this case in the conjecture.

2.3. Abelian varieties isogenous to Jacobians. We expect that the Torrelli locus τ_g satisfies the conditions required by Conjecture 2.1 if $g \leqslant 9$ (this is certainly the case for the ordinary locus and the Newton stratum having codimension 1, where the central leaf equals the whole Newton stratum). Therefore, we expect that every ordinary abelian variety over $\overline{\mathbb{F}}_p$ of dimension $\leqslant 9$ is isogenous to the Jacobian of some curve. In the case where $g = 4$, the Newton strata which have codimension $\geqslant 2$ are easy to handle, as we demonstrate below:

PROPOSITION 2.4. *Let A be a 4-dimensional principally polarized abelian variety over $\overline{\mathbb{F}}_p$ contained in a Newton stratum of codimension $\geqslant 2$. Then A is isogenous to a Jacobian.*

Proof. Let $x \in \mathcal{A}_4(\mathbb{F}_q)$ correspond to the point A. We claim that $\tau_4 \subset \mathcal{A}_4$ passes through a point isogenous to x.

First, note that τ_4 is an effective divisor of $\mathcal{A}_4$, whose Picard group is $\mathbb{Z}$. Therefore, the class of τ_4 is ample. This implies that τ_4 will intersect the closure of every positive dimensional subvariety of $\mathcal{A}_4$ in its Baily–Borel–Satake compactification, which we call $\overline{\mathcal{A}_4}$.

Let $\mathcal{I}_x$ denote the isogeny leaf through x (as defined in [8]) – it has the property that for every point $y \in \mathcal{I}_x$, the corresponding abelian variety is isogenous to A. By [8, Proposition 4.11], $\mathcal{I}_x$ is proper (Oort proves this for every Newton stratum), and is positive dimensional (whence the restriction that the Newton stratum of A has codimension $\geqslant 2$). Because $\mathcal{I}_x$ is positive dimensional, its closure has to intersect the closure of τ_4 in $\overline{\mathcal{A}_4}$. However, because $\mathcal{I}_x$ is proper, it is closed in $\overline{\mathcal{A}_4}$. Therefore, this intersection must happen in the interior. The proposition follows. □

We thus end the section with the following conjecture:

CONJECTURE 2.5. *Every 4-dimensional abelian variety over $\overline{\mathbb{F}}_p$ is isogenous to the Jacobian of some curve.*

REMARK. While our conjectures imply that for $g \leqslant 9$ every ordinary abelian variety should be isogenous to a Jacobian, there are other Newton polygon strata which suggest the opposite unless they have excessive intersection with the Torelli locus. It seems that it is hard to compute the precise dimension of these intersections, so we are hard pressed to formulate a general conjecture in this case.

3. Isogeny classes of Abelian varieties

Let A be a principally polarized abelian variety of dimension g defined over $\mathbb{F}_q$, which is ordinary and geometrically simple. Let α denote the corresponding Weil-number. Define $K = \mathbb{Q}(\alpha)$. The field K is a CM field, and define K^+ to be the maximal totally real subfield of K (of degree g over $\mathbb{Q}$). Let $\alpha_1, \alpha_2, \ldots, \alpha_g, q/\alpha_1, \ldots, q/\alpha_g$ denote the image of α under the $2g$ complex embeddings of K. Let $\theta_1, \ldots, \theta_g$ denote the arguments of $\alpha_1, \ldots, \alpha_g$.

Let $I(q^n, A)$ denote the set of principally polarized abelian varieties defined over $\mathbb{F}_{q^n}$ that are isogenous to A over $\overline{F}_q$, and let $N(q^n, A) = \#I(q^n, A)$.

CONJECTURE 3.1. *We have* $N(q^n, A) \leqslant (q^{n(g(g+1))/2})^{1/2+o(1)}$. *Moreover, for a positive density of integers n, we have* $N(q^n, A) = (q^{n(g(g+1))/2})^{1/2+o(1)}$.

In this section, we prove Conjecture 3.1 in the case of elliptic curves, prove the lower bounds for arbitrary g in the case where there exist g conjugates of the Weil-number of A which are multiplicatively independent. Zarhin in [16] proves that this always happens if $g = 2$ or 3. We also prove that the lower bounds hold in the case of ordinary abelian varieties isogenous to E^g.

3.1. Deligne's category. We recall Deligne's description of the category of ordinary abelian varieties over $\mathbb{F}_q$. To ease the exposition, we work with abelian varieties which are geometrically simple. Let $R_n = \mathbb{Z}[\alpha^n, (q/\alpha)^n]$, which is an order inside the CM field K. We say that $I \subset K$ is a fractional ideal of R_n, if I is a nontrivial finitely generated R_n-submodule of K. Let $\mathcal{I}_n$ denote the set of fractional ideals of R_n. We define $\mathcal{C}_n = \mathcal{I}_n/\sim$, where $I_1 \sim I_2$ if there exists some $x \in K^\times$ such that $xI_1 = I_2$. The following result is proved in [2, (D) on p. 242].

THEOREM 3.2 (Deligne). *The set of abelian varieties defined over* $\mathbb{F}_{q^n}$ *isogenous to A is in bijection with the elements of* $\mathcal{C}_n$.

3.1.1. Polarizations. In his paper [4], Howe describes polarizations on ordinary abelian varieties in terms of their Deligne modules. We recall this description for later use. Let Φ denote the CM type on K induced by A. Let $I \in \mathcal{C}_n$.

By [4, Proposition 4.9], a polarization on the abelian variety corresponding to I is given by a $\mathbb{Z}$-valued bilinear form on I which is of the form

$$(x, y) \mapsto \mathrm{Trace}_{K/\mathbb{Q}}(\lambda x \overline{y}),$$

where:

(1) $\overline{y}$ corresponds to complex conjugation on K applied on y.

(2) $(\ ,\ )$ restricted to $I \subset K$ is integral.

(3) The element $\lambda \in K$ is purely imaginary, and has the property that $\phi(\lambda)/i$ is positive for $\phi \in \Phi$.

The pair (I, λ) is isomorphic to the pair $(\nu I, \nu\overline{\nu}\lambda)$, for $\nu \in K^\times$. The polarization is principal if I is self-dual for the form.

3.1.2. Isogeny classes of powers of Elliptic curves. We now prove Conjecture 3.1 in the case $g = 1$, and the lower bound when the abelian variety in question is isomorphic to the power of an ordinary elliptic curve. To that end, let E denote an ordinary elliptic curve over $\mathbb{F}_q$. We let α, K and R denote the same objects as above. Let $D \in \mathbb{Z}$ be the unique square-free integer, such that $K = \mathbb{Q}[\sqrt{D}]$

THEOREM 3.3. *$N(q^n, E) \leqslant (q^n)^{1/2+o(1)}$. Moreover, for a density-one set of n, we have $N(q^n, E) = (q^n)^{1/2+o(1)}$. (The upper bound in a more precise form is due to Lenstra [6, Proposition* 1.19*].)*

Proof. Write $\mathcal{O}_K = \mathbb{Z}[\beta]$ where β is either $\sqrt{D}$ if $D \neq 1 \mod 4$ or $(1 + \sqrt{D})/2$ if $D = 1 \mod 4$. Then the index of R_n in $\mathcal{O}_K$ is $i_n = c \cdot \mathrm{Im}(\alpha^n)$ where c is either $D^{-1/2}$ or $2D^{-1/2}$. Alternatively, writing $\alpha = q^{1/2}e(\theta)$ we see that $\mathrm{Im}(\alpha^n) = q^{n/2}\sin(n\theta)$. Note that since E is an ordinary elliptic curve, θ/π is irrational.

Every order $\mathcal{O} \subset K$ is Gorenstein, and hence every element of $\mathcal{C}_n$ lies in $\mathcal{C}\ell(\mathcal{O})$ for some unique $\mathcal{O}$. Therefore, we have

$$\mathcal{C}_n = \bigcup_{R_n \subset \mathcal{O}} \mathcal{C}\ell(\mathcal{O}).$$

Now, for the order $\mathcal{O}_d$ of index d in $\mathcal{O}_K$, the class number $\mathcal{C}\ell(\mathcal{O}_d)$ satisfies (see [12, Ex. 4.12])

$$h(\mathcal{O}_d) = d[\mathcal{O}_K^\times : \mathcal{O}_d^\times]^{-1} h(\mathcal{O}_K) \cdot \prod_{p|d} \left(1 - \left(\frac{D}{p}\right)\right).$$

It follows that $h(R_n) \geqslant h(\mathcal{O}_d)$ whenever $d|i_n$. Further, the number of divisors of i_n is $i_n^{o(1)}$. Thus, we see that

$$N(q^n, E) = \sum_{d|i_n} h(\mathcal{O}_d) \leqslant i_n^{o(1)} h(R_n) = i_n^{1+o(1)} \leqslant (q^n)^{1/2+o(1)}$$

as desired.

On the other hand, for a set density one of integers n we have that $\sin(n\theta) > 1/n$, and then

$$N(q^n, E) \geqslant h(R_n) = i_n^{1+o(1)} \geqslant (q^n/n)^{1/2+o(1)} = (q^n)^{1/2+o(1)}. \qquad \square$$

We now establish the lower bound for the case of powers of an ordinary elliptic curve. The upper bound seems to us also within reach, but it requires a more delicate analysis of modules over nonmaximal rings.

PROPOSITION 3.4. *For a density-one set of n* $N(q^n, E^g) \geqslant (q^{n(g(g+1))/2})^{1/2+o(1)}$.

Proof. Let E_n denote an ordinary elliptic curve whose endomorphism ring equals R_n, and whose canonical lift corresponds to the lattice $R_n \subset \mathbb{C}$. Then, the canonical lift of the abelian variety E_n^g corresponds to the lattice $R_n^g \subset \mathbb{C}^g$. Consider the product polarization (which is principal) on E_n^g. This corresponds to a bilinear form $\mathrm{Trace}(\lambda\langle v \cdot \overline{w}\rangle)$, with respect to which R_n^g is self-dual. Here, $v, w \in R_n^g$ are vectors, $\overline{w}$ is the nontrivial automorphism of K applied to the coordinates of w, and $\langle\cdot\rangle$ is the ordinary dot product. Further, $\lambda \in K$ is a totally imaginary element which induces the principal polarization on E_n.

The number of isomorphism classes of PPAVs over $\mathbb{F}_{q^n}$ isogenous to E_n^g is bounded below by the number of isomorphism classes of unimodular R_n-lattices inside K^g, locally isomorphic as modules with the above bilinear form to R_n^g.

This quantity is bounded below by the following class number:

$$\mathrm{U}_g(\mathbb{Q}) \backslash \mathrm{U}_g(\mathbb{A}_{\mathbb{Q}}^f) / \mathrm{K}_n.$$

Here, $\mathbb{A}_{\mathbb{Q}}^f$ is the ring of finite adeles over $\mathbb{Q}$, U_g is the unitary group corresponding to the Hermitian form $\lambda < v \cdot \overline{w} >$, and $\mathrm{K}_n = \prod_p \mathrm{K}_{n,p}$ where $K_{n,p}$ is the local stabilizer of R_n^g at p. The class number actually counts the quantity we want, but weighted by the reciprocal of the number of automorphisms of each Hermitian lattice.

Let $\mathrm{K}_p \subset \mathrm{U}(\mathbb{Q}_p)$ denote the stabilizer of the lattice $\mathcal{O}_K^g$ and let $\mathrm{K} = \prod_p \mathrm{K}_p$. As we are only concerned with an asymptotic lower bound, it suffices to compute $[\mathrm{K} : \mathrm{K}_n]$ as n grows. (The class number with respect to K_n equals the product of the class number with respect to K and $[\mathrm{K} : \mathrm{K}_n]$.)

For some p, suppose that $R_n \otimes \mathbb{Z}_p = \mathbb{Z}_p + p^{n_p}\mathcal{O}_K \otimes \mathbb{Z}_p$. Modulo p^{n_p}, $\mathrm{K}_{n,p}$ is the subgroup of K_p which stabilizes the sublattice $\mathbb{Z}_p^g \subset \mathcal{O}_K \otimes \mathbb{Z}_p^g$. The stabilizer of $\mathbb{Z}_p^g$ is exactly the $\mathbb{Z}_p$ points of the special orthogonal group in g variables. Therefore, $[\mathrm{K}_p : \mathrm{K}_{n,p}]$ equals the index of the orthogonal group inside K_p modulo p^{n_p}.

For any affine algebraic group G over $\mathbb{Z}_p$ which is flat, the kernel of the reduction map $G(\mathbb{Z}_p) \to G(\mathbb{F}_p)$ is isomorphic to $p\mathfrak{g}(\mathbb{Z}_p)$ via the p-adic logarithm (the exponential is the inverse). Here, $\mathfrak{g}$ is the Lie algebra of G. It follows that $G(\mathbb{Z}/p^n\mathbb{Z})$ has size $Ap^{(n-1)\dim \mathfrak{g}}$, where A is the size of the mod-p reduction of $G(\mathbb{Z}_p)$. Therefore $[\mathrm{K}_p : \mathrm{K}_{n,p}] \gg (p^{n_p})^{g(g+1)/2}$ (the exponent $g(g+1)/2-1$ is the codimension of SO_g inside U_g).

The quantity $\prod_p p^{n_p}$ equals $[\mathcal{O}_K : R_n]$, which is $\geqslant (q^n)^{1/2+o(1)}$ for a density-one set of n. Therefore, $\prod_p [K_p : K_{n,p}] \geqslant (q^{ng(g+1)/2})^{1/2+o(1)}$, and the result follows. □

3.2. Class groups and isogeny classes. We retain notation from earlier in the section. We will deal exclusively with ordinary abelian varieties which are geometrically simple. Let $R_n^+ = \mathbb{Z}[\alpha^n + q/\alpha^n]$, an order of the totally real field K^+. For brevity, let R^+ denote R_1^+.

PROPOSITION 3.5. *The subset of $I(q, A)$ with endomorphism ring exactly equal to R is either empty, or in bijection with the kernel of the norm map*

$$N : \mathcal{C}\ell(R) \to \mathcal{C}\ell^+(R^+).$$

Here, $\mathcal{C}\ell^+(R^+)$ is the narrow class group of the totally real order R^+.

Proof. The set of abelian varieties defined over $\mathbb{F}_q$ with endomorphism ring R is in bijection with $\mathcal{C}\ell(R)$. Suppose that an invertible ideal I is self-dual for some (,), that is there exists a principally polarized abelian variety with endomorphism ring R. For any invertible R-ideal J, the lattice dual to IJ contains $I\overline{J}^{-1}$. Because R is Gorenstein and all the ideals in question are invertible, we have $[I : IJ] = [R : J] = [\overline{J}^{-1} : R] = [I\overline{J}^{-1} : I]$. Therefore, the lattice dual to IJ equals $I\overline{J}^{-1}$.

The abelian variety corresponding to IJ will be principally polarized if and only if there exists a totally positive $\beta \in R^+ \otimes \mathbb{Q}$ such that IJ is self-dual for the form

$$(x, y) \mapsto \mathrm{Trace}_{K/\mathbb{Q}}(\beta\lambda x\overline{y}),$$

that is if $IJ = I\overline{J}^{-1}/\beta$, that is J is in the kernel of the norm map. □

PROPOSITION 3.6. *Suppose that $q^{1/2}, \alpha_1, \ldots, \alpha_g$ are multiplicatively independent. Then, for a positive density of n, there exists a principally polarized abelian variety in $I(q^n, A)$ having endomorphism ring R_n.*

REMARK. In fact, there exists $c \in \mathcal{C}\ell^+(R^+)$ with the following properties:

(1) The class of c in $\mathcal{C}\ell(R^+)$ is trivial.

(2) The set of principally polarized abelian varieties isogenous to A with endomorphism ring exactly R is in bijection with the preimage of c in $\mathcal{C}\ell(R)$.

The content of Proposition 3.6 is to prove that under the above conditions on α, there exists a set of integers n with positive density such that $c \in \mathcal{C}\ell^+(R^+)$ is the trivial element.

Proof of Proposition 3.6. Recall that the abelian variety A gives rise to a CM type Φ of K. We retain the notation of Proposition 3.5. Without loss of generality, let $\phi_j(\alpha) = \alpha_j$, where $\phi_j \in \Phi$ for $1 \leqslant j \leqslant g$. Let $g_n(x)$ denote the minimal polynomial of $\alpha^n + (q/\alpha)^n$ over $\mathbb{Q}$. The dual of R_n under the bilinear form induced by the trace map is $[(\alpha^n - (q/\alpha)^n) g_n'(\alpha^n + (q/\alpha)^n)]^{-1}$.

For each n, consider the bilinear form on R_n given by

$$(x, y) \mapsto \mathrm{Trace}_{K/\mathbb{Q}}(\lambda_n x \overline{y}),$$

with $\lambda_n = (\alpha^n - (q/\alpha)^n) g_n'(\alpha^n + (q/\alpha)^n)$. We claim that the set of n for the bilinear form satisfying the polarization conditions has a density of $1/2^g$. Indeed, λ_n is purely imaginary, and we only need verify when the positivity conditions hold.

Recall that we defined θ_j to be the argument of $\alpha_j = \phi_j(\alpha)$. Therefore, $\phi_j(\lambda_n)/i = (4q)^{g/2} \sin(n\theta_j) \prod_{k \neq j} (\cos(n\theta_j) - \cos(n\theta_k))$. Thus, the result follows if we prove that the set of positive integers which for all $1 \leqslant j \leqslant g$ satisfy

$$\sin(n\theta_j) \prod_{j \neq k} (\cos(n\theta_j) - \cos(n\theta_k)) > 0$$

has a density of $1/2^g$. We have assumed that the set $\{1, \alpha_1, \ldots \alpha_g\}$ is a multiplicatively independent set. It follows that the elements $2\pi, \theta_1, \ldots \theta_g$ are $\mathbb{Q}$-linearly independent. It is a classical theorem due to Weyl that the sequence $(n\theta_1, \ldots n\theta_g)$ is equidistributed modulo the box $[0, 2\pi]^g$. The locus of points in $[0, 2\pi]^g$ which satisfy the necessary inequalities is open, and has measure $1/2^g$. The proposition follows. □

REMARK. We consider the set of points $(\theta_1 \dots \theta_g) \in \mathbb{R}^g$ which have the property that for some $1 \leqslant j \leqslant g$,

$$\sin(n\theta_j) \prod_{j \neq k} (\cos(n\theta_j) - \cos(n\theta_k)) = 0.$$

This set is clearly a union of hyperplanes of the form $\theta_j = m\pi$ and $\theta_j \pm \theta_k = 2m\pi$, as m varies over $\mathbb{Z}$. In fact, the space $\mathbb{R}^g$ along with this set of hyperplanes is exactly the affine apartment of the simple group Sp_{2g}.

We have identified a subset of $I(A, q^n)$ with a fiber of the map $N : \mathcal{C}\ell(R_n) \to \mathcal{C}\ell^+(R_n^+)$, and have proved that if $1, \alpha_1, \dots \alpha_g$ are multiplicatively independent, then for a positive proportion of n, the fiber is nonempty. The following theorem follows from these facts, and from Lemma 3.8 below:

THEOREM 3.7. *Suppose that $q^{1/2}, \alpha_1, \dots \alpha_g$ are multiplicatively independent. Then $N(A, q^n) \geqslant (q^{n(g(g+1))/2})^{1/2+o(1)}$.*

LEMMA 3.8. *For a density-one set of positive integers n, we have*

$$\frac{\#\mathcal{C}\ell(R_n)}{\#\mathcal{C}\ell^+(R_n^+)} = (q^n)^{g(g+1)/4+o(1)}.$$

Proof. It suffices to prove the result with $\mathcal{C}\ell(R_n^+)$ in place of $\mathcal{C}\ell^+(R_n^+)$. For ease of notation, let $\alpha_{g+j} \in \mathbb{C}$ denote q/α_j, for $1 \leqslant j \leqslant g$. We also define $R_n' = \mathbb{Z}[\alpha^n]$.

As n approaches ∞, the class group of R_n (and of R_n^+) is well approximated by the square root of its discriminant, so it suffices to prove that for a positive density of integers n, $\mathrm{Disc}(R_n)/\mathrm{Disc}(R_n^+)$ has the same order of magnitude as $(q^n)^{g(g+1)/2}$.

We have that $\mathrm{Disc}(R_n^+) = \prod_{j<k\leqslant g} (\alpha_j^n + \alpha_{g+j}^n - \alpha_k^n - \alpha_{g+k}^n)^2$. The discriminant of R_n' equals

$$\mathrm{Disc}(R_n') = \prod_{j<k\leqslant 2g} (\alpha_j^n - \alpha_k^n)^2.$$

Translating this in terms of polar coordinates, we see that

$$\mathrm{Disc}(R_n^+) = \prod_{j<k\leqslant g} 4q^n (\cos n\theta_j - \cos n\theta_k)^2,$$

and that

$$\mathrm{Disc}(R_n') = \prod_{j<k\leqslant 2g} q^n (\cos n\theta_j + i \sin n\theta_j - \cos n\theta_k - i \sin n\theta_k)^2.$$

By Lemma 3.9 below, we have that $\mathrm{Disc}(R') = q^{ng(g-1)}\mathrm{Disc}(R)$. Therefore, the quotient of the orders of the class groups is approximated by

$$\frac{\#\mathcal{C}\ell(R_n)}{\#\mathcal{C}\ell(R_n^+)} = \frac{q^{n2g(2g-1)/4}\prod_{j<k\leqslant 2g}(\cos n\theta_j + i\sin n\theta_j - \cos n\theta_k - i\sin n\theta_k)}{q^{ng(g-1)/2}q^{ng(g-1)/4}\prod_{j<k\leqslant g}(\cos n\theta_j - \cos n\theta_k)}.$$

It is easy to see that the term involving sines and cosines is absolutely bounded above, and is greater than $1/n$ for a density-one set of positive integers. The result follows. □

LEMMA 3.9. *We have that* $\mathrm{Disc}(R_n') = q^{ng(g-1)}\mathrm{Disc}(R_n)$.

Proof. We do the computation for $n = 1$, as there is no loss in generality. Further, because α is a local unit at every prime l such that $l \neq p$, the discriminants can differ only at p. Suppose that $R = R_1$ and $R^+ = R_1^+$.

Let $K^+ \otimes \mathbb{Q}_p = K_p^+$. Because α is ordinary, we have that $K \otimes \mathbb{Q}_p = K_p^+ \oplus K_p^+$. The image of α in $K \otimes \mathbb{Q}_p$ will be of the form $(\gamma, q/\gamma)$, where γ is a unit in $\mathcal{O}_{K_p^+}$. The image of q/α is $(q/\gamma, \gamma)$.

The order R' at p, $R' \otimes \mathbb{Z}_p$, splits into a direct sum $\mathcal{O}_1 \oplus \mathcal{O}_2$, corresponding to the decomposition $K \otimes \mathbb{Q}_p = K_p^+ \oplus K_p^+$. This is because $R' = \mathbb{Z}_p[\alpha]$, and α^n converges p-adically to $(1, 0) \in K_p^+ \oplus K_p^+$. The same is true of $R \otimes \mathbb{Z}_p$. Therefore, $R' \otimes \mathbb{Z}_p = \mathbb{Z}_p[\gamma] \oplus \mathbb{Z}_p[q/\gamma]$, and $R \otimes \mathbb{Z}_p = \mathbb{Z}_p[\gamma] \oplus \mathbb{Z}_p[1/\gamma]$. The latter statement is true because γ is a unit in $\mathbb{Z}_p[\gamma]$. We observe that $\mathrm{Disc}(\mathbb{Z}_p[q/\gamma]) = q^{g(g-1)}\mathrm{Disc}(\mathbb{Z}_p[1/\gamma])$ which finishes the proof in this case. □

4. Proofs for powers of the modular curve

The analysis in the previous section works just as well (in fact it is quite a bit easier) for powers of the modular curve $X(1)^n$ parametrizing n-tuples of elliptic curves. In this case, however, there is also a large advantage in that the isogeny orbits break up into product sets which allow us to use methods of additive combinatorics. This section is devoted to the proof of the following theorem:

THEOREM 4.1. *For any $n \geqslant 270$, there exists a proper subvariety $V \subset X(1)^n_{\overline{\mathbb{F}}_p}$ such that for every point $(j(E_1), \ldots, j(E_n))$ there exist elliptic curves $(E_1', \ldots, E_n')$ such that $(j(E_1'), \ldots, j(E_n')) \in V(\overline{\mathbb{F}}_p)$, where E_i isogenous to E_i' for $1 \leqslant i \leqslant n$.*

Chai and Oort (see [1, Section 4]) ask whether there exists a proper subvariety of a product of modular curves which intersects every ordinary isogeny class. The content of Theorem 4.1 is that the answer to the above question is *yes*.

The idea of the proof is to first use sum-product theorems to grow our product sets, and then use bilinear forms and a standard trick with completing our sum over a finite field. We begin by recalling some lemmas, starting with Rusza's triangle inequalities:

LEMMA 4.2. *For every abelian group G and triple of sets $A, B, C \subset G$ we have*

$$|A \pm C|\,|B| \leqslant |A \pm B|\,|B \pm C|$$

where the theorem holds for all eight possible choices of signs.

Proof. [11, Theorem 1.8.1 and 1.8.7]. □

Plugging in $A = C$ in the above gives the following:

COROLLARY 4.3. *For every abelian group G and pair of sets $A, B \subset G$*

$$|A \pm A|\,|B| \leqslant |A \pm B|^2$$

for all four possible choices of signs.

We shall also require sum-product results for finite fields not of prime order:

LEMMA 4.4. *Let F be a finite field. Suppose that $A \subset F$ is such that for any field $F_1 \subset F$ and constant $c \in F$ we have*

$$|A \cap (cF_1)| < \max(|A|^{9/11-o(1)}, |F_1|^{1/2}).$$

Then $\max(|A \cdot A|, |A + A|) \gg |A|^{12/11-o(1)}$.

Proof. This is [7, Theorem 1.4], which builds on the work by Katz–Shen [5]. (The paper has the slightly more restrictive condition $|A \cap (cF_1)| < |F_1|^{1/2}$, but this is amended in [10, Theorem 3.6], the thesis of Roche-Newton.) In fact, they prove something slightly stronger by replacing the $|A|^{-o(1)}$ factor by a power of $\log |A|$. □

We shall need the following slight variation of the above:

LEMMA 4.5. *Let F be a finite field of order q. Suppose that $A \subset F$ is such that $|A| = q^{1/2-o(1)}$, and that if there exists a subfield $F_1 \subset F$ with $[F : F_1] = 2$, then $|A \cap F_1| < |A|^{2/3}$. Then*

$$\max(|A \cdot A|, |A + A|, |(A + 1) \cdot (A + 1)|) \gg |A|^{12/11-o(1)}.$$

Proof. By Lemma 4.4 we are done unless there exists a field $F_1 \subset F$ with $[F : F_1] = 2$ and $c \in F$ such that

$$|A \cap (cF_1)| \gg |A|^{9/11},$$

so henceforth we assume this is the case. Now, let $A' = (A \cap cF_1) + 1$. By assumption $c \notin F_1$.

Write $a_1 = cb_1 + 1, a_2 = cb_2 + 1$ where $b_i \in F_1$. Then

$$(a_1a_2 - 1)/c^2 = b_1b_2 + \frac{1}{c} \cdot (b_1 + b_2).$$

Since $1/c \notin F_1$ we can recover both b_1b_2 and $b_1 + b_2$, and thus the set $\{b_1, b_2\}$. It follows that if $a_1a_2 = a_1'a_2'$ where $a_1, a_2, a_1', a_2' \in A'$ then the sets $\{a_1, a_2\}$ and $\{a_1', a_2'\}$ are the same. Thus $|A' \cdot A'| = |A'|(|A'| - 1)/2$, and the result follows. □

Packaging the above into a single polynomial, we obtain the following:

LEMMA 4.6. *Let F be a finite field of order q. Suppose that $A, B, C \subset F$ are subsets such that $|A|, |B|, |C|$ are of size $q^{1/2-o(1)}$, and that if there exists a subfield $F_1 \subset F$ with $[F : F_1] = 2$, then $\max |A \cap F_1|, |B \cap F_1|, |C \cap F_1| < q^{1/3}$. Then setting $P(x, y, z) = xy + z$, we have that*

$$\max(|P(A, B, C)|, |P(A + 1, B + 1, C + 1)|) \geqslant q^{23/44-o(1)}.$$

Proof. Note that A, B, C satisfy the condition of Lemma 4.5. Suppose first that $|A + A| \gg q^{6/11-o(1)}$. Then for any nonzero $b \in B$, we have by Corollary 4.3 that $|Ab + C| \geqslant q^{23/44-o(1)}$. Since $AB + C$ is a superset of $Ab + C$, the result follows in this case. We likewise handle the cases when AA is large, by applying Corollary 4.3 to the group $F^\times$. What remains is the case when $(A + 1)(A + 1) \geqslant q^{23/44-o(1)}$. In this case, arguing as above gives that $|(A+1)\cdot(B+1)| \geqslant q^{23/44-o(1)}$, and the result follows. □

For $x, y \in \mathbb{F}_q^n$ we define $x \cdot y = \sum_i x_i y_i$. We shall need the following combinatorial lemma, due to Shparlinski [13, Lemma 5], for which we give a proof for completeness.

LEMMA 4.7. *Let $\mathbb{F}_q$ be a finite field, n be a positive integer, and A, B be subsets of $\mathbb{F}_q^n$ not containing $\vec{0}$. Suppose that $A \times B$ does not intersect the variety $x \cdot y = 0$. Then $|A| \cdot |B| \leqslant q^{n+2}$.*

Proof. Let $f(x, y)$ be 1 if and only if $x \cdot y = 0$, and 0 otherwise. Then applying Cauchy–Schwartz, we get:

$$\begin{aligned}\frac{|A|^2|B|^2}{q^2} &= \left(\sum_{x\in A}\sum_{y\in B}\frac{1}{q} - f(x,y)\right)^2 \\ &\leqslant |A|\sum_{x\in A}\left(\sum_{y\in B}\frac{1}{q} - f(x,y)\right)^2 \\ &\leqslant |A|\sum_{x\in \mathbb{F}_q^n}\left(\sum_{y\in B}\frac{1}{q} - f(x,y)\right)^2 \\ &= |A|\left(|B|^2q^{n-2} - |B|\cdot\frac{2}{q}\sum_{y\in B}\sum_{x\in\mathbb{F}_q^n} f(x,y) + \sum_{y,z\in B}\sum_{x\in\mathbb{F}_q^n} f(x,y)f(x,z)\right).\end{aligned}$$

Now, for any nonzero y there are q^{n-1} values of x for which $x \cdot y = 0$, and unless y and z are parallel there are q^{n-2} values of x for which $x \cdot y = x \cdot z = 0$. Thus, substituting this into the above we obtain

$$\frac{|A|^2|B|^2}{q^2} = |A|(q^{n-1} - q^{n-2})\#\{y, z \in B, y \parallel z\} \leqslant |A|\,|B|q^n$$

and the result follows. □

Now fix $N > 44$, and consider the polynomial

$$Q(x_1, \ldots, x_{6N}) := \sum_{i=1}^{N} P(x_{6i+1}, x_{6i+2}, x_{6i+3})P(x_{6i+4}, x_{6i+5}, x_{6i+6}).$$

For a vector $\vec{c} \in \{0, 1\}^{2N}$, define

$$Q_{\vec{c}}(x_1, \ldots, x_{6N}) := \sum_{i=1}^{N} P(y_{6i+1}, y_{6i+2}, y_{6i+3})P(y_{6i+4}, y_{6i+5}, y_{6i+6}),$$

where $y_{6i+j} = c_{2i-1}$ for $1 \leqslant j \leqslant 3$, and $y_{6i+j} = c_{2i}$ for $4 \leqslant j \leqslant 6$.

Let $R(x_1, \ldots, x_{6N}) = \prod_{\vec{c}\in\{0,1\}^{2N}} Q_c$. Combining Lemmas 4.7 and 4.6 we obtain:

LEMMA 4.8. *Let F be a finite field of order q. Suppose that $A_1, \ldots, A_{6N} \subset F$ are subsets such that $|A_i|$ are of size $q^{1/2-o(1)}$, and that if there exists a subfield $F_1 \subset F$ with $[F : F_1] = 2$, then $\max_i |A_i \cap F_1| < q^{1/3}$. Then $\prod_i A_i$ intersects the variety $R = 0$.*

Proof. By Lemma 4.6 there is some $\vec{c}$ such that

$$|P(A_{3i+1} + c_i, A_{3i+2} + c_i, A_{6i+3} + c_i)| \geqslant q^{23/44-o(1)}$$

for all $i \leqslant N$. By Lemma 4.7, we are done if $q^{23N/22+o(1)} > q^{N+2}$, which holds since $N > 44$. □

Proof of Theorem 4.1. Note that it is enough to handle the case of $n = 270$, since for $m > n$ we can just pull back under the coordinate projection $X(1)^m \to X(1)^n$. Hence, we assume that $n = 270$. Assume first that $\vec{x} = (x_1, \ldots, x_n) \in X(1)^n$ with all the x_i corresponding to ordinary elliptic curves. Then by Theorem 3.3, we see that for q a large power of p, the set $I_i = I(x_i)(\mathbb{F}_q)$ of points isogenous to x_i over $\mathbb{F}_q$ is of size $q^{1/2-o(1)}$. Hence, by Lemma 4.8 (an application of Theorem 3.3 to a degree-two subfield of $\mathbb{F}_q$ shows that the intersection of I_i with this subfield has $q^{1/4-o(1)}$ points, and hence the lemma is applicable) there is a point on $\prod_i I_i$ which lies on $R = 0$ (where we take $N = 45$).

We thus define our variety V to be the union of $R = 0$ and the hypersurface S defined by any of the coordinates being supersingular. This completes the proof. □

Acknowledgements

It is a pleasure to thank Boris Bukh for help with the construction in Section 4. It is also a pleasure to thank Vivek Shende for many helpful discussions and clarifications regarding sizes of isogeny orbits, and Hunter Spink for helpful discussions about Section 3. Thanks also to Igor Shparlinski and Oliver Roche-Newton for pointing out several references to us, leading to an improvement of the constant in Theorem 4.1.

References

[1] C.-L. Chai and F. Oort, 'Abelian varieties isogenous to a Jacobian', *Ann. of Math. (2)* **176**(1) (2012), 589–635.
[2] P. Deligne, 'Variétés abéliennes ordinaires sur un corps fini', *Invent. Math.* **8** (1969), 238–243.
[3] S. DiPippo and E. Howe, 'Real polynomials with all roots on the unit circle and abelian varieties over finite fields', *J. Number Theory* **73**(2) (1998), 426–450.
[4] E. Howe, 'Principally polarized ordinary abelian varieties over finite fields', *Trans. Amer. Math. Soc.* **347**(7) (1995), 2361–2401.
[5] N. H. Katz and C.-Y. Shen, 'Garaev's inequality in finite fields not of prime order', http://www.math.rochester.edu/ojac/vol3/Katz_2008.pdf.
[6] H. W. Lenstra Jr, 'Factoring integers with elliptic curves', *Ann. of Math. (2)* **126** (1987), 649–673.

[7] L. Li and O. Roche-Newton, 'An improved sum-product estimate for general finite fields', *SIAM J. Discrete Math.* **25**(3) (2011), 1285–1296.
[8] F. Oort, 'Foliations in moduli spaces of abelian varieties', *J. Amer. Soc.* **17**(2) (2004), 267–296.
[9] F. Oort, 'Foliations in moduli spaces of abelian varieties and dimensions of leaves', in *Algebra, Arithmetic, and Geometry: in Honor of Yu. I. Manin,* Vol. II, Progress in Mathematics, 270 (Birkhauser Boston, Inc., Boston, MA, 2009), 465–501.
[10] O. Roche-Newton, 'On sum-product estimates and related problems in discrete geometry', PhD Thesis.
[11] I. Z. Ruzsa, 'Sumsets and structure', in *Combinatorial Number Theory and Additive Group Theory*, Advanced Courses in Mathematics. CRM Barcelona (Birkhäuser, Basel, 2009), 87–210.
[12] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions,* Vol. 1, *Publications of the Mathematica Society of Japan, 11*, (Princeton University Press, 1971).
[13] I. E. Shparlinski, 'On the additive energy of the distance set in finite fields', *Finite Fields Appl.* **42** (2016), 187–199.
[14] J. Tsimerman, 'The existence of an abelian varietiy over $\overline{\mathbb{Q}}$ isogenous to no Jacobian', *Ann. of Math. (2)* **176**(1) (2012), 637–650.
[15] J. Tsimerman, 'A proof of the Andre–Oort conjecture for $\mathcal{A}_g$', *Ann. of Math. (2)* **187**(2) (2018), 379–390.
[16] Y. Zarhin, 'Eigenvalues of Frobenius endomorphisms of abelian varieties of low dimension', *J. Pure Appl. Algebra* **219** (2015), 2076–2098.