ALGEBRA AND NUMBER THEORY 15:3 (2021)
https://doi.org/10.2140/ant.2021.15.711

Algebraic maps constant on isomorphism classes of unpolarized abelian varieties are constant

Eric Rains, Karl Rubin, Travis Scholl, Shahed Sharif and Alice Silverberg

We show that if a rational map is constant on each isomorphism class of unpolarized abelian varieties of a given dimension, then it is a constant map. Our results shed light on a question raised by Boneh et al. (*J. Math. Cryptol.* **14:1** (2020), 5–14) concerning a proposal for multiparty noninteractive key exchange.

1. Introduction

If A_1 and A_2 are abelian varieties, we say A_1 and A_2 are *weakly isomorphic*, written $A_1 \approx A_2$, if A_1 and A_2 are isomorphic as unpolarized abelian varieties. Let $\mathcal{A}_g$ denote the coarse moduli scheme of principally polarized abelian varieties of dimension g. One of our main results is the following.

Theorem 1.1. *Suppose that $g \in \mathbb{Z}_{\geq 2}$, that k is an algebraically closed field, and that $f : \mathcal{A}_g \dashrightarrow X$ is a rational map of k-schemes. Suppose that $f(A_1, \lambda_1) = f(A_2, \lambda_2)$ whenever $A_1 \approx A_2$ and (A_1, λ_1) and (A_2, λ_2) are in the domain of definition of f. Then f is a constant function.*

Note that Theorem 1.1 fails when $g = 1$; the j-invariant gives a nonconstant morphism $\mathcal{A}_1 \to \mathbb{P}^1$ such that $j(E_1) = j(E_2)$ whenever $E_1 \approx E_2$.

If R is a scheme, let

$$\mathcal{W}_g(R) = \{(A_1, A_2) \in (\mathcal{A}_g \times \mathcal{A}_g)(R) | A_1 \approx A_2\}.$$

We will deduce Theorem 1.1 from the following result.

Theorem 1.2. *If $g \in \mathbb{Z}_{\geq 2}$ and k is an algebraically closed field, then the set $\mathcal{W}_g(k)$ is Zariski dense in the k-scheme $\mathcal{A}_g \times \mathcal{A}_g$.*

It is widely acknowledged that in order to obtain a moduli space of abelian varieties, one must first fix a polarization. However, the mere fact that isomorphism as unpolarized abelian varieties itself is not a well behaved equivalence relation does not *a priori* exclude the possibility that some slightly coarser equivalence relation *could* give rise to a moduli space. Theorem 1.2 implies that this cannot happen: the only coarser equivalence relation that is also Zariski closed is the trivial relation in which all elements

We thank the Alfred P. Sloan Foundation and the National Science Foundation, which provided support for the research, and the June 2019 ICERM workshop on Arithmetic of Low-Dimensional Abelian Varieties (funded by the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation), where this project began.
MSC2010: primary 14K10; secondary 11G10, 11G15.
Keywords: abelian varieties, polarizations.

are equivalent. (Since the Zariski closure of an equivalence relation need not be an equivalence relation, Theorem 1.2 is somewhat stronger than this.) Furthermore, all of the results stated in this section hold even when k is replaced by a geometrically reduced scheme; see Remark 1.11. Our results can be viewed as making precise the discussion in [Mumford et al. 1994, p. 97] about "pathologies" that arise when considering the relation $\approx$.

We will prove the following result in Section 3.

Theorem 1.3. *Suppose that $g \in \mathbb{Z}_{\geq 2}$, k is an algebraically closed field, and that $f : \mathcal{A}_1^g \dashrightarrow X$ is a rational map of k-schemes. Suppose that $f(A_1, \lambda_1) = f(A_2, \lambda_2)$ whenever $A_1 \approx A_2$ and (A_1, λ_1) and (A_2, λ_2) are in the domain of definition of f. Then f is a constant function.*

A motivation behind Theorem 1.3 is the proposal for a construction of a cryptographic protocol in [Boneh et al. 2020]. In that protocol, n parties each construct a product of elliptic curves over a finite field such that any pair of products is isomorphic. Put another way, each party computes a point of $\mathcal{A}_1^g$ so that the chosen points are weakly isomorphic to each other. However, the proposal for a protocol was incomplete. The open question in [Boneh et al. 2020] was whether one can extract a numerical invariant of the product of elliptic curves that respects weak isomorphism, that is, a nonconstant map $f : \mathcal{A}_1^g \to X$ for a suitable space X such that $f(A_1) = f(A_2)$ whenever $A_1 \approx A_2$. In this context, Theorem 1.3 shows that if f is algebraic, then it is constant, and thus not useful cryptographically. It remains an open problem whether there is a useful nonalgebraic invariant of (isomorphism classes of nonpolarized) products of elliptic curves.

Since $\mathcal{A}_g$ is only a coarse moduli space, one might wonder whether Theorem 1.1 still holds if $\mathcal{A}_g$ is replaced by the fine moduli space of abelian varieties with full level n structure with $n \geq 3$ and not divisible by char(k). The following generalization of Theorem 1.1 shows that the phenomenon persists even for the fine moduli space.

Corollary 1.4. *Let $g, n \in \mathbb{Z}_{\geq 2}$, and let $\mathcal{A}_{g,n}$ be the moduli space of principally polarized abelian varieties with full level n structure. Suppose that k is an algebraically closed field with* char$(k) \nmid n$, *and $f : \mathcal{A}_{g,n} \dashrightarrow X$ is a rational map of k-schemes. View points of $\mathcal{A}_{g,n}$ as triples (A, λ, L), where A is an abelian variety with principal polarization λ, and L is a symplectic basis for the n-torsion $A[n]$ (where symplectic means with respect to the Weil pairing induced by λ). Suppose $f(A_1, \lambda_1, L_1) = f(A_2, \lambda_2, L_2)$ whenever $A_1 \approx A_2$ and (A_1, λ_1, L_1) and (A_2, λ_2, L_2) are in the domain of definition of f. Then f is a constant function.*

Suppose k is an algebraically closed field. If $\mu : A \to A^\vee$ is a polarization on a g-dimensional abelian variety A over k of degree not divisible by char(k), then there are unique positive integers $d_1 \mid \cdots \mid d_g$ such that

$$\ker \mu \cong (\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_g\mathbb{Z})^2$$

and char$(k) \nmid d_g$ (see [Mumford 1966, Theorem 1 et seq.]). Letting $D = (d_1, \ldots, d_g)$, we say that the polarization μ has *type* D. A *polarization type* is a tuple $D = (d_1, \ldots, d_g)$ where the d_i are positive integers such that $d_1 \mid \cdots \mid d_g$. If D is a polarization type, let $\mathcal{A}_{g,D}$ denote the moduli space of abelian varieties with a polarization of type D. View points of $\mathcal{A}_{g,D}$ as pairs (A, μ), where A is an abelian variety and μ is a polarization of type D.

The following result, which we prove in Section 5, is a generalization of Theorem 1.1 with $\mathcal{A}_g$ replaced by the moduli space of abelian varieties with a fixed polarization type.

Corollary 1.5. *Suppose that $g \in \mathbb{Z}_{\geq 2}$, $D = (d_1, \dots, d_g)$ is a polarization type, k is an algebraically closed field,* $\mathrm{char}(k) \nmid d_g$, *and $f : \mathcal{A}_{g,D} \dashrightarrow X$ is a rational map of k-schemes. Suppose $f(A_1, \mu_1) = f(A_2, \mu_2)$ whenever $A_1 \approx A_2$ and (A_1, μ_1) and (A_2, μ_2) are in the domain of definition of f. Then f is a constant function.*

Corollary 1.6. *Suppose that $g \in \mathbb{Z}_{\geq 2}$, that k is an algebraically closed field, and that $f : \cup_D \mathcal{A}_{g,D} \to X$ is a morphism of k-schemes, where D runs over all polarization types $(d_1, \dots, d_g)$ for which* $\mathrm{char}(k) \nmid d_g$. *Suppose that $f(A_1, \lambda_1) = f(A_2, \lambda_2)$ whenever $A_1 \approx A_2$. Then f is a constant function.*

We next discuss the proofs. If N is a positive integer, let $Y_0(N)/\operatorname{Spec}(\mathbb{Z}[1/N])$ denote the modular curve parametrizing pairs (E, C), where E is an elliptic curve and $C \subset E$ is a cyclic subgroup of E of order N. If A is a positive definite, symmetric, integer $g \times g$ matrix, define a map $\psi_A : Y_0(\det(A)) \to \mathcal{A}_g$ as follows. Suppose $(E, C) \in Y_0(\det(A))$. The matrix A induces a natural endomorphism λ_A of E^g. Since A is symmetric and positive definite, we can view λ_A as a polarization on E^g. Let $B = E^g/((\ker \lambda_A) \cap C^g)$ and let $\pi : E^g \to B$ be the quotient map. Then by [Milne 1986, Proposition 16.8] there is a unique polarization λ on B such that $\pi^*(\lambda) = \lambda_A$. As we shall see in Lemma 2.10, λ is a principal polarization, and B is weakly isomorphic to a product of elliptic curves. Define

$$\psi_A : Y_0(\det(A)) \to \mathcal{A}_g \;\text{ by }\; \psi_A(E, C) = (B, \lambda). \tag{1.7}$$

For another viewpoint on the maps ψ_A, see [Rains 2020, §2]. In Proposition 4.7 below we obtain a more concrete characterization of ψ_A in the case where the ground field is the field of complex numbers.

Let

$$X_A = \psi_A(Y_0(\det(A))).$$

Definition 1.8. If ℓ is a prime number and g is a positive integer, let $M(g, \ell)$ denote the set of positive definite symmetric $g \times g$ integer matrices whose determinant is a power of ℓ.

Theorem 1.9. *Suppose $g \in \mathbb{Z}_{\geq 2}$ and k is an algebraically closed field. Then there are infinitely many prime numbers ℓ such that if $A, A' \in M(g, \ell)$, then $\mathcal{W}_g(k) \cap (X_A \times X_{A'})(k)$ is Zariski dense in $X_A \times X_{A'}$.*

Theorem 1.10. *Suppose ℓ is a prime number, $g \in \mathbb{Z}_{\geq 1}$, and k is an algebraically closed field with* $\mathrm{char}(k) \neq \ell$. *Then as k-schemes, $\bigcup_{A \in M(g,\ell)} X_A$ is Zariski dense in $\mathcal{A}_g$.*

Theorems 1.9 and 1.10 are proved in Section 2 and Section 4, respectively. Proposition 2.11 is the only place where we require that $g > 1$.

Next we derive Theorem 1.2 from Theorems 1.9 and 1.10, we derive Theorem 1.1 from Theorem 1.2, we derive Corollary 1.4 from Theorem 1.1, and we derive Corollary 1.6 from Corollary 1.5.

Proof of Theorem 1.2. Fix a prime number $\ell \neq \mathrm{char}(k)$ that satisfies the conclusion of Theorem 1.9. We have

$$\bigcup_{A,A'\in M(g,\ell)} \big(\mathcal{W}_g(k)\cap (X_A\times X_{A'})(k)\big) = \mathcal{W}_g(k)\cap \Bigg(\bigcup_{A,A'\in M(g,\ell)} (X_A\times X_{A'})(k)\Bigg) \subset \mathcal{W}_g(k).$$

By Theorem 1.9, the set $\bigcup_{A,A'\in M(g,\ell)}\big(\mathcal{W}_g(k)\cap (X_A\times X_{A'})(k)\big)$ is Zariski dense in

$$\bigcup_{A,A'\in M(g,\ell)} (X_A\times X_{A'}) = \Bigg(\bigcup_{A\in M(g,\ell)} X_A\Bigg)\times\Bigg(\bigcup_{A'\in M(g,\ell)} X_{A'}\Bigg),$$

which by Theorem 1.10 is Zariski dense in $\mathcal{A}_g\times\mathcal{A}_g$. □

Proof of Theorem 1.1. Let U be the domain of definition of f, so $f : U \to X$ is a morphism. Consider the fiber product $\Delta_f = U\times_X U$. The universal property of Δ_f says that for any scheme W and morphisms h_1 and h_2 from W to U such that $f\circ h_1 = f\circ h_2$, there is a unique morphism $h : W\to\Delta_f$ such that h_1 and h_2 factor through h.

Applying the universal property with $W = \operatorname{Spec} k$ shows that $\Delta_f(k)$ consists of the pairs $(A_1, A_2)\in U\times U$ of abelian varieties over k such that $f(A_1) = f(A_2)$. By the hypothesis on f, if $A_1\approx A_2$ then $f(A_1) = f(A_2)$. Hence

$$(\mathcal{W}_g\cap(U\times U))(k)\subseteq\Delta_f(k).$$

Since Δ_f is a closed subscheme of $U\times U$, Theorem 1.2 implies that $\Delta_f = U\times U$, as desired. □

Proof of Corollary 1.4. Let $\pi : \mathcal{A}_{g,n}\to\mathcal{A}_g$ be the canonical map that "forgets" the level n structure. The space $\mathcal{A}_{g,n}$ is Galois over $\mathcal{A}_g$; let G denote the Galois group, so $G = \mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$. Letting X^G denote the product of $\#G$ copies of X, indexed by G, then the group G acts on X^G by permuting the factors: for $x\in X^G$ and $h, g\in G$, if the g-th coordinate of x is x_g, then the g-th coordinate of $h(x)$ is $x_{h^{-1}g}$. Let X^G/G denote the quotient of X^G by this action.

Let V denote the domain of definition of f, and let $U = \pi(V)$, which is an open subset of $\mathcal{A}_g$. Define a map $f_G : U\to X^G/G$ as follows. For $u\in U$, choose $v\in\pi^{-1}(x)$. Then $\pi^{-1}(u) = \{g(v)\}_{g\in G}\subset\mathcal{A}_{g,n}$. Let $z = (f(g(v)))_{g\in G}\in X^G$, and let $f_G(u)$ be the image of z in X^G/G.

Since $\pi(A, L) = A$, we have $f_G(A_1) = f_G(A_2)$ whenever $A_1\approx A_2$ with $A_1, A_2\in U$. By Theorem 1.1, f_G is constant. Since $\mathcal{A}_{g,n}$ is connected, it follows that f is constant. □

Proof of Corollary 1.6. By Corollary 1.5, f is constant on each $\mathcal{A}_{g,D}$. Fix two polarization types D and D'. Our goal is to show that $f(\mathcal{A}_{g,D}) = f(\mathcal{A}_{g,D'})$. Choose an elliptic curve E over k. Then E^g has polarizations μ and μ' over k of types D and D', respectively, so $(E^g,\mu)\in\mathcal{A}_{g,D}(k)$ and $(E^g,\mu')\in\mathcal{A}_{g,D'}(k)$. Since $E^g\approx E^g$, by our hypothesis we have $f(E^g,\mu) = f(E^g,\mu')$. Thus $f(\mathcal{A}_{g,D}) = f(\mathcal{A}_{g,D'})$, as desired. □

Remark 1.11. All of the above results hold if we replace the algebraically closed field k with a connected, geometrically reduced scheme S; for example, if we replace k with (Spec of) an integral domain. To see this, note that when S is geometrically integral, we can use the fact that the generic point is dense in S. For S geometrically reduced, instead consider the union of the generic points of the irreducible components. To generalize our results that assume nondivisibility by the characteristic of k (for example, $\mathrm{char}(k) \nmid n$), we replace this hypothesis with the assumption that the relevant value is relatively prime to the characteristics of all geometric generic points.

2. Proof of Theorem 1.9

The plan is to find a suitable infinite set of pairs $(x, y) \in \mathcal{W}_g(k) \cap (X_A \times X_{A'})(k)$. We will explicitly construct these pairs by choosing $x, y \in \mathcal{A}_g(k)$ that are products of isogenous CM elliptic curves. To ensure both that our products are weakly isomorphic and that there are enough pairs, we first establish basic observations about primes in CM fields.

Lemma 2.1. *Suppose ℓ is a prime number, $g \in \mathbb{Z}_{\geq 1}$, and K is an imaginary quadratic field over which ℓ splits into principal prime ideals, namely $\ell = \alpha\bar{\alpha}$ with $\alpha \in \mathcal{O}_K$. Then there are infinitely many rational prime numbers q such that*

(1) *q is inert in K,*

(2) *$q \equiv -1 \bmod g$, and*

(3) *$\alpha \bmod q\mathcal{O}_K \in (\mathcal{O}_K/q\mathcal{O}_K)^\times$ is a g-th power.*

Proof. Let $L = K(\zeta_g, \alpha^{1/g}, \bar{\alpha}^{1/g})$. Let σ be any complex conjugation in $\mathrm{Gal}(L/\mathbb{Q})$. Let $\mathfrak{q}$ be any prime of L unramified in $L/\mathbb{Q}$ whose Frobenius $\mathrm{Frob}(\mathfrak{q}) \in \mathrm{Gal}(L/\mathbb{Q})$ is σ. The Chebotarev density theorem guarantees that there are infinitely many such $\mathfrak{q}$. Let q be the rational prime below $\mathfrak{q}$. Since $\sigma|_K$ is complex conjugation, q is inert in K, giving (1). Since $\sigma|_{\mathbb{Q}(\zeta_g)}$ is complex conjugation, $q \equiv -1 \bmod g$, giving (2). Since σ has order 2, we have $\mathcal{O}_L/\mathfrak{q} \cong \mathcal{O}_K/q\mathcal{O}_K \cong \mathbb{F}_{q^2}$. In particular, reducing $\alpha^{1/g}$ modulo $\mathfrak{q}$ gives a g-th root of α in $(\mathcal{O}_K/q\mathcal{O}_K)^\times$, giving (3). □

We now establish some properties of CM elliptic curves that we will use in Proposition 2.11.

Definition 2.2. If K is an imaginary quadratic field and q is a prime number that is inert in K, let

$$G_q = (\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times.$$

Lemma 2.3. *Suppose E is an elliptic curve over an algebraically closed field k, and $\mathrm{End}(E) \cong \mathcal{O}_K$ for some imaginary quadratic field K. Let q be a prime number that is inert in K and not equal to the characteristic of k. Then the set of subgroups of E of order q is a torsor over G_q.*

Proof. Since $E[q]$ is a module over $\mathcal{O}_K/q\mathcal{O}_K \cong \mathbb{F}_{q^2}$ of size q^2, we have that $E[q] \cong \mathbb{F}_{q^2}$ as $\mathbb{F}_{q^2}$-vector spaces. So $\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times \cong G_q$ acts freely and transitively on the one-dimensional $\mathbb{F}_q$-subspaces of $E[q]$. □

Definition 2.4 [Kani 2011, §2]. Suppose A is an abelian variety over a field. If I is a regular left ideal of $\mathrm{End}(A)$ (i.e., a left ideal that contains an isogeny), let $H(I) = \bigcap_{\varphi \in I} \ker\varphi$. If H is a finite subgroup scheme of A, let $I(H) = \{\varphi \in \mathrm{End}(A) : \varphi(H) = 0\}$. A finite subgroup scheme H of A is an *ideal subgroup* of A if $H = H(I)$ for some ideal I of $\mathrm{End}(A)$. A left ideal I of $\mathrm{End}(A)$ is a *kernel ideal* if $I = I(H)$ for some finite subgroup scheme H of A.

Lemma 2.5 [Kani 2011, Proposition 23]. *Suppose E is a CM elliptic curve. If $H = H(I)$ is an ideal subgroup of E, then $\#H = [\mathrm{End}(E) : I]$.*

Theorem 2.6 [Kani 2011, Theorem 20b]. *Suppose E is a CM elliptic curve over an algebraically closed field and H is a finite subgroup scheme of E. Then H is an ideal subgroup if and only if $\mathrm{End}(E) \subseteq \mathrm{End}(E/H)$. Moreover, if H_1 and H_2 are ideal subgroups of E, then $E/H_1 \approx E/H_2$ if and only if $I(H_1)$ and $I(H_2)$ are isomorphic as $\mathrm{End}(E)$-modules.*

Lemma 2.7. *Suppose E is an elliptic curve over an algebraically closed field k, and $\mathrm{End}(E) = \mathscr{O}_K$ for some imaginary quadratic field K. Suppose q is a product of distinct prime numbers that are inert in K and not equal to $\mathrm{char}(k)$, and suppose $\mathscr{C}$ is a subgroup of E of order q. Then $\mathrm{End}(E/\mathscr{C}) = \mathbb{Z} + q\mathscr{O}_K \subset \mathscr{O}_K = \mathrm{End}(E)$. In particular, every endomorphism of $E/\mathscr{C}$ is induced by an endomorphism of E that takes $\mathscr{C}$ to $\mathscr{C}$.*

Proof. Let $q = \prod_{i=1}^n q_i$ be the prime factorization of q. Then $\mathscr{C} = \sum_{i=1}^n \mathscr{C}_i$ where each $\mathscr{C}_i$ is a subgroup of E of order q_i. Let $E_j = E/\sum_{i=1}^j \mathscr{C}_i$.

The isogeny $\pi : E \to E/\mathscr{C}$ factors into a chain of isogenies

$$E = E_0 \xrightarrow{\pi_1} E_1 \xrightarrow{\pi_2} E_2 \xrightarrow{\pi_3} \cdots \xrightarrow{\pi_n} E_n = E/\mathscr{C}.$$

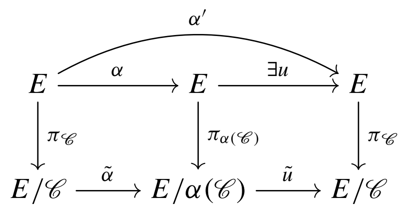
Let $\mathscr{O}_j$ be the order $\mathrm{End}(E_j)$ in K, and let f_j be its conductor, i.e., $f_j = [\mathscr{O}_K : \mathscr{O}_j]$. Since the isogeny π_j has degree q_j, either $[\mathscr{O}_j : \mathscr{O}_{j-1}] = q_j$, or $[\mathscr{O}_{j-1} : \mathscr{O}_j] = q_j$, or $\mathscr{O}_{j-1} = \mathscr{O}_j$ [Kohel 1996, Proposition 5]. Thus f_j divides $\prod_{i=1}^j q_i$. Since the q_i are distinct, $q_{j+1} \nmid f_j$. Since q_j is inert in K, $\mathscr{O}_K$ has no prime ideal of norm q_j. There is a norm-preserving bijection between prime ideals of $\mathscr{O}_j$ that do not divide f_j and prime ideals of $\mathscr{O}_K$ that do not divide f_j [Cox 2013, Proposition 7.20]. Thus, $\mathscr{O}_{j-1}$ has no prime ideal of norm q_j. By Lemma 2.5, it follows that $\ker \pi_j$ is not an ideal subgroup of E_{j-1}. Now by Theorem 2.6, we must have $[\mathscr{O}_{j-1} : \mathscr{O}_j] = q_j$. Then $[\mathscr{O}_K : \mathscr{O}_n] = \prod_{i=1}^n q_i = q$, as required. □

Lemma 2.8. *Suppose E is an elliptic curve over an algebraically closed field k, and $\mathrm{End}(E) \cong \mathscr{O}_K$ for some imaginary quadratic field K with $\mathscr{O}_K^\times = \{\pm 1\}$. Suppose q is a prime not equal to $\mathrm{char}(k)$ and inert in K, and $\mathscr{C}$ is a subgroup of E of order q. If $\alpha, \beta \in \mathscr{O}_K$ are prime to q, then $E/\alpha(\mathscr{C}) \approx E/\beta(\mathscr{C})$ if and only if $\alpha(\mathscr{C}) = \beta(\mathscr{C})$.*

Proof. Since $\alpha(\mathscr{C}) = (\alpha\bar{\beta})(\beta(\mathscr{C}))$, after replacing $\beta(\mathscr{C})$ with $\mathscr{C}$ and $\alpha\bar{\beta}$ with α it suffices to prove the claim for $\beta = 1$.

If $\alpha(\mathscr{C}) = \mathscr{C}$, then $E/\alpha(\mathscr{C}) \approx E/\mathscr{C}$, so it suffices to show the converse.

Let $\tilde{u} : E/\alpha(\mathscr{C}) \to E/\mathscr{C}$ be an isomorphism. If D is a subgroup of E, let π_D denote the quotient map $E \to E/D$. Then α induces an isogeny $\tilde{\alpha}$ such that the left-hand square of the following diagram commutes.



The map $\tilde{u} \circ \tilde{\alpha}$ is an endomorphism of $E/\mathscr{C}$. By Lemma 2.7, $\tilde{u} \circ \tilde{\alpha}$ is induced by some $\alpha' \in \mathscr{O}_K$ such that $\alpha'(\mathscr{C}) = \mathscr{C}$. That is, $\pi_{\mathscr{C}} \circ \alpha' = \tilde{u} \circ \tilde{\alpha} \circ \pi_{\mathscr{C}} = \tilde{u} \circ \pi_{\alpha(\mathscr{C})} \circ \alpha$. Since α and α' are prime to $q = \#\mathscr{C}$, we have

$$\mathscr{C} + \ker(\alpha') = \ker(\pi_{\mathscr{C}} \circ \alpha') = \ker(\tilde{u} \circ \pi_{\alpha(\mathscr{C})} \circ \alpha) = \ker(\pi_{\alpha(\mathscr{C})} \circ \alpha) = \mathscr{C} + \ker(\alpha),$$

and $\ker(\alpha) = \ker(\alpha')$. Thus $\alpha' = u\alpha$ for some $u \in \mathscr{O}_K^\times = \{\pm 1\}$. So $\alpha(\mathscr{C}) = \pm\alpha'(\mathscr{C}) = \pm\mathscr{C} = \mathscr{C}$, as desired. □

Proposition 2.9. *Suppose E is an elliptic curve over an algebraically closed field k, and* $\operatorname{End}(E) \cong \mathscr{O}_K$ *for some imaginary quadratic field K with $\mathscr{O}_K^\times = \{\pm 1\}$. Suppose q is a prime not equal to* $\operatorname{char}(k)$ *and inert in K, and $\mathscr{C}$ is a subgroup of E of order q. Suppose $\alpha_1, \dots, \alpha_g, \beta_1, \dots, \beta_g \in \mathscr{O}_K$ are prime to q, and let $\alpha = \prod_{i=1}^g \alpha_i$ and $\beta = \prod_{i=1}^g \beta_i$. Then*

$$\prod_{i=1}^{g} E/\alpha_i(\mathscr{C}) \approx \prod_{i=1}^{g} E/\beta_i(\mathscr{C}) \;\Leftrightarrow\; \alpha \equiv \beta \text{ in } G_q.$$

Proof. Let M be the diagonal matrix with diagonal entries $\alpha_1^{-1}, \dots, \alpha_{g-1}^{-1}, \alpha_g^{-1}\alpha$. Note that $M \bmod q\mathscr{O}_K \in \mathrm{SL}_g(\mathscr{O}_K/q\mathscr{O}_K)$. By [Bass 1964, Corollary 5.2], there exists $M' \in \mathrm{SL}_g(\mathscr{O}_K)$ such that $M \equiv M' \bmod q\mathscr{O}_K$. The matrix M' corresponds to an automorphism of E^g that sends $\prod_{i=1}^g \alpha_i(\mathscr{C})$ to $\mathscr{C}^{g-1} \times \alpha(\mathscr{C})$. A similar construction with β shows that

$$\prod_{i=1}^{g} E/\alpha_i(\mathscr{C}) \approx \prod_{i=1}^{g} E/\beta_i(\mathscr{C}) \;\Leftrightarrow\; (E/\mathscr{C})^{g-1} \times E/\alpha(\mathscr{C}) \approx (E/\mathscr{C})^{g-1} \times E/\beta(\mathscr{C}).$$

Note that α induces an isogeny $\tilde{\alpha} : E/\mathscr{C} \to E/\alpha(\mathscr{C})$. Let $\mathscr{O} = \mathbb{Z} + q\mathscr{O}_K$. By Lemma 2.7 we have $\mathscr{O} \cong \operatorname{End}(E/\mathscr{C}) \cong \operatorname{End}(E/\alpha(\mathscr{C})) \cong \operatorname{End}(E/\beta(\mathscr{C}))$. Thus $\ker\tilde{\alpha}$ is an ideal subgroup by Theorem 2.6. The same holds for β in place of α.

For an isogeny φ with domain $E/\mathscr{C}$, let I_φ denote the kernel ideal of $\ker(\varphi)$, i.e.,

$$I_\varphi = \{f \in \operatorname{End}(E/\mathscr{C}) : f(\ker(\varphi)) = 0\}.$$

By [Kani 2011, Theorem 46],

$$(E/\mathscr{C})^{g-1} \times E/\alpha(\mathscr{C}) \approx (E/\mathscr{C})^{g-1} \times E/\beta(\mathscr{C}) \;\Leftrightarrow\; \left(\bigoplus_{i=1}^{g-1} \mathscr{O}\right) \oplus I_{\tilde{\alpha}} \cong \left(\bigoplus_{i=1}^{g-1} \mathscr{O}\right) \oplus I_{\tilde{\beta}} \text{ as } \mathscr{O}\text{-modules}.$$

By [Kani 2011, Theorem 48] (see also [Kani 2011, Remark 49b]), the latter isomorphism is equivalent to $I_{\tilde{\alpha}} \cong I_{\tilde{\beta}}$. By Theorem 2.6,

$$I_{\tilde{\alpha}} \cong I_{\tilde{\beta}} \;\Leftrightarrow\; E/\alpha(\mathscr{C}) \approx E/\beta(\mathscr{C}).$$

By Lemma 2.8,

$$E/\alpha(\mathscr{C}) \approx E/\beta(\mathscr{C}) \;\Leftrightarrow\; \alpha(\mathscr{C}) = \beta(\mathscr{C}).$$

By Lemma 2.3, $\alpha(\mathscr{C}) = \beta(\mathscr{C})$ if and only if $\alpha \equiv \beta$ in G_q. □

Recall the map ψ_A defined in (1.7).

Lemma 2.10. *Suppose $g \in \mathbb{Z}_{\geq 1}$, and A is a $g \times g$ symmetric, positive definite integer matrix whose determinant N is not divisible by the characteristic of our base. Suppose $(E, C) \in Y_0(N)$, and let $\psi_A(E, C) = (B, \lambda)$. Let $d_1, \cdots, d_g$ be the elementary divisors of A, and for $1 \leq i \leq g$ let $E_i = E/(N/d_i)C$. Then λ is a principal polarization and $B \approx E_1 \times \cdots \times E_g$.*

Proof. Since $\lambda_A = \pi^*(\lambda) = \pi^\vee \circ \lambda \circ \pi$, where $\pi^\vee$ is the dual isogeny, we have $\deg(\lambda_A) = \deg(\pi)^2 \cdot \deg(\lambda)$. Therefore λ is a principal polarization.

Let D be the diagonal matrix with $d_1, \cdots, d_g$ on the diagonal. Then D is the Smith normal form of A, and there exist $U, V \in \mathrm{GL}_g(\mathbb{Z})$ such that $A = UDV$. If $M \in \mathrm{GL}_g(\mathbb{Z})$, let λ_M denote the natural endomorphism of E^g induced by M. Then $\lambda_A = \lambda_U \lambda_D \lambda_V$. Since

$$\ker \lambda_D = E[d_1] \times E[d_2] \times \cdots \times E[d_g]$$

we have $(\ker \lambda_D) \cap C^g = \prod_{i=1}^{g} \left(\frac{N}{d_i} C\right)$. Since $\lambda_V(C^g) = C^g$, we now have

$$\lambda_V((\ker \lambda_A) \cap C^g) = (\ker \lambda_D) \cap C^g.$$

Thus,

$$B = E^g/((\ker \lambda_A) \cap C^g) \approx E^g/((\ker \lambda_D) \cap C^g) = E_1 \times \cdots \times E_g. \qquad \square$$

Proposition 2.11. *Suppose $g \in \mathbb{Z}_{\geq 2}$. Then there are infinitely many rational primes $\ell \neq \mathrm{char}(k)$ such that if $A, A' \in M(g, \ell)$, $\det(A) = \ell^n$, and $\det(A') = \ell^m$, then there exists an infinite sequence $x_i \in Y_0(\ell^n)(k)$ such that*

$$\lim_{i \to \infty} \#\{y \in Y_0(\ell^m)(k) : \psi_A(x_i) \approx \psi_{A'}(y)\} = \infty.$$

Proof. Let K be an imaginary quadratic field with $\mathcal{O}_K^\times = \{\pm 1\}$ and such that if $\mathrm{char}(k) > 0$ then $\mathrm{char}(k)$ splits in K. Let ℓ be any prime number not equal to $\mathrm{char}(k)$ that splits into principal primes, $\ell = \alpha\bar{\alpha}$ with $\alpha \in \mathcal{O}_K$. There are infinitely many such primes ℓ by the Chebotarev density theorem. Choose an infinite sequence $\{q_i\}$ of rational primes as in Lemma 2.1. Since ℓ splits and the q_i are inert in K, we have $q_i \neq \ell$ for all i.

The classical theory of complex multiplication shows that there is an elliptic curve E_0 defined over a number field L with good reduction everywhere and with $\mathrm{End}(E_0) \cong \mathcal{O}_K$. If $\mathrm{char}(k) = 0$, then the base change E of E_0 to k via any embedding of L into k is an elliptic curve over k with $\mathrm{End}(E) \cong \mathcal{O}_K$. If $p := \mathrm{char}(k) > 0$, then since p splits in K, the curve E_0 has ordinary reduction at all primes above p; if E is the base change of E_0 to k via any reduction map of $\mathcal{O}_L$ to k, then E is an ordinary elliptic curve and $\mathrm{End}(E)$ contains a copy of $\mathcal{O}_K$, so $\mathrm{End}(E) \cong \mathcal{O}_K$. Thus, there is an elliptic curve E over k such that $\mathrm{End}(E) \cong \mathcal{O}_K$. Fix such a curve E.

If $\mathscr{C}$ is a cyclic subgroup of E of order prime to ℓ, then α induces a chain of isogenies

$$E/\mathscr{C} \to E/\alpha(\mathscr{C}) \to \cdots \to E/\alpha^n(\mathscr{C}).$$

Let $\alpha_{\mathscr{C},n} : E/\mathscr{C} \to E/\alpha^n(\mathscr{C})$ be the composition of this chain. Then $\alpha_{\mathscr{C},n}$ is a cyclic ℓ^n-isogeny, so the pair $(E/\mathscr{C}, \alpha_{\mathscr{C},n})$ defines a point in $Y_0(\ell^n)(k)$.

For each i, fix a cyclic subgroup $\mathscr{C}_i$ of E of order q_i. Define x_1 to be $(E/\mathscr{C}_1, \alpha_{\mathscr{C}_1,n})$, x_2 to be $(E/(\mathscr{C}_1 + \mathscr{C}_2), \alpha_{\mathscr{C}_1+\mathscr{C}_2,n})$, and so on. The x_i are distinct points, since the curves all have different endomorphism rings by Lemma 2.7.

Let $\ell^{n_1}, \dots, \ell^{n_g}$ be the elementary divisors of A and let $\ell^{n'_1}, \dots, \ell^{n'_g}$ be the elementary divisors of A'. By Lemma 2.10 we have

$$\psi_A(x_1) \approx E/\alpha^{n_1}(\mathscr{C}_1) \times \cdots \times E/\alpha^{n_g}(\mathscr{C}_1).$$

Let S denote a set of representatives $\beta \in \mathscr{O}_K$ of the solutions to

$$\alpha^{n_1+\cdots+n_g} \equiv \beta^g \alpha^{n'_1+\cdots+n'_g} \text{ in } G_{q_1}.$$

Since α is a g-th power in $(\mathscr{O}_K/q_1\mathscr{O}_K)^\times$, and g divides the order $q_1 + 1$ of the cyclic group G_{q_1}, we have $\#S = g$. For all $\beta \in S$, let $y_\beta = (E/\beta(\mathscr{C}_1), \alpha_{\beta(\mathscr{C}_1),m})$. By Lemma 2.10 we have

$$\psi_{A'}(y_\beta) = E/\alpha^{n'_1}(\beta(\mathscr{C}_1)) \times \cdots \times E/\alpha^{n'_g}(\beta(\mathscr{C}_1)).$$

Thus $\psi_A(x_1) \approx \psi_{A'}(y_\beta)$ by Proposition 2.9. By Lemma 2.8 the y_β are distinct. This gives g points $y \in Y_0(\ell^m)(k)$ with $\psi_A(x_1) \approx \psi_{A'}(y)$.

For x_2, we use a similar construction. By the Chinese remainder theorem, the set of subgroups of E of order q_1q_2 is a torsor over $G_{q_1} \times G_{q_2}$. Finding $\beta \in \mathscr{O}_K$ such that

$$\psi_A(x_2) \approx \psi_{A'}\big(E/\beta(\mathscr{C}_1 + \mathscr{C}_2), \alpha_{\beta(\mathscr{C}_1+\mathscr{C}_2),m}\big)$$

reduces to finding solutions β to

$$\alpha^{n_1+\cdots+n_g} \equiv \beta^g \alpha^{n'_1+\cdots+n'_g} \text{ in } G_{q_1} \times G_{q_2}.$$

There are precisely g^2 solutions β. Continuing this construction for $i = 3, 4, \dots$, we find that for each i there are g^i points $y \in Y_0(\ell^m)(k)$ such that $\psi_A(x_i) \approx \psi_{A'}(y)$. Since $g > 1$, the result follows. □

Proof of Theorem 1.9. Suppose ℓ is a prime as in Proposition 2.11, and $A, A' \in M(g, \ell)$. Let S denote the Zariski closure of $\mathcal{W}_g(k) \cap (X_A \times X_{A'})(k)$ in $X_A \times X_{A'}$. By Proposition 2.11, the set $\mathcal{W}_g(k) \cap (X_A \times X_{A'})(k)$ has an infinite number of geometric points. Thus $\dim S \geq 1$. Suppose $\dim S = 1$, so that S is a finite union of curves $\cup S_i$ and isolated points. The S_i cannot all be horizontal components — that is, of the form $X \times \{z\}$ — since this would contradict Proposition 2.11. Let S' be S with the horizontal components and isolated points removed. By Proposition 2.11, the projection map $\pi_X : S' \to X$ has unbounded degree. But π_X on each irreducible component of S' is nonconstant, so $\pi_X|_{S'}$ has finite degree. This contradiction shows that $\dim S \geq 2$, and the desired result follows. □

3. Proof of Theorem 1.3

Lemma 3.1. *Suppose p and ℓ are distinct prime numbers. There are infinitely many imaginary quadratic fields K such that p splits in K and ℓ is inert in K.*

Proof. If q is an odd prime not dividing an integer d, then q splits (resp. is inert) in $\mathbb{Q}(\sqrt{d})$ if d is a square (resp. is a nonsquare) modulo q. Thus if p and ℓ are both odd, the lemma is satisfied with $K = \mathbb{Q}(\sqrt{d})$ for any negative integer d such that both

- $d \bmod p$ is a square in $(\mathbb{Z}/p\mathbb{Z})^\times$, and
- $d \bmod \ell$ is a nonsquare in $(\mathbb{Z}/\ell\mathbb{Z})^\times$.

There are infinitely many such K, by the Chinese remainder theorem. If $p = 2$ the argument is similar, but replacing $(\mathbb{Z}/p\mathbb{Z})^\times$ above with $(\mathbb{Z}/8\mathbb{Z})^\times$. If $\ell = 2$, replace $(\mathbb{Z}/\ell\mathbb{Z})^\times$ with $(\mathbb{Z}/8\mathbb{Z})^\times$. □

Suppose A is a $g \times g$ diagonal matrix whose diagonal entries are positive integers, and let $N = \det A$. Observe that the map $\psi_A : Y_0(N) \to \mathcal{A}_g$ factors through the map $\mathcal{A}_1^g \to \mathcal{A}_g$ that sends a tuple of polarized elliptic curves $(E_1, \dots, E_g)$ to the product $E_1 \times \cdots \times E_g$ with the product polarization. Write

$$\psi_A^{(1)} : Y_0(N) \to \mathcal{A}_1^g$$

for the associated morphism. Let $d_1, \dots, d_g$ be the diagonal entries of A. If $(E, C) \in Y_0(N)$, then

$$\psi_A^{(1)}(E, C) = E_1 \times \cdots \times E_g,$$

where $E_i := E/\frac{N}{d_i}C$. Let

$$X_A^{(1)} = \psi_A^{(1)}(Y_0(N)).$$

If g is a positive integer and ℓ is a prime number, let $W_{\ell,g}$ denote the set of all $g \times g$ diagonal matrices with diagonal entries $\ell^{n_1}, \dots, \ell^{n_g}$ for some positive integers $n_1, \dots, n_g$.

Theorem 3.2. *If $g \in \mathbb{Z}_{\geq 1}$ and ℓ is a prime number not equal to the characteristic of k, then $\bigcup_{A \in W_{\ell,g}} X_A^{(1)}$ is Zariski dense in $\mathcal{A}_1^g$.*

Proof. If $\mathrm{char}(k) = 0$, let K be any imaginary quadratic field, and if $\mathrm{char}(k) > 0$, let K be an imaginary quadratic field in which $\mathrm{char}(k)$ splits and ℓ is inert. Such a K exists by Lemma 3.1. Let E_0 be an elliptic curve over k with CM by $\mathcal{O}_K$. Fix a subgroup $\mathscr{C}_0$ of E_0 of order ℓ. Let π_0 denote the quotient map $E_0 \to E_0/\mathscr{C}_0 =: E_1$. Since $\mathrm{End}(E_0)$ has no ideal of norm ℓ, $\mathscr{C}_0$ is not an ideal subgroup of E_0 by Lemma 2.5. Theorem 2.6 and [Kohel 1996, Proposition 5] now imply that $\mathrm{End}(E_1) = \mathbb{Z} + \ell\mathcal{O}_K$.

For $i \geq 1$, let $\mathscr{C}_i$ be any subgroup of E_i of order ℓ other than the kernel of the dual isogeny $\pi_{i-1}^\vee$, and let π_i be the quotient map $E_i \to E_i/\mathscr{C}_i =: E_{i+1}$. In order to show that the E_i are nonisomorphic, we will show inductively that $\mathrm{End}(E_{i+1}) = \mathbb{Z} + \ell^{i+1}\mathcal{O}_K$. Since $\mathrm{End}(E_i) \subset \mathrm{End}(E_{i-1})$, Theorem 2.6 implies that $\ker \pi_{i-1}^\vee$ is an ideal subgroup. Since $\mathrm{End}(E_i) = \mathbb{Z} + \ell^i\mathcal{O}_K$, the only ideal of index ℓ in $\mathrm{End}(E_i)$ is $\ell\mathbb{Z} + \ell^i\mathcal{O}_K$. From Lemma 2.5 and the uniqueness of the ideal of index ℓ, it follows that $\ker \pi_{i-1}^\vee$ is the unique ideal subgroup of order ℓ, namely $H(\ell\mathbb{Z} + \ell^i\mathcal{O}_K)$. The subgroup $\mathscr{C}_i$ therefore cannot also be an ideal subgroup of E_i. By Theorem 2.6, $\mathrm{End}(E_{i+1})$ must be strictly smaller than $\mathrm{End}(E_i)$. The latter observation together with [Kohel 1996, Proposition 5] implies $[\mathrm{End}(E_i) : \mathrm{End}(E_{i+1})] = \ell$, and hence $\mathrm{End}(E_{i+1}) = \mathbb{Z} + \ell^{i+1}\mathscr{O}_K$.

Let $S = \{E_i\}_{i=0}^{\infty}$. Let $(E_{n_1}, \dots, E_{n_g}) \in S^g$ and let A be the diagonal matrix with diagonal entries $\ell^{n_1}, \dots, \ell^{n_g}$. Choose any $n > \max\{n_i\}$, and let $\mathscr{C} = \ker \pi^{(n)}$. Then $(E_0, \pi^{(n)}) \in Y_0(\ell^n)(k)$ and

$$\psi_A^{(1)}(E_0, \mathscr{C}) = E_{n_1} \times \cdots \times E_{n_g}.$$

Thus, $S \subset \bigcup_A X_A^{(1)}(k)$. Since S is an infinite set of nonisomorphic elliptic curves, S is dense in $\mathcal{A}_1$. Therefore S^g is dense in $\mathcal{A}_1^g$. □

Theorem 3.3. *Suppose $g \in \mathbb{Z}_{\geq 2}$ and k is an algebraically closed field. Then there are infinitely many primes ℓ such that for all diagonal matrices A and A' in $M(g, \ell)$, $\mathcal{W}_g^{(1)}(k) \cap (X_A^{(1)} \times X_{A'}^{(1)})(k)$ is Zariski dense in $X_A^{(1)} \times X_{A'}^{(1)}$.*

Proof. The proof is the same as the proof of Theorem 1.9, only replacing $\mathcal{A}_g$ with $\mathcal{A}_1^g$, and ψ_A with $\psi_A^{(1)}$. □

Proof of Theorem 1.3. The proof of Theorem 1.3 is almost the same as that of Theorem 1.1, replacing $\mathcal{A}_g$ with $\mathcal{A}_1^g$, and invoking Theorems 3.3 and Theorem 3.2 in place of Theorems 1.9 and 1.10, respectively. □

4. Proof of Theorem 1.10

To prove Theorem 1.10, we will show that for each nonzero Siegel modular function f on $\mathcal{A}_g$, there exists $A \in M(g, \ell)$ such that the pullback modular function $\psi_A^*(f)$ is nonzero. Proposition 4.5 and Lemma 4.2 will allow us to choose such a matrix A. For background on Siegel modular functions over an arbitrary field, needed for Proposition 4.8, see [Faltings and Chai 1990, §V.1].

Lemma 4.1. *If $g \in \mathbb{Z}_{\geq 1}$ and $N \in \mathbb{Z}_{\geq 2}$, then $\mathrm{SL}_g(\mathbb{Z}[1/N])$ is dense in $\mathrm{SL}_g(\mathbb{R})$.*

Proof. Let $G \in \mathrm{SL}_g(\mathbb{R})$. Factor G as a product of elementary matrices $G = E_n \cdots E_2 E_1$, where $\det E_i = \pm 1$. For each E_i, with at most one exception the entries are 0 or ± 1. Thus there exists a $g \times g$ matrix E_i' with entries in $\mathbb{Z}[1/N]$ and $\det E_i' = \det E_i$ that is arbitrarily close to E_i. Let $G' = E_n' \cdots E_1' \in \mathrm{SL}_g(\mathbb{Z}[1/N])$. Since matrix multiplication is continuous, G' can be made arbitrarily close to G. □

Lemma 4.2. *If $g \in \mathbb{Z}_{\geq 1}$ and $N \in \mathbb{Z}_{\geq 2}$, then the set*

$$\{rGG^t : r \in \mathbb{R}^+ \text{ and } G \in \mathrm{SL}_g(\mathbb{Z}[1/N])\}$$

is dense in the set of $g \times g$ real, symmetric, positive definite matrices.

Proof. Let A be a $g \times g$ real, symmetric, positive definite matrix. Then there exists an orthogonal matrix O such that $D = OAO^t$ is diagonal and has positive entries. Let $H = \det(D)^{-1/2} O\sqrt{D}$ so that $A = \det(D) HH^t$. Note that $H \in \mathrm{SL}_g(\mathbb{R})$, so by Lemma 4.1, there exists $G \in \mathrm{SL}_g(\mathbb{Z}[1/N])$ arbitrarily close to H, and therefore $\det(D) GG^t$ can be made arbitrarily close to A. □

Definition 4.3. A $g \times g$ matrix Q is *half-integral* if $2Q_{ij} \in \mathbb{Z}$ and $Q_{ii} \in \mathbb{Z}$ for all $1 \leq i, j \leq g$, where Q_{ij} denotes the i, j entry of Q.

Lemma 4.4. *Fix $t \in \mathbb{R}$. Then there are finitely many $g \times g$ symmetric, positive semidefinite, half-integral matrices Q such that* $\mathrm{Tr}(Q) \le t$.

Proof. Suppose Q is a symmetric, positive semidefinite, half-integral matrix with $\mathrm{Tr}(Q) \le t$. Let $\lambda_1, \dots, \lambda_g$ be the eigenvalues of Q. Since $\lambda_i \ge 0$, we have

$$\sum_{1 \le i, j \le g} Q_{ij}^2 = \mathrm{Tr}(Q^2) = \sum_{i=1}^{g} \lambda_i^2 \le \left(\sum_{i=1}^{g} \lambda_i \right)^2 = \mathrm{Tr}(Q)^2 \le t^2.$$

This shows that Q, as a vector in $\mathbb{R}^{g^2}$, lies in the ball of radius t. Thus the number of possible Q is bounded by the number of half-integral points in the ball of radius t in $\mathbb{R}^{g^2}$, which is finite. □

Proposition 4.5. *Suppose $g \in \mathbb{Z}_{\ge 1}$ and S is a nonempty set of $g \times g$ symmetric, positive semidefinite, half-integral matrices. Then there exists an open cone of $g \times g$, positive definite, real, symmetric matrices A such that* $\min_{Q \in S} \mathrm{Tr}(AQ)$ *is achieved by a unique $Q \in S$.*

Proof. Let $t_0 = \min_{Q \in S} \mathrm{Tr}(Q)$. Since $\{Q \in S : \mathrm{Tr}(Q) \le t\}$ is finite for all $t \in \mathbb{R}$ by Lemma 4.4, there is a gap between t_0 and the next smallest value t_1 of $\mathrm{Tr}(Q)$ for $Q \in S$. Let $S_0 = \{Q \in S : \mathrm{Tr}(Q) = t_0\}$.

Let $\mathfrak{S}$ be the set of real symmetric $g \times g$ matrices E such that

(1) $\mathrm{Tr}(EQ_i) \ne \mathrm{Tr}(EQ_j)$ for all distinct $Q_i, Q_j \in S_0$,

(2) E is positive definite, and

(3) $\mathrm{Tr}(EQ) < t_1 - t_0$ for all $Q \in S_0$.

To see that $\mathfrak{S}$ is nonempty, observe that (1) describes the complement of a finite union of hyperplanes, which is a dense set. Therefore there is a real symmetric matrix E satisfying both (1) and (2). Scaling by a sufficiently small $\varepsilon > 0$, we can guarantee (3) as well.

Let $C = \mathbb{R}^+(I + \mathfrak{S})$, where I is the $g \times g$ identity matrix. By definition, C is a cone. The set C is open because $\mathfrak{S}$ is defined as a finite intersection of open subsets.

Suppose $A \in C$; that is, $A = r(I + E)$ for some $r \in \mathbb{R}^+$ and $E \in \mathfrak{S}$. Let $Q \in S$. Since E and Q are positive semidefinite, $\mathrm{Tr}(EQ) \ge 0$. Property (3) now implies that $\mathrm{Tr}((I + E)Q)$ is minimized only when $Q \in S_0$. Hence by (1) we have that $\mathrm{Tr}((I + E)Q)$ is minimized for a unique $Q \in S$. Since E is positive definite, so is $I + E$, and hence $I + E$ satisfies the conclusion of the proposition. By linearity of the trace, A also satisfies the conclusion of the proposition, and the desired result follows. □

Let $\mathbb{H}$ denote the complex upper half plane and let $\mathbb{H}_g$ denote the degree g Siegel upper half space. Recall that $\mathrm{Sp}_{2g}(\mathbb{Z})$ (resp. $\Gamma_0(N)$) acts on $\mathbb{H}_g$ (resp. $\mathbb{H}$) by fractional linear transformations, $Y_0(N) = \mathbb{H}/\Gamma_0(N)$, and $\mathcal{A}_g = \mathbb{H}_g/\mathrm{Sp}_{2g}(\mathbb{Z})$.

Lemma 4.6. *Suppose that A is a $g \times g$ symmetric, positive definite integer matrix and $N = \det A$. Then the map*

$$\mathbb{H} \to \mathbb{H}_g, \quad \tau \mapsto \tau A$$

induces a morphism of $\mathbb{C}$-schemes $\psi_{A,\mathbb{C}} : Y_0(N) \to \mathcal{A}_g$.

Proof. Let

$$\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N) \quad \text{and} \quad M = \begin{bmatrix} aI_g & bA \\ cA^{-1} & dI_g \end{bmatrix}$$

where I_g denotes the $g \times g$ identity matrix. Suppose $\tau \in \mathbb{H}$. Then τA is symmetric and its imaginary part is positive definite, so $\tau A \in \mathbb{H}_g$. A direct computation shows that $M \in \mathrm{Sp}_{2g}(\mathbb{Z})$ and $\sigma(\tau)A = M(\tau A)$. □

Recall the definition of ψ_A in (1.7).

Proposition 4.7. *Suppose that* $g \in \mathbb{Z}_{\geq 1}$, ℓ *is a prime*, $A \in M(g, \ell)$, *and the base scheme is* $\mathbb{C}$. *Then* $\psi_A = \psi_{A,\mathbb{C}}$.

Proof. Let $N = \det A$. Suppose $(E, C) \in Y_0(N)$. There exists $\tau \in \mathbb{H}$ such that $E = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ and $C = \langle 1/N \rangle$. We first show that $\psi_{A,\mathbb{C}}(E, C) \approx \psi_A(E, C)$.

Let $\Lambda = \mathbb{Z}^g + \tau\mathbb{Z}^g \subset \mathbb{C}^g$. Then $\mathbb{C}^g/\Lambda = E^g$. Let

$$\tilde{\Lambda}_A = \mathbb{Z}^g + \tau A\mathbb{Z}^g \quad \text{and} \quad \Lambda_A = A^{-1}\mathbb{Z}^g + \tau\mathbb{Z}^g.$$

By definition, $\psi_{A,\mathbb{C}}(E, C) \approx \mathbb{C}^g/\tilde{\Lambda}_A$. Since $\Lambda \subset \Lambda_A$, there is a natural isogeny

$$\rho : E^g = \mathbb{C}^g/\Lambda \to \mathbb{C}^g/\Lambda_A.$$

Multiplication by $A : \mathbb{C}^g \to \mathbb{C}^g$ induces an isomorphism

$$\mathbb{C}^g/\Lambda_A \xrightarrow{\sim} \mathbb{C}^g/\tilde{\Lambda}_A$$

and an isogeny

$$\lambda_A : \mathbb{C}^g/\Lambda \to \mathbb{C}^g/\Lambda,$$

where λ_A is the natural isogeny $E^g \to E^g$ induced by the matrix A. Then

$$\ker \lambda_A = A^{-1}\mathbb{Z}^g + \tau A^{-1}\mathbb{Z}^g \mod \Lambda$$

and

$$\ker \rho = (\ker \lambda_A) \cap C^g.$$

Now

$$\psi_A(E, C) \approx E^g/((\ker \lambda_A) \cap C^g) = E^g/(\ker \rho) \cong \mathbb{C}^g/\Lambda_A \cong \mathbb{C}^g/\tilde{\Lambda}_A \approx \psi_{A,\mathbb{C}}(E, C).$$

Elements of $\mathcal{A}_g$ can be viewed as pairs $(\mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \mathcal{E})$ where $\Omega \in \mathbb{H}_g$ and where $\mathcal{E} : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$ is the alternating Riemann form that satisfies $\mathcal{E}(u, \Omega v) = u^t v$ for all $u, v \in \mathbb{R}^g$. See for example [Rosen 1986].

The (nonprincipal) polarization λ_A on $E^g = \mathbb{C}^g/\Lambda$ corresponds to the alternating Riemann form that satisfies $\mathcal{E}_A(u, \tau v) = u^t Av$ for all $u, v \in \mathbb{R}^g$. Since $\mathcal{E}_A(\Lambda_A \times \Lambda_A) \subseteq \mathbb{Z}$, it follows that $\mathcal{E}_A$ is an alternating Riemann form for $\mathbb{C}^g/\Lambda_A$ as well. Since the polarization $\mathcal{E}_A$ descends from λ_A, and the polarization coming from ψ_A is the unique polarization also descending from λ_A, we have

$$\psi_A(E, C) = (\mathbb{C}^g/\Lambda_A, \mathcal{E}_A).$$

We have that $\psi_{A,\mathbb{C}}(E, C) = (\mathbb{C}^g/\tilde{\Lambda}_A, \tilde{\mathcal{E}})$ where $\tilde{\mathcal{E}}$ denotes the alternating Riemann form that satisfies $\tilde{\mathcal{E}}(u, \tau A v) = u^t v$ for all $u, v \in \mathbb{R}^g$. If $u, v \in \mathbb{R}^g$, then

$$\tilde{\mathcal{E}}(u, \tau A v) = u^t v = \mathcal{E}_A(A^{-1}u, \tau v) = \mathcal{E}_A(A^{-1}u, A^{-1}\tau A v).$$

Thus multiplication by A on $\mathbb{C}^g$ induces an isomorphism of polarized abelian varieties

$$\psi_A(E, C) = (\mathbb{C}^g/\Lambda_A, \mathcal{E}_A) \xrightarrow{\sim} (\mathbb{C}^g/\tilde{\Lambda}_A, \tilde{\mathcal{E}}) = \psi_{A,\mathbb{C}}(E, C),$$

as desired. □

Suppose g is a positive integer. Let $\mathcal{Q}$ denote the set of $g \times g$ symmetric, half-integral, positive semidefinite matrices. If f is a Siegel modular form on $\mathcal{A}_g$, ℓ is a prime not equal to the characteristic of the base, and $A \in M(g, \ell)$, let $\psi_A^*(f) = f \circ \psi_A$ denote the pullback modular form on $X_0(\det(A))$. Note that the cusp ∞ on $X_0(\det(A))$ is characterized by the fact that the universal elliptic curve has type I_1 reduction there.

Proposition 4.8. *Suppose $g \in \mathbb{Z}_{\geq 1}$, ℓ is a prime number, k an algebraically closed field with* $\mathrm{char}(k) \neq \ell$, *and f a k-valued Siegel modular form on $\mathcal{A}_g$. Then there is a function $c : \mathcal{Q} \to k$ such that for all $A \in M(g, \ell)$, the q-expansion of $\psi_A^*(f)$ at ∞ is*

$$\sum_{Q \in \mathcal{Q}} c(Q) q^{\mathrm{Tr}(AQ)}. \tag{4.9}$$

Proof. We first prove the result over $\mathbb{C}$. Let $\overline{\mathcal{A}_g}$ be a toroidal compactification of $\mathcal{A}_g$. Let $A \in M(g, \ell)$ and let $N = \det(A)$. The rational map ψ_A extends to a morphism $X_0(N) \to \overline{\mathcal{A}_g}$. Let τ_{ij} (resp. τ) with $1 \leq i \leq j \leq g$ be the standard coordinates for $\mathbb{H}_g$ (resp. $\mathbb{H}$), and let q_{ij} (resp. q) be $e^{2\pi i \tau_{ij}}$ (resp. $e^{2\pi i \tau}$). By Proposition 4.7, $\psi_A^*(q_{ij}) = q^{A_{ij}}$. Setting $q_{ji} = q_{ij}$, the modular form f has an expansion of the form

$$\sum_{Q \in \mathcal{Q}} c(Q) \prod_{i,j=1}^{g} q_{ij}^{Q_{ij}}.$$

Thus at the cusp ∞ of $X_0(N)$, the q-expansion of $\psi_A^*(f)$ is

$$\sum_{Q \in \mathcal{Q}} c(Q) \prod_{i,j=1}^{g} q^{A_{ij} Q_{ij}} = \sum_{Q \in \mathcal{Q}} c(Q) q^{\sum_{i,j=1}^{g} A_{ij} Q_{ij}} = \sum_{Q \in \mathcal{Q}} c(Q) q^{\mathrm{Tr}(AQ)}.$$

Let $\mathcal{A}_g^*$ be the minimal compactification of $\mathcal{A}_g$. There is a contraction map $\overline{\mathcal{A}_g} \to \mathcal{A}_g^*$. Composing ψ_A with this contraction, we obtain a morphism $X_0(N) \to \mathcal{A}_g^*$, which we will also call ψ_A. By [Faltings and Chai 1990, Theorem V.2.3] we have

$$\mathcal{A}_g^* = \mathrm{Proj}(\oplus_{j=0}^{\infty} \Gamma(\overline{\mathcal{A}_g}, \omega^j)),$$

where ω^j is the sheaf of Siegel modular forms of weight j. Since the sheaf of weight 2 modular forms is ample, we have

$$X_0(N) = \mathrm{Proj}(\oplus_{j=0}^{\infty} \Gamma(X_0(N), \omega_0^j)),$$

where ω_0^j is the sheaf of modular forms of weight j on $X_0(N)$. Therefore the morphism $\psi_A : X_0(N) \to \mathcal{A}_g^*$ is characterized by the pullback map

$$\psi_A^* : \bigoplus_{j=0}^{\infty} \Gamma(\overline{\mathcal{A}_g}, \omega^j) \to \bigoplus_{j=0}^{\infty} \Gamma(X_0(N), \omega_0^j).$$

Both graded algebras are finitely generated over $\mathbb{Z}[1/\ell]$, and furthermore ψ_A^* is Galois equivariant. Hence ψ_A descends to a morphism of schemes over $\mathbb{Z}[1/\ell]$. By functoriality of q-expansions, ψ_A^* over $\mathbb{Z}[1/\ell]$ is given by formula (4.9). Now base-extend to k. Let f be a Siegel modular form on $\mathcal{A}_g$. By [Faltings and Chai 1990, Theorem V.2.3], $\mathcal{A}_g^*$ has only one zero-dimensional cusp, so f has a unique q-expansion, say $\sum_{Q \in \mathcal{Q}} c(Q) \prod_{i,j=1}^{g} q_{ij}^{Q_{ij}}$. Since ψ_A^* over k is obtained by base-extension from $\mathbb{Z}[1/\ell]$, formula (4.9) holds over k as well. □

Proof of Theorem 1.10. We claim that $\cup X_A$ is Zariski dense in $\mathcal{A}_g$. The claim is trivial when $g = 1$, so we assume $g \geq 2$. It suffices to show that for all nonzero Siegel modular functions $f : \mathcal{A}_g \to k$, there exists $A \in M(g, \ell)$ such that the pullback $\psi_A^*(f)$ is nonzero. View f as a global section of the structure sheaf. Then by Proposition 4.8, there exist coefficients $c(Q) \in k$ for $Q \in \mathcal{Q}$, such that for almost all $A \in M(g, \ell)$, $\psi_A^*(f)$ admits a q-expansion $\sum_{Q \in \mathcal{Q}} c(Q) q^{\mathrm{Tr}(AQ)}$.

Let $S = \{Q \in \mathcal{Q} : c(Q) \neq 0\}$. By Proposition 4.5 applied to the set S, there is an open cone C of $g \times g$ real, symmetric, positive definite matrices A such that $\mathrm{Tr}(AQ)$ is minimized by a unique $Q \in S$.

By Lemma 4.2, there exists an element of C of the form rGG^t with $r \in \mathbb{R}^+$ and $G \in \mathrm{SL}_g(\mathbb{Z}[1/\ell])$. Since C is a cone, we may scale this element to obtain a matrix $A \in M(g, \ell) \cap C$.

Let $n = \min\{\mathrm{Tr}(AQ) : Q \in S\}$. By the definition of C, there is a unique $Q_0 \in S$ such that $\mathrm{Tr}(AQ_0) = n$. Thus, the coefficient of q^n in the q-expansion of $\psi_A^*(f)$ is $c(Q_0)$. Since $Q_0 \in S$, we have $c(Q_0) \neq 0$. Hence $\psi_A^*(f) \neq 0$, as desired. □

Remark 4.10. In the case $k = \mathbb{C}$, we can give a simpler proof of Theorem 1.10, as follows. By Lemma 4.6 and Proposition 4.7, if $A \in M(g, \ell)$ then the map $\mathbb{H} \to \mathbb{H}_g$ defined by $\tau \mapsto \tau A$ induces the map $\psi_A : Y_0(\det(A)) \to \mathcal{A}_g$. Let

$$V = \{\tau A : \tau \in \mathbb{H}, A \in M(g, \ell)\} \subseteq \mathbb{H}_g.$$

By Lemma 4.2, the topological closure of V in $\mathbb{H}_g$ contains the purely imaginary locus, i.e., the set of matrices of the form iB where B is a real, symmetric, positive definite matrix. But any holomorphic function that vanishes on the purely imaginary locus must be the zero map. It follows that the image of V in $\mathcal{A}_g$ is Zariski dense, as desired.

5. Proof of Corollary 1.5

Suppose that g and n are positive integers. Let $\mathcal{A}_{g,n}$ denote the moduli space for triples (A, λ, L), where A is a g-dimensional abelian variety, λ is a principal polarization on A, and L is a level n structure, i.e., L is a symplectic basis $(P_1, \dots, P_g, Q_1, \dots, Q_g)$ for the n-torsion $A[n]$.

Define an equivalence relation $\overset{n}{\approx}$ on $\mathcal{A}_{g,n}$ by $(A_1, \lambda_1, L_1) \overset{n}{\approx} (A_2, \lambda_2, L_2)$ if and only if $A_1 \approx A_2$ and there is an isomorphism $\varphi : A_1 \to A_2$ such that $\varphi(L_1) = L_2$. Define a set $\mathcal{U}_{g,n}(k) \subseteq (\mathcal{A}_{g,n} \times \mathcal{A}_{g,n})(k)$ by

$$\mathcal{U}_{g,n}(k) = \{(x_1, x_2) \in \mathcal{A}_{g,n}(k) \times \mathcal{A}_{g,n}(k) \mid x_1 \overset{n}{\approx} x_2\}.$$

Proposition 5.1. *If $g \in \mathbb{Z}_{\geq 2}$, k is an algebraically closed field, and n is an integer with* $\operatorname{char}(k) \nmid n$, *then the set $\mathcal{U}_{g,n}(k)$ is Zariski dense in the k-scheme $\mathcal{A}_{g,n} \times \mathcal{A}_{g,n}$.*

Proof. Let $\pi : \mathcal{A}_{g,n} \to \mathcal{A}_g$ be the forgetful map $(A, \lambda, L) \mapsto (A, \lambda)$. Then π is finite-to-one, and $(\pi \times \pi)(\mathcal{U}_{g,n}(k)) = \mathcal{W}_g(k)$. By Theorem 1.2, $\mathcal{W}_g(k)$ is Zariski dense in $\mathcal{A}_g \times \mathcal{A}_g$, so the dimension of the Zariski closure of $\mathcal{W}_g(k)$ is $2 \dim \mathcal{A}_g$. Therefore the dimension of the Zariski closure of $\mathcal{U}_{g,n}(k)$ is also $2 \dim \mathcal{A}_g = 2 \dim \mathcal{A}_{g,n}$. Since $\mathcal{A}_{g,n}$ is connected, so is $\mathcal{A}_{g,n} \times \mathcal{A}_{g,n}$, and the desired result follows. □

If D is a polarization type, define a set $\mathcal{W}_{g,D}(k) \subseteq (\mathcal{A}_{g,D} \times \mathcal{A}_{g,D})(k)$ by

$$\mathcal{W}_{g,D}(k) = \{((B_1, \mu_1), (B_2, \mu_2)) \in \mathcal{A}_{g,D}(k) \times \mathcal{A}_{g,D}(k) \mid B_1 \approx B_2\}.$$

Proposition 5.2. *If $g \in \mathbb{Z}_{\geq 2}$, k is an algebraically closed field, $D = (d_1, \dots, d_g)$ is a polarization type, and* $\operatorname{char}(k) \nmid d_g$, *then the set $\mathcal{W}_{g,D}(k)$ is Zariski dense in the k-scheme $\mathcal{A}_{g,D} \times \mathcal{A}_{g,D}$.*

Proof. Let $n = d_g$. Let $\pi_D : \mathcal{A}_{g,n} \to \mathcal{A}_{g,D}$ be the morphism on moduli spaces induced by the morphism of stacks f defined on the bottom of page 492 of [de Jong 1993]. Let ξ be a geometric generic point for the Zariski closure of $(\pi_D \times \pi_D)(\mathcal{U}_{g,n}(k))$ in $\mathcal{A}_{g,D} \times \mathcal{A}_{g,D}$. Let ξ' be a geometric generic point for $(\pi_D \times \pi_D)^{-1}(\bar{\xi})$, where $\bar{\xi}$ is the Zariski closure of ξ. Then $\mathcal{U}_{g,n}(k) \subseteq (\pi_D \times \pi_D)^{-1}(\bar{\xi}) = \overline{\xi'}$. By Proposition 5.1, the Zariski closure of $\mathcal{U}_{g,n}(k)$ is $\mathcal{A}_{g,n} \times \mathcal{A}_{g,n}$. It follows that $\overline{\xi'} = \mathcal{A}_{g,n} \times \mathcal{A}_{g,n}$. Since $\pi_D \times \pi_D$ is finite, we have

$$\dim(\bar{\xi}) = \dim(\overline{\xi'}) = \dim(\mathcal{A}_{g,n} \times \mathcal{A}_{g,n}) = \dim(\mathcal{A}_{g,D} \times \mathcal{A}_{g,D}).$$

By [de Jong 1993, Proposition 1.11], $\mathcal{A}_{g,D}$ is irreducible. It follows that $\mathcal{A}_{g,D} \times \mathcal{A}_{g,D} = \bar{\xi}$, which is the Zariski closure of $(\pi_D \times \pi_D)(\mathcal{U}_{g,n}(k))$. Thus, $(\pi_D \times \pi_D)(\mathcal{U}_{g,n}(k))$ is Zariski dense in $\mathcal{A}_{g,D} \times \mathcal{A}_{g,D}$.

Suppose $(A_1, \lambda_1, L_1) \overset{n}{\approx} (A_2, \lambda_2, L_2)$ in $\mathcal{A}_{g,n}$. Let $(B_i, \mu_i) = \pi_D(A_i, \lambda_i, L_i)$. From the definition of π_D, we have $B_i^\vee = A_i^\vee / H_i$ for some subgroup $H_i \subset A_i^\vee[n]$. By the definition of $\overset{n}{\approx}$, there is a weak isomorphism $A_2 \xrightarrow{\sim} A_1$ whose dual sends H_1 isomorphically onto H_2, and hence $B_1^\vee \approx B_2^\vee$. It follows that $B_1 \approx B_2$, and therefore $(\pi_D \times \pi_D)(\mathcal{U}_{g,n}(k)) \subseteq \mathcal{W}_{g,D}(k)$. The desired result now follows. □

The proof of Corollary 1.5 is now the same as the proof of Theorem 1.1, replacing the use of Theorem 1.2 with the use of Proposition 5.2.

References

[Bass 1964] H. Bass, "K-theory and stable algebra", *Inst. Hautes Études Sci. Publ. Math.* **22** (1964), 5–60. MR Zbl

[Boneh et al. 2020] D. Boneh, D. Glass, D. Krashen, K. Lauter, S. Sharif, A. Silverberg, M. Tibouchi, and M. Zhandry, "Multiparty non-interactive key exchange and more from isogenies on elliptic curves", *J. Math. Cryptol.* **14**:1 (2020), 5–14. MR Zbl

[Cox 2013] D. A. Cox, *Primes of the form $x^2 + ny^2$*, 2nd ed., Wiley, Hoboken, NJ, 2013. MR Zbl

[Faltings and Chai 1990] G. Faltings and C.-L. Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik (3) **22**, Springer, 1990. MR Zbl

[de Jong 1993] A. J. de Jong, "The moduli spaces of polarized abelian varieties", *Math. Ann.* **295**:3 (1993), 485–503. MR Zbl

[Kani 2011] E. Kani, "Products of CM elliptic curves", *Collect. Math.* **62**:3 (2011), 297–339. MR Zbl

[Kohel 1996] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California, Berkeley, 1996, available at https://www.proquest.com/docview/304241260.

[Milne 1986] J. S. Milne, "Abelian varieties", pp. 103–150 in *Arithmetic geometry* (Storrs, CT, 1984), edited by G. Cornell and J. H. Silverman, Springer, 1986. MR Zbl

[Mumford 1966] D. Mumford, "On the equations defining abelian varieties, I", *Invent. Math.* **1** (1966), 287–354. MR Zbl

[Mumford et al. 1994] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, 3rd ed., Ergebnisse der Mathematik (2) **34**, Springer, 1994. MR Zbl

[Rains 2020] E. M. Rains, "Elliptic double affine Hecke algebras", *SIGMA* **16** (2020), art. id. 111. MR Zbl

[Rosen 1986] M. Rosen, "Abelian varieties over $\mathbb{C}$", pp. 79–101 in *Arithmetic geometry* (Storrs, CT, 1984), edited by G. Cornell and J. H. Silverman, Springer, 1986. MR Zbl

Communicated by Martin Olsson
Received 2019-12-16 Revised 2020-07-10 Accepted 2020-10-17

rains@caltech.edu — *Department of Mathematics, California Institute of Technology, Pasadena, CA, United States*

krubin@uci.edu — *Department of Mathematics, University of California, Irvine, CA, United States*

traviswscholl@gmail.com — *Department of Mathematics, University of California, Irvine, CA, United States*

ssharif@csusm.edu — *Department of Mathematics, California State University San Marcos, San Marcos, CA, United States*

asilverb@uci.edu — *Department of Mathematics, University of California, Irvine, CA, United States*