COMPOSITIO MATHEMATICA

The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields

Manjul Bhargava and Piper Harron

Compositio Math. **152** (2016), 1111–1120.

doi:10.1112/S0010437X16007260

FOUNDATION COMPOSITIO MATHEMATICA

LONDON MATHEMATICAL SOCIETY
EST. 1865

Compositio Math. 152 (2016) 1111–1120
doi:10.1112/S0010437X16007260

The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields

Manjul Bhargava and Piper Harron

Abstract

For $n = 3$, 4, and 5, we prove that, when S_n-number fields of degree n are ordered by their absolute discriminants, the lattice shapes of the rings of integers in these fields become equidistributed in the space of lattices.

1. Introduction

Let K be a number field of degree n and $\mathcal{O}_K$ its ring of integers. Then $\mathcal{O}_K$ can be embedded in $\mathbb{R}^n$ by

$$x \mapsto (\sigma_1(x), \dots, \sigma_r(x), \tau_1(x), \dots, \tau_s(x)) \in \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n, \tag{1}$$

where $\sigma_1, \dots, \sigma_r$ denote the r real embeddings and $\tau_1, \tau_1', \dots, \tau_s, \tau_s'$ the s pairs of complex embeddings of K. This endows $\mathcal{O}_K$ with a natural positive-definite quadratic form q, namely, for $x \in \mathcal{O}_K$, we define

$$q(x) := \sigma_1(x)^2 + \cdots + \sigma_r(x)^2 + 2|\tau_1(x)|^2 + \cdots + 2|\tau_s(x)|^2. \tag{2}$$

The square of the covolume of the lattice in $\mathbb{R}^n$ given by the image of $\mathcal{O}_K$ (equivalently, the determinant of the Gram matrix of the quadratic form q) is given by the absolute value $|\mathrm{Disc}(K)|$ of the discriminant of the number field K. When K is totally real, the form $q(x)$ coincides with the usual *trace form* $\mathrm{Tr}(x^2)$ on $\mathcal{O}_K$.

The *shape* of $\mathcal{O}_K$ is defined to be the $(n-1)$-ary quadratic form, up to scaling by $\mathbb{R}^\times$, obtained by restricting q to $\{x \in \mathbb{Z}+n\mathcal{O}_K : \mathrm{Tr}^K_{\mathbb{Q}}(x) = 0\}$, which is therefore well defined up to the action of $\mathbb{G}_m(\mathbb{R}) \times \mathrm{GL}_{n-1}(\mathbb{Z})$. Alternatively, the shape of $\mathcal{O}_K$ may be defined as the $(n-1)$-ary quadratic form, up to scaling by $\mathbb{R}^\times$, obtained by restricting the real quadratic form q on K (as defined by (2)) to the projection of $\mathcal{O}_K$ onto the hyperplane in K that is orthogonal to 1. (It is convention to define the shape of $\mathcal{O}_K$ in terms of the lattice orthogonal to $\mathbb{Z}$ in $\mathcal{O}_K$, because $\mathbb{Z}$ is always a subring of $\mathcal{O}_K$, while the orthogonal complement of $\mathbb{Z}$ gives the 'new' part of the lattice.) Hence, the shape of $\mathcal{O}_K$ may be viewed as an element of

$$\mathcal{S}_{n-1} := \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/\mathrm{GO}_{n-1}(\mathbb{R}),$$

which we call the *space of shapes* of lattices of rank $n-1$. There is a natural measure μ on $\mathcal{S}_{n-1}$ obtained from the Haar measure on $\mathrm{GL}_{n-1}(\mathbb{R})$ and $\mathrm{GO}_{n-1}(\mathbb{R})$, and it is a classical result of Minkowski [Min05, (85)] that $\mu(\mathcal{S}_{n-1}) < \infty$.

In [Ter97], Terr showed that when cubic fields of any given signature are ordered by absolute discriminant, then the shapes of the rings of integers in these fields become equidistributed in $\mathcal{S}_2$ with respect to μ. The purpose of this paper is to prove the analogue of this statement also for quartic and quintic number fields.

Received 6 November 2013, accepted in final form 9 December 2015, published online 15 April 2016.
2010 Mathematics Subject Classification 11R04 (primary).
Keywords: equidistribution, lattice shapes, number fields.

Theorem 1. *Let $n = 3$, 4, or 5. When isomorphism classes of S_n-number fields of degree n and any given signature are ordered by absolute discriminant, the shapes of the rings of integers in these fields become equidistributed in $\mathcal{S}_{n-1}$ with respect to μ.*

More precisely, for $n = 3$, 4, or 5, let $N_n^{(i)}(X)$ denote the number of isomorphism classes of n-ic fields having i pairs of complex embeddings, associated Galois group S_n, and absolute discriminant less than X. Also, for a measurable subset $W \subseteq \mathcal{S}_{n-1}$ whose boundary has measure 0, let $N_n^{(i)}(X, W)$ denote the number of isomorphism classes of n-ic fields having i pairs of complex embeddings, associated Galois group S_n, absolute discriminant less than X, and ring of integers with shape in W. Then we prove that

$$\lim_{X\to\infty} \frac{N_n^{(i)}(X, W)}{N_n^{(i)}(X)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}. \tag{3}$$

The condition that the associated Galois group be S_n may be dropped in Theorem 1 in the cases $n = 3$ and $n = 5$, since 100% of all cubic fields (respectively quintic fields), when ordered by discriminant, have associated Galois group S_3 (respectively S_5). However, the condition is needed in the case $n = 4$, as the Galois group S_4 does *not* occur with density 1 among all quartic fields when ordered by discriminant. Indeed, about 9.356% of all quartic fields have associated Galois group D_4 rather than S_4, and the lattice shapes of the rings of integers in D_4-quartic fields cannot be equidistributed, as is easily seen. For example, note that if K is a D_4-quartic field, then K has a nontrivial automorphism of order 2, which means that $\mathcal{O}_K$ does too, as does its underlying lattice. It is an interesting problem to determine the distribution of lattice shapes for n-ic number fields having a given nongeneric (i.e., non-S_n) associated Galois group, even heuristically. For the simple answer in the case of C_3-cubic number fields, and related results, see [BS14]. In the general case of the associated Galois group S_n, we naturally conjecture that Theorem 1 is true for all values of n.

Our proof of Theorem 1 is uniform for $n \in \{3, 4, 5\}$. It relies on the existence of parametrizations of cubic, quartic, and quintic orders by the orbits of an algebraic group on a representation as established in [DF64, Bha04, Bha08], and the corresponding counting results of [Dav51b, Dav51c, Bha05, Bha10], together with certain geometry-of-numbers and sieving arguments and volume computations. In particular, our method yields a considerably simpler proof of Terr's result (which is the case $n = 3$).

This article is organized as follows. In § 2, we describe in a uniform manner the above parametrizations of cubic, quartic, and quintic orders from [DF64, Bha04, Bha08]. In § 3, we show how certain geometry-of-numbers considerations, in conjunction with the counting results of [Dav51b, Dav51c, Bha05, Bha10], yield expressions for the number of orders of bounded discriminant having lattice shape in a given subset W of lattice shapes. The corresponding results for orders satisfying any finite set of local conditions at finitely many primes are then discussed in § 4. In § 5, this is used, via a sieve, to derive analogous expressions for the number of *maximal* orders of bounded discriminant having lattice shape in a given subset W of lattice shapes. These expressions are given in terms of volumes of certain regions in Euclidean space. The ratios of these volumes are then computed in Section 6, yielding Theorem 1.

2. Preliminaries

The key algebraic ingredient in proving Theorem 1 for cubic, quartic, and quintic fields is the parametrizations of cubic, quartic, and quintic orders in [DF64, Bha04, Bha08]. Let us fix the degree $n \in \{3, 4, 5\}$ of number fields we are considering and, for any ring T, let V_T denote:

https://doi.org/10.1112/S0010437X16007260 Published online by Cambridge University Press

(a) the space $\mathrm{Sym}^3 T^2(\otimes T)$ of binary cubic forms over T, if $n = 3$;
(b) the space $\mathrm{Sym}^2 T^3 \otimes T^2$ of pairs of ternary quadratic forms over T, if $n = 4$; and
(c) the space $T^4 \otimes \wedge^2 T^5$ of quadruples of alternating quinary 2-forms over T, if $n = 5$.

For $n = 3$, 4, or 5, we set $r = r(n) = 2$, 3, or 6, respectively. Then the group $G_T = \mathrm{GL}_{n-1}(T) \times \mathrm{GL}_{r-1}(T)$ acts naturally on V_T. The ring of polynomial invariants for the action of $G_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$ is generated by one element, called the *discriminant*, which has degree $d = 4$, 12, or 40 for $n = 3$, 4, or 5, respectively (see [SK77]). (Note that d also gives the rank of the free T-module V_T.) We say that an element of V_T is *nondegenerate* if its discriminant is nonzero.

We then have the following theorem parametrizing rings of rank n, which follows from [DF64, § 15], [Bha04, Corollary 5], and [Bha08, Corollary 3].

Theorem 2. *The nondegenerate elements of $V_{\mathbb{Z}}$ are in canonical bijection with isomorphism classes of pairs $((R, \alpha), (S, \beta))$, where R is a nondegenerate ring of rank n and S is a rank-r resolvent ring of R, and α and β are $\mathbb{Z}$-bases for $R/\mathbb{Z}$ and $S/\mathbb{Z}$, respectively. In this bijection, the discriminant of an element of $V_{\mathbb{Z}}$ is equal to the discriminant of the corresponding ring R of rank n. Moreover, under this bijection, the action of $G_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$ results in a corresponding natural action of $G_{\mathbb{Z}} = \mathrm{GL}_{n-1}(\mathbb{Z}) \times \mathrm{GL}_{r-1}(\mathbb{Z})$ on (α, β). Finally, every isomorphism class of maximal ring R of rank n arises in this bijection, and the elements of $V_{\mathbb{Z}}$ yielding R consist of exactly one $G_{\mathbb{Z}}$-orbit.*

A *ring of rank n* is any ring that is free of rank n as a $\mathbb{Z}$-module. We say that a ring of rank n is *nondegenerate* if it has nonzero discriminant. Rings of rank 2, 3, 4, 5, or 6 are called *quadratic*, *cubic*, *quartic*, *quintic*, and *sextic* rings, respectively. A *resolvent ring* of a cubic, quartic, or quintic ring is a quadratic, cubic, or sextic ring, respectively, satisfying certain conditions and whose precise definition will not be needed here (see [Bha04, Bha08] for details).

We say that an element $x \in V_{\mathbb{Z}}$ is *irreducible* if in the corresponding pair (R, S), the ring R is isomorphic to an order in an S_n-field of degree n. In the next section, we will be interested in counting irreducible elements in $V_{\mathbb{Z}}$, up to $G_{\mathbb{Z}}$-equivalence, having bounded discriminant.

We note that Theorem 2 also holds with any field K in place of $\mathbb{Z}$, with the same proofs as in [Bha04, Bha08] (see also [WY92] for earlier results of this type). We will require here the analogue of Theorem 2 over $\mathbb{R}$.

Theorem 3. *There is a canonical bijection between the nondegenerate elements of $V_{\mathbb{R}}$ and isomorphism classes of pairs $((R, \alpha), (S, \beta))$, where R is a nondegenerate ring of rank n over $\mathbb{R}$ and S is the (unique) rank-r resolvent ring of R over $\mathbb{R}$, and α and β are $\mathbb{R}$-bases for $R/\mathbb{R}$ and $S/\mathbb{R}$, respectively. Moreover, under this bijection, the action of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ results in the corresponding natural action of $G_{\mathbb{R}} = \mathrm{GL}_{n-1}(\mathbb{R}) \times \mathrm{GL}_{r-1}(\mathbb{R})$ on (α, β).*

Theorems 2 and 3 are compatible with each other under the inclusion $V_{\mathbb{Z}} \subset V_{\mathbb{R}}$: if the ring associated to $v \in V_{\mathbb{Z}}$ via Theorem 2 is R, then the ring associated to v under Theorem 3 is $R \otimes \mathbb{R}$. Explicitly, the multiplication tables of the algebras R and S with respect to the bases α and β, for a vector $v \in V$, are given by the same integer polynomial formulas in the coordinates of v in the case of either Theorem 2 or 3, namely, by [DF64, § 15 (1) and (2)] when $n = 3$, by [Bha04, (14), (21), (22), and (23)] when $n = 4$, and by [Bha08, (16), (17), (21), and (22)] when $n = 5$.

Now a nondegenerate ring R of rank n over $\mathbb{R}$ must be a product of field extensions of $\mathbb{R}$; thus, $R \cong \mathbb{R}^r \times \mathbb{C}^s$ for some r, s with $r + 2s = n$. Hence, there are two nondegenerate orbits of

$G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ when $n=3$, three such orbits of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ when $n=4$, and three such orbits of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ when $n=5$, corresponding to the rings over $\mathbb{R}$ given by

$$\mathbb{R}^3, \mathbb{R}\times\mathbb{C}; \quad \mathbb{R}^4, \mathbb{R}^2\times\mathbb{C}, \mathbb{C}^2; \quad \mathbb{R}^5, \mathbb{R}^3\times\mathbb{C}, \mathbb{R}\times\mathbb{C}^2, \tag{4}$$

respectively. An explicit computation with these eight nondegenerate orbits arising in Theorem 3, or an elementary group theory argument, then shows that the corresponding quadratic, cubic, and sextic resolvent rings of the rings in (4) are given by

$$\mathbb{R}^2, \mathbb{C}; \quad \mathbb{R}^3, \mathbb{R}\times\mathbb{C}, \mathbb{R}^3; \quad \mathbb{R}^6, \mathbb{C}^3, \mathbb{R}^2\times\mathbb{C}^2, \tag{5}$$

respectively.

Since a nondegenerate element of $v\in V_{\mathbb{R}}$ determines a nondegenerate ring $R\cong\mathbb{R}^r\times\mathbb{C}^s$ for some r,s with $r+2s=n$ (together with an $\mathbb{R}$-basis α of $R/\mathbb{R}$), we obtain a positive-definite quadratic form q_v, defined by (2), on the trace-zero $\mathbb{R}$-subspace of R; here $\sigma_1,\ldots,\sigma_r$ and τ_1, $\tau_1',\ldots,\tau_s,\tau_s'$ denote as before the ring homomorphisms from R to $\mathbb{R}$ and the complex-conjugate pairs of ring homomorphisms from R to $\mathbb{C}$, respectively. The unique lift of the basis α to a basis of the trace-zero subspace of R makes q_v an $(n-1)$-ary quadratic form. By the last sentence of Theorem 3, this map $v\mapsto q_v$ from nondegenerate elements of $V_{\mathbb{R}}$ to nondegenerate $(n-1)$-ary quadratic forms over $\mathbb{R}$ is equivariant with respect to the action of $\mathrm{GL}_{n-1}(\mathbb{R})$ (and thus also equivariant with respect to the action of the subgroup $\mathrm{GL}_{n-1}(\mathbb{Z})$).

Finally, suppose that $v\in V_{\mathbb{Z}}\subset V_{\mathbb{R}}$ corresponds via Theorem 2 to the ring of integers $\mathcal{O}_K$ of a number field K, together with a $\mathbb{Z}$-basis α of $\mathcal{O}_K/\mathbb{Z}$. Then, by the compatibility of Theorems 2 and 3, we see that the $(n-1)$-ary quadratic form q_v defined in the previous paragraph is the same (up to a factor of n) as the quadratic form on the trace-zero part of $\mathbb{Z}+n\mathcal{O}_K$ defined in the introduction (with respect to the unique lift of the basis $n\alpha$ to a basis of the trace-zero part of $\mathbb{Z}+n\mathcal{O}_K$). Therefore, if $v\in V_{\mathbb{Z}}$ corresponds via Theorem 2 to the ring of integers $\mathcal{O}_K$ in a number field K, then the quadratic form q_v, as defined above for all vectors in $V_{\mathbb{R}}$ using Theorem 3, gives the shape of $\mathcal{O}_K$.

3. Counting

For $i\in\{0,1,\ldots,\lfloor n/2\rfloor\}$, let $V_{\mathbb{R}}^{(i)}$ denote the subset of $V_{\mathbb{R}}$ such that in the corresponding pair (R,S), the ring $R\otimes\mathbb{R}$ of rank n over $\mathbb{R}$ is isomorphic to $\mathbb{R}^{n-2i}\times\mathbb{C}^i$. Then $V_{\mathbb{R}}^{(0)}, V_{\mathbb{R}}^{(1)},\ldots,V_{\mathbb{R}}^{(\lfloor n/2\rfloor)}$ are the nondegenerate orbits of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$.

The representation of $G_{\mathbb{R}}=\mathrm{GL}_{n-1}(\mathbb{R})\times\mathrm{GL}_{r-1}(\mathbb{R})$ on $V_{\mathbb{R}}$ is not faithful: indeed, the kernel is infinite. The action of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ factors through that of $G'_{\mathbb{R}}=\mathbb{G}_m(\mathbb{R})\times\mathrm{GL}^{\pm1}_{n-1}(\mathbb{R})\times\mathrm{GL}^{\pm1}_{r-1}(\mathbb{R})$ (where $\mathbb{G}_m$ acts by scalar multiplication), via

$$(g_{n-1},\ g_{r-1})\mapsto\begin{cases}(|\det g_{n-1}|^{3/(n-1)}|\det g_{r-1}|^{1/(r-1)},\ g'_{n-1},\ g'_{r-1}) & \text{if } n=3,\\ (|\det g_{n-1}|^{2/(n-1)}|\det g_{r-1}|^{1/(r-1)},\ g'_{n-1},\ g'_{r-1}) & \text{if } n=4,\\ (|\det g_{n-1}|^{1/(n-1)}|\det g_{r-1}|^{2/(r-1)},\ g'_{n-1},\ g'_{r-1}) & \text{if } n=5,\end{cases}$$

where g'_i is given by $g_i=|\det g_i|^{1/i}g'_i$; here, for a matrix group G, we use $G^{\pm1}$ to denote the subgroup of G consisting of those elements having determinant ±1. The orbits of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ are the same as the orbits of $G'_{\mathbb{R}}$ on $V_{\mathbb{R}}$, and the orbits of $G_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$ are the same as the orbits of $G'_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$, where $G'_{\mathbb{Z}}=\mathbb{G}_m(\mathbb{Z})\times\mathrm{GL}^{\pm1}_{n-1}(\mathbb{Z})\times\mathrm{GL}^{\pm1}_{r-1}(\mathbb{Z})$. Furthermore, it is easy to see that the kernel of the representation of $G'_{\mathbb{R}}$ (or $G'_{\mathbb{Z}}$) on $V_{\mathbb{R}}$ is now finite and in fact of size 4. In particular, the action of $G'_{\mathbb{R}}$ (and thus $G'_{\mathbb{Z}}$) on $V_{\mathbb{R}}$ has generically finite stabilizers. Hence, in the sequel, it will often be convenient to refer to the actions of $G'_{\mathbb{R}}$ and $G'_{\mathbb{Z}}$ on $V_{\mathbb{R}}$ rather than those of $G_{\mathbb{R}}$ and $G_{\mathbb{Z}}$, especially in situations where the finiteness of the stabilizer is important.

For $i \in \{0, 1, \ldots, \lfloor n/2 \rfloor\}$, let $v^{(i)} \in V_{\mathbb{R}}^{(i)}$ be any fixed vector whose associated shape $q(v^{(i)})$ in $\mathcal{S}_{n-1}$ is $\begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}$. To obtain such a $v^{(i)}$, choose any $w^{(i)} \in V_{\mathbb{R}}^{(i)}$; its shape is some positive-definite $(n-1)$-ary quadratic form $q(w^{(i)})$. Since $\mathrm{GL}_{n-1}(\mathbb{R})$ acts transitively on shapes in $\mathcal{S}_{n-1}$, there exists $\gamma \in \mathrm{GL}_{n-1}(\mathbb{R})$ such that $\gamma \cdot q(w^{(i)}) = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}$. Let $v^{(i)} = \gamma \cdot w^{(i)}$, where we view $\mathrm{GL}_{n-1}(\mathbb{R}) = \mathrm{GL}_{n-1}(\mathbb{R}) \times \{1\} \subset G_{\mathbb{R}}$; then $q(v^{(i)}) = q(\gamma \cdot w^{(i)}) = \gamma \cdot q(w^{(i)}) = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}$. By scaling $v^{(i)}$ by an element of $\mathbb{R}^{\times}$ if necessary, we may furthermore assume that $|\mathrm{Disc}(v^{(i)})| = 1$.

Let $4n_i$ denote the cardinality of the stabilizer in $G'_{\mathbb{R}}$ of $v^{(i)} \in V_{\mathbb{R}}^{(i)}$. Let $\mathcal{F} \subset G'_{\mathbb{R}}$ be a fundamental domain for the left action of $G'_{\mathbb{Z}}$ on $G'_{\mathbb{R}}$. (For instance, we may take $\mathcal{F}$ to lie in a standard Siegel set; see [BHC62, Bha05, Bha10] for details.) Since the kernel of the representation of either $G'_{\mathbb{R}}$ or $G'_{\mathbb{Z}}$ on $V_{\mathbb{R}}$ has size 4, we see that $\mathcal{F}v^{(i)}$, viewed as a multiset, is the union of n_i fundamental domains for the action of $G'_{\mathbb{Z}}$ on $V_{\mathbb{R}}^{(i)}$.

Let $V_{\mathbb{Z}}^{(i)} := V_{\mathbb{R}}^{(i)} \cap V_{\mathbb{Z}}$ and, for any $G_{\mathbb{Z}}$-invariant subset $S \subset V_{\mathbb{Z}}^{(i)}$, let $N(S; X)$ denote the number of $G_{\mathbb{Z}}$-orbits of irreducible elements $x \in V_{\mathbb{Z}}^{(i)}$ such that $|\mathrm{Disc}(x)| < X$. For any nice subset $W \subset \mathcal{S}_{n-1}$, let $N(S; X, W)$ denote the number of $G_{\mathbb{Z}}$-orbits of irreducible elements $x \in V_{\mathbb{Z}}$ such that $|\mathrm{Disc}(x)| < X$ and the shape $q(x)$ of x is in W.

Let $\mathcal{R}_X := \{x \in \mathcal{F}v^{(i)} : |\mathrm{Disc}(x)| < X\}$ and $\mathcal{R}_{X,W} := \{x \in \mathcal{F}v^{(i)} : |\mathrm{Disc}(x)| < X \text{ and } q(x) \in W\}$, and let $\mathrm{Vol}(\mathcal{R}_X)$ (respectively $\mathrm{Vol}(\mathcal{R}_{X,W})$) denote the Euclidean volume of $\mathcal{R}_X$ (respectively $\mathcal{R}_{X,W}$) as a multiset.

In [Dav51b, Dav51c, Bha05, Bha10], the following theorem is shown (noting the slightly different notions of irreducibility in these references that only differ on negligible sets and thus do not matter here; see [Dav51b, p. 183], [Bha05, p. 1037], and [Bha10, p. 1583]).

Theorem 4. *We have* $N(V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{n_i}\mathrm{Vol}(\mathcal{R}_X) + o(X) = \frac{1}{n_i}\mathrm{Vol}(\mathcal{R}_1) \cdot X + o(X)$.

In fact, the number of lattice points in $\mathcal{R}_X$ is $\gg \mathrm{Vol}(\mathcal{R}_X)$ as $X \to \infty$, but when only counting the *irreducible* lattice points, the number of such irreducible points is $\sim\mathrm{Vol}(\mathcal{R}_X)$ as $X \to \infty$. This is an important point and crucial to our proof of Theorem 1.

We use Theorem 4 in order to prove the following refinement.

Theorem 5. *We have* $N(V_{\mathbb{Z}}^{(i)}; X, W) = (1/n_i)\mathrm{Vol}(\mathcal{R}_{X,W}) + o(X) = (1/n_i)\mathrm{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X)$.

Proof. We will require the following lemma.

Lemma 6. *If H is any bounded measurable set in $V_{\mathbb{R}}$, then the number of irreducible lattice points in zH is $\mathrm{Vol}(zH) + o(z^d)$ as $z \to \infty$ (i.e., reducible lattice points become negligible as z goes to infinity).*

Proof. Without the irreducibility conditions, this statement is just the theory of Riemann integration, though it can also be deduced via Davenport's lemma [Dav51a], which improves the $o(z^d)$ to $O(z^{d-1})$. Thus, to obtain the lemma, it remains to show that the reducible lattice

https://doi.org/10.1112/S0010437X16007260 Published online by Cambridge University Press

points have density 0 among all lattice points in zH as $z \to \infty$. To show this, we may use the fact that, if a lattice point in $V_{\mathbb{Z}}$ is reducible, then it must satisfy various congruence conditions; it then suffices to show that the density of points satisfying all these congruence conditions is 0. This follows in the case $n = 5$ from [Bha10, § 3.2]; the cases $n = 3$ and $n = 4$ can be handled in the identical manner (using the fact that S_3 is generated by any 2-cycle and 3-cycle, and S_4 is generated by any 3-cycle and 4-cycle). A more quantitative version of the density-0 statement for $n \in \{3, 4\}$ can be deduced from [Dav51b, §§ 4 and 5] and [Bha05, § 2.4]; this allows us to replace the $o(z^d)$ term in the lemma by $O(z^{d-1})$ in these cases. □

Let $\mathcal{R}'_{1,W}$ be a bounded, measurable subset of $\mathcal{R}_{1,W}$ such that $\mathrm{Vol}(\mathcal{R}'_{1,W}) \geqslant \mathrm{Vol}(\mathcal{R}_{1,W}) - \epsilon$, and let $\mathcal{R}'_{X,W} := X^{1/d} \cdot \mathcal{R}'_{1,W}$. Lemma 6 then implies that the number of irreducible lattice points in $\mathcal{R}'_{X,W}$ is equal to $(1/n_i)\mathrm{Vol}(\mathcal{R}'_{1,W}) \cdot X + o(X)$. Therefore, $N(V_{\mathbb{Z}}^{(i)}; X, W) \geqslant \#\{\text{irreducible lattice points in } \mathcal{R}'_{X,W}\} \geqslant (1/n_i)(\mathrm{Vol}(\mathcal{R}_{1,W}) - \epsilon) \cdot X + o(X)$. Since this is true for any ϵ, we conclude that

$$N(V_{\mathbb{Z}}^{(i)}; X, W) \geqslant \frac{1}{n_i}\mathrm{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X). \tag{6}$$

Let $\overline{W} = \mathcal{S}_{n-1} - W$. Running the same argument above with $\overline{W}$ in place of W, we have

$$N(V_{\mathbb{Z}}^{(i)}; X, \overline{W}) \geqslant \frac{1}{n_i}\mathrm{Vol}(\mathcal{R}_{1,\overline{W}}) \cdot X + o(X). \tag{7}$$

Adding (6) and (7), we obtain

$$N(V_{\mathbb{Z}}^{(i)}; X, W) + N(V_{\mathbb{Z}}^{(i)}; X, \overline{W}) \geqslant \frac{1}{n_i}\mathrm{Vol}(\mathcal{R}_{1,W}) \cdot X + \frac{1}{n_i}\mathrm{Vol}(\mathcal{R}_{1,\overline{W}}) \cdot X + o(X),$$

i.e.,

$$N(V_{\mathbb{Z}}^{(i)}; X) \geqslant \frac{1}{n_i}\mathrm{Vol}(\mathcal{R}_1) \cdot X + o(X). \tag{8}$$

However, by Theorem 4, we have equality in (8), and therefore must also have equality in (6) and (7). This concludes the proof of Theorem 5. □

In order to prove equidistribution, we require the following result, whose proof we defer to § 6.

Theorem 7. *For $n \in \{3, 4, 5\}$, we have*

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}.$$

Granting this theorem for the moment, we then obtain the following corollary.

Corollary 7.1. *When irreducible elements in $V_{\mathbb{Z}}^{(i)}$, up to $G_{\mathbb{Z}}$-equivalence, are ordered by discriminant, the shapes of these elements are equidistributed in $\mathcal{S}_{n-1}$ with respect to μ.*

4. Congruence conditions

Let S be any subset of $V_{\mathbb{Z}}$ defined by *finitely many* congruence conditions modulo prime powers. Then, in [DH71, Bha05, Bha10], the following congruence version of Theorem 4 is proven.

Theorem 8. *For $n \in \{3, 4, 5\}$, we have*

$$N(S; X) = \frac{1}{n_i}\prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_1) \cdot X + o(X),$$

where $\mu_p(S)$ denotes the p-adic density of S in $V_{\mathbb{Z}}$.

https://doi.org/10.1112/S0010437X16007260 Published online by Cambridge University Press

We also have the following congruence version of Lemma 6, whose proof is identical.

Lemma 9. *If H is any bounded measurable subset of $V_{\mathbb{R}}$, then the number of irreducible lattice points in $S \cap zH$ is*

$$\frac{1}{n_i}\prod_p \mu_p(S)\cdot \mathrm{Vol}(zH) + o(z^d) \quad \text{as } z \to \infty.$$

Running the same argument in § 3 with S instead of $V_{\mathbb{Z}}$ (noticing that S is the disjoint union of finitely many translates of lattices), we obtain the following theorem.

Theorem 10. *For $n \in \{3, 4, 5\}$, we have*

$$N(S; X, W) = \frac{1}{n_i}\prod_p \mu_p(S)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X). \tag{9}$$

Again using Theorem 7, we then obtain the following corollary about equidistribution.

Corollary 10.1. *When irreducible elements of $S \cap V_{\mathbb{Z}}^{(i)}$, up to $G_{\mathbb{Z}}$-equivalence, are ordered by discriminant, the shapes of these elements are equidistributed in $\mathcal{S}_{n-1}$ with respect to μ.*

5. Maximality

Let U denote the subset of elements of $V_{\mathbb{Z}}$ corresponding to (R, S), where R is a maximal ring of rank n, and U_p the subset of elements in $V_{\mathbb{Z}}$, where R is maximal at p. Then $U = \bigcap_p U_p$ and is defined by infinitely many congruences modulo prime powers (see [DH71, § 2], [Bha04, § 4.10], and [Bha08, § 12]). To show that (9) holds even for $S = U$, we require the following lemma, which is [DH71, § 4, Proposition 1], [Bha05, Proposition 23], and [Bha10, Proposition 19].

Lemma 11. *Let $W_p = V_{\mathbb{Z}} - U_p$. Then $N(W_p; X) = O(X/p^2)$.*

Let Y be any positive integer. Then $\bigcap_{p<Y} U_p$ is defined by finitely many congruence conditions. So, by Theorem 10, we have

$$N\biggl(\bigcap_{p<Y} U_p; X, W\biggr) = \frac{1}{n_i}\prod_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X).$$

Then

$$N(U; X, W) \leqslant N\biggl(\bigcap_{p<Y} U_p; X, W\biggr) = \frac{1}{n_i}\prod_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X).$$

Letting Y tend to infinity, we obtain $N(U; X, W) \leqslant (1/n_i)\prod_p \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X)$.

To obtain the reverse inequality, we note that

$$\bigcap_{p<Y} U_p \subset \biggl(U \cup \bigcup_{p\geqslant Y} W_p\biggr).$$

https://doi.org/10.1112/S0010437X16007260 Published online by Cambridge University Press

Therefore,

$$\begin{aligned}N(U;X,W) &\geqslant N\biggl(\bigcap_{p<Y} U_p;X,W\biggr) - \sum_{p\geqslant Y} N(W_p;X,W)\\ &= \frac{1}{n_i}\prod_{p<Y}\mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X) - \sum_{p\geqslant Y} O(X/p^2)\\ &= \frac{1}{n_i}\prod_{p<Y}\mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X) + O(X)\cdot \sum_{p\geqslant Y} 1/p^2\\ &= \frac{1}{n_i}\prod_{p<Y}\mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X) + O(X/Y).\end{aligned}$$

Letting Y tend to infinity, we obtain

$$N(U;X,W) = \frac{1}{n_i}\prod_{p}\mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X).$$

Together with Theorem 7, this implies Theorem 1.

6. Computation of volumes: proof of Theorem 7

In this section, we prove Theorem 7, namely, that

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}. \tag{10}$$

To calculate the volumes occurring in (10), we note that since $v^{(i)}$ has shape $\begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1\end{bmatrix}$, the shape of $gv^{(i)}$ for $g \in G_{\mathbb{R}}$ is simply the image of g in

$$\mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/\mathrm{GO}_{n-1}(\mathbb{R}).$$

Similarly, the shape of $gv^{(i)}$ for $g \in G'_{\mathbb{R}}$ is simply the image of g in

$$\mathrm{GL}^{\pm 1}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})/\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R}) \cong \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/\mathrm{GO}_{n-1}(\mathbb{R}),$$

where again for any matrix group G we use $G^{\pm 1}$ to denote the subgroup of G consisting of those elements having determinant ± 1.

We use the following proposition, which immediately follows from [Shi72, Proposition 2.4], [Bha05, Proposition 21], and [Bha10, Proposition 16] via an application of Lebesgue's dominated convergence theorem and the density of the bounded continuous functions in the integrable ones.

Proposition 12. *For $i \in \{0,1,\dots,\lfloor n/2\rfloor\}$, let $f \in L^1(V^{(i)}_{\mathbb{R}})$. Then there exists a nonzero constant c_i such that*

$$\int_{g\in G'_{\mathbb{R}}} f(g\cdot v^{(i)})\,dg = c_i \cdot \int_{v\in V^{(i)}_{\mathbb{R}}} |\mathrm{Disc}(v)|^{-1} f(v)\,dv.$$

(We always use dg to denote a fixed Haar measure.)

https://doi.org/10.1112/S0010437X16007260 Published online by Cambridge University Press

In the above proposition, set $f(v)$ to be in turn $\chi_{\mathcal{R}_{1,W}}(v)|\mathrm{Disc}(v)|$ and $\chi_{\mathcal{R}_1}(v)|\mathrm{Disc}(v)|$, where $\chi_{\mathcal{R}_{1,W}}$ and $\chi_{\mathcal{R}_1}$ denote the characteristic functions of $\mathcal{R}_{1,W}$ and $\mathcal{R}_1$, respectively. Then

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\int_{g\in G'_{\mathbb{R}}} \chi_{\mathcal{R}_{1,W}}(g\cdot v^{(i)})|\mathrm{Disc}(g\cdot v^{(i)})|\,dg}{\int_{g\in G'_{\mathbb{R}}} \chi_{\mathcal{R}_1}(g\cdot v^{(i)})|\mathrm{Disc}(g\cdot v^{(i)})|\,dg}. \tag{11}$$

Since $\mathcal{R}_1$ lies in a fundamental domain for the action of $G'_{\mathbb{Z}}$ on $V_{\mathbb{R}}^{(i)}$, the integrals appearing in (11) may naturally be taken over $G'_{\mathbb{Z}}\backslash G'_{\mathbb{R}}$. Now, if $g=(\lambda, g_{n-1}, g_{r-1})\in G'_{\mathbb{R}}$, then λ does not affect the shape (i.e., $q((\lambda, g_{n-1}, g_{r-1})\cdot v) = q((1, g_{n-1}, g_{r-1})\cdot v)$). Since $\mathrm{Disc}(g\cdot v^{(i)})=\lambda^d$, the ratio (11) becomes

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\int_0^1 \lambda^d\,d^\times\lambda \int_{g\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} \chi_{\mathcal{R}_{1,W}}(g\cdot v^{(i)})\,dg}{\int_0^1 \lambda^d\,d^\times\lambda \int_{g\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} \chi_{\mathcal{R}_1}(g\cdot v^{(i)})\,dg},$$

where we use G''_T to denote simply $\mathrm{GL}_{n-1}^{\pm 1}(T)\times \mathrm{GL}_{r-1}^{\pm 1}(T)$. In fact, for any $g\in G'_{\mathbb{R}}$, where $0<\lambda<1$, we have that $g\cdot v^{(i)}$ has absolute discriminant <1, and so the characteristic function $\chi_{\mathcal{R}_1}$ occurring in the integral in the denominator can be removed. Now the factor of $\mathrm{GL}_{r-1}^{\pm 1}(T)$ also does not affect the shape, and thus

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\int_{g\in \mathrm{GL}_{r-1}^{\pm1}(\mathbb{Z})\backslash \mathrm{GL}_{r-1}^{\pm1}(\mathbb{R})} dg \int_{g\in \mathrm{GL}_{n-1}^{\pm1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}^{\pm1}(\mathbb{R})} \chi_{\mathcal{R}_{1,W}}(g\cdot v^{(i)})\,dg}{\int_{g\in \mathrm{GL}_{r-1}^{\pm1}(\mathbb{Z})\backslash \mathrm{GL}_{r-1}^{\pm1}(\mathbb{R})} dg \int_{g\in \mathrm{GL}_{n-1}^{\pm1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}^{\pm1}(\mathbb{R})} dg}.$$

Since $q(g\cdot v^{(i)}) = q(v^{(i)})$ for $g\in \mathrm{GO}^{\pm1}(\mathbb{R})$, we obtain

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\int_{g\in \mathrm{GL}_{n-1}^{\pm1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}^{\pm1}(\mathbb{R})/\mathrm{GO}_{n-1}^{\pm1}(\mathbb{R})} \chi_{\mathcal{R}_{1,W}}(g\cdot v^{(i)})\,dg \int_{k\in \mathrm{GO}_{n-1}^{\pm1}(\mathbb{R})} dk}{\int_{g\in \mathrm{GL}_{n-1}^{\pm1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}^{\pm1}(\mathbb{R})/\mathrm{GO}_{n-1}^{\pm1}(\mathbb{R})} dg \int_{k\in \mathrm{GO}_{n-1}^{\pm1}(\mathbb{R})} dk}.$$

Since the $g\in \mathrm{GL}_{n-1}^{\pm1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}^{\pm1}(\mathbb{R})/\mathrm{GO}_{n-1}^{\pm1}(\mathbb{R})$ such that $g\cdot v^{(i)}$ has shape in W are exactly those that are in W, we obtain Theorem 7.

Acknowledgements

We are extremely grateful to Rob Harron, Wei Ho, Hendrik Lenstra, Melanie Matchett Wood, Peter Sarnak, and Arul Shankar for many helpful conversations. It is also a pleasure to thank the Packard Foundation and the National Science Foundation (grant DMS-1001828) for their kind support.

References

Bha04 M. Bhargava, *Higher composition laws III: the parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), 1329–1360.

Bha05 M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), 1031–1063.

Bha08 M. Bhargava, *Higher composition laws IV: the parametrization of quintic rings*, Ann. of Math. (2) **167** (2008), 53–94.

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

BS14 M. Bhargava and A. Shnidman, *On the number of cubic orders of bounded discriminant having automorphism group C_3, and related problems*, Algebra Number Theory **8** (2014), 53–88.

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

Dav51a H. Davenport, *On a principle of Lipschitz*, J. Lond. Math. Soc. (2) **26** (1951), 179–183.

Dav51b H. Davenport, *On the class-number of binary cubic forms I*, J. Lond. Math. Soc. (2) **26** (1951), 183–192.

Dav51c H. Davenport, *On the class-number of binary cubic forms II*, J. Lond. Math. Soc. (2) **26** (1951), 192–198.

DH71 H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. R. Soc. Lond. Ser. A **322** (1971), 405–420.

DF64 B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, vol. 10 (American Mathematical Society, Providence, RI, 1964).

Min05 H. Minkowski, *Diskontinuitätsbereich für arithmetische Äquivalenz*, J. reine angew. Math. **129** (1905), 220–274.

SK77 M. Sato and T. Kimura, *A classification of irreducible prehomogeneous vector spaces and their relative invariants*, Nagoya Math. J. **65** (1977), 1–155.

Shi72 T. Shintani, *On Dirichlet series whose coefficients are class numbers of integral binary cubic forms*, J. Math. Soc. Japan **24** (1972), 132–188.

Ter97 D. Terr, *The distribution of shapes of cubic orders*, PhD thesis, University of California, Berkeley (1997).

WY92 D. Wright and A. Yukie, *Prehomogeneous vector spaces and field extensions*, Invent. Math. **110** (1992), 283–314.

Manjul Bhargava bhargava@math.princeton.edu
Department of Mathematics, Fine Hall, Princeton University, Princeton, NJ 08544, USA

Piper Harron paharron@gmail.com
Honolulu, HI, USA