MOST ODD-DEGREE BINARY FORMS FAIL TO PRIMITIVELY REPRESENT A SQUARE

ASHVIN A. SWAMINATHAN

ABSTRACT. Let F be a separable integral binary form of odd degree $N \geq 5$. A result of Darmon and Granville known as "Faltings plus epsilon" implies that the degree-N *superelliptic equation* $y^2 = F(x, z)$ has finitely many primitive integer solutions. In this paper, we consider the family $\mathscr{F}_N(f_0)$ of degree-N superelliptic equations with fixed leading coefficient $f_0 \in \mathbb{Z} \smallsetminus \pm\mathbb{Z}^2$, ordered by height. For every sufficiently large N, we prove that among equations in the family $\mathscr{F}_N(f_0)$, more than 74.9% are insoluble, and more than 71.8% are everywhere locally soluble but fail the Hasse principle due to the Brauer–Manin obstruction. We further show that these proportions rise to at least 99.9% and 96.7%, respectively, when f_0 has sufficiently many prime divisors of odd multiplicity. Our result can be viewed as a strong asymptotic form of "Faltings plus epsilon" for superelliptic equations and constitutes an analogue of Bhargava's result that most hyperelliptic curves over $\mathbb{Q}$ have no rational points.

1. INTRODUCTION

Let F be a separable integral binary form of degree $N \geq 5$. When $N = 2n$ is even, the subscheme C_F of the weighted projective plane $\mathbb{P}^2_{\mathbb{Q}}(1, n, 1)$ cut out by the equation $y^2 = F(x, z)$ is known as a *hyperelliptic curve*, and by Faltings' Theorem (see [Fal83, Satz 7]), the curve C_F has only finitely many rational points. In [Bha13, Theorem 1], Bhargava established the following "strong asymptotic form" of Faltings' Theorem for hyperelliptic curves: when integral binary N-ic forms are ordered by height, the density of forms F such that the curve C_F has a rational point is $o(2^{-n})$. In other words, most even-degree binary forms fail to represent a square.

When $N = 2n + 1$ is odd, the equation $y^2 = F(x, z)$ is called *superelliptic*. In contrast with the case of hyperelliptic curves, the problem of studying rational solutions to superelliptic equations is trivial: given any pair $(x_0, z_0) \in \mathbb{Q}^2$, the triple

$$(x, y, z) = (x_0 \cdot F(x_0, z_0), F(x_0, z_0)^{n+1}, z_0 \cdot F(x_0, z_0)) \in \mathbb{Q}^3 \tag{1}$$

is a solution to the equation $y^2 = F(x, z)$, and in fact, the subscheme $S_F \subset \mathbb{P}^2_{\mathbb{Q}}(2, 2n+1, 2)$ cut out by this equation is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$. On the other hand, the problem of studying *primitive integer solutions* — triples $(x_0, y_0, z_0) \in \mathbb{Z}^3$ such that $y_0^2 = F(x_0, z_0)$ and $\gcd(x_0, z_0) = 1$ — is considerably more interesting. For instance, a result of Darmon and Granville states that $y^2 = F(x, z)$ has only finitely many primitive integer solutions (see [DG95, Theorem 1']). Given this analogue of Faltings' Theorem, it is natural to expect that an analogue of Bhargava's strong asymptotic form holds for primitive integer solutions to superelliptic equations. The purpose of this paper is to prove this expectation, i.e., that most integral odd-degree binary forms fail to *primitively* represent a square.

1.1. Superelliptic Stacky Curves.

In the rest of the paper, it will be convenient to reinterpret primitive integer solutions to the superelliptic equation $y^2 = F(x, z)$ as integral points on a certain *stacky curve*, which we denote by $\mathcal{S}_F$ and define as follows. Consider the punctured affine surface

$$\widetilde{S}_F := V(y^2 = F(x, z)) \subset \mathbb{A}^3_{\mathbb{Z}} \smallsetminus \{(0, 0, 0)\}. \tag{2}$$

The group $\mathbb{G}_m$ acts by scaling on $\widetilde{S}_F$ via $\lambda \cdot (x_0, y_0, z_0) = (\lambda^2 \cdot x_0, \lambda^{2n+1} \cdot y_0, \lambda^2 \cdot z_0)$. The map $\widetilde{S}_F \to \mathbb{P}^1_{\mathbb{Z}}$ defined by $(x, y, z) \to [x : z]$ is $\mathbb{G}_m$-equivariant, and the field of $\mathbb{G}_m$-invariant rational functions on $\widetilde{S}_F$ is generated by x/z, so the scheme quotient $\widetilde{S}_F/\mathbb{G}_m$ is isomorphic to $\mathbb{P}^1_{\mathbb{Z}}$. The associated stack quotient $\mathcal{S}_F := [\widetilde{S}_F/\mathbb{G}_m]$ is a stacky curve with coarse moduli space $\mathbb{P}^1_{\mathbb{Z}}$. The $\mathbb{G}_m$-action on $\widetilde{S}_F$ has

Date: June 23, 2022.
2020 *Mathematics Subject Classification.* 11D45, 14G05 (primary), and 20G25, 14H25 (secondary).
This research was supported by the Paul and Daisy Soros Fellowship and the NSF Graduate Research Fellowship.

a nontrivial stabilizer isomorphic to the group scheme μ_2 if and only if $y = 0$, so $\mathcal{S}_F$ has a "$\frac{1}{2}$-point" at each of the $2n+1$ distinct roots of F over the algebraic closure.

Let R be a principal ideal domain. We say that a triple (x_0, y_0, z_0) is *R-primitive* if we have $Rx_0 + Rz_0 = R$. The set of R-primitive solutions to $y^2 = F(x,z)$ is readily seen to be in bijection with the set $\widetilde{S}_F(R)$ of morphisms $\operatorname{Spec} R \to \widetilde{S}_F$ (i.e., R-points of $\widetilde{S}_F$), which in turn corresponds bijectively with the set $\mathcal{S}_F(R)$: indeed, specifying a map $\operatorname{Spec} R \to \mathcal{S}_F$ is definitionally equivalent to specifying a map $L \to \widetilde{S}_F$, where L is a torsor of $\operatorname{Spec} R$ by $\mathbb{G}_m$, but $\operatorname{Spec} R$ has no nontrivial $\mathbb{G}_m$-torsors. In what follows, we abuse notation by writing $\mathcal{S}_F(R)$ for the set of R-primitive solutions to $y^2 = F(x,z)$, regardless of whether F is separable.

1.2. **Main Results.** Our results concern families of superelliptic equations $y^2 = F(x,z)$ of degree $2n+1 \geq 3$ having fixed leading coefficient $f_0 := F(1,0) \in \mathbb{Z} \smallsetminus \{0\}$. Suppose that $|f_0|$ is not a square, let $|f_0| = m^2\kappa$, where $m, \kappa \in \mathbb{Z}$ and κ is squarefree, and define the following quantities:

$$\mu_{f_0} := \prod_{p \mid \kappa} \left(\frac{1}{p^2} + \frac{p-1}{p^{n+1}} \right) \quad \text{and} \quad \mu'_{f_0} := \prod_{p \mid \kappa} \left(1 - \frac{1}{p^{2p+1}} \right)$$

For a $\mathbb{Z}$-algebra R, we write $\mathscr{F}_{2n+1}(f_0, R) \subset R[x,z]$ for the set of binary forms of degree $2n+1$ with leading coefficient equal to f_0; when $R = \mathbb{Z}$, we abbreviate $\mathscr{F}_{2n+1}(f_0, \mathbb{Z})$ as $\mathscr{F}_{2n+1}(f_0)$. For simplicity, we sometimes write $\mathscr{F}_{2n+1}(f_0)$ to mean the family of superelliptic equations or superelliptic stacky curves defined by the forms in $\mathscr{F}_{2n+1}(f_0)$. The *height* $H(F)$ of a binary form $F(x,z) = \sum_{i=0}^{2n+1} f_i x^{2n+1-i} z^i \in \mathscr{F}_{2n+1}(f_0)$ is defined as follows

$$H(F) := \max\{|f_0^{i-1} f_i|^{2n(2n+1)/i} : i = 1, \dots, 2n+1\}.$$

With this setup, we prove the following analogue for superelliptic stacky curves of [Bha13, Theorem 1]:

Theorem 1. *For every sufficiently large n, most superelliptic stacky curves in the family $\mathscr{F}_{2n+1}(f_0)$ have no primitive integer solutions. More precisely:*

(a) *Suppose $2 \nmid f_0$. For every $n \geq 5$, a positive proportion of forms $F \in \mathscr{F}_{2n+1}(f_0)$, when ordered by height, have the property that $\mathcal{S}_F(\mathbb{Z}) = \varnothing$. Moreover, the lower density of forms $F \in \mathscr{F}_{2n+1}(f_0)$ such that $\mathcal{S}_F(\mathbb{Z}) = \varnothing$ is at least $1 - \mu_{f_0} + o(2^{-n})$.*

(b) *Suppose $2 \mid f_0$. The lower density of forms $F \in \mathscr{F}_{2n+1}(f_0)$ such that $\mathcal{S}_F(\mathbb{Z}) = \varnothing$ is at least $1 - \mu_{f_0} + O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ for some real numbers $\varepsilon_1, \varepsilon_2 > 0$.*

As shown in Table 1, the quantity $1 - \mu_{f_0}$ — which by Theorem 1 constitutes a lower bound on the density of insoluble equations in $\mathscr{F}_{2n+1}(f_0)$ in the large-n limit — rapidly approaches 1 as the number of prime factors of κ grows. Furthermore, the method used to prove Theorem 1 can be easily adapted to obtain a similar result when the family $\mathscr{F}_{2n+1}(f_0)$ is replaced by any subfamily defined by congruence conditions modulo finitely many prime powers.

Note that Theorem 1 is subject to the condition that $|f_0|$ is *not* a square. When $|f_0|$ is a square, every form $F \in \mathscr{F}_{2n+1}(f_0)$ is such that $y^2 = F(x,z)$ has a trivial solution, namely $(x,y,z) = (\operatorname{sign}(f_0), \sqrt{|f_0|}, 0)$. We expect that for most $F \in \mathscr{F}_{2n+1}(f_0)$, the equation $y^2 = F(x,z)$ has no solutions other than the trivial one. The presence of the trivial solution renders this expectation difficult to prove: e.g., to obtain the analogous result for rational points on monic odd-degree hyperelliptic curves, Poonen and Stoll [PS14] combined work of Bhargava and Gross [BG13] on equidistribution of the 2-Selmer elements of the Jacobians of these curves with a variant of Chabauty's method (cf. [SW18], in which Shankar and Wang treat the even-degree case, as well as the work of Thorne and Romano [RT21] and Laga [Lag21], which prove similar theorems for certain families of non-hyperelliptic curves). To the author's knowledge, analogues of the notion of Selmer group and of Chabauty's method remain to be formulated for superelliptic stacky curves.

$\{p \mid \kappa\} \supset$	$\{2\}$	$\{3\}$	$\{5\}$	$\{2,3\}$	$\{2,5\}$	$\{3,7\}$	$\{2,3,7\}$
$\lim_{n\to\infty} 1-\mu_{f_0} \geq$	75.0%	88.8%	96.0%	97.2%	99.0%	99.7%	99.9%
$\lim_{n\to\infty} \mu'_{f_0}-\mu_{f_0} \geq$	71.8%	88.8%	95.9%	94.0%	95.8%	99.7%	96.7%

TABLE 1. A table demonstrating the strength of the limiting lower bounds $\lim_{n\to\infty} 1-\mu_{f_0}$ (resp., $\lim_{n\to\infty} \mu'_{f_0}-\mu_{f_0}$) on the density of insoluble superelliptic equations given by Theorem 1 (resp., on the density of superelliptic equations having a Brauer–Manin obstruction to solubility given by Theorem 2).

In the course of proving Theorem 1, we actually prove the stronger statement that most superelliptic stacky curves have a 2-descent obstruction to having an integral point. Since these stacky curves typically have integral points everywhere locally, it follows that most of them fail the Hasse principle (i.e., do *not* have a $\mathbb{Z}$-point despite having a $\mathbb{Z}_v$-point for every place v of $\mathbb{Q}$) due to a 2-descent obstruction. Upon showing that such a 2-descent obstruction yields a case of the Brauer–Manin obstruction, we obtain the following analogue for superelliptic stacky curves of [Bha13, Corollary 4][1] (see also the work of Thorne [Tho15] and Thorne and Romano [RT18], which prove similar theorems for certain families of non-hyperelliptic curves):

Theorem 2. *The lower density of forms $F \in \mathscr{F}_{2n+1}(f_0)$, when ordered by height, such that the stacky curve $\mathcal{S}_F$ fails the Hasse principle due to the Brauer–Manin obstruction is at least $\mu'_{f_0}-\mu_{f_0}+o(2^{-n})$ if $2\nmid f_0$ and is at least $\mu'_{f_0}-\mu_{f_0}+O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ for some $\varepsilon_1,\varepsilon_2>0$ if $2\mid f_0$.*

The proportion $\mu'_{f_0}-\mu_{f_0}$, which can be thought of as a lower bound on the density of superelliptic equations with leading coefficient f_0 having a Brauer–Manin obstruction to solubility in the large-n limit, approaches $\approx 96.7\%$ as the number of prime factors of κ grows; see Table 1.

The *genus* of a stacky curve can be defined in terms of the Euler characteristic of an orbifold curve; see [Dar97, section entitled "Orbifolds, and the topology of M-curves"]. In [BP19], Bhargava and Poonen prove that all (suitably defined) stacky curves S of genus less than $\frac{1}{2}$ over $\mathbb{Z}$ satisfy the Hasse principle; i.e., if $S(\mathbb{R})\neq\varnothing$ and $S(\mathbb{Z}_p)\neq\varnothing$ for every prime $p\in\mathbb{Z}$, then $S(\mathbb{Z})\neq\varnothing$. On the other hand, there is no guarantee that a stacky curve of genus at least $\frac{1}{2}$ satisfies the Hasse principle: indeed, for any separable integral binary form F of degree $2n+1\geq 3$, the genus of the associated stacky curve $\mathcal{S}_F$ is given by $\frac{2n+1}{4}>\frac{1}{2}$, and Theorem 2 demonstrates that these stacky curves often fail the Hasse principle.

1.3. **Method of Proof.** Our strategy is to transform the problem of counting soluble superelliptic equations into one of counting integral orbits of a certain representation by devising a suitable orbit construction. In §3, we prove that elements of $\mathcal{S}_F(\mathbb{Z})$ naturally give rise to certain square roots of the ideal class of the inverse different of a ring R_F associated to the form F. Via a parametrization that we introduced in [Swa21], these square roots correspond to certain integral orbits for the action of the split odd special orthogonal group G on a space V of self-adjoint operators T, where the characteristic polynomial of T is equal to the *monicized form* $F_{\mathrm{mon}}(x,1):=\frac{1}{f_0}\cdot F(x,f_0 z)$.

The parametrization in [Swa21] is explicitly leading-coefficient-dependent and is thus particularly well-suited for applications concerning binary forms with fixed leading coefficient. By generalizing an equidistribution argument that we developed in joint work with Bhargava and Shankar (see [BSS21], where we used the very same parametrization to determine the second moment of the size of the 2-Selmer group of elliptic curves), one can average the bounds in Theorems 1 and 2 over all leading coefficients and thus deduce analogues of these theorems for the full family of superelliptic equations of given degree. In this paper, we fix the leading coefficient for two reasons: doing so simplifies the orbit-counting and allows us to prove a stronger result, that within each

[1]The proof of [Bha13, Corollary 4] has a gap; see Remark 12, where we explain how a certain step in the proof of Theorem 2 may be modified to obtain a complete proof of [Bha13, Corollary 4].

thin subfamily of superelliptic equations with fixed leading coefficient, most members fail the Hasse principle.

In §2, we discuss the representation of G on V, the orbits of which also correspond to 2-Selmer elements of the Jacobians of monic odd-degree hyperelliptic curves (see the work of Bhargava and Gross [BG13]), we define the ring R_F, and we recall the parametrization from [Swa21]. In §4, we bound the p-adic density of the set of elements in $V(\mathbb{Z}_p)$ that arise from $\mathbb{Z}_p$-primitive solutions via the orbit construction in §3 for each prime p. In §5, we prove Theorem 1 by combining these density bounds with orbit-counting results of Bhargava and Gross (see [BG13, §10]). Finally, in §6, we define the notions of 2-descent obstruction and Brauer–Manin obstruction for superelliptic stacky curves, and we prove Theorem 2.

2. Algebraic Preliminaries

In this section, we recall several algebraic notions that feature in our construction of orbits from integral points on superelliptic stacky curves. We begin in §2.1 by introducing the representation of G on V. Then, in §2.2, we define the ring R_F associated to a binary form F, and in §2.3, we recall a parametrization from [Swa21] of square roots of the ideal class of the inverse different of R_F. We finish in §2.4 by describing the parametrization over fields.

2.1. A Representation of the Split Odd Special Orthogonal Group.

Let W be the $\mathbb{Z}$-lattice of rank $2n+1$ equipped with a nondegenerate symmetric bilinear form $[-,-]\colon W \times W \to \mathbb{Z}$ that has signature $(n+1, n)$ after extending scalars to $\mathbb{R}$. By [Ser73, Chapter V]), the lattice W is unique up to isomorphism over $\mathbb{Z}$, and there is a $\mathbb{Z}$-basis

$$W = \mathbb{Z}\langle e_1, \dots, e_n, u, e_1', \dots, e_n' \rangle \tag{3}$$

such that $[e_i, e_j] = [e_i', e_j'] = [e_i, u] = [e_i', u] = 0$, $[e_i, e_j'] = \delta_{ij}$, and $[u, u] = 1$ for all relevant pairs (i, j). We denote by A_0 the matrix of $[-,-]$ with respect to the basis (3).

For a $\mathbb{Z}$-algebra R, let $W_R := W \otimes_{\mathbb{Z}} R$. For a field k of characteristic not equal to 2, the k-vector space W_k equipped with the bilinear form $[-,-]$ is called the *split orthogonal space* of dimension $2n+1$ and determinant $(-1)^n$ over k and is unique up to k-isomorphism [MH73, §6]. The space W_k is called "split" because it is a nondegenerate quadratic space containing a maximal isotropic subspace (defined over k) for the bilinear form $[-,-]$.

Let $T \in \mathrm{End}_R(W_R)$. Recall that the adjoint transformation $T^\dagger \in \mathrm{End}_R(W_R)$ of T with respect to the form $[-,-]$ is determined by the formula $[Tv, w] = [v, T^\dagger w]$ for all $v, w \in W_R$, and that T is said to be *self-adjoint* if $T = T^\dagger$. If T is expressed as a matrix with respect to the basis (3), then T is self-adjoint with respect to the form $[-,-]$ if and only if $T^T A_0 = A_0 T$.

Let V be the affine space defined over $\operatorname{Spec}\mathbb{Z}$ whose R-points are given by

$$V(R) = \{T \in \mathrm{End}_R(W_R) : T = T^\dagger\}$$

for any $\mathbb{Z}$-algebra R. An R-automorphism $g \in \mathrm{Aut}_R(W_R)$ is called *orthogonal* with respect to the form $[-,-]$ if $[g(v), g(w)] = [v, w]$ for all $v, w \in W_R$. If g is expressed as a matrix with respect to the basis (3), then g is orthogonal with respect to the form $[-,-]$ if and only if $g^T A_0 g = A_0$. Let $G := \mathrm{SO}(W)$ be the group scheme defined over $\operatorname{Spec}\mathbb{Z}$ whose R-points are given by

$$G(R) = \{g \in \mathrm{Aut}_R(W_R) : g \text{ is orthogonal with respect to } [-,-] \text{ and } \det g = 1\}$$

for any $\mathbb{Z}$-algebra R. The group scheme G is known as the *split odd special orthogonal group* of the lattice W, and it acts on V by conjugation: for $g \in G(R)$ and $T \in V(R)$, the map $gTg^{-1} \in \mathrm{End}_R(W_R)$ is readily checked to be self-adjoint with respect to $[-,-]$ and is therefore an element of $V(R)$. We thus obtain a linear representation $G \to \mathrm{GL}(V)$ of dimension $\dim V = 2n^2 + 3n + 1$.

Since G acts on V by conjugation, the characteristic polynomial

$$\mathrm{ch}(T) := \det(x \cdot \mathrm{id} - T) = x^{2n+1} + \sum_{i=1}^{2n+1} c_i x^{2n+1-i} \in R[x]$$

is invariant under the action of $G(R)$ for each $T \in V(R)$. In fact, by [Bou75, §8.3, part (VI) of §13.2], the coefficients $c_1, \ldots, c_{2n+1}$, which have respective degrees $1, \ldots, 2n+1$, freely generate the ring of G-invariant functions on V.

2.2. **Rings Associated to Binary Forms.** For the rest of §2, let R be a principal ideal domain (we typically take R to be $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_p$, $\mathbb{Z}/p\mathbb{Z}$, or $\mathbb{Q}_p$, where $p \in \mathbb{Z}$ is a prime), and let k be the fraction field of R. Let $n \geq 1$, and let

$$F(x,z) = \sum_{i=0}^{2n+1} f_i x^{2n+1-i} z^i \in R[x,z]$$

be a separable binary form of degree $2n+1$ with leading coefficient $f_0 \in R \smallsetminus \{0\}$.

Consider the étale k-algebra

$$K_F := k[x]/(F(x,1)).$$

Let θ denote the image of x in K_F. For each $i \in \{1, \ldots, 2n\}$, let p_i be the polynomial defined by

$$p_i(t) := \sum_{j=0}^{i-1} f_j t^{i-j},$$

and let $\zeta_i := p_i(\theta)$. To the binary form F, there is a naturally associated free R-submodule $R_F \subset K_F$ having rank $2n+1$ and R-basis given by

$$R_F := R\langle 1, \zeta_1, \zeta_2, \ldots, \zeta_{2n} \rangle. \tag{4}$$

The module R_F is of significant interest in its own right and has been studied extensively in the literature. In [BM72, proof of Lemma 3], Birch and Merriman proved that the discriminant of F is equal to the discriminant of R_F, and in [Nak89, Proposition 1.1], Nakagawa proved that R_F is actually a ring (and hence an order in K_F) having multiplication table

$$\zeta_i \zeta_j = \sum_{k=j+1}^{\min\{i+j,2n+1\}} f_{i+j-k}\zeta_k - \sum_{k=\max\{i+j-(2n+1),1\}}^{i} f_{i+j-k}\zeta_k, \tag{5}$$

where $1 \leq i \leq j \leq 2n$ and we take $\zeta_0 = 1$ and $\zeta_{2n+1} = -f_{2n+1}$ for the sake of convenience. (To be clear, these results of Nakagawa are stated for the case of irreducible F, but as noted in [Woo11, §2.1], their proofs continue to hold when F is not irreducible.)

Also contained in K_F is a natural family of free R-submodules I_F^j of rank $2n+1$ for each $j \in \{0, \ldots, 2n\}$, having R-basis given by

$$I_F^j := R\langle 1, \theta, \ldots, \theta^j, \zeta_{j+1}, \ldots, \zeta_{2n} \rangle. \tag{6}$$

Note that $I_F^0 = R_F$ is the unit ideal. By [Woo11, Proposition A.1], each I_F^j is an R_F-module and hence a fractional ideal of R_F; moreover, the notation I_F^j makes sense, because I_F^j is equal to the j^{th} power of I_F^1. By [Woo11, Proposition A.4], the fractional ideals I_F^j are invertible precisely when the form F is primitive, in the sense that $\sum_{i=0}^{2n+1} Rf_i = R$. It is a result of Simon (see [Sim08, Proposition 14], cf. [Woo11, Theorem 2.4]) that I_F^{2n-1} represents the ideal class of the inverse different of R_F.

Given a fractional ideal I of R_F having a specified basis (i.e., a *based fractional ideal*), the *norm* of I, denoted by $\mathrm{N}(I)$, is defined to be the determinant of the k-linear transformation taking

the basis of I to the basis of R_F in (4). It is easy to check that $\mathrm{N}(I_F^j) = f_0^{-j}$ for each j with respect to the basis in (6). The norm of $\kappa \in K_F^\times$ is $\mathrm{N}(\kappa) := \mathrm{N}(\kappa \cdot I_F^0)$ with respect to the basis $\langle \kappa, \kappa \cdot \zeta_1, \dots, \kappa \cdot \zeta_{2n} \rangle$ of $\kappa \cdot I_F^0$. Note that we have the multiplicativity relation

$$\mathrm{N}(\kappa \cdot I) = \mathrm{N}(\kappa) \cdot \mathrm{N}(I) \tag{7}$$

for any $\kappa \in K_F^\times$ and fractional ideal I of R_F with a specified basis.

We now explain how the objects K_F, R_F, and I_F^j transform under the action of $\gamma \in \mathrm{SL}_2(R)$ on binary forms of degree $2n+1$ defined by $\gamma \cdot F = F((x,z) \cdot \gamma)$. If $F' = \gamma \cdot F$, then γ induces an isomorphism $K_F \simeq K_{F'}$, under which the rings R_F and $R_{F'}$ happen to be identified with each other (see [Nak89, Proposition 1.2] for a direct proof and [Woo11, §2.3] for a geometric argument). On the other hand, the ideals I_F^j and $I_{F'}^j$ are isomorphic as R_F-modules but may *not necessarily* be identified under the isomorphism $K_F \simeq K_F'$. Indeed, as explained in [Bha13, (7)], these ideals are related by the following explicit rule: if $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, then for each $j \in \{0, \dots, 2n\}$, the composition

$$I_F^j \xhookrightarrow{\phi_{j,\gamma}} K_F \xrightarrow{\sim} K_{F'} \tag{8}$$

is an injective map of R_F-modules having image equal to $I_{F'}^j$, where $\phi_{j,\gamma}$ sends each $\delta \in I_F^j$ to $(-b\theta + a)^{-j} \cdot \delta \in K_F$. When $j = 0$, we recover the identification of $R_F = I_F^0$ with $R_{F'} = I_{F'}^0$ from (8).

2.3. **Parametrization of Square Roots of the Class of I_F^{2n-1}.** We say that a based fractional ideal I of R_F is a *square root of the class of the inverse different* if there exists $\delta \in K_F^\times$ such that

$$I^2 \subset \delta \cdot I_F^{2n-1} \quad \text{and} \quad \mathrm{N}(I)^2 = \mathrm{N}(\delta) \cdot \mathrm{N}(I_F^{2n-1}) \tag{9}$$

We now recall an orbit parametrization for such square roots that we introduced in [Swa21]. To do this, let $\widetilde{H}_F$ be the set of pairs (I, δ) satisfying (9). Let $H_F = \widetilde{H}_F / \sim$, where the equivalence relation $\sim$ is defined as follows: $(I_1, \delta_1) \sim (I_2, \delta_2)$ if and only if there exists $\kappa \in K_F^\times$ such that the based fractional ideals I_1 and $\kappa \cdot I_2$ are equal up to an $\mathrm{SL}_{2n+1}(R)$-change-of-basis and such that $\alpha_1 = \kappa^2 \cdot \alpha_2$. Now, take $(I, \delta) \in H_F$, and consider the symmetric bilinear form

$$\langle -, - \rangle \colon I \times I \to K_F, \quad (\alpha, \beta) \mapsto \langle \alpha, \beta \rangle = \delta^{-1} \cdot \alpha\beta. \tag{10}$$

Let $\pi_{2n-1}, \pi_{2n} \in \mathrm{Hom}_R(I_F^{2n-1}, R)$ be the maps defined on the R-basis (6) of I_F^{2n-1} by

$$\pi_{2n-1}(\theta^{2n-1}) - 1 = \pi_{2n-1}(\zeta_{2n}) = \pi_{2n-1}(\theta^i) = 0 \text{ for each } i \in \{0, \dots, 2n-2\}, \text{ and}$$
$$\pi_{2n}(\zeta_{2n}) + 1 = \pi_{2n}(\theta^i) = 0 \text{ for each } i \in \{0, \dots, 2n-1\}.$$

Let A and B respectively denote the matrices representing the symmetric bilinear forms $\pi_{2n} \circ \langle -, - \rangle \colon I \times I \to R$ and $\pi_{2n-1} \circ \langle -, - \rangle \colon I \times I \to R$ with respect to the R-basis of I, and observe that A and B are symmetric of dimension $(2n+1) \times (2n+1)$ and have entries in R. We have thus constructed a map of sets

$$\mathsf{orb}_F \colon H_F \longrightarrow \left\{ \mathrm{SL}_{2n+1}(R)\text{-orbits on } R^2 \otimes_R \mathrm{Sym}_2 R^{2n+1} \right\},$$

where by $R^2 \otimes_R \mathrm{Sym}_2 R^{2n+1}$ we mean the space of pairs of $(2n+1) \times (2n+1)$ symmetric matrices with entries in R. The following result characterizes the map orb_F:

Theorem 3 ([Swa21, Theorems 9 and 13, Proposition 12 and 14])**.** *The map orb_F defines a bijection from H_F to the set of all those $\mathrm{SL}_{2n+1}(R)$-orbits of pairs $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^{2n+1}$ such that:*

(a) $(-1)^n \cdot \det(x \cdot A + z \cdot B) = F_{\mathrm{mon}}(x, z) := \frac{1}{f_0} \cdot F(x, f_0 z)$*; and*

(b) $p_i\left(\frac{1}{f_0} \cdot -A^{-1}B\right)$ *is a matrix with entries in R for each $i \in \{1, \dots, 2n\}$.*

Moreover, for any $(I, \delta) \in H_F$, the stabilizer in $\mathrm{SL}_{2n+1}(R)$ of $\mathsf{orb}_F(I, \delta)$ contains a subgroup isomorphic to the group $R_F^\times[2]_{\mathrm{N} \equiv 1} := \{\rho \in R_F^\times : \rho^2 = 1 = \mathrm{N}(\rho)\}$.

For the purposes of this paper, it turns out (see Lemma 11) that we only need the restriction of the parametrization in Theorem 3 to those pairs (A, B) such that A defines a split quadratic form over k. This restricted parametrization can be expressed in terms of the action of $G(R)$ on $V(R)$. Indeed, suppose we are given a pair $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^{2n+1}$ such that the *invariant form* $\det(x \cdot A + z \cdot B)$ of (A, B) is equal to $(-1)^n \cdot F_{\mathrm{mon}}(x, z)$ and such that A defines a quadratic form that is split over k. Then there exists $g \in \mathrm{GL}_{2n+1}(R)$ satisfying $gAg^T = A_0$ (by the uniqueness statement in the first paragraph of §2.1), and the matrix $T = (g^T)^{-1} \cdot -A^{-1}B \cdot g^T$ is self-adjoint with respect to the matrix A_0 and has characteristic polynomial $F_{\mathrm{mon}}(x, 1)$. We thus obtain the following correspondence, the proof of which is immediate:

Proposition 4. *The map $(A, B) \mapsto T$ described above defines a natural bijection from the set of $\mathrm{SL}_{2n+1}(R)$-orbits on pairs $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^{2n+1}$ with invariant form $(-1)^n \cdot F_{\mathrm{mon}}$ such that A defines a split quadratic form over k to the set of $G(R)$-orbits on $V(R)$ with characteristic polynomial $F_{\mathrm{mon}}(x, 1)$. Under this bijection, we have that $\mathrm{Stab}_{\mathrm{SL}_{2n+1}(R)}(A, B) = \mathrm{Stab}_{G(R)}(T)$.*

Remark 5. As explained in [Swa21, §2.2], the proof of Theorem 3 is inspired by [Woo14], where Wood derives a similar parametrization in which the multiplication table of a fractional ideal of R_F gives rise to a pair of symmetric matrices with invariant form equal to F (up to a sign). In [Bha13, §2], Bhargava uses Wood's parametrization to prove analogues of Theorems 1 and 2 for rational points on hyperelliptic curves.

2.4. **Orbits over Fields.** When $R = k$ is a field, the parametrization in Theorem 3 simplifies considerably. Indeed, every fractional ideal of $R_F = K_F$ is equal to K_F, so every element of H_F is of the form (K_F, δ), where $f_0 \cdot \delta \in (K_F^\times / K_F^{\times 2})_{\mathrm{N}\equiv 1} := \{\rho \in K_F^\times : \mathrm{N}(\rho) \in k^{\times 2}\}/K_F^{\times 2}$. Moreover, condition (b) in Theorem 3 holds trivially in this case, implying that every $\mathrm{SL}_{2n+1}(k)$-orbit on $k^2 \otimes_k \mathrm{Sym}_2 k^{2n+1}$ with invariant form $F_{\mathrm{mon}}(x, 1)$ arises from an element of H_F. We thus obtain the following result, which gives a convenient description of the orbits of $\mathrm{SL}_{2n+1}(k)$ on $k^2 \otimes_k \mathrm{Sym}_2 k^{2n+1}$ that arise via the parametrization:

Proposition 6 ([Swa21, Proposition 25])**.** *When $R = k$ is a field, the set of $\mathrm{SL}_{2n+1}(k)$-orbits on $k^2 \otimes_k \mathrm{Sym}_2 k^{2n+1}$ with invariant form F_{mon} is in bijection with the set $(K_F^\times / K_F^{\times 2})_{\mathrm{N}\equiv 1}$. Under this bijection, the orbit corresponding to the pair $(K_F, \delta) \in H_F$ is sent to $f_0 \cdot \delta$.*

In what follows, we say that an orbit of $\mathrm{SL}_{2n+1}(k)$ on $k^2 \otimes_k \mathrm{Sym}_2 k^{2n+1}$ (or of $G(k)$ on $V(k)$) is *distinguished* if it corresponds to $1 \in (K_F^\times / K_F^{\times 2})_{\mathrm{N}\equiv 1}$ under the bijection of Proposition 6. In geometric terms, the orbit of a pair $(A, B) \in k^2 \otimes_k \mathrm{Sym}_2 k^{2n+1}$ is distinguished if and only if A and B share a maximal isotropic space defined over k (see [BG13, §4]).

For ease of notation, write $f = F_{\mathrm{mon}}$. Given any $(A, B) \in k^2 \otimes_k \mathrm{Sym}_2 k^{2n+1}$ with invariant form f, we may regard A and B as quadratic forms cutting out a pair of quadric hypersurfaces Q_A and Q_B in $\mathbb{P}_k^{2n}$. Let $\mathcal{F}_{(A,B)}$ denote the Fano scheme parametrizing $(n-1)$-dimensional linear spaces contained in the base locus $Q_A \cap Q_B$ of the pencil of quadric hypersurfaces spanned by Q_A and Q_B. The following proposition states that $\mathcal{F}_{(A,B)}$ is a torsor of the Jacobian of $\mathcal{S}_F$:

Proposition 7. *Let $(A, B) \in k^2 \otimes_k \mathrm{Sym}_2 k^{2n+1}$ with invariant form f. Then, if $\#k$ is sufficiently large, $\mathcal{F}_{(A,B)}$ is a torsor over k of the Jacobian of the stacky curve $\mathcal{S}_F$.*

Proof. The Jacobian of a stacky curve $\mathcal{X}$ is defined to be the 0^{th}-degree component $\mathrm{Pic}^0(\mathcal{X})$ of the group $\mathrm{Pic}(\mathcal{X})$ of divisors on $\mathcal{X}$ modulo principal divisors. Let k_{sep} be a separable closure of k, and let $\theta_1, \ldots, \theta_{2n+1} \in \mathbb{P}_k^1(k_{\mathrm{sep}})$ be the roots of F. Applying the correspondence between isomorphism classes of line bundles and divisor classes to [CC17, proof of Proposition 2.2] yields that $\mathrm{Pic}^0(\mathcal{S}_F)$ is the group generated by the classes of the divisors $(\frac{1}{2}\theta_i - \frac{1}{2}\theta_j)$ subject to the relations $2 \cdot (\frac{1}{2}\theta_i - \frac{1}{2}\theta_j) = 0$ for $1 \le i < j \le 2n+1$; i.e., we have

$$\mathrm{Pic}^0(\mathcal{S}_F) = (\mathbb{Z}/2\mathbb{Z})\langle (\tfrac{1}{2}\theta_i - \tfrac{1}{2}\theta_j) : 1 \le i < j \le 2n+1 \rangle.$$

There is a natural right action of the absolute Galois group $G_k := \mathrm{Gal}(k_{\mathrm{sep}}/k)$ on $\mathrm{Pic}^0(\mathcal{S}_F)$: for $\sigma \in G_k$, we have $(\frac{1}{2}\theta_i - \frac{1}{2}\theta_i) \cdot \sigma = (\frac{1}{2}(\sigma^{-1} \cdot \theta_i) - \frac{1}{2}(\sigma^{-1} \cdot \theta_j))$.

A result of Wang (see [Wan18, Corollary 2.5]) implies that, as long as $\#k$ is sufficiently large, the Fano scheme $\mathcal{F}_{(A,B)}$ is a torsor over k of the 2-torsion subgroup $J[2]$ of the Jacobian J of the monic odd-degree hyperelliptic curve $y^2 = f(x,1)$. Thus, to prove that $\mathcal{F}_{(A,B)}$ is a torsor of $\mathrm{Pic}^0(\mathcal{S}_F)$, it suffices to show that there is a G_k-equivariant isomorphism $\mathrm{Pic}^0(\mathcal{S}_F) \simeq J[2]$. But this is clear: the divisor classes $(\theta_i - \theta_j)$ for $1 \le i < j \le 2n+1$ generate $J[2](k_{\mathrm{sep}})$ over $\mathbb{Z}/2\mathbb{Z}$. □

Note in particular that the $\mathrm{SL}_{2n+1}(k)$-orbit of (A,B) is distinguished if and only if $\mathcal{F}_{(A,B)}$ is the trivial torsor of the Jacobian of $\mathcal{S}_F$ (which happens if and only if $\mathcal{F}_{(A,B)}(k) \neq \varnothing$).

Remark 8. As it happens, Proposition 7 admits an analogue for pencils of even-dimensional quadric hypersurfaces; see the work of Wang [Wan18] (generalizing previous work of Reid [Rei72, Theorem 4.8]), showing that the Fano scheme of maximal linear spaces in the base locus of a pencil of quadric hypersurfaces generated by a pair $(A,B) \in k^2 \otimes_k \mathrm{Sym}_2 k^{2n}$ is a torsor of the Jacobian of the hyperelliptic curve cut out by the equation $y^2 = (-1)^n \cdot \det(x \cdot A + z \cdot B)$.

We conclude this section by explaining how to visualize the simply transitive action of $\mathrm{Pic}^0(\mathcal{S}_F)$ on $\mathcal{F}_{(A,B)}(k_{\mathrm{sep}})$ from Proposition 7. For each $i \in \{1, \dots, 2n+1\}$, let Q_i be the singular fiber lying over the point θ_i in the pencil of quadrics spanned by Q_A and Q_B. Suppose that T is generic, so that each of the quadrics Q_i is a simple cone with cone point q_i. Let $\mathcal{F}_{(A,B)}(k_{\mathrm{sep}}) = \{p_1, \dots, p_{2^{2n}}\}$, and for each $\ell \in \{1, \dots, 2^{2n}\}$, let $\overline{p}_\ell$ denote the corresponding linear subspace of $\mathbb{P}^{2n}_{k_{\mathrm{sep}}}$. We illustrate this setup in the case where $n = 1$ in Figure 1.

We define an action of $\mathrm{Pic}^0(\mathcal{S}_F)$ on $\mathcal{F}_{(A,B)}(k_{\mathrm{sep}})$ by first specifying how each $(\frac{1}{2}\theta_i)$ acts on $\mathcal{F}_{(A,B)}(k_{\mathrm{sep}})$. Let $L_{i\ell} \subset \mathbb{P}^{2n}_{k_{\mathrm{sep}}}$ be the linear span of the $(n-1)$-plane $\overline{p}_\ell$ and the point q_i for each pair (i,ℓ). By [Rei72, Theorem 3.8], there exists precisely one element $p_{i(\ell)} \in \mathcal{F}_{(A,B)}(k_{\mathrm{sep}}) \smallsetminus \{p_\ell\}$ such that $\overline{p}_{i(\ell)} \subset L_{i\ell}$. For each i, let $(\frac{1}{2}\theta_i)$ act on $\mathcal{F}_{(A,B)}$ by swapping p_ℓ and $p_{i(\ell)}$ for each ℓ. Then for each pair (i,j), the divisor $(\frac{1}{2}\theta_i - \frac{1}{2}\theta_j)$ acts on $\mathcal{F}_{(A,B)}$ by swapping p_ℓ with $p_{i(j(\ell))} = p_{j(i(\ell))}$ for each ℓ. When $n = 1$, for example, the divisor $(\frac{1}{2}\theta_1 - \frac{1}{2}\theta_2)$ acts on $\mathcal{F}_{(A,B)}$ by sending (p_1, p_2, p_3, p_4) to (p_3, p_4, p_1, p_2), as we demonstrate in Figure 1.

3. Construction of an Integral Orbit from a Primitive Integer Solution

Take R and F as in §2.2, and assume that k is of characteristic 0. In §3.1, we prove that points $(x_0, y_0, z_0) \in \mathcal{S}_F(R)$ give rise to certain orbits of $G(R)$ on $V(R)$ with characteristic polynomial $F_{\mathrm{mon}}(x,1)$. To produce the desired orbit, it suffices by Theorem 3 and Proposition 4 to construct a pair $(I,\delta) \in H_F$ such that the matrix A that arises defines a split quadratic form over k. Our construction extends a result of Simon, who constructs the desired pair (I,δ) under the following special conditions: F is primitive and irreducible and y_0 is coprime to the index of R_F in its integral closure (see [Sim08, Corollary 4]). We finish in §3.2 by describing when the orbits arising from the construction are distinguished.

3.1. **The Construction.** Let $(x_0, y_0, z_0) \in \mathcal{S}_F(R)$. For convenience, we say that the point (x_0, y_0, z_0) is a *Weierstrass point* if $y_0 = 0$ and a *non-Weierstrass point* otherwise. Note that if $y_0 = 0$, then $z_0 \neq 0$ because $f_0 \neq 0$, so the binary form F factors uniquely as

$$F(x,z) = \left(x - \tfrac{x_0}{z_0} \cdot z\right) \cdot \widetilde{F}(x,z) \tag{11}$$

where $\widetilde{F} \in R[x,z]$ is a binary form of degree $2n$ with leading coefficient equal to f_0.

We start by transforming the pair (x_0, z_0) into a pair with simpler coordinates by constructing a suitable $\gamma \in \mathrm{SL}_2(R)$ such that $(x_0, z_0) \cdot \gamma = (0,1)$. Let $b_0, d_0 \in R$ be any elements such that $b_0 x_0 + d_0 z_0 = 1$ (such b_0, d_0 exist since $Rx_0 + Rz_0 = R$). We claim that there exists $K \in R$ such that

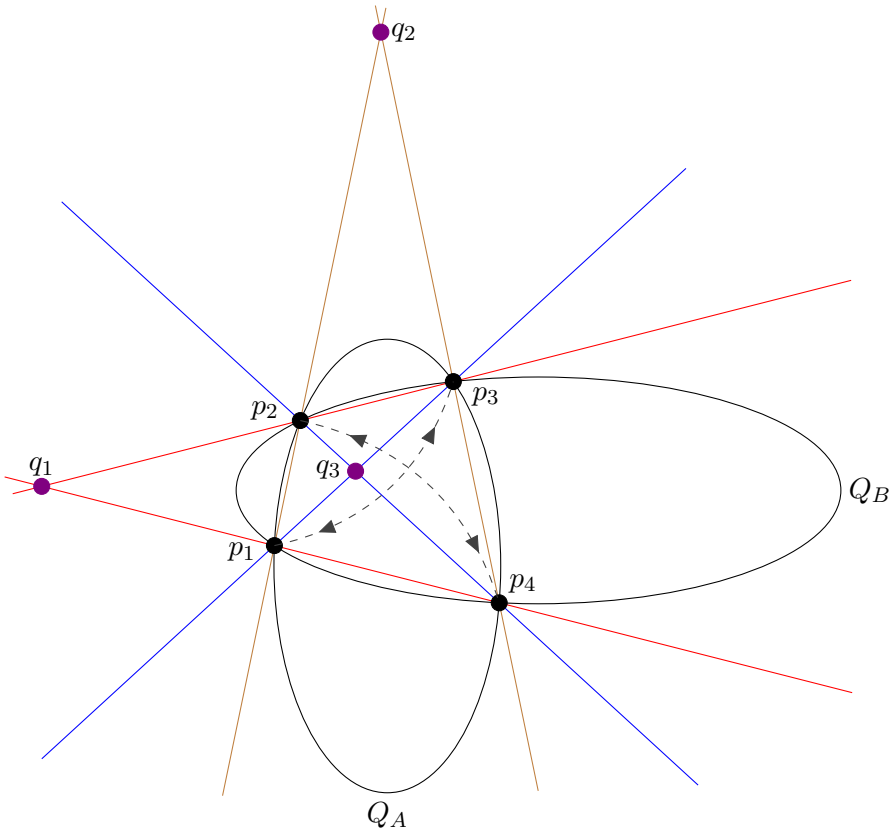

FIGURE 1. The pencil of conics spanned by Q_A and Q_B in $\mathbb{P}^2_{k_{\mathrm{sep}}}$, with singular fibers Q_1, Q_2, and Q_3 having cone points q_1, q_2, and q_3, respectively. In this case, $\mathscr{F}_{(A,B)}(k_{\mathrm{sep}}) = Q_A \cap Q_B = \{p_1, p_2, p_3, p_4\}$. The dashed arrows display the action of the degree-0 divisor $(\frac{1}{2}\theta_1 - \frac{1}{2}\theta_2)$ on $\mathscr{F}_{(A,B)}$.

$(d_0 - Kx_0) + \theta(b_0 + Kz_0) \in K_F^\times$. Indeed, if we were to have $(d_0 - Kx_0) + \theta(b_0 + Kz_0) \in K_F \smallsetminus K_F^\times$, then the pair $(x, z) = (d_0 - Kx_0, -b_0 - Kz_0)$ is a root of the equation $F(x, z) = 0$, which has finitely many roots up to scaling, implying that we can choose K to avoid this outcome (since k is of characteristic 0). Take any such $K \in R$, let $b = b_0 + Kz_0$ and $d = d_0 - Kx_0$, and let $\gamma = \left[\begin{smallmatrix} z_0 & b \\ -x_0 & d \end{smallmatrix}\right]$. Now, let F' be defined by

$$F'(x, z) = F((x, z) \cdot \gamma^{-1}) = \sum_{i=0}^{2n+1} f'_i x^{2n+1-i} z^i \in R[x, z].$$

Note that $f'_{2n+1} = y_0^2$ and that $f'_0 \neq 0$ since $f'_0 = f_0 \cdot \mathrm{N}(d + \theta b)$. If $y_0 = 0$, the binary form F' factors uniquely as

$$F'(x, z) = x \cdot \widetilde{F}'(x, z),$$

where $\widetilde{F}' \in R[x, z]$ is a binary form of degree $2n$ with leading coefficient equal to f'_0; further observe that $f'_{2n} = \widetilde{F}(x_0, z_0) \neq 0$ because F is separable. Let $\theta' = (-x_0 + \theta z_0)/(d + \theta b)$ be the root of $F'(x, 1)$ in $K_{F'} = K_F$, and consider the free rank-$(2n + 1)$ R-submodule $I' \subset K_{F'}$ defined by

$$I' := R\langle \xi, \theta', \ldots, \theta'^n, \zeta'_{n+1}, \ldots, \zeta'_{2n} \rangle, \quad \text{where} \quad \xi := \begin{cases} y_0 & \text{if } y_0 \neq 0, \\ \zeta'_{2n} + f'_{2n} & \text{if } y_0 = 0. \end{cases} \tag{12}$$

Observe that the R-module I' is a fractional ideal of $R_{F'}$ that resembles the fractional ideal $I_{F'}^n$, the only difference between them being that the basis element $1 \in I_{F'}^n$ is replaced by $\xi \in I'$.

Lemma 9. *We have that*

$$I'^2 \subset \delta' \cdot I_{F'}^{2n-1}, \quad \textit{where} \quad \delta' := \begin{cases} -\theta' & \textit{if } y_0 \neq 0, \\ \widetilde{F}'(\theta', 1) - \theta' & \textit{if } y_0 = 0 \end{cases}$$

and that $\mathrm{N}(I')^2 = \mathrm{N}(\delta') \cdot \mathrm{N}(I_{F'}^{2n-1})$.

Proof. Recall from (6) that the fractional ideal $I_{F'}^{2n-1}$ has the $\mathbb{Z}$-basis

$$I_{F'}^{2n-1} = R\langle 1, \theta', \ldots, \theta'^{2n-1}, \zeta'_{2n} \rangle.$$

To prove the claimed containment, it suffices to check that when each of the pairwise products of the basis elements of I' in (12) is divided by δ', what results is an element of $I_{F'}^{2n-1}$. We have the following computations:

$$\begin{aligned}
\xi^2/\delta' &= \zeta'_{2n} + f'_{2n} && \\
(\xi \cdot \theta'^i)/\delta' &= -y_0 \theta'^{i-1} && \text{for } i \in \{1, \ldots, n\} \\
(\xi \cdot \zeta'_j)/\delta' &= -y_0 \zeta'_{j-1} - y_0 f'_{j-1} && \text{for } j \in \{n+1, \ldots, 2n\} \\
(\theta'^i \cdot \theta'^j)/\delta' &= -\theta'^{i+j-1} && \text{for } i, j \in \{1, \ldots, n\} \\
(\theta'^i \cdot \zeta'_j)/\delta' &= -\theta'^{i-1} \zeta'_j && \text{for } i \in \{1, \ldots, n\},\ j \in \{n+1, \ldots, 2n\} \\
(\zeta'_i \cdot \zeta'_j)/\delta' &= -\zeta'_i \zeta'_{j-1} - f'_{j-1} \zeta'_i && \text{for } i, j \in \{n+1, \ldots, 2n\}
\end{aligned}$$

Using the fact that $\zeta'_i \in R_{F'}$ for each $i \in \{0, \ldots, 2n+1\}$ together with the fact that $I_{F'}^{2n-1}$ is closed under multiplication by elements in $R_{F'}$, one readily verifies that each of the expressions obtained on the right-hand side above is an element of $I_{F'}^{2n-1}$. Crucially, these expressions do not depend in piecewise fashion on the value of y_0, even though ξ and δ' do (see Remark 12).

As for the second part of the lemma, using $\mathrm{N}(I_{F'}^n) = {f'_0}^{-n}$, we find that $\mathrm{N}(I') = \widetilde{\xi} \cdot {f'_0}^{-n}$, where $\widetilde{\xi} = \xi = y_0$ if $y_0 \neq 0$ and $\widetilde{\xi} = \xi - \zeta'_{2n} = f'_{2n}$ if $y_0 = 0$. Moreover, a calculation reveals that $\mathrm{N}(\delta') = \widetilde{\xi}^2 \cdot {f'_0}^{-1}$. Combining these norm calculations, we deduce that

$$\mathrm{N}(I')^2 = (\widetilde{\xi} \cdot {f'_0}^{-n})^2 = (\widetilde{\xi}^2 \cdot {f'_0}^{-1}) \cdot ({f'_0}^{-(2n-1)}) = \mathrm{N}(\delta') \cdot \mathrm{N}(I_{F'}^{2n-1}) \qquad \square$$

We now transform I' and δ' back from $R_{F'}$ to R_F. Recall from (8) that

$$I_F^n = \phi_{n,\gamma}(I_{F'}^n) = (-b\theta' + z_0)^{-n} \cdot I_{F'}^n,$$

where we can invert $-b\theta' + z_0$ because its inverse is equal to $d + \theta b$. Since I' resembles $I_{F'}^n$, it makes sense to consider the fractional ideal

$$I := \phi_{n,\gamma}(I') = (-b\theta' + z_0)^{-n} \cdot I' = (d + \theta b)^n \cdot I', \tag{13}$$

which has norm given by

$$\mathrm{N}(I) = \mathrm{N}((d + \theta b)^n \cdot I') = \mathrm{N}(d + \theta b)^n \cdot \mathrm{N}(I') = \widetilde{\xi} \cdot f_0^{-n} \tag{14}$$

where we used the multiplicativity relation (7). Similarly, let $\delta \in K_F^\times$ be defined as follows:

$$\delta := \phi_{1,\gamma}(\delta') = \frac{\delta'}{-b\theta' + z_0} = \begin{cases} x_0 - \theta z_0 & \text{if } y_0 \neq 0, \\ \widetilde{F}(z_0\theta, z_0) + (x_0 - \theta z_0) & \text{if } y_0 = 0. \end{cases} \tag{15}$$

It then follows from Lemma 9 that

$$I^2 \subset \frac{\delta'}{-b\theta' + z_0} \cdot \frac{I_{F'}^{2n-1}}{(-b\theta' + z_0)^{2n-1}} = \delta \cdot I_F^{2n-1}, \tag{16}$$

where in the last step above, we used the fact that

$$I_F^{2n-1} = \phi_{2n-1,\gamma}(I_{F'}^{2n-1}) = (-b\theta' + z_0)^{-(2n-1)} \cdot I_{F'}^{2n-1}.$$

Notice that $\mathrm{N}(I)^2 = \mathrm{N}(\delta) \cdot \mathrm{N}(I_F)^{2n-1}$ (this can be verified directly from (14) and (15), but it also follows from the fact that $\mathrm{N}(I')^2 = \mathrm{N}(\delta') \cdot \mathrm{N}(I_{F'})^{2n-1}$ by Lemma 9).

Lemma 10. *The fractional ideal I is well-defined, in the sense that it does not depend on the choice of $\gamma = \left[\begin{smallmatrix} z_0 & b \\ -x_0 & d \end{smallmatrix}\right] \in \mathrm{SL}_2(R)$ satisfying $(x_0, z_0) \cdot \gamma = (0,1)$ and $d + \theta b \in K_F^\times$.*

Proof. Let $\gamma = \left[\begin{smallmatrix} z_0 & b \\ -x_0 & d \end{smallmatrix}\right] \in \mathrm{SL}_2(R)$ satisfying $(x_0, z_0)\cdot\gamma = (0,1)$ and $d+\theta b \in K_F^\times$ as above. Any other $\check\gamma \in \mathrm{SL}_2(R)$ satisfying $(x_0, z_0) \cdot \check\gamma$ to $(0,1)$ is a right-translate of γ by an element of the stabilizer of $(0,1)$, which is the group of unipotent matrices $M_K = \left[\begin{smallmatrix} 1 & K \\ 0 & 1 \end{smallmatrix}\right]$ for $K \in R$. So take $K \in R$, and let

$$\check\gamma = \gamma \cdot M_K = \begin{bmatrix} z_0 & b + Kz_0 \\ -x_0 & d - Kx_0 \end{bmatrix}$$

Let $\check F(x,z) = F((x,z)\cdot\check\gamma^{-1}) = \sum_{i=0}^{2n+1} \check f_i x^{2n+1-i} z^i$, and let $\check\theta$ be the root of $\check F(x,1)$ in K_F. Assume that K has been chosen so that $(d - Kx_0) + \theta(b + Kz_0) \in K_F^\times$, and notice that

$$\check\theta = \frac{-x_0 + \theta z_0}{(d - Kx_0) + \theta(b + Kz_0)} = \frac{\theta'}{1 + \theta' K}. \tag{17}$$

Just as we associated a pair (I', δ') to γ, we can associate a pair $(\check I, \check\delta)$ to $\check\gamma$ satisfying the analogous properties $\check I^2 \subset \check\delta \cdot I_{\check F}^{2n-1}$ and $\mathrm{N}(\check I)^2 = \mathrm{N}(\check\delta) \cdot \mathrm{N}(I_{\check F}^{2n-1})$. To prove the lemma, it suffices to show that

$$\phi_{n,\gamma}(I') = \phi_{n,\check\gamma}(\check I) \quad \text{and} \quad \phi_{1,\gamma}(\delta') = \phi_{1,\check\gamma}(\check\delta), \tag{18}$$

The second equality in (18) is readily deduced by inspecting (15); as for the first equality, notice that it is equivalent to the following:

$$\left(\frac{-b\theta' + z_0}{-(b + Kz_0)\check\theta + z_0}\right)^n \cdot \check I = I'. \tag{19}$$

Using (17), we find that the fraction in parentheses in (19) is equal to $1 + K\theta'$. Now, observe that we can express the ideals I' and $\check I$ as

$$I' = R\langle \widetilde\xi, \theta' \cdot I_{F'}^{n-1} \rangle \quad \text{and} \quad \check I = R\langle \widetilde\xi, \check\theta \cdot I_{\check F}^{n-1} \rangle, \tag{20}$$

where $\widetilde\xi = y_0$ if $y_0 \neq 0$ and $\widetilde\xi = f'_{2n} = \check f_{2n}$ if $y_0 = 0$. Upon combining (19) and (20), we find that

$$\begin{aligned}(1 + K\theta')^n \cdot \check I &= R\langle (1+K\theta')^n \cdot \widetilde\xi, ((1+K\theta')\widetilde\theta) \cdot ((1+K\theta') I_{\check F})^{n-1} \rangle \\ &= R\langle (1+K\theta')^n \cdot \widetilde\xi, \theta' \cdot I_{F'}^{n-1} \rangle = I',\end{aligned}$$

where the last step above follows because $\theta'^i \in I'$ for each $i \in \{0, \dots, n\}$. □

By applying the correspondence in Theorem 3 to the pair (I, δ) constructed above, we see that the point $(x_0, y_0, z_0) \in \mathcal{S}_F(R)$ gives rise to a pair $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^{2n+1}$ with invariant form $(-1)^n \cdot F_{\mathrm{mon}}$. To complete the construction, it remains to verify that A is split:

Lemma 11. *The matrix A defines a split quadratic form over k.*

Proof. It suffices to exhibit an n-dimensional isotropic space X over k for the quadratic form defined by A. We claim that

$$X = k\langle x_0 - \theta z_0, \theta(x_0 - \theta z_0), \dots, \theta^{n-1}(x_0 - \theta z_0) \rangle \subset K_F$$

does the job. Indeed, since F is separable, the elements $\theta^i(x_0 - \theta z_0)$ for $i \in \{0, \dots, n-1\}$ are linearly independent over k: if $y_0 \neq 0$, then this follows because the elements $\theta^i \in K_F$ for $i \in \{0, \dots, n-1\}$

are linearly independent and $x_0 - \theta z_0$ is an invertible element of K_F; if $y_0 = 0$, then this follows because the elements $\theta^i \in K_{\widetilde{F}}$ for $i \in \{0, \dots, n-1\}$ are linearly independent and $x_0 - \theta z_0$ is an invertible element of $K_{\widetilde{F}}$. Thus, we have that $\dim_k X = n$. Moreover, notice that

$$\pi_{2n}(\langle \theta^i(x_0 - \theta z_0), \theta^j(x_0 - \theta z_0)\rangle) = \pi_{2n}(x_0\theta^{i+j} - z_0\theta^{i+j+1}) = 0$$

for any $i, j \in \{0, \dots, n-1\}$. □

Remark 12. We defined the pair (I, δ) in piecewise fashion, according as $y_0 \neq 0$ or $y_0 = 0$. The resulting pair (A, B) nevertheless admits a "functorial" definition: indeed, the entries of A and B are polynomial functions in x_0, y_0, z_0, b, d and the coefficients of F. Thus, if our purpose was simply to construct orbits from integral points, we could have carried out the construction for $y_0 \neq 0$ and specialized the resulting pair of matrices to the case $y_0 = 0$. However, our proofs of Theorems 1 and 2 require knowledge of the element $\delta \in K_F^\times$ corresponding to the orbit arising from an integral point, and it is difficult to reverse-engineer δ from a representative (A, B) of such an orbit.

In [Bha13, §2], Bhargava establishes an analogous construction for rational points on hyperelliptic curves, one that takes a *non*-Weierstrass point on a degree-$2n$ hyperelliptic curve $y^2 = F(x, z)$ and produces a pair (I, δ) of a fractional ideal I and $\delta \in K_F^\times$ such that $I^2 \subset \delta \cdot I_F^{2n-3}$ and $\mathrm{N}(I)^2 = \mathrm{N}(\delta) \cdot \mathrm{N}(I_F^{2n-3})$. By a parametrization due to Wood (see [Woo14, Theorem 5.7]), the pair (I, δ) gives rise to a pair $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^{2n}$ such that $\det(x \cdot A + z \cdot B) = (-1)^n \cdot F(x, z)$. To handle Weierstrass points, Bhargava uses the aforementioned specialization trick but does not determine the element $\delta \in K_F^\times$ corresponding to the specialized orbit, even though this data seems necessary for the proofs of [Bha13, Theorem 3 and Corollary 4] to go through. We note here that the piecewise construction of the pair (I, δ) given in this section can be modified to work for hyperelliptic curves, thus yielding complete proofs of [Bha13, Theorem 3 and Corollary 4].

Remark 13. That the invariant form of the pair (A, B) is equal to $(-1)^n \cdot F_{\mathrm{mon}}$, that A defines a split quadratic form, and that the stabilizer of (A, B) contains a subgroup isomorphic to $R_F^\times[2]$ are properties that hold *formally*. Thus, if we replace R with any base ring and $F \in R[x, z]$ is *any* binary form of degree $2n + 1$, *any* R-primitive solution $(x, y, z) = (x_0, y_0, z_0) \in R^3$ to the superelliptic equation $y^2 = F(x, z)$ gives rise to a pair of matrices $(A, B) \in R^2 \otimes_R \mathrm{Sym}_2 R^{2n+1}$ such that the invariant form is F_{mon} and such that the stabilizer in $\mathrm{SL}_{2n+1}(R)$ contains a subgroup isomorphic to $R_F^\times[2]_{\mathrm{N}\equiv 1}$. If the base ring R is an integral domain, then A defines a split quadratic form over the fraction field k of R. Note that these properties hold even if we do not assume that $f_0 \neq 0$, that F is separable, and that k has characteristic 0, despite the fact that we used these assumptions to derive the construction.

3.2. **Distinguished Points.** We say that a point $(x_0, y_0, z_0) \in \mathcal{S}_F(R)$ is *distinguished* if its associated $G(k)$-orbit is distinguished. Note that Proposition 6 implies that (x_0, y_0, z_0) is distinguished if and only if $f_0 \cdot (x_0 - \theta z_0)$ is a square in $K_F^\times$.

When f_0 is a multiple of a perfect square by a unit $u \in R^\times$, $\mathcal{S}_F$ has a trivial R-point, namely $(u, \sqrt{u^{2n+1} \cdot f_0}, 0)$. Since $f_0 \cdot (u - \theta \cdot 0) = u \cdot f_0 \in K_F^{\times 2}$, the orbits associated to these trivial solutions are always distinguished. Whether a primitive integer solution is distinguished is *not necessarily* invariant under replacing F with an $\mathrm{SL}_2(R)$-translate. Indeed, suppose $(x_0, y_0, z_0) \in \mathcal{S}_F(R)$, take $\gamma \in \mathrm{SL}_2(R)$ such that $(x_0, z_0) \cdot \gamma = (1, 0)$, and let $F'(x, z) = F((x, z) \cdot \gamma^{-1})$. Then the point $(1, y_0, 0) \in \mathcal{S}_{F'}(R)$ is distinguished, regardless of whether the point $(x_0, y_0, z_0) \in \mathcal{S}_F(R)$ is distinguished. Nevertheless, whether a solution is distinguished is *always* preserved under replacing F with a translate by a unipotent matrix of the form M_K^T for $K \in R$.

Now take $R = \mathbb{Z}$. When $|f_0|$ is not a perfect square, we show in [Swa21, §3.3] that the non-square factors of $|f_0|$ tend to obstruct the distinguished $G(\mathbb{Q})$-orbit from arising via the map orb_F defined in §2.3. More precisely, we have the following result, which states that there are strong limitations on the forms $F \in \mathscr{F}_{2n+1}(f_0)$ for which some point of $\mathcal{S}_F(\mathbb{Z})$ is distinguished:

Theorem 14. *Let $F \in \mathscr{F}_{2n+1}(f_0)$ be separable, and suppose that there exists a point of $\mathcal{S}_F(\mathbb{Z})$ giving rise to the distinguished $G(\mathbb{Q})$-orbit via the construction in §3. Then one of the following two mutually exclusive possibilities holds for each prime $p \mid \kappa$:*

(a) *$R_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is not the maximal order in $K_F \otimes_{\mathbb{Q}} \mathbb{Q}_p$; or*
(b) *$R_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is the maximal order in $K_F \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and F/z is a unit multiple of a square modulo p.*

Moreover, the density of binary forms $F \in \mathscr{F}_{2n+1}(f_0)$ such that one of the conditions (a) *or* (b) *holds for every prime $p \mid \kappa$ is equal to $\mu_{f_0} := \prod_{p \mid \kappa} \left(\frac{1}{p^2} + \frac{p-1}{p^{n+1}}\right)$.*

Proof. Let $p \mid \kappa$. By [Swa21, Theorem 28], if $F \in \mathscr{F}_{2n+1}(f_0)$ is such that some element of the image of orb_F has distinguished $G(\mathbb{Q}_p)$-orbit, then one of conditions (a) or (b) in the theorem statement holds. By [ABZ07, Proposition 3.5], the p-adic density of $F \in \mathscr{F}_{2n+1}(f_0, \mathbb{Z}_p)$ satisfying condition (a) is p^{-2}, and it follows from [Swa21, Theorem 29] that the p-adic density of $F \in \mathscr{F}_{2n+1}(f_0, \mathbb{Z}_p)$ satisfying condition (b) is $p^{-n-1}(p-1)$. The theorem follows by combining these density calculations. □

Theorem 14 implies that points of $\mathcal{S}_F(\mathbb{Z})$ often fail to be distinguished — a fact that is crucial for the proofs of Theorems 1 and 2, because the geometry-of-numbers results from [BG13, §9] that we apply in §5 to count orbits of $G(\mathbb{Z})$ on $V(\mathbb{Z})$ only give us a count of the non-distinguished orbits.

4. Counting Orbits Arising from Local Points

Let $\mathscr{P}$ denote the ($G(\mathbb{Z})$-invariant) subset of integral elements of $V(\mathbb{Z})$ that arise via the construction in §3.1 from separable forms $F \in \mathscr{F}_{2n+1}(f_0)$. It is hard to describe $\mathscr{P}$ explicitly, and hence to determine a precise count of the number of $G(\mathbb{Z})$-orbits on $\mathscr{P}$ having bounded height. However, $\mathscr{P}$ is contained within a subset of $V(\mathbb{Z})$ defined by local conditions: indeed, $\mathscr{P} \subset V(\mathbb{Z}) \cap \bigcap_v \mathscr{P}_v$, where for each place v of $\mathbb{Q}$, we write $\mathscr{P}_v$ for the subset of $V(\mathbb{Z}_v)$ that arises via the construction from separable forms $F \in \mathscr{F}_{2n+1}(f_0, \mathbb{Z}_v)$. To prove Theorem 1, our strategy is to *bound* the number of $G(\mathbb{Z})$-orbits on $\mathscr{P}$ of bounded height by counting the total number of $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ of bounded height and sieving to those orbits that belong to $\mathscr{P}_v$ for many places v.

A key step in this strategy is, roughly speaking, to control the size of $\mathscr{P}_v$ for each v. The purpose of this section is to carry out this step. In §4.1, we determine the number of orbits arising via the construction from a given separable form $F \in \mathscr{F}_{2n+1}(f_0, \mathbb{R})$. In §4.2, we bound the p-adic density of $\mathscr{P}_p$ for odd primes $p \nmid f_0$ by working over $\mathbb{Z}/p\mathbb{Z}$, and in §4.3, we bound the 2-adic density of $\mathscr{P}_2$ when $2 \nmid f_0$ by working over $\mathbb{Z}/8\mathbb{Z}$. In §4.4, we take $p \mid f_0$ and work over $\mathbb{Z}_p$ to bound the number of orbits arising via the construction from forms $F \in \mathscr{F}_{2n+1}(f_0, \mathbb{Z}_p)$ that define the maximal order. We finish in §4.5 by working over $\mathbb{Q}_p$ to handle the remaining cases.

4.1. Orbits over $\mathbb{R}$.

For each $m \in \{0, \dots, n\}$, let $\mathscr{I}(m) \subset \mathscr{F}_{2n+1}(1, \mathbb{R})$ be the set of separable monic degree-$(2n+1)$ polynomials over $\mathbb{R}$ having exactly $2m+1$ real roots.

Proposition 15. *There are exactly $2m+1$ orbits of $G(\mathbb{R})$ on $V(\mathbb{R})$ that arise from points in $\mathcal{S}_F(\mathbb{R})$.*

Proof. Let $F \in \mathscr{F}_{2n+1}(f_0, \mathbb{R})$, and let $f(x) = F_{\mathrm{mon}}(x, 1)$. Suppose that $f \in \mathscr{I}(m)$ with real roots given in increasing order by $\lambda_1 < \cdots < \lambda_{2m+1}$, where $m \in \{0, \dots, n\}$. We now compute the number of orbits of $G(\mathbb{R})$ on $V(\mathbb{R})$ having characteristic polynomial f that arise from points in $\mathcal{S}_F(\mathbb{R})$ via the construction in §3. The $G(\mathbb{R})$-orbit associated to a point $(x_0, y_0, z_0) \in \mathcal{S}_F(\mathbb{R})$ is identified via the correspondence in Proposition 6 with some $f_0 \cdot \delta \in (K_F^\times / K_F^{\times 2})_{\mathrm{N} \equiv 1}$. This class is represented by a sequence of the form

$$(f_0(x_0 - \lambda_1 z_0), \dots, f_0(x_0 - \lambda_{2m+1} z_0), b_1, \dots, b_{n-m}) \in \mathbb{R}^{2m+1} \times \mathbb{C}^{n-m} \simeq K_F. \tag{21}$$

Otherwise, if $y_0 = 0$, then $\frac{x_0}{z_0} = \lambda_j$ for some j; letting $\widetilde{F}$ be as in (11), we see that the class $f_0 \cdot \delta \in (K_F^\times / K_F^{\times 2})_{\mathrm{N}\equiv 1}$ is represented by a sequence of the form

$$(f_0(x_0 - \lambda_1 z_0), \dots, f_0 \cdot \widetilde{F}(x_0, z_0), \dots, f_0(x_0 - \lambda_{2m+1} z_0), b_1, \dots, b_{n-m}) \in \mathbb{R}^{2m+1} \times \mathbb{C}^{n-m}, \tag{22}$$

where the term $f_0 \cdot \widetilde{F}(x_0, z_0)$ in (22) replaces the term $f_0(x_0 - \lambda_j z_0)$ in (21). The class in $(K_F^\times / K_F^{\times 2})_{\mathrm{N}\equiv 1}$ of the sequence in (21) or in (22) is given by the sequence of signs of its first $2m+1$ terms. Because $\mathrm{N}(b_j) > 0$ for every j, the condition that $\mathrm{N}(f_0 \cdot \delta)$ is a square in $\mathbb{R}^\times$ is equivalent to the condition that $\prod_{i=1}^{2m+1} f_0(x_0 - \lambda_i z_0) > 0$ if $y_0 \neq 0$ and $(f_0 \cdot \widetilde{F}(x_0, z_0)) \cdot \prod_{\substack{i=1 \\ i \neq j}}^{2m+1} f_0(x_0 - \lambda_i z_0) > 0$ if $y_0 = 0$. We now split into cases based on the signs of f_0 and z_0:

Case 1a: $f_0 > 0$, $z_0 > 0$. First suppose $y_0 \neq 0$. In this case, the sign of $f_0(x_0 - \lambda_i z_0)$ is equal to the sign of $(x_0/z_0) - \lambda_i$. The possible sequences of signs of the $f_0(x_0 - \lambda_i z_0)$ are therefore

$$+ - - - \cdots -, + + + - \cdots -, \dots, + + + + \cdots +, \tag{23}$$

giving a total of $m+1$ orbits. We label the sign sequences in (23) from left to right by an index τ that runs from 1 up to $m+1$. If $y_0 = 0$ and $\frac{x_0}{z_0} = \lambda_j$, then because $\lambda_i < \lambda_j$ when $i < j$ and $\lambda_i > \lambda_j$ when $i > j$, we obtain the same sign sequences as those listed in (23).

Case 1b: $f_0 > 0$, $z_0 < 0$. First suppose $y_0 \neq 0$. In this case, the sign of $f_0(x_0 - \lambda_i z_0)$ is equal to the opposite of the sign of $(x_0/z_0) - \lambda_i$. The possible sequences of signs of the $f_0(x_0 - \lambda_i z_0)$ are therefore

$$+ + + \cdots + +, - - + \cdots + +, \dots, - - \cdots - +, \tag{24}$$

giving a total of $m+1$ orbits. We label the sign sequences in (24) from left to right by an index τ that runs from $m+1$ up to $2m+1$. (Note that the first sign sequence in (24) is the same as the last sign sequence in (23), which is why they share the same value of τ.) If $y_0 = 0$, we again obtain the same sign sequences as those listed in (24).

Case 2a: $f_0 < 0$, $z_0 > 0$. The possible sign sequences are the same as those listed in (24), and we likewise label them from left to right by an index τ that runs from $m+1$ up to $2m+1$.

Case 2b: $f_0 < 0$, $z_0 < 0$. The possible sign sequences are the same as those listed in (23), and we likewise label them from left to right by an index τ that runs from 1 up to $m+1$. □

For each $m \in \{0, \dots, n\}$ and $\tau \in \{1, \dots, 2m+1\}$, we write $V^{(m,\tau)} \subset V(\mathbb{R})$ for the subset of operators T such that $\mathrm{ch}(T) \in \mathscr{I}(m)$ and such that the $G(\mathbb{R})$-orbit of T gives rise (via the correspondence in Proposition 6 and the above discussion) to the sign sequence with index τ.

4.2. **Bounding** $\mathrm{Vol}(\mathscr{P}_p)$ **for** $2 \neq p \nmid f_0$**.** Let $\mathrm{Vol}(\mathscr{P}_p)$ denote the p-adic density of $\mathscr{P}_p$ in $V(\mathbb{Z}_p)$ (i.e., the volume of $\mathscr{P}_p$ with respect to the Euclidean measure on $V(\mathbb{Z}_p)$ normalized so that the volume of $V(\mathbb{Z}_p)$ is 1). Let $\mathscr{I}_p(m)$ denote the set of monic degree-$(2n+1)$ polynomials over $\mathbb{Z}/p\mathbb{Z}$ (*not necessarily* separable) having m distinct irreducible factors. When $2 \neq p \nmid f_0$, we obtain the following bound on $\mathrm{Vol}(\mathscr{P}_p)$:

Proposition 16. *We have that*

$$\mathrm{Vol}(\mathscr{P}_p) \leq \min\left\{1, \sum_{m=1}^{2n+1} \frac{p+1}{2^{m-1}} \cdot \frac{\#G(\mathbb{Z}/p\mathbb{Z})}{p^{2n^2+n}} \cdot \frac{\#\mathscr{I}_p(m)}{p^{2n+1}}\right\}$$

Proof. Given a monic degree-$(2n+1)$ polynomial f over $\mathbb{Z}/p\mathbb{Z}$, let $\overline{\Sigma}_f^{\mathrm{sol}} \subset V(\mathbb{Z}/p\mathbb{Z})$ denote the mod-p reduction of the subset $\{T \in \mathscr{P}_p : \mathrm{ch}(T) \equiv f \pmod p\}$. Because G is smooth over $\mathbb{Z}_p$, the

map $G(\mathbb{Z}_p) \to G(\mathbb{Z}/p\mathbb{Z})$ is surjective, implying that $\overline{\Sigma}_f^{\mathrm{sol}}$ is $G(\mathbb{Z}/p\mathbb{Z})$-invariant. Then we have

$$\mathrm{Vol}(\mathscr{P}_p) \le \sum_{m=1}^{2n+1} \sum_{f \in \mathscr{I}_p(m)} \frac{\#\overline{\Sigma}_f^{\mathrm{sol}}}{p^{\dim V}} = \sum_{m=1}^{2n+1} \sum_{f \in \mathscr{I}_p(m)} \sum_{T \in G(\mathbb{Z}/p\mathbb{Z}) \backslash \overline{\Sigma}_f^{\mathrm{sol}}} \frac{\#\mathscr{O}(T)}{p^{2n^2+3n+1}}, \tag{25}$$

where for each $T \in V(\mathbb{Z}/p\mathbb{Z})$, we denote by $\mathscr{O}(T)$ the $G(\mathbb{Z}/p\mathbb{Z})$-orbit of T. Let $\mathrm{Stab}(T) \subset G(\mathbb{Z}/p\mathbb{Z})$ denote the stabilizer of T. Substituting $\#\mathscr{O}(T) = \#G(\mathbb{Z}/p\mathbb{Z})/\#\,\mathrm{Stab}(T)$ into (25) yields that

$$\mathrm{Vol}(\mathscr{P}_p) \le \sum_{m=1}^{2n+1} \sum_{f \in \mathscr{I}_p(m)} \sum_{T \in G(\mathbb{Z}/p\mathbb{Z}) \backslash \overline{\Sigma}_f^{\mathrm{sol}}} \frac{1}{\#\,\mathrm{Stab}(T)} \cdot \frac{\#G(\mathbb{Z}/p\mathbb{Z})}{p^{2n^2+3n+1}}. \tag{26}$$

The following lemma gives a lower bound for $\#\,\mathrm{Stab}(T)$ that is independent of $f \in \mathscr{I}_p(m)$:

Lemma 17. *For $T \in \overline{\Sigma}_f^{\mathrm{sol}}$, we have that $\#\,\mathrm{Stab}(T) \ge 2^{m-1}$.*

Proof of Lemma 17. Let $K_f = (\mathbb{Z}/p\mathbb{Z})[x]/(f)$. By Proposition 4, $\#\,\mathrm{Stab}(T) \ge \#K_f^\times[2]_{\mathrm{N}\equiv 1}$. Letting f split over $\mathbb{Z}/p\mathbb{Z}$ as $f(x) = \prod_{i=1}^m f_i(x)^{n_i}$, where the f_i are distinct and irreducible, we have that $K_f \simeq \prod_{i=1}^m (\mathbb{Z}/p\mathbb{Z})[x]/(f_i^{n_i})$. Consequently, $K_f^\times[2]$ contains the 2^m elements of the form $(\pm 1, \dots, \pm 1)$. Exactly half of these elements have norm 1, so $\#K_f^\times[2]_{\mathrm{N}\equiv 1} \ge 2^{m-1}$. □

To bound the right-hand side of (26), it remains to control the number of $G(\mathbb{Z}/p\mathbb{Z})$-orbits on $\overline{\Sigma}_f^{\mathrm{sol}}$. But there can only be as many orbits as there are points in $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, which has size $p+1$. Combining this observation with (26) and Lemma 17 yields the proposition. □

Remark 18. It is well-known (see [BG13, §6.1]) that for each odd prime p, we have

$$\#G(\mathbb{Z}/p\mathbb{Z}) = p^{n^2} \cdot \prod_{i=1}^{n} (p^{2i} - 1) \le p^{2n^2+n}. \tag{27}$$

4.3. **Bounding $\mathrm{Vol}(\mathscr{P}_2)$ for $2 = p \nmid f_0$.** Here, it turns out to be ineffective to work over $\mathbb{Z}/2\mathbb{Z}$ or even $\mathbb{Z}/4\mathbb{Z}$; instead, we work over $\mathbb{Z}/8\mathbb{Z}$. Let $\mathscr{I}_8(m)$ denote the set of monic degree-$(2n+1)$ polynomials in $(\mathbb{Z}/8\mathbb{Z})[x]$ having m distinct irreducible factors over $\mathbb{Z}/2\mathbb{Z}$. When $2 = p \nmid f_0$, we obtain the following bound on $\mathrm{Vol}(\mathscr{P}_2)$:

Proposition 19. *We have that*

$$\mathrm{Vol}(\mathscr{P}_2) \le \min\left\{1, \sum_{m=1}^{2n+1} \frac{12}{2^{2n+m-1}} \cdot 2 \cdot \frac{\#\mathscr{I}_8(m)}{8^{2n+1}}\right\}$$

Proof. Given a monic degree-$(2n+1)$ polynomial f over $\mathbb{Z}/8\mathbb{Z}$, let $\overline{\Sigma}_f^{\mathrm{sol}} \subset V(\mathbb{Z}/8\mathbb{Z})$ denote the closure under the action of $G(\mathbb{Z}/8\mathbb{Z})$ of the mod-8 reduction of the subset $\{T \in \mathscr{P}_2 : \mathrm{ch}(T) \equiv f \pmod 8\}$ (note that this subset may not be *a priori* $G(\mathbb{Z}/8\mathbb{Z})$-invariant, because G is not smooth over $\mathbb{Z}_2$ and the map $G(\mathbb{Z}_2) \to G(\mathbb{Z}/8\mathbb{Z})$ is not surjective). Then we have

$$\mathrm{Vol}(\mathscr{P}_2) \le \sum_{m=1}^{2n+1} \sum_{f \in \mathscr{I}_8(m)} \frac{\#\overline{\Sigma}_f^{\mathrm{sol}}}{8^{\dim V}} = \sum_{m=1}^{2n+1} \sum_{f \in \mathscr{I}_8(m)} \sum_{T \in G(\mathbb{Z}/8\mathbb{Z}) \backslash \overline{\Sigma}_f^{\mathrm{sol}}} \frac{\#\mathscr{O}(T)}{8^{2n^2+3n+1}}, \tag{28}$$

where for each $T \in V(\mathbb{Z}/8\mathbb{Z})$, we denote by $\mathscr{O}(T)$ the $G(\mathbb{Z}/8\mathbb{Z})$-orbit of T. Let $\mathrm{Stab}(T) \subset G(\mathbb{Z}/8\mathbb{Z})$ denote the stabilizer of T. Substituting $\#\mathscr{O}(T) = \#G(\mathbb{Z}/8\mathbb{Z})/\#\,\mathrm{Stab}(T)$ into (28) yields that

$$\mathrm{Vol}(\mathscr{P}_2) \le \sum_{m=1}^{2n+1} \sum_{f \in \mathscr{I}_8(m)} \sum_{T \in G(\mathbb{Z}/8\mathbb{Z}) \backslash \overline{\Sigma}_f^{\mathrm{sol}}} \frac{1}{\#\,\mathrm{Stab}(T)} \cdot \frac{\#G(\mathbb{Z}/8\mathbb{Z})}{8^{2n^2+3n+1}}. \tag{29}$$

The following lemma gives a lower bound for $\#\operatorname{Stab}(T)$ that is independent of $f \in \mathcal{I}_8(m)$:

Lemma 20. *For $T \in \overline{\Sigma}_f^{\mathrm{sol}}$, we have that $\#\operatorname{Stab}(T) \geq 2^{2n+m-1}$.*

Proof of Lemma 20. Let $R_f = (\mathbb{Z}/8\mathbb{Z})[x]/(f)$. By Remark 13, $\operatorname{Stab}(T)$ contains a subgroup isomorphic to $R_f^\times[2]_{\mathrm{N}\equiv 1} := \{\rho \in R_f^\times : \rho^2 = 1 = \mathrm{N}(\rho)\}$. Let f split over $\mathbb{Z}/8\mathbb{Z}$ as $f(x) = \prod_{i=1}^m f_i(x)$, where the f_i have the property that their mod-2 reductions are powers of distinct irreducible polynomials. Then it follows from [LP20, Theorem 7] together with the Chinese Remainder Theorem that $R_f \simeq \prod_{i=1}^m (\mathbb{Z}/8\mathbb{Z})[x]/(f_i)$, and $R_f^\times[2]$ contains the 2^{2n+m+1} elements of the form

$$\left(\dots, \rho_0 + \sum_{j=1}^{d_i - 1} \rho_j \theta_i^j, \dots \right) \in \prod_{i=1}^m (\mathbb{Z}/8\mathbb{Z})[x]/(f_i),$$

where ρ_0 is any element of $(\mathbb{Z}/8\mathbb{Z})^\times$ and ρ_j is any element of $\{0, 4\} \subset \mathbb{Z}/8\mathbb{Z}$ for each j, θ_i is the image of x in $(\mathbb{Z}/8\mathbb{Z})[x]/(f_i)$, and $d_i = \deg f_i$ for each i. At least $\frac{1}{4}$ of these elements have norm 1, so $\#\operatorname{Stab}(T) \geq \#R_F^\times[2]_{\mathrm{N}\equiv 1} \geq 2^{2n+m-1}$. □

Let $\widehat{G}$ be the split odd orthogonal group scheme, defined in the same way as G but without the determinant-1 condition. Observe that the determinant map $\det\colon \widehat{G}(\mathbb{Z}/8\mathbb{Z}) \to (\mathbb{Z}/8\mathbb{Z})^\times$ is surjective: for each $\sigma \in (\mathbb{Z}/8\mathbb{Z})^\times$, the diagonal matrix with row-$(n+1)$, column-$(n+1)$ entry equal to σ and all other diagonal entries equal to 1 is orthogonal with respect to A_0 and has determinant σ. Combining this observation with the computation of $\#\widehat{G}(\mathbb{Z}/8\mathbb{Z})$ in Proposition 21 (to follow) yields

$$\frac{\#G(\mathbb{Z}/8\mathbb{Z})}{8^{2n^2+n}} = \frac{\#\widehat{G}(\mathbb{Z}/8\mathbb{Z})}{4 \cdot 8^{2n^2+n}} = 2 \cdot \frac{(2^n - 1) \cdot \prod_{i=1}^{n-1}(2^{2i} - 1)}{2^{n^2}} \leq 2 \cdot 1 = 2. \tag{30}$$

To bound the right-hand side of (29), it remains to control the number of $G(\mathbb{Z}/8\mathbb{Z})$-orbits on $\overline{\Sigma}_f^{\mathrm{sol}}$. But there can only be as many orbits as there are points in $\mathbb{P}^1(\mathbb{Z}/8\mathbb{Z})$, which has size 12. Combining this observation with (29), Lemma 20, Proposition 21, and (30) yields the proposition. □

In the following proposition, we determine the value of $\#\widehat{G}(\mathbb{Z}/8\mathbb{Z})$, which was used in (30):

Proposition 21. *We have that*

$$\#\widehat{G}(\mathbb{Z}/8\mathbb{Z}) = 2^{5n^2+3n+3} \cdot (2^n - 1) \cdot \prod_{i=1}^{n-1} (2^{2i} - 1)$$

when $n \geq 1$, and $\#\widehat{G}(\mathbb{Z}/8\mathbb{Z}) = 4$ when $n = 0$.

Proof. We apply the recursive formula for computing sizes of orthogonal groups modulo 8 given in [Rei56, §4.1.3]. The first step is to diagonalize A_0. One readily verifies that there exists $g_1 \in \mathrm{GL}_{2n+1}(\mathbb{Z})$ such that $g_1 A_0 g_1^T$ is equal to the diagonal matrix with first $n+1$ diagonal entries equal to 1 and remaining n diagonal entries equal to -1. By [Jon44, proof of Lemma 3], there exists $g_2 \in \mathrm{GL}_{2n+1}(\mathbb{Z}_2)$ such that $g_2 g_1 A_0 g_1^T g_2^T$ is equivalent modulo 8 to the following diagonal matrix:

$$\begin{bmatrix} 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & \cdots & 0 & a_1 & 0 & 0 \\ 0 & \cdots & 0 & 0 & a_2 & 0 \\ 0 & \cdots & 0 & 0 & 0 & a_3 \end{bmatrix}, \text{ where } (a_1, a_2, a_3) = \begin{cases} (1,1,1) & \text{if } 2n+1 \equiv 1 \pmod 8, \\ (1,1,7) & \text{if } 2n+1 \equiv 3 \pmod 8, \\ (1,3,3) & \text{if } 2n+1 \equiv 5 \pmod 8, \\ (3,3,7) & \text{if } 2n+1 \equiv 7 \pmod 8 \end{cases} \tag{31}$$

Using (31) together with the recursive formula displayed in [Rei56, §4.1.3] yields that

$$\#\widehat{G}(\mathbb{Z}/8\mathbb{Z}) = \prod_{j=1}^{2n+1} \left(8^j + 4^{j+1} \cdot f(u_{2n+1-j}) + 2(4\sqrt{2})^j \cdot \cos(\tfrac{\pi}{4} K_{2n+1-j}) - 8 \cdot 4^j h(u_{2n+1-j})\right), \tag{32}$$

where the functions f and h are defined by

$$f(u_i) = \begin{cases} 1 & \text{if } u_i \equiv 0 \pmod 8, \\ -1 & \text{if } u_i \equiv 4 \pmod 8, \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad h(u_i) = \begin{cases} 1 & \text{if } i < 2n \text{ and } u_i \equiv 0 \pmod 8, \\ 0 & \text{otherwise} \end{cases}$$

and where the quantities u_i and h_i are given as follows:

Case 1: $(a_1, a_2, a_3) = (1, 1, 1)$. We have that

$$u_{2n+1-j} = j - 1 \quad \text{and} \quad K_{2n+1-j} = j - 2. \tag{33}$$

Case 2: $(a_1, a_2, a_3) = (1, 1, 7)$. We have that

$$u_{2n+1-j} = \begin{cases} j+5 & \text{if } j \geq 2, \\ 0 & \text{if } j = 1 \end{cases} \quad \text{and} \quad K_{2n+1-j} = \begin{cases} j-4 & \text{if } j \geq 2, \\ -15 & \text{if } j = 1 \end{cases} \tag{34}$$

Case 3: $(a_1, a_2, a_3) = (1, 3, 3)$. We have that

$$u_{2n+1-j} = \begin{cases} j+3 & \text{if } j \geq 3, \\ 3 & \text{if } j = 2, \\ 0 & \text{if } j = 1 \end{cases} \quad \text{and} \quad K_{2n+1-j} = \begin{cases} j-6 & \text{if } j \geq 3, \\ -8 & \text{if } j = 2, \\ -7 & \text{if } j = 1 \end{cases} \tag{35}$$

Case 4: $(a_1, a_2, a_3) = (3, 3, 7)$. We have that

$$u_{2n+1-j} = \begin{cases} j+9 & \text{if } j \geq 4, \\ 10 & \text{if } j = 3, \\ 7 & \text{if } j = 2, \\ 0 & \text{if } j = 1 \end{cases} \quad \text{and} \quad K_{2n+1-j} = \begin{cases} j-8 & \text{if } j \geq 4, \\ -9 & \text{if } j = 3, \\ -8 & \text{if } j = 2, \\ -15 & \text{if } j = 1 \end{cases} \tag{36}$$

Substituting (33), (34), (35), and (36) into (32) and simplifying yields the desired formula.

We can also compute $\#\widehat{G}(\mathbb{Z}/8\mathbb{Z})$ by comparing two different formulas for a quantity known as "the 2-adic density of the quadratic lattice" defined by the matrix A_0, which is up to normalization the same as the 2-adic volume of $G(\mathbb{Z}_2)$ with respect to Haar measure. We denote this quantity by α_2. One of the two formulas for α_2 is given in [Cho15], where Cho constructs a smooth model of the group scheme G over $\mathbb{Z}_2$. Letting $\widetilde{G}$ denote the special fiber of this smooth model, one can show by applying [Cho15, Lemma 4.2, Remark 4.3, and Theorem 5.2] that

$$\alpha_2 = 2 \cdot 2^{-2n^2-n} \cdot \#\widetilde{G}(\mathbb{Z}/2\mathbb{Z}) = 2^{-2n^2+n+3} \cdot \#\,\mathrm{SO}_{2n}(\mathbb{Z}/2\mathbb{Z}), \tag{37}$$

where SO_{2n} denotes the special orthogonal group on a $2n$-dimensional split orthogonal space. To be precise, α_2 is defined in [Cho15] to be $1/2$ of the quantity in (37), to account for the number of connected components of G in $\widehat{G}$. However, we have removed this factor of $1/2$ to make the definition of α_2 consistent with the one given by Conway and Sloane in [CS88, §12], who define α_2 by

$$\alpha_2 = \frac{\#\widehat{G}(\mathbb{Z}/2^r\mathbb{Z})}{(2^r)^{2n^2+n}} \tag{38}$$

for any sufficiently large positive integer r. It follows from [Kit93, Proposition 5.6.1(ii) and proof of Lemma 5.6.5] that we can take $r = 3$ in (38). Comparing (37) and (38) together with the fact that $\#\mathrm{SO}_{2n}(\mathbb{Z}/2\mathbb{Z}) = 2^{n^2-n} \cdot (2^n - 1) \cdot \prod_{i=1}^{n-1}(2^{2i} - 1)$ for $n \geq 1$ (see [Cho15, §6]) yields that

$$\#\widehat{G}(\mathbb{Z}/8\mathbb{Z}) = 2^{4n^2+4n+3} \cdot \#\mathrm{SO}_{2n}(\mathbb{Z}/2\mathbb{Z}) = 2^{5n^2+3n+3} \cdot (2^n - 1) \cdot \prod_{i=1}^{n-1}(2^{2i} - 1). \qquad \square$$

Remark 22. The strategy for the second proof of Proposition 21 can likewise be used to obtain a formula for $\#\widehat{G}(\mathbb{Z}/2^r\mathbb{Z})$ for each $r \geq 3$.

4.4. **Orbits over $\mathbb{Z}_p$.** Let p be an odd prime. When F is such that R_F is the maximal order in K_F, we have the following loose bound for the number of orbits arising from points in $\mathcal{S}_F(\mathbb{Z}_p)$:

Proposition 23. *Let p be an odd prime, and suppose that R_F is maximal in K_F. Then there are at most 2^{m-1} orbits of $G(\mathbb{Z}_p)$ on $V(\mathbb{Z}_p)$ arising from points of $\mathcal{S}_F(\mathbb{Z}_p)$ via the construction in §3. The size of the stabilizer in $G(\mathbb{Z}_p)$ of any such orbit is at least 2^{m-1}.*

Proof. By [Swa21, Theorem 20], the number of $G(\mathbb{Z}_p)$-orbits on $V(\mathbb{Z}_p)$ arising from elements of H_F via the correspondence in Theorem 3 is equal to $\#(R_F^\times/R_F^{\times 2})_{\mathrm{N}\equiv 1} = 2^{m-1}$. By Theorem 3, the stabilizer of any such orbit has size at least $\#R_F^\times[2]_{\mathrm{N}\equiv 1} = 2^{m-1}$. $\square$

When $p \nmid f_0$, Propositions 16 and 21 give tighter control on the size of $\mathscr{P}_p$ than Proposition 23, which we will only use for odd primes $p \mid f_0$. When $p \mid f_0$, it does not suffice to obtain a bound of the form $\mathrm{Vol}(\mathscr{P}_p) \ll 1$ (like the bounds obtained in Proposition 16 and 21). Indeed, since proving Theorems 1 and 2 involves averaging over *monicizations* of forms in $\mathscr{F}_{2n+1}(f_0)$ (see §5.2), we must show that $\mathrm{Vol}(\mathscr{P}_p)$ is $\ll |f_0|_p^{2n^2+n}$, which is the p-adic density of the set of monicizations of forms in $\mathscr{F}_{2n+1}(f_0, \mathbb{Z}_p)$. At least for those forms $F \in \mathscr{F}_{2n+1}(f_0, \mathbb{Z}_p)$ such that R_F is maximal, Proposition 23 will be enough to obtain the desired bound on $\mathrm{Vol}(\mathscr{P}_p)$.

4.5. **Orbits over $\mathbb{Q}_p$ for $p \mid f_0$.** Proposition 23 only applies when R_F is the maximal order in K_F; in this section, we handle the remaining forms F by controlling the number of orbits of $G(\mathbb{Q}_p)$ on $V(\mathbb{Q}_p)$ that can arise from points of $\mathcal{S}_F(\mathbb{Z}_p)$. To this end, suppose that $F \in \mathscr{F}_{2n+1}(f_0, \mathbb{Z}_p)$ splits as a product m distinct irreducible factors over $\mathbb{Z}_p$. Then we have the following result:

Proposition 24. *Let p be an odd (resp., even) prime. Then there are at most 2^{m+1} (resp., 2^{n+m+2}) orbits of $G(\mathbb{Q}_p)$ on $V(\mathbb{Q}_p)$ arising from points of $\mathcal{S}_F(\mathbb{Z}_p)$ via the construction in §3. The size of the stabilizer in $G(\mathbb{Q}_p)$ of any such orbit is at least $\#K_F^\times[2]_{\mathrm{N}\equiv 1} = 2^{m-1}$.*

Proof. By Proposition 6, it suffices to bound the number of elements of $(K_F^\times/K_F^{\times 2})_{\mathrm{N}\equiv 1}$ of the form $f_0 \cdot \delta$, where $\delta \in K_F^\times$ is the second coordinate of a pair $(I, \delta) \in H_F$ arising from a points of $\mathcal{S}_F(\mathbb{Z}_p)$ via the construction in §3.

Fix $z_0 \in \mathbb{Z}_p$, and consider the monic odd-degree hyperelliptic curve C_{F,z_0} of genus n over $\mathbb{Q}_p$ defined by the affine equation $C_{F,z_0}\colon y^2 = F_{\mathrm{mon}}(x, z_0)$. Notice that C_{F,z_0} is a quadratic twist of $C_{F,1}$ and that for $z_0' \in \mathbb{Z}_p$, the curves C_{F,z_0} and $C_{F,z_0'}$ are isomorphic over $\mathbb{Q}_p$ when z_0 and z_0' represent the same class in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$. Let $\{\eta_1, \dots, \eta_\ell\} \subset \mathbb{Z}_p$ denote a complete set of representatives of elements of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, and note that we can take $\ell = 4$ when p is odd and $\ell = 8$ when $p = 2$. Then each C_{F,z_0} is isomorphic to one of $C_{F,\eta_1}, \dots, C_{F,\eta_\ell}$.

Let $(x_0, y_0, z_0) \in \mathcal{S}_F(\mathbb{Z}_p)$ giving rise to a pair (I, δ). Then the point $(f_0 x_0, y_0)$ is a $\mathbb{Q}_p$-rational point on the curve C_{F,z_0} and hence is identified with a $\mathbb{Q}_p$-rational point (x_0', y_0') on one of the curves C_{F,η_i}. In [BG13, §5], Bhargava and Gross show that points in $C_{F,\eta_i}(\mathbb{Q}_p)$ naturally give rise to orbits of $G(\mathbb{Q}_p)$ on $V(\mathbb{Q}_p)$ having characteristic polynomial $F_{\mathrm{mon}}(x, \eta_i)$. Under the construction of Bhargava and Gross, points of $C_{F,\eta_i}(\mathbb{Q}_p)$ give rise to $G(\mathbb{Q}_p)$-orbits on $V(\mathbb{Q}_p)$ via the following composition:

$$C_{F,\eta_i}(\mathbb{Q}_p) \to J_i(\mathbb{Q}_p)/2J_i(\mathbb{Q}_p) \to H^1(G_{\mathbb{Q}_p}, J_i[2]) \simeq (K_F^\times/K_F^{\times 2})_{\mathrm{N}\equiv 1}, \tag{39}$$

where J_i denotes the Jacobian of C_{F,η_i} and where we identify the set of $G(\mathbb{Q}_p)$-orbits on $V(\mathbb{Q}_p)$ having characteristic polynomial $F_{\mathrm{mon}}(x,z_0)$ with $(K_F^\times/K_F^{\times 2})_{\mathrm{N}\equiv 1}$ via Proposition 6. The composite map in (39) is known as the *Cassels map*, and was first studied by Cassels in [Cas83].

Let $\theta' \in K_F$ be the image of x under the identification $\mathbb{Q}_p[x]/F_{\mathrm{mon}}(x,1) \simeq K_F$. If $y_0 = 0$, then $F_{\mathrm{mon}}(x, \eta_i \cdot z)$ factors uniquely as

$$F_{\mathrm{mon}}(x,\eta_i\cdot z) = \left(x - f_0\tfrac{x_0}{z_0}\eta_i\cdot z\right)\cdot \widetilde{F}_{\mathrm{mon}}(x,\eta_i\cdot z)$$

where $\widetilde{F}_{\mathrm{mon}} \in \mathscr{F}_{2n}(1,\mathbb{Z}_p)$. (The notation $\widetilde{F}_{\mathrm{mon}}$ makes sense, because $\widetilde{F}_{\mathrm{mon}}$ is indeed the monicized form of $\widetilde{F}$ as defined in (11).) Using the explicit description of the Cassels map stated in [BS09, §2], one finds that the point $(x_0', c') \in C_{F,\eta_i}(\mathbb{Q}_p)$ gives rise to the class

$$\left.\begin{array}{ll} x_0' - \theta'\eta_i & \text{if } y_0 \neq 0, \\ \widetilde{F}_{\mathrm{mon}}(\theta'\eta_i,\eta_i) + (x_0' - \theta'\eta_i) & \text{if } y_0 = 0 \end{array}\right\} \equiv f_0\cdot\delta \in (K_F^\times/K_F^{\times 2})_{\mathrm{N}\equiv 1}.$$

Meanwhile, by Proposition 6, the class in $(K_F^\times/K_F^{\times 2})_{\mathrm{N}\equiv 1}$ corresponding to $(x_0,y_0,z_0) \in \mathcal{S}_F(\mathbb{Z}_p)$ is also $f_0\cdot\delta$. Thus, the number of elements of $(K_F^\times/K_F^{\times 2})_{\mathrm{N}\equiv 1}$ of the form $f_0\cdot\delta$ arising form points of $\mathcal{S}_F(\mathbb{Z}_p)$ is bounded above by the total number of $G(\mathbb{Q}_p)$-orbits on $V(\mathbb{Q}_p)$ arising from $\mathbb{Q}_p$-rational points on any one of the finitely many curves $C_{F,\eta_1},\dots,C_{F,\eta_\ell}$. By [BG13, §6.2], the number of $G(\mathbb{Q}_p)$-orbits on $V(\mathbb{Q}_p)$ arising from each C_{F,η_i} is at most 2^{m_i-1} when p is odd (resp., 2^{n+m_i-1} when $p=2$), where m_i is the number of distinct irreducible factors of $F_{\mathrm{mon}}(x,\eta_i)$. But clearly $m_i = m$ for each i, so we get the desired upper bound of $\ell\cdot 2^{m-1}$ when p is odd (resp., 2^{n+m-1} when $p=2$).

As for the statement about stabilizers, by Theorem 3, the stabilizer of any orbit arising via orb_F contains a subgroup isomorphic to $K_F^\times[2]_{\mathrm{N}\equiv 1}$, which has size $\#K_F^\times[2]_{\mathrm{N}\equiv 1} = 2^{m-1}$. □

5. Proof of Theorem 1

For a monic polynomial $f = x^{2n+1} + \sum_{i=1}^{2n+1} c_i\cdot x^{2n+1-i} \in \mathbb{Z}[x]$, let the *height* of f be defined by $H(f) := H(c_1,\dots,c_{2n+1}) := \max\{|c_i|^{2n(2n+1)/i} : i = 1,\dots,2n+1\}$. For an element $T \in V(\mathbb{Z})$, let the *height* of (the $G(\mathbb{Z})$-orbit of) T be defined by $H(T) = H(\mathrm{ch}(T))$. We say that (the $G(\mathbb{Z})$-orbit of) T is *irreducible* if $\mathrm{ch}(T)$ is separable and the $G(\mathbb{Q})$-orbit of T is non-distinguished.

5.1. Counting Irreducible Integral Orbits of Bounded Height.

In this section, we give a count of the number of irreducible orbits of $G(\mathbb{Z})$ on $V(\mathbb{Z})$ of bounded height. We use this count in §5.2, where we sieve to those integral orbits that arise from integral points.

Recalling the notation defined in §4.1, fix $m \in \{0,\dots,n\}$ and $\tau \in \{1,\dots,2m+1\}$. Let $V(\mathbb{Z})^{(m,\tau)} := V^{(m,\tau)} \cap V(\mathbb{Z})$, and let $N(V(\mathbb{Z})^{(m,\tau)};X)$ denote the number of $G(\mathbb{Z})$-orbits of irreducible elements $T \in V(\mathbb{Z})^{(m,\tau)}$ satisfying $H(T) < X$. Then we have the following adaptation of [BG13, Theorem 10.1 and (10.27)]:

Theorem 25. *There exists a nonzero constant $\mathscr{J} \in \mathbb{Q}$ such that*

$$N(V(\mathbb{Z})^{(m,\tau)};X) = \frac{1}{2^{m+n}}\cdot|\mathscr{J}|\cdot\mathrm{Vol}(G(\mathbb{Z})\backslash G(\mathbb{R}))\cdot\int_{\substack{(c_1,\dots,c_{2n+1})\in\mathscr{F}(m)\\ H(c_1,\dots,c_{2n+1})<X}} dc_1\cdots dc_{2n+1} + o(X^{\frac{n+1}{2n}}),$$

where the fundamental volume $\mathrm{Vol}(G(\mathbb{Z})\backslash G(\mathbb{R}))$ is computed with respect to a differential ω that generates the rank-1 module of top-degree differentials of G over $\mathbb{Z}$.

Proof. In [BG13], Bhargava and Gross work with the subrepresentation $V' \subset V$ consisting of the traceless operators in V. Such traceless operators have characteristic polynomial with the coefficient c_1 of the term x^{2n} equal to 0. They prove that $N(V'(\mathbb{Z})^{(m,\tau)};X)$ is given by a formula (see [BG13, Theorem 10.1 and (10.27)]) that is almost identical to the formula in the statement of Theorem 25, except that the value of $\mathscr{J}$ may be different and the integral runs over $(0,c_2,\dots,c_{2n+1}) \in \mathscr{F}(m)$.

By simply lifting the restriction that $c_1 = 0$, it is not hard to check that the proof of [BG13, Theorem 10.1 and (10.27)] carries over with minimal modifications to prove Theorem 25. □

In the following lemma, we derive an upper bound on the constant $|\mathscr{J}|$ in Theorem 25:

Lemma 26. *We have that*

$$|\mathscr{J}| \leq 2^{2n} \cdot \mathrm{Vol}(G(\mathbb{Z}_2)) \cdot \prod_{p>2} \frac{p^{2n^2+n} \cdot \mathrm{Vol}(G(\mathbb{Z}_p))}{\#G(\mathbb{Z}/p\mathbb{Z})}.$$

Proof. Let $R = \mathbb{C}$, $\mathbb{R}$, or $\mathbb{Z}_p$ where p is a prime. Let $\mathscr{R} \subset R^{2n+1}$ be any open subset, and let $s\colon \mathscr{R} \to V(R)$ be a continuous function such that the characteristic polynomial of $s(c_1, \dots, c_{2n+1})$ is given by $x^{2n+1} + \sum_{i=1}^{2n+1} c_i x^{2n+1-i}$ for every $(c_1, \dots, c_{2n+1}) \in \mathscr{R}$. The constant $\mathscr{J}$ arises as a multiplicative factor in the following change-of-measure formula:

Proposition 27. *For any measurable function ϕ on $V(R)$, we have*

$$\int_{T \in G(R) \cdot s(\mathscr{R})} \phi(T) dT = |\mathscr{J}| \cdot \int_{\mathscr{R}} \int_{G(R)} \phi(g \cdot s(c_1, \dots, c_{2n+1})) \omega(g) dr,$$

where we regard $G(R) \cdot s(\mathscr{R})$ as a multiset, $|-|$ denotes the standard absolute value on R, dT is the Euclidean measure on $V(R)$, and dr is the restriction to $\mathscr{R}$ of the Euclidean measure on R^{2n+1}.

Proof of Proposition 27. The proof is identical to that of [BS15, Proposition 3.11]. □

In particular, the constant $\mathscr{J}$ is independent of the choices of $R = \mathbb{C}$, $\mathbb{R}$, or $\mathbb{Z}_p$ and of the region $\mathscr{R}$ and the functions s and ϕ. Thus, to compute $|\mathscr{J}|$, we can make the following convenient choices: take $R = \mathbb{Z}_p$, so that $|-| = |-|_p$; take

$$\mathscr{R} = \left\{ (c_1, \dots, c_{2n+1}) \in \mathbb{Z}_p^{2n+1} : x^{2n+1} + \sum_{i=1}^{2n+1} c_i x^{2n+1-i} \equiv f \pmod p \right\}$$

for a fixed monic irreducible degree-$(2n+1)$ polynomial $f \in (\mathbb{Z}/p\mathbb{Z})[x]$; letting $\Sigma_f := \{T \in V(\mathbb{Z}_p) : \mathrm{ch}(T) \equiv f \pmod p\}$, take s to be any continuous right-inverse to the function that sends $T \in \Sigma_f$ to the list of coefficients of $\mathrm{ch}(T)$; and take ϕ to be the function that sends $T \in \Sigma_f$ to $\frac{1}{\#\mathrm{Stab}(T)}$, where $\mathrm{Stab}(T) \subset G(\mathbb{Z}_p)$ is the stabilizer of T, and sends $T \in V(\mathbb{Z}_p) \smallsetminus \Sigma_f$ to 0. The existence of the right-inverse s is well-known; see, e.g., [SSSV21, §3.3].

Because ϕ is $G(\mathbb{Z}_p)$-invariant, Proposition 27 yields that for the above convenient choices, we have on the one hand that

$$\begin{aligned} \mathrm{Vol}(\Sigma_f) &= \int_{T \in G(\mathbb{Z}_p) \cdot s(\mathscr{R})} \frac{1}{\#\mathrm{Stab}(T)} dT \\ &= |\mathscr{J}|_p \cdot \mathrm{Vol}(G(\mathbb{Z}_p)) \cdot \int_{f' \equiv f \pmod p} \sum_{\substack{T \in G(\mathbb{Z}_p) \backslash \Sigma_f \\ \mathrm{ch}(T) = f'}} \frac{1}{\#\mathrm{Stab}(T)} dr. \end{aligned} \tag{40}$$

First suppose $p \neq 2$. We now compute the sum in the integrand in (40). Because we chose f to be irreducible over $\mathbb{Z}/p\mathbb{Z}$, the ring $R_{f'} := \mathbb{Z}_p[x]/(f')$ is the maximal order in its field of fractions $K_{f'}$, and it is in fact the unique local ring of rank $2n+1$ over $\mathbb{Z}_p$ having residue field $\mathbb{F}_{p^{2n+1}}$ (hence $R_{f'}$ does not depend on the choice of f'). Then by [Swa21, (68)], there is precisely one $G(\mathbb{Z}_p)$-orbit with characteristic polynomial f', and the size of the stabilizer of this orbit is equal to $\#R_{f'}^{\times}[2]_{\mathrm{N}\equiv 1} = 1$. Thus, we find that

$$\sum_{\substack{T \in G(\mathbb{Z}_p) \backslash \Sigma_f \\ \mathrm{ch}(T) = f'}} \frac{1}{\#\mathrm{Stab}(T)} = 1. \tag{41}$$

Combining (40) and (41) yields that

$$\mathrm{Vol}(\Sigma_f) = |\mathscr{J}|_p \cdot \mathrm{Vol}(G(\mathbb{Z}_p)) \cdot \int_{f' \equiv f \,(\mathrm{mod}\, p)} dr = |\mathscr{J}|_p \cdot \frac{\mathrm{Vol}(G(\mathbb{Z}_p))}{p^{2n+1}}. \tag{42}$$

Let $\overline{\Sigma}_f := \{T \in V(\mathbb{Z}/p\mathbb{Z}) : \mathrm{ch}(T) = f\}$. Then the mod-$p$ reduction map $\Sigma_f \to \overline{\Sigma}_f$ is surjective, and we have by [BG13, §6.1] that $\#\overline{\Sigma}_f = \#G(\mathbb{Z}/p\mathbb{Z})$. Thus, we have on the other hand that

$$\mathrm{Vol}(\Sigma_f) = \frac{\#\overline{\Sigma}_f}{p^{\dim V}} = \frac{\#G(\mathbb{Z}/p\mathbb{Z})}{p^{2n^2+3n+1}}. \tag{43}$$

Equating (42) and (43) yields that

$$|\mathscr{J}|_p = \frac{\#G(\mathbb{Z}/p\mathbb{Z})}{p^{2n^2+n} \cdot \mathrm{Vol}(G(\mathbb{Z}_p))} \tag{44}$$

when $p \neq 2$.

Next, suppose $p = 2$. We now derive an upper bound on the sum in the integrand in (40). By [Swa21, (77)], the number of $G(\mathbb{Z}_2)$-orbits with characteristic polynomial f' is equal to $2^{n-1}(2^n + 1)$. The size of the stabilizer of any such orbit is equal to $\#R_{f'}^{\times}[2]_{\mathrm{N}\equiv 1} = 1$, so we find that

$$\sum_{\substack{T \in G(\mathbb{Z}_p)\backslash\Sigma_f \\ \mathrm{ch}(T) = f'}} \frac{1}{\#\,\mathrm{Stab}(T)} = 2^{n-1}(2^n + 1). \tag{45}$$

Combining (40) and (45) yields that

$$\mathrm{Vol}(\Sigma_f) = |\mathscr{J}|_2 \cdot \mathrm{Vol}(G(\mathbb{Z}_2)) \cdot \frac{2^{n-1}(2^n+1)}{2^{2n+1}}. \tag{46}$$

Let $\overline{\Sigma}_f = \{T \in V(\mathbb{Z}/2\mathbb{Z}) : \mathrm{ch}(T) = f\}$. Then the mod-2 reduction map $\Sigma_f \to \overline{\Sigma}_f$ is surjective, and by Propositions 4 and 6, the action of $G(\mathbb{Z}/2\mathbb{Z})$ on $\overline{\Sigma}_f$ is simply transitive, so $\#\overline{\Sigma}_f = \#G(\mathbb{Z}/2\mathbb{Z})$. Thus, we have on the other hand that

$$\mathrm{Vol}(\Sigma_f) = \frac{\#\overline{\Sigma}_f}{2^{\dim V}} = \frac{\#G(\mathbb{Z}/2\mathbb{Z})}{2^{2n^2+3n+1}}. \tag{47}$$

Combining (46) and (47) yields that

$$|\mathscr{J}|_2^{-1} = 2^{2n} \cdot \mathrm{Vol}(G(\mathbb{Z}_2)) \cdot \frac{2^{2n^2-1}(2^n+1)}{\#G(\mathbb{Z}/2\mathbb{Z})} \tag{48}$$

Since G is not smooth over $\mathbb{Z}_2$, computing $\mathrm{Vol}(G(\mathbb{Z}_2))$ is far more complicated, but we do not need to know the value of $\mathrm{Vol}(G(\mathbb{Z}_2))$ for our purpose. The value of $\#G(\mathbb{Z}/2\mathbb{Z})$ is given in [Cho15, §6] to be $\#G(\mathbb{Z}/2\mathbb{Z}) = 2^{n^2} \cdot \prod_{i=1}^{n}(2^{2i} - 1)$, so it follows that

$$\frac{2^{2n^2-1}(2^n+1)}{\#G(\mathbb{Z}/2\mathbb{Z})} = (2^{-1} + 2^{-n-1}) \cdot \prod_{i=1}^{n}(1 - 2^{-2i})^{-1} \leq 1. \tag{49}$$

Applying the identity

$$|\mathscr{J}| \cdot \prod_{p} |\mathscr{J}|_p = 1 \tag{50}$$

to (44), (48), and (49) completes the proof of Lemma 26. □

5.2. **Sieving to Orbits Arising From Local Points When $2 \nmid f_0$.** Let $\mathscr{F}^*_{2n+1}(f_0)$ be the subset of all $F \in \mathscr{F}_{2n+1}(f_0)$ satisfying both conditions in Theorem 14 for every prime $p \mid \kappa$. Let δ be the upper density of forms $F \in \mathscr{F}_{2n+1}(f_0)$, enumerated by height, such that $\mathcal{S}_F(\mathbb{Z}) \neq \varnothing$. Then δ is bounded as follows:

$$\delta \leq \lim_{X\to\infty} \frac{\#\{F \in \mathscr{F}^*_{2n+1}(f_0) : H(F) < X\} + \#\big(G(\mathbb{Q})\backslash\{T \in V(\mathbb{Z}) : T \text{ is good, } H(T) < X\}\big)}{\#\{F \in \mathscr{F}_{2n+1}(f_0) : H(F) < X\}}, \tag{51}$$

where we say that $T \in V(\mathbb{Z})$ is *good* if it is irreducible and $T \in \mathscr{P}_v$ for every place v. The first term in the numerator and the denominator on the right-hand side of (51) are respectively given by

$$\#\{F \in \mathscr{F}^*_{2n+1}(f_0) : H(F) < X\} = \mu_{f_0} \cdot f_0^{-2n^2-n} \cdot 2^{2n+1} \cdot X^{\frac{n+1}{2n}} + o(X^{\frac{n+1}{2n}}), \quad \text{and} \tag{52}$$

$$\#\{F \in \mathscr{F}_{2n+1}(f_0) : H(F) < X\} = f_0^{-2n^2-n} \cdot 2^{2n+1} \cdot X^{\frac{n+1}{2n}} + o(X^{\frac{n+1}{2n}}). \tag{53}$$

We now bound the second term in the numerator on the right-hand side of (51). To do this, we use the following result, which generalizes Theorem 25 by giving an upper bound on the number of integral orbits of height up to X satisfying certain infinite sets of local conditions:

Theorem 28 (cf. [BG13, Theorem 10.12])**.** *Let $\phi\colon V(\mathbb{Z}) \to [0,1] \subset \mathbb{R}$ be a function such that there exists a function $\phi_p\colon V(\mathbb{Z}_p) \to [0,1]$ for each prime p satisfying the following conditions:*

- *For all $T \in V(\mathbb{Z})$, the product $\prod_p \phi_p(T)$ converges to $\phi(T)$; and*
- *For each p, the function ϕ_p is locally constant outside a closed set $S_p \subset V(\mathbb{Z}_p)$ of measure 0.*

Let $N_\phi(V(\mathbb{Z})^{m,\tau}; X)$ denote the number of $G(\mathbb{Z})$-orbits of irreducible elements $T \in V(\mathbb{Z})^{m,\tau}$ satisfying $H(T) < X$, where each orbit $G(\mathbb{Z}) \cdot T$ is counted with weight $\phi(T) := \prod_p \phi_p(T)$. Then we have

$$N_\phi(V(\mathbb{Z})^{(m,\tau)}; X) \leq N(V(\mathbb{Z})^{(m,\tau)}; X) \cdot \prod_p \int_{T \in V(\mathbb{Z}_p)} \phi_p(T) dT + o(X^{\frac{n+1}{2n}}).$$

Proof. The proof is identical to the first half of the proof of [BS15, Theorem 2.21] (note that the "acceptable" hypothesis in [BS15, Theorem 2.21] is not needed for the upper bound in Theorem 28). □

To apply Theorem 28 to bound the second term in the numerator of (51), we need to choose the weight functions ϕ_p. Given $T \in V(\mathbb{Z})$, denote by $m(T)$ the quantity

$$m(T) := \sum_{T' \in \mathscr{O}(T)} \frac{\#\operatorname{Stab}_{\mathbb{Q}}(T')}{\#\operatorname{Stab}_{\mathbb{Z}}(T')} = \sum_{T' \in \mathscr{O}(T)} \frac{\#\operatorname{Stab}_{\mathbb{Q}}(T)}{\#\operatorname{Stab}_{\mathbb{Z}}(T')},$$

where $\mathscr{O}(T)$ denotes a set of representatives for the action of $G(\mathbb{Z})$ on the $G(\mathbb{Q})$-orbit of T, and where $\operatorname{Stab}_{\mathbb{Q}}(T')$ and $\operatorname{Stab}_{\mathbb{Z}}(T')$ respectively denote the stabilizers of T' in $G(\mathbb{Q})$ and $G(\mathbb{Z})$. By [BG13, Proposition 10.8], counting $G(\mathbb{Q})$-orbits on $V(\mathbb{Z})$ is, up to a negligible error, no different from counting $G(\mathbb{Z})$-orbits on $V(\mathbb{Z})$, where the $G(\mathbb{Z})$-orbit of $T \in V(\mathbb{Z})$ is weighted by $1/m(T)$.

The weight $m(T)$ can be expressed as a product over primes p of local weights $m_p(T)$. Indeed, as stated in [BG13, (11.3)], we have that

$$m(T) = \prod_p m_p(T), \quad \text{where} \quad m_p(T) := \sum_{T' \in \mathscr{O}_p(T)} \frac{\#\operatorname{Stab}_{\mathbb{Q}_p}(T)}{\#\operatorname{Stab}_{\mathbb{Z}_p}(T')}, \tag{54}$$

where $\mathscr{O}_p(T)$ denotes a set of representatives for the action of $G(\mathbb{Z}_p)$ on the $G(\mathbb{Q}_p)$-orbit of T, and where $\operatorname{Stab}_{\mathbb{Q}_p}(T')$ and $\operatorname{Stab}_{\mathbb{Z}_p}(T')$ respectively denote the stabilizers of T' in $G(\mathbb{Q}_p)$ and $G(\mathbb{Z}_p)$.

For each prime p, let $\psi_p\colon V(\mathbb{Z}_p) \to \{0,1\} \subset \mathbb{R}$ be the indicator function of elements $T \in \mathscr{P}_p$ such that $\operatorname{ch}(T)$ is separable. Then upon taking $\phi_p = \psi_p/m_p$ for each p, Proposition 15 and

Theorem 28 together imply that the numerator of (51) is bounded above by

$$\sum_{m=0}^{n}\sum_{\tau=1}^{2m+1} N(V(\mathbb{Z})^{m,\tau};X)\cdot\prod_{p}\int_{T\in V(\mathbb{Z}_p)}\frac{\psi_p(T)}{m_p(T)}dT+o(X^{\frac{n+1}{2n}}). \tag{55}$$

In the following proposition, we give a formula for the integrals over $V(\mathbb{Z}_p)$ in (55):

Proposition 29. *Let p be a prime and let ψ be a continuous $G(\mathbb{Q}_p)$-invariant function on $V(\mathbb{Z}_p)$ such that every element $T\in V(\mathbb{Z}_p)$ in the support of ψ is separable. Then we have*

$$\int_{T\in V(\mathbb{Z}_p)}\frac{\psi(T)}{m_p(T)}dT=$$
$$|\mathscr{J}|_p\cdot\mathrm{Vol}(G(\mathbb{Z}_p))\cdot\int_{(c_1,\dots,c_{2n+1})\in\mathbb{Z}_p^{2n+1}}\sum_{\substack{T\in G(\mathbb{Q}_p)\backslash V(\mathbb{Z}_p)\\ \mathrm{ch}(T)=x^{2n+1}+c_1x^{2n}+\cdots+c_{2n+1}}}\frac{\psi(T)}{\#\,\mathrm{Stab}_{\mathbb{Q}_p}(T)}\,dc_1\cdots dc_{2n+1},$$

where $\mathscr{J}\in\mathbb{Q}$ is the same constant that appears in Theorem 25.

Proof. The proof is identical to that of [BG13, Corollary 11.3]. □

If $2\neq p\mid f_0$, combining Proposition 24, Lemma 26, and Proposition 29 yields that

$$\int_{T\in V(\mathbb{Z}_p)}\frac{\psi_p(T)}{m_p(T)}dT\le|\mathscr{J}|_p\cdot\mathrm{Vol}(G(\mathbb{Z}_p))\cdot\int_{\substack{\vec{c}=(c_1,\dots,c_{2n+1})\in\mathbb{Z}_p^{2n+1}\\ f_0^{i-1}|c_i\text{ for every }i}}\frac{2^{m(\vec{c})+1}}{2^{m(\vec{c})-1}}\,dc_1\cdots dc_{2n+1},$$
$$=4\cdot\mathrm{Vol}(G(\mathbb{Z}_p))\cdot|f_0|_p^{2n^2+n}, \tag{56}$$

where $m(\vec{c})$ is the number of irreducible factors of the polynomial $x^{2n+1}+\sum_{i=1}^{2n+1}c_i\cdot x^{2n+1-i}\in\mathbb{Z}_p[x]$. Similarly, when $2=p\mid f_0$, combining Proposition 24 and Proposition 29 yields that

$$\int_{T\in V(\mathbb{Z}_2)}\frac{\psi_2(T)}{m_2(T)}dT\le 8\cdot 2^n\cdot|\mathscr{J}|_2\cdot\mathrm{Vol}(G(\mathbb{Z}_2))\cdot|f_0|_2^{2n^2+n}. \tag{57}$$

Next, for odd primes $p\nmid f_0$, Proposition 16 gives an upper bound on $\mathrm{Vol}(\mathscr{P}_p)=\int_{T\in V(\mathbb{Z}_p)}\psi_p(T)dT$. Upon observing that $m_p(T)\ge 1$, we deduce that the factor at p in (55) is bounded by

$$\int_{T\in V(\mathbb{Z}_p)}\frac{\psi_p(T)}{m_p(T)}dT\le\mathrm{Vol}(\mathscr{P}_p)\le\min\left\{1,\sum_{m=1}^{2n+1}\frac{p+1}{2^{m-1}}\cdot\mathrm{Vol}(G(\mathbb{Z}_p))\cdot\frac{\#\mathscr{I}_p(m)}{p^{2n+1}}\right\} \tag{58}$$

If $2=p\nmid f_0$, then we can use Proposition 19 to similarly deduce that

$$\int_{T\in V(\mathbb{Z}_2)}\frac{\psi_2(T)}{m_2(T)}dT\le\mathrm{Vol}(\mathscr{P}_2)\le\sum_{m=1}^{2n+1}\frac{12}{2^{2n+m-1}}\cdot 2\cdot\frac{\#\mathscr{I}_8(m)}{8^{2n+1}}. \tag{59}$$

5.3. **The Final Step.** By [Lan66], the Tamagawa number of G is equal to 2, so we have

$$\mathrm{Vol}(G(\mathbb{Z})\backslash G(\mathbb{R}))\cdot\prod_p\mathrm{Vol}(G(\mathbb{Z}_p))=2. \tag{60}$$

We can now apply Theorem 25, Lemma 26, and the bounds in (56), (57), (58), and (59) to bound (55); combining the result with (52) and (53) gives a bound on δ via (51). Then, simplifying this bound using (50) and (60), we draw the following conclusions:

Case 1: $2\nmid f_0$. When $2\nmid f_0$, we have

$$\delta-\mu_{f_0}\ll\left(\sum_{m=0}^{n}2^{2n}\cdot\frac{2m+1}{2^{n+m}}\cdot\mu(\mathscr{J}(m))\right)\cdot\left(\sum_{m=1}^{2n+1}\frac{1}{2^{2n+m}}\cdot\frac{\#\mathscr{I}_8(m)}{8^{2n+1}}\right). \tag{61}$$

$$\left(\prod_{p\nmid 2f_0}\min\left\{\frac{p^{2n^2+n}}{\#G(\mathbb{Z}/p\mathbb{Z})},\sum_{m=1}^{2n+1}\frac{p+1}{2^{m-1}}\cdot\frac{\#\mathscr{I}_p(m)}{p^{2n+1}}\right\}\right)$$

where $\mu(\mathscr{I}(m)) := (2^{2n+1}\cdot X^{\frac{n+1}{2n}})^{-1}\cdot\int_{\substack{(c_1,\dots,c_{2n+1})\in\mathscr{I}(m)\\ H(c_1,\dots,c_{2n+1})<X}} dc_1\cdots dc_{2n+1}$ denotes the probability that a monic degree-$(2n+1)$ polynomial over $\mathbb{R}$ has $2m+1$ real roots, and where the implied constant is independent of n. In (61), the archimedean factor is $O(2^n)$, the factor at primes dividing f_0 is $O(1)$, and the factor at 2 is $O(2^{-2n})$.

We now bound the factor at odd primes not dividing f_0. The following lemma allows us to bound the factors at primes less than a small power of the degree $2n+1$:

Lemma 30. *We have for each fixed $A\in(0,1/3)\subset\mathbb{R}$ that*

$$\prod_{3\le p\le(2n+1)^A}\sum_{m=1}^{2n+1}\frac{p+1}{2^{m-1}}\cdot\frac{\#\mathscr{I}_p(m)}{p^{2n+1}}\ll 2^{-\varepsilon_1 n^{\varepsilon_2}},$$

where $\varepsilon_1,\varepsilon_2>0$ are real numbers that may depend on A.

Proof. We first estimate each factor in the product over primes. We split the sum at the prime p into two ranges, one for $m\le\frac{1}{2}\log(2n+1)$ and one for $m>\frac{1}{2}\log(2n+1)$. We bound the sum over $m>\frac{1}{2}\log(2n+1)$ as follows:

$$\sum_{\frac{1}{2}\log(2n+1)<m\le 2n+1}\frac{p+1}{2^{m-1}}\cdot\frac{\#\mathscr{I}_p(m)}{p^{2n+1}}\le\sum_{\frac{1}{2}\log(2n+1)<m\le 2n+1}\frac{p+1}{2^{m-1}}\le\frac{2(p+1)}{\sqrt{2n+1}}. \tag{62}$$

For the sum over $m<\frac{1}{2}\log(2n+1)$, we rely on the following result of Afshar and Porritt:[2]

Theorem 31 ([AP19, Remark 2.11])**.** *Let p be a prime, and let $1\le m\le\log(2n+1)$. Then we have the following uniform estimate:*

$$\frac{\#\mathscr{I}_p(m)}{p^{2n+1}}=\frac{1}{(2n+1)}\cdot\frac{(\log(2n+1))^{m-1}}{(m-1)!}\cdot\left(D_p\left(\frac{m-1}{\log(2n+1)}\right)+O\left(\frac{m}{(\log(2n+1))^2}\right)\right)$$

where the implied constant is absolute (i.e., does not depend on p), and where the function D_p is defined as follows. Letting $\mathscr{I}\subset(\mathbb{Z}/p\mathbb{Z})[x]$ be the set of all monic irreducible polynomials, we have

$$D_p(z)=\frac{E(1/p,z)}{\Gamma(1+z)},\quad \textit{where}\quad E(x,z)=\prod_{f\in\mathscr{I}}\left(1+\frac{zx^{\deg f}}{1-x^{\deg f}}\right)\cdot(1-x^{\deg f})^z.$$

We now turn the very careful estimate in Theorem 31 into a more easily usable form. First, notice that for any $x\in(0,1/2)\subset\mathbb{R}$ and $z\in(0,1)$ we have

$$\left(1+\frac{zx}{1-x}\right)\cdot(1-x)^z\le\left(1+\frac{zx}{1-x}\right)\cdot(1-zx)=1+\frac{(z-z^2)x^2}{1-x}\le 1+x^2. \tag{63}$$

By Carlitz's Theorem (see [Car32]), there are exactly p^{d-1} monic separable polynomials of degree d over $\mathbb{Z}/p\mathbb{Z}$, and hence at most p^{d-1} monic irreducible polynomials of degree d over $\mathbb{Z}/p\mathbb{Z}$. Using this together with (63), we deduce that

$$E(1/p,z)\le\prod_{f\in\mathscr{I}}(1+p^{-2\deg f})\le\prod_{d=1}^{\infty}(1+p^{-2d})^{p^{d-1}}. \tag{64}$$

[2]Note that a result of this type was first proven by Car in [Car82]; the dependence of the error term on the prime p was made explicit in [AP19].

To estimate the right-hand side of (64), we take its logarithm and apply the bound $\log(1+x) \le x$ (which holds for $x > -1$):

$$\log\left(\prod_{d=1}^{\infty}(1+p^{-2d})^{p^{d-1}}\right) = \sum_{d=1}^{\infty} p^{d-1}\cdot\log(1+p^{-2d}) \le \sum_{d=1}^{\infty} p^{d-1}\cdot p^{-2d} = \frac{1}{p(p-1)}. \tag{65}$$

Taking $p = 2$ in (65) and using the fact that $\Gamma(1+z) > 1/2$, we have for any prime p, any $1 \le m \le \log(2n+1)$, and all sufficiently large n that

$$D_p\left(\frac{m-1}{\log(2n+1)}\right) + O\left(\frac{m}{(\log(2n+1))^2}\right) \le 2\sqrt{e} + O\left(\frac{m}{(\log(2n+1))^2}\right) \le 4, \tag{66}$$

where e denotes the usual base of the natural logarithm. Upon combining (62), (66), and Theorem 31, we find for all sufficiently large n that

$$\begin{aligned}\sum_{m=1}^{2n+1} \frac{p+1}{2^{m-1}}\cdot\frac{\#\mathscr{J}_p(m)}{p^{2n+1}} &\le \frac{2(p+1)}{\sqrt{2n+1}} + \sum_{1\le m\le \frac{1}{2}\log(2n+1)} \frac{4(p+1)}{(2n+1)}\cdot\frac{(\frac{1}{2}\log(2n+1))^{m-1}}{(m-1)!}\\ &\le \frac{2(p+1)}{\sqrt{2n+1}} + \frac{4(p+1)}{2n+1}\cdot e^{\frac{1}{2}\log(2n+1)} = \frac{6p+6}{\sqrt{2n+1}} \le \frac{8p}{\sqrt{2n+1}},\end{aligned} \tag{67}$$

where we have used the fact that $\sum_{i=0}^{N}\frac{x^i}{i!} \le e^x$ for any $x > 0$ and integer $N \ge 0$. By Erdős' proof of Bertrand's Postulate, we have $\prod_{p<N} < 4^N$ for any $N \ge 3$. By the Prime Number Theorem, for any $\varepsilon > 0$, there exists an integer $N > 0$ such that for all $N' > N$, the number of primes less than or equal to N' is at least $(1-\varepsilon)\cdot\frac{N'}{\log N'}$ and is at most $(1+\varepsilon)\cdot\frac{N'}{\log N'}$. Combining this fact with (67), we find for any fixed $A < 1/3$ and all sufficiently large n (where "large" depends on A and ε) that

$$\prod_{3\le p\le(2n+1)^A}\sum_{m=1}^{2n+1}\frac{p+1}{2^{m-1}}\cdot\frac{\#\mathscr{J}_p(m)}{p^{2n+1}} \le \frac{8^{(1+\varepsilon)\cdot\frac{(2n+1)^A}{A\log(2n+1)}}\cdot 4^{(2n+1)^A}}{(\sqrt{2n+1})^{(1-\varepsilon)\cdot\frac{(2n+1)^A}{A\log(2n+1)}}} \ll 2^{-\varepsilon_1 n^{\varepsilon_2}},$$

for some real numbers $\varepsilon_2, \varepsilon_2 > 0$. □

The following lemma allows us to bound the factors at the remaining primes:

Lemma 32. *We have that*

$$\prod_{p>2}\frac{p^{2n^2+n}}{\#G(\mathbb{Z}/p\mathbb{Z})} \ll 1,$$

where the implied constant does not depend on n.

Proof. From (27), it follows that

$$\log\frac{p^{2n^2+n}}{\#G(\mathbb{Z}/p\mathbb{Z})} = \sum_{i=1}^{n} -\log(1-p^{-2i}) \le 2\cdot\sum_{i=1}^{n} p^{-2i} \le \frac{2}{p^2-1}, \tag{68}$$

where we have applied the bound $-\log(1-x) \le 2x$, which holds for $x \in (0, 1/2) \subset \mathbb{R}$. It is not hard to check (by comparing derivatives) that $\frac{2}{p^2-1} \le \log(1+p^{-\frac{3}{2}})$ for each $p \ge 5$. Thus,

$$\prod_{p>2}\frac{p^{2n^2+n}}{\#G(\mathbb{Z}/p\mathbb{Z})} \le \frac{e^{\frac{1}{4}}}{(1+2^{-\frac{3}{2}})(1+3^{-\frac{3}{2}})}\cdot\prod_{p}(1+p^{-\frac{3}{2}}) \ll 1.$$ □

It follows from Lemmas 30 and 32 that the factor at the odd primes not dividing f_0 is $O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ for some real numbers $\varepsilon_1, \varepsilon_2 > 0$, so by (61), we have $\delta = \mu_{f_0} + o(2^{-n})$. This completes the proof of the second statement in part (a) of Theorem 1.

We now determine the smallest n for which our method yields that a positive proportion of superelliptic stacky curves in $\mathscr{F}_{2n+1}(f_0)$ are insoluble. To this end, let $\mathscr{F}^{\max}_{2n+1}(f_0)$ be the set of forms

$F \in \mathscr{F}_{2n+1}(f_0)$ such that $R_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is the maximal order in $K_F \otimes_{\mathbb{Q}} \mathbb{Q}_p$ for every prime $p \mid f_0$ and such that condition (b) in Theorem 14 fails for some prime $p \mid \kappa$. Let $\delta_{\max}$ be the upper density of forms $F \in \mathscr{F}^{\max}_{2n+1}(f_0)$, enumerated by height, such that $\mathcal{S}_F(\mathbb{Z}) \neq \varnothing$. For each prime $p \mid f_0$, instead of applying Propositions 24 and 29 to obtain the bound (56), we can apply Proposition 23 together with the trivial bound $m_p(T) \geq 1$; doing so yields the following explicit bound on $\delta_{\max}$:

$$\delta_{\max} \leq 2 \cdot \left(\sum_{m=0}^{n} 2^{2n} \cdot \frac{2m+1}{2^{n+m}} \cdot \mu(\mathscr{I}(m)) \right) \cdot \left(\sum_{m=1}^{2n+1} \frac{12}{2^{2n+m-1}} \cdot \frac{\#G(\mathbb{Z}/8\mathbb{Z})}{8^{2n^2+n}} \cdot \frac{\#\mathcal{I}_8(m)}{8^{2n+1}} \right) \cdot \left(\prod_{p>2} \frac{p^{2n^2+n}}{\#G(\mathbb{Z}/p\mathbb{Z})} \right) \tag{69}$$

Upon applying the estimates

$$\sum_{m=0}^{n} \frac{2m+1}{2^{n+m}} \cdot \mu(\mathscr{I}(m)) \leq \frac{3}{2} \cdot \sum_{m=0}^{n} \mu(\mathscr{I}(m)) = \frac{3}{2} \quad \text{and} \quad \frac{\#\mathcal{I}_8(m)}{8^{2n+1}} \leq 1, \tag{70}$$

we deduce that $\delta_{\max} < 2^{7-n} \leq 1$ whenever $n \geq 7$. By explicitly computing $\frac{\#\mathcal{I}_8(m)}{8^{2n+1}}$ in `sage` for $n < 7$, one can check that we also have $\delta_{\max} < 1$ when $n \in \{5, 6\}$. Since the density of $\mathscr{F}^{\max}_{2n+1}(f_0)$ in $\mathscr{F}_{2n+1}(f_0)$ is positive, this completes the proof of the first statement in part (a) of Theorem 1.

Case 2: $2 \mid f_0$. When $2 \mid f_0$, we have

$$\delta - \mu_{f_0} \ll \left(\sum_{m=0}^{n} \frac{2m+1}{2^{n+m}} \cdot \mu(\mathscr{I}(m)) \right) \cdot 2^n \cdot \left(\prod_{p \nmid f_0} \min \left\{ \frac{p^{2n^2+n}}{\#G(\mathbb{Z}/p\mathbb{Z})}, \sum_{m=1}^{2n+1} \frac{p+1}{2^{m-1}} \cdot \frac{\#\mathscr{I}_p(m)}{p^{2n+1}} \right\} \right) \tag{71}$$

where the implied constant is independent of n. In (71), the archimedean factor is $O(2^{-n})$, the factor at 2 is $O(2^n)$, and the factor at primes dividing f_0 is $O(1)$. It follows from Lemmas 30 and 32 that the factor at the primes not dividing f_0 is $O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ for some real numbers $\varepsilon_1, \varepsilon_2 > 0$, so $\delta = \mu_{f_0} + O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ in this case. This completes the proof of part (b) of Theorem 1.

Remark 33. In [DPSZ02], it is shown that the density of real degree-N polynomials (not necessarily monic) having fewer than $\log(N+1)/\log\log(N+1)$ real zeros is $O((N+1)^{-b+o(1)})$ for some absolute constant $b > 0$. We expect that one can imitate the proof of this density result to obtain an analogous theorem for monic polynomials. Given such an analogue, it may be possible to improve (albeit modestly) the bounds on δ that we obtained above by bounding the probability $\mu(\mathscr{I}(m))$.

6. Obstruction to the Hasse Principle and the Proof of Theorem 2

In this section, we study how often superelliptic stacky curves satisfy the Hasse principle using the method of descent. Specifically, we describe 2-coverings of superelliptic stacky curves, and we modify the proof of Theorem 1 to show that superelliptic stacky curves often have no locally soluble 2-coverings and thus fail the Hasse principle. Upon showing that such a 2-covering obstruction to solubility is a special case of the Brauer–Manin obstruction, we obtain Theorem 2.

6.1. Defining the Brauer–Manin Obstruction for $\mathcal{S}_F$.

Let F be a separable integral binary form of degree $2n+1 \geq 3$. While a suitable theory of Brauer–Manin obstruction for stacks remains to be developed, such a theory is not required in the context of superelliptic stacky curves. Indeed, we can exploit the fact that the stack $\mathcal{S}_F$ is defined as a quotient of the punctured affine surface $\widetilde{S}_F$ (see (2)), where the usual theory of the Brauer–Manin obstruction for varieties applies.

Let $\widetilde{S}_{F,\mathbb{Q}} = \widetilde{S}_F \otimes_{\mathbb{Z}} \mathbb{Q}$, and let $\widetilde{S}_{F,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$ denote the usual Brauer–Manin set of the $\mathbb{Q}$-variety $\widetilde{S}_{F,\mathbb{Q}}$ (see [CDX19, §1] for the definition). Let

$$\widetilde{S}_F(\mathbb{A}_{\mathbb{Q}})^{\mathrm{int}} := \prod_v \widetilde{S}_F(\mathbb{Z}_v) \tag{72}$$

be the set of adelic points of $\widetilde{S}_F$ that are integral in every place (i.e., the set of everywhere-primitive adelic solutions to the superelliptic equation $y^2 = F(x,z)$, or equivalently, the set of everywhere-integral adelic points on the stacky curve $\mathcal{S}_F$). With this notation in place, we define the *Brauer–Manin set* of $\mathcal{S}_F$ by

$$\mathcal{S}_F(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} := \widetilde{S}_F(\mathbb{A}_{\mathbb{Q}})^{\mathrm{int}} \cap \widetilde{S}_{F,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}, \tag{73}$$

and we say that $\mathcal{S}_F$ *has a Brauer–Manin obstruction to having an integral point* if its Brauer–Manin set is empty (i.e., if $\mathcal{S}_F(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \varnothing$).

Because we have defined $\mathcal{S}_F(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$ as a subset of $\widetilde{S}_{F,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$, we can use the method of descent as laid out for open varieties in [CDX19] to obtain a set-theoretic "upper bound" on $\mathcal{S}_F(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$. Indeed, suppose that we have a torsor $f\colon Z \to \widetilde{S}_{F,\mathbb{Q}}$ by a group of multiplicative type or connected algebraic group Γ (all defined over $\mathbb{Q}$). Let

$$\widetilde{S}_{F,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^f := \bigcup_{\sigma \in H^1(G_{\mathbb{Q}}, \Gamma(\overline{\mathbb{Q}}))} f^\sigma(Z^\sigma(\mathbb{A}_{\mathbb{Q}})) \tag{74}$$

be the descent set of f, where $f^\sigma\colon Z^\sigma \to \widetilde{S}_{F,\mathbb{Q}}$ is the twist of $f\colon Z \to \widetilde{S}_{F,\mathbb{Q}}$ by a 1-cocycle representing $\sigma \in H^1(G_{\mathbb{Q}}, \Gamma(\overline{\mathbb{Q}}))$. Since $\widetilde{S}_{F,\mathbb{Q}}$ is smooth and geometrically integral, [CDX19, Theorem 1.1] implies that

$$\widetilde{S}_{F,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \subset \widetilde{S}_{F,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^f. \tag{75}$$

It follows from (73) and (75) that $\mathcal{S}_F$ has a Brauer–Manin obstruction to having an integral point if it has an obstruction to descent by Γ-torsors in the sense that $\widetilde{S}_F(\mathbb{A}_{\mathbb{Q}})^{\mathrm{int}} \cap \widetilde{S}_{F,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^f = \varnothing$.

6.2. **2-Coverings.** Let k be a field of characteristic not equal to 2, let $f_0 \in k^\times$, and let $F \in \mathscr{F}_{2n+1}(f_0, k)$ be separable. Let $\theta_1, \dots, \theta_{2n+1} \in k_{\mathrm{sep}}$ be the distinct roots of the polynomial $F(x,1)$, and for each $\sigma \in G_k$ and $i \in \{1, \dots, 2n+1\}$, let $\sigma(i) \in \{1, \dots, 2n+1\}$ be defined by $\theta_{\sigma(i)} = \sigma(\theta_i)$. Let $\widetilde{S}_F$ and $\mathcal{S}_F$ respectively denote the corresponding punctured affine surface and stacky curve (which are now defined over k, as opposed to $\mathbb{Z}$). In this section, we specialize the discussion of descent in §6.1 to the case where Γ is equal to the Jacobian $\mathrm{Pic}^0(\mathcal{S}_F)$ of $\mathcal{S}_F$ (see §4). Notice that $\mathrm{Pic}^0(\mathcal{S}_F)$ is a group of multiplicative type, because over k_{sep}, it is isomorphic to a finite product of copies of $\mathbb{Z}/2\mathbb{Z}$ and is thus diagonalizable. Consequently, we can apply (75) to $\mathrm{Pic}^0(\mathcal{S}_F)$-torsors.

A Galois étale covering defined over k with Galois group isomorphic to $\mathrm{Pic}^0(\mathcal{S}_F)$ as G_k-modules is called a 2-*covering*. Our strategy for describing the 2-coverings of $\widetilde{S}_F$ is to describe the 2-coverings of $\mathcal{S}_F$ and pull back along the quotient map $\widetilde{S}_F \to [\widetilde{S}_F/\mathbb{G}_m] = \mathcal{S}_F$. We now briefly recall the results of [BF05, §5], in which Bruin and Flynn explicitly construct all 2-coverings of $\mathcal{S}_F$ up to isomorphism over k (see also [Bru02, §3]). Consider the projective space $\mathbb{P}^{2n}_k$ with homogeneous coordinates $[Z_1 : \cdots : Z_{2n+1}]$ such that G_k acts on Z_i by $\sigma \cdot Z_i = Z_{\sigma(i)}$. The *distinguished covering* is defined to be the closed subscheme $C^1 \subset \mathbb{P}^{2n}_k$ cut out by the homogeneous ideal

$$I^1 := \big((\theta_i - \theta_j)(Z_\ell^2 - Z_m^2) - (\theta_\ell - \theta_m)(Z_i^2 - Z_j^2) : i,j,\ell,m \in \{1, \dots, 2n+1\}\big).$$

Let $\pi^1\colon C^1 \to \mathbb{P}^1_k$ be the map defined by

$$\pi^1([Z_1 : \cdots : Z_{2n+1}]) = \frac{\theta_j Z_i^2 - \theta_i Z_j^2}{Z_i^2 - Z_j^2}$$

for any distinct $i, j \in \{1, \dots, 2n+1\}$. For each class $\delta \in H^1(G_k, \mathrm{Pic}^0(\mathcal{S}_F))$, the twist of $\pi^1 \colon C^1 \to \mathbb{P}^1_k$ by δ is given explicitly as follows. By [BG13, last paragraphs of §4.2 and §5.1], $H^1(G_{\mathbb{Q}}, \mathrm{Pic}^0(\mathcal{S}_F))$ can be identified with $(K_F^\times / K_F^{\times 2})_{\mathrm{N}\equiv 1}$, so we may think of δ as being an element of $(K_F^\times / K_F^{\times 2})_{\mathrm{N}\equiv 1}$. Let $(\delta_1, \dots, \delta_{2n+1})$ be the image of δ under the map $K_F^\times / K_F^{\times 2} \to \left((k_{\mathrm{sep}})^\times / (k_{\mathrm{sep}})^{\times 2}\right)^{2n+1}$ given by taking the product of the distinct embeddings of each field component of K_F into k_{sep}. Then the twist of C^1 by δ is the closed subscheme $C^\delta \subset \mathbb{P}^{2n}_k$ cut out by the homogeneous ideal

$$I^\delta := \left((\theta_i - \theta_j)(\delta_\ell Z_\ell^2 - \delta_m Z_m^2) - (\theta_\ell - \theta_m)(\delta_i Z_i^2 - \delta_j Z_j^2) : i, j, \ell, m \in \{1, \dots, 2n+1\}\right),$$

and the twist of $\pi^1 \colon C^1 \to \mathbb{P}^1_k$ is the map $\pi^\delta \colon C^\delta \to \mathbb{P}^1_k$ defined by

$$\pi^\delta([Z_1 : \cdots : Z_{2n+1}]) = \frac{\theta_j \delta_i Z_i^2 - \theta_i \delta_j Z_j^2}{\delta_i Z_i^2 - \delta_j Z_j^2}$$

for any distinct $i, j \in \{1, \dots, 2n+1\}$. The following theorem enumerates the basic properties of the maps $\pi^\delta \colon C^\delta \to \mathbb{P}^1_k$:

Theorem 34 ([BF05, Lemma 5.10] and [Bru02, §3.1])**.** *With notation as above, we have:*

(a) *For each $\delta \in (K_F^\times / K_F^{\times 2})_{\mathrm{N}\equiv 1}$, the scheme C_δ is a smooth, geometrically irreducible, projective curve of genus $n \cdot 2^{2n-1} - 3 \cdot 2^{2n-2} + 1$;*
(b) *The action of G_k leaves both I^δ and π^δ invariant, so the map $\pi^\delta \colon C^\delta \to \mathbb{P}^1_k$ is defined over k;*
(c) *The map π^δ is a covering map with Galois group generated by the automorphisms $\tau_i \colon C^\delta \to C^\delta$ defined by $Z_i \to -Z_i$ for each $i \in \{1, \dots, 2n+1\}$; and*
(d) *We have that $\deg \pi^\delta = 2^{2n}$, that $\#(\pi^\delta)^{-1}(\theta_i) = 2^{2n-1}$, and that $\#(\pi^\delta)^{-1}(\alpha) = 2^{2n}$ for each $\alpha \in \mathbb{P}^1_k(k_{\mathrm{sep}}) \smallsetminus \{\theta_1, \dots, \theta_{2n+1}\}$.*

We now demonstrate that the map π^δ can actually be thought of as a 2-covering $\pi^\delta \colon C^\delta \to \mathcal{S}_F$.

Proposition 35. *For any $\delta \in (K_F^\times / K_F^{\times 2})_{\mathrm{N}\equiv 1}$, the map π^δ factors through the coarse moduli map $\mathcal{S}_F \to \mathbb{P}^1_k$ to give a 2-covering $\pi^\delta \colon C^\delta \to \mathcal{S}_F$.*

Proof. Recall that a finite étale cover of $\mathcal{S}_F$ is the pullback via $\mathcal{S}_F \to \mathbb{P}^1_k$ of a finite cover of its coarse moduli space $\mathbb{P}^1_k$ that is ramified with ramification index 2 at every point in the preimage of $\theta_i \in \mathbb{P}^1_k(k_{\mathrm{sep}})$ for each i (to account for the fact that $\mathcal{S}_F$ has a $\frac{1}{2}$-point at each θ_i) and unramified everywhere else. It follows from part (d) of Theorem 34 that the branch locus of the map π^δ consists precisely of the points θ_i and that each point in $(\pi^\delta)^{-1}(\theta_i)$ has ramification index 2. Thus, the map π^δ factors through the stacky curve $\mathcal{S}_F$, giving an étale map $\pi^\delta \colon C^\delta \to \mathcal{S}_F$.

By parts (b) and (c) of Theorem 34, to prove that π^δ is a 2-covering of $\mathcal{S}_F$ over k, it suffices to show that the group generated by the automorphisms τ_i is isomorphic to $\mathrm{Pic}^0(\mathcal{S}_F)$ as G_k-modules. Let J denote the Jacobian of the monic odd-degree hyperelliptic curve $y^2 = F_{\mathrm{mon}}(x, 1)$. We claim that the map $\tau_i \mapsto (\theta_i - \infty) \in J[2](k_{\mathrm{sep}})$ defines a G_k-equivariant isomorphism of groups. To see why this claim holds, note that the group generated by the automorphisms τ_i is isomorphic to

$$(\mathbb{Z}/2\mathbb{Z})\langle \tau_1, \dots, \tau_{2n+1} \rangle \Big/ \left(\prod_{i=1}^{2n+1} \tau_i = 1 \right)$$

and the action of $\sigma \in G_k$ on τ_i is given by $\sigma \cdot \tau_i = \tau_{\sigma^{-1}(i)}$, because the action of σ on Z_i is defined to be $\sigma(Z_i) = Z_{\sigma(i)}$. On the other hand, we have that

$$J[2](k_{\mathrm{sep}}) = (\mathbb{Z}/2\mathbb{Z})\langle (\theta_1 - \infty), \dots, (\theta_{2n+1} - \infty) \rangle \Big/ \left(\sum_{i=1}^{2n+1} (\theta_i - \infty) \right)$$

and the action of $\sigma \in G_k$ on $(\theta_i - \infty)$ is $(\theta_i - \infty)\cdot\sigma = (\sigma^{-1}\cdot\theta_i - \sigma^{-1}\cdot\infty) = (\theta_{\sigma^{-1}(i)} - \infty)$. Thus, we have the claim. The proposition now follows from the fact that $J[2] \simeq \mathrm{Pic}^0(\mathcal{S}_F)$ as G_k-modules (see the proof of Proposition 7). □

Remark 36. Note that two coverings $\pi^{\delta_1}\colon C^{\delta_1} \to \mathcal{S}_F$ and $\pi^{\delta_2}\colon C^{\delta_2} \to \mathcal{S}_F$ are isomorphic (as coverings of $\mathcal{S}_F$ defined over k) if and only if δ_1 and δ_2 represent the same class in $(K_F^\times/K_F^{\times 2})_{\mathrm{N}\equiv 1}$.

Let $(x_0, y_0, z_0) \in \mathcal{S}_F(k)$, and let $\delta \in K_F^\times$ be the element associated to the point (x_0, y_0, z_0) via the construction in §3. By (15), we have that

$$\delta = \begin{cases} x_0 - \theta z_0 & \text{if } y_0 \neq 0, \\ \widetilde{F}(z_0\theta, z_0) + (x_0 - \theta z_0) & \text{if } y_0 = 0 \end{cases}$$

where $\widetilde{F}$ is as in (11). With this notation, we have the following result, which tells us which 2-covering of $\mathcal{S}_F$ has the property that (x_0, y_0, z_0) lies in the image of its k-rational points:

Lemma 37. *We have that* $(x_0, y_0, z_0) \in \pi^{f_0\cdot\delta}(C^{f_0\cdot\delta}(k)) \subset \mathcal{S}_F(k)$.

Proof. First suppose $y_0 \neq 0$. By construction, the point $[1 : 1 : \cdots : 1] \in C^{f_0\cdot\delta}(k)$ satisfies

$$\pi^{f_0\cdot\delta}([1:1:\cdots:1]) = \frac{\theta_j(f_0\cdot\delta_i) - \theta_i(f_0\cdot\delta_j)}{f_0\cdot\delta_i - f_0\cdot\delta_j} = \frac{\theta_j\cdot f_0(x_0 - \theta_i z_0) - \theta_i\cdot f_0(x_0 - \theta_j z_0)}{f_0(x_0 - \theta_i z_0) - f_0(x_0 - \theta_j z_0)} = [x_0 : z_0] \in \mathbb{P}^1_k(k) = \mathcal{S}_F(k). \tag{76}$$

Now suppose $y_0 = 0$. Then one readily checks that the calculation in (76) goes through by replacing $[1 : 1 : \cdots : 1]$ with the point $[0 : 1 : 1 : \cdots : 1] \in C^{f_0\cdot\delta}(k)$. □

We have thus completed our description of the 2-coverings of $\mathcal{S}_F$. The 2-coverings of $\widetilde{S}_F$ are precisely the pullbacks of the coverings $\pi^\delta\colon C^\delta \to \mathcal{S}_F$ via the quotient map $\widetilde{S}_F \to \mathcal{S}_F$.

6.3. **Proof of Theorem 2.** Let $F \in \mathscr{F}_{2n+1}(f_0)$ be irreducible, let $\delta \in (K_F^\times/K_F^{\times 2})_{\mathrm{N}\equiv 1}$, and consider the associated 2-covering $\pi^\delta\colon C^\delta \to \mathcal{S}_F$ over $\mathbb{Q}$. We say that the 2-covering π^δ is *locally soluble* if for every place v of $\mathbb{Q}$, there exists a point $P_v \in \mathcal{S}_F(\mathbb{Z}_v)$ such that the number δ_v associated to P_v via (15) is such that $f_0\cdot\delta_v$ is equal to the image of δ under the natural map $(K_F^\times/K_F^{\times 2})_{\mathrm{N}\equiv 1} \to ((K_F\otimes_{\mathbb{Q}}\mathbb{Q}_v)^\times/(K_F\otimes_{\mathbb{Q}}\mathbb{Q}_v)^{\times 2})_{\mathrm{N}\equiv 1}$. (Notice that in this situation, $P_v \in \pi^\delta(C^\delta(\mathbb{Q}_v))$ by Lemma 37.) Just as Bruin and Stoll did for hyperelliptic curves in [BS09, §2], we define the *fake* 2*-Selmer set* $\mathrm{Sel}^2_{\mathrm{fake}}(\mathcal{S}_F) \subset (K_F^\times/K_F^{\times 2})_{\mathrm{N}\equiv 1}$ to be the set of locally soluble 2-coverings of $\mathcal{S}_F$.

We claim that each element $\delta \in \mathrm{Sel}^2_{\mathrm{fake}}(\mathcal{S}_F)$ gives rise to an orbit of $G(\mathbb{Z})$ on $V(\mathbb{Z})$, the associated $G(\mathbb{Q})$-orbit of which is represented by the class $\delta \in (K_F^\times/K_F^{\times 2})_{\mathrm{N}\equiv 1}$. For each place v, let $P_v \in \mathcal{S}_F(\mathbb{Z}_v) \cap \pi^\delta(C^\delta(\mathbb{Q}_v))$. Then via the construction in §3, P_v naturally gives rise to an orbit of $G(\mathbb{Z}_v)$ on $V(\mathbb{Z}_v)$, the associated $G(\mathbb{Q}_v)$-orbit of which is represented by the class $\delta \in ((K_F\otimes_{\mathbb{Q}}\mathbb{Q}_v)^\times/(K_F\otimes_{\mathbb{Q}}\mathbb{Q}_v)^{\times 2})_{\mathrm{N}\equiv 1}$. Since the algebraic group G has class number equal to 1, and since the orbit of $G(\mathbb{Q}_v)$ on $V(\mathbb{Q}_v)$ associated to δ has a representative over $\mathbb{Z}_v$ for every place v, it follows that the orbit of $G(\mathbb{Q})$ on $V(\mathbb{Q})$ has representative over $\mathbb{Z}$. Thus, we have the claim.

In the next lemma, we relate the fake 2-Selmer set to the Brauer–Manin obstruction:

Lemma 38. *If* $\mathrm{Sel}^2_{\mathrm{fake}}(\mathcal{S}_F) = \varnothing$*, then* $\mathcal{S}_F$ *has a Brauer–Manin obstruction to having a* $\mathbb{Z}$*-point.*

Proof. Let $\pi\colon C \to \widetilde{S}_{F,\mathbb{Q}}$ be any 2-covering. We have by (72), (73), (74), and (75) that

$$\mathcal{S}_F(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \subset \widetilde{S}_F(\mathbb{A}_{\mathbb{Q}})^{\mathrm{int}} \cap \widetilde{S}_{F,\mathbb{Q}}(\mathbb{A}_{\mathbb{Q}})^{\pi} = \left(\prod_v \mathcal{S}_F(\mathbb{Z}_v)\right) \cap \left(\bigcup_{\delta\in H^1(G_{\mathbb{Q}},\mathrm{Pic}^0(\mathcal{S}_F)(\overline{\mathbb{Q}}))} \pi^\delta(C^\delta(\mathbb{A}_{\mathbb{Q}}))\right)$$
$$\subset \bigcup_{\delta\in\mathrm{Sel}^2_{\mathrm{fake}}(\mathcal{S}_F)} \pi^\delta(C^\delta(\mathbb{A}_{\mathbb{Q}})),$$

and clearly the last union above is empty if $\mathrm{Sel}^2_{\mathrm{fake}}(\mathcal{S}_F) = \varnothing$. □

In proving Theorem 1, we imposed local conditions on $V(\mathbb{Z})$ to sieve to the orbits that arise from local points at each place. By definition, the exact same local conditions define orbits that arise from elements of fake 2-Selmer sets. Moreover, if $F \in \mathscr{F}_{2n+1}(f_0) \smallsetminus \mathscr{F}^*_{2n+1}(f_0)$, Theorem 14 implies that the distinguished covering is not everywhere locally soluble. Thus, by the argument in §5, we have the following result:

Theorem 39. *The upper density of forms $F \in \mathscr{F}_{2n+1}(f_0)$ such that $\mathrm{Sel}^2_{\mathrm{fake}}(\mathcal{S}_F) \neq \varnothing$ is at most $\mu_{f_0} + o(2^{-n})$ when $2 \nmid f_0$ and at most $\mu_{f_0} + O(2^{-\varepsilon_1 n^{\varepsilon_2}})$ for some $\varepsilon_1, \varepsilon_2 > 0$ when $2 \mid f_0$.*

To prove Theorem 2, it remains to determine how often it is that the stacky curves $\mathcal{S}_F$ have integral points everywhere locally. We do so as follows:

Lemma 40. *The density of forms $F \in \mathscr{F}_{2n+1}(f_0)$ such that $\mathcal{S}_F(\mathbb{Z}_v) \neq \varnothing$ for every place v is at least $\mu'_{f_0} + O(2^{-2n})$.*

Proof. By (1), we always have $\mathcal{S}_F(\mathbb{R}) \neq \varnothing$. If there is no prime $p \mid \kappa$ such that $F(x_0, z_0) = 0$ for every $[x_0 : z_0] \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, then for any prime $p \mid \kappa$, there exists a pair $(x_0, z_0) \in \mathbb{Z}^2$ such that $\gcd(x_0, z_0) = \gcd(F(x_0, z_0), p) = 1$, so $(x_0 \cdot F(x_0, z_0), F(x_0, z_0)^{n+1}, z_0 \cdot F(x_0, z_0)) \in \mathcal{S}_F(\mathbb{Z}_p)$. On the other hand, if $p \mid \kappa$ and the mod-p reduction of F has a simple zero at some point of $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$, then $\mathcal{S}_F$ has a Weierstrass point over $\mathbb{Z}_p$ and is thus soluble. Moreover, for any prime p such that $p \nmid \kappa$ but $p \mid f_0$, we have $(\kappa, f_0^{\frac{1}{2}} \kappa^{\frac{2n+1}{2}}, 0) \in \mathcal{S}_F(\mathbb{Z}_p)$, and for any prime $p \nmid f_0$, we have $(f_0, f_0^{n+1}, 0) \in \mathcal{S}_F(\mathbb{Z}_p)$.

If $p \mid \kappa$, the p-adic density of forms $F \in \mathscr{F}_{2n+1}(f_0)$ such that the mod-p reduction of F has a zero of multiplicity greater than 1 at each point of $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$ is p^{-2p-1} if $2p + 2 < 2n + 1$ and p^{-2n-1} otherwise. Thus, the density of forms $F \in \mathscr{F}_{2n+1}(f_0)$ such that $\mathcal{S}_F(\mathbb{Z}_v) \neq \varnothing$ for every place v is at least $\prod_{p \mid \kappa}(1 - p^{-2p-1} - p^{-2n-1}) = \mu'_{f_0} + O(2^{-2n})$. □

It follows from Theorem 39 and Lemma 40 that for all sufficiently large n, a positive proportion of $F \in \mathscr{F}_{2n+1}(f_0)$ are such that $\mathrm{Sel}^2_{\mathrm{fake}}(\mathcal{S}_F) = \varnothing$ and $\mathcal{S}_F(\mathbb{Z}_v) \neq \varnothing$ for every place v. Indeed,

$$(1 - \mu_{f_0}) + (\mu'_{f_0} + O(2^{-2n})) = 1 - \prod_{p \mid \kappa} \frac{1}{p^2} + \prod_{p \mid \kappa} \left(1 - \frac{1}{p^{2p+1}}\right) + O(2^{-n}),$$

which is clearly greater than 1 for every sufficiently large n. Theorem 2 now follows from Lemma 38.

Acknowledgments

It is a pleasure to thank Manjul Bhargava for suggesting the questions that led to this paper and for providing invaluable advice and encouragement. We are immensely grateful to Nils Bruin, Sungmun Cho, Benedict Gross, Bjorn Poonen, Peter Sarnak, Arul Shankar, Michael Stoll, David Zureick-Brown, and Jerry Wang for answering our questions and for sharing their insights. We also thank Levent Alpöge, Joe Harris, Aaron Landesman, Daniel Loughran, Anand Patel, Beth Romano, Efthymios Sofos, James Tao, and Melanie Wood for helpful discussions.

References

[ABZ07] A. Ash, J. Brakenhoff, and T. Zarrabi. Equality of polynomial and field discriminants. *Experiment. Math.*, 16(3):367–374, 2007.

[AP19] A. Afshar and S. Porritt. The function field Sathe-Selberg formula in arithmetic progressions and 'short intervals'. *Acta Arith.*, 187(2):101–124, 2019.

[BF05] N. R. Bruin and E. V. Flynn. Towers of 2-covers of hyperelliptic curves. *Trans. Amer. Math. Soc.*, 357(11):4329–4347, 2005.

[BG13] M. Bhargava and B. H. Gross. The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point. In *Automorphic representations and L-functions*, volume 22 of *Tata Inst. Fundam. Res. Stud. Math.*, pages 23–91. Tata Inst. Fund. Res., Mumbai, 2013.

[Bha13] M. Bhargava. Most hyperelliptic curves over $\mathbb{Q}$ have no rational points. *arXiv preprint arXiv:1308.0395*, 2013.

[BM72] B. J. Birch and J. R. Merriman. Finiteness theorems for binary forms with given discriminant. *Proc. London Math. Soc. (3)*, 24:385–394, 1972.

[Bou75] N. Bourbaki. *Éléments de mathématique. Fasc. XXXVIII: Groupes et algèbres de Lie. Chapitre VII: Sous-algèbres de Cartan, éléments réguliers. Chapitre VIII: Algèbres de Lie semi-simples déployées*. Actualités Scientifiques et Industrielles, No. 1364. Hermann, Paris, 1975.

[BP19] M. Bhargava and B. Poonen. The local-global principle for stacky curves. *arXiv preprint arXiv:2006.00167*, 2019.

[Bru02] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

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

[BS15] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math. (2)*, 181(1):191–242, 2015.

[BSS21] M. Bhargava, A. Shankar, and A. Swaminathan. The second moment of the size of the 2-Selmer group of elliptic curves. *arXiv preprint arXiv:2110.09063*, 2021.

[Car32] L. Carlitz. The arithmetic of polynomials in a Galois field. *Amer. J. Math.*, 54(1):39–50, 1932.

[Car82] M. Car. Factorisation dans $F_q[X]$. *C. R. Acad. Sci. Paris Sér. I Math.*, 294(4):147–150, 1982.

[Cas83] J. W. S. Cassels. The Mordell-Weil group of curves of genus 2. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 27–60. Birkhäuser, Boston, Mass., 1983.

[CC17] L. Candelori and F. Cameron. Vector bundles and modular forms for Fuchsian groups of genus zero. *arXiv preprint arXiv:1704.01684*, 2017.

[CDX19] Y. Cao, C. Demarche, and F. Xu. Comparing descent obstruction and Brauer-Manin obstruction for open varieties. *Trans. Amer. Math. Soc.*, 371(12):8625–8650, 2019.

[Cho15] S. Cho. Group schemes and local densities of quadratic lattices in residue characteristic 2. *Compos. Math.*, 151(5):793–827, 2015.

[CS88] J. H. Conway and N. J. A. Sloane. Low-dimensional lattices. IV. The mass formula. *Proc. Roy. Soc. London Ser. A*, 419(1857):259–286, 1988.

[Dar97] H. Darmon. Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation. *C. R. Math. Rep. Acad. Sci. Canada*, 19(1):3–14, 1997.

[DG95] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[DPSZ02] A. Dembo, B. Poonen, Q.-M. Shao, and O. Zeitouni. Random polynomials having few or no real zeros. *J. Amer. Math. Soc.*, 15(4):857–892, 2002.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[Jon44] B. W. Jones. A canonical quadratic form for the ring of 2-adic integers. *Duke Math. J.*, 11:715–727, 1944.

[Kit93] Y. Kitaoka. *Arithmetic of quadratic forms*, volume 106 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1993.

[Lag21] J. Laga. The average size of the 2-selmer group of a family of non-hyperelliptic curves of genus 3. *arXiv preprint arXiv:2008.13158*, 2021.

[Lan66] R. P. Langlands. The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 143–148. Amer. Math. Soc., Providence, R.I., 1966.

[LP20] A. Lei and A. Poulin. On certain probabilistic properties of polynomials over the ring of p-adic integers. *Amer. Math. Monthly*, 127(6):519–529, 2020.

[MH73] J. Milnor and D. Husemoller. *Symmetric bilinear forms*. Springer-Verlag, New York-Heidelberg, 1973. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73.

[Nak89] J. Nakagawa. Binary forms and orders of algebraic number fields. *Invent. Math.*, 97(2):219–235, 1989.

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

[Rei56] I. Reiner. On the two-adic density of representations by quadratic forms. *Pacific J. Math.*, 6:753–762, 1956.

[Rei72] M. Reid. *The complete intersection of two or more quadratics*. PhD thesis, University of Cambridge, 1972.

[RT18] B. Romano and J. A. Thorne. On the arithmetic of simple singularities of type E. *Res. Number Theory*, 4(2):Paper No. 21, 34, 2018.

[RT21] B. Romano and J. A. Thorne. E_8 and the average size of the 3-Selmer group of the Jacobian of a pointed genus-2 curve. *Proc. Lond. Math. Soc. (3)*, 122(5):678–723, 2021.

[Ser73] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[Sim08] D. Simon. A "class group" obstruction for the equation $Cy^d = F(x, z)$. *J. Théor. Nombres Bordeaux*, 20(3):811–828, 2008.

[SSSV21] A. Shankar, A. Siad, A. Swaminathan, and I. Varma. Geometry-of-numbers methods in the cusp and applications to class groups. *arXiv preprint arXiv:2110.09466*, 2021.

[SW18] A. Shankar and X. Wang. Rational points on hyperelliptic curves having a marked non-Weierstrass point. *Compos. Math.*, 154(1):188–222, 2018.

[Swa21] A. Swaminathan. Average 2-torsion in class groups of rings associated to binary n-ic forms. *arXiv preprint arXiv:2011.13578*, 2021.

[Tho15] J. A. Thorne. E_6 and the arithmetic of a family of non-hyperelliptic curves of genus 3. *Forum Math. Pi*, 3:e1, 41, 2015.

[Wan18] X. Wang. Maximal linear spaces contained in the based loci of pencils of quadrics. *Algebr. Geom.*, 5(3):359–397, 2018.

[Woo11] M. M. Wood. Rings and ideals parameterized by binary n-ic forms. *J. Lond. Math. Soc. (2)*, 83(1):208–231, 2011.

[Woo14] M. M. Wood. Parametrization of ideal classes in rings associated to binary forms. *J. Reine Angew. Math.*, 689:169–199, 2014.

A. A. Swaminathan ashvins@math.princeton.edu
Department of Mathematics, Princeton University, Princeton, NJ 08544, USA