Forum of Mathematics, Pi (2015), Vol. 3, e1, 41 pages
doi:10.1017/fmp.2014.2

E_6 AND THE ARITHMETIC OF A FAMILY OF NON-HYPERELLIPTIC CURVES OF GENUS 3

JACK A. THORNE
DPMMS, Wilberforce Road, Cambridge CB3 0WB, UK;
email: thorne@dpmms.cam.ac.uk

Received 1 May 2014; accepted 8 December 2014

Abstract

We study the arithmetic of a family of non-hyperelliptic curves of genus 3 over the field $\mathbb{Q}$ of rational numbers. These curves are the nearby fibers of the semi-universal deformation of a simple singularity of type E_6. We show that average size of the 2-Selmer sets of these curves is finite (if it exists). We use this to show that a positive proposition of these curves (when ordered by height) has integral points everywhere locally, but no integral points globally.

2010 Mathematics Subject Classification: 14G05 (primary); 14L30 (secondary)

Overview

In this paper, we study the problem of counting integral points on a family of algebraic curves over the field $\mathbb{Q}$ of rational numbers. More precisely, we study the average size of a cohomological proxy for the set of integral points, namely the 2-Selmer set, as we vary the curve through a fixed family.

Our methods are inspired by those of Bhargava and his collaborators, who have studied to great effect the average size of the n-Selmer groups of elliptic curves over $\mathbb{Q}$ for diverse values of n. Broadly speaking, their idea is to parameterize Selmer elements by $G(\mathbb{Q})$-orbits in $V(\mathbb{Q})$, for suitable representations V of reductive groups G over $\mathbb{Q}$; Bhargava's powerful techniques for counting integral points in fundamental domains then allow one to get a handle on these Selmer averages. (More recently, Bhargava, Gross, and Wang have generalized these methods to the context of 2-Selmer groups of Jacobians of hyperelliptic curves of arbitrary genus.)

In another work, we have given a construction that associates to a simply laced Dynkin diagram (that is, of type A_n, D_n, or E_n) a family of algebraic curves and a representation (G, V) which together are natural candidates for this program. In the cases of type A_n, the curves in these families are hyperelliptic, and we recover the situation studied in the aforementioned works of Bhargava, Gross, and Wang. In the cases of type D_n, the curves are hyperelliptic, and are equipped with additional marked points. In the exceptional cases of type E_6, E_7, and E_8, the curves obtained are non-hyperelliptic.

Our goal in this paper is therefore to carry out some of this program in the simplest exceptional situation, arising from the simply laced Dynkin diagram of type E_6. In this case, the family of curves obtained is essentially the universal family of pairs (C, P), where C is a plane quartic curve and P is a marked point on C which is a hyperflex (that is, a point at which the projective tangent line has contact of order 4 with C). We are able to push the methods far enough to get some control over the 2-Selmer sets of these curves (in particular, to show that they are bounded on average). We then apply this to prove some interesting results about the average number of integral points.

1. Introduction

Let k be a field of characteristic 0, and let Y be a smooth geometrically connected projective curve over k of genus $g > 0$. Let J denote the Jacobian of the curve Y. We define a 2-covering of the curve Y to be an abelian finite étale cover $Z \to Y$, with Z geometrically connected and $\mathrm{Aut}_Y(Z)$ a k-form of the group $(\mathbb{Z}/2\mathbb{Z})^{2g}$. An isomorphism $(Z \to Y) \to (Z' \to Y)$ of 2-coverings is just an isomorphism $Z \to Z'$ over Y. The set $\mathrm{Cov}_2(Y)$ of isomorphism classes of 2-coverings $(Z \to Y)$, if non-empty, is a torsor for the group $H^1(k, J[2])$.

Now suppose that k is a number field. We define the 2-Selmer set of Y to be the subset $\mathrm{Sel}_2(Y) \subset \mathrm{Cov}_2(Y)$ of 2-coverings $(Z \to Y)$ such that $Z(k_v) \neq \emptyset$ for every place v of k. If $Y(k)$ is non-empty, then the set $\mathrm{Sel}_2(Y)$ is non-empty. On the other hand, $\mathrm{Sel}_2(Y)$ can often be effectively computed. In such situations, $\mathrm{Sel}_2(Y)$ is a useful proxy for the set $Y(k)$. (See, for example, the paper [BS09], in which the authors give an algorithm to calculate a closely related set when Y is hyperelliptic.)

Now suppose further that the curve Y has a marked rational point $P_\infty \in Y(k)$. In this case, the Abel–Jacobi map $\mathrm{AJ} : Y \hookrightarrow J$ embeds the curve Y in its Jacobian, sending the point P_∞ to the origin. The 2-Selmer set $\mathrm{Sel}_2(Y)$ is a pointed subset of the 2-Selmer group $\mathrm{Sel}_2(J)$; these two sets admit the following cohomological description. If v is a place of k, then there is a canonical map $\delta_v : J(k_v) \to H^1(k_v, J[2])$, arising from the Kummer exact sequence of J. We then have

$$\mathrm{Sel}_2(Y) = \{x \in H^1(k, J[2]) \mid \forall v, \mathrm{Res}_v(x) \in \delta_v \mathrm{AJ}(Y(k_v))\},$$
$$\mathrm{Sel}_2(J) = \{x \in H^1(k, J[2]) \mid \forall v, \mathrm{Res}_v(x) \in \delta_v J(k_v)\}.$$

In this paper, we investigate the 2-Selmer sets of a family of non-hyperelliptic curves of genus 3:

$$X : y^3 = x^4 + y(p_2x^2 + p_5x + p_8) + p_6x^2 + p_9x + p_{12}. \tag{1.1}$$

Here, x, y are coordinates, and $p_2, \dots, p_{12}$ are coefficients. The projective closure of this equation in $\mathbb{P}^2$ defines a family $Y \to B$ of plane quartic curves, where $B = \mathbb{A}^6_{\mathbb{Q}}$ is the affine space with coordinates $p_2, \dots, p_{12}$. (Each of these curves has a unique point at infinity.) The open subscheme of B above which Y is smooth is a fine moduli space for triples (C, P_∞, t), where C is a smooth projective curve which is non-hyperelliptic of genus 3, $P_\infty \in C(k)$ is a marked point such that $4P_\infty$ is a canonical divisor, and $t \in T_{P_\infty} C$ is a non-zero element of the Zariski tangent space at P_∞. We have $p_i(C, P_\infty, \lambda t) = \lambda^i p_i(C, P_\infty, t)$. (See Lemma 4.1.)

Let us write $\mathcal{B} = \mathbb{A}^6_{\mathbb{Z}}$, coordinates again being given by $p_2, \dots, p_{12}$. We write $\mathcal{F}_0 \subset \mathcal{B}(\mathbb{Z})$ for the set of points b such that Y_b is smooth. We say that a subset $\mathcal{F} \subset \mathcal{F}_0$ is defined by congruence conditions if there exist an integer $N \geqslant 1$ and a non-empty subset $A \subset \mathcal{B}(\mathbb{Z}/N\mathbb{Z})$ such that $\mathcal{F}$ is the inverse image of A in $\mathcal{F}_0$. If $b \in \mathcal{F}_0$, then we define $H(b) = \sup_i |p_i(b)|^{72/i}$.

We can now state our main theorems.

THEOREM 1.1 (Theorem 4.3). *Let $\mathcal{F} \subset \mathcal{F}_0$ be a subset defined by congruence conditions. Then*

$$\limsup_{X \to \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ H(b) < X}} \# \mathrm{Sel}_2(Y_b)}{\sum_{\substack{b \in \mathcal{F} \\ H(b) < X}} 1} < \infty.$$

More informally, the average size of $\mathrm{Sel}_2(Y_b)$ *is bounded.*

We note that we would obtain the same result if we restricted consideration to the average over those points $b \in \mathcal{F}$ which are minimal, in some sense, and therefore give a set of representatives for isomorphism classes of pairs (C, P_∞); see Remark 4.5 below.

THEOREM 1.2 (Theorem 4.4). *Let $\epsilon > 0$. Then there exists a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions such that*

$$\limsup_{X \to \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ H(b) < X}} \# \mathrm{Sel}_2(Y_b)}{\sum_{\substack{b \in \mathcal{F} \\ H(b) < X}} 1} < 1 + \epsilon.$$

Consequently, we have

$$\liminf_{X \to \infty} \frac{\#\{b \in \mathcal{F} \mid H(b) < X, \# \mathrm{Sel}_2(Y_b) = 1\}}{\#\{b \in \mathcal{F} \mid H(b) < X\}} > 1 - \epsilon.$$

Since we can only control the average size of the 2-Selmer sets $\mathrm{Sel}_2(Y_b)$, and not the full 2-Selmer groups $\mathrm{Sel}_2(J_b)$, it does not seem possible to use the above results to follow [PS14] and show, for example, that for a positive proportion of $b \in \mathcal{F}_0$ the set of rational points is trivial (that is, $Y_b(\mathbb{Q}) = \{P_\infty\}$). However, control of $\mathrm{Sel}_2(Y_b)$ does have Diophantine consequences for points which are 'far from infinity' in some (p-adic or Archimedean) sense. As an example of this, we use the above theorems to deduce the following.

THEOREM 1.3 (Theorem 4.8). *Let $\epsilon > 0$. Then there exists a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions satisfying the following conditions.*

(1) *For every $b \in \mathcal{F}$, and for every prime p, $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$.*

(2) *We have*

$$\liminf_{X \to \infty} \frac{\#\{b \in \mathcal{F} \mid H(b) < X,\ \mathcal{X}_b(\mathbb{Z}_{(3)}) = \emptyset\}}{\#\{b \in \mathcal{F} \mid H(b) < X\}} > 1 - \epsilon.$$

In particular, a positive proportion of curves in $\mathcal{F}_0$ have integral points everywhere locally, but no integral points globally.

Methods. Our methods are inspired by those of Bhargava and his collaborators, who have proved similar (and, in general, substantially more precise) results for elliptic and hyperelliptic curves; see the papers [BS, BG, Bha]. Roughly speaking, there are three main steps.

(1) Find a reductive group G over $\mathbb{Q}$ and a representation V having the following property: for a field $k/\mathbb{Q}$, the k-orbits of $G(k)$ on $V(k)$ with prescribed invariants are related to the set $J(k)/2J(k)$, where J is the Jacobian of an algebraic curve being defined in terms of these invariants.

(2) Show that when $k = \mathbb{Q}$ there are sufficiently many orbits to describe the 2-Selmer groups (or sets) of these curves, and that (appropriate integral models of G and V having been fixed) these orbits all have integral representatives.

(3) Count the integral orbits with bounded invariants, and perform a sieve to remove those orbits not corresponding to 2-Selmer elements.

Our approach to the first two points is quite different to that taken in earlier works. For the third point, we follow Bhargava's ideas closely. (Since we aim only to get the qualitative results Theorems 1.1 and 1.2 above, we do not need to perform a sieve.) We now describe each of these steps in turn. In an earlier paper [Tho13], we have associated to each Dynkin diagram $\mathcal{D}$ of type A_n, D_n, or E_n the following data.

- A pair (G, V) consisting of a split reductive group over $\mathbb{Q}$ and an irreducible representation V of G over $\mathbb{Q}$ which is coregular: by definition, this means that the invariant ring $\mathbb{Q}[V]^G \subset \mathbb{Q}[V]$ is abstractly isomorphic to a polynomial ring.

- A family $X \to B$ of affine curves over the categorical quotient $B = \operatorname{Spec} \mathbb{Q}[V]^G$. In fact, X is a semi-universal deformation of its central fiber, which has a unique singularity, which is simple of type $\mathcal{D}$. In particular, when $\mathcal{D} = E_6$, this is exactly the family of curves (1.1) above.

Let us write $\pi : V \to B$ for the quotient map. There is also a natural discriminant $\Delta \in \mathbb{Q}[V]^G$, defined up to scalar. If $k/\mathbb{Q}$ and $b \in B(k)$, then X_b is smooth if and only if $\Delta(b) \neq 0$; in this case, $V_b = \pi^{-1}(b)$ consists of a single closed G-orbit in V, and the stabilizer $\operatorname{Stab}_G(v)$ of any $v \in V_b(k)$ is a finite k-group, for which there is a canonical isomorphism $\operatorname{Stab}_G(v) \cong J_b[2]$. (In particular, this subgroup is canonically independent of the choice of $v \in V_b(k)$.) Here, we write J_b for the Jacobian of the canonical smooth compactification Y_b of the curve X_b. After making some auxiliary choices (in particular, a subregular normal $\mathfrak{sl}_2$-triple; see Section 2 below), we obtain a commutative diagram:

$$\begin{tikzcd}
X_b(k) \arrow[r] \arrow[d] & G(k)\backslash V_b(k) \arrow[d] \\
J_b(k) \arrow[r] & H^1(k, J_b[2])
\end{tikzcd}$$

(For a precise statement and definition of the various arrows here, see Section 2.2 below. The diagram so obtained is independent of any choices made.) In particular, taking the above diagram for $k = \mathbb{R}$ and $k = \mathbb{Q}_p$ for every prime p, together with the Hasse principle for G, shows that the set $G(\mathbb{Q})\backslash V_b(\mathbb{Q})$ contains enough elements to describe the set $\operatorname{Sel}_2(Y_b)$.

We must show that these elements admit integral representatives. The arrow $X_b(k) \to G(k)\backslash V_b(k)$ in the diagram above has the crucial property that it arises from an inclusion $X \subset V$, defined over $\mathbb{Q}$. In particular, if we fix integral structures on X and V, then this morphism will have bounded denominators. This immediately implies that, provided $b \in \mathcal{B}(\mathbb{Z})$ is 'sufficiently divisible', every element of the 2-Selmer set $\operatorname{Sel}_2(Y_b)$ has an integral representative; see Section 2.5 below. In order to fix an integral structure on V, we find it convenient to give G the structure of Chevalley group, and to take inside V an admissible lattice, in the sense of [**Bor70**].

It remains to count the number of integral orbits with bounded invariants, in order to obtain an upper bound for the average size of the 2-Selmer set.

We accomplish this using Bhargava's idea of counting points by taking the average number of points in a set of translated fundamental domains. The arguments follow those of [BG, Section 10], with some minor simplifications since we do not aim for an exact count. The only place where serious work needs to be done is in the cutting off of the cusp of the fundamental domain; see Proposition 3.6. We describe the contributions of the cusp here in terms of the ambient E_6 root system, and eliminate their contribution to the 2-Selmer count by a case-by-case calculation.

The above suffices to prove Theorem 1.1. We note that it seems likely, based on previous results, that the average size of $\mathrm{Sel}_2(J_b)$ exists, and equals 3; and that the same remarks apply to the average over any subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions. On the other hand, the same heuristics suggest that the average size of $\mathrm{Sel}_2(Y_b)$ can depend on the choice of congruence family, if only because the quantities

$$\frac{\#\mathrm{Im}(Y_b(\mathbb{Q}_p) \to J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p))}{\#J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p)}$$

can vary with $b \in B(\mathbb{Q}_p)$. In Section 2.10, we exploit this by writing down curves Y_b for which the above quantity is equal to $\frac{1}{4}$. After imposing sufficiently many congruence conditions of this type, we carry out enough of the sieve to force the set $\mathrm{Sel}_2(Y_b)$ to be small on average, giving Theorem 1.2. This dependence of the average value of $\#\,\mathrm{Sel}_2(Y_b)$ (assuming it exists) on the subset $\mathcal{F}$ is our excuse for not attempting to calculate it exactly.

Generalizations. For the most part, the arguments of this paper are general, and apply verbatim to any of the families of curves constructed in [Tho13]. The only part where this is not the case is the process of cutting off the contribution of the cusp of the fundamental domain, as in Proposition 3.6. We have restricted ourselves to the case $\mathcal{D} = E_6$ here in the interest of brevity and simplicity, but it would be interesting to try to carry out the argument in other cases, for example when $\mathcal{D} = E_7$ or E_8. It does seem that in these cases the necessary calculations (see Section 5) become formidable!

One can also hope that the same circle of ideas will apply to the study of the full 2-Selmer groups $\mathrm{Sel}_2(J_b)$, and to the calculation of their exact average. The main barrier to doing this is in the first two steps of the program outlined above, namely the construction of $G(k)$-orbits in $V_b(k)$ corresponding to elements of $J_b(k)$, and the existence of integral representatives for 2-Selmer elements when $k = \mathbb{Q}$. A solution to the first problem, using techniques different to those used here, will be given in another paper [Tho].

Organization of this paper. The main new ideas in this paper are contained in Section 2 below. In this section, we define the representation (G, V) under consideration, and recall from [Tho13] its relation with the family of curves $X \to B$ above. We also discuss our choice of integral structures, and how this choice interacts with our previous constructions. In particular, in Section 2.10, we write down the congruence conditions that will be used to obtain the families of Theorem 1.2. In Section 3, we carry out Bhargava's arguments for counting points in our context. In Section 4, we apply these results to deduce our main theorems. Finally, Section 5 contains information useful in the proof of Proposition 3.6.

2. Setup

We begin by recalling, following [Tho13], some basic aspects of the theory of Vinberg's θ-groups. The reader could also consult [Spr09] or [Pan05] for more information about algebraic groups or θ-groups, respectively.

Let k be a field of characteristic 0, and let H be a split, adjoint, simple and simply laced group over k, of rank n. (Thus H is a reductive group over k with trivial center. The Dynkin diagram of H is connected, because H is simple, and has no double edges, because H is simply laced.) We assume that H is endowed with a pinning $\mathcal{P} = (T, B, \{X_\alpha\}_{\alpha \in S})$; thus $T \subset H$ is a split maximal torus, $S \subset \Phi = \Phi(H, T)$ is a root basis, and X_α is a non-zero element of the α-root space $\mathfrak{h}_\alpha$. Let $\mathcal{R}$ denote the based root datum of H corresponding to $\mathcal{P}$, and let $\sigma \in \mathrm{Aut}(\mathcal{R})$ denote the image of -1, as in [Tho13, Section 2.2]. The pinning $\mathcal{P}$ determines a splitting of the short exact sequence

$$0 \to H \to \mathrm{Aut}(H) \to \mathrm{Aut}(\mathcal{R}) \to 0,$$

and we write $\sigma \in \mathrm{Aut}(H)(k)$ also for the corresponding automorphism of H. The principal involution of H is defined to be $\theta = \check{\rho}(-1) \cdot \sigma$, where $\check{\rho} \in X_*(T)$ is the sum of the fundamental coweights. We define $G = (H^\theta)^\circ$, and $V = \mathfrak{h}^{d\theta = -1}$. Then the group G is semi-simple, and V is an irreducible representation of G. We have the following basic theorem (see [Pan05, Theorem 1.1]).

THEOREM 2.1. *V contains Cartan subalgebras of $\mathfrak{h}$. If $\mathfrak{c} \subset V$ is a Cartan subalgebra, then the map $G \to N_H(\mathfrak{c})/Z_H(\mathfrak{c}) = W(H, \mathfrak{c})$ is surjective, and the canonical restriction maps*

$$k[\mathfrak{h}]^H \to k[V]^G \to k[\mathfrak{c}]^{W(H,\mathfrak{c})}$$

are isomorphisms.

We refer to any Cartan subalgebra $\mathfrak{c} \subset \mathfrak{h}$ which happens to lie in V as a Cartan subspace.

2.1. Conjugacy classes. We say that an element $v \in V$ is regular, respectively nilpotent, respectively semi-simple, if it is so when considered as an element of $\mathfrak{h}$. We write $\Delta \in k[V]^G$ for the restriction of a discriminant polynomial of H; thus Δ is defined up to scalar, is homogeneous of degree $\#\Phi$, and for $v \in V$ we have $\Delta(v) \neq 0$ if and only if v is regular semi-simple. The restriction of Δ to a Cartan subspace $\mathfrak{c}$ vanishes to order 2 along each root hyperplane. We write $B = \operatorname{Spec} k[V]^G$. We can choose algebraically independent homogeneous generators $p_{d_1}, \ldots, p_{d_n}$ of $k[V]^G$, where p_{d_i} is of degree d_i, and $d_1, \ldots, d_n$ are the invariant degrees of H; in particular, B is isomorphic to $\mathbb{A}^n_k$. We write $\pi : V \to B$ for the natural quotient map.

Since H is pinned, V contains a canonical regular nilpotent element $E = \sum_{\alpha \in S} X_\alpha$, which is contained in a unique normal $\mathfrak{sl}_2$-triple (E, X, F) [Tho13, Corollary 2.16]. By definition, this means that $E, F \in V$, and $X \in \mathfrak{g}$ satisfy the relations

$$[X, E] = 2E, \quad [X, F] = -2F, \quad [E, F] = X. \tag{2.1}$$

We define $\kappa = E + \mathfrak{z}_V(F) = E + \{v \in V \mid [F, v] = 0\}$, an affine-linear subspace of V of dimension n, and refer to κ as the Kostant section.

THEOREM 2.2. (1) *The composite $\kappa \to V \to V /\!\!/ G$ is an isomorphism.*

(2) *Let $b \in B(k)$ be such that $\Delta(b) \neq 0$. Then $V_b = \pi^{-1}(b)$ consists of a single G-conjugacy class.*

(3) *Let $\kappa^{reg.\, ss} \subset \kappa$ denote the open subscheme of regular semi-simple elements. The natural product morphism $\mu : G \times \kappa^{reg.\, ss} \to V^{reg.\, ss}$ is finite étale.*

Let $v \in V$. We say that v is reducible if either $\Delta(v) = 0$, or $\Delta(v) \neq 0$ and v is $G(k)$-conjugate to an element of $\kappa(k)$. This depends on the choice of the base field k; in particular, if k is algebraically closed, then every element of V is reducible. If $v \in V$ is not reducible, we say that v is irreducible.

2.2. Subregular curves and Jacobians. If (e, x, f) is any normal $\mathfrak{sl}_2$-triple (that is, a tuple of elements $e, f \in V$, $x \in \mathfrak{g}$ satisfying the relation (2.1)), then we can consider the associated slice $e + \mathfrak{z}_V(f) \subset V$. The group $\mathbb{G}_m$ has a contracting action on this affine linear subspace of V, with fixed point e. We now describe this action. Let $\rho : \mathbb{G}_m \to H$ be the cocharacter with $d\rho(1) = x$. If $t \in \mathbb{G}_m$ and

$v \in e + \mathfrak{z}_V(f)$, we define $t \cdot v = \rho(t^{-1}) \cdot t^2 v$. This action satisfies $\pi(t \cdot v) = t^2 \cdot \pi(v)$. See [Tho13, Section 3.1] for more details.

Now suppose that (e, x, f) is a normal $\mathfrak{sl}_2$-triple, and that e is a subregular nilpotent (that is, e is subregular when considered as an element of $\mathfrak{h}$). Let $X = e + \mathfrak{z}_V(f)$.

THEOREM 2.3. *The induced morphism $X \to B$ is faithfully flat, with reduced connected fibers of dimension 1. If $b \in B(k)$, then X_b is smooth if and only if $\Delta(b) \neq 0$; in this case, let Y_b denote the canonical projective completion of X_b, and let J_b denote the Jacobian variety of Y_b. Then there is a canonical isomorphism $\mathrm{Stab}_G(\kappa_b) \cong J_b[2]$ of finite k-groups.*

See [Tho13, Corollary 4.9]. In order to avoid introducing unnecessary notation, we now assume that H is of type E_6. This assumption will remain in effect for the rest of this paper. In this case, we have the following additional result.

THEOREM 2.4. (1) *We can choose invariant polynomials $p_2, p_5, p_6, p_8, p_9, p_{12} \in k[V]^G$ and coordinates $x, y \in k[X]$ such that the morphism $X \to B$ is given by*

$$X : y^3 = x^4 + y(p_2 x^2 + p_5 x + p_8) + p_6 x^2 + p_9 x + p_{12}.$$

(2) *Let $Y \to B$ denote the natural compactification of X as a family of plane quartic curves, and let $P_\infty \subset Y$ denote the divisor at infinity. Let $b \in B(k)$, and suppose that $\Delta(b) \neq 0$. Then the following diagram commutes:*

$$\begin{tikzcd}
X_b(k) \arrow[r] \arrow[d] & G(k)\backslash V_b(k) \arrow[d] \\
J_b(k) \arrow[r] & H^1(k, J_b[2])
\end{tikzcd}$$

There arrows in this diagram as follows. The arrow $X_b(k) \to J_b(k)$ is induced by the Abel–Jacobi map $Y_b \hookrightarrow J_b$, sending P_∞ to the origin. The map $X_b(k) \to G(k)\backslash V_b(k)$ is induced by the inclusion $X \hookrightarrow V$. The map $G(k)\backslash V_b(k) \hookrightarrow H^1(k, J_b[2])$ is the composite of the classifying map $G(k)\backslash V_b(k) \hookrightarrow H^1(k, \mathrm{Stab}_G(\kappa_b))$, which sends the orbit $G(k) \cdot \kappa_b$ to the identity, and the isomorphism $H^1(k, \mathrm{Stab}_G(\kappa_b)) \cong H^1(k, J_b[2])$. The map $J_b(k) \to H^1(k, J_b[2])$ is the connecting homomorphism of the Kummer exact sequence associated to the isogeny $[2] : J_b \to J_b$.

See [Tho13, Theorem 4.14].

2.3. Restricted roots. It is easy to show (using, for example, the results of [Ree10]) that G is abstractly isomorphic to PSp_8, and V corresponds under this isomorphism to the 42-dimensional subrepresentation of $\wedge^4 8$; however, we will not use this here.

We write $\Phi = \Phi(H, T)$ for the root system of H, and $\Phi = \Phi^+ \cup \Phi^-$ for the decomposition into positive and negative parts induced by the root basis S. The root system $\Phi(G, T^\theta)$ will also play a role; in order to distinguish elements of $X^*(T)$ and $X^*(T^\theta)$, we will generally write elements $\alpha, \beta, \ldots \in X^*(T)$ using Greek letters, and elements $a, b, \ldots \in X^*(T^\theta)$ using Roman letters. We write Φ/σ for the set of orbits of σ on Φ.

LEMMA 2.5. (1) *The map $X^*(T) \to X^*(T^\theta)$ is surjective, and the group G is adjoint. In particular, $X^*(T^\theta)$ is spanned by $\Phi(G, T^\theta)$.*

(2) *Let $\alpha, \beta \in \Phi$. Then the image of α in $X^*(T^\theta)$ is non-zero, and α, β have the same image if and only if either $\alpha = \beta$ or $\alpha = \sigma(\beta)$.*

Proof. The fixed group T^θ is connected, and contains regular elements of T; see [Ree10, Lemma 3.1]. The group G has trivial center, by [Ree10, Section 3.8]. For the second part, see [Ree10, Section 3.3]. □

We identify Φ/σ with its image in $X^*(T^\theta)$; this makes sense by Lemma 2.5. The Cartan decomposition induces a decomposition into θ-stable subspaces:

$$\mathfrak{h} = \mathfrak{t} \oplus \bigoplus_{a \in \Phi/\sigma} \mathfrak{h}_a, \tag{2.2}$$

with $\mathfrak{t} = \mathfrak{t}^\theta \oplus V_0$ and $\mathfrak{h}_a = \mathfrak{g}_a \oplus V_a$. Here, $V_0 \subset \mathfrak{t}$ is two-dimensional, and each space $\mathfrak{g}_a$, V_a is either zero or one-dimensional. There is a corresponding decomposition

$$V = V_0 \oplus \bigoplus_{a \in \Phi_V} V_a. \tag{2.3}$$

We distinguish three cases, based on the value of $s = (-1)^{\langle \alpha, \check{\rho} \rangle}$.

(1) $a = \{\alpha\}$ and $s = 1$. In this case, $V_a = 0$, and $\mathfrak{g}_a$ is spanned by X_α.

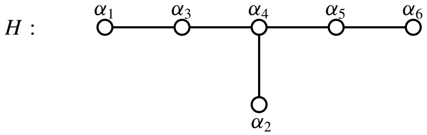
(2) $a = \{\alpha\}$ and $s = -1$. In this case, V_a is spanned by X_α, and $\mathfrak{g}_a = 0$.

(3) $a = \{\alpha, \sigma(\alpha)\}$, with $\alpha \neq \sigma(\alpha)$. In this case, V_a is spanned by $X_\alpha - s X_{\sigma(\alpha)}$, and $\mathfrak{g}_a$ is spanned by $X_\alpha + s X_{\sigma(\alpha)}$.

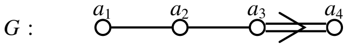
We write Φ_V for the set of elements $a \in \Phi/\sigma$ that appear as characters of T^θ in V. We write Φ_V^+ for the set of elements in Φ_V that are images of elements of

Φ^+, and define Φ_V^- similarly. Then Φ_V is the disjoint union of Φ_V^+ and Φ_V^-; we have $\#\Phi_V^+ = \#\Phi_V^- = 20$. We write $S_V \subset \Phi_V^+$ for the image of the root basis S; we have $\#S_V = \#S/\sigma = 4$.

We now introduce a root basis $S_G \subset \Phi(G, T^\theta)$. For this, it is convenient to introduce some notation. We number the simple roots $\alpha_1, \dots, \alpha_6 \in S$ as in [**Bou68**, Planche V]:



In this diagram, the pinned automorphism σ acts by reflection about the vertical axis. We define $a_1, a_2, a_3, a_4 \in X^*(T^\theta)$ to be the respective images of the roots $\alpha_3 + \alpha_4$, α_1, α_3, and $\alpha_2 + \alpha_4$. Then the set $S_G = \{a_1, \dots, a_4\} \subset \Phi(G, T^\theta)$ is a root basis for G:



We will use the decomposition $\Phi(G, T^\theta) = \Phi(G, T^\theta)^+ \cup \Phi(G, T^\theta)^-$ corresponding to this choice of root basis. Since G is adjoint, an element $b \in X^*(T^\theta)$ admits a unique decomposition $b = \sum_{i=1}^4 n_{a_i}(b)a_i$. For example, let $a_0 \in \Phi_V$ denote the image of the highest root $\alpha_0 \in \Phi^+$ of H. Then $a_0 = a_1 + 2a_2 + 3a_3 + 2a_4 = (1, 2, 3, 2)$. We define a partial order on $X^*(T^\theta)$: $a \geqslant b$ if and only if $n_{a_i}(a - b) \geqslant 0$ for each $i = 1, \dots, 4$. In Section 5 below, we have displayed a list of the elements of $\Phi_V \cup \{0\}$, along with the Hasse diagram of the induced partial order on this set. It will be helpful to note the following.

(1) We have $a_0 \geqslant a$ for all $a \in \Phi_V$.

(2) It is not true that $n_{a_i}(a) \geqslant 0$ for all $a \in \Phi_V^+$.

(3) With the numbering of Section 5, we have $\Phi_V^+ = \{1, \dots, 20\}$, and $S_V = \{17, 18, 19, 20\}$.

If $S' \subset S$ is a σ-invariant set of simple roots, then we write $\mathfrak{p}_{S'} \subset \mathfrak{h}$ for the parabolic Lie subalgebra generated by the subspaces $\mathfrak{t}$ and $\mathfrak{h}_\alpha$ ($\alpha \in \Phi^- \cup S'$). Thus $\mathfrak{p}_\emptyset$ is the unique Borel subalgebra of $\mathfrak{h}$ containing F and $\mathfrak{p}_S = \mathfrak{h}$. We write $\mathfrak{l}_{S'} \subset \mathfrak{p}_{S'}$ for the Lie subalgebra generated by the subspaces $\mathfrak{t}$ and $\mathfrak{h}_\alpha$ ($\alpha \in -S' \cup S'$). Then $\mathfrak{l}_{S'}$ is the standard Levi subalgebra of $\mathfrak{p}_{S'}$ (with respect to the maximal torus T). Each algebra $\mathfrak{l}_{S'}$ and $\mathfrak{p}_{S'}$ is θ-stable. We write $\Phi_{V,S'}^+ \subset \Phi_V^+$ for the subset of weights of T^θ which appear in $\mathfrak{p}_{S'}^{d\theta=-1}$.

The following lemma will be used later in the analysis of the irreducible elements in the cusp of a fundamental domain.

LEMMA 2.6. *Let $v \in V$, and decompose $v = v_0 + \sum_{a \in \Phi_V} v_a$ according to the Cartan decomposition* (2.3). *Suppose that one of the following holds.*

(1) *We have $v_a = 0$ if $a \in \Phi_V^+ - S_V$ and $v_a \neq 0$ if $a \in S_V$.*

(2) *There is a proper σ-invariant subset $S' \subset S$ such that $v_a = 0$ if $a \in \Phi_V^+ - \Phi_{V,S'}^+$.*

(3) *There exists $a_i \in S_G$ such that $v_a = 0$ if $n_{a_i}(a) > 0$.*

Then v is reducible.

Proof. We consider the first case. We show that v is $G(k)$-conjugate to an element of $\kappa(k)$. By hypothesis, we can write $v = \sum_{\alpha \in S} \lambda_\alpha X_\alpha + v_0 + \sum_{a \in \Phi_V^-} v_a$, for some scalars $\lambda_\alpha \in k^\times$. Since $v \in V$, we have $\lambda_{\sigma(\alpha)} = \lambda_\alpha$ for each $\alpha \in S$. Since the group H is adjoint, we can find $t \in T(k)$ such that $\alpha(t) = \lambda_\alpha^{-1}$ for each $\alpha \in S$; it is clear that we then have $t \in T^\theta(k)$.

Replacing v by $t \cdot v$, we can thus assume that $v = \sum_{\alpha \in S} X_\alpha + v_0 + \sum_{a \in \Phi_V^-} v_a$. A standard result in the theory of the Kostant section (see [Kot99, Section 2.4]) says that the natural product morphism induces an isomorphism $U \times \kappa \cong E + \mathfrak{p}_\emptyset$, where U is the unipotent radical of Borel subgroup of H with Lie algebra $\mathfrak{p}_\emptyset$. Taking θ-invariants, we obtain an isomorphism $U^\theta \times \kappa \cong E + \mathfrak{p}_\emptyset^{d\theta=-1}$. Consequently, $v \in E + \mathfrak{p}_\emptyset^{d\theta=-1}$ is $U^\theta(k)$-conjugate to an element of $\kappa(k)$.

We now consider the second case, which is equivalent to asking that $v \in \mathfrak{p}_{S'}^{d\theta=-1}$. We will show that in this case $\Delta(v) = 0$. Suppose for contradiction that $\Delta(v) \neq 0$. Then the Lie centralizer $\mathfrak{z}_\mathfrak{h}(v)$ is a Cartan subspace of V, which is contained in a unique Levi subalgebra $\mathfrak{l}'_{S'} \subset \mathfrak{p}_{S'}$, which is necessarily θ-stable. The canonical projection $\mathfrak{l}'_{S'} \to \mathfrak{l}_{S'}$ is θ-equivariant, and we deduce that θ acts as -1 on the center of $\mathfrak{l}_{S'}$ (as the center of $\mathfrak{l}'_{S'}$ is contained in $\mathfrak{z}_\mathfrak{h}(v)$).

However, this contradicts the fact that the center of $\mathfrak{l}_{S'}$ is spanned by the elements $d\check{\omega}_\alpha(1)$ ($\alpha \in S - S'$), where the $\check{\omega}_\alpha \in X_*(T)$ ($\alpha \in S$) are the fundamental coweights. Indeed, the involution θ permutes the elements $\check{\omega}_\alpha$ among themselves; so as long as $S \neq S'$, there must exist at least a one-dimensional subspace of the center of $\mathfrak{l}_{S'}$ which is fixed pointwise by θ.

We now consider the third case. We will again show that $\Delta(v) = 0$, first under the additional hypothesis that $v_a = 0$ if $n_{a_i}(a) \neq 0$. Then v is fixed by a non-trivial subtorus of T^θ, namely $A_i = \bigcap_{j \neq i} \ker a_j$. In particular, v cannot be regular, as regular elements of V have finite stabilizer in G. Now suppose that $v \in V$ satisfies instead the condition $v_a = 0$ if $n_{a_i}(a) > 0$, as in the statement of the lemma. We suppose for contradiction that v is irreducible; then $\Delta(v) \neq 0$, and v is regular semi-simple. In particular, the G-conjugacy class of v in V is closed. However, the closure of the orbit $A_i \cdot v$ contains an element w

satisfying $w_a = 0$ if $n_{a_i}(a) \neq 0$. In particular, w cannot be regular semi-simple. This contradiction concludes the proof. □

2.4. Integral structures. We now assume that $k = \mathbb{Q}$, and introduce integral structures on G and V. The torus $T^\theta \subset G$ is split maximal, and induces the Cartan decomposition $\mathfrak{g} = \mathfrak{t}^\theta \oplus \bigoplus_{a \in \Phi(G, T^\theta)} \mathfrak{g}_a$. We choose a Chevalley basis with respect to this decomposition. This means (see [Bor70]) a choice of vector $x_a \in \mathfrak{g}_a$ for each $a \in \Phi(G, T^\theta)$ satisfying the following conditions.

(1) Let $h_a = [x_a, x_{-a}]$. Then $[h_a, x_b] = \langle a^\vee, b \rangle$.

(2) If $a, b, a + b \in \Phi(G, T^\theta)$, then $[x_a, x_b] = \pm(p_{a,b} + 1)x_{a+b}$, where $p_{a,b}$ is the greatest integer such that $a - p_{a,b}b$ is a root.

The elements h_a and x_a give a basis for a $\mathbb{Z}$-form $\mathfrak{g}_\mathbb{Z} \subset \mathfrak{g}$. Moreover, the notion of admissible $\mathbb{Z}$-form of V is defined [Bor70, Section 2]; we choose an admissible $\mathbb{Z}$-form $\mathcal{V} \subset V$ which contains the nilpotent elements $E, e \in V$ fixed above. An integral model of the group G can be obtained by taking the Zariski closure of G inside $\mathrm{GL}(\mathcal{V})$; we will abuse notation slightly by now writing G for this choice of integral model. With these choices, the Cartan decomposition $V = V_0 \oplus \bigoplus_{a \in \Phi_V} V_a$ is defined over $\mathbb{Z}$ [Bor70, Lemma 2.3]; in particular, if $v \in \mathcal{V}(\mathbb{Z})$ is written as $v = v_0 + \sum_{a \in \Phi_V} v_a$, then we have $v_0, v_a \in \mathcal{V}(\mathbb{Z})$. We scale the discriminant Δ so that $\Delta \in \mathbb{Z}[\mathcal{V}]$.

Let $K \subset G(\mathbb{R})$ be a maximal compact subgroup. Let $P = T^\theta N \subset G$ denote the Borel subgroup containing T^θ and corresponding to the root basis S_G, and let $\overline{P} = T^\theta \overline{N} \subset G$ denote the opposite Borel subgroup. A Siegel set is, by definition, any subset $\mathfrak{S} \subset G(\mathbb{R})$ of the form $\mathfrak{S} = \omega \cdot T_c \cdot K$, where $\omega \subset \overline{N}(\mathbb{R})$ is a compact subset and $T_c = \{t \in T^\theta(\mathbb{R})^0 \mid \forall a \in S_G,\ a(t) \leqslant c\}$. Since G is a Chevalley group, we have access to the following result.

THEOREM 2.7. (1) *$G(\mathbb{Z})$ has a unique cusp: we can choose $\omega \subset \overline{N}(\mathbb{R})$, $c > 0$ so that $G(\mathbb{Z}) \cdot \mathfrak{S} = G(\mathbb{R})$.*

(2) *$G(\mathbb{Z})$ has class number 1: we have $G(\mathbb{A}^\infty) = G(\mathbb{Q}) \cdot G(\widehat{\mathbb{Z}})$. (Here, $\mathbb{A}^\infty = \prod'_p \mathbb{Q}_p$ denotes the ring of finite adeles of $\mathbb{Q}$.)*

Proof. For the first point, see [Bor66, Section 6, Lemma 1] and [PR94, Theorem 4.15]. For the second, see [PR94, Theorem 8.11, Corollary 2]. □

In what follows, we will fix a choice of ω and c so that the condition $G(\mathbb{Z}) \cdot \mathfrak{S} = G(\mathbb{R})$ holds. We now choose less canonical integral structures for X, Y, and B. A choice of invariant polynomials $p_2, \ldots, p_{12} \in \mathbb{Q}[V]^G$ has been fixed in Theorem 2.4; after rescaling $p_2, \dots, p_{12}$ and the coordinates x, y on X, we can assume that $p_2, \dots, p_{12}$ lie in $\mathbb{Z}[\mathcal{V}]$. We define $\mathcal{B} = \operatorname{Spec} \mathbb{Z}[p_2, \dots, p_{12}]$, and write $\pi : \mathcal{V} \to \mathcal{B}$ for the induced morphism; the fiber over $\mathbb{Q}$ recovers the categorical quotient $V \to B = V /\!\!/ G$.

We define $\mathcal{X} = \operatorname{Spec} \mathbb{Z}[x, y, p_2, \dots, p_{12}]$; then $\mathcal{X}$ is isomorphic to $\mathbb{A}^7_{\mathbb{Z}}$, and the morphism $X \to B$ extends to a morphism $\mathcal{X} \to \mathcal{B}$. We write $\mathcal{Y}$ for the natural compactification of $\mathcal{X}$ as a closed subscheme of $\mathbb{P}^2_{\mathcal{B}}$. We have the following elementary fact, which we record as a lemma for later reference. (The $\mathbb{G}_m$-actions on κ and X here are the actions coming from the fixed $\mathfrak{sl}_2$-triples, as at the beginning of Section 2.2. The $\mathbb{G}_m$-action on B is the one arising from the inclusion $\mathbb{Q}[B] = \mathbb{Q}[V]^G \subset \mathbb{Q}[V]$.)

LEMMA 2.8. *Let p be a prime. There exists an integer $N_0 \geqslant 1$, not depending on p, such that, for any $b \in \mathcal{B}(\mathbb{Z}_p)$ (respectively, $v \in \mathcal{X}(\mathbb{Z}_p)$), we have $N_0 \cdot \kappa_b \in \mathcal{V}(\mathbb{Z}_p)$ (respectively, $N_0 \cdot v \in \mathcal{V}(\mathbb{Z}_p)$). In particular, if $b \in N_0^2 \cdot \mathcal{B}(\mathbb{Z})$, then $b \in \pi(\mathcal{V}(\mathbb{Z}))$.*

We conclude this section with a fact about integral orbits.

THEOREM 2.9. *Let $b \in \mathcal{B}(\mathbb{Z})$ satisfy $\Delta(b) \neq 0$. Then $\mathcal{V}_b(\mathbb{Z})$ consists of only finitely many $G(\mathbb{Z})$-orbits.*

Proof. This follows from [**BHC62**, Theorem 6.9]. □

2.5. Integral orbits and algebraic curves.

Let $b \in \mathcal{B}(\mathbb{Z})$ be such that $\Delta(b) \neq 0$. According to Theorem 2.4, we have a canonical inclusion $G(\mathbb{Q})\backslash V_b(\mathbb{Q}) \subset H^1(\mathbb{Q}, J_b[2])$. We write $\mathcal{O}_b \subset H^1(\mathbb{Q}, J_b[2])$ for the image of $\mathcal{V}_b(\mathbb{Z})$. In this section, we prove the following result.

THEOREM 2.10. *There exists an integer $N_3 \geqslant 1$ such that, if $b \in N_3 \cdot \mathcal{B}(\mathbb{Z})$, then $\mathcal{O}_b$ contains the subset* $\operatorname{Sel}_2(Y_b) \subset H^1(\mathbb{Q}, J_b[2])$.

To prove the theorem, it suffices to prove the corresponding local statement. Let p be a prime, and let $b \in \mathcal{B}(\mathbb{Z}_p)$ be a point such that $\Delta(b) \neq 0$. Let $\mathcal{O}_{b,p} \subset H^1(\mathbb{Q}_p, J_b[2])$ denote the image of $\mathcal{V}_b(\mathbb{Z}_p)$.

LEMMA 2.11. *There exists an integer $N_3 \geqslant 1$, not depending on p, such that, if $b \in N_3 \cdot \mathcal{B}(\mathbb{Z}_p)$, then $\mathcal{O}_{b,p}$ contains the image of $Y_b(\mathbb{Q}_p)$ in $H^1(\mathbb{Q}_p, J_b[2])$ under the Abel–Jacobi map.*

We first explain how Lemma 2.11 implies Theorem 2.10. Let $c \in H^1(\mathbb{Q}, J_b[2])$ be a class corresponding to an element of $\mathrm{Sel}_2(Y_b)$. We claim that c corresponds to an element of $G(\mathbb{Q})\backslash V_b(\mathbb{Q})$; equivalently, that c lies in the kernel of the natural map $H^1(\mathbb{Q}, J_b[2]) \to H^1(\mathbb{Q}, G)$. The map $H^1(\mathbb{Q}, G) \to \prod_v H^1(\mathbb{Q}_v, G)$ is injective. Indeed, there is a short exact sequence with G' the universal cover of G:

$$\begin{tikzcd} 1 \arrow[r] & \mu_2 \arrow[r] & G' \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

and hence a commutative diagram

$$\begin{tikzcd} H^1(\mathbb{Q}, G) \arrow[r] \arrow[d] & H^2(\mathbb{Q}, \mu_2) \arrow[d] \\ \prod_v H^1(\mathbb{Q}_v, G) \arrow[r] & \prod_v H^2(\mathbb{Q}_v, \mu_2) \end{tikzcd}$$

The horizontal arrows are injective (because the cohomology of G' is trivial), and the right-hand arrow is injective (by class field theory). It follows that the left-hand arrow is injective. It therefore suffices to show that, for every place v of $\mathbb{Q}$, the image $c_v \in H^1(\mathbb{Q}_v, J_b[2])$ of c has trivial image in $H^1(\mathbb{Q}_v, G)$. However, c_v lies, by hypothesis, in the image of the natural map $Y_b(\mathbb{Q}_v) \to H^1(\mathbb{Q}_v, J_b[2])$. It follows from Theorem 2.4 that c_v corresponds to an element of $G(\mathbb{Q}_v)\backslash V_b(\mathbb{Q}_v)$; this establishes the claim.

Let us now take again $b \in N_3 \cdot \mathcal{B}(\mathbb{Z})$ such that $\Delta(b) \neq 0$, with $N_3 \geqslant 1$ as in the lemma. Take a vector $v \in V_b(\mathbb{Q})$ whose image in $H^1(\mathbb{Q}, J_b[2])$ lies in $\mathrm{Sel}_2(Y_b)$. By Lemma 2.11, $G(\mathbb{Q}_p) \cdot v$ contains an element of $\mathcal{V}_b(\mathbb{Z}_p)$; thus, there exists $g_p \in G(\mathbb{Q}_p)$ such that $g_p \cdot v \in \mathcal{V}_b(\mathbb{Z}_p)$. By Theorem 2.7, we can find $g \in G(\mathbb{Q})$ such that $gg_p^{-1} \in G(\mathbb{Z}_p)$ for every prime p. It follows that $g \cdot v \in \mathcal{V}(\mathbb{Z}_p)$ for every prime p, and hence $g \cdot v \in \mathcal{V}(\mathbb{Z})$, as desired.

Proof of Lemma 2.11. Let $c \in \mathcal{B}(\mathbb{Z}_p)$. We claim that, if $c \in 2^4 \cdot \mathcal{B}(\mathbb{Z}_p)$ (which is no condition if $p \neq 2$ – by definition, $2^4 \cdot \mathcal{B}(\mathbb{Z}_p)$ denotes the set of points $b \in \mathcal{B}(\mathbb{Z}_p)$ such that $p_i(b)$ is divisible by 2^{4i} in $\mathbb{Z}_p$), then every element of the image of $Y_c(\mathbb{Q}_p) \to J_c(\mathbb{Q}_p)/2J_c(\mathbb{Q}_p)$ is represented either by P_∞ or an element of $\mathcal{X}_c(\mathbb{Z}_p)$. Indeed, this follows from the following observations.

- Let $c = 2^4 \cdot b$, $b \in \mathcal{B}(\mathbb{Z}_p)$. Let $P \in \mathcal{Y}_b(\mathbb{Z}_p)$, and suppose that the image of P under the natural identification $Y_b(\mathbb{Q}_p) = Y_c(\mathbb{Q}_p)$ is not contained in the subset $\mathcal{X}_c(\mathbb{Z}_p) \subset \mathcal{Y}_c(\mathbb{Z}_p)$. Then P and P_∞ have the same image in $\mathcal{Y}_b(\mathbb{Z}_p/2^4 p\mathbb{Z}_p)$.

- Let $F \in \mathbb{Z}_p[\![X_1, \ldots, X_g, Y_1, \ldots, Y_g]\!]$ be a g-dimensional formal group law (for some $g \geqslant 1$). If $x \in \ker(F(p\mathbb{Z}_p) \to F(p\mathbb{Z}_p/2^4 p\mathbb{Z}_p))$, then x is 2-divisible in $F(p\mathbb{Z}_p)$ (as follows from [CX08, Proposition 9]).

- Let $b \in \mathcal{B}(\mathbb{Z}_p)$ be such that $\Delta(b) \neq 0$, and let $\mathcal{J}_b$ denote the identity component of $\mathrm{Pic}_{\mathcal{Y}_b/\mathbb{Z}_p}$, a smooth quasi-projective scheme over $\mathbb{Z}_p$ (see [BLR90, Section 9.3, Theorem 1]; we use here that the special fiber of $\mathcal{Y}_b$ is geometrically irreducible). Let F now denote the g-dimensional formal group law which is the completion of $\mathcal{J}_b$ along its identity section. If $P \in \mathcal{Y}_b(\mathbb{Z}_p)$ has the same image in $\mathcal{Y}_b(\mathbb{Z}_p/2^4 p\mathbb{Z}_p)$ as the point P_∞ at infinity, then the Cartier divisor $(P) - (P_\infty) \in \mathcal{J}_b(\mathbb{Z}_p)$ lies in the subgroup

$$\ker(F(p\mathbb{Z}_p) \to F(p\mathbb{Z}_p/2^4 p\mathbb{Z}_p)) \subset F(p\mathbb{Z}_p) = \ker(\mathcal{J}_b(\mathbb{Z}_p) \to \mathcal{J}_b(\mathbb{F}_p)).$$

Let $N_0 \geqslant 1$ be the integer of Lemma 2.8, let $N_3 = 2^4 N_0^2$, and assume now that $b = N_0^2 \cdot c$, $c \in 2^4\mathcal{B}(\mathbb{Z}_p)$. We then have a commutative diagram:

$$\begin{tikzcd}
X_b(\mathbb{Q}_p) \arrow[r] \arrow[d, "N_0^{-1}"] & G(\mathbb{Q}_p)\backslash V_b(\mathbb{Q}_p) \arrow[r] \arrow[d, "N_0^{-2}"] & H^1(\mathbb{Q}_p, J_b[2]) \arrow[d, "N_0^{-2}"] \\
X_c(\mathbb{Q}_p) \arrow[r] & G(\mathbb{Q}_p)\backslash V_c(\mathbb{Q}_p) \arrow[r] & H^1(\mathbb{Q}_p, J_c[2])
\end{tikzcd}$$

The vertical arrows are bijective. The composites of the horizontal arrows agree with the composites of the descent and Abel–Jacobi maps, by Theorem 2.4.

Suppose that $v \in V_b(\mathbb{Q}_p)$, and let $v' = N_0^{-2}v$. If v has the same image in $H^1(\mathbb{Q}_p, J_b[2])$ as P_∞ (that is, if this image is trivial), then the $G(\mathbb{Q}_p)$-orbit of v' contains κ_c, so, by Lemma 2.8, $\kappa_b = N_0 \cdot \kappa_c \in \mathcal{V}(\mathbb{Z}_p)$. If the image of v in $H^1(\mathbb{Q}_p, J_b[2])$ is non-trivial but still comes from $Y_b(\mathbb{Q}_p)$, then the $G(\mathbb{Q}_p)$-orbit of v' contains an element in the image of $\mathcal{X}_c(\mathbb{Z}_p)$, and so the $G(\mathbb{Q}_p)$-orbit of v contains an element in the image of $N_0 \cdot \mathcal{X}_c(\mathbb{Z}_p) \subset \mathcal{X}_b(\mathbb{Z}_p)$; applying Lemma 2.8 once more, we see that $N_0 \cdot \mathcal{X}_c(\mathbb{Z}_p) \subset \mathcal{V}_b(\mathbb{Z}_p)$. This concludes the proof. □

2.6. Height.

If $b \in B(\mathbb{R})$, we define its height as follows:

$$H(b) = \sup_i |p_i(v)|^{\deg(\Delta)/i}.$$

If $v \in V(\mathbb{R})$, we define $H(v) = H(\pi(v))$. By construction, $H(v)$ is homogeneous of degree $\deg \Delta = 72$; if $\lambda \in \mathbb{R}^\times$, then $H(\lambda v) = |\lambda|^{72} H(v)$. We note that this very much depends on the choice of polynomials p_i.

2.7. Measures on G.

Let $K \subset G(\mathbb{R})$ and $\overline{P} \subset G$ denote respectively the maximal compact subgroup and Borel subgroup fixed in Section 2.4. According to the theory of the Iwasawa decomposition, the natural product maps

$$\overline{N}(\mathbb{R}) \times T^\theta(\mathbb{R})^0 \times K \to G(\mathbb{R}), \quad T^\theta(\mathbb{R})^0 \times \overline{N}(\mathbb{R}) \times K \to G(\mathbb{R})$$

are diffeomorphisms. If $t \in T^{\theta}(\mathbb{R})$, let $\delta(t) = \prod_{a \in \Phi(G,T^{\theta})^-} a(t) = \det \mathrm{Ad}(t)|_{\mathrm{Lie}\,\overline{N}(\mathbb{R})}$.

Lemma 2.12. *A Haar measure on $G(\mathbb{R})$ is $dg = dt\,dn\,dk = \delta(t)^{-1} dn\,dt\,dk$. More precisely, let dt, dn, dk be Haar measures on the groups $T^{\theta}(\mathbb{R})$, $\overline{N}(\mathbb{R})$, and K, respectively. Then the integral*

$$\int_{g \in G(\mathbb{R})} f(g)\,dg = \int_{t \in T^{\theta}(\mathbb{R})^{\circ}} \int_{n \in \overline{N}(\mathbb{R})} \int_{k \in K} f(tnk)\,dt\,dn\,dk$$
$$= \int_{n \in \overline{N}(\mathbb{R})} \int_{t \in T^{\theta}(\mathbb{R})^{\circ}} \int_{k \in K} f(ntk)\delta(t)^{-1}\,dn\,dt\,dk$$

defines a Haar integral on $G(\mathbb{R})$.

Proof. This follows from well-known properties of the Iwasawa decomposition; see, for example, [Lan75, Ch. III, Section 1]. □

We now fix for the rest of this paper a left-invariant top form ω_G on G. If v is a place of $\mathbb{Q}$, then we define a Haar integral on $G(\mathbb{Q}_v)$ using the volume element $dg = |\omega_G|_v$, where $|\cdot|_v$ is the usual absolute value if $v = \infty$ and $|p|_v = p^{-1}$ if $v = p$. We use the volume element $|\omega_G|_\infty$ to fix Haar measures on the groups $T^{\theta}(\mathbb{R})^0$, K, and $\overline{N}(\mathbb{R})$, as follows. We give $T^{\theta}(\mathbb{R})^0$ the measure pulled back from the isomorphism $\prod_{a \in S_G} a : T^{\theta}(\mathbb{R})^0 \cong \mathbb{R}^4_{>0}$; $\mathbb{R}_{>0}$ gets its standard Haar measure $d^{\times}\lambda = d\lambda/\lambda$, where $d\lambda$ is the usual Lebesgue measure. We give K its probability Haar measure. There is now a unique choice of Haar measure dn on $\overline{N}(\mathbb{R})$ such that $|\omega_G|_\infty = dt\,dn\,dk$; we make this choice.

2.8. Measures on V and B.

We fix a differential top form ω_V on V induced by the integral structure on $\mathcal{V}$; it is determined up to sign. If v is a place of $\mathbb{Q}$, then the volume element $dv = |\omega_V|_v$ determines a Haar measure on $V(\mathbb{Q}_v)$. With this choice, the spaces $\mathcal{V}(\mathbb{Z}_p)$ (p a prime) and $\mathcal{V}(\mathbb{Z})\backslash V(\mathbb{R})$ have volume 1. We write $\omega_B = dp_2 \wedge \cdots \wedge dp_{12}$, and ω_κ for the pullback of this form under the canonical isomorphism $\kappa \to B$. Again, if v is a place of $\mathbb{Q}$, then the volume element $db = |\omega_B|_v$ determines a measure on $B(\mathbb{Q}_v)$. If p is a prime, then $\mathcal{B}(\mathbb{Z}_p)$ has volume 1; if $X > 1$ is a real number, then the set $\{b \in B(\mathbb{R}) \mid 1 \leqslant H(b) \leqslant X\}$ has volume $X^{\sum_i i/72} = X^{7/12}$.

Proposition 2.13. (1) *Let $\mu_\kappa : G \times \kappa \to V$ denote the product map. Then there exists $W_0 \in \mathbb{Q}^{\times}$ such that $\mu_\kappa^* \omega_V = W_0 \cdot \omega_G \wedge \omega_\kappa$.*

(2) *Let $\mathfrak{c} \subset V$ be a Cartan subspace, and let $\mu_{\mathfrak{c}} : G \times \mathfrak{c} \to V$ denote the product map. Then there exists $W_1 \in \mathbb{Q}^\times$, not depending on the choice of $\mathfrak{c}$, such that $\mu_{\mathfrak{c}}^* \omega_V = W_1 \cdot \omega_G \wedge \pi|_{\mathfrak{c}}^* \omega_B$.*

Proof. (1) The morphism μ_κ is étale. It follows that there exists a non-vanishing regular function $f \in \mathbb{Q}[G \times \kappa]$ such that $\mu_\kappa^* \omega_V = f \omega_G \wedge \omega_\kappa$. The form ω_V is G-invariant, so the function f must be pulled back from $\mathbb{Q}[\kappa]$. Since κ is abstractly isomorphic to affine space, the only non-vanishing regular functions are the constants.

(2) Let $\omega_{\mathfrak{c}}$ be an invariant differential top form (with respect to the vector space structure on $\mathfrak{c}$). Again, we can write $\mu_{\mathfrak{c}}^* \omega_V = f_1 \omega_G \wedge \omega_{\mathfrak{c}}$ for some function $f_1 \in \mathbb{Q}[G \times \mathfrak{c}]^G = \mathbb{Q}[\mathfrak{c}]$. We write $\pi|_{\mathfrak{c}}^* \omega_B = f_2 \omega_{\mathfrak{c}}$ for some function $f_2 \in \mathbb{Q}[\mathfrak{c}]$. We must show that f_1 and f_2 are equal, up to scalar.

We define a new action of $G \times \mathbb{G}_m$ on $G \times \mathfrak{c}$ by $(g, \lambda) \cdot (h, x) = (gh, \lambda x)$. Then $(g, \lambda)^* f_1 = \lambda^{\dim V - \dim \mathfrak{c}} f_1$; in particular, f_1 is homogeneous of degree $\dim V - \dim \mathfrak{c}$. On the other hand, the function f_2 is homogeneous of degree $\sum_i (d_i - 1)$. We now use the string of equalities:

$$\# \Phi = \deg \Delta = 2 \sum_i (d_i - 1) = 2(\dim V - \dim \mathfrak{c}).$$

It is easily seen that f_1 and f_2 vanish along the same set; moreover, f_2 vanishes to order 1 along each root hyperplane, and nowhere else. As the functions f_1 and f_2 are homogeneous of the same degree, they must be equal up to scalar. The result follows. □

2.9. Constructing special sections over $\mathbb{R}$. The space $V(\mathbb{R})$ contains finitely many $G(\mathbb{R})$-conjugacy classes of Cartan subalgebras; let $\mathfrak{c}_1 \ldots, \mathfrak{c}_n$ be representatives. For each $i = 1, \ldots, n$, the natural map $\pi|_{\mathfrak{c}_i^{\text{reg. ss}}} : \mathfrak{c}_i^{\text{reg. ss}} \to B(\mathbb{R})^{\text{reg. ss}}$ is a proper local homeomorphism. Consequently, there exists (see [BCR98, Proposition 9.3.9]) a finite cover U_{ij} of $\mathfrak{c}_i^{\text{reg. ss}}$ by open semi-algebraic subsets such that each $\pi|_{U_{ij}}$ is a homeomorphism. Since a semi-algebraic set has finitely many connected components [BCR98, Theorem 2.4.4], we can suppose moreover that each U_{ij} is connected.

Let $L_1, \ldots, L_r$ denote the sets $\pi(\{v \in U_{ij} \mid H(v) = 1\})$, in any order, and let $s_i : L_i \to V(\mathbb{R})$ denote the corresponding sections. Then $L_i \subset \{b \in B(\mathbb{R}) \mid \Delta(b) \neq 0, H(b) = 1\}$ is a connected semi-algebraic open subset, and $s_i : L_i \to V(\mathbb{R})$ is a semi-algebraic map. We have an equality ($\Lambda = \mathbb{R}_{>0}$):

$$V(\mathbb{R})^{\text{reg. ss}} = \bigcup_i G(\mathbb{R}) \cdot \Lambda \cdot s_i(L_i).$$

This union need not be disjoint, but this is not a problem for us. If $v \in s_i(L_i)$, let $n_i = \# \mathrm{Stab}_{G(\mathbb{R})}(v)$; this integer is independent of the choice of v.

PROPOSITION 2.14. *Let $f : V(\mathbb{R}) \to \mathbb{C}$ be a continuous function of compact support. Then, for any $i = 1, \ldots, r$ we have*

$$\int_{v \in G(\mathbb{R}) \cdot \Lambda \cdot s_i(L_i)} f(v)\, dv = \frac{|W_1|_\infty}{n_i} \int_{b \in \Lambda \cdot L_i} \int_{g \in G(\mathbb{R})} f(g \cdot s_i(b))\, dg\, db,$$

where $W_1 \in \mathbb{Q}^\times$ is the scalar of Proposition 2.13. Consequently, we have

$$\mathrm{vol}(\mathfrak{S} \cdot [1, X^{1/72}] \cdot s_i(L_i)) \leqslant |W_1|_\infty \mathrm{vol}(\mathfrak{S}) \cdot \mathrm{vol}([1, X^{1/72}] \cdot L_i).$$

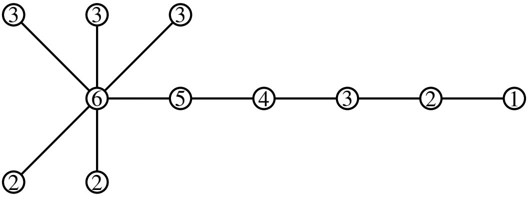
Proof. Let $\mathfrak{c} \subset V(\mathbb{R})$ be the Cartan subspace corresponding to L_i. Let us write $\mu_i : G(\mathbb{R}) \times (\Lambda \cdot L_i) \to V(\mathbb{R})$ for the morphism $(g, \lambda \cdot l) \mapsto g \cdot \lambda s_i(l)$. It follows from Proposition 2.13 that $\mu_i^* \omega_V = W_1 \omega_G \wedge \omega_B$. The displayed formula now follows from the fact that μ_i is a proper local diffeomorphism onto its image, with fibers of cardinality n_i. □

2.10. Constructing special sections over $\mathbb{Q}_p$. In this section, we construct the congruence conditions that will be used to prove Theorem 1.2.

PROPOSITION 2.15. *Let p be a prime congruent to 1 modulo 6. There exists an open compact subset $B_p \subset \mathcal{B}(\mathbb{Z}_p)$ such that, for all $b \in B_p$, we have $J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p) \cong (\mathbb{Z}/2\mathbb{Z})^2$, the map $Y_b(\mathbb{Q}_p) \to J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p)$ has image reduced to the identity, and $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$.*

Proof. We verify by explicit calculation that the curve $y^3 = x^4 - p^2$ satisfies the conditions of the proposition. In fact, we show that the special fiber of the minimal regular model contains a unique component of multiplicity 1, and the special fiber of the Néron model has component group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, and purely unipotent connected component. In order to do this, we use the quotient method of Lorenzini [LT02, Section 2]. Let ϖ be a sixth root of p, and let $K = \mathbb{Q}_p(\varpi)$. The extension $K/\mathbb{Q}_p$ is Galois, since 6 divides $p-1$. Let Y denote the projective closure of $y^3 = x^4 - p^2$ in $\mathbb{P}^2_{\mathbb{Q}_p}$. The curve Y_K is isomorphic to the curve $Z \subset \mathbb{P}^2_K$, projective closure of the equation $Y^3 = X^4 - 1$, via the substitutions $x = \varpi^3 X$, $y = \varpi^4 Y$.

Let $\mathcal{O}_K \subset K$ denote the ring of integers, and let $\mathcal{Z} \subset \mathbb{P}^2_{\mathcal{O}_K}$ denote the projective closure of the affine curve cut out by the same equation as Z. Then $\mathcal{Z}$ is a smooth projective curve over $\mathcal{O}_K$ with generic fiber Z. In particular, $\mathcal{Z}$ is regular. The group $G = \mathrm{Gal}(K/\mathbb{Q}_p)$ acts on $\mathcal{Z}$ in a manner covering its action on $\mathcal{O}_K$, and we write $\mathcal{Y}$ for the quotient $\mathcal{Z}/G$. Then $\mathcal{Y}$ is normal; it is regular outside of the points in the special fiber which are the images of the fixed points of the action of G on $\mathcal{Z}_{\mathcal{O}_K/(\varpi)}$. At such points, it has quotient singularities. Resolving these quotient singularities as in [LT02, Section 2.15] gives a regular model $\mathcal{Y}'$ of Y. The intersection graph of the special fiber of $\mathcal{Y}'$ is as follows:



Here, the vertices correspond to the reduced irreducible components of the special fiber of $\mathcal{Y}'$; two vertices are connected by an edge if the corresponding components intersect. (It turns out that, for this curve, the non-zero intersection multiplicities are all equal to one.) Each vertex is labeled with the multiplicity of the corresponding component in the special fiber of $\mathcal{Y}'$. The desired properties now follow from the description of the component group of the Néron model recalled, for example, in [Lor00, Introduction]. To see that our curve has $\mathbb{Z}_p$-points, we observe that there are solutions with $x = 1$ (since $1 - p^2$ is a cube in $\mathbb{Z}_p^\times$).

Let $b_0 \in \mathcal{B}(\mathbb{Z}_p)$ be the point corresponding to the equation $y^3 = x^4 - p^2$. It is now easy to see that any sufficiently small open compact neighborhood $B_p \subset \mathcal{B}(\mathbb{Z}_p)$ of b_0 will have the desired properties. □

PROPOSITION 2.16. *Let $U \subset \mathcal{B}(\mathbb{Z}_p)$ be an open compact subset such that, for all $b \in U$, $\Delta(b) \neq 0$. Let $V_p = (G(\mathbb{Q}_p) \cdot \kappa(\mathbb{Q}_p)) \cap \mathcal{V}(\mathbb{Z}_p) \cap \pi^{-1}(U)$. Then, after possibly shrinking U, the following statements hold.*

(1) *The set $\{g \in G(\mathbb{Q}_p) \mid g\kappa_b \in \mathcal{V}(\mathbb{Z}_p)\}$ is independent of $b \in U$. We write $g_1, \ldots, g_r$ for representatives of the $G(\mathbb{Z}_p)$-$\mathrm{Stab}_{G(\mathbb{Q}_p)}(\kappa_b)$-double cosets in this set.*

(2) *The quantities $\#\mathrm{Stab}_{G(\mathbb{Q}_p)}(\kappa_b)$ and $\#\mathrm{Stab}_{G(\mathbb{Z}_p)}(g_i\kappa_b)$ are independent of $b \in U$.*

(3) *$V_p \subset \mathcal{V}(\mathbb{Z}_p)$ is open compact.*

Moreover, the constant $W_0 \in \mathbb{Q}^\times$ being as in Proposition 2.13, we have

$$\mathrm{vol}(V_p) = |W_0|_p \,\mathrm{vol}(G(\mathbb{Z}_p))\,\mathrm{vol}(U) \sum_{i=1}^{r} \frac{1}{\#\mathrm{Stab}_{G(\mathbb{Z}_p)}(g_i\kappa_b)},$$

for any $b \in U$.

Proof. In order to simplify the notation, let us use the subscript $(\cdot)_U$ to denote intersection with $\pi^{-1}(U)$. The orbit map $\mu_U : G(\mathbb{Q}_p) \times \kappa(\mathbb{Q}_p)_U \to V(\mathbb{Q}_p)_U$ is finite and a local analytic isomorphism. If $b \in U$, let $G(\mathbb{Q}_p)^b = \{g \in G(\mathbb{Q}_p) \mid g\kappa_b \in \mathcal{V}(\mathbb{Z}_p)\} = \mu_U^{-1}(\mathcal{V}(\mathbb{Z}_p)_U) \cap \mathrm{pr}_2^{-1}(b)$. Choose $b_0 \in U$. It is easy to see that the set $\{b \in U \mid G(\mathbb{Q}_p)^b = G(\mathbb{Q}_p)^{b_0}\}$ is open, so, after replacing U by an open compact neighborhood of b_0, we can assume that $G(\mathbb{Q}_p)^b = G(\mathbb{Q}_p)^{b_0}$ for all $b \in U$.

Let $p : Z \to \kappa^{\text{reg. ss}}$ denote the stabilizer scheme; it is a finite étale group scheme. Let $y_1, \ldots, y_s$ be the distinct elements of $p^{-1}(b_0)$ in $Z(\mathbb{Q}_p)$. After possibly shrinking U further, we can find disjoint open neighborhoods $V_1, \ldots, V_s$ of $y_1, \ldots, y_s$ in $Z(\mathbb{Q}_p)$ such that each restriction $p|_{V_i} : V_i \to U$ is an analytic isomorphism, and $p^{-1}(U) = V_1 \cup \cdots \cup V_s$. In particular, $\#\,\mathrm{Stab}_{G(\mathbb{Q}_p)}(\kappa_b)$ is independent of $b \in U$.

We now show that we can choose U so that the quantity

$$\#\,\mathrm{Stab}_{G(\mathbb{Z}_p)}(g_i\kappa_b) = \#(p^{-1}(b)(\mathbb{Q}_p) \cap g_i^{-1}G(\mathbb{Z}_p)g_i)$$

is independent of $b \in U$. Since the group $g_i^{-1}G(\mathbb{Z}_p)g_i \subset G(\mathbb{Q}_p)$ is open compact, we can assume, after possibly shrinking U, that, for each $j = 1, \ldots, s$, either $V_j \subset g_i^{-1}G(\mathbb{Z}_p)g_i$ or $V_j \cap g_i^{-1}G(\mathbb{Z}_p)g_i = \emptyset$. This implies the desired property. We can write $V_p = \bigcup_{i=1}^r G(\mathbb{Z}_p)\cdot g_i \cdot \kappa(\mathbb{Q}_p)_U$. In particular, V_p is an open compact subset of $\mathcal{V}(\mathbb{Z}_p)$ and satisfies points 1–3 above.

It remains to calculate the volume of V_p. Proposition 2.13 implies the formula

$$\begin{aligned}\mathrm{vol}(V_p) &= \sum_{i=1}^r |W_0|_p \int_{b\in U}\int_{g\in G(\mathbb{Z}_p)} \frac{1}{\#\,\mathrm{Stab}_{G(\mathbb{Z}_p)}(g_i\kappa_b)}\,dg\,db \\ &= |W_0|_p\,\mathrm{vol}(G(\mathbb{Z}_p))\,\mathrm{vol}(U)\sum_{i=1}^r \frac{1}{\#\,\mathrm{Stab}_{G(\mathbb{Z}_p)}(g_i\kappa_b)},\end{aligned}$$

as desired. □

If $v \in \mathcal{V}(\mathbb{Z}_p)^{\text{reg. ss}}$, then we define (following [BS, Section 3.2])

$$m_p(v) = \sum_{i=1}^r \frac{\#\,\mathrm{Stab}_{G(\mathbb{Q}_p)}(v)}{\#\,\mathrm{Stab}_{G(\mathbb{Z}_p)}(v_i)},$$

where $v_1, \ldots, v_r$ are representatives for the $G(\mathbb{Z}_p)$-orbits of $(G(\mathbb{Q}_p)\cdot v) \cap \mathcal{V}(\mathbb{Z}_p)$. The volume of the set V_p appearing in Proposition 2.16 can thus be written as $\mathrm{vol}(V_p) = |W_0|_p(m_p(v)\cdot \mathrm{vol}(U)\cdot \mathrm{vol}(G(\mathbb{Z}_p))/\#\,\mathrm{Stab}_{G(\mathbb{Q}_p)}(v))$, for any $v \in V_p$.

Similarly, if $v \in \mathcal{V}(\mathbb{Z})^{\text{reg. ss}}$, then we define

$$m(v) = \sum_{i=1}^{r} \frac{\# \operatorname{Stab}_{G(\mathbb{Q})}(v)}{\# \operatorname{Stab}_{G(\mathbb{Z})}(v_i)},$$

where $v_1, \dots, v_r$ are representatives for the $G(\mathbb{Z})$-orbits of $(G(\mathbb{Q}) \cdot v) \cap \mathcal{V}(\mathbb{Z})$. (There are finitely many by Theorem 2.9.)

LEMMA 2.17. *For any $v \in \mathcal{V}(\mathbb{Z})^{\text{reg. ss}}$, we have $m(v) = \prod_p m_p(v)$.*

Proof. For each $g \in G(\mathbb{Q})$ such that $gv \in \mathcal{V}(\mathbb{Z})$, we have a natural bijection

$$\operatorname{Stab}_{G(\mathbb{Z})}(gv) \backslash \operatorname{Stab}_{G(\mathbb{Q})}(v) = G(\mathbb{Z}) \backslash G(\mathbb{Z}) g \operatorname{Stab}_{G(\mathbb{Q})}(v),$$

which sends $z \in \operatorname{Stab}_{G(\mathbb{Q})}(v)$ to $G(\mathbb{Z})gz$. Let $v_1, \dots, v_r \in \mathcal{V}(\mathbb{Z})$ be representatives for the set $G(\mathbb{Z}) \backslash (G(\mathbb{Q}) \cdot v \cap \mathcal{V}(\mathbb{Z}))$. We then have

$$\# G(\mathbb{Z}) \backslash \{g \in G(\mathbb{Q}) \mid gv \in \mathcal{V}(\mathbb{Z})\} = \sum_{i=1}^{r} \# \operatorname{Stab}_{G(\mathbb{Z})}(v_i) \backslash \operatorname{Stab}_{G(\mathbb{Q})}(v) = m(v).$$

The same argument applies locally, to give $\# G(\mathbb{Z}_p) \backslash \{g \in G(\mathbb{Q}_p) \mid gv \in \mathcal{V}(\mathbb{Z}_p)\} = m_p(v)$. The result now follows from the bijection of sets:

$$G(\mathbb{Z}) \backslash \{g \in G(\mathbb{Q}) \mid gv \in \mathcal{V}(\mathbb{Z})\} = \prod_p G(\mathbb{Z}_p) \backslash \{g \in G(\mathbb{Q}_p) \mid gv \in \mathcal{V}(\mathbb{Z}_p)\}.$$

The injectivity follows from the fact that $G(\mathbb{Z}) = G(\mathbb{Q}) \cap G(\widehat{\mathbb{Z}})$; the surjectivity follows from the fact (see Theorem 2.7) that $G(\mathbb{A}^\infty) = G(\mathbb{Q}) G(\widehat{\mathbb{Z}})$. □

3. Counting points

In this section, we come to the problem of counting points in $\mathcal{V}(\mathbb{Z})$ up to $G(\mathbb{Z})$-equivalence. We continue with the notation and assumptions of the previous section; thus we have a semi-simple group G acting on the representation V, and we have fixed integral structures $\mathcal{V}$ and $\mathcal{B}$ on the spaces V and $B = V /\!\!/ G$, respectively. The height function H is defined on $B(\mathbb{R})$. If $A \subset \mathcal{V}(\mathbb{Z})$ is any subset, then we write A^{irr} for the subset of $\mathbb{Q}$-irreducible points of A.

In Section 2.9, we constructed open semi-algebraic subsets $L \subset \{b \in B(\mathbb{R}) \mid \Delta(b) \neq 0,\ H(b) = 1\}$ and sections $s : L \to V(\mathbb{R})$ of π; fix one of these. Let

$\Lambda = \mathbb{R}_{>0}$; then the natural product map $L \times \Lambda \to B(\mathbb{R})$ is an open immersion. We will prove the following.

THEOREM 3.1. *There exist constants $C, \delta > 0$, not depending on the choice of L, such that*

$$\begin{aligned}\#G(\mathbb{Z})\backslash\{v \in [G(\mathbb{R}) \cdot \Lambda \cdot s(L)] \cap \mathcal{V}(\mathbb{Z})^{\mathrm{irr}} \mid H(v) < X\}\\ \leqslant C \cdot \mathrm{vol}([1, X^{1/72}] \cdot L) + O(X^{7/12-\delta}).\end{aligned}$$

The rest of this section is devoted to the proof of this theorem. We also deduce below a slight extension (Theorem 3.8), where we impose congruence conditions at finitely many primes; this will be the version used in applications to the arithmetic of algebraic curves.

REMARK 3.2. The constant C is the price we pay for using a Siegel set instead of a true fundamental domain, and not keeping track of the orders of stabilizers. Since we seek only qualitative results, this is not a problem for us. One could easily make the leading term here exact by the systematic use of multisets, as in [**BG**, Section 10]. We emphasize that we do not use multisets here.

3.1. Preliminary reductions.

Let $\mathfrak{S} = \omega \cdot T_c \cdot K \subset G(\mathbb{R})$ be as in Theorem 2.7; in particular, we have $G(\mathbb{Z}) \cdot \mathfrak{S} = G(\mathbb{R})$. It follows that every element of $(G(\mathbb{R})\cdot\Lambda\cdot s(L))\cap\mathcal{V}(\mathbb{Z})$ is $G(\mathbb{Z})$-conjugate to an element of $\mathfrak{S}\cdot\Lambda\cdot s(L)$. We obtain

$$\begin{aligned}\#G(\mathbb{Z})\backslash\{v \in (G(\mathbb{R}) \cdot \Lambda \cdot s(L)) \cap \mathcal{V}(\mathbb{Z})^{\mathrm{irr}} \mid H(v) < X\}\\ \leqslant \#(\mathfrak{S} \cdot [1, X^{1/72}] \cdot s(L) \cap \mathcal{V}(\mathbb{Z})^{\mathrm{irr}}).\end{aligned}$$

The same estimate holds if $\mathfrak{S}$ is replaced by any right translate $\mathfrak{S}h$, $h \in G(\mathbb{R})$. Accordingly, we fix a semi-algebraic subset $G_0 \subset G(\mathbb{R}) \times \Lambda$, compact and of non-empty interior, and such that $K \cdot G_0 = G_0$. In order to simplify some later formulas, we assume that the projection of G_0 onto Λ is contained in $[1, K_0]$ for some constant $K_0 > 1$, and that $\mathrm{vol}(G_0) = 1$. (A pleasant choice is $G_0 = KA_CK \times [1, C]$ for some $C > 1$, where $A_C = \{t \in T^\theta(\mathbb{R})^0 \mid \forall a \in S_G, 1 \leqslant a(t) \leqslant C\}$.) If $A \subset \mathcal{V}(\mathbb{Z})$ is any subset and $X \geqslant 1$, we define (following [**BS**, Section 2.3])

$$N(A, X) = \int_{h\in G_0} \#(\mathfrak{S}h \cdot \Lambda \cdot s(L) \cap \{v \in A^{\mathrm{irr}} \mid H(v) < X\})\, dh$$

and

$$N^*(A, X) = \int_{h\in G_0} \#(\mathfrak{S}h \cdot \Lambda \cdot s(L) \cap \{v \in A \mid H(v) < X\})\, dh.$$

We observe that both $N(A, X)$ and $N^*(A, X)$ are additive in A, in the obvious sense. The following is now clear.

LEMMA 3.3. *Let $A \subset \mathcal{V}(\mathbb{Z})$ be a G-invariant subset. Then*

$$\#G(\mathbb{Z})\backslash\{v \in (G(\mathbb{R}) \cdot \Lambda \cdot s(L)) \cap A^{\mathrm{irr}} \mid H(v) < X\} \leqslant N(A, X)$$

and

$$\#G(\mathbb{Z})\backslash\{v \in (G(\mathbb{R}) \cdot \Lambda \cdot s(L)) \cap A \mid H(v) < X\} \leqslant N^*(A, X).$$

3.2. Bhargava's trick. We now introduce a beautiful trick due to Bhargava that gives a new way to estimate the expressions $N(A, X)$ and $N^*(A, X)$ above.

LEMMA 3.4. *Let $A \subset \mathcal{V}(\mathbb{Z})$ be a subset. Given $X \geqslant 1$, $n \in \overline{N}(\mathbb{R})$, $t \in T^\theta(\mathbb{R})$, and $\lambda \in \Lambda$, define $E(n, t, \lambda, X) = nt\lambda G_0 s(L) \cap \{v \in V(\mathbb{R}) \mid H(v) < X\}$. Then*

$$N(A, X) \leqslant 2^6 \int_{g \in \omega T_c \Lambda} \#[E(n, t, \lambda, X) \cap A^{\mathrm{irr}}]\delta(t)^{-1}\, dn\, dt\, d^\times\lambda$$

and

$$N^*(A, X) \leqslant 2^6 \int_{g \in \omega T_c \Lambda} \#[E(n, t, \lambda, X) \cap A]\delta(t)^{-1}\, dn\, dt\, d^\times\lambda.$$

The Haar measure on $G(\mathbb{R})$ is as in Section 2.7, and we write $d^\times\lambda = d\lambda/\lambda$ for the standard Haar measure on $\Lambda = \mathbb{R}_{>0}$.

Proof. It suffices to treat the case of $N^*(A, X)$, when $A = \{a\}$ consists of a single element. If either a is not conjugate under $G(\mathbb{R}) \times \Lambda$ into $s(L)$, or $H(a) \geqslant X$, then both sides of the above inequality are 0. Otherwise, let $(g_1, \lambda_0), \ldots, (g_k, \lambda_0) \in G(\mathbb{R}) \times \Lambda$ be the elements such that $a \in g_i\lambda_0 s(L)$. We then have

$$N^*(A, X) = \int_{h \in G_0} \mathbf{1}_{a \in \mathfrak{S}h\Lambda \cdot s(L)}\, dh \leqslant \sum_{i=1}^{k} \mathrm{vol}(\{h \in G_0 \mid (g_i, \lambda_0) \in \mathfrak{S}h\Lambda\}).$$

This last sum becomes

$$\sum_{i=1}^{k} \int_{\lambda \in \Lambda} \int_{g \in \mathfrak{S}} \mathbf{1}_{g \in (g_i, \lambda_0) G_0^{-1}}\, dg\, d^\times\lambda \leqslant k \int_{\lambda \in \Lambda} \int_{g \in \mathfrak{S}} \mathbf{1}_{a \in (g, \lambda) G_0 s(L)}\, dg\, d^\times\lambda.$$

Finally, we use the Iwasawa decomposition (see Lemma 2.12) and the fact that $G_0 = KG_0$ to conclude that this last expression equals

$$k \int_{\lambda \in \Lambda} \int_{g \in \mathfrak{S}} \mathbf{1}_{a \in ntk\lambda G_0 s(L)} \delta(t)^{-1} \, dk \, dn \, dt \, d^\times \lambda$$
$$= k \int_{\lambda \in \Lambda} \int_{n \in \omega} \int_{t \in T_c} \mathbf{1}_{a \in E(n,t,\lambda,X)} \delta(t)^{-1} \, dn \, dt \, d^\times \lambda.$$

Since k is at most 2^6, this completes the proof. □

We will make use of the following result of Davenport, slightly extended by Bhargava [BG, Proposition 26].

PROPOSITION 3.5. *Let $R \subset \mathbb{R}^n$ be a bounded semi-algebraic subset, being defined by at most k polynomial inequalities of degree at most l. Let R' denote the image of R under any unipotent linear transformation. Then the number of integer lattice points in R' is*

$$\mathrm{vol}(R) + O(\sup\{\mathrm{vol}(\overline{R}), 1\}),$$

as $\overline{R}$ runs over all projections of R to a j-dimensional coordinate hyperplane, $1 \leqslant j \leqslant n-1$. The implied constant depends only on n, k, and l.

3.3. Cutting off the cusp.

We now write $a_0 \in \Phi_V^+$ for the restriction to T^θ of the highest root of H, as in Section 2.3. We write $S(a_0) \subset \mathcal{V}(\mathbb{Z})$ for the subset of points $v = v_0 + \sum_{a \in \Phi_V} v_a$ with $v_{a_0} = 0$.

PROPOSITION 3.6. *There exists $\delta > 0$ such that $N(S(a_0), X) = O(X^{7/12-\delta})$.*

In fact, the argument shows that one can take $\delta = 1/72$.

Proof. If $M_0, M_1 \subset \Phi_V \cup \{0\}$, we define $S(M_0, M_1) = \{v \in \mathcal{V}(\mathbb{Z}) \mid \forall a \in M_0, v_a = 0; \forall a \in M_1, v_a \neq 0\}$. We refer to a pair of subsets $M_0, M_1 \subset \Phi_V \cup \{0\}$ such that $M_1 \subset (\Phi_V \cup \{0\}) - M_0$ as a cusp datum. To prove the proposition, it is enough to write down a collection $\mathcal{C}$ of cusp data satisfying the following conditions.

- If $v \in S(a_0)^{\mathrm{irr}}$, then there exists $(M_0, M_1) \in \mathcal{C}$ such that $v \in S(M_0, M_1)$.
- If $(M_0, M_1) \in \mathcal{C}$, then $N^*(S(M_0, M_1), X) = O(X^{7/12-\delta})$ for some $\delta > 0$.

According to Lemma 2.6, $S(M_0, M_1)^{\mathrm{irr}}$ is empty if any of the following conditions holds.

(1) $M_0 = \Phi_V^+ - S_V$ and $M_1 = S_V$.

(2) There exists a proper subset $S' \subset S$ such that $\Phi_V^+ - \Phi_{V,S'}^+ \subset M_0$.

(3) There exists $a_i \in S_G$ such that M_0 contains all $a \in \Phi_V \cup \{0\}$ such that $n_{a_i}(a) > 0$.

The union of these conditions is hereditary, in the following sense: if (M_0, M_1) and (M_0', M_1') are cusp data such that $M_0 \subset M_0'$, and (M_0, M_1) satisfies one of these conditions, then so does (M_0', M_1'). This is obvious if M_0 satisfies the second or third condition. On the other hand, it is easy to see that, if M_0 satisfies the first condition, then M_0' satisfies either the first or second condition.

This suggests the following inductive procedure. First, if $M_0 \subset \Phi_V \cup \{0\}$, we write $\lambda(M_0) \subset \Phi_V \cup \{0\}$ for the set of upper bounds of $(\Phi_V \cup \{0\}) - M_0$ in the natural partial order of $\Phi_V \cup \{0\}$:

$$\lambda(M_0) = \{a \in (\Phi_V \cup \{0\}) - M_0 \mid \forall b \in (\Phi_V \cup \{0\}) - M_0, b \geqslant a \Rightarrow b = a\}.$$

One can easily check using the figures in Section 5 that $\lambda(\Phi_V^+ - S_V) = S_V$. We now generate a collection $\mathcal{C}$ of cusp data as follows.

(1) In step 1, we create the cusp datum $(\{a_0\}, \lambda(\{a_0\}))$.

(2) In step $n + 1$, we create new cusp data for each cusp datum at step n. If (M_0, M_1) is a cusp datum at step n, and we enumerate $M_1 = \{b_1, \dots, b_s\}$, then the new cusp data created are $(M_0 \cup \{b_i\}, \lambda(M_0 \cup \{b_i\}))$, $i = 1, \dots, s$.

(3) To finish step $n + 1$, we remove duplicates and delete any newly created cusp data that satisfy any of the three reducibility conditions above.

(4) The procedure terminates when no new cusp data are created at step $n + 1$.

The result of running this procedure is given in Section 5 below. It is clear that, if $v \in S(a_0)^{\text{irr}}$, then there will exist exactly one cusp datum (M_0, M_1) in $\mathcal{C}$ such that $v \in S(M_0, M_1)$. It remains to show that, for each $(M_0, M_1) \in \mathcal{C}$, there exists $\delta > 0$ such that $N^*(S(M_0, M_1), X) = O(X^{7/12-\delta})$. We will establish this by a case-by-case check.

Choose for each $a \in \Phi_V$ a generator e_a of the free rank-1 $\mathbb{Z}$-module $\mathcal{V}_a$, and let $e_{0,0}, e_{0,1}$ be a basis of $\mathcal{V}_0$. Let $\|\cdot\|$ denote the supremum norm of $V(\mathbb{R})$ with respect to this basis. Fix also a constant $J > 0$ such that $\|v\| \leqslant J$ for all $v \in \omega \cdot G_0 \cdot s(L)$.

Let $(M_0, M_1) \in \mathcal{C}$ be a cusp datum. If the set $S(M_0, M_1) \cap E(n, t, \lambda, X)$ is non-empty, then for all $a \in M_1$ we have $\lambda a(t) \geqslant 1/J$ (since there exists $v \in E(n, t, \lambda, X)$ such that $\|v_a\| \geqslant 1$). We also have $\prod_{a\in\Phi_V} a(t) = 1$ for $t \in T^\theta(\mathbb{R})$. In particular, if we write $V_{M_0} \subset V$ for the subspace given by the equations $v_a = 0$, $a \in M_0$, and $V_{M_0,M_1} \subset V_{M_0}(\mathbb{R})$ for the subset given by $\|v_a\| \geqslant 1$, $a \in M_1$, we obtain the following estimate (volumes being taken inside $V_{M_0}(\mathbb{R})$):

$$\mathrm{vol}(E(n, t, \lambda, X) \cap V_{M_0,M_1}) \ll \lambda^{42-\#M_0} \prod_{a\in M_0} a(t)^{-1}. \tag{3.1}$$

Any element $a \in (\Phi_V \cup \{0\}) - M_0$ can be written as $a = b - \sum_{i=1}^4 n_i a_i$ for some $b \in M_1$ and integers $n_i \geqslant 0$. It follows from the definition of the Siegel set $\mathfrak{S} = \omega \cdot T_c \cdot K$ that

$$\lambda a(t) = \lambda b(t) \prod_{i=1}^4 a_i(t)^{-n_i} \geqslant c^{-\sum_{i=1}^4 n_i} \lambda b(t) \gg 1.$$

Consequently, the volume of any projection of $E(n, t, \lambda, X) \cap V_{M_0,M_1}$ onto a coordinate hyperplane of $V_{M_0}(\mathbb{R})$ satisfies the same estimate (3.1).

Let $T(M_0, M_1, \lambda) \subset T_c$ denote the subset defined by the inequalities $\lambda a(t) \geqslant 1/J$, $a \in M_1$. To be completely explicit, we have

$$T(M_0, M_1, \lambda) = \{t \in T^\theta(\mathbb{R})^0 \mid \forall a \in S_G, a(t) \leqslant c;\ \forall a \in M_1, \lambda a(t) \geqslant 1/J\}.$$

The above remarks, together with Proposition 3.5, imply that we have

$$\begin{aligned} N^*(S(M_0, M_1), X) &\ll \int_{g\in\omega T_c\Lambda} \#(S(M_0, M_1) \cap E(n, t, \lambda, X))\delta(t)^{-1}\, dn\, dt\, d^\times\lambda \\ &\ll \int_{\lambda=K_0^{-1}}^{X^{1/72}} \lambda^{42-\#M_0} \int_{t\in T(M_0,M_1,\lambda)} \prod_{a\in\Phi(G,T^\theta)^+} a(t) \\ &\quad \times \prod_{a\in M_0} a(t)^{-1}\, dt\, d^\times\lambda. \end{aligned}$$

We have thus reduced the proposition to showing that for each cusp datum $S(M_0, M_1) \in \mathcal{C}$ we have

$$\int_{t\in T(M_0,M_1,\lambda)} \prod_{a\in\Phi(G,T^\theta)^+} a(t) \prod_{a\in M_0} a(t)^{-1}\, dt = O(\lambda^{\#M_0-\delta}), \tag{3.2}$$

for some $\delta > 0$. This will be established in Section 5. □

3.4. The main body, and the proof of Theorem 3.1.

PROPOSITION 3.7. *Let $N \geqslant 1$ be an integer, and let $v \in \mathcal{V}(\mathbb{Z})$. Let $A_{v,N} = v + N\mathcal{V}(\mathbb{Z})$. Then there exists $\delta > 0$ such that*

$$N^*(A_{v,N} - S(a_0), X) \leqslant \frac{|W_1|_\infty \operatorname{vol}(\mathfrak{S})}{N^{42}} \cdot \operatorname{vol}([1, X^{1/72}] \cdot L) + O(X^{7/12-\delta}).$$

Proof. Let $F(n, t, \lambda, X) = \{v \in E(n, t, \lambda, X) \mid v_{a_0} \neq 0\}$. If $\mathcal{V}(\mathbb{Z}) \cap F(n, t, \lambda, X) \neq 0$, then, just as in the proof of Proposition 3.6, we have $\lambda a_0(t) \geqslant 1/J$, and consequently $\#\mathcal{V}(\mathbb{Z}) \cap F(n, t, \lambda, X) = \operatorname{vol}(F(n, t, \lambda, X)) + O(\lambda^{41} a_0(t)^{-1})$. More generally, we have $\#A_{v,N} \cap F(n, t, \lambda, X) = N^{-42} \operatorname{vol}(F(n, t, \lambda, X)) + O(\lambda^{41} a_0(t)^{-1})$. We obtain

$$\begin{aligned} N^*(A_{v,N} - S(a_0), X) \leqslant & \int_{\lambda \in \Lambda} \int_{g \in \omega T_c} N^{-42} \operatorname{vol}(F(n, t, \lambda, X))\, \delta(t)^{-1} dn\, dt\, d^\times\lambda \\ & + \int_{\lambda = K_0^{-1}}^{X^{1/72}} \int_{g \in \omega T_c} O(\lambda^{41} a_0(t)^{-1})\, \delta(t)^{-1} dn\, dt\, d^\times\lambda. \quad (3.3) \end{aligned}$$

It is easy to see that the second term of (3.3) is $O(X^{7/12-1/72})$. On the other hand, the first term is at most

$$\begin{aligned} & \int_{\lambda \in \Lambda} \int_{g \in \omega T_c} N^{-42} \operatorname{vol}(E(n, t, \lambda, X))\, \delta(t)^{-1} dn\, dt\, d^\times\lambda \\ & = N^{-42} \int_{\lambda \in \Lambda} \int_{g \in \mathfrak{S}} \int_{v \in V(\mathbb{R})} \int_{h \in G_0} \mathbf{1}_{v \in g\lambda h s(L),\, H(v) < X}\, dh\, dg\, dv\, d^\times\lambda. \end{aligned}$$

By Proposition 2.14, this expression is bounded above by

$$\begin{aligned} & \frac{|W_1|_\infty}{N^{42}} \int_{\lambda \in \Lambda} \int_{g \in \mathfrak{S}} \int_{b \in L} \int_{h \in G_0} \mathbf{1}_{H(g\lambda h s(b)) < X}\, dh\, db\, dg\, d^\times\lambda \\ & = \frac{|W_1|_\infty}{N^{42}} \int_{h \in G_0} \operatorname{vol}(\mathfrak{S}) \operatorname{vol}([1, X^{1/72}] \cdot L)\, dh + O(1). \end{aligned}$$

The result follows. □

We now observe that $N(\mathcal{V}(\mathbb{Z}), X) \leqslant N^*(\mathcal{V}(\mathbb{Z}) - S(a_0), X) + N(S(a_0), X)$. Theorem 3.1 follows on combining Lemma 3.3 and Propositions 3.6 and 3.7.

3.5. Counting with congruence conditions. In the applications below, the following slightly more refined version of Theorem 3.1 will be useful. To state it, we must first introduce some notation. Let $p_1, \ldots, p_s$ be prime numbers, and let $V_{p_1}, \ldots, V_{p_s}$ be $G(\mathbb{Z}_{p_i})$-invariant open compact subsets of $\mathcal{V}(\mathbb{Z}_{p_1}), \ldots, \mathcal{V}(\mathbb{Z}_{p_s})$, respectively.

THEOREM 3.8. *There exist constants $C, \delta > 0$, not depending on s or the choice of V_{p_i}, such that*

$$\begin{aligned}\#G(\mathbb{Z})\backslash\{v \in \mathcal{V}(\mathbb{Z})^{\mathrm{irr}} \cap (V_{p_1} \times \cdots \times V_{p_s}) \mid H(v) < X\} \\ \leqslant C \prod_{i=1}^{s} \mathrm{vol}(V_{p_i}) X^{7/12} + O(X^{7/12-\delta}).\end{aligned}$$

Proof. Let $L_1, \ldots, L_r \subset B(\mathbb{R})$ be the sets constructed in Section 2.9, with corresponding sections $s_i : L_i \to V(\mathbb{R})$. Let $A = \mathcal{V}(\mathbb{Z}) \cap (V_{p_1} \times \cdots \times V_{p_s})$. We can find an integer $N \geqslant 1$ and vectors $v_1, \ldots, v_k \in \mathcal{V}(\mathbb{Z})$ such that A is the disjoint union of the sets $v_i + N\mathcal{V}(\mathbb{Z}) = A_{v_i,N}$. We have $k/N^{42} = \prod_{i=1}^{s} \mathrm{vol}(V_{p_i})$. The result now follows by summing the result of Propositions 3.6 and 3.7 over $L = L_1, \ldots, L_r$ and $v = v_1, \ldots, v_k$, and applying Lemma 3.3 once more. □

We now record a particular case of this theorem as a corollary. Let $p_1, \ldots, p_s$ be primes congruent to 1 modulo 6. By combining Propositions 2.15 and 2.16, we obtain open compact subsets $B_{p_i} \subset \mathcal{B}(\mathbb{Z}_{p_i})$ satisfying the following conditions.

(1) Let $b \in B_{p_i}$. Then $\#\,\mathrm{Stab}_{G(\mathbb{Q}_{p_i})}(\kappa_b) = 4$.

(2) Let $V_{p_i} = (G(\mathbb{Q}_{p_i}) \cdot \kappa(\mathbb{Q}_{p_i})) \cap \mathcal{V}(\mathbb{Z}_{p_i}) \cap \pi^{-1}(B_{p_i})$. Then V_{p_i} is open compact, and we have

$$\mathrm{vol}(V_{p_i}) = |W_0|_{p_i} \frac{m_{p_i}(v) \cdot \mathrm{vol}(B_{p_i}) \cdot \mathrm{vol}(G(\mathbb{Z}_{p_i}))}{4},$$

where $m_{p_i}(v) \in \mathbb{Z}$ is independent of the choice of $v \in V_{p_i}$.

If $A \subset \mathcal{V}(\mathbb{Z})$ is a $G(\mathbb{Z})$-invariant subset, we write $G(\mathbb{Q})\backslash A$ for the quotient by the equivalence relation $v \sim v'$ if there exists $\gamma \in G(\mathbb{Q})$ such that $\gamma v = v'$.

COROLLARY 3.9. *With notation as above, let $A = \mathcal{V}(\mathbb{Z}) \cap (V_{p_1} \times \cdots \times V_{p_s})$. Then there exist constants $C, \delta > 0$, not depending on s or the choice of $p_1, \ldots, p_s$, such that*

$$\#G(\mathbb{Q})\backslash\{v \in A^{\mathrm{irr}} \mid H(v) < X\} \leqslant \frac{C}{4^s} \prod_{i=1}^{s} \mathrm{vol}(B_{p_i}) X^{7/12} + O(X^{7/12-\delta}).$$

Proof. If $v \in \mathcal{V}(\mathbb{Z})^{\text{reg. ss}}$, define $n(v) = \#G(\mathbb{Z})\backslash(G(\mathbb{Q}) \cdot v \cap \mathcal{V}(\mathbb{Z}))$. We then have

$$\#G(\mathbb{Q})\backslash\{v \in A \mid H(v) < X\} = \sum_{\substack{v \in G(\mathbb{Z})\backslash A \\ H(v) < X}} \frac{1}{n(v)} \leqslant 2^6 \sum_{\substack{v \in G(\mathbb{Z})\backslash A \\ H(v) < X}} \frac{1}{m(v)},$$

since $n(v) \leqslant m(v) \leqslant 2^6 n(v)$. Using Lemma 2.17, we obtain the inequality $m(v)^{-1} \leqslant \prod_{i=1}^{s} m_{p_i}(v)^{-1}$; hence

$$\begin{aligned} \#G(\mathbb{Q})\backslash\{v \in A \mid H(v) < X\} &\leqslant 2^6 C \prod_{i=1}^{s} \frac{\mathrm{vol}(V_{p_i})}{m_{p_i}(v)} X^{7/12} + O(X^{7/12-\delta}) \\ &= 2^6 C \prod_{i=1}^{s} \frac{|W_0|_{p_i} \, \mathrm{vol}(G(\mathbb{Z}_{p_i})) \cdot \mathrm{vol}(B_{p_i})}{4} X^{7/12} \\ &\quad + O(X^{7/12-\delta}), \end{aligned}$$

by Theorem 3.8. Absorbing terms into the constant now gives the result in the form stated above. □

4. Application to 2-Selmer sets

We now use the results of the preceding sections to deduce our main theorems. Let us write $\mathcal{B}$ for the affine space over $\mathbb{Z}$ with coordinates $p_2, \ldots, p_{12}$, and let B denote the fiber of $\mathcal{B}$ over $\mathbb{Q}$. We consider the following family of affine curves over $\mathcal{B}$:

$$\mathcal{X} : y^3 = x^4 + y(p_2 x^2 + p_5 x + p_8) + p_6 x^2 + p_9 x + p_{12}. \tag{4.1}$$

We write $\mathcal{Y} \to \mathcal{B}$ for the natural compactification of $\mathcal{B}$ as a family of plane quartic curves, and $X \to B$ and $Y \to B$ for the $\mathbb{Q}$-fibers of these families.

LEMMA 4.1. *Let $k/\mathbb{Q}$ be a field. The smooth members over k of the family $Y \to B$ are in bijection with the set of isomorphism classes of triples (C, P_∞, t), where C is a smooth, projective, connected and non-hyperelliptic curve over k of genus 3, $P_\infty \in C(k)$ is a rational point such that $4P_\infty$ is a canonical divisor, and $t \in T_{P_\infty}(C)$ is a non-zero element of the Zariski tangent space at P_∞. If $\lambda \in k^\times$, then the triple $(C, P_\infty, \lambda t)$ has coordinates $\lambda^i p_i(C, P_\infty, t)$.*

Proof. This follows from a theorem of Pinkham: let Γ be the subsemigroup of $(\mathbb{N}, +)$ generated by 3 and 4. The family $X \to B$ is a semi-universal deformation of the monomial singularity Spec $\mathbb{Q}[\Gamma]$. If C is a non-hyperelliptic genus 3 curve and $P_\infty \in C(k)$ is a point such that $4P_\infty$ is a canonical divisor, then P_∞ is a Weierstrass point with Weierstrass semigroup Γ. Pinkham's theorem relates $X \to B$ and the family of genus 3 curves described above. (See [NM04] for more details.)

We now give a proof of the lemma that is essentially a working-out of Pinkham's theorem in this special case. If (C, P_∞, t) is a triple as above, then we calculate the following (using that C is non-hyperelliptic and $4P_\infty$ is canonical):

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$\dim_k H^0(C, \mathcal{O}_C(nP_\infty))$	1	1	1	2	3	3	4	5	6	7	8	9	10.

We choose $x \in H^0(C, \mathcal{O}_C(3P_\infty))$ with a pole of exact order 3 at P_∞, and $y \in H^0(C, \mathcal{O}_C(4P_\infty))$ with a pole of exact order 4. Let z be a coordinate at P_∞ with $dz(t) = 1$; then we can choose x and y so that their Laurent expansions at P_∞ are respectively $x = z^{-3} + \cdots$ and $y = z^{-4} + \cdots$. Then x is uniquely determined by (C, P_∞, t) up to the addition of constants, and y is uniquely determined up to the addition of constants and constant multiples of x.

The 11 monomials $1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, x^4, y^3$ lie in the ten-dimensional space $H^0(C, \mathcal{O}_C(12P_\infty))$. The first nine of these monomials are linearly independent and lie in $H^0(C, \mathcal{O}_C(11P_\infty))$. It follows that they must satisfy a unique linear relation of the form

$$y^3 = x^4 + q_1 xy^2 + q_2 x^2 y + q_3 x^3 + q_4 y^2 + q_5 xy + q_6 x^2 + q_8 y + q_9 x + q_{12}.$$

At this point, we still have the freedom to replace x by $x + a$ and y by $y + bx + c$ for any constants $a, b, c \in k$. It is now easy to check that there is a unique choice of $a, b, c \in k$ for which $q_1 = q_3 = q_4 = 0$, giving an equation of type (4.1). We have shown that any triple (C, P_∞, t) determines uniquely an equation of this type; conversely, if $p_2, \ldots, p_{12} \in k$ and the projective closure C of the equation (4.1) is smooth, then it is easy to check that C is non-hyperelliptic of genus 3, with a unique point P_∞ at infinity, and $4P_\infty$ is a canonical divisor (equivalently, P_∞ is a hyperflex in the canonical embedding). We recover a non-zero tangent vector $t \in T_{P_\infty}(C)$ by the requirement that the functions $x, y \in k(C)$ have Laurent expansions $x = z^{-3} + \cdots$, $y = z^{-4} + \cdots$ at P_∞, where z is any coordinate at P_∞ satisfying $dz(t) = 1$. This completes the proof. □

We define the height of an element $b \in \mathcal{B}(\mathbb{R})$ by the formula $H(b) = \sup_i |p_i(b)|^{72/i}$. The function H is homogeneous of degree 72: for any $\lambda \in \mathbb{R}^\times$, $H(\lambda b) = |\lambda|^{72} H(b)$. We write $\mathcal{F}_0 \subset \mathcal{B}(\mathbb{Z})$ for the set of points b such that Y_b is smooth over $\mathbb{Q}$. We say that a subset $\mathcal{F} \subset \mathcal{F}_0$ is defined by congruence conditions if there exist primes $p_1, \dots, p_s$ and open compact subsets $B_{p_i} \subset \mathcal{B}(\mathbb{Z}_{p_i})$, $i = 1, \dots, s$, such that $\mathcal{F} = \mathcal{F}_0 \cap (B_{p_1} \times \cdots \times B_{p_s})$. The following is an immediate consequence of Proposition 3.5.

Proposition 4.2. *Let $\mathcal{F} \subset \mathcal{F}_0$ be a subset defined by congruence conditions, as above. Then there exists $\delta > 0$ such that*

$$\#\{b \in \mathcal{F} \mid H(b) < X\} = \prod_{i=1}^{s} \mathrm{vol}(B_{p_i}) X^{7/12} + O(X^{7/12-\delta}).$$

We can now state our main theorems.

Theorem 4.3. *Let $\mathcal{F} \subset \mathcal{F}_0$ be a subset defined by congruence conditions. Then*

$$\limsup_{X \to \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ H(b) < X}} \# \mathrm{Sel}_2(Y_b)}{\sum_{\substack{b \in \mathcal{F} \\ H(b) < X}} 1} < \infty.$$

Theorem 4.4. *Let $\epsilon > 0$. Then there exists a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions such that*

$$\limsup_{X \to \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ H(b) < X}} \# \mathrm{Sel}_2(Y_b)}{\sum_{\substack{b \in \mathcal{F} \\ H(b) < X}} 1} < 1 + \epsilon.$$

Consequently, we have

$$\liminf_{X \to \infty} \frac{\#\{b \in \mathcal{F} \mid H(b) < X,\ \# \mathrm{Sel}_2(Y_b) = 1\}}{\#\{b \in \mathcal{F} \mid H(b) < X\}} > 1 - \epsilon.$$

The proofs of Theorems 4.3 and 4.4 are very similar, so we give here only the proof of the second result.

Proof of Theorem 4.4. Let $p_1, p_2, \dots$ be a strictly increasing sequence of primes congruent to 1 mod 6. For each $i \geqslant 1$, let $B_{p_i} \subset \mathcal{B}(\mathbb{Z}_{p_i})$ and $V_{p_i} \subset \mathcal{V}(\mathbb{Z}_{p_i})$ be the open compact subsets obtained by combining Propositions 2.15 and 2.16; see Corollary 3.9. If $s \geqslant 0$, let $\mathcal{F} \subset \mathcal{F}_0$ be the family defined by imposing the congruence conditions $B_{p_i} \subset \mathcal{B}(\mathbb{Z}_{p_i})$ of Proposition 2.16 at the primes $p_1, \dots, p_s$, and let $A \subset \mathcal{V}(\mathbb{Z})$ be the corresponding set of points. Applying Theorem 2.10 and Corollary 3.9, we find that there are constants $C, \delta > 0$, not depending on s, such that

$$\sum_{\substack{b\in\mathcal{F}\\ H(b)<X}} (\#\operatorname{Sel}_2(Y_b)-1) \leqslant \#G(\mathbb{Q})\backslash\{v\in A^{\mathrm{irr}} \mid H(v)<N_3^{72}X\}$$

$$\leqslant C\prod_{i=1}^{s}\frac{\operatorname{vol}(B_{p_i})}{4}(N_3^{72}X)^{7/12}+O(X^{7/12-\delta}).$$

Combining this with Proposition 4.2, we obtain

$$\frac{\sum_{\substack{b\in\mathcal{F}\\ H(b)<X}}(\#\operatorname{Sel}_2(Y_b)-1)}{\sum_{\substack{b\in\mathcal{F}\\ H(b)<X}}1} \leqslant \frac{N_3^{42}C+O(X^{-\delta})}{4^s+O(X^{-\delta})}.$$

Choosing s to be sufficiently large and taking the limit $X\to\infty$ now gives the result. □

REMARK 4.5. Let us say that a point $b\in\mathcal{F}_0$ is minimal if it satisfies the following conditions.

(1) There do not exist a prime p and $c\in\mathcal{B}(\mathbb{Z})$ such that $b=p\cdot c$.

(2) We have $p_5(b)\geqslant 0$, and if $p_5(b)=0$ then $p_9(b)\geqslant 0$.

It follows from Lemma 4.1 that any pair (C, P_∞) is represented by a unique minimal $b\in\mathcal{F}_0$. The analogs of Theorems 4.3 and 4.4 for the averages taken over the set of minimal equations follow immediately on noting that (with appropriately chosen congruence conditions) a positive proportion of points $b\in\mathcal{F}_0$ are minimal.

We now use the above theorems to deduce some Diophantine consequences for the curves Y_b. We begin with some preparatory lemmas.

LEMMA 4.6. *There exists an open subset $U\subset\mathcal{B}(\mathbb{Z}_3)$ such that, for all $b\in U$, $\Delta(b)\neq 0$ and the image of the map $\mathcal{X}_b(\mathbb{Z}_3)\to J_b(\mathbb{Q}_3)/2J_b(\mathbb{Q}_3)$ is non-trivial and does not contain the identity.*

Compare Proposition 2.15.

Proof. Consider the curve $\mathcal{X}_{b_0}$ given by the equation $y^3=x^4-2y$. Then $\Delta(b_0)\neq 0$, and there is map from $\mathcal{Y}_{b_0}$ to the elliptic curve $\mathcal{E}$ over $\mathbb{Z}_3$ which is the projective closure of the affine piece $\mathcal{E}^0: z^2=w^3+2w$. (The map is given by $(w, z)=(y, x^2)$.) The curve $\mathcal{E}$ has good reduction, and $\mathcal{E}(\mathbb{F}_3)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. In particular, $2\mathcal{E}(\mathbb{F}_3)$ is trivial, $\mathcal{E}^0(\mathbb{F}_3)=\mathcal{E}(\mathbb{F}_3)-\{\mathcal{O}_\mathcal{E}\}$, and the map $\mathcal{E}^0(\mathbb{Z}_3)\to\mathcal{E}(\mathbb{Q}_3)/2\mathcal{E}(\mathbb{Q}_3)$ factors

$$\mathcal{E}^0(\mathbb{Z}_3)\to\mathcal{E}^0(\mathbb{F}_3)\hookrightarrow\mathcal{E}(\mathbb{F}_3)\cong\mathcal{E}(\mathbb{Q}_3)/2\mathcal{E}(\mathbb{Q}_3).$$

By Albanese functoriality, there is a commutative diagram

$$\begin{tikzcd}
\mathcal{X}_{b_0}(\mathbb{Z}_3) \arrow[r] \arrow[d] & J_{b_0}(\mathbb{Q}_3)/2J_{b_0}(\mathbb{Q}_3) \arrow[d] \\
\mathcal{E}^0(\mathbb{Z}_3) \arrow[r] & \mathcal{E}(\mathbb{Q}_3)/2\mathcal{E}(\mathbb{Q}_3)
\end{tikzcd}$$

It follows that the image of $\mathcal{X}_{b_0}(\mathbb{Z}_3)$ in $J_{b_0}(\mathbb{Q}_3)/2J_{b_0}(\mathbb{Q}_3)$ does not contain the identity. To finish the proof of the lemma, we take U to be any sufficiently small open neighborhood of b_0 in $\mathcal{B}(\mathbb{Z}_3)$. □

LEMMA 4.7. (1) *Let p be a prime. Then there exists an open compact subset $U \subset \mathcal{B}(\mathbb{Z}_p)$ such that, for every $b \in U$, $\Delta(b) \neq 0$ and $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$.*

(2) *There exists an integer M such that, for all primes $p > M$, and for all $b \in \mathcal{B}(\mathbb{Z}_p)$, $\mathcal{X}_b(\mathbb{Z}_p) \neq 0$.*

Proof. It follows from Hensel's lemma that, if $b \in \mathcal{B}(\mathbb{Z}_p)$, $\overline{x} \in \mathcal{X}_b(\mathbb{F}_p)$, and $\mathcal{X}_{b,\mathbb{F}_p}$ is smooth at $\overline{x}$, then $\overline{x}$ is the reduction modulo p of a point $x \in \mathcal{X}_b(\mathbb{Z}_p)$; in particular, $\mathcal{X}_b(\mathbb{Z}_p)$ is not empty. It is easy to write down for every prime p a point $b \in \mathcal{B}(\mathbb{F}_p)$ such that $\mathcal{X}_b$ is smooth and has $\mathbb{F}_p$-rational points. This proves the first part of the lemma.

For the second part, we observe that the fibers of the morphism $\mathcal{Y} \to \mathcal{B}$ are geometrically irreducible. Indeed, this morphism is proper, flat, and of finite type, which implies that the subset of points of $\mathcal{B}$ where the fibers are geometrically irreducible is open; moreover, this subset is stable by the action of the natural contracting action of $\mathbb{G}_m$ on $\mathcal{B}$, and contains the point $0 \in \mathcal{B}(\mathbb{F}_p)$. It follows from the Weil bounds that, for p sufficiently large, and for every $b \in \mathcal{B}(\mathbb{F}_p)$, $\mathcal{X}_b(\mathbb{F}_p)$ contains a point at which $\mathcal{X}_b$ is smooth. This completes the proof of the lemma. □

THEOREM 4.8. *Let $\epsilon > 0$. Then there exists a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions satisfying the following conditions.*

(1) *For every $b \in \mathcal{F}$, and for every prime p, $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$.*

(2) *We have*

$$\liminf_{X \to \infty} \frac{\#\{b \in \mathcal{F} \mid H(b) < X,\ \mathcal{X}_b(\mathbb{Z}_{(3)}) = \emptyset\}}{\#\{b \in \mathcal{F} \mid H(b) < X\}} > 1 - \epsilon.$$

(We recall that $\mathbb{Z}_{(3)} \subset \mathbb{Q}$ denotes the subring of rational numbers of denominator prime to 3.) In particular, a positive proportion of $b \in \mathcal{F}_0$ have the property that, for every prime p, $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$, yet $\mathcal{X}_b(\mathbb{Z}) = \emptyset$.

Proof. We choose for every prime p an open compact subset $U_p \subset \mathcal{B}(\mathbb{Z}_p)$ satisfying the following conditions.

- For every prime p, and every $b \in U_p$, the set $\mathcal{X}_b(\mathbb{Z}_p)$ is non-empty.
- If $p = 3$, then U_p satisfies the conclusion of Lemma 4.6.
- There exists an integer M such that, for all $p > M$, $U_p = \mathcal{B}(\mathbb{Z}_p)$.

(We can make such a choice because of Lemma 4.7.) Let $p_1, p_2, \ldots$ be a strictly increasing sequence of primes such that, for each $i \geqslant 1$, $p_i > M$ and $p_i \equiv 1 \bmod 6$, and write $B_{p_i} \subset \mathcal{B}(\mathbb{Z}_{p_i})$ for the set that results from applying Propositions 2.15 and 2.16. If $s \geqslant 1$ is an integer, then we define $\mathcal{F}_s \subset \mathcal{F}_0$ to be the subset defined by the congruence conditions U_p $(p < M)$ and $B_{p_1}, \ldots, B_{p_s}$.

Arguing as in the proof of Theorem 4.4, we find that for any $\epsilon > 0$ we can choose $s \geqslant 1$ such that

$$\liminf_{X \to \infty} \frac{\#\{b \in \mathcal{F}_s \mid H(b) < X,\ \#\operatorname{Sel}_2(Y_b) = 1\}}{\#\{b \in \mathcal{F}_s \mid H(b) < X\}} > 1 - \epsilon.$$

We claim that, for each $b \in \mathcal{F}_s$ such that $\#\operatorname{Sel}_2(Y_b) = 1$, we have $\mathcal{X}_b(\mathbb{Z}_{(3)}) = \emptyset$. Indeed, for each $b \in \mathcal{F}_s$, there is a commutative diagram

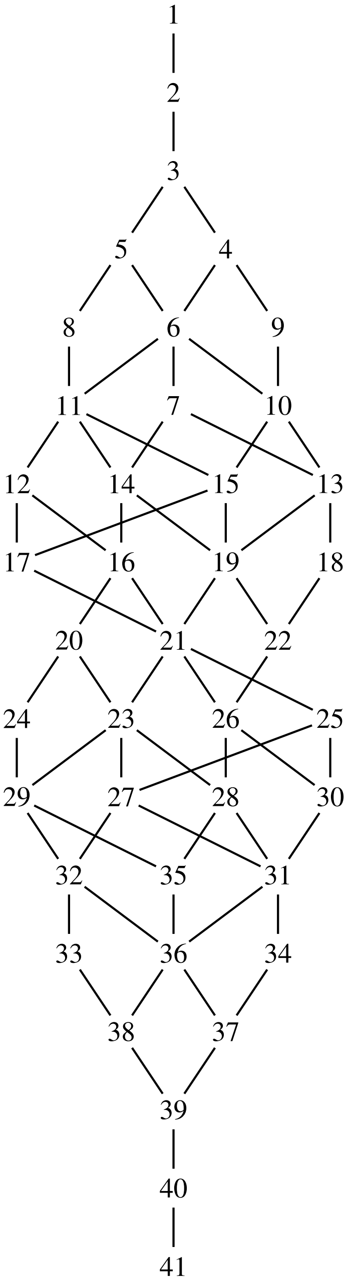
$$\begin{tikzcd}
\mathcal{X}_b(\mathbb{Z}_{(3)}) \arrow[r] \arrow[d] & \mathcal{X}_b(\mathbb{Z}_3) \arrow[d] \\
\operatorname{Sel}_2(Y_b) \arrow[r] & J_b(\mathbb{Q}_3)/2J_b(\mathbb{Q}_3)
\end{tikzcd}$$

Because of our choice of U_3, the image of the composite of the top and right-hand arrows does not contain the identity. Because $\operatorname{Sel}_2(Y_b)$ is trivial, the composite of the left-hand and bottom arrows has image contained in the trivial subgroup. It follows that $\mathcal{X}_b(\mathbb{Z}_{(3)})$ must be empty. This completes the proof. □

5. The proof of Proposition 3.6

We take up the notation and assumptions of Section 3. In the two figures on this page, we display the characters $a \in X^*(T^\theta)$ which appear in the weight decomposition of V. There are 41 weights; each weight space is one-dimensional, except for the weight space of the trivial character, which is two-dimensional. In the table on the left, we list the characters that appear, giving each a number. In the figure on the right, we display the Hasse diagram of the set $\Phi_V \cup 0$, now identified with $1, \ldots, 41$, with respect to the natural partial order on this set.

#	Weight			
1	1	2	3	2
2	1	2	3	1
3	1	2	2	1
4	1	1	2	1
5	1	2	1	1
6	1	1	1	1
7	1	0	1	1
8	1	2	1	0
9	0	1	2	1
10	0	1	1	1
11	1	1	1	0
12	1	1	0	0
13	0	0	1	1
14	1	0	1	0
15	0	1	1	0
16	1	0	0	0
17	0	1	0	0
18	−1	0	1	1
19	0	0	1	0
20	1	0	−1	0
21	0	0	0	0
22	−1	0	1	0
23	0	0	−1	0
24	1	0	−1	−1
25	0	−1	0	0
26	−1	0	0	0
27	0	−1	−1	0
28	−1	0	−1	0
29	0	0	−1	−1
30	−1	−1	0	0
31	−1	−1	−1	0
32	0	−1	−1	−1
33	0	−1	−2	−1
34	−1	−2	−1	0
35	−1	0	−1	−1
36	−1	−1	−1	−1
37	−1	−2	−1	−1
38	−1	−1	−2	−1
39	−1	−2	−2	−1
40	−1	−2	−3	−1
41	−1	−2	−3	−2



In the following table, we give the result of running the inductive procedure of Proposition 3.6. We recall that this procedure gives a collection $\mathcal{C}$ of cusp data; by definition, a cusp datum is a pair (M_0, M_1) of subsets of $\Phi_V \cup \{0\}$ such that $M_1 \subset (\Phi_V \cup \{0\}) - M_0$. For each cusp datum, we must compute the corresponding cusp integral (3.2), and show that it is $O(\lambda^{\# M_0 - \delta})$ for some $\delta > 0$. For the reader's convenience, we recall that this integral is given by the formula

$$\int_{t \in T(M_0, M_1, \lambda)} \prod_{a \in \Phi(G, T^\theta)^+} a(t) \prod_{a \in M_0} a(t)^{-1} \, dt = \int_{t \in T(M_0, M_1, \lambda)} w(t) \, dt, \tag{5.1}$$

where

$$T(M_0, M_1, \lambda) = \{t \in T^\theta(\mathbb{R})^0 \mid \forall i = 1, \ldots, 4, a_i(t) \leqslant c; \ \forall a \in M_1, \lambda a(t) \geqslant 1/J\}. \tag{5.2}$$

These integrals can be evaluated in elementary terms, and this is one way to finish the proof of the proposition. In the last column of the table below, we have written the corresponding integrand in (5.1) as a vector $w(t) = t_1^{w_1} t_2^{w_2} t_3^{w_3} t_4^{w_4}$, where $t_i = a_i(t)$. Thus, for example, the cusp integral in the first column can be rewritten as

$$\int_{t_1=0}^{c} \int_{t_2=0}^{c} \int_{t_3=0}^{c} \int_{t_4=0}^{c} t_1^7 t_2^{12} t_3^{15} t_4^8 \cdot \mathbf{1}_{\lambda t_1 t_2^2 t_3^3 t_4 \geqslant 1/J} \cdot d^\times t_1 \, d^\times t_2 \, d^\times t_3 \, d^\times t_4.$$

As the table has 68 rows, the procedure just described involves calculating 68 integrals. We now discuss a trick, due to Bhargava (see the proof of [Bha10, Lemma 11]), which allows one to reduce the amount of computation required to bound the integrals (5.1). Namely, let (M_0, M_1) be a cusp datum appearing in the table below. Given a function $p : M_1 \to \mathbb{R}_{\geqslant 0}$, we have $\prod_{a \in M_1} (\lambda a(t))^{p(a)} \gg 1$ inside $T(M_0, M_1, \lambda)$, and hence

$$\int_{t \in T(M_0, M_1, \lambda)} w(t) \, dt \ll \lambda^{\sum_{a \in M_1} p(a)} \int_{t \in T(M_0, M_1, \lambda)} w(t) \cdot \prod_{a \in M_1} a(t)^{p(a)} \, dt. \tag{5.3}$$

If the exponent of each t_i $(i = 1, \ldots, 4)$ in the function $w(t) \cdot \prod_{a \in M_1} a(t)^{p(a)}$ is (strictly) positive, then the second integral in (5.3) is bounded independently of λ, and we obtain

$$\int_{t \in T(M_0, M_1, \lambda)} w(t) \, dt \ll \lambda^{\sum_{a \in M_1} p(a)}.$$

The problem of bounding the cusp integral (5.1) is thus reduced to the problem of finding a function $p : M_1 \to \mathbb{R}_{\geqslant 0}$ which satisfies the following two conditions.

- We have $\sum_{a \in M_1} p(a) < \#M_0$.
- For each $i = 1, \ldots, 4$, we have $w_i + \sum_{a \in M_1} p(a) \cdot n_{a_i}(a) > 0$.

It is easy to check (especially using a computer) that such a function p exists for all of the cusp data appearing in the table below. This completes our proof of the proposition.

As an example, we discuss the cusp datum appearing in the final row of our table. We must find non-negative real numbers p_{13}, p_{17}, p_{24} such that $p_{13}+p_{17}+p_{24} < 16$ and the vector

$$(-5 + p_{24}, -3 + p_{17}, -1 + p_{13} - p_{24}, p_{13} - p_{24})$$

has strictly positive entries. It is not possible to choose the p_i all to be integers, but one possible choice is $(p_{13}, p_{17}, p_{24}) = (6\frac{1}{2}, 3\frac{1}{4}, 5\frac{1}{4})$.

M_0	M_1	$\#M_0$	Weight of integrand			
1	2	1	7	12	15	8
1,2	3	2	6	10	12	7
1,2,3	4,5	3	5	8	10	6
1,2,3,4	5,9	4	4	7	8	5
1,2,3,5	4,8	4	4	6	9	5
1,2,3,4,5	6,8,9	5	3	5	7	4
1,2,3,4,9	5	5	4	6	6	4
1,2,3,5,8	4	5	3	4	8	5
1,2,3,4,5,6	7,8,9	6	2	4	6	3
1,2,3,4,5,8	6,9	6	2	3	6	4
1,2,3,4,5,9	6,8	6	3	4	5	3
1,2,3,4,5,6,7	8,9	7	1	4	5	2
1,2,3,4,5,6,8	7,9,11	7	1	2	5	3
1,2,3,4,5,6,9	7,8,10	7	2	3	4	2
1,2,3,4,5,8,9	6	7	2	2	4	3
1,2,3,4,5,6,7,8	9,11	8	0	2	4	2
1,2,3,4,5,6,7,9	8,10	8	1	3	3	1
1,2,3,4,5,6,8,9	7,10,11	8	1	1	3	2
1,2,3,4,5,6,8,11	7,9,12	8	0	1	4	3
1,2,3,4,5,6,9,10	7,8	8	2	2	3	1
1,2,3,4,5,6,7,8,9	10,11	9	0	1	2	1
1,2,3,4,5,6,7,8,11	9,12,14	9	−1	1	3	2
1,2,3,4,5,6,7,9,10	8,13	9	1	2	2	0
1,2,3,4,5,6,8,9,10	7,11	9	1	0	2	1
1,2,3,4,5,6,8,9,11	7,10,12	9	0	0	2	2
1,2,3,4,5,6,8,11,12	7,9	9	−1	0	4	3

1,2,3,4,5,6,7,8,9,10	11,13	10	0	0	1	0
1,2,3,4,5,6,7,8,9,11	10,12,14	10	−1	0	1	1
1,2,3,4,5,6,7,8,11,12	9,14	10	−2	0	3	2
1,2,3,4,5,6,7,8,11,14	9,12	10	−2	1	2	2
1,2,3,4,5,6,7,9,10,13	8,18	10	1	2	1	−1
1,2,3,4,5,6,8,9,10,11	7,12,15	10	0	−1	1	1
1,2,3,4,5,6,8,9,11,12	7,10	10	−1	−1	2	2
1,2,3,4,5,6,7,8,9,10,11	12,13,14,15	11	−1	−1	0	0
1,2,3,4,5,6,7,8,9,10,13	11,18	11	0	0	0	−1
1,2,3,4,5,6,7,8,9,11,12	10,14	11	−2	−1	1	1
1,2,3,4,5,6,7,8,9,11,14	10,12	11	−2	0	0	1
1,2,3,4,5,6,7,8,11,12,14	9,16	11	−3	0	2	2
1,2,3,4,5,6,8,9,10,11,12	7,15	11	−1	−2	1	1
1,2,3,4,5,6,8,9,10,11,15	7,12	11	0	−2	0	1
1,2,3,4,5,6,7,8,9,10,11,12	13,14,15	12	−2	−2	0	0
1,2,3,4,5,6,7,8,9,10,11,13	12,14,15,18	12	−1	−1	−1	−1
1,2,3,4,5,6,7,8,9,10,11,14	12,13,15	12	−2	−1	−1	0
1,2,3,4,5,6,7,8,9,10,11,15	12,13,14	12	−1	−2	−1	0
1,2,3,4,5,6,7,8,9,11,12,14	10,16	12	−3	−1	0	1
1,2,3,4,5,6,7,8,11,12,14,16	9,20	12	−4	0	2	2
1,2,3,4,5,6,8,9,10,11,12,15	7,17	12	−1	−3	0	1
1,2,3,4,5,6,7,8,9,10,11,12,13	14,15,18	13	−2	−2	−1	−1
1,2,3,4,5,6,7,8,9,10,11,12,14	13,15,16	13	−3	−2	−1	0
1,2,3,4,5,6,7,8,9,10,11,12,15	13,14,17	13	−2	−3	−1	0
1,2,3,4,5,6,7,8,9,10,11,13,14	12,15,18	13	−2	−1	−2	−1
1,2,3,4,5,6,7,8,9,10,11,13,15	12,14,18	13	−1	−2	−2	−1
1,2,3,4,5,6,7,8,9,10,11,14,15	12,13	13	−2	−2	−2	0
1,2,3,4,5,6,7,8,9,11,12,14,16	10,20	13	−4	−1	0	1
1,2,3,4,5,6,7,8,11,12,14,16,20	9,24	13	−5	0	3	2
1,2,3,4,5,6,7,8,9,10,11,12,13,14	15,16,18	14	−3	−2	−2	−1
1,2,3,4,5,6,7,8,9,10,11,12,13,15	14,17,18	14	−2	−3	−2	−1
1,2,3,4,5,6,7,8,9,10,11,12,14,15	13,16,17	14	−3	−3	−2	0
1,2,3,4,5,6,7,8,9,10,11,12,14,16	13,15,20	14	−4	−2	−1	0
1,2,3,4,5,6,7,8,9,10,11,13,14,15	12,18,19	14	−2	−2	−3	−1
1,2,3,4,5,6,7,8,9,11,12,14,16,20	10,24	14	−5	−1	1	1
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15	16,17,18,19	15	−3	−3	−3	−1
1,2,3,4,5,6,7,8,9,10,11,12,13,14,16	15,18,20	15	−4	−2	−2	−1
1,2,3,4,5,6,7,8,9,10,11,12,14,15,16	13,17,20	15	−4	−3	−2	0
1,2,3,4,5,6,7,8,9,10,11,12,14,16,20	13,15,24	15	−5	−2	0	0
1,2,3,4,5,6,7,8,9,10,11,13,14,15,19	12,18	15	−2	−2	−4	−1
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,19	16,17,18	16	−3	−3	−4	−1
1,2,3,4,5,6,7,8,9,10,11,12,14,15,16,20	13,17,24	16	−5	−3	−1	0

Acknowledgements

As will be clear to the reader, Section 3 of this paper owes everything to the ideas of Manjul Bhargava. I wish to thank him, as well as Arul Shankar, for many helpful conversations about this circle of ideas. I would also like to thank the anonymous referees for their careful reading of the original version of this paper. In particular, they observed a mistake in the table in Section 5 which has now been corrected.

While speaking about the work [Tho13], the author suggested that the methods of this paper might show that (with notation as in the introduction) $\# \mathrm{Sel}_2(Y_b)$ is 1 on average. This was based on the erroneous belief that the appropriate product of local densities would converge to zero. On the contrary, it seems likely, although we do not prove this, that this average is strictly greater than 1 in any subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions; for an analogous statement in the hyperelliptic case, see [BS09, Lemma 4.3]. I would like to again thank Manjul Bhargava for pointing out this error.

In the period during which this research was conducted, Jack Thorne served as a Clay Research Fellow.

References

[BCR98] J. Bochnak, M. Coste and M.-F. Roy, *Real Algebraic Geometry*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 36 (Springer, Berlin, 1998), translated from the 1987 French original, Revised by the authors.

[Bha] M. Bhargava, 'Most hyperelliptic curves over $\mathbb{Q}$ have no rational points', Preprint.

[Bha10] M. Bhargava, 'The density of discriminants of quintic rings and fields', *Ann. of Math.* (2) **172**(3) (2010), 1559–1591.

[BG] M. Bhargava and B. H. Gross, 'The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point', in *Automorphic Representations and L-functions*, Tata Inst. Fundam. Res. Stud. Math., 22 (Tata Inst. Fund. Res., Mumbai, 2013), 23–91.

[Bor66] A. Borel, 'Density and maximality of arithmetic subgroups', *J. reine angew. Math.* **224** (1966), 78–89.

[Bor70] A. Borel, 'Properties and linear representations of Chevalley groups', in *Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, NJ, 1968/69)*, Lecture Notes in Mathematics, 131 (Springer, Berlin, 1970), 1–55.

[BHC62] A. Borel and Harish-Chandra, 'Arithmetic subgroups of algebraic groups', *Ann. of Math.* (2) **75** (1962), 485–535.

[BLR90] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron Models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 21 (Springer, Berlin, 1990).

[Bou68] N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines*, Actualités Scientifiques et Industrielles, No. 1337 (Hermann, Paris, 1968).

[BS] M. Bhargava and A. Shankar, 'Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves', *Ann. of Math.* (2) **181**(1) (2015), 191–242.

[BS09] N. Bruin and M. Stoll, 'Two-cover descent on hyperelliptic curves', *Math. Comput.* **78**(268) (2009), 2347–2370.

[CX08] P. L. Clark and X. Xarles, 'Local bounds for torsion points on abelian varieties', *Canad. J. Math.* **60**(3) (2008), 532–555.

[Kot99] R. E. Kottwitz, 'Transfer factors for Lie algebras', *Represent. Theory* **3** (1999), 127–138. (electronic).

[Lan75] S. Lang, $\mathrm{SL}_2(\mathbf{R})$ (Addison-Wesley Publishing Co., Reading, MA–London–Amsterdam, 1975).

[Lor00] D. Lorenzini, 'Reduction of points in the group of components of the Néron model of a Jacobian', *J. reine angew. Math.* **527** (2000), 117–150.

[LT02] D. Lorenzini and T. J. Tucker, 'Thue equations and the method of Chabauty–Coleman', *Invent. Math.* **148**(1) (2002), 47–77.

[NM04] T. Nakano and T. Mori, 'On the moduli space of pointed algebraic curves of low genus—a computational approach', *Tokyo J. Math.* **27**(1) (2004), 239–253.

[Pan05] D. I. Panyushev, 'On invariant theory of θ-groups', *J. Algebra* **283**(2) (2005), 655–670.

[PR94] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Pure and Applied Mathematics, 139 (Academic Press Inc., Boston, MA, 1994), translated from the 1991 Russian original by Rachel Rowen.

[PS14] B. Poonen and M. Stoll, 'Most odd degree hyperelliptic curves have only one rational point', *Ann. of Math.* (2) **180**(3) (2014), 1137–1166.

[Ree10] M. Reeder, 'Torsion automorphisms of simple Lie algebras', *Enseign. Math.* (2) **56**(1–2) (2010), 3–47.

[Spr09] T. A. Springer, *Linear Algebraic Groups*, 2nd edn, Progress in Mathematics, 9 (Birkhäuser Boston, Inc., Boston, MA, 1998), 2009 edition (reprint).

[Tho] J. A. Thorne, 'On the 2-Selmer groups of plane quartic curves with a marked rational point', Preprint.

[Tho13] J. A. Thorne, 'Vinberg's representations and arithmetic invariant theory', *Algebra Number Theory* **7**(9) (2013), 2331–2368.