Arithmetic statistics of isogeny Selmer groups associated to hyperelliptic curves

Martí Oller

June 4, 2026

Abstract

We determine asymptotic results for the average size of Selmer groups arising from certain isogenies related to Jacobians of hyperelliptic curves of genus $g \geq 2$. We do so by combining Bhargava's geometry-of-numbers methods with new parametrisations coming from Vinberg theory, arising from representations related to the Dynkin diagrams of type B and C. We additionally get prove some lower bounds on the average size of these isogeny Selmer groups by using a formula of Greenberg–Wiles.

Contents

1 Introduction

1.1 Statement of results

Let $n \geq 2$. Fix $B = \operatorname{Spec} \mathbb{Z}[p_2, \ldots, p_{4n}]$, and for $b \in B(\mathbb{R})$ consider the hyperelliptic curve

$$C_b \colon y^2 = x(x^{2n} + p_2(b)x^{2n-1} + \cdots + p_{4n}(b)).$$

Let J_b be the Jacobian of C_b. We note that $(0,0) \in C_b(\mathbb{Q})$, and the difference of this rational point and the point at infinity generates an order 2 subgroup of $J_b[2]$, which we denote by M. Let $M^\perp$ be the orthogonal complement of M with respect to the Weil pairing. We note that $M \leqslant M^\perp$, and that both M and $M^\perp$ are stable under $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action. Therefore, there exists an abelian variety A_b with maps

$$J_b \xrightarrow{\phi_M} A_b \xrightarrow{\phi} A_b^\vee \xrightarrow{\phi_M^\vee} J_b, \tag{1}$$

such that if $\psi = \phi \circ \phi_M$, then $J_b[\phi_M] = M$, $J_b[\psi] = M^\perp$, $A_b[\phi] = M^\perp/M$. Moreover, the total composition map $J_b \to J_b$ in (1) is the multiplication-by-2 map.

For an element $b \in B(\mathbb{R})$, let us define its *height* as

$$\operatorname{ht}(b) = \sup_{i=1,\ldots,2n} \{|p_{2i}(b)|^{1/(2i)}\}.$$

Theorem 1.1. *We have that*

$$\limsup_{X\to\infty} \frac{\sum_{\operatorname{ht}(b)<X} \# \operatorname{Sel}_\phi A_b}{\sum_{\operatorname{ht}(b)<X} 1} \leq 6.$$

Theorem 1.2. *We have that*

$$\frac{\sum_{\operatorname{ht}(b)<X} \# \operatorname{Sel}_{\phi_M^\vee} A_b^\vee}{\sum_{\operatorname{ht}(b)<X} 1} \gg (\log X)^{\log 2}.$$

Theorem 1.3. *We have that*

$$(\log X)^{\log 2} \ll \frac{\sum_{\operatorname{ht}(b)<X} \# \operatorname{Sel}_{\psi^\vee} A_b}{\sum_{\operatorname{ht}(b)<X} 1} \ll \log X.$$

Note that $\log 2 \approx 0.693$. Additionally, both Theorem 1.1 and Theorem 1.3 remain true even when finitely many congruence conditions are imposed on $B(\mathbb{Z})$: see Section 7 and Theorem 7.4.

Remark 1.4. We stress that the following results work for genus at least 2. For genus 1 we have $\phi = 1$, so in particular Theorem 1.1 is trivially true. However, the analogue of Theorems 1.2 and Theorem 1.3 is likely not true. What is known in these cases is that the average size of the Selmer group of a 2-isogeny in the given family $y^2 = x(x^2 + ax + b)$ diverges by [KL14, Corollary 1.2], and it is conjectured that it is $\asymp \sqrt{\log X}$. We will explain why we expect the genus 1 case to be different in Section 9.

Remark 1.5. We can compare the result of Theorem 1.1 with the Poonen–Rains heuristics in [PR12]. These heuristics contain some predictions for Selmer groups of self-dual isogenies $\lambda \colon A \to A^\vee$ which come from some symmetric line sheaf $\mathcal{L}$ in A. This is the case for all of our isogenies $\phi \colon A_b \to A_b^\vee$: ϕ is self-dual by Lemma 4.3, and the obstruction for ϕ to come from a symmetric line bundle is measured by an element $c_\phi \in H^1(A_b[\phi])$, which is zero in our case by [PR11, Proposition 3.12(f)]. Then, [PR12, Theorem 4.14] identifies $\mathrm{Sel}_\phi J_b$[1] with an intersection of two maximal isotropic subspaces of an infinite-dimensional quadratic space over $\mathbb{F}_2$. Then, Theorem 1.1 appears to be consistent with the predictions of the Poonen–Rains heuristics: the upper bound for our average size coincides with that of 2-Selmer groups of even hyperelliptic curves, which in both cases account for the presence of a marked rational subgroup of the Selmer group. However, we note that isogenies like ψ or ϕ_M are not self-dual, and thus do not fall within the framework of Poonen–Rains.

1.2 Method of proof

Many results on the average size of Selmer groups of isogenies that are multiplication-by-n have appeared in the literature in the past years, helped mainly by Bhargava's striking new methods in geometry-of-numbers: as seen for instance in [BS15a; BS15b; Lag24], among many others.

The standard technique in "Bhargavology" is to parametrise the elements of the Selmer groups by integral orbits of a representation (G, V) of a reductive group G defined over $\mathbb{Z}$. Finding such parametrisations is one of the main obstacles in obtaining more of these results. Previous experience suggests that many representations used in arithmetic statistics actually arise from Vinberg theory, or in other words the study of graded Lie algebras. In [Tho13], Thorne connected the Vinberg representations associated to the $\mathbb{Z}/2\mathbb{Z}$-gradings of the simply laced Lie algebras (i.e. those of type A_n, D_n or E_n) with certain families of curves arising as deformations of simple surface singularities, in such a way that the orbits of the representation should give arithmetic information about the constructed families of curves. This perspective has been used, implicitly and explicitly, to obtain statistical results on the size of 2-Selmer groups in the past: all these results have been unified and reproved in Laga's thesis [Lag24], which gives a uniform proof of all such results.

Other Vinberg representations have appeared in the literature, either coming from either non-simply laced Dynkin diagrams or higher order gradings (or both). In [RT21], a $\mathbb{Z}/3\mathbb{Z}$-grading in E_8 is used to study the 3-Selmer group of odd genus 2 curves. In [BES20], a $\mathbb{Z}/3\mathbb{Z}$-grading of G_2 was used to study 3-isogeny Selmer groups of the elliptic curves $y^2 = x^3 + k$, a perspective that was later generalised in [Bha+19] for abelian varieties. In [Lag24], a $\mathbb{Z}/2\mathbb{Z}$-grading in F_4 is used to study 2-Selmer groups of a family of Prym varieties, in a manner that serves as a template for our results.

We now explain the structure of this paper. First, in Section 2 we introduce the representations (G_B, V_B) and (G_C, V_C) arising from the stable 2-grading of the Dynkin diagrams B_{2n} and C_{2n}. Then, in Sections 3 and 5 we will show how the B and C-representations (respectively) are connected to the geometric picture of (1). First, we observe that the rings of invariants $\mathbb{Q}[V_B]^{G_B}$ and $\mathbb{Q}[V_C]^{G_C}$ are both isomorphic to an affine space $\mathbb{Q}[p_2, \dots, p_{4n}]$, where p_{2i} has degree $2i$. Therefore, any element of $V_B(\mathbb{Q})$ or $V_C(\mathbb{Q})$ can be associated to the hyperelliptic curve $C_b \colon y^2 = x(x^{2n} + p_2 x^{2n-1} + \dots + p_{4n})$. The most important results of Sections 3 and 5 are the construction of embeddings

$$\mathrm{Sel}_\psi J_b \hookrightarrow (G_B(\mathbb{Q}) \backslash V_{B,b}(\mathbb{Q})) \bigcap \frac{1}{2} V_B(\mathbb{Z}), \quad \mathrm{Sel}_{\psi^\vee} A_b \hookrightarrow (G_C(\mathbb{Q}) \backslash V_{C,b}(\mathbb{Q})) \bigcap \frac{1}{2} V_C(\mathbb{Z}),$$

where $V_{B,b}$ and $V_{C,b}$ denote the elements of V_B and V_C having invariants $b \in B$.

[1] The cited [PR12, Theorem 4.14] only identifies a *quotient* of $\mathrm{Sel}_\phi J_b$ as an intersection, but that quotient is equal to $\mathrm{Sel}_\phi J_b$ 100% of the time by [PR12, Proposition 3.4], using the fact that $A_b[\phi]$ is isomorphic to the 2-torsion of the Jacobian of $y^2 = f(x)$.

Additionally, connected to the B-representation, in Section 4 we will consider a related representation (G_A, V_A), for which will have $V_A /\!\!/ G_A \simeq B$ and a commutative diagram

$$\begin{array}{ccc} \mathrm{Sel}_\psi J_b & \longrightarrow & \mathrm{Sel}_\phi A_b \\ \downarrow & & \downarrow \\ G_B(\mathbb{Q})\backslash V_{B,b}(\mathbb{Q}) & \longrightarrow & G_A(\mathbb{Q})\backslash V_{A,b}(\mathbb{Q}), \end{array}$$

where again the rightmost map is injective and every element in its image has a representative in $\frac{1}{2}V_{A,b}(\mathbb{Z})$. It turns out that the representation (G_A, V_A) is the Vinberg representation associated to the $\mathbb{Z}/2\mathbb{Z}$-grading on A_{2n-1}, which has already been studied in [SW18]. Therefore, in Section 7 we can use the counting results of *loc. cit.* to prove Theorem 1.1.

In Section 6, we develop the necessary methods in geometry-of-numbers to prove the upper bound of Theorem 1.3. We note that $G_C = \mathrm{GL}_{2n}/\mu_2$ is not semisimple, something that differs from the cases typically considered in the literature and which introduces further technical complications. Then, in Section 8 we complete the proof of Theorems 1.2 and 1.3 by looking at the Greenberg–Wiles formula, which relates the size of the Selmer groups and their dual to a product of ratios of Tamagawa numbers. Finally, in Section 9 we give heuristics with matrix models, similarly to Poonen–Rains [PR12], to explain what the correct orders of growth of the different average sizes of the Selmer groups should be.

1.3 Acknowledgements

This paper is a version of part of the author's PhD thesis, written under the supervision of Jack Thorne. I would like to thank him for his many helpful comments and conversations. I would also like to thank Alex Bartel, Jef Laga and Rong Zhou for interesting discussions related to the contents of this paper.

2 Vinberg representations for B_{2n} and C_{2n}

We introduce some generalities about Vinberg representations, which will be later specialised to the case of $\mathbb{Z}/2\mathbb{Z}$-gradings for the Dynkin diagrams of type B_{2n} and C_{2n}. For more general context, the reader may consult [Vin76; Pan05; Ree+12].

Let H be a connected simple reductive group of adjoint type over a field K of characterstic zero. Let $\theta\colon H \to H$ be an involution. By taking differentials, it also induces an involution $d\theta$ on the Lie algebra $\mathfrak{h}$ of H. By considering ± 1 eigenspaces, we get a decomposition

$$\mathfrak{h} = \mathfrak{h}(0) \oplus \mathfrak{h}(1),$$

where $\mathfrak{h}(0) = \mathfrak{h}^{d\theta=1}$ and $\mathfrak{h}(1) = \mathfrak{h}^{d\theta=-1}$. We observe that $[\mathfrak{h}(i), \mathfrak{h}(j)] \subset \mathfrak{h}(i+j)$. If we take $G = (H^\theta)^\circ$ and $V = \mathfrak{h}(1)$, we get a representation (G, V) by taking the restriction of the adjoint representation. Of course, this representation depends on the choice of θ, but there turns out to be a "canonical" choice: the one that makes the representation *stable* in the following sense:

Definition 2.1. Suppose that K is algebraically closed. Then a vector $v \in V$ is *stable* if the G-orbit of v is closed and its stabiliser $\mathrm{Stab}_G(v)$ is finite. We say (G, V) is *stable* if V contains stable vectors. Finally, if K is not necessarily closed, we say that (G, V) is *stable* if (G_{K^s}, V_{K^s}) is.

Stable vectors have a good invariant theory (cf. [Lag24, Proposition 2.11]):

Proposition 2.2. *Suppose that $\theta\colon H \to H$ is a stable involution, with associated Vinberg representation (G, V). Then the following properties are satisfied:*

1. *Let $\mathfrak{c} \subset V$ be a Cartan subalgebra of $\mathfrak{h}$. Then the map $N_G(\mathfrak{c}) \to W_{\mathfrak{c}} := N_H(\mathfrak{c})/Z_H(\mathfrak{c})$ is surjective. Consequently, the inclusions $\mathfrak{c} \subset V \subset \mathfrak{h}$ induce isomorphisms*

$$\mathfrak{c} /\!\!/ W_{\mathfrak{c}} \simeq V /\!\!/ G \simeq \mathfrak{h} /\!\!/ H.$$

   In particular, the above quotients are isomorphic to an affine space.

2. *Let K be algebraically closed and let $x, y \in V(K)$ be regular semisimple elements. Then x and y are $G(K)$-conjugate if and only if they have the same image in $V /\!\!/ G$.*

Proposition 2.3. *[Tho13, Lemma 2.6] Let K be algebraically closed. Then there exists a unique $H(K)$-conjugacy class of stable involutions θ.*

Even if K is not necessarily algebraically closed, there always exists a choice of stable involution θ defined over K. This follows from [LR25, Example 2.20] and the fact that the outer automorphism group of both B_{2n} and C_{2n} is trivial. Moreover, θ can be constructed explicitly: to do so, fix a pinning $(T, P, \{X_\alpha\})$ of H, containing:

- $T \subset H$, a split maximal torus (determining a root system Φ_H);
- $P \subset H$, a Borel subgroup containing T (determining a root basis $S_H \subset \Phi_H$);
- X_α, a generator for $\mathfrak{h}_\alpha$ for each $\alpha \in S_H$.

Let $\check{\rho}$ be the sum of fundamental coweights with respect to S_H, and define

$$\theta = \mathrm{Ad}(\check{\rho}(-1)).$$

Then it follows from [Ree+12, Corollary 14] that θ is a stable grading. We now describe both representations explicitly, which we will denote as (G_B, V_B) and (G_C, V_C).

2.1 The B_{2n} representation

Let J_m denote the $m \times m$ matrix with 1s in the antidiagonal and 0s elsewhere. Define $H = \mathrm{SO}(J_m) = \{A \in \mathrm{SL}_m \mid {}^tAJA = J\}$. From now on, we will simply denote $\mathrm{SO}_m := \mathrm{SO}(J_m)$. If X is an $m \times n$ matrix, let us define $X^* = J_n {}^tX J_m$ (if $m = n$, this is simply reflection across the antidiagonal). We have

$$\mathfrak{h} = \left\{ \begin{pmatrix} B & A \\ -A^* & C \end{pmatrix} \middle| A \in \mathrm{Mat}_{(2n+1)\times 2n}, B \in \mathrm{Mat}_{(2n+1)\times(2n+1)}, C \in \mathrm{Mat}_{2n\times 2n}, B = -B^*, C = -C^* \right\}.$$

The 2-grading is given by

$$\mathfrak{h}(0) = \left\{ \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \in \mathfrak{h} \right\}, \quad \mathfrak{h}(1) = \left\{ \begin{pmatrix} 0 & A \\ -A^* & 0 \end{pmatrix} \in \mathfrak{h} \right\}.$$

The group G_B can be identified with $\mathrm{SO}_{2n+1} \times \mathrm{SO}_{2n}$, and $V_B = \mathfrak{h}(1)$ can be identified with $(2n+1) \boxtimes 2n$, the vector space of $(2n+1) \times 2n$ matrices, and the action of $(g, h) \in G_B$ on a matrix $A \in V_B$ can be given by gAh^{-1}.

We note that if the $(2n) \times (2n)$ matrix A^*A has characteristic polynomial $f(x) = x^{2n} + p_2 x^{2n-1} + \cdots + p_{4n}$, then the $(2n+1) \times (2n+1)$ matrix AA^* has characteristic polynomial $xf(x)$. The coefficients $p_2, \ldots, p_{4n}$ are all invariants of the representation, satisfying $p_{2i}(\lambda v) = \lambda^{2i} p_{2i}(v)$ for all $i = 1, \ldots, 2n$ and all $\lambda \in K^\times$. Let $B := V_B /\!\!/ G_B = \operatorname{Spec} K[V_B]^{G_B}$ be the GIT quotient. The following lemma holds due to general facts of Vinberg theory (see [Pan05, Corollary 3.6]):

Proposition 2.4. *We have that $B \cong \operatorname{Spec} K[p_2, \ldots, p_{4n}]$.*

We will write $\pi\colon V_B \to B$ for the invariant map, and we will write $V_{B,b}(K)$ for those elements in $V(K)$ with invariants $b \in B(K)$. We will also define the *discriminant* Δ of an element $b \in B(K)$ corresponding to the polynomial $f(x) = x^{2n} + p_2 x^{2n-1} + \cdots + p_{4n}$ as the discriminant of the polynomial $xf(x^2)$, and similarly define the discriminant of an element $v \in V_B(K)$ as the discriminant of $\pi(v)$. We will use the subscript V_B^{rs} to distinguish those elements that are regular semisimple (i.e. $\Delta(v) \neq 0$), and we will also write B^{rs} for $\pi(V_B^{rs})$, which is equivalently the set of elements of B with non-zero discriminant.

2.2 The C_{2n} representation

Let $H := \mathrm{PSp}_{4n} = \mathrm{Sp}_{4n}/\mu_2$, where

$$\mathrm{Sp}_{4n} := \{M \in \mathrm{Mat}_{4n\times 4n} \mid M^t \Omega M = \Omega\}, \quad \Omega = \begin{pmatrix} 0 & J_{2n} \\ -J_{2n} & 0 \end{pmatrix}.$$

Let $\mathfrak{h}$ be the Lie algebra of H; explicitly:

$$\mathfrak{h} = \left\{ X = \begin{pmatrix} B & A \\ C & -B^* \end{pmatrix} \middle| A, B, C \in \mathrm{Mat}_{2n\times 2n}, A = A^*, C = C^* \right\}.$$

Then the $\mathbb{Z}/2\mathbb{Z}$ grading is:

$$\mathfrak{h}(0) = \left\{ \begin{pmatrix} B & 0 \\ 0 & -B^* \end{pmatrix} \in \mathfrak{h} \right\}, \quad \mathfrak{h}(1) = \left\{ \begin{pmatrix} 0 & A \\ C & 0 \end{pmatrix} \in \mathfrak{h} \right\}.$$

The Vinberg representation (G_C, V_C) is obtained by taking $G_C = (H^\theta)^0$, here identified with $G_C = \mathrm{GL}_{2n}/\mu_2$ and $V_C = \mathfrak{h}(1)$, where G acts by restriction of the adjoint representation. Explicitly, given $g \in G_C$ and $(A, C) \in V_C$, the action is given by $g \cdot (A, C) = (gAg^*, (g^{-1})^* C g^{-1})$.

If the characteristic polynomial of the product of matrices AC is of the form $x^{2n} + p_2 x^{2n-1} + \cdots + p_{4n}$, then the coefficients $p_2, \ldots, p_{4n}$ are invariant under the action of G_C. Let $B := V_C /\!\!/ G_C$. Then, by [Pan05, Corollary 3.6], these are all the invariants of the representation, i.e. $B = \operatorname{Spec} K[p_2, \ldots, p_{4n}]$, and the corresponding ring of polynomials is freely generated. Note that $V_B /\!\!/ G_B$ and $V_C /\!\!/ G_C$ are isomorphic: we denote both spaces by B.

Similarly to before, we write $\pi\colon V_C \to B$ for the invariant map, and $V_{C,b}(K)$ for the elements in $V_C(K)$ mapping to $b \in B(K)$. The discriminant Δ of an element $b \in B(K)$ is the same as in the B_{2n} case, and we similarly define the discriminant of an element $v \in V_C(K)$ as the discriminant of $\pi(v)$. We will use the subscript V_C^{rs} to distinguish those elements that are regular semisimple.

3 Orbit parametrisations for B_{2n}

In this section, we classify the rational and integral orbits of the representation (G_B, V_B), and we connect these orbits to elements of the Selmer group $\mathrm{Sel}_\psi J$ defined in the introduction. To lighten the notation, for this section let us denote $(G, V) = (G_B, V_B)$. We fix throughout a field K of characteristic 0.

3.1 Rational orbits

In general, a $G(K^s)$-orbit of elements in $V(K)$ might break up into multiple $G(K)$-orbits in $V(K)$. We have the following general result from arithmetic invariant theory (see [BG14, Proposition 1]) indicating how this phenomenon can be studied with Galois cohomology groups:

Proposition 3.1. *Let $v \in V(K)$. The set of $G(K)$-orbits in $V(K)$ which are $G(K^s)$-conjugate to v is in bijection with the kernel of the map*

$$H^1(K, \mathrm{Stab}_G(v)) \to H^1(K, G)$$

of pointed sets.

In this section, we will first explain how to construct a given "distinguished" orbit v, and then we will show how to construct from it all the rational orbits with given invariants from an element $\alpha \in \ker(H^1(K, \mathrm{Stab}_G(v)) \to H^1(K, G))$.

A distinguished orbit

Let $b = (p_2, \dots, p_{4n}) \in B(K)$, and consider the polynomial $f(x) = x^{2n} + p_2 x^{2n-1} + \cdots + p_{4n}$. Define the K-vector space $M = K[x]/(xf(x^2)) = K[\beta]$, where β denotes the image of x inside M. Note that M is spanned by the K-linear combinations of $1, \beta, \dots, \beta^{4n}$. Define the bilinear form $(\cdot, \cdot)\colon M \times M \to K$ by:

$$(\lambda, \mu) = \text{ coefficient of } \beta^{4n} \text{ in } \lambda\mu.$$

Let $L_1 = K[x]/(xf(x))$ and let $L_2 = K[x]/(f(x))$. Then, M is isomorphic to $L_1 \oplus \beta L_2$, where there is a natural inclusion $L_1 \hookrightarrow M$ by sending $x \mapsto x^2$. In other words, L_1 is the subspace spanned by $\{1, \beta^2, \dots, \beta^{4n}\}$ and βL_2 is spanned by $\{\beta, \beta^3, \dots, \beta^{4n-1}\}$. Then, the form $(\cdot, \cdot)$ splits as a direct sum of bilinear forms in L_1 and βL_2. Using the explicit power bases, we can see that both quadratic forms on L_1 and L_2 have discriminant 1 and are in fact split, so we can isometrically identify L_1 with a quadratic space (W_1, J_{2n+1}) of dimension $2n+1$ and L_2 with a quadratic space (W_2, J_{2n}) of dimension $2n$.

Let W be the quadratic space given by $(W_1, J_{2n+1}) \oplus (W_2, J_{2n})$, and consider the multiplication-by-β map $T_\beta\colon M \to M$, which can also be seen as a map from W to W. Given that T_β is self-adjoint with respect to $(\cdot, \cdot)$, we get that the matrix of T_β on W is of the form

$$\left(\begin{array}{c|c} 0_{(2n+1)\times(2n+1)} & A \\ \hline A^* & 0_{2n\times 2n} \end{array}\right),$$

where $A \in \mathrm{Mat}_{(2n+1)\times(2n)}$. Thus, we get an element $v \in V(K)$ with invariants $b \in B(K)$ by construction. We also observe the following:

Proposition 3.2. *Let $v \in V(K)$ be the orbit previously constructed, and assume that $\Delta(v) \neq 0$. Then, the stabiliser $\mathrm{Stab}_G(v)$ is isomorphic to the kernel of the norm map $\mathrm{Res}_{L_2/K}\,\mu_2 \to \mu_2$.*

Proof. Given that v is regular semisimple, the centraliser of T_β in $\mathrm{GL}(M)$ is $M^\times$. Since the centraliser actually lies inside $\mathrm{SO}(M)$, this forces elements $\lambda \in M^\times$ to satisfy $\lambda^2 = 1$. Moreover, because λ needs to preserve both L_1 and βL_2, we see that $\lambda \in L_1^\times$. Finally, the fact that $\lambda \in \mathrm{SO}(W_1) \times \mathrm{SO}(W_2)$ forces $N_{L_1/K}(\lambda) = 1$ and $N_{L_2/K}(\overline{\lambda}) = 1$, where $\overline{\lambda}$ is the image of λ in L_2.

The conclusion is that the stabiliser is in bijection with the set of elements of $\mathrm{Res}_{L_1/K}\,\mu_2$ whose norm is 1 and whose image in L_2 also has norm 1. This can be identified with $\ker(\mathrm{Res}_{L_2/K}\,\mu_2 \to \mu_2)$, and so we are done. □

We will denote the kernel of the map $\mathrm{Res}_{L_2/K}\,\mu_2 \to \mu_2$ by $(\mathrm{Res}_{L_2/K}\,\mu_2)_{N=1}$.

The other orbits

Let $G' = \mathrm{SO}_{2n+1} \times \mathrm{O}_{2n}$. We will start by explaining how to construct all the diferent $G'(K)$-orbits, and then we will specialise to $G(K)$-orbits. Note that given $v \in V(K)$ with $\Delta(v) \neq 0$, we have that $\mathrm{Stab}_{G'}(v) \cong$

$\operatorname{Res}_{L_2/K}\mu_2$, and that $H^1(K, \operatorname{Res}_{L_2/K}\mu_2) \cong L_2^\times/L_2^{\times 2}$. We also observe that the pointed set $H^1(K, \mathrm{SO}_m)$ parametrises non-degenerate quadratic spaces of dimension m and discriminant 1, and that the trivial element of $H^1(K, \mathrm{SO}_m)$ corresponds to the (unique) split orthogonal space of dimension m. Similarly, the pointed set $H^1(K, \mathrm{O}_m)$ classifies non-degenerate quadratic spaces of dimension m, with a similar trivial element. The map $H^1(K, \mathrm{SO}_m) \to H^1(K, \mathrm{O}_m)$ has trivial kernel as a map of pointed sets, as can be seen from the usual long exact sequence in group cohomology of

$$1 \longrightarrow \mathrm{SO}_m \longrightarrow \mathrm{O}_m \xrightarrow{det} \{\pm 1\} \longrightarrow 1.$$

In fact, $H^1(K, \mathrm{SO}_m) \to H^1(K, \mathrm{O}_m)$ is injective (cf. [Knu+98, §29.E]).

Given $\alpha \in (L_2^\times/L_2^{\times 2})$ mapping to the trivial element in $H^1(K, G')$, we will show how to construct a rational orbit from it. An element $\alpha \in L_2^\times$ can be lifted to an element of $L_1^\times \cong K^\times \times L_2^\times$ by simply considering $(1, \alpha) \in L_1^\times$. Moreover, as in last section, we can naturally embed $L_1 \hookrightarrow M$, so given $\alpha \in (L_2^\times/L_2^{\times 2})$ we can naturally consider it as an element of M. Under this identification, consider the quadratic form $(\cdot,\cdot)_\alpha \colon M \times M \to K$ defined by

$$(\lambda, \mu)_\alpha = \text{ coefficient of } \beta^{4n} \text{ in } \alpha^{-1}\lambda\mu. \tag{2}$$

As before, this quadratic form splits as a direct sum of quadratic forms in L_1 and βL_2. If α has norm 1 (up to squares) in L_2, then both forms have discriminant 1, so they give a well-defined map to $H^1(K, G')$. Unwinding the definitions similarly to [BG14, §5], the condition that α lands in the kernel of $H^1(K, G')$ translates precisely to both forms $(\cdot,\cdot)_\alpha|_{L_1}$ and $(\cdot,\cdot)_\alpha|_{\beta L_2}$ being split of discriminant 1. Therefore, under appropriate change of bases in L_1 and L_2, the map T_β given an element of $V(K)$ in the same way as in the distinguished case.

Thus, given $\alpha \in (L_2^\times/L_2^{\times 2})_{N\equiv 1}$ which maps to the trivial element of $H^1(K, G')$, we have constructed a rational $G'(K)$-orbit. We now turn our attention to $G(K)$-orbits. Following [BGW15, §4.3], there is a map

$$H^1(K, (\operatorname{Res}_{L_2/K}\mu_2)_{N=1}) \to (L_2^\times/L_2^{\times 2})_{N\equiv 1}$$

which is either bijective or 2-to-1, according to whether $f(x)$ has an odd degree factor over K or not, which in turn depends on whether $L_2^\times[2]$ has an element of norm -1 or not. Therefore, a $G'(K)$-orbit in $V(K)$ splits in either one or two $G(K)$-orbits. In the case where $f(x)$ does not have an odd degree factor over K, we note that the stabiliser over K of the constructed v in $\mathrm{SO}_{2n+1} \times \mathrm{SO}_{2n}$ is the same as the stabiliser in $\mathrm{SO}_{2n+1} \times \mathrm{O}_{2n}$. By choosing $h \in \mathrm{O}_{2n}(K) \backslash \mathrm{SO}_{2n}(K)$, we can obtain a new orbit by just considering the element $(1, h) \cdot v$. If $f(x)$ has an odd degree factor over K, these two constructed orbits coincide. We summarise our results as follows:

Theorem 3.3. *Let $b \in B(K)$ with $\Delta(b) \neq 0$. Then the set of $G(K)$-orbits in $V_b(K)$ is in bijection with the set of equivalence classes (α, s), where $\alpha \in (L_2^\times)_{N\equiv 1}$ maps to the trivial element in $H^1(K, G)$ and $s \in K^\times$ satisfies $N(\alpha) = s^2$. Two pairs (α, s) and (α', s') are equivalent if there exists $c \in L_2^\times$ such that $\alpha' = c^2\alpha$ and $s' = N(c)s$. The stabiliser of such an orbit is isomorphic to* $(\operatorname{Res}_{L_2/K}\mu_2)_{N=1}$.

3.2 Connection with hyperelliptic curves

Let $b \in B^{rs}(K)$ correspond to the polynomial $f(x) \in K[x]$ with $\deg f = 2n$. Consider the hyperelliptic curve $C_b \colon y^2 = xf(x)$ and its Jacobian $J_b := \operatorname{Jac}(C_b)$. If the discriminant of $xf(x)$ is non-zero, then the roots $x_0 = 0, x_1, \ldots, x_{2n}$ of $xf(x)$ over $\overline{K}$ are all different. If we denote $P_i = (x_i, 0)$ and ∞ is the point at infinity, then $J_b[2](\overline{K})$ is generated by the elements $[(P_i) - \infty]$, with the only relation that $\sum_{i=0}^{2n}[(P_i) - \infty] = 0$.

Consider the order 2 subgroup $M \subset J_b[2]$ generated by $P_0 = (0, 0)$, and consider its orthogonal complement $M^\perp$ under the Weil pairing. For convenience, we can give an explicit description of $M^\perp(\overline{K})$: every element of $J_b[2]$ can be written uniquely as a sum $[(P_0) - \infty] + \sum_{i\in I}[(P_i) - \infty]$ for some subset $I \subset \{1, \ldots, 2n\}$.

Then, $M^{\perp}(\overline{K})$ consists of elements of this form such that $|I|$ is even. Note that $M^{\perp}(\overline{K})$ has size 2^{2n-1} and that $M \leqslant M^{\perp}$. We can construct some isogenies as in (1):

$$J_b \xrightarrow{\phi_M} A_b \xrightarrow{\phi} A_b^{\vee} \xrightarrow{\phi_M^{\vee}} J_b,$$

with $J_b[\phi_M] = M$, if $\psi = \phi \circ \phi_M$ then $J_b[\psi] = M^{\perp}$ and the whole composition is the multiplication-by-2 map.

Proposition 3.4. *Let $v \in V(K)$ with $\Delta(v) \neq 0$. Then $\mathrm{Stab}_G(v) \cong J_b[\psi]$.*

Proof. It suffices to show that $J_b[\psi] \cong (\mathrm{Res}_{L_2/K}\,\mu_2)_{N=1}$, which is an elementary computation. □

Note that we also have that we have the injective descent map $A_b^{\vee}(K)/\psi(J_b(K)) \hookrightarrow H^1(K, J_b[\psi])$. It is then natural to ask whether the elements of $A_b^{\vee}(K)/\psi(J_b(K))$ actually correspond to $G_b(K)$-orbits in $V_b(K)$. We now state the main theorem of this section.

Theorem 3.5. *The natural composition*

$$A_b^{\vee}(K)/\psi(J_b(K)) \xrightarrow{\eta_b} H^1(K, J_b[\psi]) \to H^1(K, G)$$

is trivial.

Definition 3.6. We will say an element $v \in V^{rs}(K)$ is *K-soluble* if $v \in \eta_b(A_b^{\vee}(K)/\psi(J_b(K)))$.

It is not so obvious what an explicit description of the map $A_b^{\vee}(K)/\psi(J_b(K)) \to H^1(K, J_b[\psi])$ should be. However, we can try to simplify the situation by trying to relate it to the 2-descent map $J_b(K)/2J_b(K) \to H^1(K, J_b[2])$. Consider the group $G' = \mathrm{SO}_{2n+1} \times \mathrm{O}_{2n}$: similarly to Proposition 3.4, we can see that $\mathrm{Stab}_{G'}(v) \cong \mathrm{Res}_{L_1/K}(\mu_2) \cong J_b[2]$. We then have the following commutative diagram:

$$\begin{array}{ccc} A_b^{\vee}(K)/\psi(J_b(K)) & \longrightarrow & J_b(K)/2J_b(K) \\ \downarrow{\scriptstyle \delta_\psi} & & \downarrow{\scriptstyle \delta_2} \\ H^1(K, J_b[\psi]) & \xrightarrow{\iota} & H^1(K, J_b[2]) \\ \downarrow & & \downarrow \\ H^1(K, G) & \longrightarrow & H^1(K, G') \end{array} \tag{3}$$

The map $H^1(K, J_b[2]) \to H^1(K, G') \cong H^1(K, \mathrm{SO}_{2n+1}) \times H^1(K, \mathrm{O}_{2n})$ can be given using the same recipe as in Section 3.1. Explicitly, given $\alpha \in H^1(K, J_b[2])$, which can be viewed both as an element of $L_2^{\times}/L_2^{\times 2}$ and as an element of $(L_1^{\times}/L_1^{\times 2})_{N\equiv 1}$ via $\alpha \mapsto (N_{L_2/K}(\alpha), \alpha) \in K^{\times} \times L_2^{\times} \cong L_1^{\times}$, we obtain two quadratic spaces $(\cdot,\cdot)_{\alpha}^{(1)} \colon L_1 \times L_1 \to K$ and $(\cdot,\cdot)_{\alpha}^{(2)} \colon L_2 \times L_2 \to K$ given by

$$(\mu, \lambda)_{\alpha}^{(1)} = \text{ coefficient of } \beta_1^{2n} \text{ in } \alpha^{-1}\mu\lambda \text{ (inside } L_1)$$

and

$$(\mu, \lambda)_{\alpha}^{(2)} = \text{ coefficient of } \beta_2^{2n-1} \text{ in } \alpha^{-1}\mu\lambda \text{ (inside } L_2),$$

where we are writing $L_1 = K\langle 1, \beta, \ldots, \beta^{2n}\rangle$ and $L_2 = K\langle 1, \beta, \ldots, \beta^{2n-1}\rangle$. Alternatively, if we consider the codimension 1 vector subspace $\beta_1 L_1$ of L_1, we have that $(\cdot,\cdot)_{\alpha}^{(2)}$ is equivalent to a form $(\cdot,\cdot)_{\alpha}^{(2')} \colon \beta_1 L_1 \times \beta_1 L_1 \to K$ given by $(\beta_1\mu, \beta_1\lambda)_{\alpha}^{(2')} := (\mu, \beta_1\lambda)_{\alpha}^{(1)}$ (we can check that this is well-defined).

The image of $\alpha \in H^1(K, J_b[2])$ in $H^1(K, \mathrm{SO}_{2n+1}) \times H^1(K, \mathrm{O}_{2n})$ is given by the quadratic spaces $(L_1, (\cdot,\cdot)_{\alpha}^{(1)})$ and $(L_2, (\cdot,\cdot)_{\alpha}^{(2)})$, and these quadratic spaces will correspond to the trivial element if and only if they are split of discriminant 1. We note that the discriminant of $(\cdot,\cdot)_{\alpha}^{(1)}$ is 1, while the discriminant of $(\cdot,\cdot)_{\alpha}^{(2)}$ is equal to

$N_{L_2/K}(\alpha)$. Therefore, it is not necessarily the case that the composition $J_b(K)/2J_b(K) \xrightarrow{\delta_2} H^1(K, J_b[2]) \to H^1(K, G')$ is trivial: it is a necessary condition that $N_{L_2/K}(\alpha) \in K^{\times 2}$.

Recall that there is a surjective map $H^1(K, J_b[\psi]) \to (L_2^\times/L_2^{\times 2})_{N\equiv 1}$, which is either bijective or 2-to-1. Then, the map $\iota\colon H^1(K, J_b[\psi]) \to H^1(K, J_b[2]) \cong L_2^\times/L_2^{\times 2}$ is just given by the natural inclusion $H^1(K, J_b[\psi]) \to (L_2^\times/L_2^{\times 2})_{N\equiv 1} \to L_2^\times/L_2^{\times 2}$.

Lemma 3.7. *Let $[D] \in J_b(K)/2J_b(K)$, and suppose that $\delta_2([D]) \in \mathrm{Im}(\iota)$. Then the image of $\delta_2([D])$ in $H^1(K, G')$ is trivial.*

Proof. We start by recounting the proof of [BG13, Proposition 5.2]. Consider the two quadrics in $L_1 \oplus K$ given by

$$Q_1(\lambda, a) = (\lambda, \lambda)^{(1)}_\alpha, \quad Q_2(\lambda, a) = (\lambda, \beta_1\lambda)^{(1)}_\alpha + a^2.$$

Then, it is shown in loc. cit. that there exists a rational n-dimensional subspace Y of $L_1 \oplus K$ which is isotropic with respect to both Q_1 and Q_2. In particular, given that the line $0 \oplus K$ is not contained in Y, we see that the projection of Y to L_1 is an n-dimensional isotropic subspace of Q_1, thus showing that $(\cdot,\cdot)^{(1)}_\alpha$ is split.

Now, consider the subspace $Y' = Y \cap (L_1 \oplus 0)$, of dimension at least $n-1$. We see that $Y' \cap f(\beta_1)L_1 = \{0\}$, as $(f(\beta_1), f(\beta_1))^{(1)}_\alpha = N_{L_2/K}(\alpha^{-1})N_{L_2/K}(\beta_1) \neq 0$. Therefore, the subspace $\beta_1 Y'$ of $\beta_1 L_1$ has dimension at least $n-1$, and it is also the case that for any $\beta_1\mu, \beta_1\lambda \in \beta_1 Y'$ we have that $(\beta_1\mu, \beta_1\lambda)^{(2')}_\alpha = (\mu, \beta_1\lambda)^{(1)}_\alpha = 0$ by construction. Therefore, $(\cdot,\cdot)^{(2)}_\alpha$ has a rational isotropic space of dimension $n-1$ and thus, as a quadratic space, we have that $(L_2, (\cdot,\cdot)^{(2)}_\alpha) \cong H^{n-1} \oplus V'$, where $H \sim \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$. But V' is a quadratic space of dimension 2 and discriminant 1 (by hypothesis), and therefore $V' \sim H$ as well, showing that $(\cdot,\cdot)^{(2)}_\alpha$ is split, as wanted. ☐

Proof of Theorem 3.5. First, note that the map $H^1(K, G) \to H^1(K, G')$ has a trivial pointed kernel, which is equivalent to $H^1(K, \mathrm{SO}_{2n}) \to H^1(K, \mathrm{O}_{2n})$ having a trivial pointed kernel, as noted in Section 3.1. Then, the proof follows from Lemma 3.7 and the commutativity of the diagram (3). ☐

Remark 3.8. Let $A_b^\vee[\hat{\psi}] = \{0, T_A\}$. Then, both 0 and T_A give distinguished orbits of $G(K)\backslash V_b(K)$. Whether or not these two orbits coincide depends on whether $T_A \in \psi(J_b(K))$.

Corollary 3.9. *Let K be a number field, and let $b \in B(K)$ with $\Delta(b) \neq 0$. Then there is an embedding*

$$\mathrm{Sel}_\psi(J_b) \hookrightarrow G(K)\backslash V_b(K).$$

Proof. Consider the commutative diagram

$$\begin{array}{ccccc} A_b^\vee(K)/\psi(J_b(K)) & \longrightarrow & H^1(K, J_b[\psi]) & \longrightarrow & H^1(K, G) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_v A_b^\vee(K_v)/\psi(J_b(K_v)) & \xrightarrow{\delta_{\psi,v}} & \prod_v H^1(K_v, J_b[\psi]) & \longrightarrow & \prod_v H^1(K_v, G), \end{array}$$

where the product is taken over all finite places v of K. Recall that $\mathrm{Sel}_\psi(J_b)$ is defined as the kernel of the map $H^1(K, J_b[\psi]) \to \prod_v H^1(K_v, J_b[\psi])/(\mathrm{Im}(\delta_{\psi,v}))$. Our statement then follows from the fact that the composition of maps in the second row is trivial by Theorem 3.5, and the fact that the map $H^1(K, G) \to \prod_v H^1(K_v, G)$ has trivial kernel by [Lag24, Proposition 6.8]. ☐

3.3 Integral orbits

To prove our main theorems, we will require an integral version of Corollary 3.9. We remark that even though we have originally constructed our representation over K, a field of characteristic zero, we could also have constructed (G, V) over $\mathbb{Z}$. In this case, we also have $V /\!\!/ G = B = \operatorname{Spec}\mathbb{Z}[p_2, \dots, p_{4n}]$.

Theorem 3.10. *Every element in the image of the map*

$$\mathrm{Sel}_\psi(J_b) \hookrightarrow G(\mathbb{Q})\backslash V_b(\mathbb{Q}).$$

has a representative in $\frac{1}{2}V_b(\mathbb{Z})$.

Because G has class number 1 (cf. [Lag24, Proposition 7.2]), it will suffice to see that the map

$$A_b^\vee(\mathbb{Q}_p)/\psi(J(\mathbb{Q}_p)) \hookrightarrow G(\mathbb{Q}_p)\backslash V_b(\mathbb{Q}_p)$$

falls inside the image of the inclusion map $\frac{1}{2}V_b(\mathbb{Z}_p) \to G(\mathbb{Q}_p)\backslash V_b(\mathbb{Q}_p)$ for all primes p. We start by giving an ideal parametrisation of integral orbits inside $\mathbb{Z}_p$, in an analogous way to other results in the literature, such as [Sha19, Proposition 6.7]. For the proof of Theorem 3.10, we will need to know when a $\mathbb{Z}_p$-lattice L of dimension m with a given symmetric bilinear form $L \times L \to \mathbb{Z}_p$ is isometric over $\mathbb{Z}_p$ to an m-dimensional lattice L_m with matrix J_m. We summarise known results on this next lemma:

Lemma 3.11. *Let I be a free $\mathbb{Z}_p$-module of rank m equipped with a symmetric bilinear form $\varphi\colon I \times I \to \mathbb{Z}_p$ of discriminant* 1.

- *If $p \neq 2$, then I is isometric to L_m over $\mathbb{Z}_p$.*
- *If $p = 2$ and $m = 2m' + 1$, then I is isometric to L_m over $\mathbb{Z}_2$ if $I \otimes \mathbb{Q}_2$ is a split orthogonal space.*
- *If $p = 2$ and $m = 2m'$, then I is isometric to L_m over $\mathbb{Z}_2$ if $I \otimes \mathbb{Q}_2$ is a split orthogonal space and I is an even lattice (i.e. $\varphi(x, x) \in 2\mathbb{Z}_2$ for all $x \in I$).*

In the last item, the condition that I is an even lattice is necessary, as (L_m, J_m) admits both an even and an odd lattice over $\mathbb{Z}_2$. These two lattices can be transformed to one another via an element of $\mathrm{O}_m(\mathbb{Q}_2)$ with coefficients in $\frac{1}{2}\mathbb{Z}_2$.

Proposition 3.12. *Let $b \in B(\mathbb{Z}_p)$ with $\Delta(b) \neq 0$. Then the set of orbits $G(\mathbb{Z}_p)\backslash V_b(\mathbb{Z}_p)$ is in bijection with the set of equivalence classes of (I_1, I_2, α, s), where I_1 is a fractional ideal of R_1, I_2 is a fractional ideal of R_2, $\alpha \in (L_2^\times)_{N\equiv 1}$ and $s \in \mathbb{Q}_p^\times$; satisfying:*

1. *$I_1^2 \subset \alpha R_1$ and $N(I_1)^2 = N_{L_1/\mathbb{Q}_p}(\alpha)$, where α can be interpreted as an element of $L_1 \cong \mathbb{Q}_p \times L_2$ via $\alpha \mapsto (N_{L_2/\mathbb{Q}_p}(\alpha), \alpha)$.*
2. *$I_2^2 \subset \alpha R_2$ and $N(I_2)^2 = N_{L_2/\mathbb{Q}_p}(\alpha)$.*
3. *Let $\overline{I_1}$ denote the projection of I_1 in L_2, and let $\overline{I_1}' = \{\gamma \in L_2 \mid (0, \beta_1\gamma) \in I_1\}$. Then $\overline{I_1} \subset I_2 \subset \overline{I_1}'$.*
4. *The forms $(\cdot,\cdot)_\alpha^{(1)}$ and $(\cdot,\cdot)_\alpha^{(2)}$ are split of discriminant 1 over $\mathbb{Q}_p$.*
5. *I_2 is even with respect to $(\cdot,\cdot)_\alpha^{(2)}$.*
6. *$N_{L_2/\mathbb{Q}_p}(\alpha) = s^2$.*

Two such tuples (I_1, I_2, α, s) and $(I_1', I_2', \alpha', s')$ are equivalent if and only if there exists an element $c \in L_2^\times$ such that $I_1 = cI_1'$, $I_2 = cI_2'$, $\alpha = c^2\alpha'$ and $s = N_{L_2/\mathbb{Q}_p}(c)s'$. An integral orbit (I_1, I_2, α, s) corresponds to the rational orbit given by (α, s).

Proof. First, we start with a tuple (I_1, I_2, α, s) and we construct an orbit in $G(\mathbb{Z}_p)\backslash V_b(\mathbb{Z}_p)$. First, we note that the forms $(\cdot,\cdot)^{(1)}_\alpha$ and $(\cdot,\cdot)^{(2)}_\alpha$, when restricted to I_1 and I_2 respectively, take integral values and are split of discriminant 1. Additionally, I_2 is even with respect to $(\cdot,\cdot)^{(2)}_\alpha$. Therefore, by Lemma 3.11 we can find $\mathbb{Z}_p$-bases for I_1 and I_2 such that the forms have Gram matrices J_{2n+1} and J_{2n} respecively. Then, also by construction we have that the matrix of T_β has values in $\mathbb{Z}_p$, so it gives an element of $V_b(\mathbb{Z}_p)$.

Now, suppose that we start with an orbit in $G(\mathbb{Z}_p)\backslash V_b(\mathbb{Z}_p)$. Theorem 3.3 gives (α, s) and hence properties 4 and 6. We recall that such an orbit can be constructed as the matrix of T_β in $M = \mathbb{Q}_p[x]/(xf(x^2))$. Given a basis $\{e_1, \dots, e_{4n+1}\}$ of M, the action of T_β realises $J = \mathbb{Z}_p\langle e_1, \dots, e_{4n+1}\rangle$ as an $R = \mathbb{Z}_p[x]/(xf(x^2))$-submodule. Note that $R \cong R_1 \oplus \beta R_2$. The fact that T_β respects R_1 and R_2 implies that $J = I_1 + \beta I_2$ for some fractional ideals I_1 in R_1 and I_2 in R_2, which necessarily satisfy $\overline{I_1} \subset I_2 \subset \overline{I_1}'$. The fact that the forms $(\cdot,\cdot)^{(1)}_\alpha$ and $(\cdot,\cdot)^{(2)}_\alpha$ have to be self-dual with respect to I_1 and I_2 with matrices isometric to J_{2n+1} and J_{2n} over $\mathbb{Z}_p$, respectively, give the rest of the hypotheses.

These two constructions are inverse to each other, and so we are done. □

Proof of Theorem 3.10. It suffices to show that for every element of $\hat{A}_b(\mathbb{Q}_p)/\psi(J_b(\mathbb{Q}_p))$ there is a tuple (I_1, I_2, α, s) satisfying the conditions of Proposition 3.12. We note that splitness of the forms over $\mathbb{Q}_p$ follows from Theorem 3.5. Furthermore, by [LT24, Lemma 4.9] (cf. [BG13, Proposition 8.5]), there exists a fractional ideal I_1 in R_1 such that $I_1^2 \subset \alpha R_1$ with $N(I_1)^2 = N_{L_1/\mathbb{Q}_p}(\alpha)$.

We can observe that when taking the image under the tautological map $L_1 \to L_2$, the lattices $\overline{I_1}$ and $\overline{I_1}'$ are dual to each other with respect to the form $(\cdot,\cdot)^{(2)}_\alpha$. This follows from observing that for any $\mu, \lambda \in L_2$ with liftings $\mu', \lambda' \in L_1$ we have that

$$(\mu, \lambda)^{(2)}_\alpha = (\mu', \beta\lambda')^{(1)}_\alpha.$$

Then, the process of finding a fractional ideal I_2 with the required conditions reduces to finding a lattice $\overline{I_1} \subset \Lambda \subset \overline{I_1}'$ which is self-dual and is stable under multiplication by β_2, up to considerations at $p = 2$. We further observe that any lattice Λ satisfying $\overline{I_1} \subset \Lambda \subset \overline{I_1}'$ is automatically stable under $\times\beta_2$, so it automatically is a fractional ideal.

We split our the rest of our proof in the two cases $p \neq 2$ and $p = 2$, in a similar way to [Sha19, Propositions 6.9, 6.11].

- $p \neq 2$: By [Cas78, Lemma 3.4] we can find a basis (f_i) of $\overline{I_1}$ such that its Gram matrix with respect to $(\cdot,\cdot)^{(2)}_\alpha$ is

$$\begin{pmatrix} u_1 p^{a_1} & & & \\ & u_2 p^{a_2} & & \\ & & \ddots & \\ & & & u_{2n} p^{a_{2n}} \end{pmatrix}$$

  where the a_i are non-negative integers and $u_i \in \mathbb{Z}_p^\times$. By replacing f_i with $p^{-\lfloor \frac{a_i}{2} \rfloor} f_i$, we may assume that $a_i \in \{0, 1\}$, and the resulting lattice Λ still satisfies $\overline{I_1} \subset \Lambda \subset \overline{I_1}'$. Write $\Lambda = \Lambda_0 \oplus \Lambda_1$, where Λ_i is the span of those f_j with $b_j = i$ $(i = 0, 1)$. Given that the discriminant of the form is 1 modulo squares, the dimensions of both Λ_0 and Λ_1 have to be even. We will now see that both $\Lambda_0 \otimes \mathbb{Q}_p$ and $\Lambda_1 \otimes \mathbb{Q}_p$ are split quadratic spaces.

  Let Λ_0 be spanned by $(f_1, \dots, f_{2a})$ and let Λ_1 be spanned by $(f_{2a+1}, \dots, f_{2n})$. Then, the discriminant of $\Lambda_0 \otimes \mathbb{Q}_p$ is $(-1)^a \prod_{i=1}^{2a} u_i$ and the Hasse invariant is 1, as $(u_i, u_j)_p = 1$ for all $u_i, u_j \in \mathbb{Z}_p^\times$. On the other hand, the discriminant of $\Lambda_1 \otimes \mathbb{Q}_p$ is $(-1)^{n-a} \prod_{i=2a+1}^{2n} u_i$ and its Hasse invariant is $(-1)^{(n-a)(p-1)/2} \prod_{i=2a+1}^{p} \left(\frac{u_i}{p}\right)$. A straightforward computation shows that the Hasse invariant of $(\Lambda_0 \oplus \Lambda_1) \otimes \mathbb{Q}_p$ is equal to the Hasse invariant of $\Lambda_1 \otimes \mathbb{Q}_p$, so both these invariants are equal to 1. Given that $(-1)^{(n-a)(p-1)/2}$ is equal to $(-1)^{n-a}$ up to squares (indeed, both these quantities are equal to $(-1)^{n-a}$ if $p \equiv 3 \pmod 4$ or equal to 1 modulo squares if $p \equiv 1 \pmod 4$), this forces the discriminant of $\Lambda_1 \otimes \mathbb{Q}_p$ to be equal to 1. Since the discriminant of $(\Lambda_0 \oplus \lambda_1) \otimes \mathbb{Q}_p$ is 1, and also the product of discriminants in Λ_0 and Λ_1, this implies that the discriminant of $\Lambda_0 \otimes \mathbb{Q}_p$ is also 1, proving our claim that both $\Lambda_0 \otimes \mathbb{Q}_p$ and $\Lambda_1 \otimes \mathbb{Q}_p$ are split quadratic spaces.

Thus, we can choose a basis of Λ_0 such that its Gram matrix is J_{2a}, and we can choose a basis of Λ_1 such that its basis is $pJ_{2(n-a)}$. By replacing the elements of the basis $f_{2a+1}, \dots, f_{2n}$ by $f_{2a+1}/p, \dots, f_{a+n}/p, f_{a+n+1}, \dots, f_{2n}$, we get the matrix $J_{2(n-a)}$. Therefore, we obtain a self-dual lattice $\Lambda = \Lambda_0 \oplus \Lambda_1$ with the desired inclusion conditions.

- $p = 2$: In this situation, by [Cas78, Lemma 4.1] we can find a basis of $\overline{I_1}$ such that its Gram matrix with respect to $(\cdot,\cdot)^{(2)}_\alpha$ is
$$\begin{pmatrix} 2^{a_1}Q_1 & & & \\ & 2^{a_2}Q_2 & & \\ & & \ddots & \\ & & & 2^{a_k}Q_k \end{pmatrix},$$
where $a_i \geq 0$ and the Q_i are either 1×1 matrices with an entry in $\mathbb{Z}_p^\times$ or 2×2 matrices of the form
$$Q_i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{or} \quad Q_i = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$
As before, we may assume that $a_i \in \{0,1\}$. For the 2×2 matrices, we may further assume that $a_i = 0$: if $a_i = 1$, we may substitute e_1 for $e_1/2$ to get a self-dual lattice. Therefore, we may assume that the Gram matrix is of the form
$$\begin{pmatrix} 2U & & & \\ & Q_2 & & \\ & & \ddots & \\ & & & Q_k \end{pmatrix},$$
where U is a diagonal matrix of size $2a \times 2a$ with unit entries, and the Q_i are either 1×1 or 2×2 matrices with unit determinant. Finally, we notice that for a matrix $\begin{pmatrix} 2u_1 & 0 \\ 0 & 2u_2 \end{pmatrix}$ with $u_1, u_2 \in \mathbb{Z}_p^\times$, the basis spanned by $(e_1+e_2)/2$ and $(e_1-e_2)/2$ gives a self-dual lattice. We can conclude that there exists a self-dual lattice $\overline{I_1} \subset \Lambda \subset \beta_2^{-1}\overline{I_1}$.

  It is not necessarily the case that I_2 is even with respect to the form $(\cdot,\cdot)^{(2)}_\alpha$, so it might not the case that this lattice is isometric to (L_{2n}, J_{2n}) over $\mathbb{Z}_2$. However, it is the case that both lattices are isometric under a matrix in $\mathrm{O}_{2n}(\mathbb{Q}_2)$ with coefficients in $\frac{1}{2}\mathbb{Z}_2$. Thus, the given tuple (I_1, I_2, α, s) yields an orbit in $\frac{1}{2}V(\mathbb{Z})$.

□

4 The resolvent form

We keep the notation $(G, V) = (G_B, V_B)$ from last section. As before, let K be a field of characteristic zero. Consider an element $A \in V(K)$ as a $(2n+1)\times 2n$ matrix with entries in K and associated characteristic polynomial $f(x)$. Then, A^*A is a $2n \times 2n$ matrix that is symmetric along the antidiagonal and has characteristic polynomial $f(x)$. Further, $(g,h) \in \mathrm{SO}_{2n+1} \times \mathrm{SO}_{2n}$ acts on A^*A by $(g,h)\cdot(A^*A) = hA^*Ah^*$.

Let $\mathrm{PSO}_{2n} = \mathrm{SO}_{2n}/\mu_2$. Then, we define the representation $(G_A, V_A) = (\mathrm{PSO}_{2n}, \mathrm{Sym}^2(2n))$, where $\mathrm{Sym}^2(2n)$ denotes the $2n\times 2n$ matrices that are symmetric along the antidiagonal, and G_A acts by conjugation on these matrices. This is (up to a trace zero condition that ultimately does not matter) the same representation that was studied in [SW18], corresponding to the Dynkin diagram A_{2n-1}. The ring of invariants of (G_A, V_A) is generated by the coefficients of the characteristic polynomials of the matrices of V_A, and hence we have an isomorphism between $V_A /\!\!/ G_A$ and B. We note, however, that the degrees of the elements of $V_A /\!\!/ G_A$ are half the degrees of the corresponding invariants in B.

4.1 Rational orbits

We recall [SW18, Proposition 2.1].

Proposition 4.1. *Let $b \in B^{rs}(K)$ with $\Delta(b) \neq 0$. If the associated characteristic polynomial is $f(x)$, write $L = K[x]/(f(x))$. Then if $v \in V_{A,b}(K)$, then $\mathrm{Stab}_{G_A}(v) \cong (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2$.*

Therefore, by Proposition 3.1, if $b \in B^{rs}(K)$ the $G_A(K)$-orbits in $V_{A,b}(K)$ are in bijection with the pointed kernel of

$$H^1(K, (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2) \to H^1(K, \mathrm{SO}_{2n}).$$

Similarly to (G, V), there is a map $H^1(K, (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2) \to (L^\times/K^\times L^{\times 2})_{N\equiv 1}$ which is bijective or 2-to-1 according to whether the norm map $N\colon (\mathrm{Res}_{L/K}\,\mu_2)\mu_2(K) \to \mu_2$ is surjective or not (see [SW18, Proposition 2.2] for a more explicit description).

Let β denote the image of x inside L, so that L has a K-basis $1, \beta, \ldots, \beta^{2n-1}$. Given $\alpha \in (L^\times/K^\times L^{\times 2})_{N\equiv 1}$, we can define the form $(\cdot,\cdot)_\alpha \colon L \times L \to K$ by

$$(\mu, \lambda)_\alpha = \text{coefficient of } \beta^{2n-1} \text{ in } \alpha^{-1}\mu\lambda.$$

This form has discriminant 1, up to squares. Then, we have (cf. [SW18, Theorem 2.6]):

Theorem 4.2. *There is a bijection between:*

- $\mathrm{PO}(K)$*-orbits in* $V_{A,b}(K)$*; and,*
- *elements* $\alpha \in (L^\times/K^\times L^{\times 2})_{N\equiv 1}$ *such that* $(\cdot,\cdot)_\alpha$ *is split.*

These $\mathrm{PO}(K)$*-orbits split into one or two* $\mathrm{PSO}(K)$*-orbits according to whether the norm map on* $(\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2$ *is surjective or not, respectively.*

Let $b \in B^{rs}(K)$ correspond to the invariant polynomial $f(x)$, and consider the hyperelliptic curve $C_b\colon y^2 = xf(x)$ with Jacobian $J_b = \mathrm{Jac}(C_b)$. We recall the setup of (1):

$$J_b \xrightarrow{\phi_M} A_b \xrightarrow{\phi} A_b^\vee \to J_b$$

where $J_b[\phi_M] = M$, $J_b[\phi \circ \phi_M] = M^\perp$ and the whole composition $J_b \to J_b$ is multiplication-by-2. In particular, we have that $A_b[\phi]$ is isomorphic to $M^\perp/M$. First, we note the following fact:

Lemma 4.3. *The isogeny $\phi\colon A_b \to A_b^\vee$ is self-dual.*

Proof. As suggested by the notation, the abelian varieties A_b and $A_b^\vee$ are indeed dual to each other. It is a general fact of principally polarised abelian varieties that $(J_b/M)^\vee \simeq J_b/M^\perp$, which follows from the properties of the Weil pairing.

We will show that, in fact, ϕ is a polarisation. Consider the canonical principal polarisation $\lambda_J\colon J_b \to J_b^\vee$ given by the theta divisor. Then, the associated polarisation $2\lambda_J$ has kernel $J_b[2]$. By [Mum70, §23, Corollary to Theorem 2], the polarisation $2\lambda_J$ descends to a polarisation on A_b (i.e. there is an ample line bundle $\mathcal{L}$ on A_b such that its pullback along $\phi_M\colon J_b \to A_b$ is the line bundle associated with $2\lambda_J$) if and only if the following two conditions are satisfied:

- M is contained in the kernel of $2\lambda_J$; true as $M \leqslant J_b[2]$.
- M is isotropic with respect to the Weil pairing $e_{2\lambda_J}$; true as $M \leqslant M^\perp$.

Therefore, we get a polarisation $\phi_{\mathcal{L}} \colon A_b \to A_b^\vee$. Unravelling the definitions, $\phi_{\mathcal{L}}$ satisfies $2\lambda_J = \phi_M^\vee \circ \phi_{\mathcal{L}} \circ \phi_M$ (viewing $\phi_M^\vee$ as a map between $A_b^\vee$ and $J_b^\vee$), and the kernel of $\phi_{\mathcal{L}}$ as an isogeny is isomorphic to $M^\perp/M$. Thus we can identify $\phi = \phi_{\mathcal{L}}$, and so we are done. □

We also observe the following fact about the stabiliser:

Lemma 4.4. *Under the above notation, we have* $(\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2 \cong M^\perp/M$.

This follows immediately from Proposition 3.4. Therefore, we have a map

$$A_b^\vee(K)/\phi(A_b(K)) \hookrightarrow H^1(K, (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2).$$

Theorem 4.5. *The composition*

$$A_b^\vee(K)/\phi(A_b(K)) \hookrightarrow H^1(K, (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2) \to H^1(K, G_A)$$

is trivial.

Proof. Note that there's a commutative diagram

$$\begin{array}{ccc} A_b^\vee(K)/\psi(J_b(K)) & \longrightarrow & A_b^\vee(K)/\phi(A_b(K)) \\ \downarrow & & \downarrow \\ H^1(K, J_b[\psi]) & \longrightarrow & H^1(K, A_b[\phi]) \\ \downarrow & & \downarrow \\ H^1(K, G) & \longrightarrow & H^1(K, G_A) \end{array}$$

Theorem 3.5 shows that the composition in the first column is trivial. The map in the first row is surjective, and the map in the last row is the surjective forgetful map $H^1(K, \mathrm{SO}_{2n+1} \times \mathrm{SO}_{2n}) \to H^1(K, \mathrm{SO}_{2n})$. The result follows. □

Therefore, for all $b \in B^{rs}(K)$ there is a map

$$A_b^\vee(K)/\phi(A_b(K)) \xhookrightarrow{\eta_{A,b}} G_A(K)\backslash V_{A,b}(K), \tag{4}$$

and similarly to the last section we will call a $G_A(K)$-orbit in $V_{A,b}(K)$ K-*soluble* if it intersects the image of $\eta_{A,b}$. If K is a number field, we say that an orbit is *locally soluble* if it is K_v soluble for all completions K_v. The same proof as in Corollary 3.9 yields:

Corollary 4.6. *Let K be a number field. Then for $b \in B^{rs}(K)$ we have*

$$\mathrm{Sel}_\phi(A_b) \hookrightarrow G_A(K)\backslash V_{A,b}(K).$$

In [SW18], a $G_A(K)$-orbit in $V_{A,b}(K)$ is called *reducible* (or distinguished) if it maps to the element $\alpha = 1$ in

$$H^1(K, (\mathrm{Res}_{L/K}\,\mu_2)_{N\equiv 1}/\mu_2) \to (L^\times/K^\times L^{\times 2})_{N\equiv 1}.$$

More precisely, in [SW18, §2.2] a distinguished orbit v_b is constructed, and a $\mathrm{PSO}_{2n}(K)$-orbit is called distinguished if it is $\mathrm{PO}_{2n}(K)$-equivalent to the constructed orbit v_b. This corresponds precisely to the orbits that map to $1 \in (L^\times/K^\times L^{\times 2})_{N\equiv 1}$, of which there are at most two.

4.2 Integral representatives

We will prove the equivalent of Theorem 3.10. To do so, we will use the description of integral orbits in [SW18, §2.4]. We note, however, that there is an oversight in loc. cit. in the case $p = 2$; the amended statement should read like that:

Theorem 4.7. *Let $b \in B^{rs}(\mathbb{Z}_2)$ with invariant polynomial $f(x)$, and let $L = \mathbb{Q}_2[x]/(f(x))$ and $R = \mathbb{Z}_2[x]/(f(x))$. There is a bijection between $\mathrm{O}_{2n}(\mathbb{Z}_2)$-orbits in $V_{A,b}(\mathbb{Z}_2)$ and equivalence classes of (I, α), where $\alpha \in L^\times$ and I is a fractional ideal of R satisfying $I^2 \subset \alpha R$ and $N(I)^2 = N(\alpha)$,* ***which is even with respect to the form*** *$(\cdot,\cdot)_\alpha$. Two pairs (I_1, α_1) and (I_2, α_2) are equivalent if there exists $c \in L^\times$ such that $I_1 = cI_2$ and $\alpha_1 = c^2\alpha_2$.*

Remark 4.8. There's a small convention difference in [SW18], where they take α^{-1} where we take α.

The condition of I being even with respect to the form is necessary, and in some cases the constructed ideals in [SW18, §2.4] need not be even. In that case, it can only be guaranteed that the orbit will fall inside $\frac{1}{2}V_{A,b}(\mathbb{Z}_2)$.

Theorem 4.9. *Let $b \in B^{rs}(\mathbb{Z})$. Every locally soluble orbit in $V_{A,b}(\mathbb{Q})$ has a representative in $\frac{1}{2}V_{A,b}(\mathbb{Z})$.*

Proof. As in the proof of Theorem 3.10, it is enough to see that for all p, the map

$$A_b^\vee(\mathbb{Q}_p)/\phi(A_b(\mathbb{Q}_p)) \hookrightarrow G_A(\mathbb{Q}_p)\backslash V_{A,b}(\mathbb{Q}_p)$$

always intersects $\frac{1}{2}V_{A,b}(\mathbb{Z}_p)$. For $p \neq 2$, this is immediate; if a $(2n+1) \times 2n$ matrix A has entries in $\mathbb{Z}_p$, then A^*A also does. For $p = 2$, we note that by Theorem 3.10 and Proposition 3.12 there exists an ideal called I_2 in there satisfying the hypotheses of Theorem 4.7 with the corresponding α of the rational orbit. □

5 Orbit parametrisations for C_{2n}

This section is equivalent to Section 3, but now in the C_{2n} case. For this section, let us denote $(G, V) := (G_C, V_C)$ and fix a field K of characteristic zero.

5.1 Rational orbits

Similarly to the B_{2n} case, we will start by constructing a distinguished orbit, from which we will obtain the other ones.

The distinguished orbit

Let $b = (p_2, \dots, p_{4n}) \in B(K)$, and suppose that $\Delta(b) \neq 0$. Consider the polynomial $f(x) = x^{2n} + p_2x^{2n-1} + \cdots + p_{4n}$, which is separable by hypothesis. We consider the étale algebras

$$M = \frac{K[x]}{(f(x^2))} = K[\beta], \quad L = \frac{K[x]}{(f(x))} = K[\gamma].$$

We note that $M = K\langle 1, \beta, \dots, \beta^{4n-1}\rangle$, and that there is a decomposition as K-vector spaces $M = L \oplus \beta L$, corresponding to the even and odd-degree part.

Consider the involution $\varepsilon \colon M \to M$ given by $\beta \mapsto -\beta$, and let

$$\begin{aligned}(\cdot,\cdot)\colon M \times M &\to K \\ (\mu, \lambda) &\mapsto \text{ coefficient of } \beta^{4n-1} \text{ in } \lambda\varepsilon(\mu).\end{aligned}$$

Note that $(L, L) = (\beta L, \beta L) = 0$. The Gram matrix of this form can be written as $G = \begin{pmatrix} 0 & G_1 \\ G_2 & 0 \end{pmatrix}$, where $G_1 = -{}^tG_2$. Then, there exists a change-of-basis matrix of the form $S = \begin{pmatrix} S_1 & 0 \\ 0 & S_2 \end{pmatrix}$ such that $S^tGS = \begin{pmatrix} 0 & J_{2n} \\ -J_{2n} & 0 \end{pmatrix}$ and $\det(S_1) = \det(S_2) = 1$ (e.g. by taking $S_1 = J_{2n}G_1^{-1}$, $S_2 = \mathrm{id}$).

The map $T_\beta \colon M \to M$ given by multiplication by β is anti-self-adjoint with respect to the form $(\cdot, \cdot)$. With respect to the above basis, the matrix of T_β is an element of $V(K)$.

Lemma 5.1. *Let $v \in V^{rs}(K)$. Then $\mathrm{Stab}_G(v) \cong (\mathrm{Res}_{L/K}\,\mu_2)/\mu_2$.*

Proof. Given that v is regular semisimple, the centraliser of T_β in $\mathrm{GL}(M)$ is $M^\times$. An element of the centraliser has to respect the L and βL parts, so it actually has to lie in $L^\times$. The condition that $\lambda \in L^\times$ has to respect the symplectic form translates to $\lambda^2 = 1$. Therefore, elements of the stabiliser lie in $\mathrm{Res}_{L/K}\,\mu_2$. The condition that $G = \mathrm{GL}_{2n}/\mu_2$ (as opposed to GL_{2n}) introduces the μ_2 quotient in the statement. ◻

The other orbits

By Proposition 3.1, any other rational orbits that are $G(K)$-conjugate to the constructed rational orbit are in bijection with elements in the kernel of the map $H^1(K, \mathrm{Stab}_G(v)) \to H^1(K, G)$. By looking at the commutative diagram

$$\begin{array}{ccccccc} H^1(K,\mu_2) & \longrightarrow & H^1(K,\mathrm{Res}_{L/K}\,\mu_2) & \longrightarrow & H^1(K,(\mathrm{Res}_{L/K}\,\mu_2)/\mu_2) & \longrightarrow & H^2(K,\mu_2) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^1(K,\mu_2) & \longrightarrow & H^1(K,\mathrm{GL}_{2n}) & \longrightarrow & H^1(K,\mathrm{GL}_{2n}/\mu_2) & \longrightarrow & H^2(K,\mu_2), \end{array}$$

any element in the kernel of $H^1(K, \mathrm{Stab}_G(v)) \to H^1(K, G)$ maps to the trivial element in $H^2(K, \mu_2)$, and therefore comes from an element of $H^1(K, \mathrm{Res}_{L/K}\,\mu_2) \cong L^\times/L^{\times 2}$ up to an element of $H^1(K, \mu_2) \cong K^\times/K^{\times 2}$. Moreover, any element coming from $L^\times/(K^\times L^{\times 2})$ must map to the trivial element in $H^1(K, \mathrm{GL}_{2n}/\mu_2)$, as $H^1(K, \mathrm{GL}_{2n}) = \{1\}$ by Hilbert's Theorem 90. Therefore, we conclude that the rational orbits of given invariant are in bijection with the set $L^\times/(K^\times L^{\times 2})$.

Given an element $\alpha \in L^\times/(K^\times L^\times)$, consider the form

$$\begin{aligned} (\cdot,\cdot) \colon M \times M &\to K \\ (\mu, \lambda) &\mapsto \text{ coefficient of } \beta^{4n-1} \text{ in } \alpha^{-1}\lambda\varepsilon(\mu). \end{aligned}$$

Then, a procedure analogous to the one in Section 3 gives rise to a distinct rational orbit.

Given $b \in B(K)$, let $C_b \colon y^2 = xf(x)$ be the corresponding hyperelliptic curve and $J_b = \mathrm{Jac}(C_b)$. Recall the following composition of isogenies

$$J_b \xrightarrow{\phi_M} A_b \xrightarrow{\phi} A_b^\vee \xrightarrow{\phi_M^\vee} J_b.$$

Denote $\psi^\vee = \phi_M^\vee \circ \phi$. By construction, we get:

Proposition 5.2. *We have an isomorphism $A_b[\psi^\vee] \cong (\mathrm{Res}_{L/K}\,\mu_2)/\mu_2$.*

Consequently, we get an inclusion $J_b(F)/\phi^\vee(A_b(F)) \hookrightarrow H^1(K, A_b[\psi^\vee])$.

Theorem 5.3. *The composition*

$$J_b(F)/\psi^\vee(A_b(F)) \hookrightarrow H^1(K, A_b[\psi^\vee]) \to H^1(K, \mathrm{GL}_{2n}/\mu_2)$$

is trivial.

Proof. If we look at GL_{2n}-orbits, the stabiliser in that case is isomorphic to $\mathrm{Res}_{L/K}\,\mu_2 \cong J_b[2]$, and we have a commutative diagram

$$\begin{array}{ccc} J_b(F)/2J_b(F) & \longrightarrow & J_b(F)/\psi^\vee(A_b(F)) \\ \downarrow & & \downarrow \\ H^1(K, J_b[2]) & \longrightarrow & H^1(K, A_b[\psi^\vee]) \\ \downarrow & & \downarrow \\ H^1(K, \mathrm{GL}_{2n}) & \longrightarrow & H^1(K, G) \end{array}$$

Because $H^1(K, \mathrm{GL}_{2n}) = \{1\}$, and because the top map is surjective, we conclude that the composition in the rightmost column is trivial. □

Therefore, we get an inclusion

$$J_b(F)/\psi^\vee(A_b(F)) \hookrightarrow G(F)\backslash V_b(F). \tag{5}$$

By a similar argument as in Corollary 3.9, we get:

Corollary 5.4. *We have an inclusion*

$$\mathrm{Sel}_{\psi^\vee} A_b \hookrightarrow G(\mathbb{Q})\backslash V_b(\mathbb{Q}).$$

Proof. It suffices to see that the map $H^1(\mathbb{Q}, G) \to \prod_p H^1(\mathbb{Q}_p, G)$ has a trivial pointed kernel. In this situation, we can't directly apply [Lag24, Proposition 6.8] as G is not semisimple, so we instead do a direct proof. The exact sequence

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{GL}_{2n} \longrightarrow G \longrightarrow 1$$

gives the following commutative diagram with exact rows:

$$\begin{array}{ccccc} H^1(\mathbb{Q}, \mathrm{GL}_{2n}) & \longrightarrow & H^1(\mathbb{Q}, G) & \longrightarrow & H^2(\mathbb{Q}, \mu_2) \\ \downarrow & & \downarrow & & \downarrow \\ \prod_p H^1(\mathbb{Q}_p, \mathrm{GL}_{2n}) & \longrightarrow & \prod_p H^1(\mathbb{Q}_p, G) & \longrightarrow & \prod_p H^2(\mathbb{Q}_p, \mu_2) \end{array}$$

By Hilbert's Theorem 90, $H^1(\mathbb{Q}, \mathrm{GL}_{2n})$ and $H^1(\mathbb{Q}_p, \mathrm{GL}_{2n})$ are trivial. Moreover, the Albert–Brauer–Hasse–Noether theorem implies that the map $H^2(\mathbb{Q}, \mu_2) \to \prod_p H^2(\mathbb{Q}_p, \mu_2)$ is injective. Thus, if an element $c \in H^1(\mathbb{Q}, G)$ maps to the trivial element of $\prod_p H^1(\mathbb{Q}_p, G)$, then it also maps to the trivial element of $\prod_p H^2(\mathbb{Q}_p, \mu_2)$, and the injectivity of both maps $H^1(\mathbb{Q}, G) \to H^2(\mathbb{Q}, \mu_2) \to \prod_p H^2(\mathbb{Q}_p, \mu_2)$ means that c is trivial, as desired. □

5.2 Integral orbits

We wish to show that any rational orbit corresponding to a Selmer element has integral representatives. In order to do this, first we parametrise what the integral representatives can be.

Define $R = \mathbb{Z}_p[\gamma] = \mathbb{Z}_p \cdot \langle 1, \gamma, \ldots, \gamma^{2n-1} \rangle$, an order inside L.

Proposition 5.5. *Let $b \in B(\mathbb{Z}_p)$. The set of $G(\mathbb{Z}_p)$-orbits in $V_b(\mathbb{Z}_p)$ is in bijection with equivalence classes of tuples (I_1, I_2, α), where $\alpha \in L^\times$ and I_1, I_2 are fractional ideals of R satisfying:*

1. *$I_1 I_2 \subset \alpha R$;*

2. $N(I_1)N(I_2) = N(\alpha)$;
3. $I_1 \subset I_2 \subset \gamma^{-1} I_1$;

Two tuples (I_1, I_2, α), (I_1', I_2', α') *are equivalent if there exists* $c \in L^\times$ *such that* $(I_1, I_2, \alpha) = (cI_1', cI_2', c^2\alpha')$.

Proof. Let $I = I_1 \oplus \beta I_2$ be a lattice inside M. If we consider M with basis given by any given $\mathbb{Z}$-bases of I_1, I_2, the operator T_β is an integral operator (by hypothesis 3) with associated matrices (A, C). We now need to show that there exist $\mathbb{Z}$-bases of I_1, I_2 such that $A = A^*$ and $C = C^*$.

Using last section's notation, we see that the form $(\cdot,\cdot)_\alpha$ has an integral Gram matrix (by hypothesis 1), and that the associate matrices (G_1, G_2) have the same determinant ± 1 (by hypothesis 2). Then, it is safe to choose change-of-bases matrices (S_1, S_2) with same determinant ± 1 as appropriate to make A and C self-adjoint with respect to the usual inner product.

Conversely, given two matrices $(A, C) \in V_b(\mathbb{Z})$, we construct I_1, I_2 as follows. First, construct $R = \mathbb{Z}[x]/g(x) = \mathbb{Z}[\gamma]$, and let $I_2 \cong \mathbb{Z}^n$ as abelian groups. To make I_2 into an R-module, we need to specify how γ acts: by viewing elements of I_2 as column vectors, we let γ act on I_2 as the matrix CA (this action is well-defined, because $g(CA) = 0$ by the Cayley–Hamilton theorem). We then let I_1 be the submodule $C \cdot I_2$, and obtain α from the rational orbit of (A, C). If we choose $\mathcal{B}_1$ and $\mathcal{B}_2$ to be $\mathbb{Z}$-bases of I_1 and I_2, then the matrix of the operator T_β on the basis of M given by $\mathcal{B}_1 \cup \beta\mathcal{B}_2$ is the one corresponding to (A, C). The fact that the lattice $I_1 \oplus \beta I_2$ of M is self-dual to the form $(\cdot,\cdot)_\alpha$ translates to the hypotheses $I_1 I_2 \subset \alpha R$ and $N(I_1)N(I_2) = N(\alpha)$.

Therefore, the two constructions $(A, C) \mapsto (I_1, I_2, \alpha)$ and $(I_1, I_2, \alpha) \mapsto (A, C)$ are inverse to each other, as desired. □

Theorem 5.6. *The image of the map*

$$J_b(\mathbb{Q}_p)/\psi^\vee(A_b(\mathbb{Q}_p)) \hookrightarrow G(\mathbb{Q}_p)\backslash V_b(\mathbb{Q}_p).$$

always intersects $V_b(\mathbb{Z}_p)$.

Proof. Let $L_1 = \frac{K[x]}{(xf(x))} = K[\beta_1]$, which can be decomposed as $L_1 \cong \mathbb{Q}_p \times L$. By [LT24, Lemma 4.9], there exists a fractional ideal $\tilde{I_1}$ of the order $R_1 = \mathbb{Z}_p[\beta_1]$ satisfying $\tilde{I_1}^2 \subset \tilde{\alpha} R_1$ (where $\tilde{\alpha}$ is a lifting of α to L_1) and $N(\tilde{I_1})^2 = N(\alpha)$, where the norms are taken with respect to R_1.

Take I_1 to be the reduction of $\tilde{I_1}$ to R. For an element $\lambda \in L_2$, define $\tilde{\lambda} \in L_1$ to be $\tilde{\lambda} = (0, \lambda) \in \mathbb{Q}_p \times L$. Then, similarly to the proof of Theorem 3.10, consider

$$I_1' = \{\lambda \in L_2 \mid \beta\tilde{\lambda} \in I_1\}.$$

This is a fractional ideal of R. We now claim that taking $I_2 = I_1'$ satisfies the conditions of Proposition 5.5. Indeed, by the same proof as Theorem 3.10, the ideals I_1 and I_2 are dual to each other with respect to $(\cdot,\cdot)_\alpha$, so this guarantees the first two points of the proposition. The final point is an easy computation. □

6 Counting orbits for C_{2n}

Fix $(G, V) = (G_C, V_C)$. In this section, we develop the necessary geometry-of-numbers methods we need to count $G(\mathbb{Z})$-orbits in $V(\mathbb{Z})$. We note that $G = \mathrm{GL}_{2n}/\mu_2$ is not semisimple, a fact that will introduce some important technical differences with respect to similar arguments found in the literature.

6.1 Measures

Recall that $B \cong \operatorname{Spec} \mathbb{Z}[b_2, \ldots, b_{4n}]$. We start by recording a useful numerological fact.

Lemma 6.1. *$2 + 4 + \cdots + 4n = \dim_{\mathbb{Q}} V$.*

To obtain a measure on $G = \mathrm{GL}_{2n} / \mu_2$, we start by explicitly writing down the Iwasawa decomposition of $G(\mathbb{R})$. We have that $G(\mathbb{R}) = \Lambda NTK$, where $\Lambda = \{\lambda I_{2n} \mid \lambda > 0\}$, N consists of unipotent lower triangular matrices, $T = \{\operatorname{diag}(t_1, \ldots, t_{2n}) \mid t_i > 0,\, t_1 \ldots t_{2n} = 1\}$ and K is a maximal compact subgroup isomorphic to O_{2n}/μ_2. Then, it follows that the map

$$\Lambda \times N(\mathbb{R}) \times T(\mathbb{R}) \times K \to G(\mathbb{R})$$

is a diffeomorphism by an argument similar to [Lan75, Chapter 3, §1]. We can explicitly determine a Haar measure for G in terms of Λ, N, T, K:

Proposition 6.2. *A Haar measure dg on $G(\mathbb{R})$ can be given by $dg = \delta^{-1}(t)\, d^\times \lambda\, dn\, d^\times t\, dk$, where $d^\times \lambda = \frac{d\lambda}{\lambda}$, dn and dk are Haar measures on $N(\mathbb{R})$ and K respectively, $d^\times t = \prod_{i=1}^{2n-1} \frac{dt_i}{t_i}$ and $\delta^{-1}(t) = \prod_{i=1}^{2n-1} t_i^{4n-2i}$.*

If $T = \operatorname{diag}(t_1, \ldots, t_{2n})$, write the following change of variables for $1 \leq m \leq 2n$:

$$t_m = \prod_{k=1}^{m-1} s_k^{-k} \prod_{k=m}^{2n-1} s_k^{2n-k}.$$

The conditions that $t_k/t_{k+1} < c$ for all $k \in \{1, \ldots, 2n-1\}$ translate to $s_k < c'$ for all $k \in \{1, \ldots, 2n-1\}$ and some $c' > 0$.

Using this decomposition, we can obtain a fundamental domain for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$. In fact, we can choose it to be *box-shaped at infinity*; a notion that we now explain. Given a positive constant $c > 0$, define $T_c = \{\operatorname{diag}(t_1, \ldots, t_{2n}) \in T(\mathbb{R}) \mid t_2/t_1 < c, \ldots, t_{2n}/t_{2n-1} < c\}$. Then, define a *Siegel set* to be a set of the form $\mathcal{S} = \Lambda \omega T_c K$, where ω is a compact subset of $N(\mathbb{R})$ and $c > 0$. Then, we say that a set $\mathcal{F} \subset G(\mathbb{R})$ is *box-shaped at infinity* if there exist Siegel subsets $\mathcal{S}_1, \mathcal{S}_2$ with $\mathcal{S}_1 \subset \mathcal{F} \subset \mathcal{S}_2$ and satisfying:

- There exists an open subset $\mathcal{U}_1 \subset \mathcal{S}_1$ of full measure such that every $G(\mathbb{Z})$-orbit in $G(\mathbb{R})$ intersects $\mathcal{U}_1$ at most once.
- Every $G(\mathbb{Z})$-orbit in $G(\mathbb{R})$ intersects $\mathcal{U}_2$ at least once.
- There exists a sufficiently small c such that $\mathcal{S}_1 \cap \Lambda N T_c K = \mathcal{S}_2 \cap \Lambda N T_c K$.

Proposition 6.3. *There exists a box-shaped fundamental domain for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$.*

Proof. For $G' = \mathrm{SL}_{2n} / \mu_2$, the proof of [Oll25, §4.3] shows that there exists a box-shaped fundamental domain $\mathcal{S}_1' \subset \mathcal{F}' \subset \mathcal{S}_2'$ for G' (for which the definition is the same as above, removing Λ). Considering $\mathcal{F} := \Lambda \cdot \mathcal{F}'$, $\mathcal{S}_1 := \Lambda \cdot \mathcal{S}_1'$ and $\mathcal{S}_2 := \Lambda \cdot \mathcal{S}_2'$ works. □

Within this set-up, we have the following change-of-measure formula:

Lemma 6.4. *1. Let p be a prime, and let $m_p \colon V^{rs}(\mathbb{Z}_p) \to \mathbb{R}_{\geq 0}$ be defined as*

$$m_p(v) = \sum_{v' \in G(\mathbb{Z}_p) \backslash (G(\mathbb{Q}_p) \cdot v \cap V(\mathbb{Z}_p))} \frac{\# \operatorname{Stab}_{G(\mathbb{Q}_p)}(v')}{\# \operatorname{Stab}_{G(\mathbb{Z}_p)}(v')}.$$

Then m_p is locally constant.

2. *Let* $\psi_p\colon V^{rs}(\mathbb{Z}_p)\to\mathbb{R}_{\geq 0}$ *be a bounded, locally constant function satisfying* $\psi_p(v)=\psi_p(v')$ *whenever* $v,v'\in V(\mathbb{Z}_p)$ *are* $G(\mathbb{Q}_p)$*-conjugate. Then there exists* $W_0\in\mathbb{Q}^\times$*, independent of* p*, such that*

$$\int_{v\in V^{rs}(\mathbb{Z}_p)}\psi_p(v)dv=|W_0|\operatorname{vol}(G(\mathbb{Z}_p))\int_{b\in B^{rs}(\mathbb{Z}_p)}\sum_{v\in G(\mathbb{Q}_p)\backslash V_b(\mathbb{Z}_p)}\frac{m_p(v)\psi_p(v)}{\#\operatorname{Stab}_{G(\mathbb{Q}_p)}(v)}.$$

Proof. This is analogous to [RT18, Proposition 3.3], using Lemma 6.1. □

We can also construct special subsets of $V^{rs}(\mathbb{R})$ to serve as fundamental domains of the action of $G(\mathbb{R})$ on $V^{rs}(\mathbb{R})$. Similarly to [Tho15, §2.9], we can find open subsets $L_1,\dots,L_k$ of $\{b\in B^{rs}(\mathbb{R})\mid \operatorname{ht}(b)=1\}$ together with sections $s_i\colon L_i\to V(\mathbb{R})$ of the invariant map $\pi\colon V\to B$ satisfying the following properties:

- For each i, the set L_i is connected and semialgebraic, and s_i is a semialgebraic map with bounded image.
- Let $D=\mathbb{R}_{>0}$. We then have an equality:

$$V^{rs}(\mathbb{R})=\bigcup_{i=1}^{k}G(\mathbb{R})\cdot D\cdot s_i(L_i).$$

6.2 Averaging and reductions

We now carry out the core of our geometry-of-numbers arguments to count $G(\mathbb{Z})$-orbits in $V(\mathbb{Z})$. Many of the steps are completely analogous to the case where G is semisimple, and will be duly omitted. The reader can check [BS15a, §2.3] for further context.

Let $A\subset V(\mathbb{Z})$ be a $G(\mathbb{Z})$-invariant set, and denote

$$N(A,X)=\sum_{v\in G(\mathbb{Z})\backslash A_{<X}}\frac{1}{\#\operatorname{Stab}_{G(\mathbb{Z})}(v)}.$$

Let F be a field of characterstic zero. We say that an element $v\in V(F)$ with $b=\pi(v)$ is:

- F*-reducible* if $\Delta(b)=0$ or if there exists an element $w=(A,C)$ in the $G(\mathbb{Q})$-orbit of v such that either $A=J_{2n}$ or $C=J_{2n}$; and F*-irreducible* otherwise.
- F-soluble if $\Delta(b)\neq 0$ and v lies in the image of

$$J_b(F)/\psi^\vee(A_b^\vee(F))\hookrightarrow G(F)\backslash V_b(F)$$

  of (5).

Given $A\subset V(\mathbb{Z})$, we will denote by A^{irr} its set of $\mathbb{Q}$-irreducible elements, and we will also denote by $V(\mathbb{R})^{sol}$ the set of $\mathbb{R}$-soluble elements of $V(\mathbb{R})$.

Theorem 6.5. *There exists a constant* $C>0$ *such that*

$$N(V(\mathbb{Z})^{irr}\cap V(\mathbb{R})^{sol},X)=CX^{\dim V}\log X+O(X^{\dim V})$$

as $X\to\infty$*.*

Similarly to [Lag24, Theorem 8.8, Proposition 8.10], it suffices to prove the following result. Let I be a subset of $\{1,\dots,k\}$, and denote $L_I=\cap_{i\in I}\pi(G(\mathbb{R})\cdot s_i(L_i))$. Also denote s_I to be the restriction of some s_i for $i\in I$ (which might depend on the choice of i, but ultimately that choice does not matter). The following theorem implies Theorem 6.5.

Theorem 6.6. *Suppose I is a non-empty subset of $\{1,\ldots,k\}$ and let $(L,s)=(L_I,s_I)$. Then there exists a constant C_I such that*

$$N(V(\mathbb{Z})^{irr}\cap V(\mathbb{R})^{sol},X)=C_IX^{\dim V}\log X+O(X^{\dim V})$$

as $X\to\infty$.

From now on, let us fix $(L,s)=(L_I,s_I)$ for some choice of I. We now carry out the main steps of the proof of Theorem 6.6 (and therefore of Theorem 6.5). We begin with an averaging trick, which works just the same as in [BS15a, §2.3]. Fix $G_0\subset G(\mathbb{R})\times\mathbb{R}_{>0}$, a compact, semialgebraic subset of non-empty interior satisfying $KG_0=G_0$, $\mathrm{vol}(G_0)=1$ and $G_0=G_0'\times[1,K_0]$ for some $G_0'\subset G(\mathbb{R})$ and $K_0>1$. Let $A\subset V(\mathbb{Z})\cap G(\mathbb{R})\cdot D\cdot s(L)$ be a $G(\mathbb{Z})$-invariant set. Then

$$N(A,X)=\frac{1}{r}\int_{d>0}\int_{g\in\mathcal{F}}\#[A\cap(gd\cdot s(L))_{<X}]\,dg\,d^\times d. \tag{6}$$

If we take a set $A\subset V(\mathbb{Z})\cap G(\mathbb{R})\cdot D\cdot s(L)$ that is not necessarily $G(\mathbb{Z})$-invariant, we *define* $N(A,X)$ to be the expression in (6). We will need some reductions. Let us denote:

- $V(\mathbb{Z})^{cusp}$ to be the *cuspidal region*, which is the subset of $(A,C)\in V(\mathbb{Z})$ such that $a_{1,2n}=0$ or $c_{1,2n}=0$.
- $V(\mathbb{Z})^{main}=V(\mathbb{Z})\setminus V(\mathbb{Z})^{cusp}$.
- $V(\mathbb{Z})^{bigstab}$ to be the subset of elements $v\in V(\mathbb{Z})$ such that $\#\,\mathrm{Stab}_{G(\mathbb{Q})}(v)>1$.

Proposition 6.7. *The following hold:*

1. $N(V(\mathbb{Z})^{cusp}\cap V(\mathbb{Z})^{irr},X)=O(X^{\dim V})$
2. $N(V(\mathbb{Z})^{main}\cap V(\mathbb{Z})^{red},X)=o(X^{\dim V}\log X)$.
3. $N(V(\mathbb{Z})^{bigstab}\cap V(\mathbb{Z})^{irr},X)=o(X^{\dim V}\log X)$.

We will prove them the first item in Section 6.3, while the second and third item follow from the same proof as in [Lag24, Propositions 8.16 and 8.21].

The consequence of these reductions is that to count irreducible elements, it suffices to count elements in the main body of the representation. This will be done using geometry-of-numbers, and more specifically the following version of Davenport's lemma, due to Barroero–Widmer [BW14, Theorem 1.3]:

Lemma 6.8. *Let $m,n\geq 1$ be integers and let $Z\subset\mathbb{R}^{m+n}$ be a semialgebraic subset. For $T\in\mathbb{R}^m$, let $Z_T=\{x\in\mathbb{R}^n\mid(T,x)\in Z\}$, and suppose that all such sets Z_T are bounded. Then for any unipotent upper-triangular matrix $u\in\mathrm{GL}_n(\mathbb{R})$, we have*

$$\#(Z_T\cap u\mathbb{Z}^n)=\mathrm{vol}(Z_T)+O(\max\{1,Z_{T,j}\}),$$

where $Z_{T,j}$ runs over all orthogonal projections of Z_T to all j-dimensional coordinate subspaces, ($1\leq j\leq n-1$). Moreover, the implied constant depends only on Z.

We can then estimate the number of points inside the main body. This will be done similarly to [Lag24, Proposition 8.15], with a key difference introduced by G not being semisimple.

Proposition 6.9. *Let $A=V(\mathbb{Z})^{main}\cap G(\mathbb{R})\cdot D\cdot s(L)$. There exists a constant $C>0$ such that $N(A,X)=CX^{\dim V}\log X+O(X^{\dim V})$.*

Proof. In the main body, an element $v=(A,C)\in V(\mathbb{Z})^{main}$ has that $a_{1,2n}\neq 0$ and $c_{1,2n}\neq 0$. Given that the space $\omega\cdot G_0\cdot s(L)$ is bounded, there exists a constant $J>0$ such that $|a_{i,j}|,|c_{i,j}|\leq J$ for all $(A,C)\in\omega\cdot G_0\cdot s(L)$.

Then, the condition that $a_{1,2n} \neq 0$ and $c_{1,2n} \neq 0$ for an element $v = (A, C) \in (d\lambda nt \cdot s(L))_{<X}$ translates to asking that $d\lambda^2 t_1^2 \leq 1/J$ and $d\lambda^{-2} t_{2n}^{-2} \leq 1/J$. Note that $t_1 = \prod_{k=1}^{2n-1} s_k^{2n-k} \gg 1$ and $t_{2n} = \prod_{k=1}^{2n-1} s_k^{-k} \ll 1$, so these two last conditions imply that $d^{-1} \ll \lambda^2 \ll d$.

We wish to apply Davenport's lemma (Lemma 6.8). First, we estimate the size of the error term. Let Φ_V be the set of weights of V under the action of T, which correspond to the distinct matrix entries of the corresponding matrices (A, C). Let Φ_A denote the weights falling in the matrix A, and let Φ_C denote those falling in C. Let $M \subset \Phi_V$ be a subset, and define $V(M) = \{v \in V(\mathbb{R}) \mid v_a = 0 \, \forall a \in M\}$. Let $m_a = \#M \cap \Phi_A$ and $m_c = \#M \cap \Phi_C$. The volume of the projection to $V(M)(\mathbb{Z})$ is of the order of

$$d^{\dim V - \#M} \lambda^{2m_c - 2m_a} \prod_{w \in M} w(t)^{-1}$$

We can compare the weights to the highest weights, which correspond to the entries $a_{1,2n}$ and $c_{1,2n}$. Then, the volume of the projection is

$$\ll d^{\dim V} (d\lambda^2 t_1 t_{2n})^{-m_a} (d\lambda^{-2} (t_1 t_{2n})^{-1})^{-m_c}.$$

This is at its biggest when $\{m_a, m_c\} = \{0, 1\}$, in either order, which corresponds to the projections in the case when $M = \{a_{1,2n}\}$ or $M = \{c_{1,2n}\}$. In the first of these cases (the second one is analogous), we can compute that $a_{1,2n}(t)\delta^{-1}(t)$ can be written as a product of s_i with strictly positive exponents. Given that $d^{-1} \ll \lambda^2 \ll d$, we get that

$$\int_{d=1}^{X} \int_{d^{-1/2} \ll \lambda \ll d^{1/2}} \int_{t_{i+1}/t_i \ll 1} d^{\dim V - 1} \lambda^{-2} (t_1 t_{2n})^{-1} \, \delta^{-1}(t) \, d^\times \lambda \, d^\times t \, d^\times d \ll X^{\dim V}.$$

As for the main body, we compute that it is of the order of

$$\int_{d=1}^{X} \int_{\lambda = d^{-1/2}}^{d^{1/2}} d^{\dim V} d^\times \lambda d^\times d \sim X^{\dim V} \log X.$$

This concludes the proof. □

The proof of Theorem 6.6 (and therefore of Theorem 6.5) then follows from Proposition 6.9 and the three items of Proposition 6.7.

6.3 Cutting off the cusp

In this section, we prove the first item of Proposition 6.7. We start with some reduciblity conditions:

Lemma 6.10. *Let $v = (A, C) \in V(\mathbb{Q})$ and $1 \leq k \leq n$. Suppose that both A and C contain a $k \times (2n - k)$ top-right block of entries equal to zero. Then $\Delta(v) = 0$.*

Proof. In this situation, the product AC is a block lower-triangular matrix whose diagonals are square matrices of size k, $2n - 2k$ and k. In particular, the characteristic polynomial of AC factors as the product of the three (two if $k = n$) characteristic polynomials of the blocks. It is an elementary computation to show that the characteristic polynomials of the first and the last block are the same, and therefore that the total invariant polynomial has discriminant zero. □

Lemma 6.11. *Let $v = (A, C) \in V(\mathbb{Q})$. Suppose that the top-right $n \times n$ block of either A or C is zero. Then v is reducible.*

Proof. Suppose, without loss of generality, that the top-right $n \times n$ block of A is equal to zero, meaning that there exists $g \in \mathrm{GL}_{2n}(\mathbb{Q})$ such that $gAg^* = J_{2n}$. This implies that there is an element in the $G(\mathbb{Q})$-orbit of v which is of the form (J_{2n}, C'), so v is reducible. □

With these conditions in mind, we can carry out the cutting off the cusp. We note, however, that there will be some notable differences with usual cases in the literature, as now G is not semisimple. We note that the action of $D \times \Lambda \times T$ on V gives every entry of the matrices of V a weight. If $(A, C) \in V$, then $d \in D$ scales every entry of A and C by d, while $\lambda \in \Lambda$ scales entries of A by λ^2 and entries of C by λ^{-2}.

We recall the change of variables for $1 \leq m \leq 2n$:

$$t_m = \prod_{k=1}^{m-1} s_k^{-k} \prod_{k=m}^{2n-1} s_k^{2n-k}.$$

The weight of each entry of $(A, C) \in V$ with respect to T can be written as a product $\prod_{k=1}^{2n-1} s_k^{a_k}$ for some integers a_k. Let Φ_V denote the set of weights on V, which consists of the matrix entries $a_{i,j}$ and $c_{i,j}$, with $i + j \leq 2n + 1$. We denote $\Phi_V = \Phi_A \sqcup \Phi_C$, where Φ_A consists of the $a_{i,j}$ entries and Φ_C consists of the $c_{i,j}$ entries. We can define an ordering on Φ_V: if $a, b \in \Phi_V$, we will say that $a \leq b$ if the exponent of every s_k in the weight of a is lower or equal to the corresponding exponent of s_k in b. Then, an explicit computation shows that the entries $a_{1,2n}$ and $c_{1,2n}$ are maximal elements of Φ_V. Visually, the weights increase as we go to the top and to the right of these matrices.

Let M_0, M_1 be disjoint subsets of Φ_V, and let $S(M_0, M_1)$ denote the elements $v \in V(\mathbb{Z})$ such that $v_a = 0$ if $a \in M_0$ and $v_a \neq 0$ if $a \in M_1$. Let $\mathcal{C}$ denote the collection of non-empty subsets M_0 such that if $a \in M_0$ and $b \geq a$, then $b \in M_0$. Given $M_0 \in \mathcal{C}$, denote $\lambda(M_0) = \{a \in \Phi_V \setminus M_0 \mid M_0 \cup \{a\} \in \mathcal{C}\}$ (i.e. the subset of maximal elements of M_0).

Then, to prove the first item of Proposition 6.7, it suffices to show that for every $M_0 \in \mathcal{C}$, either $S(M_0, \lambda(M_0))^{irr} = \emptyset$ or $N(S(M_0, \lambda(M_0)), X) = O(X^{\dim V})$. First, we note that if $a_{i,i} \in M_0$ for any $1 \leq i \leq n$ or if $a_{n,n+1} \in M_0$, then $S(M_0, \lambda(M_0))^{irr} = \emptyset$ by Lemmas 6.10 and 6.11. Then, for all i, there exists $v_i \in \lambda(M_0) \cap \Phi_A$ such that $w(a_{i,i}) \leq w(v_i)$ if $1 \leq i \leq n-1$ and $w(a_{n,n+1}) \leq w(v_i)$. If $v \in \lambda(M_0) \cap \Phi_A$, then we must have that $d\lambda^2 w(v) \gg 1$. Therefore, given that $\prod_{i=1}^{n-1} w(a_{i,i}) w(a_{n,n+1}) = t_n/t_{n+1} < c$, we have that

$$\prod_{i=1}^{n} (d\lambda^2 w(v_i)) \gg d^n \lambda^{2n} \gg 1,$$

which means that $\lambda^2 \gg d^{-1}$. The analogous argument with entries in C yields $\lambda^2 \ll d$.

Pick $M_0 \in \mathcal{C}$ and write $m_a = \#(M_0 \cap \Phi_A)$, $m_c = \#(M_0 \cap \Phi_C)$. Then, Davenport's lemma ensures that the number of lattice points in $S(M_0, \lambda(M_0))$ with height at most X is

$$\ll \int_{d=1}^{X} \int_{\lambda=d^{-1/2}}^{d^{1/2}} \int_{s_k < c\, \forall k} d^{\dim V - \# M_0} \lambda^{2(m_c - m_a)} \prod_{v \in M_0} w(v)^{-1} \delta^{-1}(s)\, d^\times d\, d^\times \lambda\, d^\times s.$$

If all the exponents of s_k are strictly positive in the integral, then the value of the integral is $O(X^{\dim V - \# M_0 + |m_c - m_a|})$, or $O(X^{\dim V - \# M_0} \log X)$ if $m_c - m_a = 0$. In any case, it is $O(X^{\dim V})$, as wanted. When the exponents of s_k are not necessarily positive, we use a trick due to Bhargava, adapted here to our circumstances. We note that if $a \in M_1$, then

$$d\lambda^2 w(a) \gg 1 \quad \text{or} \quad d\lambda^{-2} w(a) \gg 1$$

according to whether $a \in \Phi_A$ or $a \in \Phi_C$, respectively. Then, we can multiply by a product $\prod_{a \in M_1} (d\lambda^{\pm 2} w(a))^{p(a)}$ for some values $p(a) \gg 1$ to get a new estimate.

Proposition 6.12. *Suppose there exists a function $p\colon M_1 \to \mathbb{R}_{\geq 0}$ such that:*

- $\sum_{a \in M_1} p(a) \leq \# M_0$,
- $\sum_{a \in M_1 \cap \Phi_A} p(a) - \sum_{a \in M_1 \cap \Phi_C} p(a) = m_a - m_c$,

- *The exponents of s_k in*
$$\prod_{a\in M_1}(w(a))^{p(a)}\prod_{a\in M_0}w(a)^{-1}\delta^{-1}(s)$$
are all strictly positive.

Then $N(M_0,\lambda(M_0),X)=O(X^{\dim V})$.

Proof. The conditions guarantee that $N(M_0,\lambda(M_0),X)=O(X^{\dim V-\#M_0+\sum_{a\in M_1}p(a)}\log X)$, so if $\sum_{a\in M_1}p(a)<\#M_0$ we are done. Otherwise, if $\sum_{a\in M_1}p(a)=\#M_0$, replacing p by $(1-\varepsilon)p$ for a sufficiently small $\varepsilon>0$ yields

$$\begin{cases} O(X^{\dim V-\varepsilon\sum_{a\in M_1}p(a)+\varepsilon|\sum_{a\in M_1\cap\Phi_A}p(a)-\sum_{a\in M_1\cap\Phi_C}p(a)|}) & \text{if } \sum_{a\in M_1\cap\Phi_A}p(a)\neq\sum_{a\in M_1\cap\Phi_C}p(a)\\ O(X^{\dim V-\varepsilon\sum_{a\in M_1}p(a)}\log X) & \text{otherwise.}\end{cases}$$

In any case, it is $O(X^{\dim V})$. ☐

Proposition 6.13. *For every $M_0\in\mathcal{C}$, there exists $p\colon M_1\to\mathbb{R}_{\geq 0}$ satisfying the conditions of Proposition 6.12.*

Proof. We proceed by induction on $n\geq 2$. We start by doing the $n=2$ case explicitly. We label the weights of Φ_V in this case:

$$(A,C)=\left(\begin{pmatrix}6&4&2&1\\8&5&3&\\9&7&&\\10&&&\end{pmatrix},\begin{pmatrix}16&14&12&11\\18&15&13&\\19&17&&\\20&&&\end{pmatrix}\right)$$

For reference, we also write explicitly the action of T on (A,C), which is indexed by (s_1,s_2,s_3):

$$\left(\begin{pmatrix}(2,0,-2)&(2,0,2)&(2,4,2)&(6,4,2)\\(-2,0,-2)&(-2,0,2)&(-2,4,2)&\\(-2,-4,-2)&(-2,-4,2)&&\\(-2,-4,-6)&&&\end{pmatrix},\begin{pmatrix}(-2,0,2)&(2,0,2)&(2,4,2)&(2,4,6)\\(-2,0,-2)&(2,0,-2)&(2,4,-2)&\\(-2,-4,-2)&(2,-4,-2)&&\\(-6,-4,-2)&&&\end{pmatrix}\right)$$

We have that $\delta^{-1}(s)=s_1^{12}s_2^{16}s_3^{12}$. Taking into account Lemmas 6.10 and 6.11, we write down the list of all non-trivial possibilities for M_0, together with a choice of $p\colon M_1\to\mathbb{R}_{\geq 0}$. We omit repetitions we would get by swapping A and C. Here, ε denotes a small positive real number.

M_0	weight	p
$\{1\}$	$d^{19}\lambda^{-2}(6,12,14)$	$1\cdot(2)$
$\{1,11\}$	$d^{18}(4,8,4)$	0
$\{1,2\}$	$d^{18}\lambda^{-4}(4,8,8)$	$2\cdot(4)$
$\{1,2,11\}$	$d^{17}\lambda^{-2}(2,4,2)$	$1\cdot(4)$
$\{1,2,11,12\}$	$d^{16}(0,0,0)$	$\varepsilon(3)+\varepsilon(13)+\varepsilon(4)+\varepsilon(14)$
$\{1,2,4\}$	$d^{17}\lambda^{-6}(2,8,6)$	$1\cdot\frac{3}{2}(6)+\frac{3}{2}(5)$
$\{1,2,4,11\}$	$d^{16}\lambda^{-4}(0,4,0)$	$(1+\varepsilon)(6)+(1+\varepsilon)(5)+2\varepsilon(14)$
$\{1,2,4,11,12\}$	$d^{15}\lambda^{-2}(-2,0,-2)$	$\varepsilon(3)+\varepsilon(13)+(2+\frac{\varepsilon}{2})(6)+(2+\frac{\varepsilon}{2})(5)+(1+\varepsilon)(14)$

Now, by induction we assume that the theorem holds for $n-1$. Let $M_0\in\mathcal{C}$. Inside Φ_V, let Φ_{n-1} denote the subset of weights corresponding to the inner $(2n-2)\times(2n-2)$ matrices of (A,C) (that is, removing the first and last rows and columns). If $M_0\cap\Phi_{n-1}$ is non-empty, then use induction to get a function $p_{n-1}\colon M_1\cap\Phi_{n-1}\to\mathbb{R}_{\geq 0}$ satisfying:

- $\sum_{a\in M_1\cap\Phi_{n-1}}p_{n-1}(a)\leq\#(M_0\cap\Phi_{n-1})$

- $\sum_{a\in M_1\cap\Phi_{n-1}\cap\Phi_A} p_{n-1}(a) - \sum_{c\in M_1\cap\Phi_{n-1}\cap\Phi_C} p_{n-1}(c) = \#(M_0\cap\Phi_A\cap\Phi_{n-1}) - \#(M_0\cap\Phi_C\cap\Phi_{n-1})$
- The exponents in

$$\prod_{a\in M_1\cap\Phi_{n-1}} (w(a))^{p_{n-1}(a)} \prod_{a\in M_0\cap\Phi_{n-1}} w(a)^{-1} \prod_{k=2}^{2n-2} s_k^{2n(k-1)(2n-k-1)}$$

  are strictly positive.

If $M_0\cap\Phi_{n-1}$ is empty, we can carry out the argument with $p_{n-1}=0$. Then, it suffices to find $p_1\colon M_1\to\mathbb{R}_{\geq 0}$ satisfying:

- $\sum_{a\in M_1} p_1(a) \leq \#(M_0\cap(\Phi_V\setminus\Phi_{n-1}))$
- $\sum_{a\in M_1\cap\Phi_A} p_1(a) - \sum_{c\in M_1\cap\Phi_C} p_1(c) = \#(M_0\cap(\Phi_A\setminus\Phi_{n-1})) - \#(M_0\cap(\Phi_C\setminus\Phi_{n-1}))$
- The exponents in

$$\prod_{a\in M_1} (w(a))^{p_1(a)} \prod_{a\in M_0\cap(\Phi_V\setminus\Phi_{n-1})} w(a)^{-1} \prod_{k=1}^{2n-1} s_k^{2n(2n-1)}$$

  are non-negative.

Let $m_a = \#((M_0\cap\Phi_A)\setminus\Phi_{n-1})$ and $m_c = \#((M_0\cap\Phi_C)\setminus\Phi_{n-1})$, which are the number of elements of M_0 in the top row of A and C respectively. Then, $a_{1,2n-m_a}, c_{1,2n-m_c}\in M_1$. We select p_1 according to the following cases, where without loss of generality we assume that $a\geq c$:

- $m_a+m_c<2n$. In this situation, we choose the function p_1 to be $p_1(a_{1,2n-m_a})=m_a$, $p_1(c_{1,2n-m_c})=m_c$ and 0 everywhere else.
- $m_a+m_c\geq 2n$ and $m_c\leq n$. In this situation, we choose $p_1(a_{1,2n-m_a})=m_a-1$, $p_1(a_{n,n+1})=1$, $p(c_{1,2n-m_c})=m_c$ and 0 everywhere else.
- $m_a+m_c\geq 2n$ and $m_c>n$. Let $M=m_a+m_c-2n+\frac{1}{2}$, where we note that $M\leq m_a$ and $M\leq m_c$. We note that, for all $1\leq k\leq n-1$, at least one of $a_{k,k+1}$ and $c_{k,k+1}$ belongs to M_1 by Lemma 6.10. If $a_{k,k+1}\in M_1$, then we note that $w(a_{k,k+1})w(c_{k,k})=s_{2n-k}^{2n}$ and $w(a_{k,k+1})w(c_{k+1,k+1})=s_k^{2n}$; with similar formulae if $c_{k,k+1}\in M_1$. We also note that $a_{n,n+1}, c_{n,n+1}\in M_1$ by Lemma 6.11, and that $w(a_{n,n+1})w(c_{n,n+1})=s_n^{4n}$. With all that said, we choose p_1 in the following manner:
  - $p_1(a_{1,2n-m_a})=m_a-M$ and $p_1(c_{1,2n-m_c})=m_c-M$.
  - For all $2n-m_c\leq k\leq n-1$, if $a_{k,k+1}\in M_1$ we put $p_1(a_{k,k+1})=2$, $p_1(c_{k,k})=1$ and $p_1(c_{k+1,k+1})=1$. Otherwise, we put $p_1(c_{k,k+1})=2$, $p_1(a_{k,k})=1$ and $p_1(a_{k+1,k+1})=1$.
  - For all $2n-m_a\leq k<2n-m_c$, if $a_{k,k+1}\in M_1$ we put $p_1(a_{k,k+1})=1$ and $p_1(c_{k+1,k+1})=1$. Otherwise, we put $p_1(c_{k,k+1})=1$ and $p_1(a_{k,k})=1$.
  - $p_1(a_{n,n+1})=p_1(c_{n,n+1})=\frac{1}{2}$.

□

7 Proof of Theorem 1.1

We are now in a position to prove our main theorems. We start with in this section with Theorem 1.1, where we will use Theorem 4.9 in conjunction with the counting results of [SW18] (which are a particular case of [Lag24, §8]). We start by noting the following result from [Lag23, Lemma 7.1]:

Lemma 7.1. *Let $K = \mathbb{R}$ or $\mathbb{Q}_p$ for some prime p, and write $|\cdot|_K \colon K^\times \to \mathbb{R}_{>0}$ for the normalised absolute value of K. Let A be an abelian variety over K with dual abelian variety $A^\vee$, and let $\lambda\colon A \to A^\vee$ be a self-dual isogeny, which will have degree m^2 for some $m \in \mathbb{Z}_{\geq 1}$. Then the quantity*

$$c(\lambda) := \frac{\#(A^\vee(K)/\lambda(A(K)))}{\#A[\lambda](K)}$$

satisfies $c(\lambda) = 1/|m|_K$.

In particular, for our map of interest $\phi\colon A_b \to A_b^\vee$, we will have that

$$c_p(\phi_b) = \begin{cases} 2^{-(n-1)} & \text{if } p = \infty, \\ 2^{(n-1)} & \text{if } p = 2, \\ 1 & \text{otherwise.} \end{cases}$$

We turn our interest to counting $G_A(\mathbb{Z})$-orbits in $V_A(\mathbb{Z})$. We will do so by imposing infinitely many congruence conditions:

Definition 7.2. A map $w\colon V_A(\mathbb{Z}) \to [0,1]$ is said to be *defined by infinitely many congruence conditions* if for each prime p there exist functions $w_p\colon V_A(\mathbb{Z}_p) \to [0,1]$ such that

- w_p is $G_A(\mathbb{Z}_p)$-invariant;
- w_p is locally constant outside the subset $\{v \in V_A(\mathbb{Z}_p) \mid \Delta(v) = 0\}$;

which satisfy $w = \prod_p w_p$. We additionally say that w is *acceptable* if the product

$$\prod_p \int_{v \in V_A(\mathbb{Z}_p)} w(v) dv$$

does not diverge to zero, where dv is normalised so that the volume of $V_A(\mathbb{Z}_p)$ is equal to 1 for all p.

Remark 7.3. The acceptability condition is achieved in many instances in the literature by guaranteeing that $1 - \int_{v \in V_A(\mathbb{Z}_p)} w(v) dv = O(p^{-2})$ for large enough p.

Consider a $G_A(\mathbb{Z})$-invariant subset $A \subset V_A(\mathbb{Z})$, and let $w\colon V_A(\mathbb{Z}) \to \mathbb{R}$ be an acceptable function defined by infinitely many congruence conditions. We denote

$$N_w^*(A, X) = \sum_{v \in G_A(\mathbb{Z}) \backslash A_{<X}} \frac{w(v)}{\# \operatorname{Stab}_{G_A(\mathbb{Z})}(v)}.$$

Recall that a $G_A(\mathbb{R})$-orbit in $V_{A,b}(\mathbb{R})$ is called $\mathbb{R}$-soluble if it falls in the image of $\eta_{A,b}$ in (4). Observe that the number of $G_A(\mathbb{R})$-soluble orbits in $V_{A,b}(\mathbb{R})$ is $\#A_b^\vee(\mathbb{R})/\phi(A_b(\mathbb{R}))$. Then, analogously to [Lag24, Theorem 8.18] we get that

$$N_w^*(A, X) \leq \left(\prod_p \int_{v \in V_A(\mathbb{Z}_p)} w(v) dv \right) \frac{|W_1|}{2^{n-1}} \operatorname{vol}(G_A(\mathbb{Z}) \backslash G_A(\mathbb{R})) \operatorname{vol}(B(\mathbb{R})_{<X}) + o(X^{\dim V_A}),$$

where $W_1 \in \mathbb{Q}^\times$ is a fixed scalar number, and where $w = \prod_p w_p$ are the congruence conditions defining w.

To estimate the size of $\operatorname{Sel}_\phi(A_b)$, we note that the non-trivial torsion point $T_b \in A_b^\vee[\hat{\psi}]$ generates a subgroup S_T in $\operatorname{Sel}_\phi(A_b)$ of order dividing 2. In the map

$$\operatorname{Sel}_\phi(A_b) \hookrightarrow G_A(K) \backslash V_{A,b}(K),$$

the elements of $\mathrm{Sel}_\phi(A_b)$ which intersect the reducible orbits correspond exactly to the subgroup S_T, and the complement of S_T falls entirely in the irreducible orbits. Given that $\# S_T \le 2$, it suffices to bound $\mathrm{Sel}_\phi(A_b) \setminus S_T$ by looking at irreducible orbits.

We can prove our results in higher generality by imposing congruence conditions on B. We say that a set $\mathcal{B} \subset B(\mathbb{Z})^{rs}$ is *defined by finitely many congruence conditions* if it is the preimage of the reduction map $B(\mathbb{Z})^{rs} \to B(\mathbb{Z}/N\mathbb{Z})$ for some $N \ge 1$. We will prove the following:

Theorem 7.4. *Let $\mathcal{B} \subset B(\mathbb{Z})$ be defined by finitely many congruence conditions. Then*

$$\lim_{X\to\infty} \frac{\sum_{b\in\mathcal{B},\, \mathrm{ht}(b)<X} \#(\mathrm{Sel}_\phi(A_b) \setminus S_T)}{\#\{b \in \mathcal{B} \mid \mathrm{ht}(b) < X\}} \le 4.$$

Proof. Let $\mathcal{B}_p$ denote the closure of $\mathcal{B}$ inside $B^{rs}(\mathbb{Z}_p)$. For our counting result, it will suffice to count those irreducible $G_A(\mathbb{Z})$-orbits in $V_A(\mathbb{Z})$ corresponding to Selmer elements, as given by Theorem 4.9. Given that we are only guaranteed to have orbits in $\frac{1}{2}V_A(\mathbb{Z})$, and that $\mathrm{Sel}_\phi(A_b) \simeq \mathrm{Sel}_\phi(A_{\lambda\cdot b})$ for any $\lambda \in \mathbb{Q}^\times$, it will suffice to look at orbits with invariants in $2\cdot\mathcal{B}$, for which Selmer elements will always have integral representatives. We choose the counting function

$$w(v) = \begin{cases} \left(\sum_{v'\in G_A(\mathbb{Z})\backslash(G_A(\mathbb{Q})\cdot v\cap V_A(\mathbb{Z}))} \frac{\#\,\mathrm{Stab}_{G_A(\mathbb{Q})}(v')}{\#\,\mathrm{Stab}_{G_A(\mathbb{Z})}(v')}\right)^{-1} & \text{if } \pi(v) \in 2\cdot\mathcal{B} \text{ and } v \text{ is locally soluble,} \\ 0 & \text{otherwise.} \end{cases}$$

This is defined by congruence conditions by the functions

$$w_p(v) = \begin{cases} \left(\sum_{v'\in G_A(\mathbb{Z}_p)\backslash(G_A(\mathbb{Q}_p)\cdot v\cap V_A(\mathbb{Z}_p))} \frac{\#\,\mathrm{Stab}_{G_A(\mathbb{Q}_p)}(v')}{\#\,\mathrm{Stab}_{G_A(\mathbb{Z}_p)}(v')}\right)^{-1} & \text{if } \pi(v) \in 2\cdot\mathcal{B}_p \text{ and } v \text{ is soluble,} \\ 0 & \text{otherwise,} \end{cases}$$

by an analogous argument to [BS15a, Proposition 3.6]. The last part of [Lag24, Lemma 8.5] gives

$$\begin{aligned} \int_{v\in V_A(\mathbb{Z}_p)} w(v)dv &= |W_1|_p \,\mathrm{vol}(G_A(\mathbb{Z}_p)) \int_{b\in 2\cdot\mathcal{B}_p} \frac{\# A_b^\vee(\mathbb{Q}_p)/\phi(A_b(\mathbb{Q}_p))}{\# A_b[\phi](\mathbb{Q}_p)} db \\ &= |W_1|_p \,\mathrm{vol}(G_A(\mathbb{Z}_p)) |2^{-(n-1)}|_p |2^{n(2n+1)}|_p \,\mathrm{vol}(\mathcal{B}_p), \end{aligned}$$

using Lemma 7.1 in the last line. An explicit computation on $\mathrm{vol}(G_A(\mathbb{Z}_p))$ shows that is it $1 - O(p^{-2})$, where the implicit constant is independent of p. Therefore, w is acceptable in the sense of Definition 7.2. Under this counting function, we have that for any given locally soluble $v \in V_A(\mathbb{Z})$ with $\pi(v) \in \mathcal{B}$:

$$\sum_{v'\in G_A(\mathbb{Q})v\cap V_A(\mathbb{Z})} \frac{w(v')}{\#\,\mathrm{Stab}_{G_A(\mathbb{Z})}(v')} = \frac{1}{\#\,\mathrm{Stab}_{G_A(\mathbb{Q})}(v)}.$$

100% of the time, this quantity is equal to 1 by [SW18, Proposition 23]. Thus, we have that

$$\sum_{b\in\mathcal{B}_{<X}} \#(\mathrm{Sel}_\phi(A_b) \setminus S_T) = N_w^*(V_A(\mathbb{Z})^{irr} \cap V_A(\mathbb{R})^{sol}, 2X) + o(X^{n(2n+1)}).$$

With an elementary point-counting argument, we can see that

$$\lim_{X\to\infty} \frac{\prod_p \mathrm{vol}(\mathcal{B}_p)\,\mathrm{vol}(B(\mathbb{Z})_{<2X})}{\#\{b \in \mathcal{B} \mid \mathrm{ht}(b) < X\}} = 2^{n(2n-1)}.$$

Putting it all together, we have that

$$\frac{N_w^*(V_A(\mathbb{Z})^{irr} \cap V_A(\mathbb{R})^{sol}, 2X)}{\#\{b \in \mathcal{B} \mid \mathrm{ht}(b) < X\}} \le \mathrm{vol}(G_A(\mathbb{Z})\backslash G_A(\mathbb{R})) \prod_p \mathrm{vol}(G_A(\mathbb{Z}_p)),$$

which equals the Tamagawa number of $G_A = \mathrm{PSO}_{2n}$, which is 4. This concludes the proof. □

Theorem 1.1 then follows from Theorem 7.4, since S_T has size at most 2.

8 Proof of Theorems 1.2 and 1.3

We will obtain the lower bounds of Theorems 1.2 and 1.3 by looking at the Tamagawa ratio

$$\mathcal{T}(A_b/J_b) = \frac{\#\operatorname{Sel}_{\phi_M^\vee}(A_b^\vee)}{\#\operatorname{Sel}_{\phi_M}(J)}.$$

In our situation, the Greenberg–Wiles formula [NSW08, Theorem 8.7.9] states that

$$\mathcal{T}(A_b/J_b) = \prod_{p\leq\infty} c_p(\phi_{M,b}^\vee) = \prod_{p\leq\infty} \frac{\#J_b(\mathbb{Q}_p)/\phi_M^\vee(A_b^\vee(\mathbb{Q}_p))}{2},$$

This infinite product is convergent, as for all primes away from $\{2,\infty\}$ of good reduction for J_b the local factor is equal to 1. In fact, we also have that $\#J_b(\mathbb{Q}_p)/\phi_M^\vee(A_b^\vee(\mathbb{Q}_p)) \leq 8$, as it is a subset of $H^1(\mathbb{Q}_p, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ (so in particular, $c_p(\phi_{M,b}^\vee) \leq 2$ if $p \neq 2$, and also $c_p(\phi_{M,b}^\vee) \geq \frac{1}{2}$). By [Sch96, Lemma 3.8], if $p \neq 2, \infty$ we additionally have

$$c_p(\phi_{M,b}) = \frac{c_p(J_b)}{c_p(A_b^\vee)} = \frac{\#J_b(\mathbb{Q}_p)/J_{b,0}(\mathbb{Q}_p)}{\#A_b^\vee(\mathbb{Q}_p)/A_{b,0}^\vee(\mathbb{Q}_p)}.$$

We note that a consequence of [Sch96, Lemma 3.8], combined with Lemma 7.1 is that the Tamagawa number of A_b at a prime $p \neq 2, \infty$ coincides with the Tamagawa number of $A_b^\vee$ at p.

A consequence of the above discussion is that we can obtain a lot of information about the sizes of Selmer groups if we understand the ratios between the Tamagawa numbers of J_b and A_b. For statistical purposes, we can ignore the cases $p = 2, \infty$, as they are uniformly controlled. We are interested in the cases when p is of bad reduction for J_b, which for $C_b \colon y^2 = xf(x)$ happens exactly when $p \mid \Delta(xf(x)) = f(0)^2\Delta(f)$. It is sufficient for us to understand the Tamagawa numbers when the discriminant is “as squarefree as possible”. For J_b, the Tamagawa numbers can be computed with relatively standard arguments:

Lemma 8.1. *Suppose $\Delta(b) \neq 0$ and $p \neq 2, \infty$. We have that*

$$c_p(J_b) = \begin{cases} 1 & \text{if } p \nmid f(0) \text{ and } p \parallel \Delta(f), \\ 2 & \text{if } p \parallel f(0) \text{ and } p \nmid \Delta(f). \end{cases}$$

Proof. In the first case, the discriminant of C_b is squarefree, and it is well-known that in that case the Tamagawa number is 1. To elaborate: the equations for the standard affine chart of C_b already define a minimal regular model, and the special fibre $\mathcal{C}_{b,\mathbb{F}_p}$ has only has one connected component. Then, because the reduction is semistable, the Tamagawa number can be computed from the dual graph of $\mathcal{C}_{b,\mathbb{F}_p}$, and because this has only one component it follows that $c_p(J_b) = 1$.

In the second case, the minimal regular model for C_b is obtained by performing one blow-up at the point $(0,0) \in C_b(\mathbb{Q}_p)$. The result is a minimal regular model $\mathcal{C}_{b,\mathbb{Z}_p}$ such that $\mathcal{C}_{b,\mathbb{F}_p}$ has two connected components, intersecting at two different points. It follows from [BLR90, Theorem 9.6.1] that the Tamagawa number is 2 in that case. ☐

Obtaining the Tamagawa numbers for A_b is a bit more subtle. We start by fixing some notation: if A is an abelian variety over $\mathbb{Q}_p$ with semistable reduction, then the connected component of the special fibre of its Néron model $\mathcal{A}$ fits into an exact sequence

$$1 \longrightarrow \mathcal{T} \longrightarrow \mathcal{A}^0_{\mathbb{F}_p} \longrightarrow \mathcal{B} \longrightarrow 1,$$

where $\mathcal{B}$ is an $\mathbb{F}_p$-abelian variety, and $\mathcal{T}$ is a torus. Let ℓ be a prime, and denote the Tate module of A by $T_\ell(A)$. There is a canonical filtration

$$T_\ell(A) \supset \mathcal{M}_f(A) \supset \mathcal{M}_t(A) \supset 0,$$

where $\mathcal{M}_f(A) = T_\ell(A)^{I_p}$ (here I_p denotes the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$), and $\mathcal{M}_t(A)$ is the orthogonal complement of $\mathcal{M}_f(\hat{A})$ with respect to the Weil pairing. We then have the following result (cf. [BK01, Lemma 3]):

Lemma 8.2. *Let B, B' be abelian varieties over $\mathbb{Q}_p$, and let κ be a $G_{\mathbb{Q}_p}$-submodule of $B[\ell]$, where ℓ is a prime. Suppose $\varphi\colon B \to B'$ is an isogeny with kernel κ. Denote by $\overline{\mathcal{M}_f(A)}, \overline{\mathcal{M}_t(A)}$ the projections of $\mathcal{M}_f(A), \mathcal{M}_t(A)$ to $B[\ell]$. Then*

$$\mathrm{ord}_\ell(\Phi_{A'^\vee}(\overline{\mathbb{F}_p})) - \mathrm{ord}_\ell(\Phi_{A^\vee}(\overline{\mathbb{F}_p})) = \dim(\kappa \cap \overline{\mathcal{M}_f(A)}) + \dim(\kappa \cap \overline{\mathcal{M}_t(A)}) - \dim(\kappa).$$

Lemma 8.3. *Suppose $\Delta(b) \neq 0$ and $p \neq 2, \infty$. We have that*

$$c_p(A_b) = c_p(A_b^\vee) = \begin{cases} 1 & \text{if } p \nmid f(0) \text{ and } p \parallel \Delta(f), \\ 1 & \text{if } p \parallel f(0) \text{ and } p \nmid \Delta(f). \end{cases}$$

Proof. In both cases, it suffices to understand how the kernel M of the 2-isogeny $\phi_M\colon J_b \to A_b$ interacts with $\overline{\mathcal{M}_f(A)}$ and $\overline{\mathcal{M}_t(A)}$.

In the first case, the statement is equivalent to asking that $M \subset \overline{\mathcal{M}_f(A)}$ but $M \cap \overline{\mathcal{M}_t(A)} = \{0\}$. The former is forced by the fact that $\#\Phi_{A_b}(\overline{\mathbb{F}_p}) \geq 1$. Let $\tilde{C}$ be the normalisation of the special fibre of C, which is explicitly given as follows: if $xf(x) \equiv (x-a)^2 g(x) \pmod p$ for some $a \neq 0$ in $\mathbb{F}_p$, then $\tilde{C}\colon t^2 = g(x)$. Let $\tilde{\mathcal{J}}$ be the Jacobian of $\tilde{C}$. Then we have

$$1 \to T \hookrightarrow \mathcal{J}^0_{\mathbb{F}_p} \to \tilde{\mathcal{J}} \to 1.$$

Suppose that the roots of $xf(x)$ are $x_0 = 0, x_1, \ldots, x_{2n}$, with the corresponding $P_i = (x_i, 0) \in C(\overline{\mathbb{F}_p})$, and suppose that $x_{2n-1} = x_{2n} \pmod p$. Then any element of $\mathcal{J}^0_{\mathbb{F}_p}[2]$ can be uniquely written as $\sum_{i\in I}[(P_i) - \infty]$ for some subset $I \subset \{0, \ldots, 2n-2\}$. In this situation, $\tilde{\mathcal{J}}[2]$ is the quotient of $\mathcal{J}^0_{\mathbb{F}_p}[2]$ by the relation $[(P_0) - \infty] + \cdots + [(P_{2n-2}) - \infty] = 0$, and $T[2]$ is therefore generated by $[(P_0) - \infty] + \cdots + [(P_{2n-2}) - \infty]$, which may be identified with $[(P_{2n-1}) - \infty] + [(P_{2n}) - \infty]$. We note in particular that $[(P_0) - \infty] \notin T[2]$, and given that $\mathcal{M}_t(A) \cong T_\ell(T)$, we conclude that $M \cap \overline{\mathcal{M}_t(A)} = \{0\}$.

In the second case, it suffices to see that $M \cap \overline{\mathcal{M}_f(A)} = \{0\}$, or equivalently that $[(0,0) - \infty] \notin \overline{\mathcal{M}_f(A)}$. This follows from observing that $(0,0)$ and ∞ lie in different components of $\mathcal{C}$, and using explicit descriptions of Raynaud's specialisation maps as in [Bak08, Appendix A]. ☐

Remark 8.4. Note that the analogue of Lemma 8.3 would not be true in the genus 1 case. There we would have that $c_p(A_b) = 2$ if $p \nmid f(0)$ and $p \parallel \Delta(f)$, as in that situation $T = \mathcal{J}^0_{\mathbb{F}_p}$.

Therefore, in "most" cases of bad reduction, we have that $c_p(J_b)/c_p(A)$ is either 1 or 2. This imbalance forces the overall Selmer ratio to be large on average.

Theorem 8.5. *As $X \to \infty$, we have that*

$$\frac{\sum_{\mathrm{ht}(b)<X} \mathcal{T}(A_b/J_b)}{\sum_{\mathrm{ht}(b)<X} 1} \gg (\log X)^{\log 2}.$$

Proof. We have

$$\log_2(\mathcal{T}(A_b/J_b)) = \sum_{\substack{p \parallel f(0) \\ p \nmid \Delta(f)}} 1 + t_{err}(A_b/J_b).$$

Note that the primes that will contribute to either term on the right hand side are $p \ll X^N$ for $N = 4n-2$. We first deal with the term t_{err}. Let us write $t_{err}(A_b/J_b) = \sum_p t_{err,p}(A_b/J_b)$ according to the contributions of the Tamagawa ratio at p. Then

$$\sum_{\mathrm{ht}(b)<X} t_{err}(A_b/J_b) = \sum_{\mathrm{ht}(b)<X} \sum_{p \ll X^N} t_{err,p}(A_b/J_b) = \sum_{p \ll X^N} \sum_{\mathrm{ht}(b)<X} t_{err,p}(A_b/J_b),$$

We note that $t_{err,p}(A_b/J_b)$ is non-zero only if $p^2 \mid f(0)\Delta(f)$ (i.e. "about $1/p^2$ of the time"), and that $|t_{err,p}(A_b/J_b)| \leq 1$. Given that $\sum_{\mathrm{ht}(b)<X} 1 = O(X^{\dim V})$, it follows that

$$\sum_{\mathrm{ht}(b)<X} t_{err,p}(A_b/J_b) = O\left(\frac{X^{\dim V}}{p^2}\right).$$

Thus

$$\sum_{\mathrm{ht}(b)<X} t_{err}(A_b/J_b) = \sum_{p \ll X^N} O\left(\frac{X^{\dim V}}{p^2}\right) = O\left(X^{\dim V}\right),$$

so

$$\frac{\sum_{\mathrm{ht}(b)<X} t_{err}(A_b/J_b)}{\sum_{\mathrm{ht}(b)<X} 1} = O(1).$$

Similarly, we get that

$$\frac{\sum_{\mathrm{ht}(b)<X} \sum_{\substack{p \| f(0) \\ p \nmid \Delta(f)}} 1}{\sum_{\mathrm{ht}(b)<X} 1} \sim \sum_{p \leq X^N} \frac{1}{p} \sim \log\log X.$$

The result then follows from the convexity of the logarithm. □

Theorem 1.2 directly follows from Theorem 8.5. For Theorem 1.3: the lower bound follows with the same argument, given that $c_p(A_b) = c_p(A_b^\vee)$ if $p \neq 2, \infty$. As hinted in the introduction, a version of this theorem is also true when we apply finitely many congruence conditions, similarly to Theorem 7.4. We carry over the same notions from previous section in this regard.

Theorem 8.6. *Let $\mathcal{B} \subset B(\mathbb{Z})$ be a subset defined by finitely many congruence conditions. Then*

$$(\log X)^{\log 2} \ll \lim_{X\to\infty} \frac{\sum_{b\in\mathcal{B},\, \mathrm{ht}(b)<X} \# \mathrm{Sel}_{\psi^\vee}(A_b)}{\#\{b \in \mathcal{B} \mid \mathrm{ht}(b) < X\}} \ll \log X.$$

Proof. Let us start with the case $\mathcal{B} = B(\mathbb{Z})$. The lower bound follows directly from the arguments of Theorem 8.5, as $\# \mathrm{Sel}_{\psi^\vee}(A_b) \geq \mathcal{T}(A_b/J_b)$. In turn, the upper bound follows from Theorem 6.5: we note that each element of $\mathrm{Sel}_{\psi^\vee} A_b$ embeds inside a different $G_C(\mathbb{Z})$-orbit of $V_{C,b}(\mathbb{Z}) \cap V^{sol}(\mathbb{R})$. If we restrict to $\mathrm{ht}(b) < X$, then the number of such orbits is $O(X^{\dim V} \log X)$, since:

- The irreducible $G_C(\mathbb{Z})$-orbits in $V_C(\mathbb{Z})$ are controlled by Theorem 6.5 and are $O(X^{\dim V} \log X)$; and
- The reducible $G_C(\mathbb{Z})$-orbits in $V_C(\mathbb{Z})$ are, at most, twice the number of orbits in $G_A(\mathbb{Z})$ acting on $V_A(\mathbb{Z})$, so they are $O(X^{\dim V})$.

Hence the theorem holds for the case $\mathcal{B} = B(\mathbb{Z})$. When we apply finitely many congruence conditions, the proof carries over with minimal changes. For the lower bound, the proof of Theorem 8.5 goes through relatively unchanged, while the proof of the upper bound follows from combining Theorem 6.5 with the methods of Section 7. □

9 Heuristics with matrix models

In previous sections we have obtained asymptotics for the average sizes of $\mathrm{Sel}_\phi A_b$, $\mathrm{Sel}_{\psi^\vee} A_b$ and $\mathrm{Sel}_{\phi_M^\vee} A_b^\vee$, but some natural questions remain. For instance, what is the correct order of magnitude for the growth of $\# \mathrm{Sel}_{\psi^\vee} A_b$ (if it even exists)? What is the expected behaviour of the average size of $\mathrm{Sel}_\psi J_b$? We will give some heuristic answers to these questions using matrix models coming from [KT17], which are themselves inspired from the Poonen–Rains heuristics [PR12].

To start with, let us focus on the 2-isogeny Selmer group $\mathrm{Sel}_{\phi_M^\vee} A_b^\vee$. By definition, this Selmer group is the kernel of the map

$$\mathbb{Q}(S,2) \to \prod_{v\in S} \frac{H^1(\mathbb{Q}_v, A_b^\vee[\phi_M^\vee])}{\mathrm{Im}(J_b(\mathbb{Q}_v)/\phi_M^\vee(A_b^\vee(\mathbb{Q}_v)))}, \tag{7}$$

where S is the set of places of $\mathbb{Q}$ that includes the primes dividing $\Delta(b)$, together with 2 and ∞, and $\mathbb{Q}(S,2) \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ is the subgroup of elements unramified outside S. Note that $H^1(\mathbb{Q}_v, A_b^\vee[\phi_M^\vee]) \cong \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2$, and as seen in the previous section:

$$\frac{\# J_b(\mathbb{Q}_v)/\phi_M^\vee(A_b^\vee(\mathbb{Q}_v))}{2} = \frac{c_p(J_b)}{c_p(A_b^\vee)}.$$

The map in (7) is a linear map between $\mathbb{F}_2$-vector spaces, and we will model it as a random linear map: that is, we assume that in the matrix of the map under some fixed basis, all the entries are chosen uniformly at random. In this situation, it is an elementary computation to show that the expected size of the kernel of a random linear map $\mathbb{F}_2^N \to \mathbb{F}_2^M$ is $1 + 2^{N-M} - 2^{-M}$.

We have that $N = \dim_{\mathbb{F}_2} \mathbb{Q}(S,2)$, a quantity that is approximately $\omega(\Delta(b))$. On the other hand, we recover from the computations in the proof of Theorem 8.5 that M is approximately $\omega(\Delta(b)) - \omega(b_{2n})$. The main term in the expected value of the size of the kernel of $\mathbb{F}_2^N \to \mathbb{F}_2^M$ is 2^{N-M}, so we expect the average size of $\mathrm{Sel}_{\phi_M^\vee} A_b^\vee$ to be, approximately, the expected value of $2^{\omega(b_{4n})}$. In the set $1 \le m \le X$, the values of $\omega(m)$ approximate a Poisson distribution with mean $\log\log X$: this is a classical result by Landau (see e.g. [Sat53]). If Z follows a Poisson distribution of mean μ and $x > 0$, then

$$\mathbb{E}[x^Z] = e^{(x-1)\mu}.$$

Therefore,

$$\mathbb{E}[2^{\omega(b_{4n})}] = e^{\log\log X} = \log X.$$

Thus, the expected value of $\#\,\mathrm{Sel}_{\phi_M^\vee} A_b^\vee$ should be of the order of $\log X$ (we do not make predictions about a leading constant).

Let us now comment on $\mathrm{Sel}_{\phi_M} J_b$. A similar discussion to the one above shows that the average size of this Selmer group should be reasonably modelled by the kernel of a random map $\mathbb{F}_2^N \to \mathbb{F}_2^M$, where in this case $N \approx \omega(\Delta(b))$ and $M \approx \omega(\Delta(b)) + \omega(b_{2n})$. In this situation,

$$\mathbb{E}[2^{N-M}] \approx (\log X)^{-1},$$

so the average size of $\mathrm{Sel}_{\phi_M} J_b$ should be $O(1)$. Again, we do not make predictions on what the correct bound should be.

It seems reasonable to compare these predictions for the Selmer groups of the 2-isogenies with whatever expectations we might obtain from geometry-of-numbers. For $\mathrm{Sel}_{\phi^\vee} A_b$, we used the representation (G_C, V_C), and to count the Selmer orbits in these representation precisely, we would need to impose infinitely many congruence conditions. As we saw in Section 7, applying infinitely many congruence conditions when counting $G(\mathbb{Z})$-orbits in $V(\mathbb{Z})$ only gives an upper bound on the size of Selmer elements. However, in many situations this upper bound is expected to be optimal, and is conditional on a uniformity estimate – see [Lag24, Conjecture 8.19] and the surrounding discussion for further context. In our situation, an explicit computation shows that the corresponding congruence conditions that would be applied to count Selmer elements (similarly to Section 7) can be shown to have positive density. If we assume the analogue of [Lag24, Conjecture 8.19] in our situation, this would imply that the average size of $\mathrm{Sel}_{\phi^\vee} A_b$ should be of the exact order of $\log X$.

It is slightly trickier to make a precise prediction on the average size of $\mathrm{Sel}_\psi J_b$ using purely geometry-of-numbers. Theorem 3.10 suggests that we look at the representation (G_B, V_B). Some standard computations show that the number of irreducible $G(\mathbb{Z})$-orbits in $V(\mathbb{Z})$ is of the order of $X^{\dim V_B}$, but that the number of integral orbits in the cusp is $X^{\dim V_B} \log X$. However, the infinitely many congruence conditions corresponding to the Selmer elements appear to have density zero, so normal sieving arguments would not work. It appears that any precise results on this direction would require a very precise control over error terms; similarly to [Lag24, Conjecture 8.19], this appears to be rather complicated in general with our current methods.

Finally, we mention that all the above discussions are for curves of genus $g \geq 2$. In the genus 1 case, our curves would be elliptic curves of the form $E_{a,b}\colon y^2 = x(x^2 + ax + b)$, with $\phi = \mathrm{id}$ and ϕ_M, $\phi_M^\vee$ being the natural 2-isogenies associated to such a curve. This is exactly the situation of [KL14, Corollary 1.2], where it is shown that the average size of $\mathrm{Sel}_{\phi_M} E_{a,b}$ diverges, and it is predicted that its order of growth should be of the order of $\sqrt{\log X}$. This difference in the expected order of magnitude is likely related to the fact that the analogue of Lemma 8.3 is not true in genus 1 (the upper row should be equal to 2, as can be seen through Tate's algorithm). In this situation, our matrix model heuristics predict, through analogous computations to the above ones, that the average size of both $\mathrm{Sel}_{\phi_M} E_{a,b}$ and $\mathrm{Sel}_{\phi_M^\vee} E_{a,b}^\vee$ should be of the order of $\sqrt{\log X}$, as predicted by [KL14].

References

[Bak08] Matthew Baker. "Specialization of linear systems from curves to graphs". In: *Algebra Number Theory* 2.6 (2008). With an appendix by Brian Conrad, pp. 613–653. ISSN: 1937-0652,1944-7833. DOI: 10.2140/ant.2008.2.613. URL: https://doi.org/10.2140/ant.2008.2.613.

[BW14] Fabrizio Barroero and Martin Widmer. "Counting lattice points and O-minimal structures". In: *Int. Math. Res. Not. IMRN* 18 (2014), pp. 4932–4957. ISSN: 1073-7928,1687-0247. DOI: 10.1093/imrn/rnt102. URL: https://doi.org/10.1093/imrn/rnt102.

[BES20] Manjul Bhargava, Noam Elkies, and Ari Shnidman. "The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$". In: *J. Lond. Math. Soc. (2)* 101.1 (2020), pp. 299–327. ISSN: 0024-6107,1469-7750. DOI: 10.1112/jlms.12271. URL: https://doi.org/10.1112/jlms.12271.

[BG13] Manjul Bhargava and Benedict 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*. Vol. 22. Tata Inst. Fundam. Res. Stud. Math. Tata Inst. Fund. Res., Mumbai, 2013, pp. 23–91. ISBN: 978-93-80250-49-6.

[BG14] Manjul Bhargava and Benedict H. Gross. "Arithmetic invariant theory". In: *Symmetry: representation theory and its applications*. Vol. 257. Progr. Math. Birkhäuser/Springer, New York, 2014, pp. 33–54. ISBN: 978-1-4939-1589-7; 978-1-4939-1590-3. DOI: 10.1007/978-1-4939-1590-3_3. URL: https://doi.org/10.1007/978-1-4939-1590-3_3.

[BGW15] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang. "Arithmetic invariant theory II: Pure inner forms and obstructions to the existence of orbits". In: *Representations of reductive groups*. Vol. 312. Progr. Math. Birkhäuser/Springer, Cham, 2015, pp. 139–171. ISBN: 978-3-319-23442-7; 978-3-319-23443-4. DOI: 10.1007/978-3-319-23443-4_5. URL: https://doi.org/10.1007/978-3-319-23443-4_5.

[BS15a] Manjul Bhargava and Arul Shankar. "Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves". In: *Ann. of Math. (2)* 181.1 (2015), pp. 191–242. ISSN: 0003-486X,1939-8980. DOI: 10.4007/annals.2015.181.1.3. URL: https://doi.org/10.4007/annals.2015.181.1.3.

[BS15b] Manjul Bhargava and Arul Shankar. "Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0". In: *Ann. of Math. (2)* 181.2 (2015), pp. 587–621. ISSN: 0003-486X,1939-8980. DOI: 10.4007/annals.2015.181.2.4. URL: https://doi.org/10.4007/annals.2015.181.2.4.

[Bha+19] Manjul Bhargava et al. "3-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field". In: *Duke Math. J.* 168.15 (2019), pp. 2951–2989. ISSN: 0012-7094,1547-7398. DOI: 10.1215/00127094-2019-0031. URL: https://doi.org/10.1215/00127094-2019-0031.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*. Vol. 21. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1990, pp. x+325. ISBN: 3-540-50587-3. DOI: 10.1007/978-3-642-51438-8. URL: https://doi.org/10.1007/978-3-642-51438-8.

[BK01] Armand Brumer and Kenneth Kramer. “Non-existence of certain semistable abelian varieties”. In: *Manuscripta Math.* 106.3 (2001), pp. 291–304. ISSN: 0025-2611,1432-1785. DOI: 10.1007/PL00005885. URL: https://doi.org/10.1007/PL00005885.

[Cas78] J. W. S. Cassels. *Rational quadratic forms*. Vol. 13. London Mathematical Society Monographs. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978, pp. xvi+413. ISBN: 0-12-163260-1.

[KT17] Daniel M. Kane and Jack A. Thorne. “On the ϕ-Selmer groups of the elliptic curves $y^2 = x^3 - Dx$”. In: *Math. Proc. Cambridge Philos. Soc.* 163.1 (2017), pp. 71–93. ISSN: 0305-0041,1469-8064. DOI: 10.1017/S0305004116000724. URL: https://doi.org/10.1017/S0305004116000724.

[KL14] Zev Klagsbrun and Robert J. Lemke Oliver. “The distribution of the Tamagawa ratio in the family of elliptic curves with a two-torsion point”. In: *Res. Math. Sci.* 1 (2014), Art. 15, 10. ISSN: 2522-0144,2197-9847. DOI: 10.1186/s40687-014-0015-4. URL: https://doi.org/10.1186/s40687-014-0015-4.

[Knu+98] Max-Albert Knus et al. *The book of involutions*. Vol. 44. American Mathematical Society Colloquium Publications. With a preface in French by J. Tits. American Mathematical Society, Providence, RI, 1998, pp. xxii+593. ISBN: 0-8218-0904-0. DOI: 10.1090/coll/044. URL: https://doi.org/10.1090/coll/044.

[Lag23] Jef Laga. “Arithmetic statistics of Prym surfaces”. In: *Math. Ann.* 386.1-2 (2023), pp. 247–327. ISSN: 0025-5831,1432-1807. DOI: 10.1007/s00208-022-02398-5. URL: https://doi.org/10.1007/s00208-022-02398-5.

[Lag24] Jef Laga. “Graded Lie Algebras, Compactified Jacobians and Arithmetic Statistics”. In: *J. Eur. Math. Soc.* (2024). Published online first. DOI: 10.4171/JEMS/1526.

[LR25] Jef Laga and Beth Romano. *Families of curves in Vinberg representations*. 2025. arXiv: 2508.09607 [math.NT]. URL: https://arxiv.org/abs/2508.09607.

[LT24] Jef Laga and Jack A. Thorne. *100% of odd hyperelliptic Jacobians have no rational points of small height*. 2024. arXiv: 2405.10224 [math.NT]. URL: https://arxiv.org/abs/2405.10224.

[Lan75] Serge Lang. $\mathrm{SL}_2(\mathbf{R})$. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1975, pp. xvi+428.

[Mum70] David Mumford. *Abelian varieties*. Vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. Tata Institute of Fundamental Research, Bombay; by Oxford University Press, London, 1970, pp. viii+242.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Second. Vol. 323. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2008, pp. xvi+825. ISBN: 978-3-540-37888-4. DOI: 10.1007/978-3-540-37889-1. URL: https://doi.org/10.1007/978-3-540-37889-1.

[Oll25] Martí Oller. “The density of ADE families of curves having squarefree discriminant”. en. In: *Journal de théorie des nombres de Bordeaux* 37.3 (2025), pp. 989–1029. DOI: 10.5802/jtnb.1349. URL: https://jtnb.centre-mersenne.org/articles/10.5802/jtnb.1349/.

[Pan05] Dmitri I. Panyushev. “On invariant theory of θ-groups”. In: *J. Algebra* 283.2 (2005), pp. 655–670. ISSN: 0021-8693,1090-266X. DOI: 10.1016/j.jalgebra.2004.03.032. URL: https://doi.org/10.1016/j.jalgebra.2004.03.032.

[PR11] Bjorn Poonen and Eric Rains. “Self cup products and the theta characteristic torsor”. In: *Math. Res. Lett.* 18.6 (2011), pp. 1305–1318. ISSN: 1073-2780,1945-001X. DOI: 10.4310/MRL.2011.v18.n6.a18. URL: https://doi.org/10.4310/MRL.2011.v18.n6.a18.

[PR12] Bjorn Poonen and Eric Rains. “Random maximal isotropic subspaces and Selmer groups”. In: *J. Amer. Math. Soc.* 25.1 (2012), pp. 245–269. ISSN: 0894-0347,1088-6834. DOI: 10.1090/S0894-0347-2011-00710-8. URL: https://doi.org/10.1090/S0894-0347-2011-00710-8.

[Ree+12] Mark Reeder et al. “Gradings of positive rank on simple Lie algebras”. In: *Transform. Groups* 17.4 (2012), pp. 1123–1190. ISSN: 1083-4362,1531-586X. DOI: 10.1007/s00031-012-9196-3. URL: https://doi.org/10.1007/s00031-012-9196-3.

[RT18] Beth Romano and Jack A. Thorne. “On the arithmetic of simple singularities of type E”. In: *Res. Number Theory* 4.2 (2018), Paper No. 21, 34. ISSN: 2522-0160,2363-9555. DOI: 10.1007/s40993-018-0110-5. URL: https://doi.org/10.1007/s40993-018-0110-5.

[RT21] Beth Romano and Jack A. Thorne. “E_8 and the average size of the 3-Selmer group of the Jacobian of a pointed genus-2 curve”. In: *Proc. Lond. Math. Soc. (3)* 122.5 (2021), pp. 678–723. ISSN: 0024-6115,1460-244X. DOI: 10.1112/plms.12388. URL: https://doi.org/10.1112/plms.12388.

[Sat53] L. G. Sathe. “On a problem of Hardy on the distribution of integers having a given number of prime factors. II”. In: *J. Indian Math. Soc. (N.S.)* 17 (1953), pp. 83–141. ISSN: 0019-5839,2455-6475.

[Sch96] Edward F. Schaefer. “Class groups and Selmer groups”. In: *J. Number Theory* 56.1 (1996), pp. 79–114. ISSN: 0022-314X,1096-1658. DOI: 10.1006/jnth.1996.0006. URL: https://doi.org/10.1006/jnth.1996.0006.

[Sha19] Ananth N. Shankar. “2-Selmer groups of hyperelliptic curves with marked points”. In: *Trans. Amer. Math. Soc.* 372.1 (2019), pp. 267–304. ISSN: 0002-9947,1088-6850. DOI: 10.1090/tran/7546. URL: https://doi.org/10.1090/tran/7546.

[SW18] Arul Shankar and Xiaoheng Wang. “Rational points on hyperelliptic curves having a marked non-Weierstrass point”. In: *Compos. Math.* 154.1 (2018), pp. 188–222. ISSN: 0010-437X,1570-5846. DOI: 10.1112/S0010437X17007515. URL: https://doi.org/10.1112/S0010437X17007515.

[Tho13] Jack A. Thorne. “Vinberg’s representations and arithmetic invariant theory”. In: *Algebra Number Theory* 7.9 (2013), pp. 2331–2368. ISSN: 1937-0652,1944-7833. DOI: 10.2140/ant.2013.7.2331. URL: https://doi.org/10.2140/ant.2013.7.2331.

[Tho15] Jack A. Thorne. “E_6 and the arithmetic of a family of non-hyperelliptic curves of genus 3”. In: *Forum Math. Pi* 3 (2015), e1, 41. ISSN: 2050-5086. DOI: 10.1017/fmp.2014.2. URL: https://doi.org/10.1017/fmp.2014.2.

[Vin76] È. B. Vinberg. “The Weyl group of a graded Lie algebra”. In: *Izv. Akad. Nauk SSSR Ser. Mat.* 40.3 (1976), pp. 488–526, 709. ISSN: 0373-2436.