ODD DEGREE NUMBER FIELDS WITH ODD CLASS NUMBER

WEI HO, ARUL SHANKAR, and ILA VARMA

Abstract

For every odd integer $n \geq 3$, we prove that there exist infinitely many number fields of degree n and associated Galois group S_n whose class number is odd. To do so, we study the class groups of families of number fields of degree n whose rings of integers arise as the coordinate rings of the subschemes of $\mathbb{P}^1$ cut out by integral binary n-ic forms. By obtaining upper bounds on the mean number of 2-torsion elements in the class groups of fields in these families, we prove that a positive proportion (tending to 1 as n tends to ∞) of such fields have trivial 2-torsion subgroups in their class groups and narrow class groups. Conditional on a tail estimate, we also prove the corresponding lower bounds and obtain the exact values of these averages, which are consistent with the heuristics of Cohen and Lenstra, Cohen and Martinet, Malle, and Dummit and Voight. Additionally, for any order $\mathcal{O}_f$ of degree n arising from an integral binary n-ic form f, we compare the sizes of $\mathrm{Cl}_2(\mathcal{O}_f)$, the 2-torsion subgroup of ideal classes in $\mathcal{O}_f$, and of $\mathcal{I}_2(\mathcal{O}_f)$, the 2-torsion subgroup of ideals in $\mathcal{O}_f$. For the family of orders arising from integral binary n-ic forms and contained in fields with fixed signature (r_1, r_2), we prove that the mean value of the difference $|\mathrm{Cl}_2(\mathcal{O}_f)| - 2^{1-r_1-r_2}|\mathcal{I}_2(\mathcal{O}_f)|$ is equal to 1, generalizing a result of Bhargava and the third-named author for cubic fields. Conditional on certain tail estimates, we also prove that the mean value of $|\mathrm{Cl}_2(\mathcal{O}_f)| - 2^{1-r_1-r_2}|\mathcal{I}_2(\mathcal{O}_f)|$ remains 1 for certain families obtained by imposing local splitting and maximality conditions.

Contents

DUKE MATHEMATICAL JOURNAL
Vol. 167, No. 5, © 2018 DOI 10.1215/00127094-2017-0050
Received 5 December 2016. Revision received 11 August 2017.
First published online 3 March 2018.
2010 *Mathematics Subject Classification*. Primary 11R29; Secondary 11R45.

1. Introduction

The Cohen–Lenstra heuristics (see [16]) give precise predictions for the distribution of ideal class groups in families of quadratic fields. Very few cases of these conjectures have been proved; among them are the celebrated results of Davenport and Heilbronn [19] on the average number of 3-torsion elements in the class groups of quadratic fields, and the results of Fouvry and Klüners [21] on the 4-ranks of the class groups of quadratic fields. These heuristics were generalized by Cohen and Martinet [17] to describe the distribution of ideal class groups in families of number fields of fixed degree over a fixed base field. In 2010, Malle [28] proposed a modification of the Cohen–Martinet heuristics to account for observed variations in the asymptotic behavior of the p-part of the class groups of families over a base field containing the pth roots of unity. For example, for $p = 2$ and odd n, the modified heuristics yield the following predictions on the mean number of 2-torsion ideal classes in degree n S_n-number fields over $\mathbb{Q}$ with signature (r_1, r_2), that is, number fields with r_1 real embeddings and r_2 pairs of conjugate complex embeddings, and whose normal closure over $\mathbb{Q}$ has Galois group S_n.

CONJECTURE 1 (Cohen–Lenstra–Martinet–Malle)
Fix an odd integer $n \geq 3$ and a pair of nonnegative integers (r_1, r_2) such that $r_1 + 2r_2 = n$. Consider the set of isomorphism classes of degree n S_n-number fields with signature (r_1, r_2). The average number of 2-torsion elements in the ideal class groups of such fields is

$$1 + 2^{1-r_1-r_2} \tag{1}$$

when these fields are ordered by discriminant.

The only proven cases of the above conjecture are when $n = 3$, due to Bhargava [2, Theorem 5]. In this article, we provide evidence toward *all* cases of Conjecture 1 by computing the average size of the 2-torsion subgroups of ideal class groups of certain infinite families of number fields of fixed odd degree n; even though we do not average over the family of all number fields of a given signature ordered by discriminant, the mean values coincide with (1), conditional on a certain tail estimate. Unconditionally, we prove that an infinite number of odd degree n S_n-fields with signature (r_1, r_2) have odd class number. We also compute the average size of the 2-torsion subgroup of the *narrow* class groups of the same infinite families, which allows us to give analogues of the Cohen–Lenstra–Martinet–Malle heuristics predicting the asymptotic behavior of the narrow class groups in families of number fields of fixed odd degree and signature.

In order to state our results more precisely, we first describe the families of number fields we study, which arise from families of integral binary n-ic forms. Given an integer $n \geq 3$, to a nonzero integral binary n-ic form $f \in \mathrm{Sym}_n(\mathbb{Z}^2)$, we may naturally associate the coordinate ring R_f of the subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ cut out by f (see Nakagawa [29] and Wood [38]). Define the family $\mathfrak{R}_H$ to be the multiset of rings

$$\mathfrak{R}_H = \{R_f \mid f \in \mathrm{Sym}_n(\mathbb{Z}^2)\}.$$

There is a *height* ordering on $\mathfrak{R}_H$ arising from the height ordering H on $\mathrm{Sym}_n(\mathbb{Z}^2)$, where $H(f)$ is defined as the maximum absolute value of the coefficients of f. Note that although two rings in $\mathfrak{R}_H$ may be isomorphic, their heights need not be equal. For example, if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, and we define the action $\gamma f(x, y) := f((x, y)\gamma)$ on the space of integral binary n-ic forms, then it is always true that $R_f \cong R_{\gamma f}$, but it is not in general true that $H(f) = H(\gamma f)$. Nevertheless, there is a well-defined isomorphism class of rings $R_{[f]}$ associated to an $\mathrm{SL}_2(\mathbb{Z})$-orbit $[f] \in \mathrm{SL}_2(\mathbb{Z})\backslash \mathrm{Sym}_n(\mathbb{Z}^2)$ since $R_{[f]}$ is isomorphic to R_g if and only if $g = \gamma f$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Such orbits $[f]$ may be ordered by their *Julia invariant*, which is an invariant defined in [27] for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathrm{Sym}_n(\mathbb{Z}^2)$ (see Section 3.3 for details). Thus, we also define the family $\mathfrak{R}_J$ to be the multiset of rings

$$\mathfrak{R}_J = \{R_{[f]} \mid [f] \in \mathrm{SL}_2(\mathbb{Z})\backslash \mathrm{Sym}_n(\mathbb{Z}^2)\},$$

ordered by Julia invariant J, where $J(R_{[f]}) := J([f])$. Asymptotics on the size of $\mathfrak{R}_J$ were obtained by Bhargava and Yang [13].

In this article, we compute averages taken over certain families contained in $\mathfrak{R}_H$ or $\mathfrak{R}_J$. Let $\mathfrak{R}_H^{r_1,r_2} \subset \mathfrak{R}_H$ and $\mathfrak{R}_J^{r_1,r_2} \subset \mathfrak{R}_J$ be the respective subfamilies consisting of all Gorenstein[1] integral domains whose fraction field has signature (r_1, r_2), that is, has r_1 real embeddings and r_2 pairs of conjugate complex embeddings. Also, let $\mathfrak{R}_{H,\max}^{r_1,r_2} \subset \mathfrak{R}_H^{r_1,r_2}$ (resp., $\mathfrak{R}_{J,\max}^{r_1,r_2} \subset \mathfrak{R}_J^{r_1,r_2}$) be the subfamily containing all maximal orders. It is worthwhile to note that a given order $\mathcal{O}$ in a number field with signature (r_1, r_2) may occur in $\mathfrak{R}_H^{r_1,r_2}$ or $\mathfrak{R}_{H,\max}^{r_1,r_2}$ an infinite number of times (up to isomorphism) but only occurs with finite multiplicity in $\mathfrak{R}_J^{r_1,r_2}$ or $\mathfrak{R}_{J,\max}^{r_1,r_2}$ by a result of Birch and Merriman [14, Theorem 2].

[1]From [38, Proposition 2.1, Corollary 2.3] it follows that the ring R_f is Gorenstein if and only if f is *primitive*, that is, the coefficients of f do not share any common prime factors.

For any subfamilies $\Sigma_H \subseteq \mathfrak{R}_H^{r_1,r_2}$ and $\Sigma_J \subseteq \mathfrak{R}_J^{r_1,r_2}$, we denote the average number of 2-torsion elements of ideal class groups over Σ_H ordered by height and over Σ_J ordered by Julia invariant as follows:

$$\begin{aligned}
\mathrm{Avg}_H(\Sigma_H, \mathrm{Cl}_2) &= \lim_{X\to\infty} \frac{\sum_{\substack{R_f\in\Sigma_H\\ |H(f)|<X}} |\mathrm{Cl}_2(R_f)|}{\sum_{\substack{R_f\in\Sigma_H\\ |H(f)|<X}} 1}, \\
\mathrm{Avg}_J(\Sigma_J, \mathrm{Cl}_2) &= \lim_{X\to\infty} \frac{\sum_{\substack{R_{[f]}\in\Sigma_J\\ |J(f)|<X}} |\mathrm{Cl}_2(R_f)|}{\sum_{\substack{R_{[f]}\in\Sigma_J\\ |J(f)|<X}} 1},
\end{aligned} \tag{2}$$

where $\mathrm{Cl}_2(R_f)$ denotes the 2-torsion subgroup of the ideal class group of R_f. Additionally, we can replace $\mathrm{Cl}_2(R_f)$ with the 2-torsion subgroup $\mathrm{Cl}_2^+(R_f)$ of the *narrow* class group of R_f in the right-hand sides of the equalities in (2); we denote these means by $\mathrm{Avg}_H(\Sigma_H, \mathrm{Cl}_2^+)$ and $\mathrm{Avg}_J(\Sigma_J, \mathrm{Cl}_2^+)$, respectively. The notation $\mathrm{Avg}_*(*, *) \leq c$ will be used to indicate that the limsups of fractions as in (2) are bounded by c. We then have the following theorem.

THEOREM 2

Fix an odd integer $n > 3$ and a corresponding signature (r_1, r_2). Then we have

(a) $\mathrm{Avg}_H(\mathfrak{R}_{H,\max}^{r_1,r_2}, \mathrm{Cl}_2) \leq 1 + 2^{1-r_1-r_2}$ *and* $\mathrm{Avg}_J(\mathfrak{R}_{J,\max}^{r_1,r_2}, \mathrm{Cl}_2) \leq 1 + 2^{1-r_1-r_2}$, *and*

(b) $\mathrm{Avg}_H(\mathfrak{R}_{H,\max}^{r_1,r_2}, \mathrm{Cl}_2^+) \leq 1 + 2^{-r_2}$ *and* $\mathrm{Avg}_J(\mathfrak{R}_{J,\max}^{r_1,r_2}, \mathrm{Cl}_2^+) \leq 1 + 2^{-r_2}$.

If the tail estimates in (33) hold, then both (a) and (b) are equalities. Additionally, the same upper bounds (and conditional equalities) hold when further imposing any finite set of local conditions on the fields in $\mathfrak{R}_{H,\max}^{r_1,r_2}$ and $\mathfrak{R}_{J,\max}^{r_1,r_2}$.

When $n = 3$, the Julia invariant of a ring R_f associated to a binary cubic form f coincides with its discriminant, and the family $\mathfrak{R}_J$ is essentially the same as the family of all cubic rings ordered by discriminant. The mean size of the 2-torsion subgroup of class groups of totally real (resp., complex) cubic fields ordered by discriminant was determined to be $5/4$ (resp., $3/2$) in [2], confirming Conjecture 1 for $n = 3$. Additionally, the average number of 2-torsion elements in the narrow class groups of totally real cubic fields ordered by discriminant is 2, which was proved by Bhargava and the third-named author [11]. On the other hand, even though the family $\mathfrak{R}_H$ also contains all cubic rings, each such ring occurs infinitely often. Nevertheless, we determine that the average number of 2-torsion elements in class groups and narrow class groups of cubic fields ordered by height coincides with the analogous results in [2] and [11] when ordering by discriminant.

THEOREM 3

We have

(a) $\mathrm{Avg}_H(\mathfrak{R}^{3,0}_{H,\max}, \mathrm{Cl}_2) = 5/4$,

(b) $\mathrm{Avg}_H(\mathfrak{R}^{1,1}_{H,\max}, \mathrm{Cl}_2) = 3/2$,

(c) $\mathrm{Avg}_H(\mathfrak{R}^{3,0}_{H,\max}, \mathrm{Cl}_2^+) = 2$.

In conjunction with [11, Theorem 1], Theorem 3 gives evidence that the Cohen–Lenstra–Martinet–Malle heuristics may hold for any natural ordering of fields, as they hold when ordering by either discriminant or height. Additionally, Theorem 2(b) gives evidence toward the prediction that the average number of 2-torsion elements in the narrow class groups of *all* isomorphism classes of odd degree number fields with fixed signature (r_1, r_2) is equal to

$$1 + 2^{-r_2}, \tag{3}$$

which additionally coincides with heuristics formulated by Dummit and Voight [20].

Theorems 2 and 3 immediately imply that most fields within these families have no nontrivial 2-torsion elements in their class groups. By applying results of [14], we may quantify the number of such fields, even while allowing arbitrary splitting conditions at a finite set of primes.

THEOREM 4

Fix an odd integer $n \geq 3$ and a corresponding signature (r_1, r_2). Let S be a finite set of primes and for each prime $p \in S$, fix a degree n étale extension M_p of $\mathbb{Q}_p$.

(a) *There are an infinite number of degree n S_n-fields K with signature (r_1, r_2) such that $K \otimes \mathbb{Q}_p = M_p$ for each $p \in S$, and K has odd class number. More precisely,*

$$\#\{K : |\mathrm{Disc}(K)| < X \text{ and } 2 \nmid |\mathrm{Cl}(K)|\} \gg X^{\frac{n+1}{2n-2}},$$

where the implied constants depend on n and S.

(b) *If $r_2 \geq 1$, then there are an infinite number of degree n S_n-fields L with signature (r_1, r_2) such that $L \otimes \mathbb{Q}_p = M_p$ for each $p \in S$, and L has odd narrow class number. More precisely,*

$$\#\{L : |\mathrm{Disc}(L)| < X \text{ and } 2 \nmid |\mathrm{Cl}^+(L)|\} \gg X^{\frac{n+1}{2n-2}},$$

where the implied constants depend on n and S.

Such results on the infinitude of fields with odd class number originate with Gauss [22], who proved using genus theory that the set of quadratic fields with class number indivisible by 2 are exactly the quadratic fields with prime discriminant. The first generalization of Gauss's result to the indivisibility of class numbers of quadratic fields by odd primes p arises as applications of the aforementioned results of Davenport and Heilbronn [19], which imply that at least half of imaginary quadratic fields and at least $5/6$ of real quadratic fields have class number indivisible by 3 when such fields are ordered by discriminant. Nakagawa and Horie [30] refined the proof of [19] to show that even after imposing certain congruence conditions at a finite set of primes, the number of such quadratic fields with class number indivisible by 3 remains infinite; this strengthening implies results such as the existence of infinitely many hyperelliptic curves over $\mathbb{Q}$ of a given genus with no integral points. Finally, the results of Bhargava and the third-named author [12] imply that one can find an infinite number of quadratic fields with class number indivisible by 3 and satisfying *any* (nonempty) local specifications at a finite set of primes.

In the imaginary quadratic case, Hartung [23] gave another proof of the infinitude of fields with class number indivisible by 3 using Kronecker–Weber relations. In conjunction with trace formula methods, Horie in [24] and [25] extended these results to determine that for all sufficiently large primes p, there exist infinitely many imaginary quadratic fields with class number indivisible by p and satisfying prescribed splitting and ramification conditions at a finite set of (odd) primes. Using the indivisibility of coefficients of modular forms of half-integer weight, Bruinier [15] and Ono and Skinner [31] strengthened the result to include most primes $p \geq 5$ and a wider class of local specifications that could be imposed at a finite number of primes. Jochnowitz [26] also used such methods to generalize the results of [23], [24], and [25] to the real quadratic case. The most general result was obtained by Wiles [37] and Beckwith [1] using trace formula methods in conjunction with the geometry of Shimura curves and the theory of mock modular forms of half-integer weight, respectively. Applications of such results include unconditional versions of modularity lifting theorems in the residually reducible case (see [33]) as well as the nonvanishing of certain L-values associated to elliptic curves with rational torsion points (see [35]).

Beyond the case of quadratic fields, the only known result of this nature is [11, Corollary 3], which implies that the majority of cubic fields (of any signature) have odd class number. Theorem 4 is the first of its kind to treat infinite (even multiple) degrees and signatures. Additionally, it immediately implies the following result concerning the narrow class number, which differs from the class number at most by a factor of a power of 2.

COROLLARY 5

Let $n \geq 3$ be an odd integer. If $r_2 \geq 1$, then there are an infinite number of degree n S_n-fields with signature (r_1, r_2) for which the narrow class number equals the class *number. In particular, there are an infinite number of such fields that have units of every signature.*[2]

Our methods are not limited to studying class groups of (maximal orders in) number fields; we also study the ideal class groups of general orders in $\mathfrak{R}_H^{r_1,r_2}$ and $\mathfrak{R}_J^{r_1,r_2}$. Specifically, for each odd $n \geq 3$, we compute on average how many 2-torsion ideal classes in the class groups of such orders arise from nontrivial elements of order 2 in the *ideal groups* of such orders. More precisely, if $\mathcal{O}$ is an order in a number field, let the ideal group $\mathcal{I}(\mathcal{O})$ be the group of invertible fractional ideals of $\mathcal{O}$ (which the class group $\mathrm{Cl}(\mathcal{O})$ is a quotient of). Denote the 2-torsion subgroups of $\mathrm{Cl}(\mathcal{O})$ and $\mathcal{I}(\mathcal{O})$ by $\mathrm{Cl}_2(\mathcal{O})$ and $\mathcal{I}_2(\mathcal{O})$ for any prime p. Although $\mathcal{I}_2(\mathcal{O})$ is trivial for maximal orders $\mathcal{O}$, this is not always true for nonmaximal orders $\mathcal{O}$.

In [11], the mean value of the difference $|\mathrm{Cl}_2(\mathcal{O})| - \frac{1}{2^{1-r_1-r_2}}|\mathcal{I}_2(\mathcal{O})|$ is determined to be 1, when averaging over maximal orders $\mathcal{O}$ in cubic fields of a fixed signature (r_1, r_2), over all orders in such cubic fields, or even over certain acceptable families of orders defined by local conditions (in all cases ordered by discriminant). An analogous result is also known for 3-torsion ideal classes of acceptable families of quadratic orders and fields (see [12]). In this article, we obtain a similar statement for $\mathfrak{R}_J^{r_1,r_2}$ and $\mathfrak{R}_H^{r_1,r_2}$:

THEOREM 6

Fix an odd integer $n \geq 3$ and signature (r_1, r_2).

(a) *The average size of*

$$\left|\mathrm{Cl}_2(\mathcal{O})\right| - \frac{1}{2^{r_1+r_2-1}}\left|\mathcal{I}_2(\mathcal{O})\right|$$

over $\mathcal{O} \in \mathfrak{R}_H^{r_1,r_2}$ ordered by height or over $\mathcal{O} \in \mathfrak{R}_J^{r_1,r_2}$ ordered by Julia invariant is 1.

(b) *The average size of*

$$\left|\mathrm{Cl}_2^+(\mathcal{O})\right| - \frac{1}{2^{r_2}}\left|\mathcal{I}_2(\mathcal{O})\right|$$

over $\mathcal{O} \in \mathfrak{R}_H^{r_1,r_2}$ ordered by height or over $\mathcal{O} \in \mathfrak{R}_J^{r_1,r_2}$ ordered by Julia invariant is 1.

In fact, we prove a much stronger statement indicating that the above averages remain equal to 1 when taken over any *very large* family in $\mathfrak{R}_H^{r_1,r_2}$ or $\mathfrak{R}_J^{r_1,r_2}$ (see Definition 6.1). For any *acceptable* family in $\mathfrak{R}_H^{r_1,r_2}$ or $\mathfrak{R}_J^{r_1,r_2}$ (as defined in Section 3.1),

[2]Recall that for any number field K with r_1 distinct real embeddings, there is a signature homomorphism $\mathcal{O}_K^\times \to \{\pm 1\}^{r_1}$ that takes a unit to its *signature*, that is, to the sign of its image under each real embedding.

the analogous averages are shown to have an upper bound equal to 1; furthermore, conditional on the tail estimates in (33), averages over acceptable families in $\mathfrak{R}_H^{r_1,r_2}$ and $\mathfrak{R}_J^{r_1,r_2}$ also have lower bound equal to 1 (see Theorem 6.2). Some notable acceptable families include $\mathfrak{R}_{H,\max}^{r_1,r_2}$ and $\mathfrak{R}_{J,\max}^{r_1,r_2}$ as well as subfamilies of $\mathfrak{R}_{H,\max}^{r_1,r_2}$ and $\mathfrak{R}_{J,\max}^{r_1,r_2}$ that are defined by local conditions at any finite set of primes.

Our strategy for proving Theorems 2, 3, and 6 uses Wood's parameterization (see [39]) of 2-torsion ideal classes of rings in $\mathfrak{R}_H^{r_1,r_2}$ and $\mathfrak{R}_J^{r_1,r_2}$ by certain integral orbits of the representation $\mathbb{Z}^2 \otimes \mathrm{Sym}^2(\mathbb{Z}^n)$; we then determine asymptotic counts of the relevant orbits using geometry-of-numbers techniques developed by [2], [3], and [9]. However, our geometry-of-numbers arguments are complicated by the fact that we simultaneously consider an infinite set of representations, one for each odd $n \geq 3$, which have increasingly intricate invariant rings. Similar infinite sets have been handled previously in [4], [6], and [7]. An essential ingredient for our result is a sieve that counts binary n-ic forms that correspond to maximal rings (equivalently, degree n fields). For the family of binary n-ic forms ordered by height, this sieve is carried out in [10], and we carry out an analogous sieve for binary n-ic forms ordered by Julia invariant.

When ordering by height, we study the orbits of $\mathrm{SL}_n(\mathbb{Z})$ acting on the space $\mathbb{Z}^2 \otimes \mathrm{Sym}_2(\mathbb{Z}^n)$ of pairs (A, B) of integral n-ary quadratic forms. Each such pair gives rise to an *invariant binary n-ic form*

$$f_{(A,B)}(x, y) := \det(Ax - By)$$

when A and B are viewed as symmetric $n \times n$ matrices. If $R_f \in \mathfrak{R}_H^{r_1,r_2}$ for some signature (r_1, r_2), then certain *projective* $\mathrm{SL}_n(\mathbb{Z})$-orbits of pairs (A, B) with invariant binary n-ic $f_{(A,B)} = f$ are equipped with a composition law coming from the group structure on the 2-torsion subgroup of the class group of R_f. (The notion of projectivity is defined in Section 2.3.) This implies that the number of such orbits is determined by the number of 2-torsion ideal class elements of R_f. Thus, to compute the averages when ordering by height in Theorem 6, we compare the number of rings (with multiplicity) in $\mathfrak{R}_H^{r_1,r_2}$ of bounded height to the number of relevant $\mathrm{SL}_n(\mathbb{Z})$-orbits whose binary n-ic invariant is bounded by the same height. To obtain Theorems 2 and 3, we restrict to maximal orders, namely, those rings $R_f \in \mathfrak{R}_{H,\max}^{r_1,r_2}$; however, a conjectural tail estimate is required to obtain a lower bound.

When ordering by Julia invariant, we count the number of $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_n(\mathbb{Z})$-orbits of $\mathbb{Z}^2 \otimes \mathrm{Sym}_2(\mathbb{Z}^n)$ relative to the number of $\mathrm{SL}_2(\mathbb{Z})$-orbits of $\mathrm{Sym}_n(\mathbb{Z}^2)$. As described above, the rings R_f associated to a binary n-ic form f are invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$ on f; that is, for any $\gamma f \in [f] = \mathrm{SL}_2(\mathbb{Z}) \cdot f$, we have $R_{\gamma f} \cong R_f$. It follows from [39] that if $\mathcal{O}_{[f]} \in \mathfrak{R}_J^{r_1,r_2}$ for some signature (r_1, r_2), then *projective* $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_n(\mathbb{Z})$-orbits of pairs of n-ary quadratic forms (A, B) with $[f_{(A,B)}] = [f]$ are in bijection with 2-torsion elements of the class group of $\mathcal{O}_{[f]}$. We then use the same geometry-of-numbers methods utilized when ordering by height to conclude Theorems 2 and 6 when ordering by Julia invariant. Note that when $n = 3$, the Julia invariant coincides with the discriminant of a binary cubic form, and so our argument can be viewed as a generalization of that given in [11].

Briefly, the article is organized as follows. In Section 2, we recall and expand on the details of the construction of rings R_f of rank n from binary n-ic forms f given in [29] and [38]. We also describe the correspondence given in [39] between SL_n-orbits of pairs of n-ary quadratic forms and order 2 ideal classes of such rings R_f. Section 3 discusses asymptotic counts of acceptable families in $\mathfrak{R}_H^{r_1,r_2}$ and $\mathfrak{R}_J^{r_1,r_2}$. Section 4 focuses on using geometry-of-numbers methods to count the projective integral orbits of pairs of n-ary quadratic forms whose binary n-ic invariant f is contained in $\mathfrak{R}_H^{r_1,r_2}$ or $\mathfrak{R}_J^{r_1,r_2}$. In Section 5, we describe several sieves that allow us to restrict our count from Section 4 to orbits that correspond to invertible ideal classes in orders (or maximal orders). Finally, in Section 6, the analytic methods in Sections 4 and 5 are combined with the algebraic interpretation of the orbits given in Section 2 to conclude the main results.

2. Parameterizations of 2-torsion ideal classes and composition laws

Let $n \geq 3$ be a fixed odd integer. In this section, we begin by recalling from [29] and [38] how rings of rank n naturally arise from integral binary n-ic forms. We then recall the parameterization given in [39] of 2-torsion ideal classes in such rings by orbits of pairs of n-ary quadratic forms. In Section 2.3, we describe a composition law for certain orbits of pairs of n-ary quadratic forms arising from the group law on ideal classes in rings. In Section 2.4, we discuss *reducible* elements in the space of such integral pairs and the properties of the corresponding 2-torsion ideal classes via the parameterization; these are elements that will be excluded in the volume computations in later sections. Finally, in Section 2.5, we use a rigidified version of the parameterization theorem in [39] over principal ideal domains to explicitly describe the stabilizers and orbits of these representations for a few specific base rings.

2.1. Rings associated to binary n-ic forms

We first describe the construction of a rank n ring over $\mathbb{Z}$ and ideals from an integral binary n-ic form. Let $f(x, y) = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n$, where $f_i \in \mathbb{Z}$. We begin with the case where $f_0 \neq 0$, and let $B_{f_0} = \mathbb{Z}[\frac{1}{f_0}]$. Define the ring R_f as a subring of $B_{f_0}[\theta]/f(\theta, 1)$, generated as a $\mathbb{Z}$-module as

$$R_f = \langle 1, f_0\theta, f_0\theta^2 + f_1\theta, \ldots, f_0\theta^{n-1} + f_1\theta^{n-2} + \cdots + f_{n-2}\theta\rangle. \tag{4}$$

For $k > 0$, define $\zeta_k = f_0\theta^k + \cdots + f_{k-1}\theta$, and let $\zeta_0 = 1$. It is shown in both [29] and [38] that $R_f = \langle \zeta_0, \ldots, \zeta_{n-1}\rangle$ is closed under multiplication and thus is a ring.

We define the following $\mathbb{Z}$-submodule of $B_{f_0}[\theta]/f(\theta,1)$:

$$I_f = \langle 1, \theta, \zeta_2, \ldots, \zeta_{n-1} \rangle. \tag{5}$$

As shown in [29] and [38], the module I_f is closed under multiplication by elements of R_f and thus is an ideal of R_f. It is easy to check that for $0 \le k \le n-1$, we have

$$I_f^k = \langle 1, \theta, \theta^2, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1} \rangle \tag{6}$$

as a $\mathbb{Z}$-submodule of $B_{f_0}[\theta]/f(\theta,1)$. For n odd, the ideal I_f^{n-3} is a square of the ideal $I_f^{\frac{n-3}{2}}$, which has the following explicit basis as a $\mathbb{Z}$-module:

$$I_f^{\frac{n-3}{2}} = \langle 1, \theta, \theta^2, \ldots, \theta^{\frac{n-3}{2}}, \zeta_{\frac{n-3}{2}+1}, \ldots, \zeta_{n-1} \rangle.$$

Additionally, there is a natural action of $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ on the set of binary n-ic forms f sending $\gamma \cdot f(x,y) = f((x,y)\gamma)$; under this action, the ring R_f and the ideal I_f (and its powers) are invariant (up to isomorphism). If f is irreducible, then R_f is an order of $\mathbb{Q}[\theta]/f(\theta,1)$, and the discriminants of R_f and f coincide (see [29, Proposition 1.1]). In addition, the form f is *primitive* (i.e., the greatest common divisor of its coefficients is 1) if and only if R_f is Gorenstein, which is equivalent to the property that I_f is an invertible fractional ideal (see [38, Proposition 2.1, Corollary 2.3]).

In fact, by recording the basis (6), the ideals I_f^k may be considered as *based ideals* of R_f, that is, ideals of R_f along with an ordered basis as a rank n $\mathbb{Z}$-module. The *norm* $\mathrm{N}(I)$ of a based ideal I of R_f is the determinant of the $\mathbb{Z}$-linear transformation taking the chosen basis of I to the basis of R_f given by (4).

We also introduce dual elements to θ^k for all $0 \le k \le n-1$. Let $\{\check{\theta}_0, \check{\theta}_1, \ldots, \check{\theta}_{n-1}\}$ be the B_{f_0}-module basis of $\mathrm{Hom}_{B_{f_0}}(B_{f_0}[\theta]/f(\theta,1), B_{f_0})$ dual to $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$. Additionally, define $\check{\zeta}_{n-1} := \frac{\check{\theta}_{n-1}}{f_0}$, and note that $\check{\zeta}_{n-1}(\zeta_k) = \delta_{k,n-1}$ for all $0 \le k \le n-1$. In [39, Proposition 2.1], Wood computes that for any $r \in B_{f_0}[\theta]/f(\theta,1)$ and $0 \le k \le n-2$,

$$\check{\theta}_k(r) = \check{\zeta}_{n-1}(\zeta_{n-1-k} r) + f_{n-1-k} \check{\zeta}_{n-1}(r), \tag{7}$$

which will be useful for computations in the following section.

Remark 2.1

If $f_0 = 0$ but $f \not\equiv 0$, there exists a $\mathrm{GL}_2(\mathbb{Z})$-transformation that takes f to another binary n-ic form f' with a nonzero leading coefficient. To obtain the ring R_f and the ideal class I_f (which are, up to isomorphism, $\mathrm{GL}_2(\mathbb{Z})$-invariant), one may use the above constructions for f' (see [38, Section 2]).

The above construction holds if one replaces $\mathbb{Z}$ with any integral domain T (see [38]); this gives an explicit way of associating a ring R_f, which is rank n as a T-module, and a distinguished (based) ideal I_f of R_f to a binary n-ic form over T. We refer to R_f as the *ring associated to* f and I_f as the *distinguished ideal* of R_f or f. Geometrically, for nonzero forms f, the ring R_f is the ring of functions on the subscheme X_f of $\mathbb{P}^1_T$ cut out by the binary n-ic form f, and the ideal I_f^k is the pullback of $\mathcal{O}(k)$ from $\mathbb{P}^1_T$ to X_f (see [38, Theorem 2.4]).

We are interested in counting the 2-torsion ideal classes of the rings R_f associated to irreducible forms f when n is odd. A key ingredient is a parameterization of such ideal classes in terms of pairs of $n \times n$ symmetric matrices, which we recall next.

2.2. *Parameterization of order 2 ideal classes in* R_f

For any base ring T, let $U(T) = \mathrm{Sym}_n(T^2)$ denote the space of binary n-ic forms with coefficients in T. Let $V(T) = T^2 \otimes \mathrm{Sym}_2(T^n)$ denote the space of pairs (A, B) of symmetric $n \times n$ matrices with coefficients a_{ij} of A and b_{ij} of B in T (for $1 \leq i, j \leq n$), where $a_{ij} = a_{ji}$ and $b_{ij} = b_{ji}$. The group $\mathrm{SL}_n(T)$ acts naturally on $V(T)$, where $\gamma \in \mathrm{SL}_n(T)$ acts on (A, B) by

$$\gamma(A, B) = (\gamma A \gamma^t, \gamma B \gamma^t). \tag{8}$$

The map $\pi : V(T) \to U(T)$ sending $(A, B) \mapsto \det(Ax - By)$ is clearly $\mathrm{SL}_n(T)$-equivariant. We call $f_{(A,B)} := \pi(A, B)$ the *binary n-ic invariant* or *resolvent form* of the pair (A, B) (or of the $\mathrm{SL}_n(T)$-equivalence class of (A, B)). Recall that a binary n-ic form f is *nondegenerate* if and only if its discriminant $\Delta(f)$ is nonzero, and we will call the pair (A, B) *nondegenerate* if and only if $f_{(A,B)}$ is nongenerate. In [39, Theorem 1.3], Wood describes the $\mathrm{SL}_n(\mathbb{Z})$-orbits of $V(\mathbb{Z})$ in terms of fractional ideals of the rings R_f from Section 2.1.

THEOREM 2.2 ([39, Theorem 1.3])
Let $f \in U(\mathbb{Z})$ be a nondegenerate primitive binary n-ic form with integral coefficients. Then there is a bijection between $\mathrm{SL}_n(\mathbb{Z})$-orbits of $(A, B) \in V(\mathbb{Z})$ with $f_{(A,B)} = f$ and equivalence classes of pairs (I, δ), where I is a fractional ideal of R_f and $\delta \in (R_f \otimes_{\mathbb{Z}} \mathbb{Q})^\times$ with $I^2 \subset \delta I_f^{n-3}$ as ideals and $\mathrm{N}(I)^2 = \mathrm{N}(\delta)\,\mathrm{N}(I_f^{n-3})$. Two pairs (I, δ) and (I', δ') are equivalent if there exists $\kappa \in (R_f \otimes_{\mathbb{Z}} \mathbb{Q})^\times$ such that $I' = \kappa I$ and $\delta' = \kappa^2 \delta$.

For forms f with $f_0 \neq 0$ (see Remark 2.1), we now explicitly describe the bijective map of Theorem 2.2, as some of these computations will be needed in Section 2.4.

Fix a primitive nondegenerate binary cubic form $f(x,y) = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n \in U(\mathbb{Z})$ with $f_0 \neq 0$, and let R_f denote the ring described in (4).

We begin by constructing an element of $V(\mathbb{Z})$ from a pair (I,δ) where I denotes a fractional ideal of R_f and δ denotes an invertible element of $R_f \otimes_{\mathbb{Z}} \mathbb{Q}$ such that $I^2 \subset \delta I_f^{n-3}$ and $\mathrm{N}(I)^2 = \mathrm{N}(\delta)\,\mathrm{N}(I_f^{n-3})$. Under these assumptions, we can define a map

$$\begin{aligned} \varphi : I \otimes_{R_f} I &\to I_f^{n-3}, \\ \alpha \otimes \alpha' &\mapsto \frac{\alpha\alpha'}{\delta}. \end{aligned} \tag{9}$$

For the $\mathbb{Z}$-module $\langle 1,\theta,\ldots,\theta^{n-3}\rangle$, there is a quotient map $I_f^{n-3} \to I_f^{n-3}/\langle 1,\theta,\ldots,\theta^{n-3}\rangle$, and when φ is composed with this quotient map, it gives a symmetric bilinear map that corresponds to an $\mathrm{SL}_n(\mathbb{Z})$-orbit of $V(\mathbb{Z})$. Equivalently, let $\alpha_1,\ldots,\alpha_n$ in $R_f \otimes_{\mathbb{Z}} \mathbb{Q}$ denote elements that generate I over $\mathbb{Z}$ and for which the change-of-basis matrix from $\langle \zeta_0,\zeta_1,\ldots,\zeta_{n-1}\rangle$ to $\langle \alpha_1,\ldots,\alpha_n\rangle$ has positive determinant. From the assumption that $I^2 \subset \delta I_f^{n-3}$, we have that for all $i,j \in \{1,\ldots,n\}$,

$$\frac{\alpha_i\alpha_j}{\delta} = c_{ij}^{(0)} + c_{ij}^{(1)}\theta + \cdots + c_{ij}^{(n-3)}\theta^{n-3} + b_{ij}\zeta_{n-2} + a_{ij}\zeta_{n-1}, \tag{10}$$

where $a_{ij}, b_{ij}, c_{ij}^{(k)} \in \mathbb{Z}$ for $0 \le k \le n-3$. Then $(A,B) = ((a_{ij}),(b_{ij}))$ yields the desired pair of integral symmetric $n \times n$ matrices.

To describe the reverse map, let $(A,B) \in V(\mathbb{Z})$ satisfy $\pi(A,B) = f$, and denote the coefficients of A as a_{ij} and of B as b_{ij}. Note that $\det A = f_0$, so requiring $f_0 \neq 0$ is equivalent to requiring A to be invertible. We want to construct a fractional ideal I of R_f along with an element $\delta \in (R_f \otimes_{\mathbb{Z}} \mathbb{Q})^\times$ such that $I^2 \subset \delta I_f^{n-3}$ and $\mathrm{N}(I)^2 = \mathrm{N}(\delta)\,\mathrm{N}(I_f^{n-3})$. Theorem 5.7 of [39] implies that it is equivalent to giving a $\mathbb{Z}$-basis $\langle \alpha_1,\ldots,\alpha_n\rangle$ for I and a map of R_f-modules $\varphi : I \otimes_{R_f} I \to I_f^{n-3}$ such that the composition

$$I \otimes_{\mathbb{Z}} I \to I \otimes_{R_f} I \to I_f^{n-3} \to I_f^{n-3}/\langle 1,\theta,\ldots,\theta^{n-3}\rangle \tag{11}$$

is equal to (A,B) when written in terms of $\langle \alpha_1,\ldots,\alpha_n\rangle$. Indeed, independent of the choice of i and j in $\{1,\ldots,n\}$, we have the equality $\delta = \frac{\alpha_i\alpha_j}{\varphi(\alpha_i \otimes \alpha_j)}$. (This is due to the fact that any map $I \otimes_{R_f} I \to I_f^{n-3}$ factors through an injective map $I^2 \to I_f^{n-3}$, which must be multiplication by an invertible element of $R_f \otimes_{\mathbb{Z}} \mathbb{Q}$.) Thus, we would like to describe I in terms of the $\mathbb{Z}$-basis $\langle \alpha_1,\ldots,\alpha_n\rangle$ and construct the map φ.

If the composition of maps in (11) corresponds to (A,B) relative to a $\mathbb{Z}$-basis $\langle \alpha_1,\ldots,\alpha_n\rangle$, then the map $I \otimes_{\mathbb{Z}} I \to I \otimes_{R_f} I \to I_f^{n-3}$ can be described on elements of the $\mathbb{Z}$-basis $\langle \alpha_i \otimes \alpha_j\rangle$ of $I \otimes I$ as

$$\begin{aligned}\varphi(\alpha_i \otimes \alpha_j) &= \sum_{k=0}^{n-3} c_{ij}^{(k)} \theta^k + b_{ij}\zeta_{n-2} + a_{ij}\zeta_{n-1} \\ &= c_{ij}^{(0)} + \sum_{k=1}^{n-3} (c_{ij}^{(k)} + b_{ij} f_{n-k-2} + a_{ij} f_{n-k-1})\theta^k \\ &\quad + (b_{ij} f_0 + a_{ij} f_1)\theta^{n-2} + a_{ij} f_0 \theta^{n-1}, \end{aligned} \tag{12}$$

where $c_{ij}^{(k)}$ are integers for $k \in \{0, \dots, n-3\}$ and $1 \le i, j \le n$. Thus, the coefficients $c_{ij}^{(k)}$ must satisfy

$$c_{ij}^{(k)} = \begin{cases} \check{\theta}_k(\varphi(\alpha_i \otimes \alpha_j)) - f_{n-k-2} \cdot b_{ij} - f_{n-k-1} \cdot a_{ij} & \text{if } 1 \le k \le n-3, \\ \check{\theta}_k(\varphi(\alpha_i \otimes \alpha_j)) & \text{if } k = 0. \end{cases}$$

Using equation (7), we then have that $c_{ij}^{(k)}$ for $k > 0$ must satisfy

$$\begin{aligned} c_{ij}^{(k)} &= f_{n-k-1}\check{\zeta}_{n-1}\big(\varphi(\alpha_i \otimes \alpha_j)\big) + \check{\zeta}_{n-1}\big(\zeta_{n-k-1} \cdot \varphi(\alpha_i \otimes \alpha_j)\big) \\ &\quad - f_{n-k-2} \cdot b_{ij} - f_{n-k-1} \cdot a_{ij} \\ &= \check{\zeta}_{n-1}\big(\zeta_{n-k-1} \cdot \varphi(\alpha_i \otimes \alpha_j)\big) - f_{n-k-2} \cdot b_{ij} \\ &= \check{\zeta}_{n-1}\big((f_0\theta^{n-k-1} + f_1\theta^{n-k-2} + \cdots + f_{n-k-2}\theta) \cdot \varphi(\alpha_i \otimes \alpha_j)\big) \\ &\quad - f_{n-k-2} \cdot b_{ij}. \end{aligned}$$

The middle equality follows from the fact that $\check{\zeta}_{n-1}(\varphi(\alpha_i \otimes \alpha_j)) = a_{ij}$ by equation (12). By [39, Proposition 3.3], if we write an element α of I as a row vector $(a_1, a_2, \dots, a_n)$ relative to the $\mathbb{Z}$-basis $\langle \alpha_1, \dots, \alpha_n \rangle$ corresponding to (A, B), then $\theta \in B_{f_0}[\theta]/f(\theta, 1)$ must act on I by right multiplication by BA^{-1}; that is,

$$\theta \cdot \alpha = (a_1, a_2, \dots, a_n) \cdot BA^{-1}.$$

Thus, if we create $n-2$ matrices $C^{(k)}$ such that its ijth entry is equal to $c_{ij}^{(k)}$, then we have for $k > 0$:

$$\begin{aligned} C^{(k)} &= \big(f_0 \cdot (BA^{-1})^{n-k-1} + f_1 \cdot (BA^{-1})^{n-k-2} + \cdots + f_{n-k-2} \cdot BA^{-1}\big)A \\ &\quad - f_{n-k-2}B \\ &= \big(f_0 \cdot (BA^{-1})^{n-k-2} + f_1 \cdot (BA^{-1})^{n-k-3} + \cdots + f_{n-k-3} \cdot BA^{-1}\big)B. \end{aligned} \tag{13}$$

Additionally,

$$C^{(0)} = \big(f_0 \cdot (BA^{-1})^{n-1} + f_1 \cdot (BA^{-1})^{n-2} + \cdots + f_{n-2} \cdot BA^{-1} + f_{n-1}\big)A.$$

Furthermore, since the action of θ gives the action of R_f on I, this completely determines the map φ and I as an R_f-module. By [39, Propositions 5.1 and 5.4], this implies that I can be realized as a fractional ideal, and thus there is a well-defined element of $(R_f \otimes_{\mathbb{Z}} \mathbb{Q})^{\times}$ satisfying

$$\delta = \frac{\alpha_i \alpha_j}{\varphi(\alpha_i \otimes \alpha_j)},$$

independent of the choice of i and j. Additionally, for each $1 \leq j \leq n$, we have that the α_i's satisfy the following ratios:

$$\begin{aligned}\alpha_1 : \alpha_2 : \cdots : \alpha_{n-1} : \alpha_n = {} & c_{1,j}^{(0)} + \cdots + c_{1,j}^{(n-3)} \theta^{n-3} + b_{1,j} \zeta_{n-2} + a_{1,j} \zeta_{n-3} \\ & : c_{2,j}^{(0)} + \cdots + c_{2,j}^{(n-3)} \theta^{n-3} + b_{2,j} \zeta_{n-2} + a_{2,j} \zeta_{n-3} : \cdots \\ & : c_{n-1,j}^{(0)} + \cdots + c_{n-1,j}^{(n-3)} \theta^{n-3} + b_{n-1,j} \zeta_{n-2} + a_{n-1,j} \zeta_{n-3} \\ & : c_{n,j}^{(0)} + \cdots + c_{n,j}^{(n-3)} \theta^{n-3} + b_{n,j} \zeta_{n-2} + a_{n,j} \zeta_{n-3}.\end{aligned}$$

The ratios must be independent of the choice of j, so this in conjunction with δ determines $\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$. The action of $\mathrm{SL}_n(\mathbb{Z})$ on $V(\mathbb{Z})$ corresponds to the action $g_n \in \mathrm{SL}_n(\mathbb{Z})$ on the chosen basis for I which sends

$$\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle \mapsto \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle \cdot g_n^t. \tag{14}$$

Thus, the ideal I is invariant under the action of $\mathrm{SL}_n(\mathbb{Z})$.

2.3. Composition of elements of $V(\mathbb{Z})$ with the same binary n-ic invariant

Let $\mathcal{O}$ be an S_n-order, that is, an order in a degree n S_n-number field K over $\mathbb{Q}$. Consider the set of pairs (I, δ), where I is a fractional ideal of $\mathcal{O}$, $\delta \in K^{\times}$, $I^2 \subset (\delta)$, and $N(I)^2 = N(\delta)$. Recall that we called two such pairs (I, δ) and (I', δ') *equivalent* if there exists $\kappa \in K^{\times}$ such that $I' = \kappa I$ and $\delta' = \kappa^2 \delta$. We have a natural law of composition on equivalence classes of such pairs given by

$$(I, \delta) \circ (I', \delta') = (II', \delta\delta'). \tag{15}$$

We say that a pair (I, δ) is *projective* if I is projective as an $\mathcal{O}$-module, that is, if I is invertible as a fractional ideal of $\mathcal{O}$; the pair (I, δ) is projective if and only if $I^2 = (\delta)$. The set of equivalence classes of projective pairs (I, δ) for $\mathcal{O}$ forms a group under the composition law (15), which we denote by $\mathrm{H}(\mathcal{O})$.

There exists a natural group homomorphism from $\mathrm{H}(\mathcal{O})$ to $\mathrm{Cl}_2(\mathcal{O})$, given by sending the pair (I, δ) to the ideal class of I. This map is clearly well defined and surjective. The kernel consists of equivalence classes of pairs (I, δ) where I is a principal ideal; each such equivalence class has a representative of the form $(\mathcal{O},\delta)$ where δ is a norm 1 unit. Therefore, we obtain the exact sequence

$$1 \to \frac{\mathcal{O}^\times_{N=1}}{(\mathcal{O}^\times)^2} \to \mathrm{H}(\mathcal{O}) \to \mathrm{Cl}_2(\mathcal{O}) \to 1, \tag{16}$$

which implies that $\mathrm{H}(\mathcal{O})$ is an extension of the 2-torsion subgroup of the class group of $\mathcal{O}$. Using Dirichlet's unit theorem and the fact that $-1 \in \mathcal{O}^\times$ has norm -1, we immediately obtain the following lemma.

LEMMA 2.3
Let $\mathcal{O}$ be an order in an S_n-number field of degree n and signature (r_1,r_2). Then $|\mathrm{H}(\mathcal{O})| = 2^{r_1+r_2-1}|\,\mathrm{Cl}_2(\mathcal{O})|$.

We next compare certain elements of $\mathrm{H}(\mathcal{O})$ to the 2-torsion subgroup $\mathrm{Cl}_2^+(\mathcal{O})$ of the *narrow* class group $\mathrm{Cl}^+(\mathcal{O})$ of $\mathcal{O}$. Recall that $\mathrm{Cl}^+(\mathcal{O})$ is the quotient of the ideal group $\mathcal{I}(\mathcal{O})$ of $\mathcal{O}$ by the group $P^+(\mathcal{O})$ of *totally positive* principal fractional ideals of $\mathcal{O}$, that is, ideals of the form $a\mathcal{O}$ where a is an element of $\mathrm{Frac}(\mathcal{O})^\times$ such that $\sigma(a)$ is positive for every embedding $\sigma : \mathrm{Frac}(\mathcal{O}) \to \mathbb{R}$. We say that such an element a is *totally positive* and denote this condition by $a \gg 0$.

LEMMA 2.4
Let $\mathcal{O}$ be an order in a degree n S_n-number field with signature (r_1,r_2). If $\mathrm{H}^+(\mathcal{O})$ denotes the subgroup of $\mathrm{H}(\mathcal{O})$ consisting of projective pairs (I,δ) such that $\delta \gg 0$, then

$$\left|\mathrm{H}^+(\mathcal{O})\right| = 2^{r_2}\left|\mathrm{Cl}_2^+(\mathcal{O})\right|. \tag{17}$$

Proof
Let $\mathcal{O}^\times_{\gg 0}$ denote the totally positive units of $\mathcal{O}$, and define $\mathrm{sgn} : \mathcal{O}^\times \to \{\pm 1\}^{r_1}$ as the signature homomorphism, which takes a unit to the sign of its image under each real embedding $\sigma : \mathrm{Frac}\,\mathcal{O} \to \mathbb{R}$. Let r be the nonnegative integer satisfying $|\mathrm{Image(sgn)}| = 2^r$, and let

$$\mathcal{C}_2^{\gg 0}(\mathcal{O}) = \left\{[I] : \text{there exists } \delta \gg 0 \text{ such that } I^2 = (\delta)\right\}$$

be the set of equivalence class of ideals whose square is totally positive, where two ideals are equivalent if they differ by a principal ideal (in the usual sense). We then have the following commutative diagram of exact sequences:

$$
\begin{tikzcd}
1 \arrow[drr] & & & & & & & & & & 1 \arrow[dll] \\
1 \arrow[rr] & & \mathcal{O}^{\times}_{\gg 0}/(\mathcal{O}^{\times})^2 \arrow[rr] \arrow[drr] & & \mathcal{O}^{\times}/(\mathcal{O}^{\times})^2 \arrow[rr, "\mathrm{sgn}"] & & \{\pm 1\}^{r_1} \arrow[rr] & & \{\pm 1\}^{r_1}/\mathrm{sgn}(\mathcal{O}^{\times}) \arrow[rr] \arrow[dll] & & 1 \\
 & & & & \mathrm{H}^+(\mathcal{O}) \arrow[dr, "\alpha"'] & & \mathrm{Cl}_2^+(\mathcal{O}) \arrow[dl, "\beta"] & & & & \\
 & & & & & \mathcal{C}_2^{\gg 0}(\mathcal{O}) \arrow[dl] \arrow[dr] & & & & & \\
 & & & & 1 & & 1 & & & &
\end{tikzcd}
$$

where the map α sends a pair (I,δ) with $\delta \gg 0$ to the equivalence class $[I]$, and the map β sends a coset $I + P^+(\mathcal{O})$ to the equivalence class $[I]$. We have that $|\mathcal{O}^{\times}/(\mathcal{O}^{\times})^2| = 2^{r_1+r_2}$ and $|\{\pm 1\}^{r_1}/\mathrm{sgn}(\mathcal{O}^{\times})| = 2^{r_1-r}$, so $|\mathcal{O}^{\times}_{\gg 0}/(\mathcal{O}^{\times})^2| = 2^{r_1-r+r_2}$. The equality (17) follows immediately. $\square$

We now relate *projective* orbits of $V(\mathbb{Z})$ to the size of the 2-torsion subgroup of the ideal class group of the corresponding rings. We say that a pair $(A,B) \in V(\mathbb{Z}) \cap \pi^{-1}(f)$ is *projective* if the corresponding pair (I,δ) under the bijection of Theorem 2.2 is projective. We then have the following result.

PROPOSITION 2.5
Let $\mathcal{O}$ be an S_n-order corresponding to an integral, nondegenerate, irreducible, and primitive binary n-ic form f. Then $\mathrm{H}(\mathcal{O})$ is in natural bijection with the set of projective $\mathrm{SL}_n(\mathbb{Z})$-orbits on $V(\mathbb{Z}) \cap \pi^{-1}(f)$. The number of such projective orbits is equal to

$$2^{r_1+r_2-1}\left|\mathrm{Cl}_2(\mathcal{O})\right|,$$

where (r_1,r_2) is the signature of the fraction field of $\mathcal{O}$.

Proof
From Theorem 2.2, projective orbits in $V(\mathbb{Z}) \cap \pi^{-1}(f)$ are in bijection with pairs (I,δ), where I is a fractional ideal of $\mathcal{O}$, $\delta \in K^{\times}$, and $I^2 = \delta I_f^{n-3}$. The set of such pairs is clearly in bijection with $\mathrm{H}(\mathcal{O})$ by simply sending (I,δ) to $(I \cdot I_f^{-\frac{n-3}{2}}, \delta)$. The second assertion of the proposition now follows immediately from Lemma 2.3. $\square$

2.4. *Reducible elements in* $V(\mathbb{Z})$

We say that an element $(A, B) \in V(\mathbb{Q})$ is *reducible* if the quadrics in $\mathbb{P}^{n-1}(\mathbb{Q})$ corresponding to A and B have a common rational isotropic subspace of dimension $(n-1)/2$ in $\mathbb{P}^{n-1}(\mathbb{Q})$. The condition of reducibility has the following arithmetic significance.

THEOREM 2.6

Let (A, B) be a projective element of $V(\mathbb{Z})$ whose binary n-ic invariant is primitive, irreducible, and nondegenerate, and let (I, δ) denote the corresponding pair as given by Theorem 2.2. Then (A, B) is reducible if and only if δ is a square in $(R_f \otimes_{\mathbb{Z}} \mathbb{Q})^\times$.

Proof

Suppose first that $\delta = r^2$ is the square of an invertible element in $(R_f \otimes \mathbb{Q})^\times$. By replacing I with $r^{-1}I$ and δ with $r^{-2}\delta$, we may assume that $\delta = 1$. Let $\alpha_1, \dots, \alpha_{\frac{n-1}{2}}$ be a $\mathbb{Z}$-basis for $I \cap (\mathbb{Z} \oplus \mathbb{Z}\theta \oplus \cdots \oplus \mathbb{Z}\theta^{\frac{n-3}{2}})$, and extend it to a basis $\alpha_1, \dots, \alpha_n$ of I. It follows from (10) that, with these coordinates, we have $a_{ij} = b_{ij} = 0$ for $1 \le i, j \le (n-1)/2$, which is sufficient for (A, B) to be reducible.

Now assume that (A, B) is reducible; we would like to prove that δ is a square. Let $x_1, x_2, \dots, x_n$ denote a set of coordinates for $\mathbb{P}^{n-1}$. By replacing (A, B) with an $\mathrm{SL}_n(\mathbb{Q})$-translate if necessary, we may assume that the common isotropic subspace is the one generated by $x_1, \dots, x_{(n-1)/2}$. This implies that $a_{ij} = b_{ij} = 0$ for $1 \le i, j \le (n-1)/2$. From (12) and (13), we see that the quantity $\alpha_i\alpha_j/\delta$ is given by the ijth coordinate of the matrix

$$\begin{aligned}
D &:= C^{(0)} + \Big(\sum_{k=1}^{n-3} (C^{(k)} + f_{n-k-2}B + f_{n-k-1}A) \cdot \theta^k\Big) \\
&\qquad + (f_0 B + f_1 A) \cdot \theta^{n-2} + f_0 A \cdot \theta^{n-1} \\
&= \sum_{k=0}^{n-1} \Big(\sum_{j=0}^{n-k-1} f_{n-k-j-1}(BA^{-1})^j \Big) A \cdot \theta^k \\
&= \sum_{\substack{j+k \le n-1 \\ j,k \ge 0}} f_{n-j-k-1}(BA^{-1})^j A \cdot \theta^k
\end{aligned} \tag{18}$$

where $f = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n$ is the binary n-ic invariant of (A, B). (Note that A is invertible because f is assumed to be irreducible, so $f_0 = \det A \neq 0$.)

We now prove that the 11-coefficient d_{11} of D is a square using the fact that $a_{ij} = b_{ij} = 0$ for $1 \le i, j \le (n-1)/2$. This implies that $\delta = \alpha_1^2/d_{11}$ is a square as well. First, from (18), note that the coefficients of θ^{n-1} and θ^{n-2} of d_{11} are 0, since $a_{11} = b_{11} = 0$. We start with the following lemma.

LEMMA 2.7
The coefficient of θ^{n-3} in d_{11} is a square.

Proof
From (18) and the fact that $a_{11} = b_{11} = 0$, the coefficient of θ^{n-3} in d_{11} is equal to the 11-coefficient of the matrix $f_0(BA^{-1})^2A = f_0BA^{-1}B$. Let M denote the cofactor matrix of A, that is, the ij-coefficient m_{ij} of M is equal to $(-1)^{i+j}$ times the determinant of the matrix obtained by removing the ith row and the jth column of A. Then the coefficient of θ^{n-3} in d_{11} is equal to the 11-coefficient of BMB.

We now describe the coefficients of M. Let A^{top} denote the top-right $(n-1)/2$, $(n+1)/2$ submatrix of A. Note that, since A is symmetric, the bottom-left $(n+1)/2, (n-1)/2$ submatrix of A is simply the transpose of A^{top}. For $i \in [(n+1)/2, n]$, let A_i denote the $(n-1)/2, (n-1)/2$ matrix obtained by removing the $(i-(n-1)/2)$th column of A^{top}. Then removing the $(i-(n-1)/2)$th row of the transpose of A^{top} yields A_i^t. Since the top-right $(n-1)/2, (n-1)/2$ block of A is 0, it follows that for $i, j > (n-1)/2$, we have $m_{ij} = (-1)^{i+j}\,\mathrm{Det}(A_i)\,\mathrm{Det}(A_j)$. Therefore, we have

$$\begin{aligned}
\text{11-coefficient of } BMB &= \sum_{i,j=1}^{n} b_{1i}m_{ij}b_{j1} \\
&= \sum_{i,j=(n+1)/2}^{n} (-1)^{i+j}b_{1i}b_{1j}\det A_i \det A_j \\
&= \Big(\sum_{k=(n+1)/2}^{n} (-1)^k b_{1k}\det A_k\Big)^2,
\end{aligned}$$

as necessary. □

Next, we show that the constant coefficient of d_{11} (considered as a polynomial in θ) is a square.

LEMMA 2.8
The constant coefficient $d_{11}(0)$ of $d_{11}(\theta)$ is a square.

Proof
Because the binary n-ic invariant of (A, B) is f, we have $\det(Ax - By) = \det(Ix - BA^{-1}y)\det(A) = f(x, y)$. Since BA^{-1} satisfies its characteristic polynomial, we

obtain

$$\sum_{j=0}^{n} f_{n-j}(BA^{-1})^j = 0.$$

By (18), we compute $d_{11}(0)$ to be the 11-coefficient of the matrix

$$\begin{aligned}\Big(\sum_{j=0}^{n-1} f_{n-j-1}(BA^{-1})^j\Big)A &= \Big(\sum_{j=0}^{n-1} f_{n-(j+1)}(BA^{-1})^{j+1}\Big)AB^{-1}A\\ &= \Big(\sum_{j=0}^{n} f_{n-j}(BA^{-1})^j\Big)AB^{-1}A - f_nAB^{-1}A\\ &= -f_nAB^{-1}A.\end{aligned}$$

Note that B is invertible because $\det B = f_n \neq 0$ since f is irreducible. The lemma now follows from the proof of Lemma 2.7 and symmetry (and the fact that n is odd). □

We next show that $d_{11}(m)$ is a square for every integer m, by applying Lemma 2.8 on the pair $(A, B - mA)$. Let g denote the binary n-ic invariant of the pair $(A, B - mA)$, and let g_k denote the coefficient of $x^{n-k}y^k$ in $g(x, y)$. We have

$$g(x, y) = \det\big(Ax - (B - mA)y\big) = \det\big(A(x + my) - By\big) = f(x + my, y).$$

As a consequence, we compute the g_k to be

$$g_k = \sum_{j=0}^{k} \binom{n-j}{k-j} f_j m^{k-j}.$$

By applying Lemma 2.8 to $(A, B - mA)$, we see that the 11-coefficient of the following matrix is a square:

$$\begin{aligned}&\Big(\sum_{j=0}^{n-1} g_{n-j-1}(BA^{-1} - mI)^j\Big)A\\ &= \Big(\sum_{k=0}^{n-1} g_k(BA^{-1} - mI)^{n-k-1}\Big)A\\ &= \left(\sum_{k=0}^{n-1}\left(\sum_{j=0}^{k}\binom{n-j}{k-j} f_j m^{k-j}\right)(BA^{-1} - mI)^{n-k-1}\right)A\end{aligned}$$

$$
\begin{aligned}
&= \left(\sum_{k=0}^{n-1} \left(\sum_{j=0}^{k} \binom{n-j}{k-j} f_j m^{k-j} \right) \right. \\
&\quad \times \left. \left(\sum_{i=0}^{n-k-1} (-1)^{k+i} \binom{n-k-1}{i} (BA^{-1})^i m^{n-k-i-1} \right) \right) A \\
&= \left(\sum_{k=0}^{n-1} \sum_{j=0}^{k} \sum_{i=0}^{n-k-1} (-1)^{i+k} f_j (BA^{-1})^i m^{n-i-j-1} \binom{n-j}{k-j} \binom{n-k-1}{i} \right) A \\
&= \left(\sum_{i,j\geq 0}^{i+j\leq n-1} f_j (BA^{-1})^i m^{n-i-j-1} \sum_{k=j}^{n-i-1} (-1)^{k+i} \binom{n-j}{k-j} \binom{n-k-1}{i} \right) A \\
&= \Big(\sum_{i,j\geq 0}^{i+j\leq n-1} f_j (BA^{-1})^i m^{n-i-j-1} \Big) A, \qquad (19)
\end{aligned}
$$

where the last equality is a consequence of the following lemma.

LEMMA 2.9
For nonnegative integers n, i, and j satisfying $i + j \leq n-1$, we have

$$\sum_{k=j}^{n-i-1} (-1)^{k+i} \binom{n-j}{k-j} \binom{n-k-1}{i} = (-1)^{n+1}.$$

Proof
By taking the ith derivative of both sides of the identity

$$\frac{(1+x)^{n-j}-1}{x} = \sum_{k=j}^{n-1} x^{n-k-1} \binom{n-j}{n-k}$$

and setting $x = -1$, we obtain the lemma. □

Comparing the formulas (19) and (18) with $\theta = m$ shows that $d_{11}(m)$ is a square for any integer m. It is a classical result that a polynomial that takes only square values on integers must itself be a square. We include a proof for completeness.

LEMMA 2.10
Suppose that $f(x) \in \mathbb{Z}[x]$ takes square values at every integer. Then $f(x) = g(x)^2$ for some integer polynomial $g(x)$.

Proof

Suppose for the sake of contradiction that $f(x)$ is a nonconstant square-free polynomial. Then the resultant $R(f, f')$ of f and its derivative is a nonzero constant. Choose a prime p such that $p \nmid R(f, f')$ and such that $p \mid f(n)$ for some integer n; such a prime p exists since there exist infinitely many primes dividing some value of f applied to integers. We have that $p \mid f(n+p)$ also. By the assumption that f takes square values, we also have that p^2 divides both $f(n)$ and $f(n+p)$. However, because $f(n+p) \equiv f(n) + pf'(n) \pmod{p^2}$, we find that $p \mid f'(n)$ and thus $p \mid R(f, f')$, yielding a contradiction. □

Thus it follows that the 11-coefficient of D is a square, concluding the proof of Theorem 2.6. □

Remark 2.11

Theorem 2.6 also follows from a different interpretation of orbits of $V(\mathbb{Q})$ in terms of Jacobians of hyperelliptic curves, found in Wang's dissertation (see [36]).

For an order $\mathcal{O}$, let $\mathcal{I}_2(\mathcal{O})$ denote the 2-torsion subgroup of the ideal group of $\mathcal{O}$, that is, the group of invertible fractional ideals I of $\mathcal{O}$ such that $I^2 = \mathcal{O}$. Note that the group $\mathcal{I}_2(\mathcal{O})$ is trivial when $\mathcal{O}$ is maximal. We have the following result parameterizing elements of $\mathcal{I}_2(\mathcal{O})$ for all primitive orders $\mathcal{O}$ arising from integral binary n-ic forms.

PROPOSITION 2.12

Let $\mathcal{O}_f$ be an order corresponding to the integral, primitive, irreducible, and nondegenerate binary n-ic form f. Then $\mathcal{I}_2(\mathcal{O}_f)$ is in natural bijection with the set of projective reducible $\mathrm{SL}_n(\mathbb{Z})$-orbits on $V(\mathbb{Z}) \cap \pi^{-1}(f)$.

Proof

Theorem 2.6 shows that a projective $\mathrm{SL}_n(\mathbb{Z})$-orbit on $V(\mathbb{Z})$ corresponding to the pair (I, δ) is reducible exactly when δ is a square, say $\delta = \kappa^2$. The map from projective reducible $\mathrm{SL}_n(\mathbb{Z})$-orbits on $V(\mathbb{Z}) \cap \pi^{-1}(f)$ to $\mathcal{I}_2(R)$ that sends such an orbit to $\kappa^{-1} I \cdot I_f^{-\frac{n-3}{2}}$ is clearly a bijection. □

2.5. *Parameterizations over other rings*

Let T be a principal ideal domain. We now describe an analogue of Theorem 2.2 over T, and we study a rigidified version of the parameterization to better understand the orbits and stabilizers of the group action. The following theorem describes how

$\mathrm{SL}_n(T)$-orbits of $V(T)$ are related to rank n rings and ideal classes; it is a restatement of [39, Theorem 6.3], using the fact that our base ring T is a principal ideal domain.

THEOREM 2.13 ([39, Theorem 6.3])
Let $f \in U(T)$ be a nondegenerate primitive binary n-ic form. Then there is a bijection between $\mathrm{SL}_n(T)$-orbits of $(A,B) \in V(T)$ with $f_{(A,B)} = f$ and equivalence classes of pairs (I,δ), where $I \subset K_f := T[x]/(f(x,1))$ is an ideal of R_f and $\delta \in K_f^\times$ satisfying $I^2 \subset \delta I_f^{n-3}$ as ideals and $\mathrm{N}(I)^2 = \mathrm{N}(\delta)\,\mathrm{N}(I_f^{n-3})$. Two pairs (I,δ) and (I',δ') are equivalent if there exists $\kappa \in K_f^\times$ such that $I' = \kappa I$ and $\delta' = \kappa^2\delta$.

Note that in [39, Section 6] the theorems are stated for $\mathrm{SL}_n^\pm(T)$-orbits instead of $\mathrm{SL}_n(T)$-orbits, where $\mathrm{SL}_n^\pm(T)$ denotes the elements of determinant ±1 in $\mathrm{GL}_n(T)$. However, since n is odd here, we have $\mathrm{SL}_n^\pm(T) \cong \{\pm1\} \times \mathrm{SL}_n(T)$, and since -1 acts trivially on pairs (A,B) by (8), the $\mathrm{SL}_n(T)$-orbits are precisely the same as the $\mathrm{SL}_n^\pm(T)$-orbits.

In order to understand the stabilizer of the action of $\mathrm{SL}_n(T)$ on an element $(A,B) \in V(T)$, we now discuss precisely with what the elements (instead of $\mathrm{SL}_n(T)$-orbits) of $V(T)$ are in correspondence, in terms of the pair (I,δ) along with a basis for I.

PROPOSITION 2.14 ([39, Theorems 6.1, 6.3])
Let $f \in U(T)$ be a nondegenerate primitive binary n-ic form. Let $K_f := T[x]/(f(x,1))$. Then the nonzero elements $(A,B) \in V(T)$ with $f_{(A,B)} = f$ are in bijection with equivalence classes of triples $(I,\mathcal{B},\delta)$ where $I \subset K_f$ is a based ideal of R_f, with an ordered basis given by an isomorphism $\mathcal{B} : I \to T^n$ of T-modules, and $\delta \in K_f^\times$, satisfying $I^2 \subset \delta I_f^{n-3}$ as ideals and $\mathrm{N}(I)^2 = \mathrm{N}(\delta)\,\mathrm{N}(I_f^{n-3})$. Two such triples $(I,\mathcal{B},\delta)$ and $(I',\mathcal{B}',\delta')$ are equivalent if and only if there exists $\kappa \in K_f^\times$ such that $I' = \kappa I$, $\mathcal{B} \circ (\times\kappa) = \mathcal{B}'$, and $\delta' = \kappa^2\delta$.

As stated, Proposition 2.14 is a "symmetric" version of the first part of [39, Theorem 6.1]. For any $(A,B) \in V(T)$ corresponding to $(I,\mathcal{B},\delta)$ in Proposition 2.14, the action of $\mathrm{SL}_n(T)$ on (A,B) as in (8) induces an action of $\mathrm{SL}_n(T)$ on the basis $\mathcal{B}$ through the correspondence, namely, as given in (14). This action of $\mathrm{SL}_n(T)$ takes I to itself and does not affect δ, so $\mathrm{SL}_n(T)$ acts on the triples $(I,\mathcal{B},\delta)$. Quotienting both sides of the correspondence in Proposition 2.14 by $\mathrm{SL}_n(T)$ yields precisely Theorem 2.13.

For the computations in later sections, we are interested in the stabilizer of $(A,B) \in V(T)$ in $\mathrm{SL}_n(T)$. Any $g \in \mathrm{SL}_n(T)$ that fixes (A,B) must correspond to an automorphism of the corresponding triple $(I,\mathcal{B},\delta)$; as g preserves the map $\mathcal{B}$, it is, up to scaling, an automorphism of I as a $\mathbb{Z}[T]$-module. Because the discriminant of the corresponding form f is nonzero, such a module homomorphism is given by multiplication by a nonzero scalar. Since g also fixes δ, in fact g corresponds to multiplication by an element $\kappa \in K_f^\times$ with $\kappa^2 = 1$. (In fact, such κ lie in $R_f^\times$.) Furthermore, since multiplication on $\mathcal{B}$ by κ exactly corresponds to multiplication by the matrix g, we must have $\mathrm{N}(\kappa) = \det(g) = 1$. It is also easy to check that any such κ yields an element $g \in \mathrm{SL}_n(T)$ that stabilizes (A, B). We thus have the following description of the stabilizers.

COROLLARY 2.15

Fix a principal ideal domain T. Let $(A, B) \in V(T)$ be a nondegenerate element with primitive binary n-ic invariant f, corresponding to the ring R_f and the pair (I, δ) under Theorem 2.13. Then the stabilizer group in $\mathrm{SL}_n(T)$ of (A, B) corresponds to the norm 1 elements $R_f^\times[2]_{\mathrm{N}\equiv 1}$ of the 2-torsion in $R_f^\times$.

In the cases where T is a field or $\mathbb{Z}_p$, we may also describe the $\mathrm{SL}_n(T)$-orbits of $V(T)$ corresponding to a given binary n-ic invariant in a simple way. We restrict to *projective* orbits, that is, those corresponding to (I, δ) where I is projective as an R_f-module. (In the case where T is a field, this will be no restriction.)

COROLLARY 2.16

Let T be a field or $\mathbb{Z}_p$. Let f be a separable nondegenerate binary n-ic form with coefficients in T. Then the projective $\mathrm{SL}_n(T)$-orbits of $V(T)$ with invariant binary n-ic form f are in bijection with elements of $(R_f^\times/(R_f^\times)^2)_{\mathrm{N}\equiv 1}$.

Proof

Let $T = k$ be a field, and let f be a separable nondegenerate binary n-ic form over k. Then R_f is a commutative k-algebra of dimension n, and in particular, a direct product of field extensions of k and thus a principal ideal ring. It is easy to check that $I_f = R_f$. In this case, Theorem 2.13 implies that $\mathrm{SL}_n(k)$-orbits on $V(k)$ with binary n-ic invariant f correspond to equivalence classes of pairs (I, δ), where I is a fractional ideal of R_f and $\delta \in R_f^\times$ such that $I^2 = \delta I_f^{n-3} = \delta R_f$. The only ideals in R_f are products of either the unit ideal or the zero ideal in each of the factors; since δ must be invertible, we have $I = R_f$ and so $\mathrm{N}(\delta) = 1$. Thus, the equivalence classes of the pairs (I, δ) are parameterized by norm 1 elements δ of $R_f^\times/(R_f^\times)^2$.

Now let $T = \mathbb{Z}_p$. The ring R_f is a direct product of finite extensions of $\mathbb{Z}_p$ and is thus a principal ideal ring. For projective pairs (I, δ) as in Theorem 2.13, the norm condition implies that $I^2 = \delta I_f^{n-3}$. As a result, the ideal I is again determined by the element δ of $R_f^\times$. Furthermore, since $n - 3$ is even, we obtain that

$$\mathrm{N}(\delta) = \Big(\frac{\mathrm{N}(I)}{\mathrm{N}(I_f^{(n-3)/2})}\Big)^2$$

is a square, so the set of equivalence classes of pairs (I, δ) are parameterized by $(R_f^\times/(R_f^\times)^2)_{\mathrm{N}\equiv 1}$. $\square$

Example 2.17
For $k = \mathbb{R}$, for a given f as above, we have that R_f is isomorphic to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ for some nonnegative integers r_1 and r_2 with $r_1 + 2r_2 = n$. Then the number of $\mathrm{SL}_n(\mathbb{R})$-orbits with invariant binary n-ic form f is 2^{r_1-1}, and the order of the stabilizer in $\mathrm{SL}_n(\mathbb{R})$ is $2^{r_1+r_2-1}$.

3. Counting binary n-ic forms in acceptable families

Our goal in this section is to determine asymptotics for the number of irreducible elements in *acceptable* families of binary n-ic forms having bounded height, as well as to determine asymptotics for the number of irreducible $\mathrm{SL}_2(\mathbb{Z})$-orbits on $\mathrm{SL}_2(\mathbb{Z})$-invariant acceptable families having bounded Julia invariant. We first define an acceptable family of binary n-ic forms, as well as how to compute the size of such families when ordered by height. We then define the Julia invariant and recall a result of [13] on the asymptotics of orbits of binary n-ic forms ordered by Julia invariant.

3.1. *Acceptable families of binary n-ic forms*

Recall that $U(T) = \mathrm{Sym}_n(T^2)$ denotes the space of binary n-ic forms over a ring T, and an element $\gamma \in \mathrm{SL}_2(T)$ acts on $f \in U(T)$ via $\gamma f(x,y) = f((x,y)\gamma)$. Let $\Delta(f)$ denote the discriminant of a form $f \in U(T)$. Let $U(\mathbb{R})^{(r_2)}$ denote the set of binary n-ic forms with coefficients in $\mathbb{R}$ that have nonzero discriminant and r_2 pairs of complex conjugate roots for some fixed $r_2 \in \{0, \ldots, (n-1)/2\}$.

Definition 3.1
For each finite prime p, let $\Sigma_p \subset U(\mathbb{Z}_p) \setminus \{\Delta = 0\}$ be a nonempty open set whose boundary has measure 0, and let $\Sigma_\infty = U(\mathbb{R})^{(r_2)}$ for some such r_2. We say that a collection $\Sigma = (\Sigma_p)_p \cup \Sigma_\infty$ is *acceptable* if, for all large enough primes p, the set Σ_p contains all elements $f \in V(\mathbb{Z}_p)$ with $p^2 \nmid \Delta(f)$. We refer to each Σ_ν where ν is any finite or infinite place of $\mathbb{Q}$ as a *local specification* of Σ at ν. To a collection Σ, we associate a family $\mathcal{U}(\Sigma)$ of integral binary n-ic forms given by

$$\mathcal{U}(\Sigma) = \big\{f \in U(\mathbb{Z}) : f \in \Sigma_\nu \text{ for all places } \nu\big\},$$

and we say that $\mathcal{U}(\Sigma)$ is *acceptable* if Σ is acceptable.

Note that if Σ_p is $\mathrm{SL}_2(\mathbb{Z}_p)$-invariant for every prime p (the set Σ_∞ is automatically $\mathrm{SL}_2(\mathbb{R})$-invariant), then $\mathcal{U}(\Sigma)$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant. In this case, we say that such a collection Σ is SL_2-*invariant*. Additionally, for any $\mathcal{U}(\Sigma)$, note that there is a multisubset $\Sigma_H = \{R_f \mid f \in \mathcal{U}(\Sigma)\}$ inside $\mathfrak{R}_H$. Similarly, for any SL_2-invariant $\mathcal{U}(\Sigma)$, there is also a multisubset $\Sigma_J = \{R_{[f]} \mid [f] \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{U}(\Sigma)\}$. We say that a family Σ_H or Σ_J is *acceptable* if it is defined by an acceptable family $\mathcal{U}(\Sigma)$ of integral binary n-ic forms.

3.2. *Binary n-ic forms ordered by height*

In this section, we order real and integral binary n-ic forms by the following height function:

$$H(f_0x^n + \cdots + f_ny^n) := \max|f_i|. \tag{20}$$

For any subset S of $U(\mathbb{R})$ or $U(\mathbb{Z})$, we denote the set of elements in S having height less than X by $S_{H<X}$. For a subset S of $U(\mathbb{Z})$, we denote the subset of irreducible elements in S by S^{irr}. Asymptotics for the number of integral irreducible binary n-ic forms having square-free discriminant and bounded height is determined in [10]. The key ingredient in that result is a tail estimate on the number of integral binary n-ic forms having bounded height whose discriminants are divisible by p^2 for large primes p. Namely, let $W_p \subset U(\mathbb{Z})$ denote the set of integral binary n-ic forms with $p^2 \mid \Delta(f)$. Then the following tail estimate is proved in [10].

PROPOSITION 3.2
We have

$$\#\Big(\bigcup_{p>M} W_p\Big)_{H<X} = O\Big(\frac{X^{n+1}}{\sqrt{M}}\Big) + o(X^{n+1}).$$

The next theorem follows from Proposition 3.2 just as [8, Theorem 2.21] follows from [8, Theorem 2.13].

THEOREM 3.3
Let Σ be an acceptable collection of local specifications. Then we have

$$\#\mathcal{U}(\Sigma)^{\mathrm{irr}}_{H<X} = \mathrm{Vol}(\Sigma_{\infty,H<X})\prod_p \mathrm{Vol}(\Sigma_p) + o(X^{n+1}). \tag{21}$$

Note that since $\mathrm{Vol}(\Sigma_{\infty,H<X})$ grows like a nonzero constant times X^{n+1}, the error term in the right-hand side of (21) is indeed smaller than the main term.

3.3. $\mathrm{SL}_2(\mathbb{Z})$*-orbits on binary* n*-ic forms ordered by Julia invariant*

Every binary n-ic form with real coefficients whose leading coefficient a_0 is nonzero can be written as

$$f(x,y) = a_0(x-\alpha_1 y)\cdots(x-\alpha_n y),$$

with $\alpha_i \in \mathbb{C}$. For $t = (t_1,\ldots,t_n) \in \mathbb{R}^n$, consider the positive definite binary quadratic form

$$Q_t(x,y) = \sum_{i=1}^{n} t_i^2 (x-\alpha_i y)(x-\bar{\alpha}_i y).$$

Work of Julia [27] and Stoll and Cremona [34] shows that if t is chosen to minimize the quantity

$$\vartheta(f) = \frac{a_0^2 |\operatorname{Disc} Q_t|^{n/2}}{t_1^2\cdots t_n^2}, \tag{22}$$

then ϑ is an $\mathrm{SL}_2(\mathbb{R})$-invariant of f, that is, $\vartheta(f) = \vartheta(\gamma\cdot f)$ for any $\gamma \in \mathrm{SL}_2(\mathbb{R})$. We call ϑ the *Julia invariant* of the binary n-ic form $f(x,y)$. The Julia invariant is not a polynomial invariant, but it is homogeneous of degree 2, in the sense that $\vartheta(\lambda f) = \lambda^2\vartheta(f)$ for $\lambda \in \mathbb{R}^\times$. Indeed, the roots of f and λf are the same; when we replace f with λf, the a_0 in the right-hand side of (22) is replaced with $\lambda^2 a_0$ while the remaining quantities stay the same. In this section, we will order $\mathrm{SL}_2(\mathbb{Z})$-orbits $[f]$ of $U(\mathbb{Z})$ by the degree 1 invariant

$$J(f) = \sqrt{\vartheta(f)}. \tag{23}$$

Note that we may define the Julia invariant for forms f with leading coefficient 0 by using an $\mathrm{SL}_2(\mathbb{R})$-equivalent form with nonzero leading coefficient.

Asymptotics for the number of irreducible $\mathrm{SL}_2(\mathbb{Z})$-orbits on integral binary n-ic forms were recently computed by Bhargava and Yang [13]. The following theorem is a rewording of [13, Theorem 9].

THEOREM 3.4

Let n be a positive integer, and let $r_2 \in \{0,1,\ldots,\lfloor n/2\rfloor\}$. Let Σ be a collection of local specifications such that the family $\mathcal{U}(\Sigma)$ is defined by finitely many congruence conditions, and $\Sigma_\infty = U(\mathbb{R})^{(r_2)}$. Then there exists a constant c_{n,r_2}, depending only on n and r_2, such that

$$\#\big(\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{U}(\Sigma)^{\mathrm{irr}}_{J<X}\big) = c_{n,r_2}\prod_p \mathrm{Vol}(\Sigma_p)X^{n+1} + O(X^{n+1-\frac{2}{n}}). \tag{24}$$

To prove Theorem 3.4, the authors construct a fundamental domain F for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $U(\mathbb{R})^{(r_2)}$. This fundamental domain has the property that $F_{J<X} = XF_{J<1}$. Estimating the number of irreducible integral binary n-ic forms in $F_{J<X}$ is difficult because $F_{J<X}$ is not compact and has a cusp going to infinity. Using an averaging technique, they prove that the cuspidal region of $F_{J<X}$ contains negligibly many irreducible integral binary n-ic forms, while the noncuspidal region has negligibly many reducible binary n-ic forms. This allows them to prove that the left-hand side of (24) is well approximated by the volume of $F_{J<X}$, yielding the result. In fact, the constant $c_{n,k}$ in Theorem 3.4 is simply $\mathrm{Vol}(F_{J<1})$. We now prove the following theorem.

THEOREM 3.5

Let Σ be an acceptable SL_2*-invariant collection of local specifications. Then we have*

$$\begin{aligned}&\#\big(\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{U}(\Sigma)^{\mathrm{irr}}_{J<X}\big)\\ &\quad= \mathrm{Vol}\big(\mathrm{SL}_2(\mathbb{Z})\backslash\Sigma_{\infty,J<X}\big)\prod_p \mathrm{Vol}(\Sigma_p) + o(X^{n+1}).\end{aligned}$$

Proof

For every $\epsilon > 0$ there exists an acceptable collection $(\Sigma'_\nu)_\nu$ such that $\Sigma_\infty = \Sigma'_\infty$, $\Sigma_p \subset \Sigma'_p$ for each prime p, $\prod_p \mathrm{Vol}(\Sigma_p) \geq \prod_p \mathrm{Vol}(\Sigma'_p) - \epsilon$, and the set $\mathcal{U}(\Sigma')$ is defined by finitely many congruence conditions. From Theorem 3.4, we obtain

$$\begin{aligned}\#\big(\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{U}(\Sigma)^{\mathrm{irr}}_{J<X}\big) &\leq \#\big(\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{U}(\Sigma')^{\mathrm{irr}}_{J<X}\big)\\ &= \mathrm{Vol}\big(\mathrm{SL}_2(\mathbb{Z})\backslash\Sigma_{\infty,J<X}\big)\prod_p \mathrm{Vol}(\Sigma'_p) + o(X^{n+1})\\ &\leq \mathrm{Vol}\big(\mathrm{SL}_2(\mathbb{Z})\backslash\Sigma_{\infty,J<X}\big)\Big(\prod_p \mathrm{Vol}(\Sigma_p) + \epsilon\Big) + o(X^{n+1}).\end{aligned}$$

Letting ϵ tend to zero, we obtain the required upper bound on $\#(\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{U}(\Sigma)^{\mathrm{irr}}_{J<X})$.

To obtain the lower bound, we proceed as follows. For $\epsilon > 0$, we take sets $F^{(\epsilon)}_{J<1}$ to be a semialgebraic bounded subset of $F_{J<1}$ such that $\mathrm{Vol}(F^{(\epsilon)}_{J<1}) \geq (1-\epsilon)\,\mathrm{Vol}(F_{J<1})$. We denote $XF^{(\epsilon)}_{J<1}$ by $F^{(\epsilon)}_{J<X}$. Just as [8, Theorem 2.21] follows from [8, Theorem 2.13], we obtain from Proposition 3.2 the estimate

$$\#\big(F^{(\epsilon)}_{J<X} \cap \mathcal{U}(\Sigma)^{\mathrm{irr}}\big) = \mathrm{Vol}(F^{(\epsilon)}_{J<X})\prod_p \mathrm{Vol}(\Sigma_p) + o(X^{n+1}). \tag{25}$$

From the proof of [13, Theorem 9], we have the following estimate on the number of integral elements in the "cuspidal region":

$$\#\big((F_{J<X}\backslash F^{(\epsilon)}_{J<X})\cap\mathcal{U}(\Sigma)^{\mathrm{irr}}\big)\le\epsilon X^{n+1}+O(X^{n+1-\frac{2}{n}}).\tag{26}$$

Combining (25) and (26) yields the required lower bound on $\#(\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{U}(\Sigma)^{\mathrm{irr}}_{J<X})$ and completes the proof of Theorem 3.5. ☐

4. Counting orbits of pairs of $n\times n$ symmetric matrices

The main goal of this section is to determine asymptotics for the number of irreducible $\mathrm{SL}_n(\mathbb{Z})$-orbits of pairs of $n\times n$ symmetric matrices having bounded height and the number of irreducible $\mathrm{SL}_2(\mathbb{Z})\times\mathrm{SL}_n(\mathbb{Z})$-orbits of pairs of $n\times n$ symmetric matrices having bounded Julia invariant. We first construct fundamental domains for the action of $\mathrm{SL}_n(\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z})\times\mathrm{SL}_n(\mathbb{Z})$ on pairs of real $n\times n$ symmetric matrices. We then show that the cusps of these fundamental domains have a negligible number of irreducible integral points. Additionally, we show that the number of reducible integral points in the main body of these fundamental domains is also negligible. A theorem of Davenport [18, Main Theorem] allows us to conclude that the number of irreducible integral points of bounded height in the fundamental domain for the action of $\mathrm{SL}_n(\mathbb{Z})$ or the number of irreducible integer points of bounded Julia invariant in the fundamental domain for the action of $\mathrm{SL}_2\times\mathrm{SL}_n(\mathbb{Z})$ is asymptotically equal to the volumes of their respective main bodies.

Fix an odd integer $n\ge 3$, and let $m=(n-1)/2$. Recall that $V(T)=T^2\otimes\mathrm{Sym}_2(T^n)$ is the space of pairs of $n\times n$ symmetric matrices (A,B) over a ring T. The group $G(T):=\mathrm{SL}_2(T)\times\mathrm{SL}_n(T)$ acts on $V(T)$ via the action

$$(\gamma_2,\gamma_n)\cdot(A,B)=(\gamma_nA\gamma_n^t,\gamma_nB\gamma_n^t)\gamma_2^t\quad\text{for all }(\gamma_2,\gamma_n)\in G(T).\tag{27}$$

It is easy to verify that we have

$$\pi\big((\gamma_2,\gamma_n)\cdot(A,B)\big)=\gamma_2^*\big(\pi(A,B)\big)\quad\text{for all }(\gamma_2,\gamma_n)\in G(T),\tag{28}$$

where

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}^*:=\begin{pmatrix}a&-c\\b&-d\end{pmatrix}.$$

The space $V(\mathbb{R})$ inherits a height function H and Julia invariant J via π:

$$H(A,B):=H\big(\pi(A,B)\big),$$
$$J(A,B):=J\big(\pi(A,B)\big),$$

where H and J are defined on $U(\mathbb{R})$ as in Section 3. From (28), it follows that H is $\mathrm{SL}_n(\mathbb{R})$-invariant and J is $G(\mathbb{R})$-invariant on $V(\mathbb{R})$.

We say that an element $(A,B)\in V(\mathbb{Z})$ with $\pi(A,B)=f$ is *absolutely irreducible* if

(1) f corresponds an order in an S_n-field, and

(2) (A, B) is not reducible in the sense of Theorem 2.6.

We denote the set of absolutely irreducible elements in $V(\mathbb{Z})$ by $V(\mathbb{Z})^{\mathrm{irr}}$.

4.1. *Construction of fundamental domains*

For $0 \le r_2 \le m = (n-1)/2$, recall that $U(\mathbb{R})^{(r_2)}$ denotes the set of binary n-ic forms in $U(\mathbb{R})$ that have nonzero discriminant and r_2 distinct pairs of complex conjugate roots in $\mathbb{P}^1(\mathbb{C})$. Let $V(\mathbb{R})^{(r_2)}$ denote the set of elements in $V(\mathbb{R})$ whose image under π lies in $U(\mathbb{R})^{(r_2)}$. In this section, we construct fundamental domains for the actions of $\mathrm{SL}_n(\mathbb{Z})$ and $G(\mathbb{Z})$ on $V(\mathbb{R})^{(r_2)}$ for $0 \le r_2 \le m$.

Fundamental sets for the action of $\mathrm{SL}_n(\mathbb{R})$ *and* $G(\mathbb{R})$ *on* $V(\mathbb{R})^{(r_2)}$

Fix an integer r_2 with $0 \le r_2 \le m$, and let $r_1 = n - 2r_2$. For $f \in U(\mathbb{R})^{(r_2)}$, the $\mathbb{R}$-algebra R_f corresponding to f is isomorphic to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Corollary 2.16 states that the $\mathrm{SL}_n(\mathbb{R})$-orbits of $\pi^{-1}(f)$ are in bijection with elements $\delta \in (R_f^\times/R_f^{\times 2})_{N\equiv 1}$, which in turn is in natural bijection with the subset $\mathcal{T}(r_2) \subset \{\pm 1\}^{r_1} \times \{1\}^{r_2}$ of elements having an even number of -1 factors (independent of the choice of $f \in U(\mathbb{R})^{(r_2)}$). For an element $\delta \in \mathcal{T}(r_2)$, let $V(\mathbb{R})^{(r_2),\delta}$ denote the set of $v \in V(\mathbb{R})^{(r_2)}$ such that v corresponds to the pair $(R_{\pi(v)}, \delta)$ under the bijection of Theorem 2.13. It follows that for $f \in U(\mathbb{R})^{(r_2)}$ and $\delta \in \mathcal{T}(r_2)$, the set $\pi^{-1}(f) \cap V(\mathbb{R})^{(r_2),\delta}$ consists of a single $\mathrm{SL}_n(\mathbb{R})$-orbit. Therefore, to construct a fundamental domain for the action of $\mathrm{SL}_n(\mathbb{R})$ on $V(\mathbb{R})^{(r_2),\delta}$, it is enough to pick one element $v_f \in V(\mathbb{R})^{(r_2),\delta}$ for each $f \in U(\mathbb{R})^{(r_2)}$. However, we require our fundamental set to be semialgebraic in order to apply our geometry-of-numbers techniques.

Below, we give such a section $s_\delta : U(\mathbb{R})^{(r_2)} \to V(\mathbb{R})$ for general δ, which will be necessary for constructing the fundamental sets, but first we describe, for the case of $\delta = (1, 1, \dots, 1)$, the very pretty explicit section $e : U(T) \to V(T)$ of π for any ring T. When $T = \mathbb{R}$, it is easy to check that $e(f) \in V(\mathbb{R})^{(r_2),\delta}$ for $f \in U(\mathbb{R})^{(r_2)}$. For $n = 3$, the section e takes a binary cubic form $f(x, y) = f_0x^3 + f_1x^2y + f_2xy^2 + f_3y^3$ to the pair

$$\left(\begin{pmatrix} 0 & 0 & 1 \\ 0 & -f_0 & 0 \\ 1 & 0 & -f_2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & f_1 & 0 \\ 0 & 0 & f_3 \end{pmatrix}\right).$$

For $n = 5$, the map e sends a binary quintic form $f(x, y) = f_0x^5 + f_1x^4y + f_2x^3y^2 + f_3x^2y^3 + f_4xy^4 + f_5y^5$ to

$$\left(\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & f_0 & 0 & 0 \\ 0 & 1 & 0 & f_2 & 0 \\ 1 & 0 & 0 & 0 & f_4 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & -f_1 & 0 & 0 \\ 1 & 0 & 0 & -f_3 & 0 \\ 0 & 0 & 0 & 0 & -f_5 \end{pmatrix}\right).$$

For general n, a binary n-ic form $f(x,y) = f_0x^n + f_1x^{n-1}y + f_2x^{n-2}y^2 + \cdots + f_ny^n$ is mapped under e to $((a_{ij}),(b_{ij}))$, where:

- $a_{k,n-k} = 1$ for $1 \le k < \frac{n-1}{2}$ or $\frac{n-1}{2} < k < n$,
- $b_{k,n-1-k} = 1$ for $1 \le k < n$,
- $a_{\frac{n-1}{2}+k,\frac{n-1}{2}+k} = (-1)^{\frac{n-1}{2}} f_{2k}$ for $0 \le k \le \frac{n-1}{2}$,
- $b_{\frac{n-1}{2}+k,\frac{n-1}{2}+k} = (-1)^{\frac{n+1}{2}} f_{2k+1}$ for $0 \le k \le \frac{n-1}{2}$,
- $a_{ij} = 0$ otherwise,
- $(b_{ij} = 0)$ otherwise.

We now handle the case of general δ. For a fixed $\delta \in \mathcal{T}(r_2)$ and an element $f = f_0x^n + \cdots + f_ny^n \in U(\mathbb{R})^{(r_2)}$ with $f_0 \neq 0$, consider the pair (R_f, δ). Given the basis $\langle 1, \theta, \ldots, \theta^{n-1}\rangle$ for R_f, the corresponding pair (A, B) may be written explicitly using (9) and (10). From the definitions of θ and δ, it follows that $\phi(\theta^i \otimes \theta^j)$ may be written as polynomials of degree less than n in θ, whose coefficients are polynomials in the f_i and $1/f_0$. Since ζ_{n-2} and ζ_{n-1} are polynomials in θ both with leading coefficient f_0, the coefficients of A and B are polynomials in the f_i and $1/f_0$. We define the function $s_\delta : U(\mathbb{R})^{(r_2)} \to V(\mathbb{R})$ by sending such a binary n-ic form f to this pair (A, B).

We now have the following lemma.

LEMMA 4.1
Let $S \subset U(\mathbb{R})$ be a compact semialgebraic set that does not contain zero. Then there exists a finite subset $T \subset \mathrm{SO}_2(\mathbb{R})$ and semialgebraic subsets $S_\tau \subset S$ for each $\tau \in T$ such that the leading coefficients of $\tau \cdot f$ are bounded away from zero independent of $f \in S_\tau$ and such that the union of the S_τ's is S.

Proof
The set $\tilde{S} = S \times \{(x,y) : x^2 + y^2 = 1\} \subset U(\mathbb{R}) \times \mathbb{R}^2$ is semialgebraic. The function $S \to \mathbb{R}_{\ge 0}$ given by

$$f \mapsto \max_{x^2+y^2=1} \left|f(x,y)\right|$$

is continuous and nonzero. Hence its image is bounded away from zero by some $\epsilon > 0$. Therefore, the set

$$S_1 := \left\{\left(f,(x,y)\right) : f \in S, (x,y) \in \mathbb{R}^2, x^2 + y^2 = 1, \left|f(x,y)\right| > \epsilon/2\right\}$$

is semialgebraic and its projection to S is all of S. Given an element $\lambda = (x, y) \in \mathbb{R}^2$ with $x^2 + y^2 = 1$, let S_λ denote the set of elements f in S such that $(f, \lambda) \in S_1$. Since the projections of semialgebraic sets are semialgebraic, it follows that S_λ is semialgebraic. Since S is compact, and the S_λ are open inside S, there exists a finite subset T' of $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ such that the union of S_λ over all λ in this finite set is S. Given $\lambda = (x, y)$, choose $\tau \in \mathrm{SO}_2(\mathbb{R})$ to be the matrix $\left(\begin{smallmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{smallmatrix}\right)$, where $\cos t = x$ and $\sin t = y$. The leading coefficient of $\tau \cdot f$ is $(\tau \cdot f)(1, 0) = f(x, y) > \epsilon/2$. The lemma follows by taking T to be the finite set of matrices τ in $\mathrm{SO}_2(\mathbb{R})$ corresponding to the finite set T' of pairs $\lambda = (x, y)$ in $\mathbb{R}^2$, and setting S_τ to be S_λ, for τ corresponding to λ. □

We can clearly choose the sets S_τ to be disjoint in the above lemma. The set $S = U(\mathbb{R})_{H=1}$ satisfies the conditions of the above lemma. For a fixed r_2, we may write $U(\mathbb{R})^{(r_2)}_{H=1}$ as a finite disjoint union of the sets $S^{(r_2)}_\tau = S_\tau \cap U(\mathbb{R})^{(r_2)}$. We now take our fundamental set for the action of $\mathrm{SL}_n(\mathbb{R})$ on $V(\mathbb{R})^{(r_2),\delta}$ to be the finite union

$$\mathcal{R}^{(r_2),\delta}_H := \bigcup_\tau \mathbb{R}_{>0} \cdot (\tau^*)^{-1} s_\delta (\tau \cdot S^{(r_2)}_\tau).$$

We define a fundamental set $\mathcal{R}^{(r_2),\delta}_J$ for the action of $G(\mathbb{R})$ on $V(\mathbb{R})^{(r_2),\delta}$ in exactly the same way by considering the set $S = L_n$, where L_n is constructed in [13, Section 3] to be a semialgebraic bounded fundamental set for the action of $\mathrm{SL}_2(\mathbb{R})$ on the set of elements in $U(\mathbb{R})$ having Julia invariant 1. Let $\mathcal{R}^{(r_2),\delta}_H(X)$ (resp., $\mathcal{R}^{(r_2),\delta}_J(X)$) denote the set of elements in $\mathcal{R}^{(r_2),\delta}_H$ (resp., $\mathcal{R}^{(r_2),\delta}_J$) having height (resp., Julia invariant) bounded by X. The sets $(\tau^*)^{-1} s_\delta(\tau \cdot S^{(r_2)}_\tau)$ are bounded for $S = U(\mathbb{R})_{H=1}$ and $S = L_n$ because every $f \in \tau \cdot S_\tau$ has bounded coefficients and has leading coefficient bounded away from zero. Since both height and Julia invariant on $V(\mathbb{R})$ have degree n, the coefficients of elements (A, B) in $\mathcal{R}^{(r_2),\delta}_H(X)$ and $\mathcal{R}^{(r_2),\delta}_J(X)$ are bounded by $O(X^{1/n})$, where the implied constant is independent of (A, B).

Fundamental domains for $\mathrm{SL}_n(\mathbb{Z})\backslash \mathrm{SL}_n(\mathbb{R})$ *and* $G(\mathbb{Z})\backslash G(\mathbb{R})$

Let $\mathrm{SL}_n(\mathbb{R}) = N_n T_n K_n$ be the Iwasawa decomposition of $\mathrm{SL}_n(\mathbb{R})$, where $N_n \subset \mathrm{SL}_n(\mathbb{R})$ denotes the set of unipotent lower triangular matrices, $T_n \subset \mathrm{SL}_n(\mathbb{R})$ denotes the set of diagonal matrices, and $K_n = \mathrm{SO}_n(\mathbb{R}) \subset \mathrm{SL}_n(\mathbb{R})$ is the maximal compact subgroup. Let $\mathfrak{S}_H$ be a Siegel domain in $\mathrm{SL}_n(\mathbb{R})$ defined as

$$\mathfrak{S}_H := N'_n T'_n K_n,$$

where $N'_n \subset N_n$ is the set of elements in N_n whose coefficients are bounded by 1 in absolute value and $T'_n \subset T_n$ is given by

$$T_n' := \{\operatorname{diag}(t_1^{-1}, t_2^{-1}, \ldots, t_n^{-1}) : t_1/t_2 > c, \ldots, t_{n-1}/t_n > c\},$$

for some constant $c > 0$ that is sufficiently small to ensure the existence of a fundamental domain $\mathcal{F}_H$ for the action of $\mathrm{SL}_n(\mathbb{Z})$ on $\mathrm{SL}_n(\mathbb{R})$ that is contained in $\mathfrak{S}_H$. Next, we pick $N_2' \subset N$ to be the set of elements whose coefficients are bounded by 1 in absolute value, and we pick $T_2' \subset T_2$ to be the set

$$T_2' := \{\operatorname{diag}(t^{-1}, t) : t > 1/4\}.$$

Let

$$\mathfrak{S}_J := (N_2', N_n')(T_2', T_n')(K_2, K_n)$$

be a Siegel domain. Then $\mathfrak{S}_J$ contains a fundamental domain $\mathcal{F}_J$ for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$.

Fundamental domains for the action of $\mathrm{SL}_n(\mathbb{Z})$ *on* $V(\mathbb{R})^{(r_2)}$

The size of the stabilizer in $\mathrm{SL}_n(\mathbb{R})$ of $v \in V(\mathbb{R})^{(r_2,\delta)}$ can be computed from Corollary 2.15. This size depends only on r_2 and we denote it by $\sigma(r_2)$. It is well known that the size of the stabilizer in $\mathrm{SL}_2(\mathbb{R})$ of a generic element $f \in U(\mathbb{R})^{(r_2)}$ is 3 if $n = 3$ and $r_2 = 0$, and 1 otherwise. It follows that the size of the stabilizer in $G(\mathbb{R})$ of a generic element in $V(\mathbb{R})^{(r_2),\delta}$ is $\sigma'(r_2)$, where $\sigma'(r_2) = 3\sigma(r_2)$ if $n = 3$ and $r_2 = 0$, and $\sigma'(r_2) = \sigma(r_2)$ otherwise. By arguments identical to those in [8, Section 2.1], we see that $\mathcal{F}_H \cdot \mathcal{R}_H^{(r_2),\delta}$ is a $\sigma(r_2)$-fold cover of a fundamental domain for the action of $\mathrm{SL}_n(\mathbb{Z})$ on $V(\mathbb{R})^{(r_2),\delta}$ and that $\mathcal{F}_J \cdot \mathcal{R}_J^{(r_2),\delta}$ is a $\sigma'(r_2)$-fold cover of a fundamental domain for the action of $G(\mathbb{Z})$ on $V(\mathbb{R})^{(r_2),\delta}$, where $\mathcal{F}_H \cdot \mathcal{R}_H^{(r_2),\delta}$ and $\mathcal{F}_J \cdot \mathcal{R}_J^{(r_2),\delta}$ are regarded as multisets. More precisely, the $\mathrm{SL}_n(\mathbb{Z})$-orbit of any $v \in V(\mathbb{R})^{(r_2),\delta}$ is represented $\#\mathrm{Stab}_{\mathrm{SL}_n(\mathbb{R})}(v)/\#\mathrm{Stab}_{\mathrm{SL}_n(\mathbb{Z})}(v)$ times in $\mathcal{F}_H \cdot \mathcal{R}_H^{(r_2),\delta}$, with the analogous statement also holding for the multiset $\mathcal{F}_J \cdot \mathcal{R}_J^{(r_2),\delta}$.

For an $\mathrm{SL}_n(\mathbb{Z})$-invariant set $S \subset V(\mathbb{Z})^{(r_2),\delta} := V(\mathbb{R})^{(r_2),\delta} \cap V(\mathbb{Z})$, let $N_H(S; X)$ denote the number of absolutely irreducible $\mathrm{SL}_n(\mathbb{Z})$-orbits on S that have height bounded by X. For a $G(\mathbb{Z})$-invariant set $S' \subset V(\mathbb{Z})^{(r_2),\delta}$, let $N_J(S'; X)$ denote the number of absolutely irreducible $G(\mathbb{Z})$-orbits on S' whose Julia invariant is bounded by X. Let $v \in V(\mathbb{Z})$ be absolutely irreducible with resolvent form f. Then f corresponds to an order $\mathcal{O}$ in an S_n-number field and $\mathcal{O}^\times[2]_{N\equiv 1}$ is trivial. Furthermore, f has trivial stabilizer in $\mathrm{SL}_2(\mathbb{Z})$ since $\mathrm{Aut}(\mathcal{O})$ is trivial. Therefore, v has trivial stabilizer in $\mathrm{SL}_n(\mathbb{Z})$ and $G(\mathbb{Z})$. For any set $L \subset V(\mathbb{Z})$, let L^{irr} denote the set of absolutely irreducible elements in L. Let $\mathcal{R}_H^{(r_2),\delta}(X)$ (resp., $\mathcal{R}_J^{(r_2),\delta}(X)$) denote the set of elements in $\mathcal{R}_H^{(r_2)}$ (resp., $\mathcal{R}_J^{(r_2)}$) having height (resp., Julia invariant) bounded by X. Then we have the following.

PROPOSITION 4.2
Let notation be as above. We have

$$\begin{aligned} N_H(S;X) &= \frac{1}{\sigma(r_2)}\#\{\mathcal{F}\mathcal{R}_H^{(r_2),\delta}(X)\cap S^{\mathrm{irr}}\},\\ N_J(S';X) &= \frac{1}{\sigma'(r_2)}\#\{\mathcal{F}\mathcal{R}_J^{(r_2),\delta}(X)\cap S'^{\mathrm{irr}}\}. \end{aligned} \tag{29}$$

4.2. Averaging and cutting off the cusp
Let G_0 (resp., G_0') be a bounded open nonempty K_n-invariant (resp., $K_2\times K_n$-invariant) set in $\mathrm{SL}_n(\mathbb{R})$ (resp., $G(\mathbb{R})$). We abuse notation and refer to Haar measures in both groups $\mathrm{SL}_n(\mathbb{R})$ and $G(\mathbb{R})$ by $\mathrm{d}h$. From Proposition 4.2 and by an argument identical to the proof of [8, Theorem 2.5], we obtain

$$\begin{aligned} N_H(S;X) &= \frac{1}{\sigma(r_2)\operatorname{Vol}(G_0)}\int_{h\in\mathcal{F}_H}\#\{hG_0\cdot\mathcal{R}_H^{(r_2),\delta}(X)\cap S^{\mathrm{irr}}\}\,\mathrm{d}h,\\ N_J(S';X) &= \frac{1}{\sigma'(r_2)\operatorname{Vol}(G_0')}\int_{h\in\mathcal{F}_J}\#\{hG_0'\cdot\mathcal{R}_J^{(r_2),\delta}(X)\cap S'^{\mathrm{irr}}\}\,\mathrm{d}h, \end{aligned} \tag{30}$$

where the volumes of G_0 and G_0' are computed with respect to $\mathrm{d}h$. We use (30) to define $N_H(S;X)$ (resp., $N_J(S';X)$) even when S (resp., S') is not $\mathrm{SL}_n(\mathbb{Z})$-invariant (resp., $G(\mathbb{Z})$-invariant). Let $\mathcal{F}_H'\subset\mathcal{F}_H$ and $\mathcal{F}_J'\subset\mathcal{F}_J$ denote the sets of elements $\gamma\in\mathcal{F}_H$ and $\gamma\in\mathcal{F}_J$ such that $|a_{11}(v)|<1$ for every element $v\in\gamma\cdot G_0\mathcal{R}_H^{(r_2),\delta}(X)$ and $v\in\gamma\cdot G_0'\mathcal{R}_J^{(r_2),\delta}(X)$, respectively. We will refer to the integrals of the integrands in (30) over $\mathcal{F}_H'$ and $\mathcal{F}_J'$ as the "cuspidal" part of the integral, and to the integrals over $\mathcal{F}_H\setminus\mathcal{F}_H'$ and $\mathcal{F}_J\setminus\mathcal{F}_J'$ as the "main body" of the integral.

Absolutely irreducible points in the cusp
We will prove that the number of absolutely irreducible integral points in the cusp is negligible.

PROPOSITION 4.3
We have

$$\int_{h\in\mathcal{F}_H'}\#\{hG_0\cdot\mathcal{R}_H^{(r_2),\delta}(X)\cap V(\mathbb{Z})^{\mathrm{irr}}\}\,\mathrm{d}h = O(X^{n+1-\frac{1}{n}}),$$
$$\int_{h\in\mathcal{F}_J'}\#\{hG_0'\cdot\mathcal{R}_J^{(r_2),\delta}(X)\cap V(\mathbb{Z})^{\mathrm{irr}}\}\,\mathrm{d}h = O(X^{n+1-\frac{1}{n}}).$$

First, we list sufficient conditions to guarantee that an element $(A,B)\in V(\mathbb{Z})$ is not absolutely irreducible.

LEMMA 4.4
Let $(A,B) \in V(\mathbb{Z})$ be such that all the variables in one of the following sets vanish:
(a) $\{a_{ij}, b_{ij} : 1 \le i \le k, 1 \le j \le n-k\}$ *for some* $1 \le k \le n-1$*;*
(b) $\{a_{ij}, b_{ij} : 1 \le i, j \le (n-1)/2\}$.
Then (A,B) is not absolutely irreducible.

Proof
If (A,B) satisfies condition (a), then it is easy to see that the binary n-ic invariant of (A,B) has a repeated factor over $\mathbb{Q}$. Thus, the discriminant of the form vanishes. If (A,B) satisfies condition (b), then clearly the quadratic forms A and B have a common isotropic subspace of dimension $(n-1)/2$. In either case, the pair (A,B) is not absolutely irreducible. □

Recall that the condition for $t = (t_1^{-1}, \dots, t_n^{-1})$ to be an element of T_n' is that $t_i/t_{i+1} > c$ for $1 \le i \le n-1$. To simplify this condition, we use a change of variables. Let $s_i = t_i/t_{i+1}$ for $1 \le i \le n-1$. Then $s = (s_1, \dots, s_{n-1})$ is contained in T' if and only if $s_i > c$ for each i. The action of the torus $T_2 \times T_n$ of $G(\mathbb{R})$ on $V(\mathbb{R})$ multiplies each coefficient by a monomial in $t, s_1, \dots, s_{n-1}$. We denote the set of coefficients of $V(\mathbb{R})$ by Var; we have

$$\mathrm{Var} := \{a_{ij}, b_{ij} : 1 \le i \le j \le n\}.$$

To each variable c_{ij} in Var, we associate two weights: first, the monomial $w_H(c_{ij})$ in the s_i by which the action of T_n scales c_{ij}, and second, the monomial $w_J(c_{ij})$ in t and the s_i by which the action of $T_2 \times T_n$ scales c_{ij}. We multiplicatively extend the function w_H and w_J to products of integral powers of elements in Var. We define a partial ordering on Var by setting $\alpha_1 \lesssim_H \alpha_2$ (resp., $\alpha_1 \lesssim_J \alpha_2$) whenever $w_H(\alpha_2)/w_H(\alpha_1)$ (resp., $w_J(\alpha_2)/w_J(\alpha_1)$) is a product of nonnegative powers of s_i for each i (resp., of t and s_i for each i). The variable a_{11} has minimal weight under both these partial orderings. For a subset $\mathrm{Var}' \subset \mathrm{Var}$, let $V(\mathbb{Z})(\mathrm{Var}')$ denote the set of $v \in V(\mathbb{Z})$ such that $\alpha(v) = 0$ for $\alpha \in \mathrm{Var}'$. Then we have the following immediate consequence of Lemma 4.4.

LEMMA 4.5
Let $\mathrm{Var}' \subset \mathrm{Var}$ be a set that is closed under one of the partial orderings $\lesssim_H$ and $\lesssim_J$. If $V(\mathbb{Z})(\mathrm{Var}')^{\mathrm{irr}}$ is nonempty, then Var' must be contained in the set

$$\mathrm{Var}_0 := \{a_{ij} \in \mathrm{Var} : i + j \le n\} \\ \cup \{b_{ij} \in \mathrm{Var} : i + j \le n-1\} \setminus \{b_{mm}\},$$

where $m = (n-1)/2$.

Proof of Proposition 4.3

By the arguments of [9, Section 3], it suffices to display the following data in order to prove the part of Proposition 4.3 regarding the height (resp., the Julia invariant): a function $\psi : \mathrm{Var}_0 \backslash a_{11} \to \mathrm{Var} \backslash \mathrm{Var}_0$ such that

(1) $\alpha \lesssim_H \psi(\alpha)\ \forall \alpha \in \mathrm{Var}_0 \backslash a_{11}$ (resp. $\alpha \lesssim_J \psi(\alpha)\ \forall \alpha \in \mathrm{Var}_0 \backslash a_{11}$), and

(2) $w_H(\prod_{\alpha\in \mathrm{Var}_0} \alpha^{-1}\psi(\alpha)) \cdot h_H$ (resp. $w_J(\prod_{\alpha\in \mathrm{Var}_0} \alpha^{-1}\psi(\alpha)) \cdot h_J$) is a product of negative powers of the s_i (resp., negative powers of t and the s_i),

where $\psi(a_{11})$ is defined to be 1, and where h_H and h_J are factors arising from the Haar measures of $\mathrm{SL}_n(\mathbb{R})$ and $G(\mathbb{R})$ and are given by

$$h_H := \prod_{k=1}^{n-1} s_k^{-nk(n-k)} \qquad \text{and} \qquad h_J := t^{-2} \prod_{k=1}^{n-1} s_k^{-nk(n-k)}.$$

First note that such a function ψ satisfying the required conditions regarding the Julia invariant automatically satisfies the required conditions regarding the height (since $\alpha \lesssim_J \beta$ implies $\alpha \lesssim_H \beta$). We define ψ as follows:

$$\begin{aligned} \psi(a_{ij}) &:= \begin{cases} a_{1n} & \text{for } i = 1, \\ a_{i(n-i+1)} & \text{for } i > 1 \text{ and } j \neq m, \\ a_{(m+1)(m+1)} & \text{for } i > 1 \text{ and } j = m, \end{cases} \\ \psi(b_{ij}) &:= \begin{cases} b_{j(n-j)} & \text{for } j < m, \\ b_{mm} & \text{for } j = m, \\ b_{(n-j-1)(j+1)} & \text{for } j > m. \end{cases} \end{aligned} \tag{31}$$

The function ψ clearly satisfies the first of the two required conditions. From an elementary computation, we see that

$$w_J\Big(\prod_{\alpha\in \mathrm{Var}_0} \alpha^{-1}\psi(\alpha)\Big) \cdot h_J = t^{-1} \prod_{k=1}^{m} s_k^{-2k} \prod_{k=m+1}^{n-1} s_k^{-2(k-m)+1}.$$

This concludes the proof of Proposition 4.3. ☐

Reducible points in the main body

We say that an element $v \in V(\mathbb{Z})$ is *bad* if v is not absolutely irreducible. Denote the set of bad elements in $V(\mathbb{Z})$ by $V(\mathbb{Z})^{\mathrm{bad}}$. We have the following theorem proving that the number of bad elements in the main body is negligible.

PROPOSITION 4.6

We have

$$\int_{h\in\mathcal{F}_H\backslash\mathcal{F}'_H} \#\{hG_0\cdot\mathcal{R}_H^{(r_2),\delta}(X)\cap V(\mathbb{Z})^{\mathrm{bad}}\}\,\mathrm{d}h = o(X^{n+1}),$$

$$\int_{h\in\mathcal{F}_J\backslash\mathcal{F}'_J} \#\{hG'_0\cdot\mathcal{R}_J^{(r_2),\delta}(X)\cap V(\mathbb{Z})^{\mathrm{bad}}\}\,\mathrm{d}h = o(X^{n+1}).$$

Proof

For an integer k with $2\le k\le n$, let $V(\mathbb{Z})^{\neq k}$ denote the set of elements $v\in V(\mathbb{Z})$ such that, for each prime p, the reduction modulo p of the resolvent of v does *not* factor into a product of an irreducible degree k factor and $n-k$ linear factors. We claim that if the resolvent f of an element $v\in V(\mathbb{Z})$ does not correspond to an order in an S_n-field, then v belongs to $V(\mathbb{Z})^{\neq k}$ for some k. Indeed, if v lies in the complement of $V(\mathbb{Z})^{\neq n}$, then the reduction modulo p of f is irreducible for some prime p, implying that f is irreducible and hence R_f is an order. Furthermore, the Galois group of the Galois closure of the fraction field of R_f contains a k-cycle for each k, implying that this Galois group is S_n. Hence we may write

$$V(\mathbb{Z})^{\mathrm{bad}} = \Big(\bigcup V(\mathbb{Z})^{\neq k}\Big)\cup V(\mathbb{Z})^{\mathrm{red}},$$

where $V(\mathbb{Z})^{\mathrm{red}}$ denotes the set of elements that are reducible in the sense of Theorem 2.6.

For each prime p, let $V(\mathbb{F}_p)^{=k}$ denote the set of elements whose cubic resolvents factor into a product of a degree k irreducible factor and $n-k$ distinct linear factors. Let $V(\mathbb{F}_p)^{\mathrm{irr}}$ denote the set of elements in $v\in V(\mathbb{F}_p)$ such that every lift $\tilde{v}\in V(\mathbb{Z})$ is not reducible in the sense of Theorem 2.6. Let $V(\mathbb{F}_p)^{\mathrm{nostab}}$ denote the set of elements which have trivial stabilizer in $G(\mathbb{F}_p)$. Then, from [9, Section 3], it suffices to prove the following estimates:

$$\#V(\mathbb{F}_p)^{=k}\gg\#V(\mathbb{F}_p),\qquad\text{and}\qquad\#V(\mathbb{F}_p)^{\mathrm{irr}}\gg\#V(\mathbb{F}_p).\tag{32}$$

Let $U(\mathbb{F}_p)^{=k}$ denote the set of binary n-ic forms that factor into a degree k irreducible polynomial and $n-k$ distinct linear factors. For every element $f\in U(\mathbb{F}_p)^{=k}$, the algebra R_f is isomorphic to a product of a degree k extension of $\mathbb{F}_p$ and $n-k$ copies of $\mathbb{F}_p$. Therefore, the stabilizer in $\mathrm{SL}_n(\mathbb{F}_p)$ of every element $v\in V(\mathbb{F}_p)^{=k}$ is independent of v and p. Every lift in $U(\mathbb{F}_p)^{=k}$ has at least one lift to $V(\mathbb{F}_p)^{=k}$ (corresponding to $\delta=1$). It follows that

$$\#V(\mathbb{F}_p)^{=k}\gg\#U(\mathbb{F}_p)^{=k}\cdot\#\mathrm{SL}_n(\mathbb{F}_p)\gg\#V(\mathbb{F}_p),$$

as desired.

The proof of the inequality (32) is similar. It follows from the observation that every element in $V(\mathbb{F}_p)^{=n}$ that corresponds to a nonidentity element in $\mathbb{F}_{p^n}^\times/(\mathbb{F}_{p^n}^\times)^2_{N\equiv1}$, under the bijection of Corollary 2.16, belongs to $V(\mathbb{F}_p)^{\mathrm{irr}}$. □

Absolutely irreducible points in the main body

Let $L \subset V(\mathbb{Z})$ be a lattice or a translate of a lattice in $V(\mathbb{R})$, and let $L^{(r_2),\delta}$ denote $L \cap V(\mathbb{Z})^{(r_2),\delta}$. We have already proved that the number of irreducible integral points in the cusp is negligible and that the number of reducible integral points in the main body is negligible. Therefore, from (30), Proposition 4.3, and Proposition 4.6, we have

$$\begin{aligned} N_H(L^{(r_2),\delta}, X) &= \frac{1}{\sigma(r_2)\operatorname{Vol}(G_0)} \\ &\quad \times \int_{h \in \mathcal{F}_H \setminus \mathcal{F}'_H} \#\big\{hG_0 \cdot \mathcal{R}_H^{(r_2),\delta}(X) \cap L\big\}\,\mathrm{d}h + o(X), \\ N_J(L^{(r_2),\delta}, X) &= \frac{1}{\sigma'(r_2)\operatorname{Vol}(G'_0)} \\ &\quad \times \int_{h \in \mathcal{F}_J \setminus \mathcal{F}'_J} \#\big\{hG'_0 \cdot \mathcal{R}_J^{(r_2),\delta}(X) \cap L\big\}\,\mathrm{d}h + o(X). \end{aligned}$$

To estimate the number of lattice points in $hG_0 \cdot \mathcal{R}_H^{(r_2),\delta}(X)$ and $hG'_0 \cdot \mathcal{R}_J^{(r_2),\delta}(X)$, we have the following result of Davenport [18, Main Theorem].

PROPOSITION 4.7

Let $\mathcal{R}$ be a bounded, semialgebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m, defined by at most k polynomial inequalities each having degree at most ℓ. Then the number of integral lattice points (*counted with multiplicity*) *contained in the region $\mathcal{R}$ is*

$$\operatorname{Vol}(\mathcal{R}) + O\big(\max\big\{\operatorname{Vol}(\bar{\mathcal{R}}), 1\big\}\big),$$

where $\operatorname{Vol}(\bar{\mathcal{R}})$ *denotes the greatest d-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $n-d$ coordinates to zero, where d takes all values from* 1 *to $n-1$. The implied constant in the second summand depends only on n, m, k, and ℓ.*

The coefficient a_{11} has minimal weight among all the coefficients. Furthermore, for $h \in \mathcal{F}_H \setminus \mathcal{F}'_H$, the volume of the projection of $hG_0 \cdot \mathcal{R}^{(r_2)}(X)$ onto the a_{11}-coordinate is bounded away from zero by the definition of $\mathcal{F}'_H$. Therefore, for $h \in \mathcal{F}_H \setminus \mathcal{F}'_H$, all proper projections of $hG_0 \cdot \mathcal{R}^{(r_2)}(X)$ are bounded by a constant times its projection onto the $a_{11} = 0$ hyperplane. Proposition 4.7 thus implies that

$$\begin{aligned} &N_H(L^{(r_2),\delta}, X) \\ &\quad = \frac{1}{\sigma(r_2)\operatorname{Vol}(G_0)} \int_{h \in (\mathcal{F}_H \setminus \mathcal{F}'_H)} \#\big\{hG_0 \cdot \mathcal{R}_H^{(r_2),\delta}(X) \cap L\big\}\,\mathrm{d}h + o(X^{n+1}) \end{aligned}$$

$$= \frac{1}{\sigma(r_2)\,\mathrm{Vol}(G_0)} \int_{h\in(\mathcal{F}\setminus\mathcal{F}')} \mathrm{Vol}_L\big(hG_0\cdot\mathcal{R}_H^{(r_2),\delta}(X)\big)\,\mathrm{d}h + o(X^{n+1})$$

$$= \frac{1}{\sigma(r_2)\,\mathrm{Vol}(G_0)} \mathrm{Vol}(\mathcal{F}_H)\,\mathrm{Vol}_L\big(G_0\cdot\mathcal{R}_H^{(r_2),\delta}(X)\big) + o(X^{n+1})$$

$$= \frac{1}{\sigma(r_2)} \mathrm{Vol}_L\big(\mathcal{F}_H\cdot\mathcal{R}_H^{(r_2),\delta}(X)\big) + o(X^{n+1}),$$

where the volume Vol_L of sets in $V(\mathbb{R})$ is computed with respect to the Euclidean measure on $V(\mathbb{R})$ normalized so that L has covolume 1, and where the third equality follows since $\mathrm{Vol}(\mathcal{F}')$ tends to zero as X tends to infinity, and $\mathrm{Vol}_H(hG_0\cdot\mathcal{R}^{(r_2)}(X))$ is independent of h, and the final equality follows from the Jacobian change of variables in Theorem 6.3.

An identical argument yields the analogous estimate for $N_J(L^{(r_2),\delta},X)$. Let L_p denote the closure of L in $V(\mathbb{Z}_p)$. Then for measurable sets B in $V(\mathbb{R})$, we have

$$\mathrm{Vol}_L(B) = \mathrm{Vol}(B)\cdot\mathrm{Vol}(L_p),$$

where $\mathrm{Vol}(B)$ is computed with respect to the Euclidean measure in $V(\mathbb{R})$ normalized so that $V(\mathbb{Z})$ has covolume 1, and the volumes of $L\subset V(\mathbb{Z}_p)$ are computed with respect to the Haar measure on $V(\mathbb{Z}_p)$ normalized so that $V(\mathbb{Z}_p)$ has volume 1. We thus have the following theorem.

THEOREM 4.8
Let notation be as above. Then we have

$$N_H(L^{(r_2),\delta},X) = \frac{1}{\sigma(r_2)} \mathrm{Vol}\big(\mathcal{F}_H\cdot\mathcal{R}_H^{(r_2),\delta}(X)\big)\prod_p \mathrm{Vol}(L_p) + o(X^{n+1}),$$

$$N_J(L^{(r_2),\delta},X) = \frac{1}{\sigma'(r_2)} \mathrm{Vol}\big(\mathcal{F}_J\cdot\mathcal{R}_J^{(r_2),\delta}(X)\big)\prod_p \mathrm{Vol}(L_p) + o(X^{n+1}).$$

Remark 4.9
Using the Selberg sieve identically as in [32, Section 3], we may improve the error term in Proposition 4.6, and thus in Theorem 4.8, to $O(X^{n+1-\frac{1}{5n}})$. However, this additional saving will not be necessary for the results in this article.

5. Sieving to projective elements and acceptable sets

In this section, we first determine asymptotics for $\mathrm{SL}_n(\mathbb{Z})$-orbits and $G(\mathbb{Z})$-orbits on certain families having bounded height. Second, we determine asymptotics for $\mathrm{SL}_n(\mathbb{Z})$-orbits and $G(\mathbb{Z})$-orbits on acceptable sets conditional on a tail estimate. This tail estimate is unknown for $n \geq 5$, but is known when $n = 3$ (see [2, Proposition 23]). We begin by describing the very large and acceptable families we study.

For each prime p, let $\Lambda_p \subset V(\mathbb{Z}_p) \setminus \{\Delta = 0\}$ be a nonempty open set whose boundary has measure 0. Let Λ_∞ denote $V(\mathbb{R})^{(r_2),\delta}$ for some integer r_2 with $0 \leq r_2 \leq (n-1)/2$ and some $\delta \in \{\pm 1\}^{n-2r_2} \times \{1\}^{r_2}$. To a collection $\Lambda = (\Lambda_\nu)_\nu$ of these local specifications, we associate the set

$$\mathcal{V}(\Lambda) := \big\{ v \in V(\mathbb{Z}) : v \in \Lambda_\nu \text{ for all } \nu \big\}.$$

We say that the collection $\Lambda = (\Lambda_\nu)_\nu$ is *very large* (resp., *acceptable*) if, for all large enough primes p, the set Λ_p contains all elements $v \in V(\mathbb{Z}_p)$ such that v is projective and the invariant form f of v is primitive; that is, the coefficients of f are relatively prime (resp., $p^2 \nmid \Delta(v)$). We say that $\mathcal{V}(\Lambda)$ is *very large* or *acceptable* if Λ is also very large or acceptable.

5.1. *Sieving to projective elements*

We define $V(\mathbb{Z}_p)^{\text{proj}}$ to be the set of elements $(A, B) \in V(\mathbb{Z}_p)$ whose binary n-ic invariants are not divisible by p and correspond to a pair (I, δ) such that $I^2 = (\delta)$. Then

$$V(\mathbb{Z})^{(r_2),\text{proj}} = V(\mathbb{Z})^{(r_2)} \cap \Big(\bigcap_p V(\mathbb{Z}_p)^{\text{proj}} \Big).$$

For a prime p, let W_p now denote the set of elements in $V(\mathbb{Z})$ that do not belong to $V(\mathbb{Z}_p)^{\text{proj}}$. We would like to estimate the number of elements in W_p for large p. We have the following theorem.

THEOREM 5.1
We have

$$N_H\Big(\bigcup_{p \geq M} W_p, X \Big) = O(X^{n+1}/M^{1-\epsilon}) + o(X^{n+1}),$$

$$N_J\Big(\bigcup_{p \geq M} W_p, X \Big) = O(X^{n+1}/M^{1-\epsilon}) + o(X^{n+1}),$$

where the implied constant is independent of X and M.

Proof
If $(A, B) \in W_p$ gives rise to the binary n-ic form f, then the ring R_f is nonmaximal at p, which implies that $p^2 \mid \Delta(A, B) = \Delta(f)$. Let $(A, B) \in W_p$, regarded as an element of $V(\mathbb{Z}_p)$, correspond to a pair (I, δ) with $I^2 \neq (\delta) I_f^{n-3}$. Then the reduction of (A, B) modulo p corresponds to the pair $(I \otimes \mathbb{F}_p, \overline{\delta})$, where $\overline{\delta}$ is the reduction of δ modulo p. From Nakayama's lemma, it follows that $I^2 \otimes \mathbb{F}_p \neq (\overline{\delta}) I_f^{n-3} \otimes \mathbb{F}_p$.

Let $(A_1, B_1) \in V(\mathbb{Z})$ be any element congruent to (A, B) modulo p. Denote the binary n-ic form associated to (A_1, B_1) by f_1. If (A_1, B_1) corresponds to the pair (I_1, δ_1), then it follows (again from Nakayama's lemma) that $I_1^2 \neq (\delta_1) I_{f_1}^{n-3}$. Thus $(A_1, B_1) \in W_p$.

Also, the set of elements in W_p whose binary n-ic invariants are divisible by p is the preimage under $V(\mathbb{Z}_p) \to V(\mathbb{F}_p)$ of the set of elements in $V(\mathbb{F}_p)$ having binary n-ic invariant 0. It follows that W_p is defined via congruence conditions modulo p; that is, the set W_p is the preimage of some subset of $V(\mathbb{F}_p)$ under the reduction modulo p map.

To prove the theorem, we start with the fundamental domain $\mathcal{F}_H$ chosen in Section 4.1. For every $0 < \epsilon < 1$, we pick a set $\mathcal{F}^{(\epsilon)} \subset \mathcal{F}_H$ which is open and bounded and whose measure is $(1 - \epsilon)$ times the measure of $\mathcal{F}_H$. Let $\mathcal{R}$ be the union of the $\mathcal{R}^{(r_2),\delta}$ over all possible r_2 and δ, and let $\mathcal{R}_X$ denote the set of elements in $\mathcal{R}$ having height bounded by X. Then, since the set $\mathcal{F}^{(\epsilon)} \cdot \mathcal{R}_X$ is homogeneously expanding with X and since the reduction of the set W_p modulo p has codimension greater than 2 in $V(\mathbb{F}_p)$, we obtain

$$\begin{aligned}\#\Big\{\mathcal{F}^{(\epsilon)} \cdot \mathcal{R}_X \cap \Big(\bigcup_{p \geq M} W_p\Big)\Big\}\\ = O(X^{n+1}/M \log M) + O(X^n)\end{aligned}$$

from an immediate application of [5, Theorem 3.3]. We further obtain

$$\#\big\{(\mathcal{F} \backslash \mathcal{F}^{(\epsilon)}) \cdot \mathcal{R}_X \cap V(\mathbb{Z})^{\mathrm{irr}}\big\} = O(\epsilon X^{n+1})$$

from the methods of the previous section. The first assertion of the theorem follows. The second assertion follows in an identical fashion by starting with $\mathcal{F}_J$ instead of $\mathcal{F}_H$. $\square$

We now have the following theorem.

THEOREM 5.2
Let r_2 be an integer such that $0 \leq r_2 \leq (n-1)/2$, and let $\delta \in \{\pm 1\}^{n-2r_2} \times \{1\}^{r_2}$ be fixed. Let Λ be a very large collection of local specifications such that $\Lambda_\infty = V(\mathbb{R})^{(r_2),\delta}$. Then we have

$$N_H\big(\mathcal{V}(\Lambda), X\big) = \frac{1}{\sigma(r_2)} \operatorname{Vol}\big(\mathcal{F}_H \cdot \mathcal{R}_H^{(r_2),\delta}(X)\big) \prod_p \operatorname{Vol}(\Lambda_p) + o(X^{n+1}),$$

$$N_J\big(\mathcal{V}(\Lambda), X\big) = \frac{1}{\sigma'(r_2)} \operatorname{Vol}\big(\mathcal{F}_J \cdot \mathcal{R}_J^{(r_2),\delta}(X)\big) \prod_p \operatorname{Vol}(\Lambda_p) + o(X^{n+1}),$$

where the volumes of sets in $V(\mathbb{Z}_p)$ are computed with respect to the Euclidean measure normalized so that $V(\mathbb{Z}_p)$ has measure 1.

The first estimate asserted by Theorem 5.2 follows from Theorem 5.1 just as [8, Theorem 2.21] follows from [8, Theorem 2.13]. The second estimate follows from a proof identical to that of Theorem 3.5 (which itself uses the methods of the proof of [8, Theorem 2.21]).

5.2. Sieving to acceptable sets (conditional on a tail estimate)

Let Λ be an acceptable collection of local specifications with $\Lambda_\infty = V(\mathbb{R})^{(r_2),\delta}$. Then we have the following theorem whose proof is identical to the proof of the upper bound in [8, Theorem 2.21].

THEOREM 5.3

We have

$$N_H\big(\mathcal{V}(\Lambda), X\big) \le \frac{1}{\sigma(r_2)} \operatorname{Vol}\big(\mathcal{F}_H \cdot \mathcal{R}_H^{(r_2),\delta}(X)\big) \prod_p \operatorname{Vol}(\Lambda_p) + o(X^{n+1}),$$

$$N_J\big(\mathcal{V}(\Lambda), X\big) \le \frac{1}{\sigma(r_2)} \operatorname{Vol}\big(\mathcal{F}_J \cdot \mathcal{R}_J^{(r_2),\delta}(X)\big) \prod_p \operatorname{Vol}(\Lambda_p) + o(X^{n+1}),$$

where the volumes of sets in $V(\mathbb{R})$ are computed with respect to Euclidean measure normalized so that $V(\mathbb{Z})$ has covolume 1, *and the volumes of sets in $V(\mathbb{Z}_p)$ are computed with respect to the Euclidean measure normalized so that $V(\mathbb{Z}_p)$ has volume* 1.

For a prime p, let $\mathcal{W}_p$ denote the set of elements in $V(\mathbb{Z})$ such that $p^2 \mid \Delta$. The following estimates are unknown but likely to be true:

$$\begin{aligned} N_H\Big(\bigcup_{p\ge M} \mathcal{W}_p, X\Big) &= O(X^{n+1}/M^{1-\epsilon}) + o(X^{n+1}),\\ N_J\Big(\bigcup_{p\ge M} \mathcal{W}_p, X\Big) &= O(X^{n+1}/M^{1-\epsilon}) + o(X^{n+1}). \end{aligned} \tag{33}$$

We now have the following theorem.

THEOREM 5.4

Assume that one of the equations in (33) holds. Let Λ be an acceptable collection of local specifications with $\Lambda_\infty = V(\mathbb{R})^{(r_2),\delta}$. Then we have

$$N_H\big(\mathcal{V}(\Lambda), X\big) = \frac{1}{\sigma(r_2)} \operatorname{Vol}\big(\mathcal{F}_H \cdot \mathcal{R}_H^{(r_2),\delta}(X)\big) \prod_p \operatorname{Vol}(\Lambda_p) + o(X^{n+1}),$$

$$N_J\big(\mathcal{V}(\Lambda), X\big) = \frac{1}{\sigma(r_2)} \mathrm{Vol}\big(\mathcal{F}_J \cdot \mathcal{R}_J^{(r_2),\delta}(X)\big) \prod_p \mathrm{Vol}(\Lambda_p) + o(X^{n+1}),$$

where the volumes of sets in $V(\mathbb{R})$ are computed with respect to Euclidean measure normalized so that $V(\mathbb{Z})$ has covolume 1*, and the volumes of sets in $V(\mathbb{Z}_p)$ are computed with respect to the Euclidean measure normalized so that $V(\mathbb{Z}_p)$ has volume* 1.

Proof
We first assume that the first equation in (33) holds. Then the first assertion of the theorem follows just as [8, Theorem 2.21] follows from [8, Theorem 2.13]. The second estimate follows from a proof identical to that of Theorem 3.5.

We now assume that the second equation in (33) holds. Then the second assertion of the theorem follows just as [8, Theorem 2.21] follows from [8, Theorem 2.13]. To prove the first assertion, we use methods from the proof of [5, Lemma 3.7]. The set $\mathcal{F}_H \cdot \mathcal{R}_H^{(r_2),\delta}(X) \setminus \{\Delta = 0\}$ can be covered with countably many fundamental domains for the action of $G(\mathbb{Z})$ on $V(\mathbb{R})^{(r_2),\delta}$. Therefore, for any $\epsilon > 0$, there exist s fundamental domains for the action of $G(\mathbb{Z})$ on $V(\mathbb{R})^{(r_2),\delta}$ whose union covers all but measure ϵX^{n+1} of the finite measure multiset $\mathcal{F}_H \cdot \mathcal{R}_H^{(r_2),\delta}(X)$, where s is independent of X. (To ensure that s is independent of X, we merely choose s fundamental domains when $X = 1$, and then scale these fundamental domains for large X.) Once again arguments in the proof of [8, Theorem 2.21] imply the bound

$$\frac{N_H(\mathcal{V}(\Lambda), X)}{X^{n+1}} \geq \frac{1}{\sigma(r_2)}\Big(\mathrm{Vol}\big(\mathcal{F}_H \cdot \mathcal{R}_H^{(r_2),\delta}(1)\big) - \epsilon\Big) \prod_{p<M} \mathrm{Vol}(\Lambda_p)$$
$$+ O(s/M^{1-\delta}) + o(s).$$

Letting M tend to ∞, and then ϵ to 0, and then s to ∞ yields the required lower bound. The upper bound follows from Theorem 5.3. This concludes the proof of Theorem 5.4. □

6. Proof of the main theorems

We are now ready to prove Theorems 2–6. To do so, we establish Theorem 6.2, which determines an upper bound for the average sizes of the 2-torsion subgroup in the class groups of acceptable families of orders of fixed signature ordered by height or by Julia invariant. For certain *very large* families, we obtain that the average sizes are in fact equal to 1; for all other acceptable families, the lower bound being equal to 1 is dependent on the tail estimates described in (33). The proof of Theorem 6.2 involves the computation of local volumes in order to determine the number of absolutely irreducible lattice points in $\mathcal{F}_H$ of bounded height and $\mathcal{F}_J$ of bounded Julia invariant. The results of Section 2 then allow us to conclude the theorem, and it immediately implies Theorems 2, 3, and 6. We obtain Theorem 4 from combining Theorems 2 and 3 with the results of [14].

We adopt the notation of the introduction. Recall that for an infinite collection Σ of local specifications, $\mathcal{U}(\Sigma)$ is the associated set of integral binary n-ic forms, and acceptable sets $\mathcal{U}(\Sigma)$ give rise to acceptable families $\Sigma_H \subseteq \mathfrak{R}_H$ (and acceptable families $\Sigma_J \subseteq \mathfrak{R}_J$ if $\mathcal{U}(\Sigma)$ is also $\mathrm{SL}_2(\mathbb{Z})$-invariant). We now describe the collections for which we obtain equalities on the average sizes in Theorem 6.

Definition 6.1

We say that $\Sigma = (\Sigma_v)_v$ and $\mathcal{U}(\Sigma)$ are *very large* if, for all sufficiently large primes p, the set Σ_p is precisely $U(\mathbb{Z}_p) \setminus pU(\mathbb{Z}_p)$. We say that a family $\Sigma_H \subseteq \mathfrak{R}_H$ is *very large* if it is defined by a very large family $\mathcal{U}(\Sigma)$, that is, $\mathfrak{R}_H = \{R_f \mid f \in \mathcal{U}(\Sigma)\}$. A family $\Sigma_J \subseteq \mathfrak{R}_J$ is *very large* if it is defined by a very large $\mathrm{SL}_2(\mathbb{Z})$-invariant family $\mathcal{U}(\Sigma)$.

THEOREM 6.2

Fix an integer n and a signature (r_1, r_2) with $r_1 + 2r_2 = n$. Let $\mathfrak{R}_1 \subset \mathfrak{R}_H^{r_1,r_2}$ be a family of rings that arises from an acceptable set of integral binary n-ic forms, and let $\mathfrak{R}_2 \subset \mathfrak{R}_J^{r_1,r_2}$ be a family of rings that arises from an acceptable $\mathrm{SL}_2(\mathbb{Z})$-invariant set of binary n-ic forms. Then we have the following.

(a) *The average sizes of*

$$\left|\mathrm{Cl}_2(\mathcal{O})\right| - \frac{1}{2^{r_1+r_2-1}}\left|\mathcal{I}_2(\mathcal{O})\right|$$

over $\mathcal{O} \in \mathfrak{R}_1$ ordered by height and over $\mathcal{O} \in \mathfrak{R}_2$ ordered by Julia invariant are bounded above by 1.

(b) *The average sizes of*

$$\left|\mathrm{Cl}_2^+(\mathcal{O})\right| - \frac{1}{2^{r_2}}\left|\mathcal{I}_2(\mathcal{O})\right|$$

over $\mathcal{O} \in \mathfrak{R}_1$ ordered by height and over $\mathcal{O} \in \mathfrak{R}_2$ ordered by Julia invariant are bounded above by 1.

If we assume that $\mathfrak{R}_1$ and $\mathfrak{R}_2$ arise from very large sets of binary n-ic forms, then the average sizes in (a) and (b) are equal to 1*, independent of the choice of very large set. Furthermore, conditional on the tail estimates in (33), the average sizes in (a) and (b) are indeed equal to* 1 *for all $\mathfrak{R}_1$ or $\mathfrak{R}_2$ arising from any acceptable set of binary n-ic forms.*

We will prove Theorem 6.2 in the following sections.

6.1. Computing the product of local volumes

We first prove a statement about the "compatibility of measures." Let $\mathrm{d}v$ and $\mathrm{d}f$ denote Euclidean measures on V and U, respectively, normalized so that $V(\mathbb{Z})$ and $U(\mathbb{Z})$ have covolume 1. Let ω be an algebraic differential form that generates the rank 1 module of top degree left-invariant differential forms on SL_n over $\mathbb{Z}$. We have the following theorem, whose proof is identical to that of [8, Propositions 3.11 and 3.12].

THEOREM 6.3

Let T be $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ for some prime p. Let $s : U(T) \to V(T)$ be a continuous section for π, that is, a continuous function such that the invariant binary n-ic of $w_f := s(f)$ is f. Then there exists a rational nonzero constant $\mathcal{J}$ such that for any measurable function ϕ on $V(T)$, we have

$$\int_{v\in\mathrm{SL}_n(T)\cdot s(U(T))} \phi(v)\,\mathrm{d}v = |\mathcal{J}| \int_{U(T)} \int_{\mathrm{SL}_n(T)} \phi(g\cdot w_f)\omega(g)\,\mathrm{d}f,$$

$$\int_{V(T)} \phi(v)\,\mathrm{d}v = |\mathcal{J}| \int_{\substack{f\in U(T)\\ \Delta(f)\neq 0}} \Big(\sum_{v\in\frac{V(T)(f)}{\mathrm{SL}_n(T)}} \frac{1}{|\mathrm{Stab}_{\mathrm{SL}_n(T)}(v)|} \times \int_{g\in\mathrm{SL}_n(T)} \phi(g\cdot v)\omega(g)\Big)\,\mathrm{d}f,$$

where we regard $\mathrm{SL}_n(T)\cdot s(R)$ as a multiset, and $\frac{V(T)(f)}{\mathrm{SL}_n(T)}$ denotes a set of representatives for the action of $\mathrm{SL}_n(T)$ on elements in $V(T)$ having invariant f.

For $r_2 \in \{1, \dots, (n-1)/2\}$ and for $f \in V(\mathbb{Z}_p)$, we define local masses

$$m_p(f) := \frac{|(R_f^\times/(R_f^\times)^2)_{N\equiv 1}|}{|R_f^\times[2]_{N\equiv 1}|},$$

$$m_\infty(r_2) := \frac{|((\mathbb{R}^{n-2r_2}\times\mathbb{C}^{r_2})^\times/((\mathbb{R}^{n-2r_2}\times\mathbb{C}^{r_2})^\times)^2)_{N\equiv 1}|}{|(\mathbb{R}^{n-2r_2}\times\mathbb{C}^{r_2})^\times[2]_{N\equiv 1}|}.$$

We denote the numerator and the denominator of the right-hand side in the equation defining $m_\infty(r_2)$ by $\tau(r_2)$ and $\sigma(r_2)$, respectively. For a prime p, let $\Sigma_p \subset U(\mathbb{Z}_p) \setminus pU(\mathbb{Z}_p)$ be a nonempty open set whose boundary has measure 0. Let Λ_p denote the set of projective elements in $V(\mathbb{Z}_p)$ whose invariant binary form belongs to Σ_p. We have the following corollary to Theorem 6.3.

COROLLARY 6.4

Let notation be as above. We have

$$\mathrm{Vol}\big(\mathcal{F}_H\cdot\mathcal{R}_H^{(r_2),\delta}(X)\big) = |\mathcal{J}|\,\mathrm{Vol}(\mathcal{F}_H)\,\mathrm{Vol}\big(U(\mathbb{R})^{(r_2)}_{H<X}\big),$$

$$\mathrm{Vol}\big(\mathcal{F}_J \cdot \mathcal{R}_J^{(r_2),\delta}(X)\big) = \frac{\sigma'(r_2)}{\sigma(r_2)} |\mathcal{J}| \,\mathrm{Vol}(\mathcal{F}_H)\,\mathrm{Vol}\big(\mathrm{SL}_2(\mathbb{Z})\backslash U(\mathbb{R})^{(r_2)}_{J<X}\big),$$

$$\mathrm{Vol}(\Lambda_p) = |\mathcal{J}| \,\mathrm{Vol}\big(\mathrm{SL}_n(\mathbb{Z}_p)\big) \int_{f \in \Sigma_p} m_p(f)\,\mathrm{d}f,$$

where the volumes of $\mathcal{F}_H$ and $\mathrm{SL}_n(\mathbb{Z}_p)$ are computed with respect to ω, and $\sigma'(r_2)$ denotes the size of the stabilizer in $G(\mathbb{R})$ of a generic element of $V(\mathbb{R})^{(r_2)}$.

Proof

The first equality follows immediately from Theorem 6.3. Next, note that we have $\mathcal{F}_J = \mathcal{F}_2 \times \mathcal{F}_H$, where $\mathcal{F}_2$ is a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathrm{SL}_2(\mathbb{R})$. Let the multiset $I \subset U(\mathbb{R})$ denote the invariants of the multiset $\mathcal{F}_2 \cdot \mathcal{R}_J^{(r_2),\delta}(X)$. Then I generically represents each element of $\mathrm{SL}_2(\mathbb{Z})\backslash U(\mathbb{R})^{(r_2)}_{J<X}$ exactly $\sigma'(r_2)/\sigma(r_2) = s(r_2)$ times, since $s(r_2)$ is the size of the stabilizer in $\mathrm{SL}_2(\mathbb{R})$ of an element in $U(\mathbb{R})^{(r_2)}$. (We have already seen that $s(r_2) = 3$ when $n = 3$ and $r_2 = 0$, and $s(r_2) = 1$ otherwise.) The second equality now follows immediately from Theorem 6.3.

To obtain the final equality, note that Theorem 6.3 implies

$$\int_{\Lambda_p} \mathrm{d}v = |\mathcal{J}| \,\mathrm{Vol}\big(\mathrm{SL}_n(\mathbb{Z}_p)\big) \int_{f \in \Sigma_p} \sum_{v \in \frac{\det^{-1}(f)}{\mathrm{SL}_n(\mathbb{Z}_p)}} \frac{1}{|\mathrm{Stab}_{\mathrm{SL}_n(\mathbb{Z}_p)}(v)|}\,\mathrm{d}v,$$

where the sum runs over representatives in projective $\mathrm{SL}_n(\mathbb{Z}_p)$-orbits of $\det^{-1}(f)$. The result now follows from Corollary 2.15. ☐

Denote $n - 2r_2$ by r_1 so that $r_1 + 2r_2 = n$. By Corollaries 2.15 and 2.16 and Example 2.17, we have

$$\tau(r_2) = 2^{r_1 - 1}, \qquad \sigma(r_2) = 2^{r_1 + r_2 - 1}, \qquad \text{and} \qquad m_\infty(r_2) = 2^{-r_2}. \tag{34}$$

In [11, Lemma 22], the values of $m_p(f)$ are computed for cubic rings. We now compute these values for degree n rings using a similar argument.

LEMMA 6.5

Let R be a nondegenerate ring of degree n over $\mathbb{Z}_p$. Then

$$\frac{|(R^\times/(R^\times)^2)_{N\equiv 1}|}{|R^\times[2]_{N\equiv 1}|} \tag{35}$$

is 1 if $p \neq 2$ and 2^{n-1} if $p = 2$.

Proof

The unit group of $R^\times$ is the direct product of a finite Abelian subgroup and $\mathbb{Z}_p^n$, and the norm 1 part $R^\times_{N\equiv 1}$ is also a direct product of a finite Abelian group and $\mathbb{Z}_p^{n-1}$. For G a finite Abelian group or $G = \mathbb{Z}_p^n$ when $p \neq 2$, we have

$$\frac{|G/G^2|}{|G[2]|} = 1,$$

so the value of (35) is 1 for $p \neq 2$. When $p = 2$, because 2 is not a unit in $\mathbb{Z}_2$, the $\mathbb{Z}_2$-module $2\mathbb{Z}_2^{n-1}$ has index 2^{n-1} in $\mathbb{Z}_2^{n-1}$ instead, implying that (35) evaluates to 2^{n-1}. □

It follows that for a fixed prime p, the value of $m_p(f)$ is independent of $f \in U(\mathbb{Z}_p)^{\text{prim}}$. We denote this value by m_p. We conclude with the following theorem.

THEOREM 6.6

We have

$$\frac{1}{\sigma(r_2)} \operatorname{Vol}\big(\mathcal{F}_H \cdot \mathcal{R}_H^{(r_2),\delta}(X)\big) \prod_p \operatorname{Vol}(\Lambda_p) = 2^{r_2} \operatorname{Vol}\big(U(\mathbb{R})^{(r_2)}_{H<X}\big) \prod_p \operatorname{Vol}(\Sigma_p) \qquad \textit{and}$$

$$\frac{1}{\sigma'(r_2)} \operatorname{Vol}\big(\mathcal{F}_J \cdot \mathcal{R}_J^{(r_2),\delta}(X)\big) \prod_p \operatorname{Vol}(\Lambda_p) = 2^{r_2} \operatorname{Vol}\big(\mathrm{SL}_2(\mathbb{Z})\backslash U(\mathbb{R})^{(r_2)}_{J<X}\big) \prod_p \operatorname{Vol}(\Sigma_p).$$

Proof

From Corollary 6.4 and Lemma 6.5, we obtain

$$\begin{aligned}\frac{1}{\sigma(r_2)} \operatorname{Vol}\big(\mathcal{F}_H \cdot \mathcal{R}_H^{(r_2),\delta}(X)\big) \prod_p \operatorname{Vol}(\Lambda_p) &= \frac{1}{\sigma(r_2)} |\mathcal{J}| \operatorname{Vol}(\mathcal{F}_H) \operatorname{Vol}\big(U(\mathbb{R})^{(r_2)}_{H<X}\big) \\ &\quad \times \prod_p |\mathcal{J}|_p \operatorname{Vol}\big(\mathrm{SL}_n(Z_p)\big) m_p \operatorname{Vol}(\Sigma_p) \end{aligned} \tag{36}$$

and

$$\begin{aligned}
&\frac{1}{\sigma'(r_2)} \operatorname{Vol}\big(\mathcal{F}_J \cdot \mathcal{R}_J^{(r_2),\delta}(X)\big) \prod_p \operatorname{Vol}(\Lambda_p) \\
&\quad = \frac{1}{\sigma(r_2)} |\mathcal{J}| \operatorname{Vol}(\mathcal{F}_H) \operatorname{Vol}\big(\mathrm{SL}_2(\mathbb{Z})\backslash U(\mathbb{R})^{(r_2)}_{J<X}\big) \\
&\qquad \times \prod_p |\mathcal{J}|_p \operatorname{Vol}\big(\mathrm{SL}_n(Z_p)\big) m_p \operatorname{Vol}(\Sigma_p). \qquad (37)
\end{aligned}$$

We simplify the right-hand side of these expressions by noting that

$$|\mathcal{J}| \prod_p |\mathcal{J}|_p = 1, \qquad (38)$$

$$\operatorname{Vol}(\mathcal{F}_H) \prod_p \operatorname{Vol}\big(\mathrm{SL}_n(\mathbb{Z}_p)\big) = 1, \qquad (39)$$

$$\frac{1}{\sigma(r_2)} \prod_p m_p = 2^{r_2}, \qquad (40)$$

where (38) follows from the product formula, (39) comes from the Tamagawa number of $\mathrm{SL}_n(\mathbb{Q})$ being 1, and (40) follows from (34) and Lemma 6.5. Combining these with (36) and (37) yields the theorem. $\square$

6.2. Proof of Theorem 6.2

Let $\mathfrak{R} \subset \mathfrak{R}_H$ be an acceptable family of rings having fixed signature (r_1, r_2). Then the rings in $\mathfrak{R}$ are in bijection with an acceptable set $\mathcal{U}(\Sigma) \subset U(\mathbb{Z})$ of binary n-ic forms with $\Sigma_\infty = U(\mathbb{R})^{(r_2)}$. Let $\Lambda^{(\delta)}$ be a collection of local specifications for V, where Λ_p consists of projective elements in $V(\mathbb{Z}_p)$ whose invariants belong to Σ_p and $\Lambda_\infty = V(\mathbb{R})^{(r_2),\delta}$. Then $\Lambda = (\Lambda_\nu)_\nu$ is acceptable. Furthermore, if $\mathfrak{R}$ is very large, then so is Λ.

From Propositions 2.5 and 2.12 and Lemma 2.4, we know that

$$\sum_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} 2^{r_1+r_2-1}\big|\mathrm{Cl}_2(\mathcal{O})\big| - \big|\mathcal{I}_2(\mathcal{O})\big| = \sum_\delta N_H\big(\mathcal{V}(\Lambda^{(\delta)}), X\big),$$

$$\sum_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} 2^{r_2}\big|\mathrm{Cl}_2^+(\mathcal{O})\big| - \big|\mathcal{I}_2(\mathcal{O})\big| = N_H\big(\mathcal{V}(\Lambda^{(\delta_{\gg 0})}), X\big),$$

where the first sum is over all possible δ, and $\delta_{\gg 0}$ denotes the element $(1, 1, \ldots, 1) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. As a result, we have

$$
\begin{aligned}
&\lim_{X\to\infty} \frac{\sum_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} 2^{r_1+r_2-1}|\mathrm{Cl}_2(\mathcal{O})| - |\mathcal{I}_2(\mathcal{O})|}{\sum_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} 1} \\
&\quad \le \lim_{X\to\infty} \frac{\sum_{\delta} N_H(\mathcal{V}(\Lambda^{(\delta)}),X)}{\#\mathcal{U}(\Sigma)_{H<X}} = 2^{r_1+r_2-1}, \\
&\lim_{X\to\infty} \frac{\sum_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} 2^{r_2}|\mathrm{Cl}_2^+(\mathcal{O})| - |\mathcal{I}_2(\mathcal{O})|}{\sum_{\substack{\mathcal{O}\in\mathfrak{R}\\ H(\mathcal{O})<X}} 1} \\
&\quad \le \lim_{X\to\infty} \frac{N_H(\mathcal{V}(\Lambda^{(\delta\gg 0)}),X)}{\#\mathcal{U}(\Sigma)_{H<X}} = 2^{r_2},
\end{aligned}
\tag{41}
$$

where we use Theorems 5.3 and 3.3 to evaluate the numerators and the denominators of the middle terms in the above equation, and where we use Theorem 6.6 to evaluate the product of local volumes that arise.

Similarly, let $\mathfrak{R}\subset\mathfrak{R}_J$ be an acceptable family of rings having fixed signature (r_1,r_2). Then the rings in $\mathfrak{R}$ are in bijection with $\mathrm{SL}_2(\mathbb{Z})$-orbits on an acceptable set $\mathcal{U}(\Sigma)\subset U(\mathbb{Z})$ of binary n-ic forms with $\Sigma_\infty = U(\mathbb{R})^{(r_2)}$. We define $\Lambda^{(\delta)}$ as above, and we obtain

$$
\begin{aligned}
&\lim_{X\to\infty} \frac{\sum_{\substack{\mathcal{O}\in\mathfrak{R}\\ J(\mathcal{O})<X}} 2^{r_1+r_2-1}|\mathrm{Cl}_2(\mathcal{O})| - |\mathcal{I}_2(\mathcal{O})|}{\sum_{\substack{\mathcal{O}\in\mathfrak{R}\\ J(\mathcal{O})<X}} 1} \\
&\quad \le \lim_{X\to\infty} \frac{\sum_{\delta} N_J(\mathcal{V}(\Lambda^{(\delta)}),X)}{\#\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{U}(\Sigma)_{J<X}} = 2^{r_1+r_2-1} \qquad \text{and} \\
&\lim_{X\to\infty} \frac{\sum_{\substack{\mathcal{O}\in\mathfrak{R}\\ J(\mathcal{O})<X}} 2^{r_2}|\mathrm{Cl}_2^+(\mathcal{O})| - |\mathcal{I}_2(\mathcal{O})|}{\sum_{\substack{\mathcal{O}\in\mathfrak{R}\\ J(\mathcal{O})<X}} 1} \\
&\quad \le \lim_{X\to\infty} \frac{N_J(\mathcal{V}(\Lambda^{(\delta\gg 0)}),X)}{\#\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{U}(\Sigma)_{J<X}} = 2^{r_2},
\end{aligned}
\tag{42}
$$

where we use Theorems 5.3 and 3.5 to evaluate the numerators and the denominators of the middle terms in the above equation, and where we use Theorem 6.6 to evaluate the product of local volumes that arise.

If the families $\mathfrak{R}$ are very large, then from Theorem 5.2, the inequalities in (41) and (42) can be replaced with equalities. Likewise, if we assume that one of the estimates in (33) holds, then from Theorem 5.4, the inequalities in (41) and (42) can be replaced with equalities. This concludes the proof of Theorem 6.2. □

6.3. Proof of Theorem 4

Since Theorem 6.2 implies Theorems 2, 3, and 6, it remains to prove Theorem 4. We first prove a corollary of Theorem 2 and Theorem 3 on the proportion of maximal orders in $\mathfrak{R}^{r_1,r_2}_{J,\max}$ which have odd (narrow) class number.

COROLLARY 6.7

Fix an odd integer $n \geq 3$ and signature (r_1, r_2). If $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}_{J,\max}$ corresponds to an acceptable set of binary n-ic forms, then we have the following.

(a) *A positive proportion (at least $1 - 2^{1-r_1-r_2}$) of maximal orders in $\mathfrak{R}$ have odd class number.*

(b) *If r_2 is also assumed to be nonzero, then a positive proportion (at least $1 - 2^{-r_2}$) of $\mathfrak{R}$ have odd narrow class number. Thus, at least a proportion of $1 - 2^{-r_2}$ of $\mathfrak{R}$ have narrow class number equal to the class number.*

Proof

Fix a signature (r_1, r_2), and suppose for the sake of a contradiction that a lower proportion than $1 - 2^{1-r_1-r_2}$ of rings of integers of number fields with signature (r_1, r_2) that correspond to integral binary n-ic forms have odd class number. This implies that a larger proportion than $2^{1-r_1-r_2}$ of such maximal orders would have nontrivial 2-torsion subgroup in their class group and thus have $|\mathrm{Cl}_2| \geq 2$. Then the limsup of the mean number of 2-torsion elements in class groups of such maximal orders would be strictly larger than $1 + \frac{1}{2^{n-1-r_2}}$, contradicting Theorem 2(a), Theorem 3(a), Theorem 3(b), or [11, Corollary 3].

Now suppose for the sake of a contradiction that a lower proportion than $1 - 2^{-r_2}$ of maximal orders in number fields of signature (r_1, r_2) in $\mathfrak{R}$ have odd narrow class number. We would then be able to conclude that a larger proportion than 2^{-r_2} of such maximal orders would have at least two distinct 2-torsion elements in its narrow class group. Then the limsup of the mean number of 2-torsion elements in the narrow class groups of such maximal orders would be strictly larger than $1 + 2^{-r_2}$, contradicting Theorem 2(b). When $n = 3$, note that the narrow class group of a complex cubic field is always equal to its class group. $\square$

THEOREM 6.8

Fix a signature (r_1, r_2). If $\mathfrak{R} \subset \mathfrak{R}^{r_1,r_2}_{J,\max}$ is an acceptable family of rings, then

(a) $\#\{R \in \mathfrak{R} : |\mathrm{Disc}(R)| < X \text{ and } 2 \nmid |\mathrm{Cl}(R)|\} \gg X^{\frac{n+1}{2n-2}}$;

(b) *if $r_2 \geq 1$, then* $\#\{R \in \mathfrak{R} : |\mathrm{Disc}(R)| < X \text{ and } 2 \nmid |\mathrm{Cl}^+(R)|\} \gg X^{\frac{n+1}{2n-2}}$.

Proof

In [10], it is proved that there exists a nonempty open bounded set $B \subset U(\mathbb{R})$, whose closure does not contain any element having discriminant 0, such that for any $X > 0$, every element $f \in X \cdot B \cap U(\mathbb{Z})$ is *strongly reduced*; that is, the basis given in (4) is the unique Minkowski-reduced basis of the ring R_f corresponding to f. It is further shown that if two distinct elements f_1 and f_2 of $U(\mathbb{Z})$ are strongly reduced, then the rings R_{f_1} and R_{f_2} corresponding to f_1 and f_2 are not isomorphic.

Let Σ denote the collection of local specifications defining $\mathfrak{R}$, and let $\mathfrak{R}_B$ denote the family of maximal S_n-orders R, where $R = R_f$ arises from an integral binary n-ic form $f \in \mathcal{U}(\Sigma) \cap \mathbb{R}_{>0} \cdot B$. We endow this family of binary n-ic forms with the natural height

$$H_B(f) := \min\{X : f \in X \cdot B\},$$

thereby defining a height function on the family $\mathfrak{R}_B$ of maximal S_n-orders. The average sizes of Cl_2 and Cl_2^+ over the rings in $\mathfrak{R}_B$, ordered by H_B, are bounded by $1 + 2^{1-r_1-r_2}$ and $1 + 2^{-r_2}$, respectively; the proof for the analogous statement when rings are ordered by height H adapts to this situation without change. Therefore, by the same argument as in the proof of Corollary 6.7, we see that a positive proportion of rings in $\mathfrak{R}_B$ have odd class number.

Let $c > 0$ be a constant such that every element in cB has discriminant bounded by 1 in absolute value. Then every element in $cX^{1/(2n-2)}B$ has discriminant bounded by X. Since we have

$$\#\{\mathcal{U}(\Sigma) \cap cX^{1/(2n-2)}B\} \gg X^{\frac{n+1}{2n-2}},$$

the theorem follows. $\square$

Note that the conditions required in Theorem 4 are indeed acceptable, so Theorem 4 follows directly from Theorem 6.8.

Acknowledgments. We thank Manjul Bhargava, Christophe Delaunay, Robert Harron, Gunter Malle, Michael Stoll, Xiaoheng Wang, and Melanie Matchett Wood for helpful conversations and comments. We also thank the anonymous referees for many useful suggestions.

Ho's work was partially supported by National Science Foundation (NSF) grant DMS-1406066, and Varma's work was partially supported by NSF grant DMS-1502834.

References

[1] O. BECKWITH, *Indivisibility of class numbers of imaginary quadratic fields*, Res. Math. Sci. **4** (2017), no. 20. MR 3709663. *(1000)*

[2] M. BHARGAVA, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), 1031–1063. MR 2183288. DOI 10.4007/annals.2005.162.1031. *(996, 998, 1002, 1033)*

[3] ———, *The density of discriminants of quintic rings and fields*, Ann. of Math. (2) **172** (2010), 1559–1591. MR 2745272. DOI 10.4007/annals.2010.172.1559. *(1002)*

[4] ———, *Most hyperelliptic curves over $\mathbb{Q}$ have no rational points*, preprint, arXiv:1308.0395v1 [math.NT]. *(1002)*

[5] ———, *The geometric sieve and the density of squarefree values of invariant polynomials*, preprint, arXiv:1402.0031v1 [math.NT]. *(1034, 1036)*

[6] M. BHARGAVA and B. H. GROSS, "The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point" in *Automorphic Representations and L-Functions*, Tata Inst. Fund. Res. Stud. Math. **22**, Tata Inst. Fund. Res., Mumbai, 2013, 23–91. MR 3156850. *(1002)*

[7] M. BHARGAVA, B. H. GROSS, and X. WANG, *A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension*, with an appendix by T. Dokchitser and V. Dokchitser, J. Amer. Math. Soc. **30** (2017), 451–493. MR 3600041. DOI 10.1090/jams/863. *(1002)*

[8] 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** (2015), 191–242. MR 3272925. *(1019, 1021, 1026, 1027, 1035, 1036, 1038)*

[9] ———, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, preprint, arXiv:1312.7859v1 [math.NT]. *(1002, 1029, 1030)*

[10] M. BHARGAVA, A. SHANKAR, and X. WANG, *Squarefree values of polynomial discriminants, II*, in preparation. *(1002, 1019, 1043)*

[11] M. BHARGAVA and I. VARMA, *On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields*, Duke Math. J. **164** (2015), 1911–1933. MR 3369305. *(998, 999, 1000, 1001, 1003, 1039, 1043)*

[12] ———, *The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders*, Proc. Lond. Math. Soc. (3) **112** (2016), 235–266. MR 3471250. DOI 10.1112/plms/pdv062. *(1000, 1001)*

[13] M. BHARGAVA and A. YANG, *On the number of integral binary n-ic forms having bounded Julia invariant*, preprint, arXiv:1312.7339v1 [math.NT]. *(997, 1018, 1020, 1021, 1025)*

[14] B. J. BIRCH and J. R. MERRIMAN, *Finiteness theorems for binary forms with given discriminant*, Proc. Lond. Math. Soc. (3) **24** (1972), 385–394. MR 0306119. *(997, 999, 1037)*

[15] J. H. BRUINIER, *Nonvanishing modulo ℓ of Fourier coefficients of half-integral weight modular forms*, Duke Math. J. **98** (1999), 595–611. MR 1695803. *(1000)*

[16] H. COHEN and H. W. LENSTRA, JR., "Heuristics on class groups of number fields" in *Number Theory, Noordwijkerhout 1983*, Lecture Notes in Math. **1068**, Springer, Berlin, 1984, 33–62. MR 0756082. *(996)*

[17] H. COHEN and J. MARTINET, *Class groups of number fields: Numerical heuristics*, Math. Comp. **48** (1987), 123–137. MR 0866103. DOI 10.2307/2007878. *(996)*

[18] H. DAVENPORT, *On a principle of Lipschitz*, J. Lond. Math. Soc. (2) **26** (1951), 179–183. MR 0043821. DOI 10.1112/jlms/s1-26.3.179. *(1022, 1031)*

[19] H. DAVENPORT and H. HEILBRONN, *On the density of discriminants of cubic fields, II*, Proc. R. Soc. Lond. Ser. A **322** (1971), 405–420. MR 0491593. *(996, 1000)*

[20] D. S. DUMMIT and J. VOIGHT, *The* 2*-Selmer group of a number field and heuristics for narrow class groups and signature ranks of units*, preprint, arXiv:1702.00092v1 [math.NT]. *(999)*

[21] É. FOUVRY and J. KLÜNERS, *On the* 4*-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), 455–513. MR 2276261. *(996)*

[22] C. F. GAUSS, *Disquisitiones arithmeticae*, Yale Univ. Press, New Haven, 1966. MR 0197380. *(999)*

[23] P. HARTUNG, *Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by* 3, J. Number Theory **6** (1974), 276–278. MR 0352040. *(1000)*

[24] K. HORIE, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields*, Invent. Math. **88** (1987), 31–38. MR 0877004. *(1000)*

[25] ———, *Trace formulae and imaginary quadratic fields*, Math. Ann. **288** (1990), 605–612. MR 1081266. *(1000)*

[26] N. JOCHNOWITZ, *Congruences between modular forms and implications for the Hecke algebra*, Ph.D. dissertation, Harvard University, Cambridge, Mass., 1976. MR 2940744. *(1000)*

[27] G. JULIA, *Étude sur les formes binaires non quadratiques à indéterminées réelles, ou complexes*, Mémoires de l'Académie des Sciences de l'Institut de France **55** (1917), 1–296. MR 3532882. *(997, 1020)*

[28] G. MALLE, *On the distribution of class groups of number fields*, Experiment. Math. **19** (2010), 465–474. MR 2778658. *(996)*

[29] J. NAKAGAWA, *Binary forms and orders of algebraic number fields*, Invent. Math. **97** (1989), 219–235. MR 1001839. *(997, 1003, 1004)*

[30] J. NAKAGAWA and K. HORIE, *Elliptic curves with no rational points*, Proc. Amer. Math. Soc. **104** (1988), 20–24. MR 0958035. *(1000)*

[31] K. ONO and C. SKINNER, *Fourier coefficients of half-integral weight modular forms mod ℓ*, Ann. of Math. (2) **147** (1998), 453–470. MR 1626761. DOI 10.2307/121015. *(1000)*

[32] A. SHANKAR and J. TSIMERMAN, *Counting S_5-fields with a power saving error term*, Forum Math. Sigma **2** (2014), art. ID e13. MR 3264252. *(1032)*

[33] C. M. SKINNER and A. J. WILES, *Residually reducible representations and modular forms*, Publ. Math. Inst. Hautes Études Sci. **89** (1999), 5–126. MR 1793414. *(1000)*

[34] M. STOLL and J. E. CREMONA, *On the reduction theory of binary forms*, J. Reine Angew. Math. **565** (2003), 79–99. MR 2024647. *(1020)*

[35] V. VATSAL, *Canonical periods and congruence formulae*, Duke Math. J. **98** (1999), 397–419. MR 1695203. DOI 10.1215/S0012-7094-99-09811-3. *(1000)*

[36] X. WANG, *Pencils of quadrics and Jacobians of hyperelliptic curves*, Ph.D. dissertation, Harvard University, Cambridge, Mass., 2013. MR 3167287. *(1015)*

[37] A. WILES, *On class groups of imaginary quadratic fields*, J. Lond. Math. Soc. (2) **92** (2015), 411–426. MR 3404031. *(1000)*

[38] M. M. WOOD, *Rings and ideals parameterized by binary n-ic forms*, J. Lond. Math. Soc. (2) **83** (2011), 208–231. MR 2763952. *(997, 1003, 1004, 1005)*

[39] ———, *Parametrization of ideal classes in rings associated to binary forms*, J. Reine Angew. Math. **689** (2014), 169–199. MR 3187931. DOI 10.1515/crelle-2012-0058. *(1002, 1003, 1004, 1005, 1006, 1007, 1008, 1016)*

Ho

Department of Mathematics, University of Michigan, Ann Arbor, Michigan, USA; weiho@umich.edu

Shankar

Department of Mathematics, University of Toronto, Toronto, Canada; ashankar@math.toronto.edu

Varma

Department of Mathematics, Columbia University, New York, New York, USA; ila@math.columbia.edu