20130806

Special point problems with elliptic modular surfaces

Jonathan Pila

Abstract

We prove a "special point" result for products of elliptic modular surfaces, elliptic curves, multiplicative groups and complex lines, and deduce a result about vanishing linear combinations of singular moduli and roots of unity.

2010 Mathematics Subject Classification: 11G18, 03C64

Keywords: André-Oort conjecture, Zilber-Pink conjecture, Mann theorem.

1. Introduction

The objectives of this paper are twofold: to generalise the main result of [34], and to obtain an analogue for singular moduli of Mann's theorem [25] on linear relations between roots of unity. In particular we affirm the "mixed André-Oort conjecture" for products of *elliptic modular surfaces* (see §2.2). This is a special case of a "generalised André-Oort conjecture" suggested by André [3], where it is affirmed in the case of a single elliptic modular surface; it is also a special case of the Zilber-Pink conjecture [7, 40, 41, 56]. More generally we establish a "special point" result for varieties of the form

$$X = B_1 \times \ldots \times B_n \times E_1 \times \ldots \times E_m \times \mathbb{G}^\ell \times \mathbb{C}^k,$$

where k, ℓ, m, n are non-negative integers, B_i are elliptic modular surfaces associated with suitable congruence subgroups $\Gamma_i \subset \mathrm{SL}_2(\mathbb{Z})$, E_j are elliptic curves defined over $\mathbb{C}$, and $\mathbb{G} = \mathbb{G}_{\mathrm{m}} = \mathbb{G}_{\mathrm{m}}(\mathbb{C})$ is the multiplicative group of non-zero complex numbers (we identify a variety with its set of complex points).

By a *subvariety* $T \subset X$ we will mean a Zariski closed irreducible subvariety of X. Associated with X is a collection of subvarieties called *special subvarieties*. These are defined in detail below (§4). Let us say here that we may (and will) assume that the E_i are all non-CM. Then a special subvariety of X is a cartesian product of special subvarieties in $\prod_i B_i, \prod_j E_j, \mathbb{G}^\ell$, and $\mathbb{C}^k$. In $\prod_j E_j$ (and respectively $\mathbb{G}^\ell$) these are *torsion cosets*, namely translates of abelian subvarieties (respectively subtori) by torsion points. The special subvarieties of $\mathbb{C}^k$ we take to be subvarieties with a Zariski-dense set of rational points. Special subvarieties of dimension 0 are called *special points*, and they are Zariski-dense in any special subvariety. The "special point" result asserts the converse of this: a subvariety $T \subset X$ with a Zariski-dense set of special points is special. This may be equivalently stated as follows.

1.1. Theorem. *A Zariski closed algebraic subset $V \subset X$ defined over $\mathbb{C}$ contains only finitely many maximal special subvarieties.*

For a Shimura variety and its special subvarieties the "special point" problem is known as the *André-Oort conjecture* (AO; [1, 28]) and has been affirmed, under GRH for CM fields, in work of Klingler, Ullmo, and Yafaev [22, 51]. Unconditional results have been obtained in various special cases [2, 9, 34, 36, 37, 50]. Each B_i contains the associated modular curve $Y_i = \Gamma_i \backslash \mathbb{H}$ (where $\mathbb{H}$ is the complex upper half-plane) as a special subvariety, so the present result includes the result of [34] affirming AO for a product of modular curves, in particular for the Shimura variety $Y(1)^n$ whose complex points may be identified with $\mathbb{C}^n$ parameterising n-tuples of elliptic curves by their j-invariants. In the case $n = 2$ this is a result of André [2]; a proof that is unconditional and effective has recently been given by Kühne [23] and (see [23]) independently by Bilu, Masser, and Zannier. In $Y(1)^n$ the special points are n-tuples of *singular moduli*, the j-invariants of CM elliptic curves.

For multiplicative groups and abelian varieties, the "special point" problem is known as the *Manin-Mumford conjecture*. For abelian varieties it is a theorem of Raynaud [42, 43]; for the multiplicative group it is a special case of a ("multiplicative Mordell-Lang") theorem of Laurent [24]; in the semiabelian setting it is due to Hindry [21]. For $k = n = 0$ Theorem 1.1 recovers a rather special case. Our present result improves that in [34] here in allowing the E_j to be defined over $\mathbb{C}$ rather than $\overline{\mathbb{Q}}$.

In fact we can generalise Theorem 1.1 to a version in which some finite number of Hecke orbits of moduli are considered to be special in addition to the CM ones, giving a version that includes the "Mordell-Lang" statement for $Y(1)^n$ established in our joint paper [19] with Philipp Habegger (extending it to finite subsets of $\mathbb{C}$ rather than $\overline{\mathbb{Q}}$).

The case of Theorem 1.1 (and of its generalisation 6.6) with $k = 0$, together with all the results mentioned above, are comprehended within the Zilber-Pink conjecture (ZP), in which the ambient variety is a mixed Shimura variety. An additional feature in 1.1 is the factor $\mathbb{C}^k$ for which, by itself, the special point result reduces to a triviality. It amounts essentially to a uniformity aspect of the result, which was already observed in [34, §13]. Here we explicate a particular consequence: the aforementioned modular analogue of Mann's theorem.

Let $a, b \in \overline{\mathbb{Q}}^*$. André's original result applied to the curve $ax + by = 1$ in $Y(1)^2$ (which is never modular), implies that there are only finitely many pairs (j_1, j_2) of singular moduli with

$$aj_1 + bj_2 = 1.$$

Theorem 1.1 applied to the product of $Y(1)^n$ with $\mathbb{G}^\ell \times \mathbb{C}^{n+\ell+1}$ gives a stronger finiteness statement about linear relations among singular moduli and roots of unity.

1.2. Definition. Let n, ℓ be non-negative integers.

1. A tuple $(j_1, \ldots, j_n, \zeta_1, \ldots, \zeta_\ell)$ is called an *(n, ℓ)-tuple* if the j_i are special, the ζ_j are roots of unity, and they satisfy a non-trivial relation

$$a_1 j_1 + \ldots + a_n j_n + b_1 \zeta_1 + \ldots + b_\ell \zeta_\ell + c = 0$$

where a_i, b_j, c are rational numbers.

2. An (n, ℓ)-tuple is called *non-degenerate* if

(i) there do not exist a non-empty subset $I \subset \{1, \ldots, n\}$ and a singular modulus j such that $j_i = j$ for all $i \in I$ and $\sum_{i \in I} a_i = 0$,

(ii) no proper (non-empty) subsum of $b_1\zeta_1 + \ldots + b_\ell\zeta_\ell + c$ vanishes (but we allow c to be absent if $\ell = 0$).

1.3. Theorem. *For given n, ℓ there are only finitely many non-degenerate (n, ℓ)-tuples.*

Modulo some rather elementary considerations to characterise special subvarieties of linear subvarieties, this theorem follows from [34, Theorem 13.2]. For roots of unity only (i.e. $n = 0$) the result is due to Mann [25]. It preceded the Manin-Mumford conjecture, which may be deduced from it in the multiplicative case (see [12]). Mann's result is effective (even explicit); ours is not. For further developments see [15, 13] and §7.8. For $\ell = 0$ and $n = 2$ the finiteness result follows from the proof of AO for $Y(1)^2$ in [33] (see also Kühne [23, Theorem 3]). None of these results appear to enable effective determination of the finitely many $(2, 0)$-tuples, as asked at the AIM conference on "Unlikely intersections in algebraic groups and Shimura varieties", Centro De Giorgi, Pisa, 2011. Here again we frame a version allowing a finite number of Hecke orbits.

We follow the strategy of [34], opposing the Counting Theorem for rational points on definable sets in o-minimal structures [38] with lower bounds for the size of the Galois orbit of a special point as originally proposed by Umberto Zannier for reproving the Manin-Mumford conjecture [39]. This shows the efficacy of the Point-Counting strategy in the mixed setting. As in [34] we also use o-minimality in other parts of the argument, and it is crucial to the uniformity aspects (which are crucial to 1.4).

A key ingredient in this strategy is a certain functional algebraic independence statement which I have dubbed "Ax-Lindemann-Weierstrass". The statement and proof here generalise those in [34]; the proof, which uses point counting in definable sets as in [34, 37, 52], is therefore presented efficiently, in §5.

The proof of Theorem 1.1 is carried out in §6. It has an inductive structure in which it is crucial to observe that the special subvarieties (and even weakly special subvarieties) occur as "special points" of certain semialgebraic families. This was easily observed in [34] for the case of products of modular curves, and has also been carried out for Siegel modular varieties [37] and general Shimura varieties [50]. The corresponding structure here is somewhat cumbersome in detail; §4 is devoted to this. Finally the proof of 1.4 is carried out in §7.

The present results overlap with those of Habegger [18], with no inclusion in either direction. Habegger treats fibred products of elliptic surfaces over a general base curve, while we treat cartesian products of elliptic surfaces over a modular base curve.

Acknowledgements. I thank Philipp Habegger, Jacob Tsimerman, and Boris Zilber for helpful conversations and communications. Part of the research and writing of this paper was carried out while I was participating in the "Model Theory and Applications"

programme at the Max Planck Institute for Mathematics (April-June 2012). I thank the organisers for inviting me to participate, and the Max Planck Institute for its hospitality and for the excellent environment it provides for mathematics. I am grateful to the Clay Mathematics Institute for supporting my visit.

2. Preliminaries

Elliptic modular surfaces

2.1. Notation. The semidirect product $\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ acts on $\mathbb{H} \times \mathbb{C}$ by

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, (u,v)\right)(\tau, z) = \left(\frac{a\tau + b}{c\tau + d}, \frac{z + u\tau + v}{c\tau + d}\right).$$

This action may be extended to $\mathrm{SL}_2(\mathbb{R}) \ltimes \mathbb{R}^2$ in the obvious way. We will write

$$\ell(g, \tau) = c\tau + d \quad \text{for } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}), \quad \tau \in \mathbb{H}.$$

For a congruence subgroup $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ we set

$$\Gamma^+ = \{(g, \lambda) \in \mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2 : g \in \Gamma\}.$$

We take a fundamental domain F_Γ for the action of Γ on $\mathbb{H}$ consisting of finitely many images γF_0 of the usual fundamental domain F_0 for $\mathrm{SL}_2(\mathbb{Z})$ with $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. For $\tau \in \mathbb{H}$ we let $L_\tau = \{\alpha + \beta\tau \in \mathbb{C} : 0 \leq \alpha, \beta \leq 1\}$, a (closure of a) fundamental domain for $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ on $\mathbb{C}$. Then

$$F_\Gamma^+ = \{(\tau, z) : \tau \in F_\Gamma, z \in L_\tau\}$$

is a fundamental domain for the action of Γ^+ on $\mathbb{H} \times \mathbb{C}$.

2.2. Elliptic modular surfaces. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup, which we assume does not contain $-\mathrm{id}$, and so acts effectively on $\mathbb{H}$. The quotient of $\mathbb{H} \times \mathbb{C}$ by Γ^+ is a quasiprojective algebraic surface fibred over the modular curve $Y_\Gamma = \Gamma\backslash\mathbb{H}$, with a section. Such a surface, which we will denote B_Γ, is called an *elliptic modular surface.* It is an elliptic surface: the fibre over $y \in Y$, the image of $\tau \in \mathbb{H}$, is the elliptic curve corresponding to $\tau \in \mathbb{H}$. For further information see [47, 49]. The map $\pi : \mathbb{H} \times \mathbb{C} \to B_\Gamma$ is given by suitable quotients of theta-functions (see e.g. [33] for the case of the Legendre surface $L : y^2 = x(x-1)(x-\lambda), L = \Gamma(2)\backslash\mathbb{H} \times \mathbb{C}$).

Uniformisation, group action, real coordinates, definability

We will be dealing throughout with certain transcendental uniformisations $\pi : U \to X$, where X is a quasi projective variety, and π is invariant under the action of some discrete subgroup Γ of a real group G of biholomorphic automorphisms of U.

2.3. Definition.

1. For an elliptic modular surface $X = \Gamma^+\backslash\mathbb{H} \times \mathbb{C}$ as above, we have $U_X = \mathbb{H} \times \mathbb{C}$ and π_X the quotient map. We have $\Gamma_X = \Gamma^+$, with fundamental domain $F_X = F_\Gamma^+$ as described above, and $G_X = \mathrm{SL}_2(\mathbb{R}) \ltimes \mathbb{R}^2$. We take real coordinates on U_X by writing $(\tau, z) = (x, y, u, v)$ where $\tau = x + iy$ and $z = u + v\tau$. We use real and imaginary parts on X.

2. For an elliptic curve $X = E$ we choose some $\sigma \in \mathbb{H}$ such that $\mathbb{C}/\Lambda_\sigma$, where $\Lambda_\sigma = \mathbb{Z} + \mathbb{Z}\sigma$, is analytically isomorphic to E. So $U_X = \mathbb{C}$, the uniformisation π_X given e.g. by the Weierstrass $\wp$-function and its derivative. We have $\Gamma_X = \mathbb{Z}^2$, $G_X = \mathbb{R}^2$ (where (u, v) acts by translation by $u + v\sigma$). We take $F_X = \{w = u + v\sigma \in \mathbb{C} : 0 \le u, v < 1\}$. We put real coordinates on $\mathbb{C}$ by writing $w = u + v\sigma$, and use real and imaginary parts on X.

3. For $X = \mathbb{G}$ we take $U_X = \mathbb{C}$ and $\pi_X = \exp$. We have $\Gamma_X = \mathbb{Z}$ and $G_X = \mathbb{R}$, with $u \in \mathbb{R}$ acting by translation by $2\pi iu$. We take $F_X = \mathbb{R} \times i[0, 2\pi)$. We use $\mathrm{Re}(z)/2\pi$ and $\mathrm{Im}(z)/2\pi$ as real coordinates on U_X, real and imaginary parts on X.

4. For $X = \mathbb{C}$ we take $U = \mathbb{C}$ and $\pi_X = \mathrm{id}$, the identity map. We take $\Gamma_X = G_X = \{1\}$ and $F_X = \mathbb{C}$, and we use real and imaginary parts on U_X and X.

5. In general X is a cartesian product of quasiprojective varieties X_i of the above kinds. Then U_X, Γ_X, G_X, F_X are the corresponding cartesian products of U_{X_i}, Γ_{X_i}, G_{X_i}, F_{X_i} and the real coordinates on U_X, X are the cartesian product of the real coordinates on U_{X_i}, X_i.

Different forms of X are considered in various parts of the paper. We try to make it clear in each (sub-)section which form of X is being considered and drop "X" as a subscript.

2.4. Definability and point-counting. For the definition of an "o-minimal structure over $\mathbb{R}$" and a summary of key properties see [34]. For a development of the theory see [11]. To apply the Counting Theorem [38, 34] it is essential that the uniformising maps, restricted to the relevant fundamental domains, are *definable in an o-minimal structure over* $\mathbb{R}$ (and indeed in the same structure). In fact, all these (restricted) maps are definable in $\mathbb{R}_{\mathrm{an\ exp}}$. For the elliptic modular uniformisations this is due to Peterzil-Starchenko [31]. On the other factors the definability in $\mathbb{R}_{\mathrm{an\ exp}}$ is obvious. The o-minimality of $\mathbb{R}_{\mathrm{an\ exp}}$ is due to van den Dries-Miller [14], building on the o-minimality of $\mathbb{R}_{\mathrm{exp}}$, due to Wilkie [53], and of $\mathbb{R}_{\mathrm{an}}$. The latter follows from Gabrielov's theorem [17], as observed by van den Dries [10].

Henceforward, *definable* means definable (with parameters) in $\mathbb{R}_{\mathrm{an\ exp}}$.

"Subvarieties" of U

In all the cases we consider U is open in the corresponding ambient complex space $\mathbb{C}^N$, and semialgebraic as a subset of the relevant ambient real space $\mathbb{R}^{2N}$. We will call such a domain a *semialgebraic complex domain*.

We will need to consider various complex algebraic "subvarieties" of our uniformising spaces U. Due to the $\mathbb{H}$ factors, these U are not themselves complex algebraic, and may not contain any complex algebraic subvarieties of $\mathbb{C}^N$ (e.g. $\mathbb{H}$ does not, being biholomorphic via an algebraic map to the open unit disc).

2.5. Definition. For a semialgebraic complex domain U, a *subvariety* of U will mean a non-empty connected component W of $U \cap Y$ for some complex irreducible variety $Y \subset \mathbb{C}^N$.

3. Special points

Special points

In this subsection we take

$$X = B_1 \times \ldots \times B_n \times \mathbb{G}^\ell \times \mathbb{C}^k, \qquad U = \big(\mathbb{H} \times \mathbb{C}\big)^n \times \mathbb{C}^\ell \times \mathbb{C}^k.$$

Let $\sigma \in \mathbb{H}$. The *Hecke orbit* of σ is $\mathrm{GL}_2^+(\mathbb{Q})\sigma$. We say τ_1, τ_2 are *Hecke equivalent* if they are in the same Hecke orbit.

3.1. Definition. Let $\Sigma \subset \mathbb{H}$ and $d \in \mathbb{N}^+$.

1. A *special point* of $\mathbb{H}$ is a point $\tau \in \mathbb{H}$ with $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$. A Σ-*special point* of $\mathbb{H}$ is a point τ such that τ is either special or in the Hecke orbit of σ for some $\sigma \in \Sigma$.
2. Let $\tau \in \mathbb{H}$. A τ-*special point* of $\mathbb{C}$ is a division point of the lattice Λ_τ.
3. An exp-*special point* of $\mathbb{C}$ is a rational multiple of $2\pi i$.
4. A d-*special point* in $\mathbb{C}$ is a point t with $[\mathbb{Q}(t) : \mathbb{Q}] \leq d$.

3.2. Definition. With X, U as above, let $\Sigma \subset \mathbb{H}$, $d \in \mathbb{N}^+$. A point

$$(\tau_1, z_1, \ldots, \tau_n, z_n, w_1, \ldots, w_m, \zeta_1, \ldots, \eta_\ell, t_1, \ldots, t_k) \in U$$

is called (Σ, d)-*special* if:

1. each τ_i is Σ-special,
2. each z_i is τ_i-special,
3. each ζ_i is exp-special, and
4. each t_i is d-special.

We now define, for a subset $S \subset Y(1)(\mathbb{C})$, the (S, d)-special points of X. This will be in terms of the j-invariant of the elliptic curves parameterised by the corresponding points of the B_i. For $x \in \mathbb{C}$ write E_x for an elliptic curve with j-invariant $j(E) = x$. Such a curve is unique up to isomorphism over $\mathbb{C}$. We consider an elliptic curve E_x to be S-special if it is isogenous to E_s for some $s \in S$. Suppose $x = j(\tau), y = j(\sigma)$ where $\sigma, \tau \in \mathbb{H}$. Then E_x and E_y are isogenous precisely if $\tau \in \mathrm{GL}_2^+(\mathbb{Q})\sigma$. As $j^{-1}(x)$ is an $\mathrm{SL}_2(\mathbb{Z})$-orbit in $\mathbb{H}$, this condition is independent of the pre-image chosen. We will then say that x, y (like τ, σ) are *Hecke equivalent* and in the same *Hecke orbit* (it is obviously an equivalence relation). The following definition is therefore independent of the chosen $\Sigma \subset j^{-1}(S)$ provided it contains at least one pre-image of each $s \in S$.

3.3. Definition. Let $S \subset Y(1)(\mathbb{C})$ and $d \in \mathbb{N}^+$. Let $\Sigma \subset \mathbb{H}$ consist of one element $\sigma \in j^{-1}(s)$ for each $s \in S$. An *(S,d)-special point* of X is the image under π of a (Σ, d)-special point of U.

Galois orbits of special points

In this subsection we take

$$X = B_1 \times \ldots \times B_n \times \mathbb{G}^\ell$$

and fix a finite subset $S \subset Y(1)(\mathbb{C})$. We may assume that the elements of S are non-special and pairwise Hecke inequivalent. We set $K = \mathbb{Q}(S)$.

3.4. Definition. Let $u \in X$ be an S-special point. We define the S-complexity of u, denoted $\Delta_S(u)$, as follows. Let us write $u = (P_1, \ldots, P_n, y_1, \ldots, y_\ell)$ with $P_i \in E_i$ a torsion point of order T_i and $y_i \in \mathbb{G}$ torsion of order R_i.

1. If E_i is CM, we let D_i be the discriminant of the endomorphism ring of E_i, and take $\Delta(P_i) = \max(|D_i|, T_i)$.

2. If E_i is isogenous to E_s for some $s \in S$, we let N_i be the minimal degree of a cyclic isogney $E_s \to E_i$ and take $\Delta(P_i) = \max(N_i, T_i)$.

3. We take $\Delta(y_i) = R_i$.

Finally we set

$$\Delta_S(u) = \max\big(\Delta(P_i), \Delta(y_j)\big).$$

3.5. Lemma. *With X, S fixed as above and $K = \mathbb{Q}(S)$, there exist positive constants c, δ, depending on X, S, such that, if $u \in X$ is S-special,*

$$[K(u) : K] \geq c\Delta_S(u)^\delta.$$

Proof. It suffices to show there exist $c, \delta > 0$ such that, if P is one of the P_i, and y is one of the y_i,

$$[K(P) : K] \geq c\Delta(P)^\delta, \quad [K(y) : K] \geq c\Delta(R)^\delta.$$

In the following, c_i, δ_i are positive constants depending (at most) on X, S.

Let B be a transcendence basis of K and $d = [K : \mathbb{Q}(B)]$. We deal with $K(y)$ first. We have $[\mathbb{Q}(y) : \mathbb{Q}] \geq c_1\Delta^{\delta_1}$ for suitable c_1 for any $\delta_1 < 1$, by estimates for the Euler ϕ-function (see e.g. Hardy and Wright [20, Th. 327]). Then

$$[K(y) : K] \geq (1/d)[\mathbb{Q}(B, y), \mathbb{Q}(B)] = (1/d)[\mathbb{Q}(y) : \mathbb{Q}] \geq (c_1/d)\Delta(y)^{\delta_1}.$$

The argument for P is similar. First suppose that P lies in a CM fibre E whose endomorphism ring has discriminant D. Suppose $T \leq |D|^8$. Let $v = j(E)$. By Siegel we have

$$[\mathbb{Q}(v) : \mathbb{Q}] \geq c_2(\delta)|D|^{\delta_2}$$

for suitable positive $c_2(\delta)$ (ineffective) for any $\delta_2 < 1/2$. Since there is a rational map from B to the corresponding modular curve Y, and a finite map from Y to $Y(1)$,

$$[K(P) : K] \geq (1/d)[\mathbb{Q}(B, P) : \mathbb{Q}(B)] = (1/d)[\mathbb{Q}(P) : \mathbb{Q}] \geq c_2|D|^{\delta_2} \geq c_3\Delta(P)^{\delta_3}$$

by our assumption on T. On the other hand if $T \geq |D|^8$, we have (by Silverberg [48], Corollary 3 and Lemma 5), if L is a field of definition for E

$$[L(P):L] \geq c_4 T^{\delta_4} \big([L:\mathbb{Q}]\big)^{-1}$$

for suitable positive c_4 provided $\delta_4 < 1$; take say $\delta = 1/2$. A field of definition L for E may be taken with $[L:\mathbb{Q}] \leq c_5[\mathbb{Q}(v):\mathbb{Q}] \leq c_6|D| \leq c_6 T^{1/8}$ (effectively) and so

$$[K(P):K] \geq c_6[\mathbb{Q}(P):\mathbb{Q}] \geq c_7 T^{1/4} = c_7 \Delta(P)^{1/4}.$$

Finally we suppose that P lies on E having a cyclic isogeny of degree N to E_s, $s \in S$. Suppose first that s is algebraic. Suppose $T \leq N^8$. By the results of Masser and Wüstholz [27] (or their subsequent improvements [8, 29]) we know that

$$[\mathbb{Q}\big(j(E), j(E_s)\big) : \mathbb{Q}\big(j(E_s)\big)] \geq c_8 N^{\delta_8}$$

for suitable positive c_8, δ_8 (c_8 depends on E_s but we may take $\delta_8 = 1/(4 + o(1))$ [29]).

Then

$$[K(P):K] \geq (1/d)[\mathbb{Q}(B,P):\mathbb{Q}] \geq c_9 N^{\delta_8} \geq c_9 \Delta(P)^{\delta_9}.$$

So suppose $T \geq N^8$. We have an isogeny $\phi : E_s \to E$ of degree N. Let $Q \in \phi^{-1}(P)$, a point of order at least NT. By results of Masser [26],

$$[\mathbb{Q}(Q):\mathbb{Q}] \geq c_{10}(NT)^{\delta_{10}} \geq c_{10} T^{\delta_{11}}$$

so that

$$[\mathbb{Q}(P):\mathbb{Q}] \geq c_{10} T^{\delta_{11}}/N \geq c_{11} T^{\delta_{12}}$$

and then

$$[K(P):K] \geq c_{12}[\mathbb{Q}(P):\mathbb{Q}] \geq c_{13} T^{\delta_{12}} \geq c_{13} \Delta(P)^{\delta_{13}}.$$

If s is transcendental we assume $s \in B$ then $[\mathbb{Q}(j(E)) : \mathbb{Q}(j(E_s)] = \deg \Phi_N$ and the rest of the argument is the same. □

Height bounds for special points

We need to show that the pre images in U of special points in X lying in a fixed fundamental domain for the Γ-action have height that is bounded by a power of their complexity.

Suppose $y \in \mathbb{G}$ is a special point, a root of unity of (minimal) order R. Then the pre image $\zeta \in F_{\mathbb{G}}$ of y is of the form $\zeta = 2\pi i q$ where $q \in \mathbb{Q}$ and $H(q) \leq R$ (in fact $H(q) = R$).

Consider now the uniformisation $\pi : \mathbb{H} \times \mathbb{C} \to B$ of an elliptic modular surface B, with fundamental domain F_B.

3.6. Lemma.

1. If $P \in B$ is special then its pre-image $(\tau, z) \in F$ corresponds (in the real coordinates) to a point $(x+iy, u+v\tau)$ where $x \in \mathbb{Q}$, y is quadratic, and $u, v \in \mathbb{Q}$, and

$$H(x, y, u, v) \leq C\Delta(P).$$

2. If $P \in B$ is s-special but not special, where $s \in \mathbb{C}$ with pre-image $\sigma \in F_0$, then the pre-image $(\tau, z) \in F$ of P has $z = u + v\tau$ with $u, v \in \mathbb{Q}$ and there is a $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$ with $\tau = g\sigma$ such that

$$H(u, v, a, b, c, d) \leq C\Delta(u)^{10}.$$

Proof. 1. The assertion for τ is (easy and) established in [34, 5.7]. For z it is easy.

2. The assertion for z is again easy. For τ it is (not hard and) in [19, 5.2]. □

4. Special subvarieties

For this section (and the next) it is convenient to omit the E_i factors from X, by viewing E_i as the corresponding fibre of some elliptic modular surface. Let then

$$X = B_1 \times \ldots \times B_n \times \mathbb{G}^\ell \times \mathbb{C}^k, \qquad U = \big(\mathbb{H} \times \mathbb{C}\big)^n \times \mathbb{C}^\ell \times \mathbb{C}^k.$$

We define "linear", "weakly special" and "special" subvarieties of U. We start by defining them in a product of elliptic modular surfaces.

Linear subvarieties of U_X for $X = B_1 \times \ldots \times B_n$

4.1. Definition. Let n be a non-negative integer. An *augmented partition* will mean a collection T of disjoint subsets $T_a, a = 1, \ldots, \#T$ of $\{1, \ldots, n\}$, each with a distinguished subset $T_a^{\mathrm{d}} \subset T_a$ (with $T_a^{\mathrm{d}} = T_a$ and $T_a^{\mathrm{d}} = \emptyset$ allowed). We set $T_a^{\mathrm{f}} = R_a - R_a^{\mathrm{d}}$, the complementary set. The *underlying set* of T we denote $\overline{T} = \cup_a T_a$.

For a subset $A \subset \{1, \ldots, n\}$ we let

$$U^A = \big(\mathbb{H} \times \mathbb{C}\big)^{\#A}$$

coordinatised by $\tau_j, z_j, j \in A$. We let

$$X^A = \prod_{j \in A} B_j$$

and we have a uniformisation

$$\pi_A : U^A \to X^A.$$

invariant under the corresponding product $\Gamma^A = \Pi_{j \in A} \Gamma_j^+$.

Let T be an augmented partition whose underlying set is A. For each partitand T_a of T let j_a^T be the smallest index in T_a. We let $\mathrm{SL}_2(\mathbb{R})^A$ be $\mathrm{SL}_2(\mathbb{R})^{\#A}$ whose elements are tuples indexed by A, and we let

$$\mathrm{SL}_2(\mathbb{R})^T \subset \mathrm{SL}_2(\mathbb{R})^A$$

be the set of tuples $g = (g_j) \in \mathrm{SL}_2(\mathbb{R})^A$ with the condition that $g_{j_a^T} = 1$ for each $a = 1, \dots \#T$. We now let

$$U^T \subset U^A \times \mathrm{SL}_2(\mathbb{R})^A$$

be the subset defined by the equations

$$\tau_j = g_j \tau_{j_a^T}$$

where $j \in T_a, a = 1, \dots, \#T$, and

$$z_j = 0$$

for all $j \in T_a^{\mathrm{f}}$, $a = 1, \dots, \#T$.

We view this as a family of subsets of U^A parameterised by points of $\mathrm{SL}_2(\mathbb{R})^A$, the fibre over $g \in \mathrm{SL}_2(\mathbb{R})$ being denoted

$$U^{T,g} \subset U^A.$$

We observe that $U^{T,g}$ is stable under the action of

$$G^{T,g} = \prod_a \{(g_j \alpha g_j^{-1})_{j \in T_a} : \alpha \in \mathrm{SL}_2(\mathbb{R})\}^+.$$

For now we make no rationality assumptions on g. But let us observe here that if $g \in \mathrm{GL}_2^+(\mathbb{Q})^A$ then $U^{T,g}$, and we set $X^{T,g} = \pi_A(U^{T,g})$, then the restriction $\pi^{T,g}$ of π_A to $U^{T,g}$ is invariant under

$$\Gamma^{T,g} = \prod_a \bigcap_{j \in T_a} g_j \Gamma_j g_j,$$

a product of congruence subgroups. It has a fundamental domain $F^{T,g}$ contained in finitely many translates under Γ^A of a fundamental domain for $\pi_A : U^A \to X^A$ under Γ^A.

4.2. Definition. Let R, S, T be augmented partitions. We write $R \prec T$ if the following conditions are satisfied:

1. Each partitand R_a of R is a union of partitands of T. We will write $b \prec a$ if $T_b \subset R_a$.
2. Each $R_a^{\mathrm{d}} \subset \bigcup_{b \prec a} T_b^{\mathrm{d}}$.

We write

$$(R, S) \prec T$$

if $R \prec T$, $S \prec T$ and $\overline{R} \cup \overline{S} = \overline{T}$.

Suppose R, S, T are augmented partitions with $(R, S) \prec T$. We write

$$\mathrm{SL}_2(\mathbb{R})^{(R,S),T} \subset \mathrm{SL}_2(\mathbb{R})^R \times \mathrm{SL}_2(\mathbb{R})^S \times \mathrm{SL}_2(\mathbb{R})^T$$

to denote the subset consisting of pairs (k, h, g) such that k, h are "consistent" with g, meaning that if $T_b, T_c \subset R_a$ and $j_a^R = j_b^T$ then, for each $j \in T_c$, we have

$$h_j = g_j h_c,$$

and for each $j \in T_b$ we have

$$h_j = g_j$$

and likewise for S. Now suppose as before that $A = \overline{T}$. Put $B = \overline{R}$. We will use variables σ_j, w_j for U^B to distinguish them from the corresponding variables in U^A. We let

$$M^S = \mathbb{C}^N, \quad N = \sum_a \#S_a^{\mathrm{d}}(\#S_a^{\mathrm{f}} + 2),$$

denote the space of coefficients $p = (p_{jk}, r_j, s_j)$ of a system of equations comprising (assuming some choice of $h \in \mathrm{SL}_2(\mathbb{R})^S$ has been made), for each $a = 1, \ldots, \#S$ and $j \in S_a^{\mathrm{d}}$, an equation

$$\ell(h_j, \tau_j) z_j = r_j \tau_{j_a^S} + s_j + \sum_{k \in S_a^{\mathrm{f}}} p_{jk} \ell(h_k, \tau_k) z_k.$$

We let

$$L^R = \mathbb{C}^N, \quad N = \sum_a \#R_a^{\mathrm{f}}(\#R_a^{\mathrm{f}} + 1),$$

denote the space of coefficients $q = (q_{jh})$ of a system of equations comprising (assuming some choice of $k \in \mathrm{SL}_2(\mathbb{R})^R$ and a choice of $(\sigma_j, w_j) \in U^B$ have been made), for each $a = 1, \ldots, \#R$ and $j \in R_a^{\mathrm{d}}$, an equation

$$\ell(k_j, \tau_j)(z_j - w_j) = \sum_{h \in R_a^{\mathrm{f}}} q_{jh} \ell(k_h, \tau_k) z_h.$$

4.3. Definition. With $(R, S) \prec T$ and further notation as above we define now the subset

$$W^{(R,S),T} \subset U^A \times U^B \times \mathrm{SL}_2(\mathbb{R})^{(R,S),T} \times L^R \times M^S$$

to be the tuples $(\tau, z, \sigma, w, k, h, g, q, p)$, satisfying:

1. $(\tau, z) \in U^{T,g}$;
2. $(\sigma, w) \in U_k^B$;
3. $\tau_i = \sigma_i$;
4. the equations corresponding to $q \in M^S$, given h;
5. the equations corresponding to $p \in L^R$, given k and w.

In the applications T and $g \in \mathrm{SL}_2(\mathbb{R})^T$ will be fixed, and we view $W^{(R,S),T}$ as a family of subsets

$$W^{(R,S),T}_{(\sigma,w,k,h,g,q,p)} \subset U^{T,g}$$

parameterised by the points of the projection

$$P^{(R,S),T}_g \subset U^B \times \mathrm{SL}_2(\mathbb{R})^{(R,S),T} \times L^R \times M^S$$

of its points with the given g, and we in turn view $P^{(R,S),T}_g$ as a family of copies $U^{R,k}$ fibred over the points with the given g and k of $\mathrm{SL}_2(\mathbb{R})^{(R,S),T} \times L^R \times M^S$.

4.4. Definition. A *linear subvariety* of $U^{T,g}$ is a subvariety of the form

$$W^{(R,S),T}_{(\sigma,w,k,h,g,q,p)}$$

for some $(\sigma, w, k, h, g, q, p) \in P^{(R,S),T}_g$. Abusing the notation, we refer to $W^{(R,S),T}_{(\sigma,w,k,h,g,q,p)}$ as the *translate* of $W^{(R,S),T}_{(k,h,g,q,p)}$ by $(\sigma, w) \in U^{R,k}$.

We may observe that $U^{T,g}$ is a linear subvariety of itself by taking $(R, S) \prec T$ with R empty and S to be the same partition as T but $S^{\mathrm{d}}_a = T^{\mathrm{f}}_a$, with equations $z_j = 0$ for $j \in S^{\mathrm{d}}_a$.

Weakly special and special subvarieties of U_X for $X = B_1 \times \ldots \times B_n$

4.5. Definition. A linear subvariety $W^{(R,S),T}_{(\sigma,w,k,h,g,q,p)}$ is called *weakly special* if

1. The components of k, h, g all belong to the image of $\mathrm{GL}^+_2(\mathbb{Q})$ in $\mathrm{SL}_2(\mathbb{R})$;
2. The components of q all belong to $\mathbb{Q}$;
3. For each partitand R_a of R, **either** the corresponding coordinates of p belong to $\mathbb{Q}$ **or** they all belong to some imaginary quadratic field **and** the corresponding $\sigma_j, j \in R_a$ all belong to this same field.

Since the σ_j corresponding to $j \in R_a$ are (for a weakly special subvariety) related by elements of $\mathrm{GL}^+_2(\mathbb{Q})$, the last condition is equivalent to one of them being in the appropriate quadratic field.

We will refer to an element $g \in \mathrm{SL}_2(\mathbb{R})$ as belonging to $\mathrm{GL}^+_2(\mathbb{Q})$ if it belongs to the image of the latter in the former. One may observe now that $U^{T,g}$ is weakly special just if g consists of matrices from $\mathrm{GL}^+_2(\mathbb{Q})$.

4.6. Definition. Let $\Sigma \subset \mathbb{H}$. A weakly special subvariety $W^{(R,S),T}_{(\sigma,w,k,h,g,q,p)}$ is called Σ-*special* if (σ, w) is a Σ-special point of U^B.

It is easily seen that these subgroup schemes over special subvarieties in $\mathbb{H}^n$ are indeed special subvarieties as defined in [40, 41].

Linear, weakly special, and special subvarieties of U_X for $X = \mathbb{G}^\ell$

Now we have to define analogous notions for $\mathbb{G}^\ell$, where the combinatorial baggage is much lighter. Let ℓ be a non-negative integer. Let $B \subset A \subset \{1, \ldots, \ell\}$. We write

$$\mathbb{C}^A = \mathbb{C}^{\#A}$$

coordinatised by $\zeta_j, j \in A$, and for $\mathbb{C}^B$ we will use $\eta_j, j \in B$ to distinguish the variables from the two spaces. We also write $\mathbb{G}^A$ for the corresponding factors in $\mathbb{G}^\ell$, and we have

$$\exp_A : \mathbb{C}^A \to \mathbb{G}^A.$$

We let

$$N^{B,A} = \mathbb{C}^{B \times (A-B)}$$

denote the space of coefficients $r = (r_{jm})$ of a system of equations comprising, for each $j \in B$, an equation

$$\zeta_j - \eta_j = \sum_{m \in A-B} r_{jm} z_m.$$

4.7. Definition. With $B \subset A \subset \{1, \ldots, \ell\}$ and further notation as above we define the subset

$$W^{B,A} \subset \mathbb{C}^A \times \mathbb{C}^B \times N^{B,A}$$

to be the set of tuples (ζ, η, r) satisfying the above equations.

We view $W^{B,A}$ as a family of subsets $W^{B,A}_{(\eta,r)} \subset \mathbb{C}^A$ parameterised by points $(\eta, r) \in \mathbb{C}^B \times N^{B,A}$.

4.8. Definition. An exp-*linear subvariety* of $\mathbb{C}^A$ is a fibre of $W^{B,A}$ for some $B \subset A$. A linear subvariety $W^{B,A}_{(\eta,r)}$ is called exp-*weakly special* if the coordinates of r are all rational. An exp-weakly special subvariety $W^{B,A}_{(\eta,r)}$ is called exp-*special* if $\eta \in \mathbb{C}^B$ is a special point.

Linear, weakly special, and special subvarieties of U_X for $X = \mathbb{C}^k$

Finally we need the analogous notions for $\mathbb{C}^k$ as uniformisation of itself by the identity map.

4.9. Definition. Let $d \in \mathbb{N}^+$. An id-*linear* subvariety of $\mathbb{C}^k$ is a Zariski closed (irreducible) subvariety of $\mathbb{C}^k$. An id-*weakly special* subvariety of $\mathbb{C}^k$ is the same thing, and a *(d-id)-special* subvariety of $\mathbb{C}^k$ is a Zariski closed (irreducible) subvariety with a Zariski-dense set of d-special points.

Linear, weakly special, and special subvarieties of U

Let R be an augmented partition, $A \subset \{1, \ldots, \ell\}$, k a non-negative integer. Let

$$U = \big(\mathbb{H} \times \mathbb{C}\big)^R \times \mathbb{C}^A \times \mathbb{C}^k.$$

4.10. Definition. A linear subvariety of U is a cartesian product of linear subvarieties in $\big(\mathbb{H} \times \mathbb{C}\big)^R$, $\mathbb{C}^A$, and $\mathbb{C}^k$. Likewise for *weakly special* and *special* subvarieties.

4.11. Definition. A *weakly special subvariety* $T \subset X$ is the image $\pi(W)$ where W is a weakly special subvariety of U. Likewise for *special subvarieties*.

A weakly special $T \subset X$ is a subvariety (Zariski closed and irreducible). To see this, note we have observed that T is the image of W over a finite number of fundamental domains, hence its algebraicity may be seen for example by results of Peterzil-Starchenko [32, Theorem 5.3]. We observe a further fact in this direction below. In particular, the image

$$X^{T,g,A} = \pi(U^{T,g} \times \mathbb{C}^A) \subset X^{\overline{T}} \times \mathbb{G}^A$$

is a special subvariety.

We now assume that there are no $\mathbb{C}^k$ factors:

$$X = B_1 \times \ldots \times B_n \times \mathbb{G}^\ell$$

Then the linear subvarieties of U come in finitely many semialgebraic families

$$W^{(R,S),T,(B,A)}$$

indexed by the combinatorial data: $(R,S) \prec T$, $B \subset A \subset \{1,\ldots,\ell\}$. In particular, the linear subvarieties form a definable (even semialgebraic) family. A countable set of parameters (k,h,g,q,p,r) give rise to weakly special subvarieties. For a given choice of these we may take

$$D = ((R,S),T,k,h,g,q,p,A,B,r)$$

and view the set $W^{(R,S),T,(B,A)}$ with those parameters fixed as a set

$$W^D \subset U^{T,g} \times \mathbb{C}^A \times U^{R,k} \times \mathbb{C}^B$$

which we view as a family of weakly special subvarieties

$$W^D_{((\sigma,w),\eta)} \subset U^{T,g} \times \mathbb{C}^A$$

parameterised by points

$$((\sigma,w),\eta) \in U^D = U^{R,k} \times \mathbb{C}^B.$$

The special subvarieties correspond to the parameters being special points.

4.12. Definition. A set D as above we call a *weakly special format.*

4.13. Proposition. *With D a weakly special format as above, the set*

$$W^D \subset U^{T,g} \times \mathbb{C}^A \times U^R_k \times \mathbb{C}^B$$

is a special subvariety.

Proof. Immediate from the definitions. □

Therefore, with $X^D = \pi_D(U^D)$, we have that $\pi(W^D)$ is a special subvariety

$$T^D \subset X \times X^D,$$

and corresponds to a family of weakly special subvarieties of X parameterised by the points of X^D. The fibre $T^D_x \subset X$ is a special subvariety precisely if $x \in X^D$ is a special point.

Recalling that $U^D = U^{R,k}$ is a certain subvariety of $U^{\overline{R}}$, the uniformisation

$$U^D \to X^D$$

is invariant under a group Γ^D which is the cartesian product of $(\Gamma_i^*)^+$ for suitable congruence subgroups Γ_i^* of Γ_i, with fundamental domain F_D.

4.14. Proposition. *The uniformisation*

$$\pi : U \times U^D \to X \times X^D$$

has a fundamental domain consisting of (the intersection of $U \times U^D$ with) finitely many fundamental domains for the action of $\Gamma \times \Gamma^A$ on $U \times U^A$.

Proof. Immediate by previous observations. □

5. Ax-Lindemann-Weierstrass

In this section we continue to take

$$X = B_1 \times \ldots \times B_n \times \mathbb{G}_{\mathrm{m}}^\ell \times \mathbb{C}^k, \qquad U = \big(\mathbb{H} \times \mathbb{C}\big)^n \times \mathbb{C}^\ell \times \mathbb{C}^k,$$

and a Zariski closed algebraic subset $V \subset X$. We set

$$\mathcal{Z} = \pi^{-1}(V), \qquad Z = \pi^{-1} \cap F$$

the latter being a definable set (the former generally not).

By a *maximal algebraic subvariety* of $\mathcal{Z}$ we mean an algebraic subvariety W of U in the sense of 2.4, with $W \subset \pi^{-1}(V)$, and maximal among such objects.

5.1. Theorem. *A maximal algebraic subvariety $W \subset \mathcal{Z}$ is weakly special.*

Proof. The proof closely follows the scheme of proof of [34, 6.8], with which the reader is assumed to be familiar, with modifications for the interaction between the $\mathbb{H}$ and $\mathbb{C}$ factors parameterising elliptic modular surfaces. The subvariety W is parameterised by algebraic functions on some choice of variables corresponding to the factors of U. The variables for the $\mathbb{H}$ factors will be called $\mathbb{H}$-variables. The variables for the $\mathbb{C}$ factors will be called $\wp$-variables (respectively exp-variables, respectively id-variables) according as they correspond to elliptic modular factors (respectively $\mathbb{G}$ factors, respectively $\mathbb{C}$ factors) of X.

Choice of parameterising variables

We choose a set of parameterising variables as follows. First we take a maximal set of algebraically independent $\mathbb{H}$-variables τ_i (so all other $\mathbb{H}$-variables are algebraically dependent on W on these). Next we choose a maximally independent (over the τ_i) subset of the $\wp$-variables among which we denote by z_j the ones whose corresponding $\mathbb{H}$-variable is among the τ_i, the others w_a. Next we choose a maximal independent (over the τ_i, z_j, w_a) of the exp-variables, calling these ζ_b. Finally we choose a maximal set of independent id-variables, t_c. The various sets of variables we will also regard as tuples denoted τ, z, w, ζ, t.

The other variables are "dependent", and parameterised by algebraic functions. The "dependent" $\mathbb{H}$-variables are parameterised by algebraic functions $\sigma_i(\tau)$. Among the dependent $\wp$-variables we distinguish those that have a corresponding $\mathbb{H}$-variable among the τ_i, parameterising these by $\phi_i(\tau, z, w)$, and those parameterising these by $\psi_i(\tau, z, w)$. The dependent exp-variables are parameterised by $\theta_i(\tau, z, w, \zeta)$, and the dependent id-variables by $\kappa(\tau, z, w, \zeta, t)$. The tuples we denote $\sigma, \phi, \psi, \theta, \kappa$. For reasons of brevity it is sometimes convenient to concatenate tuples into a single tuple and write e.g. $\phi\psi$. The dependencies are

$$\sigma = \sigma(\tau), \quad \phi\psi = \phi\psi(\tau,\ z,\ w), \quad \theta = \theta(\tau,\ z,\ w,\ \zeta) \quad \kappa = \kappa(\tau,\ z,\ w,\ \zeta,\ t).$$

Then W may be parameterised locally as

$$\Big(\tau,\ z,\ w,\ \zeta,\ t;\ \sigma,\ \phi,\ \psi,\ \theta,\ \kappa\Big)$$

where the semi-colon separates the free and dependent variables.

The τ-dependencies

Exchanging variables if need be, we are able (as is [34]) to take some "free" $\mathbb{H}$-variable, say τ_1, to its boundary. We distinguish cases according to whether the corresponding $\wp$-variable is among the free variables, or the dependent ones, taking the former case that it is z_1 first. We write $\hat{\tau}$ for the tuple of free $\mathbb{H}$-variables excluding τ_1, and $\hat{z}$ for the free $\wp$-variables with free corresponding $\wp$-variables excluding z_1. So we have

$$\Big(\tau_1,\ \hat{\tau},\ z_1,\ \hat{z},\ w,\ \zeta,\ t;\ \sigma,\ \phi,\ \psi,\ \theta,\ \kappa\Big) \subset \mathcal{Z}$$

locally on some product of open disks and an "upper-half disk" U_1 for τ_1 on its boundary, and by analytic continuation everywhere, where now the dependencies are

$$\sigma = \sigma(\tau_1, \hat{\tau}), \quad \phi\psi = \phi\psi(\tau_1, \hat{\tau}, z,\ w), \quad \theta = \theta(\tau_1, \hat{\tau},\ z,\ w, \zeta), \quad \kappa = \kappa(\tau_1, \hat{\tau}, z, w, \zeta, t).$$

We take $g_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ with $a/c \in U_1$. Then we take $g \in \mathrm{SL}_2(\mathbb{Z})$ of the form

$$g = g_s = \begin{pmatrix} a & b+sa \\ c & d+sc \end{pmatrix}, \quad s \in \mathbb{R}.$$

For sufficiently large s and $\tau \in U_1'$, $g\tau_1 \in U_1'$ and all the parameterising functions are well-defined and non-singular. Therefore we have

$$\Big(g\tau_1,\ \hat\tau,\ z_1,\ \hat z,\ w,\ \zeta,\ t;\ \sigma(g\tau_1,\hat\tau),\ \phi\psi\theta\kappa(g\tau_1,\hat\tau,\ldots)\Big) \subset \mathcal{Z}$$

where the variables not indicated remain as previously. Then the Γ-transforms of this locus are also contained in $\mathcal{Z}$, in particular the g^{-1}-image

$$\Big(\tau_1,\ \hat\tau,\ \ell_g(\tau_1)z_1,\ \hat z,\ w,\ \zeta,\ t;\ \sigma(g\tau_1,\hat\tau),\ \phi\psi\theta\kappa(g\tau_1,\hat\tau,z_1,\hat z,\ldots)\Big) \subset \mathcal{Z}$$

for the same domains of the variables. For fixed $\tau_1, \hat\tau, w, \zeta, t$, the z_1 dependence may be extended to the whole z_1-plane less finitely many points. Then we may change variables calling $\ell_g(\tau_1)z_1$ again z_1 to find

$$\Big(\tau_1,\ \hat\tau,\ z_1,\ \hat z,\ w,\ \zeta,\ t;\ \sigma(g\tau_1,\hat\tau),\ \phi\psi\theta\kappa(g\tau_1,\hat\tau,z_1/\ell_{g^{-1}}(\tau_1),\hat z,\ldots)\Big) \subset \mathcal{Z}.$$

Now we act by further elements of Γ to bring the locus back into our fixed fundamental domain, where it will intersect Z in a set of the full dimension of W.

We choose elements h_i to bring the dependent $\mathbb{H}$-variables back to their fundamental domain. The action by h_i affects the corresponding w_i and ψ_i. If we set

$$h\sigma = (.., h_i\sigma_i, ..), \quad w^* = (.., \frac{w_i}{\ell_{h_i}(\sigma_i)}, ..), \quad \psi^* = (.., \frac{\psi_i}{\ell_{h_i}(\sigma_i)}, ..)$$

then we have

$$\Big(\tau_1,\ \hat\tau,\ z_1,\ \hat z,\ w^*,\ \zeta,\ t;\ h\sigma(g\tau_1,\hat\tau),\ \phi\psi^*\theta\kappa(g\tau_1,\hat\tau,z_1/\ell_{g^{-1}}(\tau_1),\hat z,w^*,\ldots)\Big) \subset \mathcal{Z}.$$

Now we may rename variables to replace w^* by w and we find

$$\Big(\tau_1,\ \hat\tau,\ z_1,\ \hat z,\ w,\ \zeta,\ t;\ h\sigma(g\tau_1,\hat\tau),\ \phi\psi^*\theta\kappa(g\tau_1,\hat\tau,z_1/\ell_{g^{-1}}(\tau_1),\hat z,..,w_i\ell_{h_i}(\sigma_i),..)\Big) \subset \mathcal{Z}.$$

Finally, we choose translations λ_i on the variables parameterised by the coordinates of $\phi\psi^*$, and μ_i translations of the coordinates of θ such that, writing λ, μ for the tuples and

$$W_{g_s,h,\lambda,\mu}$$

for the locus

$$\Big(\tau_1,\ \hat\tau,\ z_1,\ \hat z,\ w,\ \zeta,\ t;\ h\sigma(g\tau_1,..),\ \phi\psi^*\big(g\tau_1,..,z_1/\ell_{g^{-1}}(\tau_1),..,w_i\ell_{h_i}(\sigma_i),..\big)-\lambda,$$

$$\theta\big(g\tau_1,..,z_1/\ell_{g^{-1}}(\tau_1),..,w_i\ell_{h_i}(\sigma_i),..,\zeta\big)-\mu, \kappa\big(g\tau_1,..,z_1/\ell_{g^{-1}}(\tau_1),..,w_i\ell_{h_i}(\sigma_i),..,\zeta,t\big)\Big),$$

we have

$$\dim_{\mathbb{R}} W_{g_s,h,\lambda,\mu} \cap Z = \dim_{\mathbb{R}} W_{g_s,h,\lambda,\mu}.$$

Now since all the functions here are algebraic, it is straightforward to see (as established in [34, 5.3, 5.4, 5.5]) that, for a large integer s, the height of all the $h_i, \ell_{h_i}, \lambda_i, \mu_i$ are bounded polynomially in s.

We may take an element of Γ corresponding to the data g_0, s, h, λ, μ by taking identity elements for the remaining group variables. Considering g_0 to be fixed, the corresponding element will be denoted

$$(g_s, h, \lambda, \mu) \in \Gamma.$$

For any $g_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with a/c as above, sufficiently large real s, and any h, λ, μ in the respective real groups we have an algebraic locus

$$W_{(g_s,h,\lambda,\mu)}$$

given by

$$\Big(\tau_1,\ \hat{\tau},\ z_1,\ \hat{z},\ w,\ \zeta,\ t;\ h\sigma(g\tau_1,..),\ \phi\psi^*\big(g\tau_1,..,z_1/\ell_{g^{-1}}(\tau_1),..,w_i\ell_{h_i}(\sigma_i),..\big)-\lambda,$$

$$\theta\big(g\tau_1,..,z_1/\ell_{g^{-1}}(\tau_1),..,w_i\ell_{h_i}(\sigma_i),..,\theta\big)-\mu, \kappa\big(g\tau_1,..,z_1/\ell_{g^{-1}}(\tau_1),..,w_i\ell_{h_i}(\sigma_i),..,\zeta,t\big).$$

This is a definable family of open subsets of complex algebraic varieties. Then the set

$$R = R_{g_0} = \{(g_s, h, \lambda, \mu) \in G : \dim_{\mathbb{R}} \big(W_{(g_s,h,\lambda,\mu)} \cap Z\big) = \dim_{\mathbb{R}} W\}$$

(with certain coordinates of (g_s, h, λ, μ) fixed as described above) is a definable set with "many" rational (indeed integer) points. Here "many" means that, for some positive c, δ, we have $N(R,T) \geq cT^\delta$ for (arbitrarily) large T, where $N(R,T)$ counts the rational points of R up to height T. And for $(g_s, h, \lambda, \mu) \in R$ we have $W_{(g_s,h,\lambda,\mu)} \subset \pi^{-1}(V)$ by analytic continuation.

Then R contains some semi-algebraic "blocks" (see [34, 3.4]) B that (as T increases) contain arbitrarily many integer points. Thus we can choose (g_s, h, λ, μ) depending semialgebraically on some real parameter x such that the family

$$W(x) = W_{(g_s,h,\lambda,\mu)(x)}$$

is contained in $\mathcal{Z}$, and contains some $W_{(g_s,h,\lambda,\mu)}$ corresponding to an integer point

$$(g_s, h, \lambda, \mu)(x_0) \in \Gamma$$

of R at a smooth point s_0 (if all the integer points in B are in its singular set, then we consider the singular set, which has some bounded degree in terms of the degree of the blocks. Since we have "many" integer points, we eventually find a smooth one).

First we may observe that, near the smooth point $(g_s, h, \lambda, \mu)(x_0)$, we have

$$W(x) = W_{(g_s,h,\lambda,\mu)(x)} \subset \pi^{-1}(V)$$

also for complex values of the parameter x. This is because for each fixed choice of values for the "free" variables, the functions that define $\pi^{-1}(V)$ are complex analytic functions vanishing for real x in a neighbourhood of x_0, which therefore vanish identically.

Now suppose that one of the functions

$$\tau^* = h_i(x)\sigma_i\big(g_s(x)\tau_1, \hat{\tau}\big) \in \overline{\mathbb{C}(\tau_1, \hat{\tau}, x)}$$

is nonconstant. Then x is algebraic over

$$\mathbb{C}(\tau_1, \hat{\tau}, \tau^*)$$

and we have an algebraic subvariety $W' \cap \pi^{-1}(V)$ of dimension $\dim W + 1$ parameterised by

$$\Big(\tau_1, \hat{\tau}, \tau^*, z_1, \hat{z}, w, \zeta, t; \ldots\Big).$$

But since W was assumed to be maximal, its Γ translate $W_{(g_s,h,\lambda,\mu)(x_0)}$ is also maximal. So such a W' contradicts our hypothesis on W. Thus the function

$$h_i(x)\sigma_i\big(g_s(x)\tau_1, \hat{\tau}\big)$$

must be constant.

Now suppose that σ_i does not have its real locus coincident with that of τ_1. Then by a suitable choice of fundamental domain for the corresponding variable, and small enough domain for τ_1, we can take $h_i = 1$. However, $g_s(x)$ is certainly non-constant, and we conclude that σ_i does not depend on τ_1. The same argument shows that none of the functions θ_i, κ_j depend on τ_1.

Suppose then that σ_i does have its real axis coincident with τ_1. Considering two Γ-points on the x-curve we find, as in [34, p1817], that σ_i satisfies an identity, namely

$$\sigma(g\tau) = h\sigma(\tau), \quad g = g_{s_1}g_{s_2}^{-1} = \begin{pmatrix} 1 - ac(s_2 - s_1) & a^2(s_2 - s_1) \\ -c^2(s_2 - s_1) & 1 + ac(s_2 - s_1) \end{pmatrix}, h \in \mathrm{SL}_2(\mathbb{Z}).$$

We may choose families g_t for any a/c in the real boundary of τ_1, and it follows as in [34, p1817-1818] (or see [35]) that σ_i is itself an $\mathrm{SL}_2(\mathbb{R})$ transformation, and indeed is given by an element of $\mathrm{GL}_2^+(\mathbb{Q})$. Then σ_i depends only on τ_1, as an element of $\mathrm{SL}_2(\mathbb{R})$ cannot depend complex algebraically on another variable.

This takes care of the dependencies of the σ_i on τ_1 in this case (that the $\wp$-variable associated to τ_1 was among the free variables). The other case however may be argued with only a slight variation. We then have $W \subset \mathcal{Z}$ parameterised by

$$\Big(\tau_1,\ \hat{\tau},\ z,\ w,\ \zeta,\ t;\ \sigma,\ \phi_1,\ \hat{\phi},\ \psi,\ \theta,\ \kappa\Big)$$

on some suitable product of disks and an "upper-half disk" for τ_1. Here ϕ_1 parameterises the $\wp$-variable z_1 associated to τ_1. Now for families g_s as above an sufficiently large s we have

$$\Big(g\tau_1,\ \hat{\tau},\ z,\ w,\ \zeta,\ t;\ \sigma(g\tau_1, ..),\ \phi_1(g\tau_1, ..),\ \hat{\phi}\psi\theta\kappa(g\tau_1, ..)\Big) \subset \mathcal{Z}$$

whence

$$\Big(\tau_1,\ \hat\tau,\ z,\ w,\ \zeta,\ t;\ \sigma(g\tau_1,..),\ \ell_g(\tau_1)\ \phi_1(g\tau_1,..),\ \hat\phi\psi\theta\kappa(g\tau_1,..)\Big) \subset \mathcal{Z}.$$

Then as before

$$\Big(\tau_1,\ \hat\tau,\ z,\ w^*,\ \zeta,\ t;\ h\sigma(g\tau_1,..),\ \ell_g(\tau_1)\ \phi_1(g\tau_1,..),\ \hat\phi\psi^*\theta\kappa(g\tau_1,..)\Big) \subset \mathcal{Z}$$

from which, after renaming variables, the locus

$$\Big(\tau_1, \hat\tau, z,\ w, \zeta, t;\ h\sigma(g\tau_1,..),\ \ell_g(\tau_1)\ \phi_1(g\tau_1,.., w_i\ell_{h_i}(\sigma_i),..),\ \hat\phi\psi^*\theta\kappa(g\tau_1,..w_i\ell_{h_i}(\sigma_i),..)\Big)$$

is contained in $\mathcal{Z}$ and the argument proceeds in the same way to show that σ_i is either independent of τ_1 or depends only on τ_1 through an element of $\mathrm{GL}_2^+(\mathbb{Q})$.

Thus, we see that the dependencies among the non-constant $\mathbb{H}$ variables are given pairwise by elements of $\mathrm{GL}_2^+(\mathbb{Q})$. Also we have seen that the θ_i, κ_j do not depend on the τ_a. Similarly, a dependent $\wp$-variable cannot depend on any $\mathbb{H}$-variable other than the one it is associated to, because we can carry out the argument to vary W without having to "move" this variable.

The z and w dependencies

Now we consider the dependencies among $\wp$-variables. Let us consider some ϕ_i. Among the free $\wp$-variables we now denote by z_j those whose associated $\mathbb{H}$-variable is free or independent of τ_i, and by w_k those whose associated $\mathbb{H}$-variable is dependent on τ_i or is τ_i itself. We have

$$W : \Big(\ldots, \tau_i, \ldots, z_j, \ldots, w_a, \ldots, \zeta_b, \ldots, t_c, \ldots; \ldots, \phi_i(..\tau_i, .., z_j, .., w_a, ..), \ldots\Big) \subset \mathcal{Z}.$$

We find some region where ϕ_i and all the other algebraic functions remain defined for $z_j + s\lambda$, where $\lambda \in \Lambda_j$ the lattice in the z_j variable, for all sufficiently large real positive s. Then the maximality of W leads to identities (as in [34, p1819])

$$\phi_i(\ldots, z_j + s_2\lambda, \ldots) = \phi_i(\ldots, z_j + s_1\lambda, \ldots) - \alpha\tau_i - \beta.$$

Here s_1, s_2 are large positive integers $s_1 \neq s_2$, $\alpha, \beta \in \mathbb{Z}$, and the identity holds for all z_j and all other variables. Differentiating with respect to z_j, the algebraic function with a period is constant, and we see that ϕ_i depends linearly on z_j, say

$$\phi_j = qz_j + b$$

where q, b may of course depend on the other variables. However, since $s_1, s_2 \in \mathbb{Z}$ we see that

$$Nq\lambda$$

for some $0 \neq N \in \mathbb{Z}$, and since we may take any $\lambda \in \Lambda_j$ we in fact have

$$Nq\Lambda_j \subset \Lambda_i.$$

This restricts q to a countable set (so it cannot depend on the other variables), moreover as the $\mathbb{H}$-variable associated to z_j is independent of τ_i, we must have $q = 0$.

If we repeat the same argument with the w_k, we also find linear dependence in the above form. Then q is again independent of all other variables, and we find that

$$\phi_i = \sum_k q_{ik} w_k + b(\tau_i)$$

where $N_{ik} q_{ik} \Lambda_k \subset \Lambda_i$. Now the lattices are in the same Hecke orbit, but will not have CM for general τ_i, so we have $q_k \in \mathbb{Q}$. Now we consider the dependence on τ_i. We take a positive integer p such that

$$g = \begin{pmatrix} 1 & ps \\ 0 & 1 \end{pmatrix} \in \Gamma_i, \quad s \in \mathbb{Z}.$$

We may assume τ_i in a region where $b(g\tau_i)$ is defined for all sufficiently large real s. We have

$$\Big(..., g\tau_i, ..., z_j, ..., w_a, ..., \zeta_b, ..., t_c, ...; \sigma(.., g\tau_i, ..), \ldots, \phi_i(.., g\tau_i, .., w_a, ..), \ldots\Big) \subset \mathcal{Z}$$

and we take the g^{-1}-image to get

$$\Big(..., \tau_i, ..., z_j, ..., w_a, ..., \zeta_b, ..., t_c, ...; \sigma(.., g\tau_i, ..), \ldots, \ell_g(\tau_i)\phi_i(.., g\tau_i, .., w_a, ..), \ldots\Big) \subset \mathcal{Z}.$$

We transform σ back to our fixed fundamental domain to see that the locus

$$\Big(.., \tau_i, .., z_j, .., \frac{w_a}{\ell_{h_k}(\sigma_k)}, .., \zeta_b, ...t_c, ...; h\sigma(.., g\tau_i, ..), ..., \ell_g(\tau_i)\phi_i(.., g\tau_i, .., w_a, ..), ...\Big) \subset \mathcal{Z}$$

and rename variables

$$\Big(.., \tau_i, ..z_j, .., w_a, .., \zeta_b, .., t_c, ..; h\sigma(.., g\tau_i, ..), ..., \ell_g(\tau_i)\phi_i(.., g\tau_i, .., \ell_{h_k}(\sigma_k)w_k, ..), ...\Big) \subset \mathcal{Z}.$$

Then ϕ_i (and the other $\wp$-variables) can be brought back to a fixed fundamental region by a suitable (respective) lattice element. This leads to an identity

$$\phi_i(.., \tau_i + ps, .., \ell_{h_k}(\sigma_k)w_k, ..) = \phi_i(.., \tau_i, .., w_k, ..) - \alpha\tau_i - \beta.$$

We may consider this identity in particular with all $w_k = 0$. This gives

$$b(\tau_i + ps) = b(\tau_i) - \alpha\tau_i - \beta$$

for suitable $\alpha, \beta \in \mathbb{Z}$. Differentiating twice, the algebraic function with a period is constant and we see that

$$b(\tau_i) = q\tau_i^2 + r\tau_i + s$$

where moreover $q, r \in \mathbb{Q}$. Now we consider transforming τ_i by a general family of g as before. This leads to

$$\ell_g(\tau_i)\Big(\sum_k q_k \ell_{h_k}(\sigma_k g\tau_i)w_k + b(g\tau_i)\Big) = \sum_k q_k w_k + b(\tau_i) - \alpha\tau_i - \beta.$$

Considering all $w_k = 0$ shows that $q = 0$ and $r, s \in \mathbb{Q}$, i.e. that

$$\phi_i = \sum_k q_{ik} w_k + r\tau_i + s, \quad q_{ik}, r, s \in \mathbb{Q}$$

where w_k are the free $\wp$-variables whose associated $\mathbb{H}$-variable is dependent on τ_i (possibly τ_i itself).

Now we consider the $\wp$-dependencies of ψ_i. Here there are two cases. In the first the associated $\mathbb{H}$-variable σ_i depends on some free τ_j. We can exchange σ_i and τ_j, and argue as above. This leads to the same form as above

$$\psi_i = \sum_k q_k w_k + r\sigma_i + s, \quad q_k, r, s \in \mathbb{Q}$$

where w_k are the $\wp$-variables whose associated $\mathbb{H}$-variable is dependent on τ_j (possibly τ_i itself). In the second case the associated $\mathbb{H}$-variables is constant. Now the same analysis finds

$$\psi_i = \sum_k q_{ik} w_k + b_i$$

over w_k whose associated $\mathbb{H}$-variables are constant with q_k such that $Nq_k\Lambda_k \subset \Lambda_i$ for suitable integer N (some fixed σ_i may have CM, so it is possible that the q_k belong to the associated field).

The ζ dependencies

We consider now the dependence of the θ_i, which we have already seen do not depend on the τ_j. We denote all the free $\wp$-variables by z_j. Proceeding with a similar analysis changing z_j to $z_j + s\lambda, \lambda \in \Lambda_j$ we find that

$$\theta_i = qz_j + b$$

where $q\Lambda_j \subset 2\pi i\mathbb{Z}$. This however forces $q = 0$. Thus θ_i does not depend on any of the free $\wp$-variables. By similar arguments the dependence of the θ_i on the ζ_j must be linear of the form

$$\theta_i = \sum q_{i\ell}\zeta_\ell + b_i, \quad q_{i\ell} \in \mathbb{Q}, \quad b_i \in \mathbb{C}.$$

Finally, the id-variables cannot depend on any of the variables except the t-variables. This completes the proof. □

6. Proof of Theorem 1.1

In this section we will prove Theorem 1.1, but we start with a version omitting the E_i-factors and the $\mathbb{C}^k$ factors. Let

$$X = B_1 \times \ldots \times B_n \times \mathbb{G}^\ell.$$

6.1. Theorem. *Let $V \subset X \times \mathbb{C}^k$ be a Zariski closed algebraic subset, let $\Sigma \subset \mathbb{H}$ be a finite set, and d a positive integer. Then there is a finite set $\mathcal{D} = \mathcal{D}(V)$ of weakly special formats and a positive integer $\Delta = \Delta(V, \Sigma, d)$ with the following property.*

Let $y \in \mathbb{C}^k$ be a d-special point and $V_y \subset X$ the corresponding fibre of V. If $T \subset V_y$ is a maximal (Σ, d)-special subvariety then there exists $D \in \mathcal{D}$ and $u \in U^D$ a (Σ, d)-special point with $\Delta(u) \le \Delta$ such that

$$T = \pi\big(W_u^D\big).$$

Proof. Replacing V by the Zariski closure of its Σ-special points, we may assume that V is defined over some finite algebraic extension of a finitely generated extension of $\mathbb{Q}$. Viewing V as a definable family of fibres $V_y \subset X$, the set of D such that some translate $W_u^D \subset V_y$ and is maximal among such translates is a definable set, but countable by Ax-Lindemann-Weierstrass. Therefore this set is finite, and we denote it $\mathcal{D}$.

Now let $h \in \{0, \ldots, \dim X\}$ and suppose it is established that there is a Δ_h such that, for $y \in \mathbb{C}^k$ a d-special point, any maximal special $W \subset V_y$ of dimension $\dim W \ge h$ is of the form $W = W_u^D$ where $u \in U^D$ with $\Delta(u) \le \Delta_h$ (and note that we know this for $h = \dim X$), then we establish the same assertion for $h - 1$.

Let then $\mathcal{D}_{h-1} \subset \mathcal{D}$ be the subset of elements D whose translates W_u^D have dimension $h-1$, and let $y \in \mathbb{C}^k$ be a d-special point. Let $V_y^D \subset X_y^D$ be the subvariety of points $\pi_D(u) \in X^D$ for which $W_u^D \subset V_y$ (Zariski closed subvariety by 4.13). Write $Z_y^D = \pi_D^{-1}(V_y^D) \cap F_D$ and suppose $u \in Z_y^D$ a Σ-special point such that $W_u^D \subset V_y$ but is not contained in any special subvariety $W_{u'}^{D'} \subset V_y$ of larger dimension. The degree of the field $K_{y,h}$ of definition of V_y and all its special subvarieties of dimension $\ge h$ over K is bounded depending only on V, Σ, d, and so u has, for suitable positive c, δ, at least

$$c\Delta(u)^\delta$$

conjugates u^* over this field for which $W_{u^*}^D$ is likewise not contained in any special subvariety of larger dimension. Each such point gives rise to an Σ-special point $\sigma^* \in Z_y^D$. Now apply the Counting Theorem to the family V as in [19]; the coordinates τ of the σ^* that are Hecke equivalent to $\sigma \in \Sigma$ may not be algebraic, but they are the images of rational points in $\mathrm{GL}_2^+(\mathbb{R})$ under the map $g \mapsto g\sigma$, and the Counting Theorem is applied to a definable subset Y in a suitable product of $\mathbb{H}$ and $\mathrm{GL}_2^+(\mathbb{R})$, as in [19, Proof of Theorem 3]. The height estimate in the $\mathrm{GL}_2^+(\mathbb{R})$ factors is provided by Lemma 3.6, and one finds that the Σ-special points give rise to points in Y which are rational in the $\mathrm{GL}_2^+(\mathbb{R})$ coordinates, quadratic in the $\mathbb{H}$ coordinates and of height at most

$$C\Delta(u)^K$$

for suitable constants C, K. The points are thus contained in $c\Delta(u)^\epsilon$ blocks with $\epsilon = \delta/2$ say and these blocks are projected back to $\mathbb{H}^n$ to obtain $c'\Delta(u)^\epsilon$ there. If $\Delta(u)$ is sufficiently large compared to $\Delta_h, C, K, c, \delta$ this means that Z_y contains a semialgebraic variety of larger dimension than W_u^D, and by [36, Lemma 4.1] there is a complex algebraic subvariety of $\pi^{-1}(V)$ containing it, and by Theorem 5.1 a weakly special subvariety of larger dimension containing at least one (in fact many) of these points, which must then be special. This contradicts the fact the $W_{u^*}^D$ are not contained in any larger special subvariety, and implies that $\Delta(u) \leq \Delta_{h-1}$ for some suitable constant $\Delta_{h-1}(V)$.

Repeating this argument leads to the conclusion for $h = 0$, which proves the theorem with $\Delta = \max(\Delta_{\dim X}, \ldots, \Delta_0)$. □

Now let

$$X = B_1 \times \ldots \times B_n \times \mathbb{G}^\ell \times \mathbb{C}^k.$$

6.2. Theorem. *Let $V \subset X$ be a Zariski closed algebraic subset, $\Sigma \subset \mathbb{H}$ a finite set, and d a positive integer. Then V contains only finitely many maximal (Σ, d)-special subvarieties.*

Proof. Viewing V as a family of subsets of $B_1 \times \ldots \times B_n \times \mathbb{G}^\ell$ and applying Theorem 6.1, we see that there are only finitely many possibilities for (D, u) for a maximal special subvariety $W_u^D \subset V_y$ for any d-special $y \in \mathbb{C}^k$. For each such (D, u) we consider the d-special points of $\mathbb{C}^k$ such that $W_u^D \subset V_y$. The Zariski closure of this set consists of finitely many d-special subvarieties of $\mathbb{C}^k$, $Y^{(D,u)}$. Then the finite set of $W_u^D \times Y^{(D,u)}$ includes all the maximal (Σ, d)-special subvarieties of V. □

Now we return to the setting of Theorem 1.1. We will prove a more general version allowing U-special points in $\prod B_i$, and d-rational points in $\mathbb{C}^k$. Let

$$X = B_1 \times \ldots \times B_n \times E_1 \times \ldots \times E_m \times \mathbb{G}^\ell \times \mathbb{C}^k.$$

6.3. Definition. Let X as above, $S \subset Y(1)(\mathbb{C})$ a finite set, and d a positive integer. An (S, d)-*special point* of X is a point

$$R = (P_1, \ldots, P_n, Q_1, \ldots, Q_m, y_1, \ldots, y_\ell, t_1, \ldots, t_k)$$

such that

1. Each $P_i \in B_i$ is a torsion point on an S-special fibre;
2. Each $Q_j \in E_j$ is a torsion point;
3. Each y_h is a torsion point;
4. Each t_b is a d-special point.

Now suppose X, S, d as above. We want to define (S,d)-special subvarieties of X. Now some of the E_i may be S-special, and then we can regard X as a subvariety of X' obtained by adding additional elliptic modular factors B'_i and regarding $V \subset X'$. Therefore in framing the definition we may assume that the E_i are all non-S-special.

6.4. Definition. Let X, S, d as above, with all the E_i non-S-special. Then an (S,d)-*special subvariety* of X is a cartesian product of

1. An S-special subvariety of $B_1 \times \ldots \times B_n$;
2. A torsion coset of $E_1 \times \ldots \times E_m$;
3. A torsion coset of $\mathbb{G}^\ell$;
4. A d-special subvariety of $\mathbb{C}^k$.

6.5. Proposition. *Suppose X, S, d as above with all the E_i non-S-special. Let*

$$S^* = S \cup \{j(E_i), i = 1, \ldots, m\}$$

and put

$$X' = B_1 \times \ldots \times B_n \times B'_1 \times \ldots \times B'_m \times \mathbb{G}^\ell \times \mathbb{C}^k.$$

If $T \subset X'$ is an (S^*, d)-special subvariety of X which contains an (S,d)-special point of X then it is an (S,d)-special subvariety of X.

Proof. Since the E_i are not S-special, there cannot be relations between the τ-coordinates in X' corresponding to them and the other τ-coordinates, and T must factor into a product. □

6.6. Theorem. *Let $S \subset Y(1)(\mathbb{C})$ be a finite set and d a non-negative integer. Let $V \subset X$ be a Zariski closed algebraic subset. Then V contains only finitely many maximal (S,d)-special subvarieties.*

Proof. Let $S^* = S \cup \{j(E_i), i = 1, \ldots, m\}$. View $V \subset X \subset X'$ as above and apply Theorem 6.2 to find finitely many maximal (S^*, d)-special subvarieties of V. Take the finite subset that contain (S,d)-special points of X. Then these are the maximal (S,d)-special subvarieties of V. □

6.7. Remarks. 1. One would like to extend "finite generation" to the fibres. This would encompass Mordell-Lang in products of elliptic curves and $\mathbb{G}^\ell$.

2. It would be interesting to see if the the present methods could prove the special point problem for powers $\mathcal{P}^n$ of the Poincaré biextension $\mathcal{P}$ of an elliptic modular curve studied in [4, 5, 6].

7. Linear relations between singular moduli

Let us call elements $g_1, \ldots, g_n \in \mathrm{GL}_2^+(\mathbb{Q})$ "independent modulo $\mathrm{SL}_2(\mathbb{Z})$" if they are in distinct $\mathrm{SL}_2(\mathbb{Z})$ orbits when considered in $\mathrm{PSL}_2(\mathbb{R})$, i.e. there are no relations $g_i = \gamma g_j$ as fractional linear transformations of $\mathbb{H}$ where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

7.1. Proposition. *Suppose $g_1, \ldots, g_n \in \mathrm{GL}_2^+(\mathbb{Q})$ are independent modulo $\mathrm{SL}_2(\mathbb{Z})$. Then the functions*

$$1, j(g_1\tau), \ldots, j(g_n\tau)$$

on $\mathbb{H}$ are linearly independent over $\mathbb{C}$.

Proof. We use the q-expansion

$$j(\tau) = \sum_{m=-1}^{\infty} c(m)q^m = \frac{1}{q} + 744 + \sum_{m=0}^{\infty} c(m)q^m$$

where $q = \exp(2\pi i\tau)$ and $c(m) \in \mathbb{Z}$ are well known to be positive, in fact they grow rapidly by a result of Petersson (see e.g. [30, §3, eqn. (24), p 202]).

If $g \in \mathrm{GL}_2^+(\mathbb{Q})$ we may write $g = \gamma h$ where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $h\tau = r\tau + s$ where $r, s \in \mathbb{Q}$ with $0 < r$ and $0 \leq s < 1$. Let us write $g \sim r\tau + s$ in this situation. The g_i are $\mathrm{SL}_2(\mathbb{Z})$-inequivalent iff the corresponding linear functions $r_i\tau + s_i$ are distinct. Different g_i may have the same r_i, so we will re-index them as g_{ij} so that

$$g_{ij} \sim r_i\tau + s_{ij}, \quad r_1 < \ldots < r_k.$$

Suppose the functions are linearly dependent over $\mathbb{C}$, so we have a relation

$$\sum_{i,j} a_{ij} j(g_{ij}\tau) = b, \quad a_{ij}, b \in \mathbb{C}.$$

Let us consider $\tau = it$ with $t \in [1, \infty)$. We have $q = \exp(-2\pi t)$ and so

$$(*) \qquad \sum_{m=-1}^{\infty} c(m) \sum_{i,j} a_{ij} q^{mr_i} \exp\left(2\pi i m s_{ij}\right) = b$$

identically in q. Thus, apart from the constant term

$$744 \sum_{i,j} a_{ij} = b$$

the coefficient of each distinct power of q on the left-hand side of $(*)$ must vanish. Now it is easy to see that for infinitely many suitable m, the only contribution to the coefficient of t^{mr_1} comes from the r_1 terms (just take m to be a large prime number), and so, since $c(m) \neq 0$, for infinitely many m we have

$$\sum_{1,j} a_{1j} \exp\left(2\pi i m s_{1j}\right) = 0.$$

As the $\exp(2\pi i s_{1j})$ are distinct, we must have $a_{1j} = 0$ for all j. Then the same holds for $r_2, \ldots, r_k$ and finally we see that $b = 0$ as well. □

In the following, a "partition" of $\{1, \ldots, N\}$ will mean a pair $(A_0, \{A_1, \ldots, A_M\})$ where $A_0 \subset \{1, \ldots, N\}$, possibly empty, and $A_1, \ldots, A_M$ is a partition of $\{1, \ldots, N\} \backslash A_0$ in the usual sense (no $A_j, j > 0$ is empty, and the partitands are unordered). We allow $A_0 = \{1, \ldots, N\}, M = 0$.

7.2. Proposition. *Suppose $V \subset Y(1)^n$ is a linear subvariety defined over $\mathbb{C}$. Then a maximal weakly special $Y \subset j^{-1}(V)$ has the following form. There is a "partition" $(A_0, \{A_1, \ldots, A_k\})$ of $\{1, \ldots, n\}$ and $c_i \in \mathbb{C}$ for $i \in A_0$ such that $(z_1, \ldots, z_n) \in Y$ provided*

$$z_i = g_{ij} z_j$$

for some $g_{ij} \in \mathrm{SL}_2(\mathbb{Z})$ whenever $i, j \in A_k, k > 0$, and

$$z_i = c_i \in \mathbb{C}$$

for each $i \in A_0$.

Proof. Let $Y \subset j^{-1}(V)$ be a maximal weakly special subvariety. Choose I maximal such that the variables x_i are algebraically independent on V. Then every other x_j is linearly dependent on them, so by Proposition 7.1 the corresponding z_j must satisfy a relation $z_j = g_{ij} z_i$ for some $i \in I$, with $g_{ij} \in \mathrm{SL}_2(\mathbb{Z})$ or be constant. □

A weakly special subvariety T as in Proposition 7.2 is uniquely determined by the "partition" $A = (A_0, \{A_1, \ldots, A_m\})$ and the tuple $c = (c_k : k \in A_0)$. Let us denote it $T_{A,c}$. Let us say that a "partition" $B = (B_0, \{B_1, \ldots, B_h\})$ is a *refinement* of A if, for each $i > 0$, $B_i \subset A_j$ for some $j \geq 0$, while $B_0 \subset A_0$. If B is a refinement of A but $B \neq A$ then we must have $h > m$, and then the corresponding $T_{B,d}$ has bigger dimension than $T_{A,c}$.

7.3. Proposition. *Let $V \subset Y(1)^n$ be a linear subvariety defined over $\mathbb{C}$, and $T \subset \mathbb{C}^n$ weakly special. Then T is a maximal weakly special subvariety of V if and only if:*

1. *$T \subset V$*
2. *$T = T_{A,c}$ for some "partition" A and tuple c*
3. *There is no refinement B of A with $B \neq A$ and tuple d with $d_i = c_i$ for $i \in B_0$ such that $T_{B,d} \subset V$.*

Proof. Clear from the discussion above. □

7.4. Proposition. *Let $V \subset Y(1)^n$ be a linear subvariety defined over $\mathbb{C}$ and $T = T_{A,c}$ a weakly special linear subvariety as above. Then $T \subset V$ if and only if, for any linear equation*

$$\sum_{i=1}^{n} a_i x_i = b$$

vanishing on V we have

$$\sum_{i \in A_j} a_i = 0, \quad j = 1, \ldots, m, \quad \text{and} \sum_{i \in A_0} a_i c_i = b.$$

Proof. Take new variables $\xi_j, j = 1, \ldots, m$. Putting $x_i = \xi_j$ for $i \in A_j, j = 1, \ldots, m$ and $\alpha_j = \sum_{i \in A_j} a_i$ we see that the above equation holds on T just if

$$\sum_{j=1}^{k} \alpha_j \xi_j = b - \sum_{i \in A_0} a_i c_i$$

for all choices of the ξ_j, which means that $\alpha_j = 0, j = 1, \ldots, m$ and $b = \sum_{i \in A_0} a_i c_i$ as required. □

We also observe the following.

7.5. Proposition. *Let $V \subset Y(1)^n$ be linear, defined over $\mathbb{C}$, and $S \subset Y(1)(\mathbb{C})$. If T is a maximal S-special subvariety of V then it is also a maximal weakly special subvariety of V.*

Proof. Suppose $T = T_{A,c}$. Since T is special, all the c_i are special. If $T_{B,c}$ is weakly special with $T \subset T_{B,d}$ then $d_i = c_i$ are special, so $T_{B,d}$ is special. □

In $\mathbb{G}^\ell$, if we consider linear relations

$$V : \sum_{i=1}^{\ell} a_i x_i = b$$

to be solved in roots of unity $x_i = \zeta_i$ we see that, if $(\zeta_1, \ldots, \zeta_\ell)$ is a solutions for which some subsum $\sum_{i \in A} a_i \zeta_i$ vanishes, then we can multiply the corresponding $\zeta_i, i \in A$ by an arbitrary root of unity ζ, yielding a torsion coset of positive dimension. Torsion cosets $T \subset V$ thus corresponds to a "partition" $(A_0, \{A_1, \ldots, A_m\})$ of $\{1, \ldots, n\}$, and tuple $\zeta = (\zeta_1, \ldots, \zeta_n)$ of roots of unity such that $\sum_{i \in A_k} a_i \zeta_i = 0$ for $i = 1, \ldots, k$ while $\sum_{i \in A_0} a_i \zeta_i = b$. Putting $A = (A_0, \{A_1, \ldots, A_m\})$ and $\zeta = (\zeta_i : i \in A_0)$ we may call this coset $T_{A,\zeta}$. The parameter ζ is unique if we specify that $\zeta_j = 1$ for the smallest index in each $A_j, j \geq 1$.

Then $T_{A,\zeta}$ is maximal if there is no refinement $(B_0, \{B_1, \ldots, B_h\})$ of the partition $A = (A_0, \{A_1, \ldots, A_m\})$ and tuple $\eta = (\eta_1, \ldots, \eta_n)$ of roots of unity with the same properties such that $T_{A,\zeta} \subset T_{B,\eta}$ but $B \neq A$. The zero-dimensional torsion cosets $T \subset V$ which are maximal correspond to the *indecomposable* solutions (no subsum vanishes) in the terminology of Dvornicich-Zannier [15]; sometimes called *non-degenerate* solutions.

According to Mann's theorem [25], see also refinements and extensions in [15], given d, ℓ there are only finitely many indecomposable solutions, and indeed this is obtained with explicit effective bounds. We state a more general form of Theorem 1.3 allowing S-special j-invariants for any finite $S \subset \mathbb{C}$ and d-special coefficients.

7.6. Definition. Let d be a positive integer, let n, ℓ non-negative integers and let $S \subset Y(1)(\mathbb{C})$.

1. A tuple $(j_1, \ldots, j_n, \zeta_1, \ldots, \zeta_\ell)$ is called an *(S, d, n, ℓ)-tuple* if the j_i are S-special, the ζ_j are roots of unity, and they satisfy a non-trivial relation

$$a_1 j_1 + \ldots + a_n j_n + b_1 \zeta_1 + \ldots + b_\ell \zeta_\ell + c = 0$$

where a_i, b_j, c are algebraic numbers, each of degree $\leq d$ over $\mathbb{Q}$.

2. An (S,d,n,ℓ)-tuple is called *non-degenerate* if

(i) there does not exist a non-empty subset $I \subset \{1,\ldots,n\}$ and a singular modulus j such that $j_i = j$ for all $i \in I$ and $\sum_{i\in I} a_i = 0$,

(ii) no proper (non-empty) subsum of $b_1\zeta_1 + \ldots + b_\ell\zeta_\ell + c$ vanishes (but c may be absent if $\ell = 0$).

7.7. Theorem. *For given d, n, ℓ and finite $S \subset Y(1)(\mathbb{C})$ there are only finitely many non-degenerate (S,d,n,ℓ)-tuples.*

Proof. Let d, n, ℓ, S be given and apply Theorem 6.2 to the variety

$$V \subset X, \quad X = \mathbb{C}^n \times \mathbb{G}^\ell \times \mathbb{C}^{n+\ell+1}$$

defined by

$$a_1x_1 + \ldots + a_nx_n + b_1y_1 + \ldots + b_\ell\, y_\ell + c = 0$$

where $(x_1,\ldots,x_n) \in \mathbb{C}^n$, $(y_1,\ldots,y_\ell) \in \mathbb{G}^\ell$, and $p = (a_1,\ldots,a_n,b_1,\ldots,b_\ell,c) \in \mathbb{C}^{n+\ell+1}$. For $p \in \mathbb{C}^{n+\ell+1}$ we let $V_p \subset \mathbb{C}^n \times \mathbb{G}^\ell$ be the fibre of V. We see that, for any p whose coordinates have degree $\le d$ over $\mathbb{Q}$, there are just finitely many possibilities for maximal

$$T = T_{A,j} \times T_{B,\zeta} \subset V_p.$$

We see that $T_{A,j}$ determines j uniquely, as does $T_{B,\zeta}$ determine ζ (with the above normalising assumption $\zeta_i = 1$ on least indices in partitands). Then T is of dimension zero just if the (S,d,n,ℓ)-tuple (j,ζ) is non-degenerate. □

7.8. Remarks. 1. For roots of unity only (i.e. $n = 0$), an effective result on (in our terms) non-degenerate $(\emptyset, d, 0, \ell)$-tuples was obtained by Schinzel [45], substantially improved by Zannier [54], and further in [15].

2. For arbitrary *complex* coefficients, an effective bound on the *number* of non-degenerate solutions to a linear equation in roots of unity is due to Schlickewei [46], substantially improved by Evertse [16]. The corresponding uniform AO statement for families of subvarieties of $Y(1)^n$ follows from AO for all such powers $Y(1)^\nu$ by "automatic uniformity" as shown by Scanlon [44]. On such uniformity aspects of ZP see Zannier [55, 1.3.8] and the Appendix B by Masser.

3. The result presumably holds (and is implied by ZP) with finite generation on the $\mathbb{G}^\ell$ points as well, but this is not accessible to the present methods.

References

1. Y. André, *G-functions and geometry,* Aspects of Mathematics E13, Vieweg, Braunschweig, 1989.
2. Y. André, Finititude des couples d'invariants modulaire singuliers sur une courbe algébrique plane non modulaire, *J. Reine Angew. Math.* **505** (1998), 203–208.
3. Y. André, *Shimura varieties, subvarieties, and CM points,* Six lectures at the Franco - Taiwan arithmetic festival, Aug.-Sept. 2001.

4. D. Bertrand, Unlikely intersections in Poincaré biextensions over elliptic schemes, preprint 2011, and *Notre Dame J. Formal Logic* (Oléron proceedings), to appear.
5. D. Bertrand with an appendix by B. Edixhoven, Special points and Poincaré biextensions, arXiv preprint 2011.
6. D. Bertrand, D. Masser, A. Pillay, and U. Zannier, Relative Manin-Mumford for semi-abelian surfaces, preprint 2011.
7. E. Bombieri, D. Masser, and U. Zannier, Anomalous subvarieties – structure theorems and applications, *IMRN* **19** (2007), 33 pages.
8. S. David, Minorations de formes linéaires de logarithms elliptiques, *Mém. Soc. Math. France. (N.S.)* **62** (1995).
9. C. Daw and A. Yafaev, An unconditional proof of the André-Oort conjecture for Hilbert modular surfaces, *Manuscripta Math.* **135** (2011), 263-271.
10. L. van den Dries, A generalization of the Tarski-Seidenberg Theorem and some non-definability results, *Bull. Amer. Math. Soc.* **15** (1986), 189–193).
11. L. van den Dries, *Tame topology and o-minimal structures,* LMS Lecture Note Series **248**, CUP, 1998.
12. L. van den Dries and A. Günaydin, The fields of real and complex numbers with a small multiplicative group, *Proc. London. Math. Soc.* **93** (2006), 43–81.
13. L. van den Dries and A. Günaydin, Mann Pairs, *Trans. Amer. Math. Soc.* **362** (2010), 2393–2414.
14. L. van den Dries and C. Miller, On the real exponential field with restricted analytic functions, *Israel J. Math.* **85** (1994), 19–56.
15. R. Dvornicich and U. Zannier, On sums of roots of unity, *Monatshefte Math.* **129** (2000), 97–108.
16. J.-H. Evertse, The number of solutions of linear equations in roots of unity, *Acta Arith.* **89** (1999), 45-51.
17. A. Gabrielov, Projections of semi-analytic sets, *Funct. Anal. Appl.* **2** (1968), 282–291.
18. P. Habegger, Special points on fibred powers of elliptic surfaces, arXiv preprint, 2011, and *Crelle*, to appear.
19. P. Habegger and J. Pila, Some unlikely intersections beyond André–Oort, *Compositio* **148** (2012), 1–27.
20. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers,* Fifth edition, OUP, 1979.
21. M. Hindry, Autour d'une conjecture de Serge Lang, *Inventiones* **94** (1988), 575–603.
22. B. Klingler and A. Yafaev, The André-Oort conjecture, preprint, available from first author's webpage.
23. L. Kühne, An effective result of André–Oort type, *Annals* **176** (2012), 651–671.
24. M. Laurent, Équations diophantiennes exponentielles, *Inventiones* **78** (1984), 299–327.

25. H. B. Mann, On linear relations between roots of unity, *Mathematika* **12** (1965), 107–117.
26. D. Masser, Small values of the quadratic part of the Néron-Tate height on an abelian variety, *Compositio* **53** (1984), 153–170.
27. D. Masser and G. Wüstholz, Isogeny estimates for abelian varieties, and finiteness results, *Annals* **137** (1993), 459–472.
28. F. Oort, Canonical lifts and dense sets of CM points, *Arithmetic Geometry, Cortona, 1994,* 228–234, F. Catanese, editor, Symp. Math., XXXVII, CUP, 1997.
29. F. Pellarin, Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques, *Acta Arith.* **100** (2001), 203–243.
30. H. Petersson, Über die Entwicklungskoeffizienten der automorphen Formen, *Acta Math.* **58** (1932), 169–215.
31. Y. Peterzil and S. Starchenko, Uniform definability of the Weierstrass $\wp$ functions and generalized tori of dimension one, *Selecta Math. N. S.* **10** (2004), 525–550.
32. Y. Peterzil and S. Starchenko, Tame complex analysis and o-minimality, *Proceedings of the ICM, Hyderabad, 2010.*
33. J. Pila, Rational points of definable sets and results of André-Oort–Manin-Mumford type, *IMRN* **2009**, No. 13, 2476–2507, doi:10.1093/imrn/rnp022.
34. J. Pila, O-minimality and the André-Oort conjecture for $\mathbb{C}^n$, *Annals* **173** (2011), 1779–1840.
35. J. Pila, Modular Ax-Lindemann-Weierstrass with derivatives, *Notre Dame J. Formal Logic* (Oléron proceedings), to appear.
36. J. Pila and J. Tsimerman, The André-Oort conjecture for the moduli space of abelian surfaces, *Compositio* **149** (2013), 204–216, and arXiv.
37. J. Pila and J. Tsimerman, Ax-Lindemann for $\mathcal{A}_g$, arXiv preprint, 2012.
38. J. Pila and A. J. Wilkie, The rational points of a definable set, *DMJ* **133** (2006), 591–616.
39. J. Pila and U. Zannier, Rational points in periodic analytic sets and the Manin-Mumford conjecture, *Rend. Lincei Mat. Appl.* **19** (2008), 149–162.
40. R. Pink, A combination of the conjectures of Mordell-Lang and André-Oort, *Geometric methods in algebra and number theory,* F. Bogomolov, Y. Tschinkel, editors, pp 251–282, Prog. Math. **253**, Birkhauser, Boston MA, 2005.
41. R. Pink, A common generalization of the conjectures of André-Oort, Manin-Mumford, and Mordell-Lang, manuscript dated 17 April 2005 available from the author's webpage.
42. M. Raynaud, Courbes sur une variété abélienne et points de torsion, *Inventiones* **71** (1983), no. 1, 207–233.
43. M. Raynaud, Sous-variétés d'une variété abélienne et points de torsion, in *Arithmetic and Geometry, Volume I,* pp 327–352, Progr. Math. **35**, Birkhauser, Boston MA, 1983.
44. T. Scanlon, Automatic uniformity, *IMRN* **2004**, No. 62.

45. A. Schinzel, Reducibility of lacunary polynomials VIII, *Acta Arith.* **50** (1988), 91–106.
46. H. Schlickewei, Equations in roots of unity, *Acta Arith.* **76** (1996), 99–108.
47. T. Shioda, On elliptic modular surfaces, *J. Math. Soc. Japan* **24** (1972), 20–59.
48. A. Silverberg, Torsion points on abelian varieties of CM-type, *Compositio* **68** (1988), 241–249.
49. J. Top and N. Yui, Explicit equations of some elliptic modular surfaces, *Rocky Mountain J. Math.* **37** (2007), 663–687.
50. E. Ullmo, Quelques applications du théorème de Ax-Lindemann hyperbolique, preprint, 2012, available from the author's webpage.
51. E. Ullmo and A. Yafaev, Galois orbits and equidistribution of special subvarieties: towards the André-Oort conjecture, preprint, 2006, available from the first author's webpage.
52. E. Ullmo and A. Yafaev, Hyperbolic Ax-Lindemann theorem in the cocompact case, preprint, 2011, available from the first author's webpage.
53. A. J. Wilkie, Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function, *J. Amer. M. Soc.* **9** (1996), 1051–1094.
54. U. Zannier, On the linear independence of roots of unity over finite extensions of $\mathbb{Q}$, *Acta Arith.* **52** (1989), 171–182.
55. U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry,* with appendices by D. Masser, *Annals of Mathematics Studies* **181**, Princeton University Press, 2012.
56. B. Zilber, Exponential sums equations and the Schanuel conjecture, *J. London Math. Soc. (2)* **65** (2002), 27–44.

Mathematical Institute, University of Oxford, Oxford, UK pila@maths.ox.ac.uk