Comment. Math. Helv. 100 (2025), 225–267
DOI 10.4171/CMH/584

The mean number of 2-torsion elements in the class groups of cubic orders

Ashvin A. Swaminathan

Abstract. We determine the mean number of 2-torsion elements in class groups of cubic orders, when such orders are enumerated by discriminant. Specifically, we prove that when isomorphism classes of totally real (resp., complex) cubic orders are enumerated by discriminant, the average 2-torsion in the class group is $1 + \frac{1}{4} \times \frac{\zeta(2)}{\zeta(4)}$ (resp., $1 + \frac{1}{2} \times \frac{\zeta(2)}{\zeta(4)}$). In particular, we find that the average 2-torsion in the class group increases when one ranges over all orders in cubic fields instead of restricting to the subfamily of rings of integers of cubic fields, where the average 2-torsion in the class group was first determined in work of Bhargava to be $\frac{5}{4}$ (resp., $\frac{3}{2}$).

By work of Bhargava–Varma, proving this result amounts to obtaining an asymptotic count of the number of "reducible" $\mathrm{SL}_3(\mathbb{Z})$-orbits on the space $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^3$ of 3×3 symmetric integer matrices having bounded invariants and satisfying local conditions. In this paper, we resolve the generalization of this orbit-counting problem where the dimension 3 is replaced by any fixed odd integer $N \geq 3$. More precisely, we determine asymptotic formulas for the number of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathrm{Sym}^2 \mathbb{Z}^N$ satisfying general infinite sets of congruence conditions.

1. Introduction

1.1. Main results

A striking result of Bhargava's thesis was the determination of the average size of the 2-torsion subgroup in the class groups of cubic number fields, enumerated by discriminant (see [1, Theorem 5.4] and [4, Theorem 5]). Specifically, Bhargava proved that when totally real (resp., complex) cubic fields are enumerated by the absolute values of their discriminants, the average 2-torsion in the class group is equal to $\frac{5}{4}$ (resp., $\frac{3}{2}$). This result remains one of just a handful of cases of the heuristics on class groups of number fields, formulated in the foundational works of Cohen–Lenstra [15], Cohen–Martinet [16], and Malle [22], that have ever been proven.

Mathematics Subject Classification 2020: 11R29 (primary); 11E76, 11H55, 11R45 (secondary).
Keywords: class groups, cubic orders, irreducibility.

The main result of this paper constitutes a generalization of Bhargava's breakthrough to the full family of all *orders* in cubic fields. We prove the following result.

Theorem 1.1.A. *When irreducible cubic orders $\mathcal{O}$ over $\mathbb{Z}$ are enumerated by the absolute values of their discriminants, the average size of* $\mathrm{Cl}(\mathcal{O})[2]$ *is:*

(a) $1 + \frac{1}{4} \times \frac{\zeta(2)}{\zeta(4)}$ *for the family of totally real cubic orders $\mathcal{O}$, and*

(b) $1 + \frac{1}{2} \times \frac{\zeta(2)}{\zeta(4)}$ *for the family of complex cubic orders $\mathcal{O}$.*

Remark. Note that $\frac{\zeta(2)}{\zeta(4)} = \frac{15}{\pi^2} \approx 1.51982 > 1$.

Let $N = 2n + 1 \geq 3$ be an odd integer, and let U_N be the affine space over $\mathbb{Z}$ whose R-points are given by binary N-ic forms over R for any $\mathbb{Z}$-algebra R. When $N = 3$, the Delone–Faddeev–Levi correspondence [20] states that the map sending an irreducible binary cubic form $f \in U_3(\mathbb{Z})$ to the ring R_f of global sections of the subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ cut out by f defines a bijection between the irreducible orbits of $\mathrm{GL}_2(\mathbb{Z})$ on $U_3(\mathbb{Z})$ and the set of isomorphism classes of orders in cubic number fields. In light of this, studying cubic orders amounts to studying irreducible integral binary cubic forms that lie in a fundamental region $\mathcal{F}$ for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $U_3(\mathbb{R})$.

The region $\mathcal{F}$ may be chosen so that the set of $f \in \mathcal{F}$ with discriminant $\mathrm{disc}(f) \ll X$ is approximately the set of $f \in \mathcal{F}$ whose coefficients are all $\ll X^{1/4}$. Thus, we expect that the averages in Theorem 1.1.A should remain the same if we replace the family of cubic orders, enumerated by discriminant, with the family of cubic orders of the form R_f,[1] where f runs through irreducible integral binary cubic forms enumerated by *height*; here we define the height $\mathrm{H}(f)$ of a binary form to be the maximum of the absolute values of its coefficients. Indeed, by modifying the proof of Theorem 1.1.A, we obtain the following variant.

Theorem 1.1.B. *When irreducible binary cubic forms $f \in U_3(\mathbb{Z})$ are enumerated by height, the average size of* $\mathrm{Cl}(R_f)[2]$ *is:*

(a) $1 + \frac{1}{4} \times \frac{\zeta(2)}{\zeta(4)}$ *for the family of totally real binary cubic forms f, and*

(b) $1 + \frac{1}{2} \times \frac{\zeta(2)}{\zeta(4)}$ *for the family of complex binary cubic forms f.*

To prove Theorems 1.1.A and 1.1.B, we utilize an orbit parametrization, discovered by Bhargava when $N = 3$ (see [2, Theorem 4]), and generalized to all odd N by Wood (see [30, Theorem 1.3]). Fix an irreducible binary N-ic form $f \in U_N(\mathbb{Z})$, and assume f is primitive if $N > 3$. Let $K_f := \mathbb{Q} \otimes_{\mathbb{Z}} R_f$, and let W_N denote the affine space over $\mathbb{Z}$ whose R-points are given by pairs of symmetric $N \times N$ matrices over

[1] Note that each cubic order $\mathcal{O}$ in this family occurs infinitely many times, once for every f such that $\mathcal{O} \simeq R_f$!

R. Then the Bhargava–Wood parametrization takes as input a pair (I, δ), where I is a 2-torsion ideal class of the order R_f and $\delta \in K_f^\times / K_f^{\times 2}$ is a generator of I^2 having square norm, and it produces as output the $\mathrm{SL}_N(\mathbb{Z})$-orbit of a pair $(A, B) \in W_N(R)$ such that

$$\mathrm{inv}(A, B) := (-1)^n \det(xA - yB) = f(x, y).$$

The set of pairs (I, δ) corresponding to a form $f \in U_N(\mathbb{Z})$ naturally partitions into two subsets depending on whether or not $\delta \equiv 1 \in K_f^\times / K_f^{\times 2}$. Via the parametrization, pairs (I, δ) with $\delta \not\equiv 1$ (resp., $\delta \equiv 1$) correspond to so-called *irreducible* (resp., *reducible*) $\mathrm{SL}_N(\mathbb{Z})$-orbits on $W_N(\mathbb{Z})$. Here, (the $\mathrm{SL}_N(\mathbb{Z})$-orbit of) a pair $(A, B) \in W_N(\mathbb{Z})$ is said to be reducible if, when A and B are viewed as symmetric bilinear forms over $\mathbb{Q}$, they share an isotropic space over $\mathbb{Q}$ of maximal dimension. Geometrically, A and B may be viewed as defining a pair of quadric hypersurfaces in $\mathbb{P}^{N-1}$, and the condition that (A, B) is reducible is equivalent to stipulating that the (finite) Fano scheme parametrizing maximal linear spaces contained in the intersection of these two quadrics has a $\mathbb{Q}$-rational point.

Note that if (I, δ) is a pair with $\delta \equiv 1$, then I is the class of a 2-*torsion ideal* of R_f (i.e., a fractional ideal of R_f that squares to the unit ideal). Thus, the set of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits of pairs $(A, B) \in \mathrm{inv}^{-1}(f) \cap W_N(\mathbb{Z})$ is in bijection with the 2-torsion subgroup of the ideal group $\mathcal{I}(R_f)$. If R_f is the maximal order in K_f (i.e., R_f is integrally closed in K_f), then $\mathcal{I}(R_f)$ is torsion-free, and the only 2-torsion ideal is the trivial one. Thus, there is exactly one reducible orbit corresponding to f via the parametrization, and the problem of determining the average size of the 2-torsion in the class groups of maximal orders R_f amounts to counting just the irreducible orbits. A systematic method for counting irreducible orbits of representations (where the definition of "irreducible" depends on the representation) was developed by Bhargava in his thesis (see, e.g., [6]) and was later vastly streamlined in the seminal work of Bhargava and Shankar on Selmer groups of elliptic curves (see, e.g., [10]). Using this method to count just the irreducible orbits, Bhargava and Varma proved the following precursor to Theorem 1.1.A.

Theorem 1.2.A ([13, Theorem 2]). *When irreducible cubic orders $\mathcal{O}$ are enumerated by the absolute values of their discriminants, the average size of* $\mathrm{Cl}(\mathcal{O})[2]$ *is:*

(a) $1 + \frac{1}{4} \times \underset{\mathrm{disc}(\mathcal{O})>0}{\mathrm{Avg}} \#\mathcal{I}(\mathcal{O})[2]$ *for the family of totally real cubic orders $\mathcal{O}$, and*

(b) $1 + \frac{1}{2} \times \underset{\mathrm{disc}(\mathcal{O})<0}{\mathrm{Avg}} \#\mathcal{I}(\mathcal{O})[2]$ *for the family of complex cubic orders $\mathcal{O}$.*

Just as Theorem 1.2.A was a precursor to Theorem 1.1.A, we have the following result of Ho, Shankar, and Varma, which holds for *any* N and was a precursor to Theorem 1.1.B in the case $N = 3$.

Theorem 1.2.B ([21, Theorem 6]). *Let $U_N(\mathbb{Z})^{(r)}$ be the set of irreducible forms $f \in U_N(\mathbb{Z})$ having r real roots and $(N-r)/2$ pairs of complex roots. When forms $f \in U_N(\mathbb{Z})^{(r)}$, primitive if $N > 3$, are enumerated by height, the average size of* $\mathrm{Cl}(R_f)[2]$ *is*

$$1 + 2^{1-(N+r)/2} \times \operatorname*{Avg}_{\substack{f \in U_N(\mathbb{Z})^{(r)} \\ f \text{ prim. if } N>3}} \#\mathcal{I}(R_f)[2].$$

To determine precise numerical values of the average 2-torsion in the class group for the families of orders considered in Theorems 1.2.A and 1.2.B, one needs to determine the average 2-torsion in their ideal groups. Via the Bhargava–Wood parametrization, this amounts to counting reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $W_N(\mathbb{Z})$. Systematic methods for counting reducible orbits were not available until recently, when the author, in joint work with Shankar, Siad, and Varma, developed a new technique that applies to reducible orbits of many representations of importance in arithmetic statistics [25].

In the context of the action of SL_N on W_N, our new technique proceeds according to the following series of steps. First, we prove in Section 3 (see Proposition 3.2) that the count of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $W_N(\mathbb{Z})$ lying above irreducible binary forms is the same as the corresponding count for $G_N(\mathbb{Z})$-orbits on $W_N^0(\mathbb{Z})$, where $G_N \subset \mathrm{SL}_N$ is a certain closed subgroup and $W_N^0 \subset W_N$ is a certain linear subspace all of whose $\mathbb{Q}$-points are reducible (see Sections 2.2.4–2.2.5 for the precise definitions of G_N and W_N^0). Second, we prove that the action of G_N on W_N^0 satisfies the following strong local-to-global principle:

Theorem 1.3. *Let $f \in U_N(\mathbb{Z})$ be a binary N-ic form with nonzero discriminant. For each prime p, choose $(A_p, B_p) \in \mathrm{inv}^{-1}(f) \cap W_N^0(\mathbb{Z}_p)$. Then there exists $(A, B) \in W_N^0(\mathbb{Z})$, unique up to the action of $G_N(\mathbb{Z})$, such that (A, B) is $G_N(\mathbb{Z}_p)$-equivalent to (A_p, B_p) for each prime p.*

To prove Theorem 1.3, we rely on [25, Theorem 22], which is a general result that provides criteria under which the integral orbits of a representation satisfy a local-to-global principle. Theorem 1.3 follows by verifying that the representation of G_N on W_N^0 satisfies these criteria.

As a consequence of Theorem 1.3, counting $G_N(\mathbb{Z})$-orbits on $W_N^0(\mathbb{Z})$ amounts to counting $G_N(\mathbb{Z}_p)$-orbits on $W_N^0(\mathbb{Z}_p)$ for every prime p. In Section 3.1 we combine this local-to-global principle with results of Bhargava–Shankar–Wang [12] to obtain an asymptotic for the count of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $W_N(\mathbb{Z})$ satisfying certain infinite families of congruence conditions, which we define precisely as follows.

Definition 1.4. We call a subset $\mathfrak{S} \subset W_N^0(\mathbb{Z})$ a *big family in* $W_N^0(\mathbb{Z})$ if

$$\mathfrak{S} = \mathrm{inv}^{-1}\left(U_N(\mathbb{Z})^{(r)}\right) \cap W_N^0(\mathbb{Z}) \cap \bigcap_p \mathfrak{S}_p,$$

where the sets $\mathfrak{S}_p \subset W_N^0(\mathbb{Z}_p)$ satisfy the following properties:

(1) $\mathfrak{S}_p$ is $G_N(\mathbb{Z}_p)$-invariant and is the preimage under reduction modulo p^j of a nonempty subset of $W_N^0(\mathbb{Z}/p^j\mathbb{Z})$ for some $j > 0$ for each p; and

(2) for all sufficiently large p, $\mathfrak{S}_p$ contains all elements $(A, B) \in W_N^0(\mathbb{Z}_p)$ such that $Q(A, B)$ is a p-adic unit, where Q is a certain relative invariant for the action of G_N on W_N^0 over $\mathbb{Z}$ (see Proposition 2.1 for the precise definition of Q).

We call a subset $S \subset W_N(\mathbb{Z})$ a *big family in* $W_N(\mathbb{Z})$ if

$$S = \mathrm{inv}^{-1}\big(U_N(\mathbb{Z})^{(r)}\big) \cap \bigcap_p S_p,$$

where the sets $S_p \subset W_N(\mathbb{Z}_p)$ are $\mathrm{SL}_N(\mathbb{Z}_p)$-invariant, and the intersections $\mathfrak{S}_p = S_p \cap W_N^0(\mathbb{Z}_p)$ define a big family

$$\mathfrak{S} = \mathrm{inv}^{-1}\big(U_N(\mathbb{Z})^{(r)}\big) \cap W_N^0(\mathbb{Z}) \cap \bigcap_p \mathfrak{S}_p$$

in $W_N^0(\mathbb{Z})$.

Define the *height* of (A, B) by $\mathrm{H}(A, B) := \mathrm{H}(\mathrm{inv}(A, B))$. The following result gives an asymptotic for the count of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits of bounded height in a big family in $W_N(\mathbb{Z})$.

Theorem 1.5. *Let $X > 0$, and let $\mathrm{N}_N^{(r)}(X)$ be the number of binary forms in $U_N(\mathbb{Z})^{(r)}$ whose coefficients are of size at most X. Let $S \subset \mathrm{inv}^{-1}(U_N(\mathbb{Z})^{(r)})$ be a big family in $W_N(\mathbb{Z})$. Then the number of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on S of height less than X is given by*

$$\mathrm{N}_N^{(r)}(X) \times \prod_p \int_{f \in U_N(\mathbb{Z}_p)} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap S_p \cap W_N^0(\mathbb{Z}_p)}{G_N(\mathbb{Z}_p)}\right) df + o(X^{N+1}),$$

where df is the Haar measure on $U_N(\mathbb{Z}_p)$, normalized so that $\mathrm{Vol}(U_N(\mathbb{Z}_p)) = 1$.

Theorem 1.5 expresses the asymptotic count of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on S of bounded height in terms of a product of local integrals. The integrand of the integral at p – namely, the number of $G_N(\mathbb{Z}_p)$-orbits of pairs $(A, B) \in S_p \cap W_N^0(\mathbb{Z}_p)$ with $\mathrm{inv}(A, B) = f$ – appears to be quite difficult to evaluate in general, even for small degrees N and simple choices of the sets S_p. On the other hand, the integral at p can be rendered more tractable by performing a suitable change-of-variables, where instead of integrating over $f \in U_N(\mathbb{Z}_p)$, one integrates over $(A, B) \in W_N^0(\mathbb{Z}_p)$. Upon performing this change-of-variables at each prime p, we obtain the following variant of Theorem 1.5.

Theorem 1.6. *Let $X > 0$, and let $S \subset \mathrm{inv}^{-1}(U_N(\mathbb{Z})^{(r)})$ be a big family in $W_N(\mathbb{Z})$. Then the number of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on S of height less than X is given by*

$$\mathrm{N}_N^{(r)}(X) \times \prod_p \xi_{p,n} \int_{w \in S_p \cap W_N^0(\mathbb{Z}_p)} |Q(w)|_p \, dw + o(X^{N+1}),$$

where

$$\xi_{p,n} := (1 - p^{-1})^{-1}(1 - p^{-n-1})^{-1} \times \prod_{i=2}^{n} (1 - p^{-i})^{-1},$$

$|-|_p$ denotes the usual p-adic absolute value, and where dw denotes the Haar measure on $W_N^0(\mathbb{Z}_p)$, normalized so that $\mathrm{Vol}(W_N^0(\mathbb{Z}_p)) = 1$.

The formulation of the asymptotic given in Theorem 1.6 is far more conducive to evaluation in specific examples. For instance, taking $S_p = W_N(\mathbb{Z}_p)$ for every prime p, we obtain the following asymptotic formula for the total count of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $W_N(\mathbb{Z})$.

Theorem 1.7. *Suppose $X > 0$. Then the number of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $\mathrm{inv}^{-1}(U_N(\mathbb{Z})^{(r)})$ of height less than X is given by*

$$\mathrm{N}_N^{(r)}(X) \times \prod_{i=2}^{N} \zeta(i) + o(X^{N+1}).$$

Strikingly, Theorem 1.7 implies that the average number of reducible orbits lying above an integral binary N-ic form is equal to $\prod_{i=2}^{N} \zeta(i)$, which is simply the fundamental volume of the group SL_N (i.e., the volume of $\mathrm{SL}_N(\mathbb{Z})\backslash \mathrm{SL}_N(\mathbb{R})$ with respect to Haar measure on $\mathrm{SL}_N(\mathbb{R})$, suitably normalized). This phenomenon – that the average number of reducible orbits lying above a given set of invariants equals the fundamental volume of the group – holds for many other representations of interest in arithmetic statistics. Indeed, as proven in [25, Theorem 1], this holds for the representation of the split orthogonal group on the space of N-ary quadratic forms for every integer $N \geq 3$, odd or even; furthermore, as explained in [25, Question 2 and subsequent discussion], this also holds for the representations of GL_2 on binary cubic and quartic forms.

We now turn our attention to applying Theorem 1.6 to prove our main results on class group statistics, namely Theorems 1.1.A and 1.1.B. We say that a pair $(A, B) \in W_N(\mathbb{Z}_p)$ is *projective* if it corresponds to a 2-torsion ideal class under the Bhargava–Wood parametrization. As explained in Definition 4.2 (see Section 4.2, to follow), the condition of projectivity is given by a congruence condition modulo p for each prime p.

It is possible to determine the proportion of projective elements of $W_N(\mathbb{Z}_p)$ for each prime p; this was essentially achieved in [13, §6] for $N = 3$ and [21, §6.1]

for $N \geq 3$. On the other hand, to apply Theorem 1.6 it is necessary to determine the proportion of projective elements of $W_N^0(\mathbb{Z}_p)$ *having a specified* Q*-invariant*, and this appears to be intractable in general. Nonetheless, when $N = 3$, the condition of being projective is not too complicated, and the relevant p-adic integrals can be evaluated. We thus obtain the following result giving the average 2-torsion in the ideal groups of cubic orders enumerated by discriminant.

Theorem 1.8.A. *When either totally real or complex irreducible cubic orders $\mathcal{O}$ are enumerated by the absolute values of their discriminants, the average* 2*-torsion in the ideal group is* $\frac{\zeta(2)}{\zeta(4)}$.

We also simultaneously obtain the following variant of Theorem 1.8.A for the family of cubic orders defined by binary cubic forms enumerated by height.

Theorem 1.8.B. *When forms $f \in U_3(\mathbb{Z})^{(r)}$ are enumerated by height, the average* 2*-torsion in the ideal group is* $\frac{\zeta(2)}{\zeta(4)}$.

Theorem 1.1.A (resp., Theorem 1.1.B) now follows immediately upon combining Theorem 1.2.A (resp., Theorem 1.2.B in the case $N = 3$) with Theorem 1.8.A (resp., Theorem 1.8.B). As for orders defined by binary forms of higher odd degree, we obtain the following weaker result by simply combining Theorem 1.7 with Theorem 1.2.B.

Theorem 1.9. *Let $N > 3$. When primitive forms $f \in U_N(\mathbb{Z})^{(r)}$ are enumerated by height, the average sizes of $\mathcal{I}(R_f)[2]$ and $\mathrm{Cl}(R_f)[2]$ are bounded.*

1.2. Historical context and related work

The problem of studying the arithmetic statistics of nonmaximal orders in number fields dates back to the seminal work of Davenport [17, 18], who determined the density of discriminants of orders in cubic fields (i.e., he obtained an asymptotic formula for the number of cubic orders having bounded discriminant). This result was generalized in work of Bhargava, Shankar, and Tsimerman [11, Theorem 8], who determined the density of discriminants of cubic orders satisfying general infinite sets of local specifications. As for orders of higher degree, Bhargava used the parametrizations of quartic/quintic orders that he developed in his thesis [3, 5] to determine asymptotic formulas for the number of orders having bounded discriminant in quartic/quintic fields with Galois group equal to the full symmetric group [4, 6].

More recently, progress has been made toward understanding the distribution of *class groups* of orders in number fields. The first result in this direction is due to Bhargava and Varma [14], who determined the average 3-torsion in the class groups of quadratic orders. Specifically, they showed that when real (resp., complex) quadratic

orders are enumerated by discriminant, the average 3-torsion in the class group is given by $1 + \frac{1}{3} \times \frac{\zeta(2)}{\zeta(3)}$ (resp., $1 + \frac{\zeta(2)}{\zeta(3)}$). This extends an earlier result of Davenport and Heilbronn [19], who determined the corresponding average to be $\frac{4}{3}$ (resp., 2) for the family of maximal quadratic orders (i.e., rings of integers of quadratic number fields).

As explained in Section 1.1, Bhargava and Varma proved Theorem 1.2.A, which describes the average 2-torsion in the class groups of cubic orders in terms of the average 2-torsion in their ideal groups [13], and their result was generalized to orders defined by binary forms of any odd degree $N \geq 3$ by Ho, Shankar, and Varma, who proved Theorem 1.2.B. A similar result was proven for *monogenic* orders – i.e., orders defined by *monic* binary forms – of odd degree by Siad in [26, Theorem 9]. In the case of monogenic orders of odd degree N, the problem of counting 2-torsion ideals boils down to a problem of counting reducible orbits of the aforementioned representation of the split orthogonal group acting on the space of N-ary quadratic forms. As explained in Section 1.1, asymptotics akin to Theorems 1.5–1.7 were proven for reducible orbits of this representation in [25]; these asymptotics were then applied in [28, §5.6] with $N = 3$ to determine the average 2-torsion in the ideal groups of monogenic cubic orders. Combining this with the aforementioned result of Siad, we deduced (see [28, Theorem 173]) that when monogenic cubic orders are enumerated by height, the average 2-torsion in the class group is given by $\frac{5}{4} + \frac{1}{4} \times \frac{\zeta(2)}{\zeta(3)}$ (resp., $\frac{3}{2} + \frac{1}{2} \times \frac{\zeta(2)}{\zeta(3)}$). This extends an earlier result of Bhargava, Hanke, and Shankar [9], who determined the corresponding average to be $\frac{3}{2}$ (resp., 2) for the family maximal monogenic cubic orders.

We note that the problem of counting reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $W_N(\mathbb{Z})$ was first considered by Bhargava, Shankar, and Wang in [12], where they used geometry-of-numbers methods to determine upper bounds of roughly the correct order of magnitude on the number of reducible orbits having large Q-invariant. They applied these upper bounds to prove a squarefree sieve for binary forms. In this paper, their bounds serve as a key ingredient in the proofs of our main theorems. Thus, we indirectly use *upper bounds* for the count of reducible orbits to obtain *precise asymptotics* for this count!

It is natural to ask what can be said for binary forms of even degree. We expect that the methods of [27, 29] can be adapted to determine the average 2-torsion in the class group of orders defined by binary forms of even degree in terms of the average 2-torsion in the ideal group; however, in the even-degree setting, the parametrization of 2-torsion ideal classes is significantly more complicated (e.g., it depends on the leading coefficient of the binary forms under consideration, and one must count reducible orbits in multiple families of representations). It is also natural to ask whether analogues of Theorems 1.5–1.7 can be proven for the action of SL_N on pairs of

$N \times N$ symmetric matrices, where $N = 2n \geq 4$ is even. This representation was studied by Bhargava in [7] (cf. the closely related work of Bhargava, Gross, and Wang [8]), where he shows that this representation does *not* possess an analogous notion of reducibility and is thus able to determine asymptotics for the count of its integral orbits.

2. Algebraic preliminaries

In this section, we introduce the representation of SL_N on W_N and prove several useful results about the action of various subgroups of SL_N on various linear subspaces in W_N. In particular, we define and study the subgroup G_N and the linear subspace W_N^0 referenced in Section 1.1. We conclude by proving Theorem 1.3, which gives a local-to-global principle for the action of G_N on W_N^0.

2.1. Action of SL_N on W_N

For integers $m, m' > 0$, let $\mathrm{Mat}_{m\times m'}$ denote the affine scheme over $\mathbb{Z}$ whose R-points are given by the set of $m \times m'$ matrices with entries in R for any $\mathbb{Z}$-algebra R. As in Section 1.1, let $N = 2n + 1 \geq 3$ be an odd integer, and let W_N be the space of pairs of $N \times N$ symmetric matrices (i.e., we have $W_N(R) = R^2 \otimes_R \mathrm{Sym}^2 R^N$ for any $\mathbb{Z}$-algebra R). The space W_N has a natural structure of SL_N-representation given as follows: for any $g \in \mathrm{SL}_N(R)$ and any $(A, B) \in W_N(R)$, let

$$g \cdot (A, B) = \left(gAg^T, gBg^T\right) \in W_N(R),$$

where for a matrix M, we denote by M^T its transpose.

Let U_N be the affine scheme over $\mathbb{Z}$ whose R-points are binary N-ic forms over R for any $\mathbb{Z}$-algebra R. Define a map inv: $W_N \to U_N$ as follows: given a pair $(A, B) \in W_N(R)$, we set

$$\mathrm{inv}(A, B) := (-1)^n \det(xA - yB) \in U_N(R).$$

One readily checks that the coefficients of $\mathrm{inv}(A, B)$ are SL_N-invariant; in fact, it is known [24] that if $f_i \colon W_N \to \mathbb{A}^1$ is the map that takes $(A, B) \in W_N(R)$ and returns the $x^{N-i}y^i$-coefficient of $\mathrm{inv}(A, B)$, then the ring of polynomial invariants for the action of SL_N on W_N is freely generated by the functions f_i for $i \in \{0, \ldots, N\}$. In [21, §4.1], an explicit algebraic section σ_0 defined over $\mathbb{Z}$ was constructed for the map inv: $W_N \to U_N$ (by "algebraic" and "defined over $\mathbb{Z}$," we mean that the matrix entries of σ_0 are polynomials with integer coefficients). Concretely, this section takes

$$f(x, y) = \sum_{i=0}^{N} f_i x^{N-i} y^i \in U_N(R)$$

to the pair

$$\sigma_0(f) = \left(\left[\begin{array}{c|c} & \begin{array}{ccc} & & 1 \\ & \iddots & \\ 1 & & \end{array} \\ \hline \begin{array}{ccc} & & 1 \\ & \iddots & \\ 1 & & \end{array} & \begin{array}{ccc} f_0 & & \\ & \ddots & \\ & & f_{N-1} \end{array} \end{array}\right], \left[\begin{array}{c|c} & \begin{array}{ccc} & & 1 \\ & \iddots & \\ 1 & & \end{array} \\ \hline \begin{array}{ccc} & & 1 \\ & \iddots & \\ 1 & & \end{array} & \begin{array}{ccc} -f_1 & & \\ & \ddots & \\ & & -f_N \end{array} \end{array}\right] \right),$$

where empty entries are used to denote zeros, and where we have inserted horizontal and vertical lines immediately after row and column n in both matrices.

Let K be a field. As mentioned in Section 1.1, a pair $(A, B) \in W_N(K)$ is said to be *reducible* over K if the symmetric bilinear forms defined by A and B share a maximal (i.e., n-dimensional) isotropic space, and *irreducible* otherwise. The condition of being (ir)reducible is evidently $\mathrm{SL}_N(K)$-invariant, so we may speak of the (ir)reducible $\mathrm{SL}_N(K)$-orbits on $W_N(K)$. If R is an integral domain with field of fractions K, we say that an $\mathrm{SL}_N(R)$-orbit on $W_N(R)$ is (ir)reducible if the corresponding property holds for the $\mathrm{SL}_N(K)$-orbit containing it.

In the case $N = 3$, we will have occasion to combine the action of SL_3 on W_3 with the action of GL_2 on U_3. Recall that GL_2 acts on U_3 via linear change-of-variable; i.e., given $\gamma \in \mathrm{GL}_2(R)$ and $f \in U_3(R)$, we have

$$(\gamma \cdot f)(x, y) = f((x, y) \cdot \gamma).$$

The ring of polynomial invariants for the action of GL_2 on U_3 is freely generated by a single element known as the *discriminant*. We have an action of $\mathrm{GL}_2 \times \mathrm{SL}_3$ on W_3 defined as follows: given $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2(R)$, $g \in \mathrm{SL}_3(R)$, and $(A, B) \in W_N(R)$, we set

$$(\gamma, g) \cdot (A, B) = \left(g(aA - bB)g^T, g(cA - dB)g^T\right).$$

The map inv: $W_3 \to U_3$ is equivariant for the GL_2-action, and the ring of polynomial invariants for the action of $\mathrm{GL}_2 \times \mathrm{SL}_3$ on W_3 is generated by the function obtained by postcomposing the map inv with the discriminant map $U_3 \to \mathbb{A}^1$.

2.2. Action of subgroups of SL_N on linear subspaces in W_N

For a matrix M, denote its row-i, column-j entry by M_{ij}. We now introduce three linear subspaces in W_N and study the actions of certain subgroups of SL_N on them.

2.2.1. Action of $\mathrm{SL}_n \times \mathrm{SL}_{n+1}$ on W_N^{top}. Let $W_N^{\mathrm{top}} \subset W_N$ denote the linear subspace whose R-points are given by

$$W_N^{\mathrm{top}}(R) := \left\{(A, B) \in W_N(R) : A_{ij} = B_{ij} = 0 \text{ if } i, j \le n \text{ or } i, j \ge n+1\right\}$$

for any $\mathbb{Z}$-algebra R. When it is convenient, we think of elements of W_N^{top} as being pairs of $n \times (n+1)$ matrices, by considering just the top-right $n \times (n+1)$ blocks.

Let $\mathrm{SL}_n \times \mathrm{SL}_{n+1} \subset \mathrm{SL}_N$ be the subgroup consisting of block-diagonal matrices, where the diagonal consists of one $n \times n$ block followed by one $(n+1) \times (n+1)$ block, both having determinant 1. The action of SL_N on W_N restricts to an action of $\mathrm{SL}_n \times \mathrm{SL}_{n+1}$ on W_N^{top}.

We now describe the action of $\mathrm{SL}_n \times \mathrm{SL}_{n+1}$ on W_N^{top} over a field K.

Proposition 2.1. *The ring of polynomial invariants of the action of* $\mathrm{SL}_n \times \mathrm{SL}_{n+1}$ *on* W_N^{top} *is generated by a single polynomial* Q *such that for any field* K *and any* $Q_0 \in K^\times$*, the set*

$$Q^{-1}(Q_0) \subset W_N^{\mathrm{top}}(K)$$

is nonempty and consists of a single $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(K)$*-orbit. Moreover, the stabilizer of any element of this orbit is trivial.*

Proof. Proposition 2.1 amounts to stating that the representation of $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(K)$ on $W_N^{\mathrm{top}}(K)$ is "prehomogeneous," and the proof is identical to that of [12, Proposition 3.1]. The main observation is that, for any integer $n_0 \ge 2$, the representation of $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(K)$ on $W_N^{\mathrm{top}}(K)$ in the case $n = n_0$ is related to the representation of $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(K)$ on $W_N^{\mathrm{top}}(K)$ in the case $n = n_0 - 1$ by what Sato and Kimura call a "castling transform" (see [23, §2]). Since the property of being prehomogeneous is preserved under castling transforms, it suffices to prove the lemma in the case $n = 1$, where the action of $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(K)$ on $W_N^{\mathrm{top}}(K)$ may be identified with the action of $\mathrm{SL}_2(K)$ on $\mathrm{Mat}_{2\times 2}(K)$ by right-multiplication. The desired polynomial invariant function Q for this action is given simply by the determinant.

We now describe the invariant Q for $n > 1$. Given a $\mathbb{Z}$-algebra R and a pair $(A, B) \in W_N^{\mathrm{top}}(R)$, we take $Q(A, B)$ to be the "hyperdeterminant" of (A, B), which is defined explicitly as follows. For each $i \in \{1, \ldots, n+1\}$, let $A^{(i)}$ and $B^{(i)}$ be the $n \times n$ matrices obtained from A and B, respectively, by considering the top-right $n \times (n+1)$ block and deleting the ith column. Then $Q(A, B)$ is the determinant of the $(n+1) \times (n+1)$ matrix whose row-i, column-j entry is the $x^{n-j+1}y^{j-1}$-entry of the binary n-ic form $(-1)^{i+1} \det(xA^{(i)} - yB^{(i)})$.

That $Q^{-1}(Q_0)$ is nonempty for any $Q_0 \in K^\times$ follows by examining the following pair of matrices in $W_N^{\mathrm{top}}(K)$:

$$\left(\begin{bmatrix} & & & 1 \\ & & 1 & \\ & \iddots & & \\ 1 & & & \end{bmatrix}, \begin{bmatrix} & & & \pm Q_0 \\ & & 1 & \\ & \iddots & & \\ 1 & & & \end{bmatrix}\right) \tag{1}$$

The pair in (1) evidently has Q-invariant Q_0 or $-Q_0$, depending on the choice of sign of the entry "$\pm Q_0$." In fact, this pair gives an explicit section of the map

$$Q\colon W_N^{\mathrm{top}} \to \mathbb{A}^1,$$

defined over $\mathbb{Z}$. As for the claim about stabilizers, the action of $\mathrm{SL}_2(K)$ by right-multiplication on matrices of nonzero determinant in $\mathrm{Mat}_{2\times 2}(K)$ obviously has trivial stabilizers, and stabilizers are preserved under castling transforms. ∎

2.2.2. Action of L_N on $W_N^{\mathrm{top},0}$. Let $W_N^{\mathrm{top},0} \subset W_N^{\mathrm{top}}$ be the linear subspace whose R-points are given by

$$W_N^{\mathrm{top},0}(R) := \big\{(A, B) \in W_N^{\mathrm{top}}(R) : A_{ij} = 0 \text{ if } i + j \le 2n + 1 \text{ and } B_{ij} = 0 \text{ if } i + j \le 2n\big\}$$

for any $\mathbb{Z}$-algebra R. Let $L_N \subset \mathrm{SL}_n \times \mathrm{SL}_{n+1}$ be the lower-triangular subgroup. Then the action of $\mathrm{SL}_n \times \mathrm{SL}_{n+1}$ on W_N^{top} restricts to an action of L_N on $W_N^{\mathrm{top},0}$. Given $(A, B) \in W_N^{\mathrm{top},0}(R)$, we have the following formula for the Q-invariant up to sign:

$$Q(A, B) = \pm \prod_{i=1}^{n} A_{i,N+1-i}^{n+1-i} \prod_{i=1}^{n} B_{i,N-i}^{i}. \tag{2}$$

We now describe this restricted action of $L_N(K)$ on $W_N^{\mathrm{top},0}(K)$ for K a field.

Proposition 2.2. *Let K be a field, and let $Q_0 \in K^\times$. Then the set*

$$Q^{-1}(Q_0) \cap W_N^{\mathrm{top},0}(K)$$

is nonempty and consists of a single $L_N(K)$-orbit. Moreover, the stabilizer of any element of this orbit is trivial.

Proof. The nonemptiness statement follows immediately from the existence of the explicit section (1), which has image contained in $W_N^{\mathrm{top},0}$. The statement about stabilizers is obvious.

As for the transitivity statement, take $(A, B) \in Q^{-1}(Q_0) \cap W_N^{\mathrm{top},0}(K)$. It suffices to show that (A, B) is $L_N(K)$-equivalent to (1). First, by replacing (A, B) with a

suitable translate under the action of a diagonal element in $L_N(K)$, we may assume that $A_{ij} = 1$ for all $i + j = N + 1$ and that $B_{ij} = 1$ for all $i + j = N$, except when $(i, j) = (1, N - 1)$, in which case $B_{1(N-1)} = \pm Q_0$. Now, call a lower-triangular unipotent element $g \in \mathrm{SL}_N(K)$ *elementary* if $g_{ij} = 0$ for all but one pair (i, j) with $i > j$. It is easy to verify by inspection that, by hitting (A, B) with a suitable sequence of elementary unipotent elements of $L_N(K)$, we can successively clear out the values of the following matrix entries:

$$\begin{gathered} B_{1(2n+1)},\ A_{2(2n+1)},\ B_{2(2n)},\ B_{2(2n+1)},\ \ldots, \\ A_{k(2n+3-k)},\ \ldots,\ A_{k(2n+1)},\ B_{k(2n+2-k)},\ \ldots,\ B_{k(2n+1)},\ \ldots, \\ A_{n(n+3)},\ \ldots,\ A_{n(2n+1)},\ B_{n(n+2)},\ \ldots,\ B_{n(2n+1)}. \end{gathered} \tag{3}$$

We may thus assume that the matrix entries of (A, B) that are listed in (3) are all equal to 0. But then (A, B) is equal to (1), which is sufficient. ∎

Corollary 2.3. *If two elements of $Q^{-1}(Q_0) \cap W_N^{\mathrm{top},0}(K)$ are equivalent under the action of $g \in (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(K)$, then we have $g \in L_N(K)$.*

Proof. Suppose for some $g_1 \in (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(K)$ and elements $(A_1, B_1), (A_2, B_2) \in Q^{-1}(Q_0) \cap W_N^{\mathrm{top},0}(K)$, we have

$$g_1 \cdot (A_1, B_1) = (A_2, B_2).$$

By Proposition 2.2, there exists $g_2 \in L_N(K)$ such that

$$g_2 \cdot (A_1, B_1) = (A_2, B_2),$$

so $g_2^{-1} g_1$ stabilizes (A_1, B_1), but by Proposition 2.1, the stabilizer of (A_1, B_1) in $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(K)$ is trivial, so $g_1 = g_2$, as necessary. ∎

2.2.3. Fundamental domain for $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p) \curvearrowright W_N^{\mathrm{top}}(\mathbb{Z}_p)$. Using the results of Sections 2.2.1–2.2.2, we now construct a fundamental domain for the action of $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$ on $W_N^{\mathrm{top}}(\mathbb{Z}_p)$; this fundamental domain plays a crucial role in the proof of Theorem 1.7 (see Section 4.1).[2]

We start by choosing a convenient partition of $W_N^{\mathrm{top}}(\mathbb{Z}_p)$ into subsets indexed by pairs of nonnegative-integer-vectors of length n. Given

$$\vec{a} = (a_1, \ldots, a_n), \quad \vec{b} = (b_1, \ldots, b_n) \in \mathbb{N}^n,$$

[2]Note that by a "fundamental domain" for the action of a group on a set, we mean a subset that contains exactly one element of each orbit.

define a subset $\mathcal{L}_{\vec{a},\vec{b}}(p)$ as follows:

$$\begin{aligned}\mathcal{L}_{\vec{a},\vec{b}}(p) := (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p) \\ \times \big\{(A,B) \in W_N^{\mathrm{top},0}(\mathbb{Z}_p) : v_p(A_{ij}) = a_i \text{ for } (i,j) \text{ with } i+j = N+1, \\ v_p(B_{ij}) = b_i \text{ for } (i,j) \text{ with } i+j = N\big\}.\end{aligned}$$

Take $(A,B) \in \mathcal{L}_{\vec{a},\vec{b}}(p)$. By the proof of Proposition 2.2, we can use the action of $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Q}_p)$ to make

$$\begin{aligned}A_{ij} &= 0 \quad \text{for each } (i,j) \text{ with } i+j > N+1, \text{ and} \\ B_{ij} &= 0 \quad \text{for each } (i,j) \text{ with } i+j > N,\end{aligned}$$

without changing A_{ij} for each (i,j) with $i+j = N+1$ and B_{ij} for each (i,j) with $i+j = N$. Then one readily computes using (2) that

$$|Q(A,B)|_p^{-1} = \prod_{i=1}^{n} p^{(n+1-i)a_i + ib_i}. \tag{4}$$

The following proposition gives the desired fundamental domain in terms of the sets $\mathcal{L}_{\vec{a},\vec{b}}(p)$.

Proposition 2.4. *For each $\vec{a}, \vec{b} \in \mathbb{N}^n$, a fundamental domain for the action of*

$$(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$$

on the set $\mathcal{L}_{\vec{a},\vec{b}}(p)$ is given by

$$\begin{aligned}\big\{(A,B) \in W_N^{\mathrm{top},0}(\mathbb{Z}_p) : A_{ij} = p^{a_i} \text{ for } (i,j) \text{ with } i+j = N+1, \\ A_{ij} \in \{0,\dots,p^{a_{N+1-j}} - 1\}. \\ \text{for } (i,j) \text{ with } i+j > N+1 \text{ and } i \le n, \\ B_{ij} = p^{b_i} \text{ for } (i,j) \text{ with } i+j = N \text{ and } i > 1, \\ v_p(B_{1(N-1)}) = b_1, \\ B_{ij} \in \{0,\dots,p^{b_i} - 1\} \text{ for } (i,j) \text{ with } i+j > N \text{ and } i \le n\big\}.\end{aligned} \tag{5}$$

A fundamental domain for the action of $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$ on the set

$$\big\{(A,B) \in W_N^{\mathrm{top}}(\mathbb{Z}_p) : Q(A,B) \neq 0\big\}$$

is given by the (disjoint) union of the set (5) over all $\vec{a}, \vec{b} \in \mathbb{N}^n$.

Proof. First note that we have

$$\mathcal{L}_{\vec{a},\vec{b}}(p) \cap W_N^{\mathrm{top},0}(\mathbb{Z}_p) = \big\{(A,B) \in W_N^{\mathrm{top},0}(\mathbb{Z}_p) : \\ v_p(A_{ij}) = a_i \text{ for } (i,j) \text{ with } i+j = N+1, \\ v_p(B_{ij}) = b_i \text{ for } (i,j) \text{ with } i+j = N\big\}. \tag{6}$$

Indeed, the left-hand side of (6) obviously contains the right-hand side. As for the reverse containment, if $(A,B) \in \mathcal{L}_{\vec{a},\vec{b}}(p) \cap W_N^{\mathrm{top},0}(\mathbb{Z}_p)$, then there exist an element $g \in (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$ and a pair (A',B') belonging to the right-hand side of (6) such that

$$(A,B) = g \cdot (A',B').$$

By Corollary 2.3, we must have $g \in L_N(\mathbb{Z}_p)$, so since the action of $L_N(\mathbb{Z}_p)$ preserves the right-hand side of (6), the pair (A,B) must belong to it as well.

The next step is to show that the action of $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$ can be used to move points in $W_N^{\mathrm{top}}(\mathbb{Z}_p)$ into the linear subspace $W_N^{\mathrm{top},0}(\mathbb{Z}_p)$.

Lemma 2.5. *Let $Q_0 \in \mathbb{Z}_p \smallsetminus \{0\}$. Then every $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$-orbit on $Q^{-1}(Q_0) \subset W_N^{\mathrm{top}}(\mathbb{Z}_p)$ meets $W_N^{\mathrm{top},0}(\mathbb{Z}_p)$.*

Proof of Lemma 2.5. The proof is similar to that of [28, Lemma 206]. Take

$$(A,B) \in Q^{-1}(Q_0) \cap W_N^{\mathrm{top}}(\mathbb{Z}_p).$$

Then there exists $g \in (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Q}_p)$ such that $g \cdot (A,B) \in W_N^{\mathrm{top},0}(\mathbb{Z}_p)$, because the section (1) of Q is defined over $\mathbb{Z}_p$ with image contained in $W_N^{\mathrm{top},0}$, and because the elements of the set $Q^{-1}(Q_0) \cap W_N^{\mathrm{top}}(\mathbb{Z}_p)$ belong to the same $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Q}_p)$-orbit by Proposition 2.1.

By the p-adic Iwasawa decomposition, we have that

$$(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Q}_p) = L_N(\mathbb{Q}_p)(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p),$$

so there exists $g_1 \in L_N(\mathbb{Q}_p)$ and $g_2 \in (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$ such that $g = g_1 g_2$. But L_N acts on $W_N^{\mathrm{top},0}$ (see Section 2.2.2 for further details), so $g_2 \cdot (A,B) \in W_N^{\mathrm{top},0}(\mathbb{Q}_p)$. Since $g_2 \in (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$ and $(A,B) \in W_N^{\mathrm{top}}(\mathbb{Z}_p)$, we must in fact have that $g_2 \cdot (A,B) \in W_N^{\mathrm{top},0}(\mathbb{Z}_p)$. ∎

Now, by Lemma 2.5 and Corollary 2.3, it suffices to show that (5) is a fundamental domain for the action of $L_N(\mathbb{Z}_p)$ on $\mathcal{L}_{\vec{a},\vec{b}}(p) \cap W_N^{\mathrm{top},0}(\mathbb{Z}_p)$, but this follows by adapting the proof of Proposition 2.2 to work over $\mathbb{Z}_p$. Take

$$(A,B) \in \mathcal{L}_{\vec{a},\vec{b}}(p) \cap W_N^{\mathrm{top},0}(\mathbb{Z}_p).$$

First, instead of using diagonal transformations to make

$$A_{ij} = 1 \quad \text{for } (i,j) \text{ with } i+j = N+1, \text{ and}$$
$$B_{ij} = 1 \quad \text{for } (i,j) \text{ with } i+j = N, \text{ except when } (i,j) = (1, N-1),$$

we use these transformations to make

$$A_{ij} = p^{a_i} \quad \text{for } (i,j) \text{ with } i+j = N+1, \text{ and}$$
$$B_{ij} = p^{b_i} \quad \text{for } (i,j) \text{ with } i+j = N, \text{ except when } (i,j) = (1, N-1).$$

Then, instead of using elementary unipotent transformations to make the remaining matrix entries zero, we use these transformations to reduce these matrix entries modulo $p^{a_1}, \dots, p^{a_n}, p^{b_1}, \dots, p^{b_n}$. This establishes that each orbit for the action of $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$ on $\mathscr{L}_{\vec{a},\vec{b}}(p)$ meets the set (5) at least once.

On the other hand, if (A, B), (A', B') belong to the set (5) and there exists an element $g \in (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$ such that $(A, B) = g \cdot (A', B')$, then by Corollary 2.3, we must have $g \in L_N(\mathbb{Z}_p)$. Write $g = g_1 g_2$, where g_1 is unipotent and g_2 is diagonal. Denote the diagonal entries of g_2 by $(g_2)_{ii}$. Observe that we have the equalities

$$(g_2)_{ii}(g_2)_{jj} A'_{ij} = (g \cdot A')_{ij} = A_{ij} = p^{a_i} = A'_{ij} \tag{7}$$

for (i,j) with $i+j = N+1$ and $i \le n$, and that we have

$$(g_2)_{ii}(g_2)_{jj} B'_{ij} = (g \cdot B')_{ij} = B_{ij} = p^{b_i} = B'_{ij} \tag{8}$$

for (i,j) with $i+j = N$ and $1 < i \le n$. Combining (7) and (8) with the fact that $Q(A,B) = Q(A',B')$ along with the formula (2), we see that (8) holds when $i = 1$ too. Then combining (7) and (8) with the condition $\det g_2 = 1$ yields the following system of equations:

$$\begin{aligned}(g_2)_{ii}(g_2)_{(N-i)(N-i)} &= (g_2)_{ii}(g_2)_{(N+1-i)(N+1-i)} \\ &= \prod_{j=1}^{N} (g_2)_{jj} = 1 \quad \text{for each } i \in \{1, \dots, n\}.\end{aligned}$$

By comparing the products $\prod_{i=1}^{n}(g_2)_{ii}(g_2)_{(N-i)(N-i)}$ and $\prod_{j=1}^{N}(g_2)_{jj}$, we deduce that $(g_2)_{NN} = 1$, from which it follows that all $(g_2)_{ii} = 1$, and hence that $g_2 = \mathrm{id}$.

Next, denote the entries of g_1 by $(g_1)_{ij}$. Then the condition $B = g_1 \cdot B'$ implies that

$$B_{1(2n+1)} \equiv B'_{1(2n+1)} \pmod{p^{b_1}},$$

so the condition $B_{1(2n+1)}, B'_{1(2n+1)} \in \{0, \dots, p^{b_1} - 1\}$ forces $B_{1(2n+1)} = B'_{1(2n+1)}$ and hence that $(g_1)_{N(N-1)} = 0$. Since $(g_1)_{N(N-1)} = 0$, the condition $A = g_1 \cdot A'$ implies that

$$A_{2(2n+1)} \equiv A'_{2(2n+1)} \pmod{p^{a_1}},$$

so the condition $A_{2(2n+1)}, A'_{2(2n+1)} \in \{0, \dots, p^{a_1} - 1\}$ forces $A_{2(2n+1)} = A'_{2(2n+1)}$, and hence that $(g_1)_{21} = 0$. Continuing in this manner according to the sequence of matrix entries in (3), we see that the matrix entries of (A, B) and (A', B') coincide. ∎

2.2.4. The subgroup $G_N \subset \mathrm{SL}_N$. Let $G_N \subset \mathrm{SL}_N$ be the subgroup whose R-points are given by

$$G_N(R) := \{g \in \mathrm{SL}_N(R) : g_{ij} = 0 \text{ for all } (i, j) \text{ such that } i \leq n \text{ and } j \geq n + 1\}$$

for any $\mathbb{Z}$-algebra R.

An algebraic group G is said to have *class number* 1 *over* $\mathbb{Q}$ if the group $G(\mathbb{A}_\mathbb{Q})$ of adelic rational points is the "Frobenius" product of the subgroup $G(\mathbb{Q})$ of rational points with the subgroup $G(\mathbb{A}_\mathbb{Z})$ of adelic integral points, i.e., we have

$$G(\mathbb{A}_\mathbb{Q}) = G(\mathbb{Q})G(\mathbb{A}_\mathbb{Z}).$$

The following result establishes that this property holds for $G = G_N$.

Proposition 2.6. *The algebraic group G_N has class number* 1 *over* $\mathbb{Q}$.

Proof. The idea of the proof is to realize G_N as the Frobenius product of two subgroups, each of which has class number 1 over $\mathbb{Q}$, and then to use this product structure to deduce that G_N itself has class number 1 over $\mathbb{Q}$.

Let H_1 be the lower-triangular unipotent subgroup of G_N whose R-points are given by

$$H_1(R) := \big\{h \in G_N(R) : h_{ii} = 1 \text{ for all } i \text{ and } h_{jk} = 0 \text{ if } j < k \text{ or } j > k \geq n + 1 \text{ or } n \geq j > k\big\}$$

for any $\mathbb{Z}$-algebra R, and let H_2 be the block-diagonal subgroup of G_N whose R-points are given by

$$H_2(R) := \{g \in \mathrm{GL}_n(R) \times \mathrm{GL}_{n+1}(R) : \det g = 1\} \subset G_N(R).$$

Lemma 2.7. *The algebraic group G_N is the Frobenius product of its subgroups H_1 and H_2, i.e., for any $\mathbb{Z}$-algebra R, we have $G_N(R) = H_1(R)H_2(R)$. Moreover, we have that $H_1(R) \cap H_2(R) = 1$.*

Proof of Lemma 2.7. The second claim is clear from the definitions of H_1 and H_2. As for the first claim, take $g \in G_N(R)$, and write it in box form as follows:

$$g = \left[\begin{array}{c|c} g' & 0 \\ \hline g''' & g'' \end{array}\right],$$

where $g' \in \mathrm{GL}_n(R)$, $g'' \in \mathrm{GL}_{n+1}(R)$, and $g''' \in \mathrm{Mat}_{(n+1)\times n}(R)$. Then it is easy to see that

$$g = \left[\begin{array}{c|c} \mathrm{id} & 0 \\ \hline g'''g'^{-1} & \mathrm{id} \end{array}\right] \times \left[\begin{array}{c|c} g' & 0 \\ \hline 0 & g'' \end{array}\right],$$

where by "id" (resp., "0") we mean the identity (resp., zero) matrix of the relevant dimensions. ∎

The group H_1 has class number 1 over $\mathbb{Q}$ because it is isomorphic to the additive group $\mathbb{G}_a^{n^2+n}$; that H_2 has class number 1 over $\mathbb{Q}$ follows immediately from the fact that the same holds for the groups GL_n and GL_{n+1}. The next lemma gives a criterion under which the Frobenius product of two groups of class number 1 over $\mathbb{Q}$ is itself a group of class number 1 over $\mathbb{Q}$.

Lemma 2.8. *Let Γ be an algebraic group over $\mathbb{Z}$ that is the Frobenius product of two sub-algebraic-groups Γ_1 and Γ_2, both of which have class number 1 over $\mathbb{Q}$, and suppose that $\Gamma_1(\mathbb{A}_\mathbb{Z})\Gamma_2(\mathbb{Q}) \subset \Gamma_2(\mathbb{Q})\Gamma_1(\mathbb{A}_\mathbb{Q})$. Then Γ has class number 1 over $\mathbb{Q}$.*

Proof of Lemma 2.8. Clearly, $\Gamma(\mathbb{A}_\mathbb{Q}) \supset \Gamma(\mathbb{Q})\Gamma(\mathbb{A}_\mathbb{Z})$. As for the reverse inclusion, we have that

$$\begin{aligned} \Gamma(\mathbb{A}_\mathbb{Q}) = \Gamma_1(\mathbb{A}_\mathbb{Q})\Gamma_2(\mathbb{A}_\mathbb{Q}) &= \Gamma_1(\mathbb{Q})\Gamma_1(\mathbb{A}_\mathbb{Z})\Gamma_2(\mathbb{Q})\Gamma_2(\mathbb{A}_\mathbb{Z}) \\ &\subset \Gamma_1(\mathbb{Q})\Gamma_2(\mathbb{Q})\Gamma_1(\mathbb{A}_\mathbb{Q})\Gamma_2(\mathbb{A}_\mathbb{Z}) \\ &= \Gamma_1(\mathbb{Q})\Gamma_2(\mathbb{Q})\Gamma_1(\mathbb{Q})\Gamma_1(\mathbb{A}_\mathbb{Z})\Gamma_2(\mathbb{A}_\mathbb{Z}) \\ &= \Gamma(\mathbb{Q})\Gamma(\mathbb{A}_\mathbb{Z}). \end{aligned}$$ ∎

By Lemma 2.8, it now suffices to check that the criterion

$$H_1(\mathbb{A}_\mathbb{Z})H_2(\mathbb{Q}) \subset H_2(\mathbb{Q})H_1(\mathbb{A}_\mathbb{Q})$$

holds. This is an immediate consequence of the following matrix identity:

$$\left[\begin{array}{c|c} \mathrm{id} & 0 \\ \hline g''' & \mathrm{id} \end{array}\right] \times \left[\begin{array}{c|c} g' & 0 \\ \hline 0 & g'' \end{array}\right] = \left[\begin{array}{c|c} g' & 0 \\ \hline 0 & g'' \end{array}\right] \times \left[\begin{array}{c|c} \mathrm{id} & 0 \\ \hline g''^{-1}g'''g' & \mathrm{id} \end{array}\right].$$ ∎

2.2.5. Action of G_N on W_N^0. Let $W_N^0 \subset W_N$ be the linear subspace whose R-points are defined by

$$W_N^0(R) := \{(A, B) \in W_N(R) : A_{ij} = B_{ij} = 0 \text{ if } i, j \leq n\}$$

for any $\mathbb{Z}$-algebra R. Notice that, when R is an integral domain, every pair $(A, B) \in W_N^0(R)$ is reducible. The action of SL_N on W_N restricts to an action of G_N on W_N^0.

We extend the definition of the Q-invariant to any pair $(A, B) \in W_N^0(R)$ by defining $Q(A, B)$ to be the Q-invariant of the projection of (A, B) onto the linear subspace $W_N^{\mathrm{top}}(R)$ that sends the $(n+1) \times (n+1)$ entries in the bottom-right of A and B to zero. A fundamental property of the Q-invariant is that it divides the discriminant of the invariant binary form to order two, i.e., we have, $Q(A, B)^2 \mid \mathrm{disc}(\mathrm{inv}(A, B))$ for any $(A, B) \in W_N^0(R)$; for a proof, see [12, Theorem 3.5].

The function Q is notably *not* G_N-invariant, despite being invariant under the action of the subgroup $\mathrm{SL}_n \times \mathrm{SL}_{n+1} \subset G_N$; see, e.g., the proof of Proposition 3.3 (to follow). We note that the explicit section σ_0 described in Section 2.1 has image contained in the locus of points in W_N^0 with Q-invariant equal to $(-1)^{n+1}$.

We now describe the action of G_N on W_N^0 over a field K.

Proposition 2.9. *Let K be a field, and let $f \in U_N(K)$. Then the set*

$$\{(A, B) \in \mathrm{inv}^{-1}(f) \cap W_N^0(K) : Q(A, B) \neq 0\}$$

is nonempty and consists of a single $G_N(K)$-orbit. Moreover, the stabilizer of any element of this orbit is trivial.

Proof. That $\mathrm{inv}^{-1}(f) \cap W_N^0(R)$ is nonempty holds over any $\mathbb{Z}$-algebra R because of the existence of the aforementioned explicit section σ_0.

To see that $\{(A, B) \in \mathrm{inv}^{-1}(f) \cap W_N^0(K) : Q(A, B) \neq 0\}$ consists of a single $G_N(K)$-orbit, take $(A_0, B_0) \in \mathrm{inv}^{-1}(f) \cap W_N^0(K)$ with $Q_0 = Q(A_0, B_0) \in K^\times$. We claim that there exists $g_1 \in (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(K) \subset G_N(K)$ such that $(A, B) := g_1 \cdot (A_0, B_0)$ has the following shape, where empty entries are used to denote zeros, and star entries are used to denote numbers whose particular values are irrelevant:

$$(A, B) = \tag{9}$$

$$\left(\left[\begin{array}{ccc|ccccc} & & & & & & 1 \\ & & & & & 1 & \\ & & & & \iddots & & \\ & & & 1 & & & \\ \hline & & & * & * & \cdots & * & * \\ & & 1 & * & * & \cdots & * & * \\ & \iddots & & \vdots & \vdots & \ddots & \vdots & \vdots \\ & 1 & & * & * & \cdots & * & * \\ 1 & & & * & * & \cdots & * & * \end{array}\right], \left[\begin{array}{ccc|ccccc} & & & & & & & \pm Q_0 \\ & & & & & & 1 & \\ & & & & & \iddots & & \\ & & & & 1 & & & \\ \hline & & & 1 & * & \cdots & * & * & * \\ & & \iddots & & \vdots & \ddots & \vdots & \vdots & \vdots \\ & 1 & & & * & \cdots & * & * & * \\ \pm Q_0 & & & & * & \cdots & * & * & * \end{array}\right]\right).$$

In the above, we have inserted horizontal and vertical lines immediately after row and column n in the matrices A and B. The claim follows from Proposition 2.1 upon observing that by choosing the sign of the entry "$\pm Q_0$" appropriately, we can arrange for $Q(A, B) = Q_0$. In fact, by postcomposing g_1 with a suitable diagonal element in $G_N(K)$, we may take (A, B) to be of the form (9), with the entries "$\pm Q_0$" replaced by "1."

Now, just as in the proof of Proposition 2.2, by hitting (A, B) with a suitable sequence of elementary unipotent elements of $G_N(K)$, we can successively clear out the values of the following matrix entries:

$$\begin{aligned} &A_{(n+1)(n+2)},\ \ldots,\ A_{(n+1)(2n+1)},\ B_{(n+1)(n+2)},\ \ldots,\ B_{(n+1)(2n+1)},\\ &\qquad A_{(n+2)(n+3)},\ \ldots,\ A_{(n+2)(2n+1)},\ \ldots,\\ &B_{k(k+1)},\ \ldots,\ B_{k(2n+1)},\ A_{(k+1)(k+2)},\ \ldots,\ A_{(k+1)(2n+1)},\ \ldots,\\ &\qquad B_{(2n-1)2n},\ B_{(2n-1)(2n+1)},\ A_{(2n)(2n+1)},\ B_{(2n)(2n+1)}. \end{aligned} \tag{10}$$

We may thus assume that the matrix entries of (A, B) that are listed in (10) are all equal to 0. But then (A, B) lies in the image of the section σ_0, which is sufficient.

As for the claim about stabilizers, let (A_0, B_0) be as above. Suppose $g \in G_N(K)$ stabilizes (A_0, B_0). By Lemma 2.7, we may write $g = g_1 g_2$, where $g_i \in H_i(K)$ for each $i \in \{1, 2\}$. Since the projection map $W_N^0 \to W_N^{\text{top}}$ is invariant under the action of $H_1(K)$, it follows that g_2 must stabilize the projection of (A_0, B_0) onto $W_N^{\text{top}}(K)$. Thus, by Proposition 2.1, we have $g_2 = \text{id}$. Now, it is clear by inspection that the action of $H_1(K)$ on $W_N^0(K)$ has trivial stabilizers, so $g_1 = \text{id}$, and thus $g = g_1 g_2 = \text{id}$ too. ∎

We now work over $\mathbb{Z}_p$ for a prime p. We note that the p-adic absolute value $|Q(A, B)|_p$ is invariant under the action of $G_N(\mathbb{Z}_p)$. The following result describes the action of $G_N(\mathbb{Z}_p)$ on the locus of pairs in $W_N^0(\mathbb{Z}_p)$ with p-adic unit Q-invariant.

Proposition 2.10. *Let $f \in U_N(\mathbb{Z}_p)$. Then the set*

$$\{(A, B) \in \text{inv}^{-1}(f) \cap W_N^0(\mathbb{Z}_p) : |Q(A, B)|_p = 1\}$$

is nonempty and consists of a single $G_N(\mathbb{Z}_p)$-orbit. Moreover, the stabilizer of any element of this orbit is trivial.

Proof. The nonemptiness statement follows immediately from the existence of the explicit section σ_0, which has image contained in the locus of points in W_N^0 with Q-invariant equal to ± 1.

Next, let $W_N^{00} \subset W_N^0$ be the linear subspace whose R-points are given by

$$\begin{aligned} W_N^{00}(R) := \big\{(A, B) \in W_N^0(R) : A_{ij} = 0 \text{ if } i + j \leq 2n + 1 \\ \text{and } B_{ij} = 0 \text{ if } i + j \leq 2n\big\}. \end{aligned}$$

We remark that the explicit section σ_0 described in Section 2.1 has image contained in W_N^{00}. For the transitivity statement, by Lemma 2.5 it suffices to show that

$$\{(A, B) \in \text{inv}^{-1}(f) \cap W_N^{00}(\mathbb{Z}_p) : |Q(A, B)|_p = 1\}$$

is contained in a single $G_N(\mathbb{Z}_p)$-orbit, and the proof of Proposition 2.9 can be easily adapted to verify this.

Finally, the statement about stabilizers follows immediately from Proposition 2.9, which implies that the stabilizer in $G_N(\mathbb{Q}_p)$, and hence in $G_N(\mathbb{Z}_p)$, of any $(A, B) \in \mathrm{inv}^{-1}(f) \cap W_N^0(\mathbb{Z}_p)$ is trivial. This concludes the proof of Proposition 2.10. ∎

2.2.6. Fundamental domain for $G_N(\mathbb{Z}_p) \curvearrowright W_N^0(\mathbb{Z}_p)$. Using the results of the preceding subsubsections, we now construct a fundamental domain for the action of $G_N(\mathbb{Z}_p)$ on $W_N^0(\mathbb{Z}_p)$. Given $\vec{a} = (a_1, \ldots, a_n), \vec{b} = (b_1, \ldots, b_n) \in \mathbb{N}^n$, define a subset $\mathcal{W}_{\vec{a},\vec{b}}(p)$ as follows:

$$\mathcal{W}_{\vec{a},\vec{b}}(p) := \big\{(A, B) \in W_N^{00}(\mathbb{Z}_p) : A_{ij} = p^{a_i} \text{ for } (i, j) \text{ with } i + j = N + 1, \\ B_{ij} = p^{b_i} \text{ for } (i, j) \text{ with } i + j = N\big\}. \quad (11)$$

The following result gives the desired fundamental domain in terms of $\mathcal{W}_{\vec{a},\vec{b}}(p)$.

Proposition 2.11. *A fundamental domain for the action of $G_N(\mathbb{Z}_p)$ on the set*

$$\{(A, B) \in W_N^0(\mathbb{Z}_p) : Q(A, B) \neq 0\}$$

is given by

$$\bigsqcup_{\vec{a},\vec{b} \in \mathbb{N}^n} \mathcal{F}_{\vec{a},\vec{b}}(p),$$

where the sets $\mathcal{F}_{\vec{a},\vec{b}}(p)$ are defined as follows:

$$\mathcal{F}_{\vec{a},\vec{b}}(p) := \big\{(A, B) \in \mathcal{W}_{\vec{a},\vec{b}}(p) : \\ A_{ij} \in \{0, \ldots, p^{a_{N+1-j}} - 1\} \text{ for } (i, j) \text{ with } i + j > N + 1,\ i < j, \\ B_{ij} \in \{0, \ldots, p^{b_i} - 1\} \text{ for } (i, j) \text{ with } i + j > N,\ i \leq n, \\ B_{ij} \in \{0, \ldots, p^{b_{N-i}} - 1\} \text{ for } (i, j) \text{ with } i + j > N,\ n < i < j\big\}. \quad (12)$$

Proof. This follows by adapting the proof of Proposition 2.9 to work over $\mathbb{Z}_p$ (just as we adapted the proof of Proposition 2.2 to obtain Proposition 2.4). It follows from Proposition 2.4 that every $(A', B') \in W_N^0(\mathbb{Z}_p)$ with $Q(A', B') \neq 0$ is $G_N(\mathbb{Z}_p)$-equivalent to an element $(A, B) \in W_N^{00}(\mathbb{Z}_p)$ with

$$\begin{aligned} A_{ij} &= p^{a_i} && \text{for } (i, j) \text{ with } i + j = N + 1, \\ B_{ij} &= p^{b_i} && \text{for } (i, j) \text{ with } i + j = N \text{ and } i > 1, \text{ and} \\ B_{1(N-1)} &= u \cdot p^{b_1} && \text{for some } u \in \mathbb{Z}_p^\times, \text{ where } \vec{a}, \vec{b} \in \mathbb{N}^n. \end{aligned}$$

Using the action of the diagonal matrix with diagonal entries $(u^{-1}, 1, \ldots, 1, u) \in G_N(\mathbb{Z}_p)$, we can further arrange that $(A, B) \in \mathcal{W}_{\vec{a},\vec{b}}(p)$. So take $(A, B) \in \mathcal{W}_{\vec{a},\vec{b}}(p)$.

Instead of using elementary unipotent transformations to make the remaining nondiagonal matrix entries zero, we use these transformations to reduce these matrix entries modulo $p^{a_1}, \dots, p^{a_n}, p^{b_1}, \dots, p^{b_n}$. This establishes that each orbit for the action of $G_N(\mathbb{Z}_p)$ on $\mathcal{W}_{\vec{a},\vec{b}}(p)$ meets $\mathcal{F}_{\vec{a},\vec{b}}(p)$ at least once.

On the other hand, suppose we have $(A, B), (A', B') \in \mathcal{F}_{\vec{a},\vec{b}}(p)$ and $g \in G_N(\mathbb{Z}_p)$ such that $(A, B) = g \cdot (A', B')$. Write $g = g_1 g_2$, where $g_i \in H_i(\mathbb{Z}_p)$ for each $i \in \{1, 2\}$, and factor g_2 as $g_2 = g_2' g_2''$, where g_2' is a diagonal matrix with diagonal entries $(u, 1, \dots, 1, u^{-1})$ for some $u \in \mathbb{Z}_p^\times$, and where $g_2'' \in (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$. Since $g_1^{-1} \cdot (A, B)$ and (A', B') both lie in $\mathcal{W}_{\vec{a},\vec{b}}(p)$, we have by (2) along the invariance of Q under the action of $\mathrm{SL}_n \times \mathrm{SL}_{n+1}$ that

$$Q(g_1^{-1} \cdot (A, B)) = Q(g_2'' \cdot (A', B')).$$

But $g_1^{-1} \cdot (A, B) = g_2' \cdot (g_2'' \cdot (A', B'))$, so

$$u \cdot Q(g_2'' \cdot (A', B')) = Q(g_2' \cdot (g_2'' \cdot (A', B')) = Q(g_2'' \cdot (A', B')),$$

from which it follows that $u = 1$ and $g_2 = g_2'' \in (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$. Then, since the projections of $g_1^{-1} \cdot (A, B)$ and (A', B') onto $W_N^{\mathrm{top},0}(\mathbb{Z}_p)$ belong to the fundamental domain (5), it follows that $g_2 = \mathrm{id}$.

Next, denote the entries of g_1 by $(g_1)_{ij}$. The condition $A = g_1 \cdot A'$ implies that

$$A_{(n+1)(n+2)} \equiv A'_{(n+1)(n+2)} \pmod{p^{a_n}},$$

and then the condition $A_{(n+1)(n+2)}, A'_{(n+1)(n+2)} \in \{0, \dots, p^{a_n} - 1\}$ forces

$$A_{(n+1)(n+2)} = A'_{(n+1)(n+2)},$$

and hence that $(g_1)_{(n+1)n} = 0$. As $(g_1)_{(n+1)n} = 0$, the condition $A = g_1 \cdot A'$ implies that

$$A_{(n+1)(n+3)} \equiv A'_{(n+1)(n+3)} \pmod{p^{a_{n-1}}},$$

so the condition $A_{(n+1)(n+3)}, A'_{(n+1)(n+3)} \in \{0, \dots, p^{a_{n-1}} - 1\}$ forces

$$A_{(n+1)(n+3)} = A'_{(n+1)(n+3)},$$

and hence that $(g_1)_{(n+1)(n-1)} = 0$.

Continuing in this manner according to the sequence of matrix entries in (10) (and using the condition $B = g_1 \cdot B'$ when appropriate), we deduce that $g_1 = \mathrm{id}$, and hence that $(A, B) = (A', B')$. ∎

We now cover each of the sets $\mathcal{F}_{\vec{a},\vec{b}}(p)$ with a finite disjoint union of images of sections of the map inv. Fix $\vec{a}, \vec{b} \in \mathbb{N}^n$. Fix the matrix entries

$$A_{ij} = p^{a_i} \quad \text{for } (i, j) \text{ with } (i, j) = N + 1,$$
$$B_{ij} = p^{b_i} \quad \text{for } (i, j) \text{ with } i + j = N,$$

just as in (11). Further fix matrix entries

$$\begin{aligned} A_{ij} &\in \{0, \ldots, p^{a_{N+1-j}} - 1\} && \text{for each } (i,j) \text{ with } i + j > N + 1 \text{ and } i < j, \\ B_{ij} &\in \{0, \ldots, p^{b_i} - 1\} && \text{for each } (i,j) \text{ with } i + j > N \text{ and } i \le n, \text{ and} \\ B_{ij} &\in \{0, \ldots, p^{b_{N-i}} - 1\} && \text{for each } (i,j) \text{ with } i + j > N \text{ and } n < i < j, \end{aligned}$$

just as in (12). Call the data of these chosen matrix entries (A°, B°); then we may regard (A°, B°) as a function on $\mathbb{Z}_p^{N+1}$ which takes a tuple

$$t = (A_{(n+1)(n+1)}, \ldots, A_{NN}, B_{(n+1)(n+1)}, \ldots, B_{NN}) \in \mathbb{Z}_p^{N+1}$$

and produces the pair of matrices (A, B) with the previously fixed off-diagonal matrix entries, and with diagonal entries given by the components of t.

We may now speak of the quantity $\mathrm{inv}(A^\circ, B^\circ)$, which is a binary form whose coefficients may be thought of as an affine linear transformation of the $N + 1$ indeterminates

$$A_{(n+1)(n+1)},\ \ldots,\ A_{NN},\ B_{(n+1)(n+1)},\ \ldots,\ B_{NN}.$$

Write the coefficients of the indeterminates in an $(N+1)\times(N+1)$ matrix $M(A^\circ, B^\circ)$ as follows: the ith row corresponds to the coefficient of $x^{N-i+1}y^{i-1}$ in $\mathrm{inv}(A^\circ, B^\circ)$, and the columns correspond to the coefficients of

$$A_{(n+1)(n+1)},\ B_{(n+1)(n+1)},\ A_{(n+2)(n+2)},\ B_{(n+2)(n+2)},\ \ldots,\ A_{NN},\ B_{NN},$$

in that order. Then one verifies by inspection that $M(A^\circ, B^\circ)$ is lower-triangular, and the diagonal entries are monomials in the matrix entries A_{ij} with $i + j = N + 1$ and $(i,j) \neq (n+1, n+1)$, along with the matrix entries B_{ij} with $i + j = N$ (note that these are precisely the matrix entries dividing the Q-invariant, and that none of them are zero). Thus, $M(A^\circ, B^\circ)$ is invertible over $\mathbb{Q}_p$, and there exists a column vector $C(A^\circ, B^\circ) \in \mathbb{Z}_p^{N+1}$ such that

$$\begin{aligned} &M(A^\circ, B^\circ) \\ &\cdot \begin{bmatrix} A_{(n+1)(n+1)} & B_{(n+1)(n+1)} & A_{(n+2)(n+2)} & B_{(n+2)(n+2)} & \cdots & A_{NN} & B_{NN} \end{bmatrix}^T \\ &\quad + C(A^\circ, B^\circ) \end{aligned}$$

is the column vector whose entries are the coefficients of $\mathrm{inv}(A^\circ, B^\circ)$. Consequently, we arrive at the following result.

Lemma 2.12. *Let (A°, B°) be fixed as above. Given $f \in U_N(\mathbb{Z}_p)$, there exists a unique tuple $t \in \mathbb{Q}_p^{N+1}$ such that* $\mathrm{inv}(A^\circ, B^\circ)(t) = f$. *Moreover, for any $G_N(\mathbb{Z}_p)$-invariant subset $\mathfrak{S}_p \subset W_N^0(\mathbb{Z}_p)$ that is the preimage under reduction modulo p^j of a nonempty subset of $W_N^0(\mathbb{Z}/p^j\mathbb{Z})$ for some $j > 0$, the set $\mathfrak{U}(A^\circ, B^\circ)$ of forms*

$f \in U_N(\mathbb{Z}_p)$ such that $(A^\circ, B^\circ)(t) \in \mathcal{F}_{\vec{a},\vec{b}}(p) \cap \mathfrak{S}_p$, where $t \in \mathbb{Z}_p^{N+1}$ is the tuple corresponding to f, is the closure of a nonempty open subset. In fact, $\mathcal{U}(A^\circ, B^\circ)$ is defined by congruence conditions modulo a power of p depending only on $\vec{a}$, $\vec{b}$, n, and j.

Proposition 2.11 and Lemma 2.12 imply the following result, which plays a crucial role in the proof of Theorem 1.5 (see Section 3.1).

Proposition 2.13. *For any $\mathfrak{S}_p$ as in Lemma 2.12, the function that sends $f \in U_N(\mathbb{Z}_p)$ to the number of $G_N(\mathbb{Z}_p)$-equivalence classes of pairs in $\mathrm{inv}^{-1}(f) \cap \mathcal{W}_{\vec{a},\vec{b}}(p) \cap \mathfrak{S}_p$ is locally constant. This function is defined by congruence conditions modulo a power of p depending only on $\vec{a}$, $\vec{b}$, n, and $\mathfrak{S}_p$, and is also absolutely bounded by such a power of p.*

Proof. We first prove local constancy. By Proposition 2.11, it suffices to show that the function that sends $f \in U_N(\mathbb{Z}_p)$ to the number of pairs $(A, B) \in \mathcal{F}_{\vec{a},\vec{b}}(p) \cap \mathfrak{S}_p$ with $\mathrm{inv}(A, B) = f$ is locally constant. So take $f \in U_N(\mathbb{Z}_p)$. Among the pairs (A°, B°) constructed above, let S_f be the subset of pairs such that $f \in \mathcal{U}(A^\circ, B^\circ)$, and let $\overline{S}_f$ be the complement of S_f. Let

$$\mathcal{U}_1 = \bigcup_{(A^\circ,B^\circ)\in\overline{S}_f} \mathcal{U}(A^\circ, B^\circ) \quad \text{and} \quad \mathcal{U}_2 = \bigcap_{(A^\circ,B^\circ)\in S_f} \mathcal{U}(A^\circ, B^\circ).$$

Then for any $g \notin \mathcal{U}_1$ (resp., $g \in \mathcal{U}_2$), the number of pairs $(A, B) \in \mathcal{F}_{\vec{a},\vec{b}}(p) \cap \mathfrak{S}_p$ with $\mathrm{inv}(A, B) = g$ is at most (resp., at least) $\#S_f$. Hence, for any $g \in \mathcal{U}_2 - \mathcal{U}_1$, the number of pairs $(A, B) \in \mathcal{F}_{\vec{a},\vec{b}}(p) \cap \mathfrak{S}_p$ with $\mathrm{inv}(A, B) = g$ is equal to $\#S_f$. This establishes the desired local constancy, as each $\mathcal{U}(A^\circ, B^\circ)$ is the closure of a nonempty open subset, so $\mathcal{U}_2 - \mathcal{U}_1$ is an open neighborhood of f.

That the function is defined by congruence conditions modulo a power of p depending only on $\vec{a}$, $\vec{b}$, and n follows from the fact that this holds for each of the sets $\mathcal{U}(A^\circ, B^\circ)$, and hence also for the set $\mathcal{U}_2 - \mathcal{U}_1$. Finally, the claimed bound is an immediate corollary of Proposition 2.11 and Lemma 2.12. ∎

2.3. Proof of Theorem 1.3

We claim that the integral orbits of G_N on W_N^0 satisfy the desired local-to-global principle as long as the following four properties hold:

(1) the algebraic group G_N has class number 1 over $\mathbb{Q}$;

(2) for every $f \in U_N(\mathbb{C})$ with nonzero discriminant, the set $\mathrm{inv}^{-1}(f) \cap W_N^0(\mathbb{C})$ is nonempty and consists of a single $G_N(\mathbb{C})$-orbit;

(3) for every $f \in U_N(\mathbb{C})$ with nonzero discriminant, each element of $\mathrm{inv}^{-1}(f) \cap W_N^0(\mathbb{C})$ has trivial stabilizer in $G_N(\mathbb{C})$; and

(4) for every $f \in U_N(\mathbb{Z})$ with nonzero discriminant, the set $\mathrm{inv}^{-1}(f) \cap W_N^0(\mathbb{Z})$ is nonempty.

This claim follows from [25, Theorem 22], which is a general theorem giving criteria under which the orbits of a finite-dimensional representation of an algebraic group satisfy a local-to-global principle. Note that the first three properties above have already been verified in Propositions 2.6 and 2.9, and the fourth property follows immediately from the existence of the explicit section σ_0. This completes the proof of Theorem 1.3. ∎

For the sake of concreteness, we now give a self-contained proof of Theorem 1.3. Given a principal ideal domain R with fraction field K and an element $w \in W_N^0(R)$ having nonzero Q-invariant, write

$$G_N(K)_w := \{g \in G_N(K) : g \cdot w \in G_N(R)\}.$$

Then the set of $G_N(R)$-orbits contained in the $G_N(K)$-orbit of w is in bijection with the double coset space

$$G_N(R)\backslash G_N(K)_w / \mathrm{Stab}_{G_N(K)}(w) = G_N(R)\backslash G_N(K)_w,$$

where the last step follows from Proposition 2.9.

Now, fix $w_0 \in W_N^0(\mathbb{Z})$ with $Q(w_0) \neq 0$, and suppose for each prime p we have $w_p \in W_N^0(\mathbb{Z}_p)$ with $\mathrm{inv}(w_p) = f$. Our goal is to construct an element $w \in W_N^0(\mathbb{Z})$, unique up to the action of $G_N(\mathbb{Z})$, that is $G_N(\mathbb{Z}_p)$-equivalent to w_p for each prime p. To do this, consider the diagonal embedding $G_N(\mathbb{Q}) \hookrightarrow \prod_p G_N(\mathbb{Q}_p)$. We claim that this embedding induces a bijection

$$G_N(\mathbb{Z})\backslash G_N(\mathbb{Q})_{w_0} \to \prod_p G_N(\mathbb{Z}_p)\backslash G_N(\mathbb{Q}_p)_{w_0}. \tag{13}$$

Note that the product on the right-hand side of (13) is in fact a finite product, because if p is a prime such that $G_N(\mathbb{Z}_p)\backslash G_N(\mathbb{Q}_p)_{w_0} \neq 1$, then by Proposition 2.10, we must have $p \mid Q(w_p) \mid \mathrm{disc}(f)$. Verifying injectivity of the map in (13) is easy: if $g_1, g_2 \in G_N(\mathbb{Q})_{w_0}$ have the same image, then

$$g_1 g_2^{-1} \in G_N(\mathbb{Q}) \cap \bigcap_p G_N(\mathbb{Z}_p) = G_N(\mathbb{Z}).$$

As for surjectivity, if $(g_p)_p \in \prod_p G_N(\mathbb{Z}_p)\backslash G_N(\mathbb{Q}_p)_{w_0}$, then since G_N has class number 1 over $\mathbb{Q}$ (by Proposition 2.6), there exists $g \in G_N(\mathbb{Q})$ such that g maps to g_p under the map $G_N(\mathbb{Q}) \to G_N(\mathbb{Z}_p)\backslash G_N(\mathbb{Q}_p)$; but then

$$g \cdot w_0 \in W_N^0(\mathbb{Q}) \cap \bigcap_p W_N^0(\mathbb{Z}_p) = W_N^0(\mathbb{Z}),$$

implying that $g \in G_N(\mathbb{Q})_{w_0}$.

By Proposition 2.9, which implies that the $G_N(\mathbb{Q}_p)$-orbit of w_0 is equal to that of w_p for each prime p, we may view the tuple $(w_p)_p$ as an element of the right-hand side of (13). Then, under the bijection, the tuple $(w_p)_p$ corresponds to the $G_N(\mathbb{Z})$-orbit of the desired element $w \in W_N^0(\mathbb{Z})$, as necessary. ∎

As an immediate consequence of Theorem 1.3 along with Proposition 2.10, we have the following result concerning global integral orbits having unit Q-invariant.

Corollary 2.14. *Let $f \in U_N(\mathbb{Z})$. Then the set*

$$\{(A, B) \in \mathrm{inv}^{-1}(f) \cap W_N^0(\mathbb{Z}) : |Q(A, B)| = 1\}$$

is nonempty and consists of a single $G_N(\mathbb{Z})$-orbit.

3. Asymptotic formulas for the count of reducible orbits

In this section, we use the local-to-global principle in Theorem 1.3 to deduce Theorem 1.5, which gives an asymptotic formula for the count of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $W_N(\mathbb{Z})$ in terms of a product of local integrals. We then perform a change-of-variables argument to rewrite each of these integrals in a more convenient form, thus proving Theorem 1.6.

3.1. Proof of Theorem 1.5

Let $\mathfrak{S}$ be a big family in $W_N^0(\mathbb{Z})$. We start by proving the following asymptotic formula for the count of $G_N(\mathbb{Z})$-orbits on $\mathfrak{S}$ of bounded height.

Theorem 3.1. *The number of $G_N(\mathbb{Z})$-orbits on $\mathfrak{S}$ of height up to X is given by*

$$\mathrm{N}_N^{(r)}(X) \times \prod_p \int_{f \in U_N(\mathbb{Z}_p)} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap \mathfrak{S}_p}{G_N(\mathbb{Z}_p)}\right) df + o(X^{N+1}). \tag{14}$$

Moreover, when $N = 3$, the number of $(\mathrm{GL}_2 \times G_3)(\mathbb{Z})$-orbits on $\mathfrak{S}$ with discriminant having absolute value less than X is given by

$$\mathrm{N}_\Delta^{(r)}(X) \times \prod_p \int_{f \in U_3(\mathbb{Z}_p)} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap \mathfrak{S}_p}{G_3(\mathbb{Z}_p)}\right) df + o(X), \tag{15}$$

where $\mathrm{N}_\Delta^{(r)}(X)$ is the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of irreducible binary cubic forms in $U_3(\mathbb{Z})^{(r)}$ of discriminant up to X in absolute value.

Remark. The techniques for counting orbits developed in the works of Bhargava et al. work systematically for quite general representations of reductive groups. Theorem 3.1 constitutes a rare example of a situation in which we can determine precise asymptotics for the integral orbits of the action of a nonreductive group (namely, G_N).

Proof of Theorem 3.1. We first prove (14), and then we explain how the proof of (15) differs. The proof is analogous to that of [25, Theorem 24], but we include the details for the sake of completeness. Fix an integer $\mathfrak{b} \geq 1$, and factorize it into primes as

$$\mathfrak{b} = \prod_p p^{e_p}.$$

We start by proving an analogue of Theorem 3.1 with $\mathfrak{S}$ replaced by the subfamily

$$\mathfrak{S}(\mathfrak{b}) := \{w \in \mathfrak{S} : |Q(w)| = \mathfrak{b}\};$$

note that $\mathfrak{S}(\mathfrak{b})$ is itself a big family in $W_N^0(\mathbb{Z})$, where

$$\mathfrak{S}(\mathfrak{b})_p = \{w \in \mathfrak{S}_p : |Q(w)|_p = |\mathfrak{b}|_p\}.$$

If $\mathfrak{S}(\mathfrak{b}) = \varnothing$, then there is nothing to prove, so assume that $\mathfrak{S}(\mathfrak{b}) \neq \varnothing$. For each prime $p \mid \mathfrak{b}$, we partition $U_N(\mathbb{Z}_p)$ as

$$U_N(\mathbb{Z}_p) = \bigsqcup_{j=1}^{m_p} U_{p,j},$$

where each $U_{p,j}$ is a level set for the function that sends $f \in U_N(\mathbb{Z}_p)$ to

$$\#\big(G_N(\mathbb{Z}_p)\backslash(\mathrm{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p)\big).$$

Write "$E(m)$" to mean "a power of m that depends only on n and $\mathfrak{S}$." Then Proposition 2.13 implies that $U_N(\mathbb{Z}_p)$ can be covered by open sets, each of which is defined by congruence conditions modulo $E(p^{e_p})$, such that this orbit-counting function is constant on each open. It follows that $U_{p,j}$ is defined by congruence conditions modulo $E(p^{e_p})$. The quantity $\#(G_N(\mathbb{Z}_p)\backslash(\mathrm{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p))$ is independent of the choice of $f \in U_{p,j}$ (by the definition of a level set) and by Proposition 2.13, this quantity is $\ll E(p^{e_p})$.

Now for each prime $p \nmid \mathfrak{b}$, Proposition 2.10 tells us that

$$\#\big(G_N(\mathbb{Z}_p)\backslash(\mathrm{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p)\big) = 1$$

for each $f \in \mathrm{inv}(\mathfrak{S}(\mathfrak{b})_p)$. It then follows from Theorem 1.3 that the quantity

$$\#\left(\frac{\mathrm{inv}^{-1}(f)\cap \mathfrak{S}(\mathfrak{b})}{G_N(\mathbb{Z})}\right) = \prod_p \#\left(\frac{\mathrm{inv}^{-1}(f)\cap \mathfrak{S}(\mathfrak{b})_p}{G_N(\mathbb{Z}_p)}\right)$$
$$= \prod_{p\mid \mathfrak{b}} \#\left(\frac{\mathrm{inv}^{-1}(f)\cap \mathfrak{S}(\mathfrak{b})_p}{G_N(\mathbb{Z}_p)}\right) \tag{16}$$

is independent of the choice of $f \in \mathrm{inv}(\mathfrak{S}(\mathfrak{b})) \cap \bigcap_p U_{p,j_p}$ for each tuple $(j_p)_{p\mid\mathfrak{b}} \in \prod_{p\mid\mathfrak{b}}\{1,\dots,m_p\}$. Therefore, we have

$$\sum_{\substack{f\in U_N(\mathbb{Z})\cap\bigcap_p U_{p,j_p}\\ \mathrm{H}(f)<X}} \#\left(\frac{\mathrm{inv}^{-1}(f)\cap \mathfrak{S}(\mathfrak{b})}{G_N(\mathbb{Z})}\right) = \#\left(\frac{\mathrm{inv}^{-1}(f^*)\cap \mathfrak{S}(\mathfrak{b})}{G_N(\mathbb{Z})}\right)$$
$$\times \sum_{\substack{f\in \mathrm{inv}(\mathfrak{S}(\mathfrak{b}))\cap\bigcap_p U_{p,j_p}\\ \mathrm{H}(f)<X}} 1, \tag{17}$$

where $f^* \in \mathrm{inv}(\mathfrak{S}(\mathfrak{b})) \cap \bigcap_{p\mid\mathfrak{b}} U_{p,j_p}$ is any fixed element. Since $\mathfrak{S}$ is a big family, and since the aforementioned explicit section σ_0 has image contained in the locus of pairs (A, B) with $Q(A, B) = \pm 1$, it follows that

$$\mathrm{inv}(\mathfrak{S}(\mathfrak{b})_p) = U_N(\mathbb{Z}_p)$$

for every $p \gg 1$ that does not divide $\mathfrak{b}$. As the set $\mathrm{inv}(\mathfrak{S}(\mathfrak{b})) \cap \bigcap_p U_{p,j_p}$ is defined by congruence conditions modulo $E(\mathfrak{b})$, since $\mathrm{inv}(\mathfrak{S}(\mathfrak{b})_p) \cap U_{p,j_p}$ is defined by congruence conditions modulo $E(p^{e_p})$ for each p, we obtain the following asymptotic:

$$\sum_{\substack{f\in \mathrm{inv}(\mathfrak{S}(\mathfrak{b}))\cap\bigcap_p U_{p,j_p}\\ \mathrm{H}(f)<X}} 1 = \mathrm{N}_N^{(r)}(X) \times \prod_{p\mid\mathfrak{b}} \int_{f\in \mathrm{inv}(\mathfrak{S}(\mathfrak{b})_p)\cap U_{p,j_p}} df$$
$$\times \prod_{p\nmid\mathfrak{b}} \int_{f\in \mathrm{inv}(\mathfrak{S}(\mathfrak{b})_p)} df + O\big(E(\mathfrak{b})X^{N+1-\delta}\big) \tag{18}$$

for some sufficiently small $\delta > 0$. Substituting the asymptotic (18) into the right-hand side of (17), applying (16) to the resulting expression, and summing that over tuples $(j_p)_{p\mid\mathfrak{b}} \in \prod_{p\mid\mathfrak{b}}\{1,\dots,m_p\}$ gives the following:

$$\sum_{\substack{f\in U_N(\mathbb{Z})\\ \mathrm{H}(f)<X}} \#\left(\frac{\mathrm{inv}^{-1}(f)\cap \mathfrak{S}(\mathfrak{b})}{G_N(\mathbb{Z})}\right) = \mathrm{N}_N^{(r)}(X)$$
$$\times \prod_p \int_{f\in U_N(\mathbb{Z}_p)} \#\left(\frac{\mathrm{inv}^{-1}(f)\cap \mathfrak{S}(\mathfrak{b})_p}{G_N(\mathbb{Z}_p)}\right) df + O\big(E(\mathfrak{b})X^{N+1-\delta}\big). \tag{19}$$

Next, we prove that the theorem holds with "=" replaced by "≥." For any real number $M > 1$, let $\mathfrak{S}[M] := \{w \in \mathfrak{S} : |Q(w)| < M\}$. Summing (19) over $\mathfrak{b} < M$ gives

$$\sum_{\substack{f \in U_N(\mathbb{Z}) \\ \mathrm{H}(f)<X}} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap \mathfrak{S}[M]}{G(\mathbb{Z})}\right) = \mathrm{N}_N^{(r)}(X)$$
$$\times \sum_{\mathfrak{b}<M} \prod_p \int_{f \in U_N(\mathbb{Z}_p)} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p}{G(\mathbb{Z}_p)}\right) df + O\big(E(M)X^{N+1-\delta}\big). \quad (20)$$

Dividing through by $\mathrm{N}_N^{(r)}(X)$, letting $X \to \infty$, and replacing $\mathfrak{S}$ with $\mathfrak{S}[M]$, it follows from (20) that

$$\liminf_{X\to\infty} \frac{\sum_{\substack{f \in U_N(\mathbb{Z}) \\ \mathrm{H}(f)<X}} \#\left(\frac{\mathrm{inv}^{-1}(f)\cap\mathfrak{S}}{G_N(\mathbb{Z})}\right)}{\mathrm{N}_N^{(r)}(X)} \geq \sum_{\mathfrak{b}<M} \prod_p \int_{f \in U_N(\mathbb{Z}_p)} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p}{G_N(\mathbb{Z}_p)}\right) df. \quad (21)$$

Now, letting $M \to \infty$ on the right-hand side of (21) and factoring the sum into an Euler product, we obtain the following:

$$\begin{aligned}
&\sum_{\mathfrak{b}=1}^{\infty} \prod_p \int_{f \in U_N(\mathbb{Z}_p)} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap \mathfrak{S}(\mathfrak{b})_p}{G_N(\mathbb{Z}_p)}\right) df \\
&\quad = \prod_p \sum_{e=0}^{\infty} \int_{f \in U_N(\mathbb{Z}_p)} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap \mathfrak{S}(p^e)_p}{G_N(\mathbb{Z}_p)}\right) df \\
&\quad = \prod_p \int_{f \in U_N(\mathbb{Z}_p)} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap \mathfrak{S}_p}{G_N(\mathbb{Z}_p)}\right) df. \quad (22)
\end{aligned}$$

Combining (21) with (22), we find that Theorem 3.1 holds with "=" replaced by "≥."

It thus remains to prove the theorem with "=" replaced by "≤." Let $\mathfrak{S}[M]' := \mathfrak{S} \smallsetminus \mathfrak{S}[M]$. Then for each $w \in \mathfrak{S}[M]'$, we have that $|Q(w)| \geq M$. In [12], Bhargava, Shankar, and Wang determined bounds for the number of reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $W_N(\mathbb{Z})$ having large Q-invariant (for those orbits on which the notion of Q-invariant can be extended naturally). In particular, by [12, (14), (16), and Theorem 4.1] along with Proposition 3.2 (to follow), we can choose $\delta \in (0, 1)$ so that

$$\sum_{\substack{f \in U_N(\mathbb{Z}) \\ \mathrm{H}(f)<X}} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap \mathfrak{S}[M]'}{G_N(\mathbb{Z})}\right) = O_\varepsilon\big(X^{N+1+\varepsilon}/M\big) + O\big(X^{N+1-\delta}\big). \quad (23)$$

On the other hand, it follows from (20) that

$$\sum_{\substack{f \in U_N(\mathbb{Z}) \\ \mathrm{H}(f)<X}} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap \mathfrak{S}[M]}{G_N(\mathbb{Z})}\right) \leq \mathrm{N}_N^{(r)}(X)$$
$$\times \prod_p \int_{f \in U_N(\mathbb{Z}_p)} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap \mathfrak{S}_p}{G_N(\mathbb{Z}_p)}\right) df + O\big(E(M)X^{N+1-\delta}\big). \tag{24}$$

Taking M to grow as a sufficiently small power of X and combining (23) with (24) yields (14).

As for the proof of (15), the only steps that differ are the deductions of (18) and (23). For (18), one simply applies the asymptotics for counting $\mathrm{GL}_2(\mathbb{Z})$-orbits of binary cubic forms satisfying local conditions obtained by Bhargava, Shankar, and Tsimerman in [11, Theorem 26]. For (23), one simply applies the estimate proven by Bhargava in [4, Proposition 23]. ∎

To deduce Theorem 1.5 from Theorem 3.1, we require the following result relating $G_N(\mathbb{Z})$-orbits on $W_N^0(\mathbb{Z})$ with reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $W_N(\mathbb{Z})$.

Proposition 3.2. *Let $f \in U_N(\mathbb{Z})$ be irreducible. The $G_N(\mathbb{Z})$-orbits on $\mathrm{inv}^{-1}(f) \cap W_N^0(\mathbb{Z})$ are in bijection with the reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $\mathrm{inv}^{-1}(f) \cap W_N(\mathbb{Z})$.*

Analogously, let $\Delta \in \mathbb{Z} \smallsetminus \{0\}$. The $(\mathrm{GL}_2 \times G_3)(\mathbb{Z})$-orbits on $\mathrm{disc}^{-1}(\Delta) \cap W_3^0(\mathbb{Z})$ are in bijection with the reducible $(\mathrm{GL}_2 \times \mathrm{SL}_3)(\mathbb{Z})$-orbits on $\mathrm{disc}^{-1}(\Delta) \cap W_3(\mathbb{Z})$.

Proof. We first claim that if we have $(A_1, B_1), (A_2, B_2) \in \mathrm{inv}^{-1}(f) \cap W_N^0(\mathbb{Z})$ and $g_1 \in \mathrm{SL}_N(\mathbb{Z})$ such that

$$g_1 \cdot (A_1, B_1) = (A_2, B_2),$$

then $g_1 \in G_N(\mathbb{Z})$. Indeed, by Proposition 2.9, there exists $g_2 \in G_N(\mathbb{Q})$ such that

$$g_2 \cdot (A_1, B_1) = (A_2, B_2),$$

so $g_1^{-1} g_2 \in \mathrm{SL}_N(\mathbb{Q})$ stabilizes (A_1, B_1). But by [29, Proposition 14], the stabilizer in $\mathrm{SL}_N(\mathbb{Z})$ of any element of $\mathrm{inv}^{-1}(f)$ is trivial, so

$$g_1 = g_2 \in \mathrm{SL}_N(\mathbb{Z}) \cap G_N(\mathbb{Q}) = G_N(\mathbb{Z}),$$

as claimed.

It follows from the above claim that there are at least as many reducible $\mathrm{SL}_N(\mathbb{Z})$-orbits on $\mathrm{inv}^{-1}(f) \cap W_N(\mathbb{Z})$ as there are $G_N(\mathbb{Z})$-orbits $\mathrm{inv}^{-1}(f) \cap W_N^0(\mathbb{Z})$. It therefore suffices to show that every reducible $\mathrm{SL}_N(\mathbb{Z})$-orbit on $W_N(\mathbb{Z})$ meets the linear subspace $W_N^0(\mathbb{Z})$, but this was proven in [12, §3.4, bottom of p. 12]. The proof of the analogous claim about $(\mathrm{GL}_2 \times G_3)(\mathbb{Z})$-orbits on $\mathrm{disc}^{-1}(\Delta) \cap W_3^0(\mathbb{Z})$ is essentially identical, with [29, Proposition 14] replaced by [4, §2.1, p. 1039]. ∎

Theorem 1.5 now follows from Theorem 3.1 and Proposition 3.2 by taking $\mathfrak{S} = S \cap W_N^0(\mathbb{Z})$, where S is a big family in $W_N(\mathbb{Z})$.

3.2. Change-of-variables formulas, and proof of Theorem 1.6

The purpose of this section is to deduce Theorem 1.6 from Theorem 1.5. The objective is, for each prime p, to reexpress the integral over $U_N(\mathbb{Z}_p)$ that occurs in the asymptotic given by Theorem 1.5 in terms of an integral over $W_N^0(\mathbb{Z}_p)$. To do this, we first write the integral over $U_N(\mathbb{Z}_p)$ as an integral over $G_N(\mathbb{Z}_p) \times U_N(\mathbb{Z}_p)$; we then perform a change-of-variables to relate the natural measure on $G_N \times U_N$ with the natural measure on W_N^0 (note that $\dim G_N \times U_N = \dim G_N + \dim U_N = \dim W_N^0$).

We also prove a second change-of-variables formula relating the natural measure on W_N^{top} with the natural measure on $(\mathrm{SL}_n \times \mathrm{SL}_{n+1}) \times \mathbb{A}^1$, where $\mathbb{A}^1$ parametrizes the Q-invariant (note that $\dim((\mathrm{SL}_n \times \mathrm{SL}_{n+1}) \times \mathbb{A}^1) = \dim \mathrm{SL}_n + \dim \mathrm{SL}_{n+1} + \dim \mathbb{A}^1 = \dim W_N^{\text{top}}$). This second change-of-variables plays a crucial role in the proof of Theorem 1.7 (see Section 4.1, to follow).

3.2.1. Explicit choices of volume forms. We start by making explicit choices of volume forms on U_N, W_N^0, and G_N. Take df, dw, dh_1, and dh_2 to be generators of the $\mathbb{Z}$-modules of right-invariant volume forms on U_N, W_N^0, H_1, and H_2, respectively, all defined over $\mathbb{Z}$. On G_N we take the measure $dg = dh_1 dh_2$ (recall that G_N is the Frobenius product of H_1 and H_2 by Lemma 2.7).

We now give an explicit formula for dg on an open subscheme of G_N. For a square matrix M, we denote the minor obtained by deleting the first row and column by $M_{(1,1)}$; if M is 1-dimensional, then we set $M_{(1,1)} := 1$. Let G_N° be the open subscheme of G_N whose R-points are given by matrices

$$g = \left[\begin{array}{c|c} g' & 0 \\ \hline g''' & g'' \end{array}\right] \in G_N(R)$$

such that $g'_{(1,1)} \in R^\times$ for any $\mathbb{Z}$-algebra R. Then we may realize G_N° as an open subscheme of the affine space

$$\mathcal{M} := \operatorname{Spec} \mathbb{Z}\big[\{M_{ij} : 1 \le i, j \le n, \text{ where } (i,j) \ne (1,1) \text{ and } j \le n \text{ if } i \le n\}\big]$$

via the map that sends a matrix $g \in G_N(R)$ to its list of matrix entries g_{ij}, excluding the entries g_{ij} for any (i,j) such that $i \le n$ and $j \ge n+1$ or $(i,j) = (1,1)$.

Let $\prod dM_{ij}$ be the Haar measure on $\mathcal{M}$, normalized so that $\mathcal{M}(\mathbb{Z})$ has covolume 1 in $\mathcal{M}(\mathbb{R})$. We denote by $\prod dg_{ij}$ the restriction of this measure to G_N° via the embedding $G_N^\circ \subset \mathcal{M}$ defined above, and by abuse of notation, we also denote by dg the restriction to G_N° of the volume form on G_N. Then a calculation shows that the

measure

$$\left(g'_{(1,1)}\right)^{-1}(\det g'')^{n-1} \times \prod dg_{ij}$$

is invariant under the right-action of G_N, and so on G_N°, we have

$$dg = \left(g'_{(1,1)}\right)^{-1}(\det g'')^{n-1} \times \prod dg_{ij},$$

up to sign. As for the left-action of G_N, if we take

$$h = \left[\begin{array}{c|c} h' & 0 \\ \hline h''' & h'' \end{array}\right] \in G_N(R), \tag{25}$$

then one readily verifies that

$$d(hg) = \rho(h)dg, \quad \text{where } \rho(h) := |\det h''|^N. \tag{26}$$

Note that the formula (26) holds on all of G_N, not just on the open subscheme G_N°.

We finish by making explicit choices of the volume forms on $\mathbb{A}^1$ and $\mathrm{SL}_n \times \mathrm{SL}_{n+1}$. Take dq to be any volume form on $\mathbb{A}^1$ defined over $\mathbb{Z}$, and take dh to be any volume form on $\mathrm{SL}_n \times \mathrm{SL}_{n+1}$ defined over $\mathbb{Z}$. The forms dq and dh are necessarily left- and right-invariant.

3.2.2. Stating the change-of-variables formulas. We are now in position to state our change-of-variables formula relating the measure dw on W_N^0 with the measure $dg\,df$ on $G_N \times U_N$.

Proposition 3.3. *Let $R = \mathbb{R}$ or $\mathbb{Z}_p$ for a prime p. Let $\phi: W_N^0(R) \to \mathbb{R}$ be an integrable function. Then there exists a nonzero rational number $\mathcal{J} \in \mathbb{Q}^\times$, possibly depending on N, such that*

$$\frac{1}{|\mathcal{J}|}\int_{w \in W_N^0(R)} \phi(w)|Q(w)|\,dw = \int_{\substack{f \in U_N(R) \\ \Delta(f)\neq 0}} \sum_{[w] \in \frac{\mathrm{inv}^{-1}(f)\cap W_N^0(R)}{G_N(R)}} \int_{g \in G_N(R)} \phi(g \cdot w)\,dg\,df,$$

where $|-|$ denotes the usual absolute value on R.

Proof. We follow the general strategy used in the proof of [25, Proposition 14]. Take $R = \mathbb{R}$, and let $\mathcal{U} \subset U_N(\mathbb{R})$ be an open set and let $\sigma: \mathcal{U} \to W_N^0(\mathbb{R})$ be a continuous section of inv (note that such a section exists, namely the aforementioned explicit section σ_0). We first claim that for some $\mathcal{J} \in \mathbb{Q}^\times$, we have

$$\int_{w \in G_N(\mathbb{R})\cdot\sigma(\mathcal{U})} \phi(w)|Q(w)|\,dw = |\mathcal{J}| \int_{f \in \mathcal{U}} \int_{g \in G_N(\mathbb{R})} \phi(g \cdot \sigma(f))\,dg\,df. \tag{27}$$

By the Stone–Weierstrass theorem, it suffices to treat the case where σ is piecewise analytic. In that case, we have

$$\int_{w \in G_N(\mathbb{R}) \cdot \sigma(\mathcal{U})} \phi(w) |Q(w)|\, dw = \int_{f \in \mathcal{U}} \int_{g \in G_N(\mathbb{R})} |\mathcal{J}(g, f)| \phi(g \cdot \sigma(f))\, dg\, df,$$

where $\mathcal{J}_\sigma(g, f)$ is the determinant of the Jacobian matrix coming from the change-of-variables taking the measure $Q(w)\, dw$ on W_N^0 to the product measure $dg\, df$ on $G_N \times U_N$.

We now show that $\mathcal{J}_\sigma(g, f)$ is independent of g. Take $h \in G_N(\mathbb{R})$, and consider the transformation on $W_N^0(\mathbb{R})$ that sends $w \mapsto h \cdot w$. Then there exists a function $\chi_Q \colon G_N(\mathbb{R}) \to \mathbb{R}_{>0}$ such that

$$Q(h \cdot w) d(h \cdot w) = \chi_Q(h) Q(w)\, dw;$$

indeed, one checks that if h is expressed as in (25), we have

$$Q(h \cdot w) = |\det h''|^{-1} Q(w) \quad \text{and} \quad d(h \cdot w) = |\det h''|^{N+1} \cdot dw,$$

so $\chi_Q(h) = |\det h''|^N$. On the other hand, the transformation $w \mapsto h \cdot w$ acts on $G_N(\mathbb{R}) \times \mathcal{U}$ by sending $(g, f) \mapsto (hg, f)$. Letting $\rho \colon G_N(\mathbb{R}) \to \mathbb{R}_{>0}$ be as in (26), we have that

$$\mathcal{J}_\sigma(hg, f) d(hg)\, df = \rho(h) \mathcal{J}_\sigma(hg, f)\, dg\, df.$$

But we also have that

$$\begin{aligned} \mathcal{J}_\sigma(hg, f) d(hg)\, df &= Q(h \cdot w)\, d(h \cdot w) \\ &= \chi_Q(h) Q(w)\, dw = \chi_Q(h) \mathcal{J}_\sigma(g, f)\, dg\, df. \end{aligned}$$

Upon comparing the above two displayed equations, and using the fact that

$$\rho(h) = |\det h''|^N = \chi_Q(h),$$

we deduce that the function $\mathcal{J}_\sigma(g, f)$ is independent of g.

That $\mathcal{J}_\sigma(g, f)$ is independent of σ follows from an argument identical to Step 2 in the proof of [10, Proposition 3.10] (this step requires that the measure dg be right-invariant). Thus, we can take σ to be the polynomial section σ_0. With this choice of section, that $\mathcal{J}_{\sigma_0}(g, f)$ is independent of f and equal to a nonzero rational constant follows from an argument identical to Steps 3 and 4 in the proof of [10, Proposition 3.10].

We have thus proven (27). Proposition 3.3 – including the case where $R = \mathbb{Z}_p$ for a prime p – now follows from (27) and the principle of permanence of identities, just as [10, Proposition 3.7] is deduced from [10, Proposition 3.10]. ∎

We shall also require the following change-of-variables formula relating the push-forward of the measure dw from W_N^0 to W_N^{top} with the product of the Haar measure on $\mathrm{SL}_n \times \mathrm{SL}_{n+1}$ and the measure dq on $\mathbb{A}^1$. The proof is analogous to that of Proposition 3.3, so we omit it.

Proposition 3.4. *Let p be prime. Let $\phi\colon W_N^{\mathrm{top}}(\mathbb{Z}_p) \to \mathbb{R}$ be an integrable function, and extend ϕ to a function on W_N^0 by precomposing with the natural projection map $W_N^0 \to W_N^{\mathrm{top}}$. Then there exists a nonzero rational number $\mathcal{J}' \in \mathbb{Q}^\times$, possibly depending on N, such that*

$$\int_{w \in W_N^0(\mathbb{Z}_p)} \frac{\phi(w)}{|Q(w)|}\, dw = |\mathcal{J}'|_p \times \int_{q \in \mathbb{Z}_p \smallsetminus \{0\}} \sum_{[w] \in \frac{Q^{-1}(q) \cap W_N^{\mathrm{top}}(\mathbb{Z}_p)}{(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)}} \int_{h \in (\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)} \phi(h \cdot w)\, dh\, dq.$$

We now compute the constants $|\mathcal{J}|$ and $|\mathcal{J}'|$ and show, in particular, that they do not actually depend on N.

Lemma 3.5. *We have that $|\mathcal{J}| = |\mathcal{J}'| = 1$.*

Proof. We first prove that $|\mathcal{J}/\mathcal{J}'| = 1$. By Corollary 2.14, there is exactly one $G_N(\mathbb{Z})$-orbit on $W_N^0(\mathbb{Z})$ with unit Q-invariant lying above a binary form $f \in U_N(\mathbb{Z})$. In particular, the average number of $G_N(\mathbb{Z})$-orbits on $W_N^0(\mathbb{Z})$ with unit Q-invariant is equal to 1. On the other hand, combining Theorem 3.1 with Propositions 3.3 and 3.4 and Lemma 3.6 and using the formula (33), we find that the average number of $G_N(\mathbb{Z})$-orbits on $W_N^0(\mathbb{Z})$ with unit Q-invariant is equal to

$$|\mathcal{J}| \times \prod_p \frac{1}{\mathrm{Vol}(G_N(\mathbb{Z}_p))} \int_{w \in \mathcal{L}_{\vec{0},\vec{0}}(p)} dw = \left|\frac{\mathcal{J}}{\mathcal{J}'}\right|.$$

Next, to compute $|\mathcal{J}'|$, it suffices to compute $|\mathcal{J}'|_p$ for each p, because $\mathcal{J}' \in \mathbb{Q}^\times$. To do this, we construct convenient sets in $W_N^{\mathrm{top}}(\mathbb{Z}_p)$ and compute their volumes in two different ways: first, using Proposition 3.4, and second, by means of a point count over $\mathbb{F}_p$. Equating the results of the two volume computations yields then the value of $|\mathcal{J}'|_p$.

To this end, fix $\overline{q} \in \mathbb{F}_p^\times$, and let $\phi_p\colon W_N^{\mathrm{top}}(\mathbb{Z}_p) \to \mathbb{R}$ be the indicator function of the set

$$\Sigma := \big\{(A, B) \in W_N^{\mathrm{top}}(\mathbb{Z}_p) : Q(A, B) \equiv \overline{q} \pmod p\big\}.$$

By Propositions 2.1 and 2.4, the group $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)$ acts simply transitively on the set of elements in Σ having any fixed Q-invariant. Hence, from Proposition 3.4,

we obtain

$$\begin{aligned}\mathrm{Vol}(\Sigma) &= |\mathcal{J}'|_p \times \mathrm{Vol}\big((\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)\big) \int_{\substack{q \in \mathbb{Z}_p \\ q \equiv \overline{q} \pmod p}} dq \\ &= |\mathcal{J}'|_p \times \mathrm{Vol}\big((\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)\big) \times p^{-1}. \end{aligned} \tag{28}$$

On the other hand, Proposition 2.1 implies that the group $(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{F}_p)$ acts simply transitively on the mod-p reduction $\overline{\Sigma}$ of Σ. Thus, we have

$$\#\overline{\Sigma} = \#(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{F}_p). \tag{29}$$

Since

$$\begin{aligned}\mathrm{Vol}(\Sigma) &= p^{-\dim W_N^{\mathrm{top}}} \times \#\overline{\Sigma}, \\ \mathrm{Vol}\big((\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)\big) &= p^{-\dim(\mathrm{SL}_n \times \mathrm{SL}_{n+1})} \times \#(\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{F}_p),\end{aligned}$$

and

$$1 + \dim \mathrm{SL}_n \times \mathrm{SL}_{n+1} = \dim W_N^{\mathrm{top}},$$

it follows from (28) and (29) that $|\mathcal{J}'|_p = 1$ for all p. ∎

We now turn our attention to the proof of Theorem 1.6. For this, let S be a big family in $W_N(\mathbb{Z})$. An application of Proposition 3.3 with $R = \mathbb{Z}_p$ and with ϕ equal to the indicator function of $S_p \cap W_N^0(\mathbb{Z}_p)$, along with Lemma 3.5, yields that

$$\begin{aligned}&\int_{f \in U_N(\mathbb{Z}_p)} \#\left(\frac{\mathrm{inv}^{-1}(f) \cap S_p \cap W_N^0(\mathbb{Z}_p)}{G_N(\mathbb{Z}_p)}\right) df \\ &\quad = \frac{1}{\mathrm{Vol}(G_N(\mathbb{Z}_p))} \int_{w \in S_p \cap W_N^0(\mathbb{Z}_p)} |Q(w)|_p \, dw. \end{aligned} \tag{30}$$

In the next lemma, we determine $\mathrm{Vol}(G_N(\mathbb{Z}_p))$.

Lemma 3.6. *We have that*

$$\mathrm{Vol}\big(G_N(\mathbb{Z}_p)\big) = \xi_{p,n}^{-1} = (1 - p^{-1})(1 - p^{-n-1}) \times \prod_{i=2}^{n} (1 - p^{-i})^2,$$

and also that

$$\mathrm{Vol}\big((\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p)\big) = (1 - p^{-n-1}) \times \prod_{i=2}^{n} (1 - p^{-i})^2.$$

Proof. We prove only the claimed formula for $\mathrm{Vol}(G_N(\mathbb{Z}_p))$, as the other formula can be proven similarly. Since G_N is smooth over $\mathbb{Z}$, we have that

$$\mathrm{Vol}\big(G_N(\mathbb{Z}_p)\big) = \#G_N(\mathbb{F}_p)/p^{\dim G_N}.$$

It is easy to see that $\dim G_N = 3n^2 + 3n$, and by Lemma 2.7, we have that

$$\begin{aligned}\#G_N(\mathbb{F}_p) &= \#H_1(\mathbb{F}_p) \times \#H_2(\mathbb{F}_p)\\ &= \#\mathbb{A}^{n^2+n}(\mathbb{F}_p) \times \big(\#\,\mathrm{SL}_n(\mathbb{F}_p) \times \#\,\mathrm{GL}_{n+1}(\mathbb{F}_p)\big)\\ &= p^{n^2+n} \times (p-1)^{-1} \times \prod_{i=0}^{n-1}(p^n - p^i) \times \prod_{i=0}^{n}(p^{n+1} - p^i).\end{aligned}$$

∎

Finally, substituting the formula for $\mathrm{Vol}(G_N(\mathbb{Z}_p))$ given by Lemma 3.6 into (30) and combining the result with Theorem 1.5 yields Theorem 1.6.

4. Evaluation of local volumes for applications

In this section, we evaluate the local integrals in Theorem 1.6 in two cases:

(1) where $S_p = W_N(\mathbb{Z}_p)$ for each prime p; and

(2) where S_p is the set of projective elements in $W_3(\mathbb{Z}_p)$ for each prime p.

As a consequence of (1), we deduce Theorem 1.7, and as a consequence of (2), we deduce Theorems 1.8.A and 1.8.B.

4.1. Proof of Theorem 1.7

To deduce Theorem 1.7 from Theorem 1.6, we must take $S = W_N(\mathbb{Z})$ and evaluate the integral over $\mathbb{Z}_p$ for each prime p. We do this as follows.

Proposition 4.1. *Fix a prime p. Then we have that*

$$\frac{1}{\mathrm{Vol}(G_N(\mathbb{Z}_p))} \int_{w \in W_N^0(\mathbb{Z}_p)} |Q(w)|_p \, dw = \prod_{i=2}^{N} \frac{1}{1-p^{-i}}.$$

Proof. Our strategy is to partition $W_N^0(\mathbb{Z}_p)$ into the union over $\vec{a}, \vec{b} \in \mathbb{N}^n$ of the preimage under projection

$$\pi\colon W_N^0(\mathbb{Z}_p) \to W_N^{\mathrm{top}}(\mathbb{Z}_p)$$

of the set $\mathcal{L}_{\vec{a},\vec{b}}(p)$ defined in Section 2.2.3. Taking ϕ to be the indicator function of $\pi^{-1}(\mathcal{L}_{\vec{a},\vec{b}}(p))$ and applying Proposition 3.4 and Lemma 3.5 yields that

$$\int_{w\in\pi^{-1}(\mathcal{L}_{\vec{a},\vec{b}}(p))} |Q(w)|_p \, dw = \frac{\mathrm{Vol}((\mathrm{SL}_n \times \mathrm{SL}_{n+1})(\mathbb{Z}_p))}{(\prod_{i=1}^n p^{(n+1-i)a_i+ib_i})^2} \times \int_{\substack{q\in\mathbb{Z}_p \\ v_p(q)=\sum_{i=1}^n (n+1-i)a_i+ib_i}} \#\left(\frac{Q^{-1}(q)\cap\mathcal{L}_{\vec{a},\vec{b}}(p)}{(\mathrm{SL}_n\times\mathrm{SL}_{n+1})(\mathbb{Z}_p)}\right) dq. \tag{31}$$

Now, let v_p denote the usual p-adic valuation. Proposition 2.4 along with the formula (4) for the Q-invariant implies that we have for all q with

$$v_p(q) = \sum_{i=1}^n (n+1-i)a_i + ib_i$$

that

$$\#\left(\frac{Q^{-1}(q)\cap\mathcal{L}_{\vec{a},\vec{b}}(p)}{(\mathrm{SL}_n\times\mathrm{SL}_{n+1})(\mathbb{Z}_p)}\right) = \prod_{i=1}^n p^{(n-i)a_i+ib_i}, \tag{32}$$

so substituting (32) along with the calculation of $\mathrm{Vol}((\mathrm{SL}_n \times \mathrm{SL}_{n+1}(\mathbb{Z}_p))$ from Lemma 3.6 into the right-hand side of (31) yields

$$\int_{w\in\pi^{-1}(\mathcal{L}_{\vec{a},\vec{b}}(p))} |Q(w)|_p \, dw = \frac{(1-p^{-1})(1-p^{-n-1})\times\prod_{i=2}^n(1-p^{-i})^2\times\prod_{i=1}^n p^{(n-i)a_i+ib_i}}{(\prod_{i=1}^n p^{(n+1-i)a_i+ib_i})^3}. \tag{33}$$

Summing (33) over all $\vec{a},\vec{b}\in\mathbb{N}^n$ and using the calculation of $\mathrm{Vol}(G_N(\mathbb{Z}_p))$ from Lemma 3.6, we have that

$$\begin{aligned}
&\frac{1}{\mathrm{Vol}(G_N(\mathbb{Z}_p))}\int_{w\in W_N^0(\mathbb{Z}_p)} |Q(w)|_p \, dw \\
&\quad= \frac{1}{\mathrm{Vol}(G_N(\mathbb{Z}_p))}\sum_{\vec{a},\vec{b}\in\mathbb{N}^n}\int_{w\in\pi^{-1}(\mathcal{L}_{\vec{a},\vec{b}}(p))} |Q(w)|_p \, dw \\
&\quad= \prod_{i=1}^n \sum_{\vec{a}\in\mathbb{N}^n} \frac{1}{p^{(2n+3-2i)a_i}} \times \sum_{\vec{b}\in\mathbb{N}^n} \frac{1}{p^{2ib_i}} \\
&\quad= \prod_{i=1}^n \frac{1}{1-p^{-(N-(2i-2))}} \times \frac{1}{1-p^{-2i}} = \prod_{i=2}^N \frac{1}{1-p^{-i}},
\end{aligned}$$

which is the desired result. ∎

Theorem 1.7 now follows by combining Proposition 4.1 with Theorem 1.6, and by evaluating the resulting Euler product.

4.2. Proofs of Theorems 1.8.A and 1.8.B

Let R be a principal ideal domain.

Definition 4.2. We say that (the $(\mathrm{GL}_2 \times \mathrm{SL}_3)(R)$-orbit of) a pair $(A, B) \in W_3(R)$ is *projective* if the following property is satisfied. Write

$$\mathrm{inv}(A, B) = \sum_{i=0}^{3} f_i x^{3-i} y^i,$$

and for each $k \in \{0, 1, 2\}$, let $C^{(k)}$ be the 3×3 matrix over R defined as follows:

$$C^{(0)} = BA^*B, \quad C^{(1)} = B, \quad C^{(2)} = A,$$

where A^* denotes the adjugate matrix of A. Let $M \in \mathrm{Mat}_{3\times 6}(R)$ be the matrix whose kth row consists of the entries of $C^{(k)}$ lying on or above the diagonal, written as a list in some order that is uniform over k. Then the pair (A, B) is projective if and only if the greatest common divisor of the 3×3 minors of M is equal to 1.

One can check from the above definition that

(1) projectivity is a $(\mathrm{GL}_2 \times \mathrm{SL}_3)(R)$-invariant condition;

(2) projectivity over $\mathbb{Z}$ is equivalent to projectivity over $\mathbb{Z}_p$ for every prime p;

(3) projectivity over $\mathbb{Z}_p$ is a mod-p condition (i.e., whether or not a pair (A, B) is projective is determined by the residue class of (A, B) modulo p); and

(4) any pair $(A, B) \in W_3^0(\mathbb{F}_p)$ with $Q(A, B) \neq 0$ is projective – this last claim follows from Proposition 2.9, which implies that it suffices to verify the claim for the image of the section σ_0, which is easily done. In particular, the set of projective elements of $W_3(\mathbb{Z})$ is a big family in $W_3(\mathbb{Z})$.

The motivation to introduce the notion of projectivity is the following parametrization result, which relates 2-torsion ideals of rings defined by binary cubic forms to projective reducible $\mathrm{SL}_3(\mathbb{Z})$-orbits on $W_3(\mathbb{Z})$:

Theorem 4.3. *The elements of the group $\mathcal{I}(R_f)[2]$ are in natural bijection with the projective reducible $\mathrm{SL}_3(\mathbb{Z})$-orbits of pairs $(A, B) \in W_3(\mathbb{Z})$ with*

$$-\det(xA - yB) = f(x, y).$$

Proof. Consider the set H_f of equivalence classes of pairs (I, δ), where I is a fractional ideal of R_f and $\delta \in K_f^\times$ are such that we have the containment $I^2 \subset (\delta)$ and equality of norms $\mathrm{N}(I)^2 = \mathrm{N}(\delta)$, and where two such pairs (I_1, δ_1) and (I_2, δ_2) are equivalent if there exists $\kappa \in K_f^\times$ such that

$$I_1 = \kappa I_2 \quad \text{and} \quad \delta_1 = \kappa^2 \delta_2.$$

By [30, Theorem 5.7], the set H_f is in natural bijection with the set of $\mathrm{SL}_3(\mathbb{Z})$-orbits of pairs $(A, B) \in W_3(\mathbb{Z})$ with $-\det(xA - yB) = f(x, y)$; for an explicit construction of this bijection, see [21, §2.2, p. 1007].

Now, we have an injection $\mathcal{I}(R_f)[2] \hookrightarrow H_f$, given by sending I to the equivalence class of $(I, 1)$; thus, we may regard $\mathcal{I}(R_f)[2]$ as a subset of H_f, and it suffices to determine the image of this subset under the bijection referenced above. This image was determined in [13, Lemma 16] to be the set of projective reducible $\mathrm{SL}_3(\mathbb{Z})$-orbits of pairs $(A, B) \in W_3(\mathbb{Z})$ with $-\det(xA - yB) = f(x, y)$. Note that a different but equivalent definition of projectivity is used in [13] – there, an orbit is projective if it corresponds to the equivalence class of a pair (I, δ) with I invertible. The equivalence of the two definitions can be shown using the aforementioned explicit construction of the bijection (see [21, §2.2, p. 1007]), from which it follows that I is invertible if and only if it corresponds to a pair (A, B) such that the gcd criterion in Definition 4.2 is satisfied. ∎

By Theorem 4.3, proving Theorems 1.8.A and 1.8.B amounts to determining asymptotics for the number of projective reducible $\mathrm{SL}_3(\mathbb{Z})$-orbits on $W_3(\mathbb{Z})$. An argument entirely analogous to the proof of Proposition 3.2 implies that these asymptotics are the same as the asymptotics for the number of projective $G_3(\mathbb{Z})$-orbits on $W_3^0(\mathbb{Z})$. By Theorem 3.1, Proposition 3.3, and Lemma 3.5, this amounts to evaluating a certain p-adic integral for each prime p, which we do as follows.

Proposition 4.4. *Fix a prime p. Then we have that*

$$\frac{1}{\mathrm{Vol}(G_3(\mathbb{Z}_p))} \int_{\substack{w \in W_3^0(\mathbb{Z}_p) \\ w \text{ is proj.}}} |Q(w)|_p \, dw = 1 + p^{-2}.$$

Proof. Our strategy is to slice up the set of projective elements of $W_3^0(\mathbb{Z}_p)$ into level sets for the function $w \mapsto v_p(Q(w))$, to evaluate the integral on each level set, and to sum up the results. To this end, given an integer $k \geq 1$, let

$$L_k := \{(A, B) \in W_3^0(\mathbb{Z}_p) : v_p(Q(A, B)) = k - 1\},$$

given $a, b, c, d \in \mathbb{F}_p$, let

$$S_{a,b,c,d} := \big\{(A, B) \in W_3^0(\mathbb{F}_p) : A_{12} = a,\ A_{13} = b, \\ B_{12} = c,\ B_{13} = d, \text{and } (A, B) \text{ is proj.}\big\},$$

and given $m \in \mathbb{Z}/p^k\mathbb{Z}$, denote by $\bar{m}$ the mod-p reduction of m. Then we have that

$$\int_{\substack{w \in L_k \\ w \text{ is proj.}}} |Q(w)|_p \, dw = p^{1-k} \times p^{-4k} \\ \times \sum_{\substack{M \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}/p^k\mathbb{Z}) \\ v_p(\det M) = k-1}} p^{-6} \times \#S_{\bar{M}_{11}, \bar{M}_{12}, \bar{M}_{21}, \bar{M}_{22}}. \quad (34)$$

We now determine the size of the set $S_{a,b,c,d}$ for each choice of $a, b, c, d \in \mathbb{F}_p$:

• Let $(A, B) \in W_3^0(\mathbb{F}_p)$. As mentioned above, if $Q(A, B) \neq 0$, then (A, B) is projective. Thus, if $ad - bc \neq 0$, then $\#S_{a,b,c,d} = p^6$.

• Now suppose that $Q(A, B) = 0$. A calculation reveals that if p divides all of A_{12}, A_{13}, B_{12}, and B_{13}, then (A, B) is not projective. Thus, for (A, B) to be projective, at least one of these four matrix entries must be a unit. We now fiber over these four matrix entries and determine the number of possibilities for the pair (A, B) in each fiber. Fix four elements $a, b, c, d \in \mathbb{F}_p$ with

$$ad - bc = 0 \quad \text{and} \quad \{0\} \neq \{a, b, c, d\}.$$

We claim that $\#S_{a,b,c,d}$ is independent of the choice of a, b, c, d. Indeed, if $a', b', c', d' \in \mathbb{F}_p$ with

$$a'd' - b'c' = 0 \quad \text{and} \quad \{0\} \neq \{a', b', c', d'\},$$

then there exists $\gamma \in H_2(\mathbb{F}_p)$ such that if we set $(A', B') := \gamma \cdot (A, B)$, then

$$(A'_{12}, A'_{13}, B'_{12}, B'_{13}) = (a, b, c, d).$$

Thus, γ induces a bijection between $S_{a,b,c,d}$ and $S_{a',b',c',d'}$, so it suffices to compute $\#S_{0,1,0,0}$. A calculation reveals that a pair (A, B) with

$$(A_{12}, A_{13}, B_{12}, B_{13}) = (0, 1, 0, 0)$$

is projective if and only if $B_{22}B_{33} - B_{23}^2 \neq 0$. Using this characterization, it is easy to check that $\#S_{0,1,0,0} = p^5(p - 1)$.

Substituting the formulas for $\#S_{a,b,c,d}$ obtained above into the right-hand side of (34), we find that

$$\int_{\substack{w \in L_k \\ w \text{ is proj.}}} |Q(w)|_p \, dw = p^{1-5k} \times \begin{cases} c(k) & \text{if } k = 1, \\ p^{-1}(p - 1) \times c(k) & \text{if } k \geq 2. \end{cases} \tag{35}$$

where

$$c(k) := \#\{M \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}/p^k\mathbb{Z}) : v_p(\det M) = k - 1 \text{ and } M \not\equiv 0 \pmod{p}\}.$$

Let $c'(k) := \#\{M \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}/p^k\mathbb{Z}) : v_p(\det M) = k - 1\}$. Then we have

$$c(k) = c'(k) - p^4 c'(k - 2), \tag{36}$$

where for convenience we set $c'(m) = 0$ if $m \leq 0$. The next lemma computes $c'(k)$.

Lemma 4.5. *Let $k \geq 1$ be as above. Then $c'(k) = p^{2k-1}(p^2 - 1)(p^k - 1)$.*

Proof of Lemma 4.5. For $d \in \mathbb{Z}/p^k\mathbb{Z}$, let

$$M(d) := \{M \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}/p^k\mathbb{Z}) : M_{11}M_{22} = M_{12}M_{21} = d\},$$

and let

$$N(d) := \{(a,b) \in (\mathbb{Z}/p^k\mathbb{Z})^2 : ab = d\}.$$

Then $M(d) = N(d)^2$, and so if we set $c''(k) := \#\{M \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}/p^k\mathbb{Z}) : \det M = 0\}$ of matrices over $\mathbb{Z}/p^k\mathbb{Z}$ with determinant 0, then we have

$$c''(k) = \sum_{d\in\mathbb{Z}/p^k\mathbb{Z}} M(d) = \sum_{d\in\mathbb{Z}/p^k\mathbb{Z}} N(d)^2. \tag{37}$$

Let ϕ denote Euler's totient function. First suppose $v_p(d) < k$, and fix a number $j \in \{0,\dots,v_p(d)\}$. If d factors as $d = ab$ where $v_p(a) = j$, then we have that there are $\phi(p^{k-j})$ choices for a and $\phi(p^{k-v_p(d)+j})\phi(p^{k-v_p(d)})^{-1}$ choices for b. Summing over all j, we find that

$$N(d) = \sum_{j=0}^{v_p(d)} \phi(p^{k-v_p(d)})^{-1}\phi(p^{k-j})\phi(p^{k-v_p(d)+j}) \quad \text{if } v_p(d) < k. \tag{38}$$

Now suppose $d \equiv 0 \pmod{p^k}$. Suppose d factors as $d = ab$, let $i = v_p(a)$ if $v_p(a) < k$ and $i = k$ otherwise. Then there are $\phi(p^{k-i})$ choices for a, and for each $j \in \{k-i,\dots,k\}$, there are $\phi(p^{k-j})$ choices for b. Summing over all i and j, we find that

$$N(0) = \sum_{i=0}^{k}\sum_{j=k-i}^{k} \phi(p^{k-i})\phi(p^{k-j}). \tag{39}$$

Substituting the results of (38) and (39) into (37) and evaluating the sum, we deduce that

$$c''(k) = p^{2k-1}\big(p^k(p+1)-1\big). \tag{40}$$

Finally, note that we have

$$c'(k) = p^4c''(k-1) - c''(k).$$

Substituting in the formula (40) for $c''(k)$ yields the lemma. ∎

Substituting the formula for $c'(k)$ given by Lemma 4.5 into (36) yields

$$c(k) = c'(k) - p^4c'(k-2) = \begin{cases} p(p-1)(p^2-1) & \text{if } k = 1, \\ p^{3k-3}(p^2-1)^2 & \text{if } k \geq 2. \end{cases}$$

Substituting this expression for $c(k)$ into the right-hand side of (35), summing up over all positive integers k, and dividing by the volume $\mathrm{Vol}(G_3(\mathbb{Z}_p))$ as given in Lemma 3.6 yields the proposition. ∎

Acknowledgments. It is a pleasure to thank Manjul Bhargava, Andrew Granville, Arul Shankar, Artane Siad, Ila Varma, and Melanie Matchett Wood for several helpful discussions. We are also grateful to the anonymous referee for numerous insightful comments and corrections.

Funding. This material is based in part upon work supported by the National Science Foundation, under the Graduate Research Fellowship as well as Award No. 2202839.

References

[1] M. Bhargava, *Higher composition laws*. PhD thesis, Princeton University, 2001

[2] M. Bhargava, Higher composition laws. II. On cubic analogues of Gauss composition. *Ann. of Math. (2)* **159** (2004), no. 2, 865–886 Zbl 1169.11044 MR 2081442

[3] M. Bhargava, Higher composition laws. III. The parametrization of quartic rings. *Ann. of Math. (2)* **159** (2004), no. 3, 1329–1360 Zbl 1169.11045 MR 2113024

[4] M. Bhargava, The density of discriminants of quartic rings and fields. *Ann. of Math. (2)* **162** (2005), no. 2, 1031–1063 Zbl 1159.11045 MR 2183288

[5] M. Bhargava, Higher composition laws. IV. The parametrization of quintic rings. *Ann. of Math. (2)* **167** (2008), no. 1, 53–94 Zbl 1173.11058 MR 2373152

[6] M. Bhargava, The density of discriminants of quintic rings and fields. *Ann. of Math. (2)* **172** (2010), no. 3, 1559–1591 Zbl 1220.11139 MR 2745272

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

[8] 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. *J. Amer. Math. Soc.* **30** (2017), no. 2, 451–493 Zbl 1385.11043 MR 3600041

[9] M. Bhargava, J. Hanke, and A. Shankar, The mean number of 2-torsion elements in the class groups of n-monogenized cubic fields. 2020, arXiv:2010.15744v1

[10] 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), no. 1, 191–242 Zbl 1307.11071 MR 3272925

[11] M. Bhargava, A. Shankar, and J. Tsimerman, On the Davenport–Heilbronn theorems and second order terms. *Invent. Math.* **193** (2013), no. 2, 439–499 Zbl 1294.11191 MR 3090184

[12] M. Bhargava, A. Shankar, and X. Wang, Squarefree values of polynomial discriminants I. *Invent. Math.* **228** (2022), no. 3, 1037–1073 Zbl 1492.11150 MR 4419629

[13] 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), no. 10, 1911–1933 Zbl 1335.11093 MR 3369305

[14] M. Bhargava and I. Varma, The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders. *Proc. Lond. Math. Soc. (3)* **112** (2016), no. 2, 235–266 Zbl 1407.11126 MR 3471250

[15] H. Cohen and H. W. Lenstra, Jr., Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, pp. 33–62, Lecture Notes in Math. 1068, Springer, Berlin, 1984 Zbl 0558.12002 MR 0756082

[16] H. Cohen and J. Martinet, Class groups of number fields: numerical heuristics. *Math. Comp.* **48** (1987), no. 177, 123–137 Zbl 0627.12006 MR 0866103

[17] H. Davenport, On the class-number of binary cubic forms. I. *J. London Math. Soc.* **26** (1951), 183–192 Zbl 0044.27002 MR 0043822

[18] H. Davenport, Corrigendum: On the class-number of binary cubic forms. I. *J. London Math. Soc.* **27** (1952), no. 4, 512 MR 1574296

[19] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420 Zbl 0212.08101 MR 0491593

[20] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*. Transl. Math. Monogr. 10, American Mathematical Society, Providence, RI, 1964 Zbl 0133.30202 MR 0160744

[21] W. Ho, A. Shankar, and I. Varma, Odd degree number fields with odd class number. *Duke Math. J.* **167** (2018), no. 5, 995–1047 Zbl 1422.11225 MR 3782066

[22] G. Malle, On the distribution of class groups of number fields. *Experiment. Math.* **19** (2010), no. 4, 465–474 Zbl 1297.11139 MR 2778658

[23] M. Sato and T. Kimura, A classification of irreducible prehomogeneous vector spaces and their relative invariants. *Nagoya Math. J.* **65** (1977), 1–155 Zbl 0321.14030 MR 0430336

[24] G. W. Schwarz, Representations of simple Lie groups with a free module of covariants. *Invent. Math.* **50** (1978/79), no. 1, 1–12 Zbl 0391.20033 MR 0516601

[25] A. Shankar, A. Siad, A. Swaminathan, and I. Varma, Geometry-of-numbers methods in the cusp. [v1] 2021, [v3] 2024, arXiv:2110.09466v3, to appear in *Algebra Number Theory*

[26] A. Siad, Monogenic fields with odd class number. Part I: Odd degree. 2020, arXiv:2011.08834v1

[27] A. Siad, Monogenic fields with odd class number. Part II: Even degree. 2020, arXiv:2011.08842v1

[28] A. A. Swaminathan, 2-Selmer groups, 2-class groups, and the arithmetic of binary forms. PhD thesis, Princeton University, 2022

[29] A. A. Swaminathan, A new parametrization for ideal classes in rings defined by binary forms, and applications. *J. Reine Angew. Math.* **798** (2023), 143–191 Zbl 1525.11133 MR 4579703

[30] M. M. Wood, Parametrization of ideal classes in rings associated to binary forms. *J. Reine Angew. Math.* **689** (2014), 169–199 Zbl 1317.11039 MR 3187931

Received 15 February 2023.

Ashvin A. Swaminathan
Department of Mathematics, Harvard University, Cambridge, MA 02138, USA;
swaminathan@math.harvard.edu