Counting nonsingular matrices with primitive row vectors

A problem in the geometry of numbers

Samuel Holmin
holmin@kth.se

Master's Thesis in Mathematics at KTH
Presented June 3, 2010

Supervisor: Pär Kurlberg

Abstract

We count the number of nonsingular integer $n \times n$-matrices with primitive row vectors, determinant k, and Euclidean matrix norm less than T, and find that as $T \to \infty$ this is asymptotically

$$c'_{n,k} T^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon})$$

for all $\varepsilon > 0$ and a certain constant $c'_{n,k} > 0$. The corresponding problem for singular matrices has previously been solved by Wigman, and without the constraint of primitive rows, the problem has been solved in the case of nonsingular matrices by Duke, Rudnick and Sarnak, and in the case of singular matrices by Katznelson.

We also investigate the density of matrices with primitive rows in the space of matrices with determinant k. We find that this density converges to 1 as $n \to \infty$. Perhaps more interestingly, we find that for fixed n, the density is approximately 1 for k divisible by no small numbers (large primes, for instance), and that the density for matrices with a determinant divisible by all small numbers (say, $k = m!$ for some large m) approximates the density for singular matrices ($k = 0$).

Contents

Chapter 1

Introduction

In this thesis, we solve a new problem in the geometry of numbers. We say that an integer vector $v \in \mathbb{Z}^n$ is **primitive** if it cannot be written as an integer multiple $m \neq 1$ of some other integer vector $w \in \mathbb{Z}^n$. Let A be an integer $n \times n$-matrix with nonzero determinant k and primitive row vectors. We ask how many such matrices A there are of **Euclidean norm** at most T, that is, $\|A\| \leq T$, where $\|A\| := \sqrt{\sum a_{ij}^2} = \sqrt{\operatorname{tr}(A^t A)}$. Let $N'_{n,k}(T)$ be this number (the prime in the notation denotes the primitivity of the rows). The function $N'_{n,k}$ jumps irregularly as T increases, so we will direct our interest towards estimating its asymptotic growth, as well as confining its fluctuations to a small error term. We will also investigate the density of matrices with primitive rows in the space of all integer $n \times n$-matrices with a given determinant, and discover some surprising facts.

The problem is given a visual interpretation in section 1.2, but what originally motivated its study were a series of related counting problems considered in the articles [DRS], [Kat] and [Wig]. Let $M_{n,k}$ be the set of integer $n \times n$-matrices with determinant k, and let $N_{n,k}(T) := |B_T \cap M_{n,k}|$, where B_T is the (closed) ball of radius T centered at the origin in the space of real $n \times n$-matrices $M_n(\mathbb{R})$ equipped with the Euclidean norm. We will assume that $n \geq 2$ is fixed, and for convenience we will assume $k > 0$ throughout unless stated otherwise.

Duke, Rudnick and Sarnak [DRS] found the asymptotic behavior of $N_{n,k}$, namely

$$N_{n,k}(T) = c_{n,k} T^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(n+1)+\varepsilon}),$$

as $T \to \infty$, for a certain constant $c_{n,k}$ and all $\varepsilon > 0$ (for $n = 2$, an even better error term $O(T^{4/3})$ is known). Their methods did not work for singular matrices (that is, for $k = 0$), and later Katznelson [Kat] proved that

$$N_{n,0}(T) = c_{n,0} T^{n(n-1)} \log T + O(T^{n(n-1)}).$$

The proof ideas of these two very different cases are sketched out in section 1.3.

Let $M'_{n,k}$ be the set of matrices in $M_{n,k}$ with primitive row vectors, and let $N'_{n,k}(T) := |B_T \cap M'_{n,k}|$. Wigman [Wig] considered the growth of the number of matrices inside balls of increasing radius in $M'_{n,0}$ (albeit under a different norm, but the result carries over to our case with the Euclidean norm, with changed constants), and proved that as $T \to \infty$,

$$\begin{aligned} N'_{n,0}(T) &= c'_{n,0} T^{n(n-1)} \log T + O(T^{n(n-1)}), \qquad n \geq 4, \\ N'_{3,0}(T) &= c'_{3,0} T^{3(3-1)} \log T + O(T^{3(3-1)} \log\log T), \\ N'_{2,0}(T) &= c'_{2,0} T^{2(2-1)} + O(T). \end{aligned}$$

The history of the constraint of primitivity can be traced to the **primitive circle problem**, which asks how many primitive vectors there are of length at most T in $\mathbb{Z}^n$ given any (large) T, and the case $n = 2$ is in fact equivalent to it. We discuss the primitive circle problem in Appendix A and we make the simple derivation for the asymptotics of $N'_{2,0}$ in Appendix B.

With the questions regarding the growth of $N_{n,k}$, $N_{n,0}$ and $N'_{n,0}$ resolved, it is natural for us to ask how $N'_{n,k}$ behaves for $k \neq 0$. Our main result is:

Theorem 1.1. *Let $k \neq 0$. Then*

$$N'_{n,k}(T) = c'_{n,k} T^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon}),$$

as $T \to \infty$ for a certain constant $c'_{n,k}$ and all $\varepsilon > 0$.

Chapter 3 is dedicated to the proof of this theorem.

We will find that

$$c'_{n,k} = \frac{C_1}{k^{n-1}} \sum_{d_1 \cdots d_n = |k|} \prod_{i=1}^{n} \sum_{g | d_i} \mu(g) \left(\frac{d_i}{g}\right)^{i-1},$$

for $k \neq 0$, which may be compared to the other constants

$$\begin{aligned} c_{n,k} &= \frac{C_1}{k^{n-1}} \sum_{d_1 \cdots d_n = |k|} \prod_{i=1}^{n} d_i^{i-1} \\ c_{n,0} &= C_0 \frac{n-1}{\zeta(n)} \\ c'_{n,0} &= C_0 \frac{n-1}{\zeta(n-1)^n \zeta(n)} \qquad (n \geq 3) \\ c'_{2,0} &= \frac{\pi T^2}{\zeta(2)} \end{aligned}$$

where ζ is the Riemann zeta function, μ is the Möbius function, and C_0 and C_1 are constants defined as follows (these depend on n, but we will always regard n as fixed). Let ν be the Haar measure on $\mathrm{SL}_n(\mathbb{R})$ (we will introduce Haar measures in section 2.2) and let w be the measure constructed in Appendix D. Write V_n for the volume of the unit ball in $\mathbb{R}^n$ and S_{n-1} for the surface area of the $(n-1)$-dimensional unit sphere in $\mathbb{R}^n$. Then

$$\begin{aligned} C_1 &= \lim_{T\to\infty} \frac{\nu(B_T \cap \mathrm{SL}_n(\mathbb{R}))}{T^{n(n-1)}} = \frac{V_{n(n-1)}S_{n-1}}{2\zeta(2)\cdots\zeta(n)} \\ &= \frac{1}{\zeta(2)\cdots\zeta(n)} \frac{\pi^{n^2/2}}{\Gamma\left(\frac{n}{2}\right)\Gamma\left(\frac{n(n-1)}{2}+1\right)}, \\ C_0 &= w(B_1) = \frac{V_{n(n-1)}S_{n-1}}{2} = \frac{\pi^{n^2/2}}{\Gamma\left(\frac{n}{2}\right)\Gamma\left(\frac{n(n-1)}{2}+1\right)}. \end{aligned}$$

1.1 Density

Knowing already the growth of $N_{n,k}$, it will be interesting to compare this to the growth of $N'_{n,k}$. Their quotient can be interpreted as a density. Let X be a normed space and let B_T be the (closed) ball of radius T centered at the origin. Let $M' \subseteq M$ be two subsets of X such that the intersection of either with any ball in X is finite. We define the **density** of M' in M to be the limit (if it exists)

$$\mathrm{density}(M'/M) := \lim_{T\to\infty} \frac{|B_T \cap M'|}{|B_T \cap M|}.$$

We will in particular investigate the density of matrices with primitive rows in the space $M_{n,k}$,

$$D_n(k) := \mathrm{density}(M'_{n,k}/M_{n,k}) = \lim_{T\to\infty} \frac{N'_{n,k}(T)}{N_{n,k}(T)} = \frac{c'_{n,k}}{c_{n,k}}.$$

The density may also be thought of as a probability, in the following sense. Pick a matrix A from $M_{n,k}$ inside the ball B_T (which we think of as large), randomly with a uniform distribution. What is the probability that A belongs to $M'_{n,k}$? In other words, what is the probability that the matrix $A \in M_{n,k} \cap B_T$ has primitive row vectors? This is precisely $N'_{n,k}(T)/N_{n,k}(T)$. For large T, this probability is approximated by $D_n(k)$, which therefore captures intuitively the notion of what should be the probability that a random matrix with determinant k has all row vectors primitive.

It is a classical problem to determine the density of primitive vectors in the space $\mathbb{Z}^n$ (this is equivalent to the primitive circle problem), and one can show that (we do this in Appendix A) this density is exactly $1/\zeta(n)$, where ζ is the Riemann zeta function.

Comparing the functions $N_{n,0}$ and $N'_{n,0}$, we see that

$$D_n(0) = \frac{1}{\zeta(n-1)^n}$$

for $n \geq 3$. We will be interested in the value of $D_n(k)$ for large n and large k. The limit of $D_n(k)$ as $k \to \infty$ does not exist, but it does exist for particular sequences of k.

Definition 1.2. We say that a sequence of integers is **totally divisible** if its terms are eventually divisible by all positive integers smaller than m, for any m. We say that a sequence of integers is **rough** if its terms eventually have no divisors smaller than m (except for 1), for any m.

Example 1.3. Let $p_1, p_2, p_3, \ldots$ be the sequence of prime numbers. Examples of totally divisible sequences are:

$$0,\ 0,\ 0,\ \ldots$$
$$1!,\ 2!,\ 3!,\ \ldots$$
$$(p_1)^1,\ (p_1p_2)^2,\ (p_1p_2p_3)^3,\ \ldots$$

Examples of rough sequences are:

$$1,\ 1,\ 1,\ \ldots$$
$$p_1,\ p_2,\ p_3,\ \ldots$$

Examples of sequences which are neither totally divisible nor rough are:

$$1,\ 2,\ 3,\ \ldots$$
$$p_1,\ p_1p_2,\ p_1p_2p_3,\ \ldots$$

The p**-adic norm** $|k|_p$ of an integer $k \neq 0$ is p^{-m}, if p is a prime and p^m is the largest power of p that divides k. Define $|0|_p := 0$ for all primes p. Thus, a sequence $(k_1, k_2, \ldots)$ is totally divisible if and only if $|k_i|_p \to 0$ as $i \to \infty$ for all primes p, and $(k_1, k_2, \ldots)$ is rough if and only if $|k_i|_p \to 1$ as $i \to \infty$ for all primes p.

We state our main results about the density D_n. We prove these in chapter 4.

Theorem 1.4. *Let k be an integer (possibly 0). Then*

$$D_n(k) \to 1$$

uniformly as $n \to \infty$.

That is, roughly speaking, almost all large matrices have all rows primitive. This is what we would intuitively expect, as almost all vectors in $\mathbb{Z}^n$ are primitive for large n. What happens for large k is more surprising.

Theorem 1.5. *Let $n \geq 3$ be fixed. Then*

$$D_n(k_i) \to 1$$

as $i \to \infty$ if and only if the sequence $(k_1, k_2, \ldots)$ is rough.

This means that almost all matrices in $M_{n,k}$ have all rows primitive if k has no small divisors.

Theorem 1.6. *Let $n \geq 3$ be fixed. Then*

$$D_n(k_i) \to \frac{1}{\zeta(n-1)^n}$$

as $i \to \infty$ if the sequence $(k_1, k_2, \ldots)$ is totally divisible.

We prove Theorem 1.6 for nonzero k_i, but it is somewhat remarkable that this formulation holds for $k = 0$ also. The case of $k = 0$ was proved by Wigman [Wig], where he found that $D_n(0) = 1/\zeta(n-1)^n$ exactly (which therefore becomes a special case of the formulation of Theorem 1.6). Theorem 1.6 may therefore be restated as

$$D_n(k_i) \to D_n(0)$$

if $(k_1, k_2, \ldots)$ is totally divisible, for fixed n. A provocative reading of Theorem 1.6 is that if the determinant of a matrix A is divisible by all small integers (for some large value of "small"), the matrix A behaves, in a certain sense (in terms of density), as if it were singular.

The converse of Theorem 1.6 is also believed to be true.

Conjecture 1.7. *Let $n \geq 3$ be fixed. Then*

$$D_n(k) > D_n(0)$$

for all $k \neq 0$, and $D_n(k_i) \to D_n(0)$ if and only if the sequence $(k_1, k_2, \ldots)$ is totally divisible.

We give a proof of the conjecture in the case $n = 3$ in Appendix C, where it will also be shown that for any given fixed n, it has at most a finite number of counterexamples. The proof can be repeated for other small n, and it has been verified for $n = 4$ also. Combining this conjecture with Theorem 1.5, we can say that $1/\zeta(n-1)^n \leq D_n(k)$ with equality if and only if $k = 0$, and $D_n(k) \leq 1$ with equality if and only if $k = \pm 1$.

For completeness, let us state what happens in the very different case $n = 2$.

Proposition 1.8. *Let $n = 2$. Then*

$$D_2(k_i) \to 0$$

if and only if $\lim_{i\to\infty} \sum_{p|k_i} 1/p \to \infty$. *Moreover,*

$$D_2(k_i) \to 1$$

if and only if $\lim_{i\to\infty} \sum_{p|k_i} 1/p \to 0$. *The sums are taken over all primes p which divide k_i.*

Example 1.9. Let p_m be the mth prime number. Then $D_2(p_m) \to 1$ and $D_2(p_1 \cdots p_m) \to 0$ as $m \to \infty$ (the latter follows from the well-known fact that $\sum_p 1/p = \infty$).

1.2 A visual interpretation

Consider a matrix $A \in M_{n,k}$ with row vectors $r_1, \dots, r_n$. The matrix encodes an **integral lattice** Γ in $\mathbb{R}^n$, defined by the set of integer linear combinations of the rows $r_1, \dots, r_n$:

$$\Gamma := \{m_1 r_1 + \cdots + m_n r_n : m_1, \dots, m_n \in \mathbb{Z}\}.$$

The linearly independent vectors $r_1, \dots, r_n$ are said to be a **basis** for the lattice Γ (we then say the lattice has **dimension** n), and they further define a **fundamental domain** F for the lattice, with volume k:

$$F := \{\alpha_1 r_1 + \cdots + \alpha_n r_n : 0 \leq \alpha_1, \dots, \alpha_n < 1\}.$$

An illustrative way to think of an n-dimensional lattice in $\mathbb{R}^n$, having fixed a basis, is as a tiling of n-space by translations of its fundamental domain. That is, $\mathbb{R}^n$ is the disjoint union of all the **tiles** $F_\gamma := F + \gamma = \{x + \gamma : x \in F\}$, where γ varies in Γ. Indeed, this is often how one draws a lattice on a blackboard: we draw a grid of lines (for a lattice in $\mathbb{R}^2$), and declare the lattice to consist of the points of intersection of the lines.

We will say that the union of the boundaries of the tiles

$$R := \bigcup_{\gamma\in\Gamma} \partial(F_\gamma)$$

is an **integral grid**, and we will call an integral grid **primitive** if it is not properly contained in some other integral grid. A moment's thought tells us that a grid R is primitive if and only if the rows $r_1, \dots, r_n$ inducing it are all primitive vectors. We say further that R has **covolume** k.

The grid R is determined by the matrix A, but not uniquely: it is easy to see that there are exactly $n!2^n$ matrices whose row vectors induce R (we may reorder the vectors or change their signs). On the contrary, any given lattice has infinitely many bases, and even worse, it may have some bases which consist only of primitive vectors and some which do not — consider for example the two bases $\{(1,0),(0,2)\}$ and $\{(1,0),(1,2)\}$ of the same lattice.

We may thus restate our original problem as follows. How many primitive integral grids with covolume k are there, given any $k>0$ – there are infinitely many, so we restrict ourselves (somewhat arbitrarily) to counting only integral grids determined by a matrix A such that $\|A\| \leq T$. The answer to this question will be a multiple $n!2^n$ of the answer to our original problem.

This arbitrariness can be alleviated by considering instead the density of primitive grids in the space of all integral grids with covolume k. Indeed, the density is independent of the norm used: this is due to Theorem 2.19. The density of primitive grids coincides with $D_n(k)$.

1.3 Proof ideas

The proof in [DRS] and our proof of Theorem 1.1 can be summarized as follows. The set $M_{n,k}$ is partitioned into a finite number of orbits $A\,\mathrm{SL}_n(\mathbb{Z})$ for $A \in M_{n,k}$ in Hermite normal form. We may thus count the matrices in each orbit separately. As it happens, the number of matrices in each orbit scales as $1/(\det A)^{n-1}$ of the number of matrices in $\mathrm{SL}_n(\mathbb{Z})$. We can interpret $\mathrm{SL}_n(\mathbb{Z})$ as a lattice in the space $\mathrm{SL}_n(\mathbb{R})$, and the problem is reduced to a lattice point counting problem (it is important to note that this uses the more general notion of a lattice described in section 2.3). This method works for our problem as well, as $M'_{n,k}$, too, admits a partition into orbits of $\mathrm{SL}_n(\mathbb{Z})$.

The proof in [Kat] goes as follows. The rows of a given singular matrix $A \in M_{n,0}$ lie in the orthogonal complement $L_u(\mathbb{R})$ of u for some $u \in \mathbb{R}^n$. Let $A_u(\mathbb{Z})$ be the set of matrices whose rows belong to $L_u(\mathbb{Z})$. To cover $M_{n,0}$, only the sets $A_u(\mathbb{Z})$ for primitive $u \in \mathbb{Z}^n$ are needed. Each $A_u(\mathbb{Z})$ is a lattice, and the matrices in $M_{n,0}$ are counted in each lattice separately. However, in this case, the $A_u(\mathbb{Z})$ are not pairwise disjoint: for example, $A_u(\mathbb{Z})$ and $A_{-u}(\mathbb{Z})$ contain the same points, but aside from this, the intersections are of lower dimension and their contribution to the sum is negligible.

The proof in [Wig] follows along the same lines as the one in [Kat]: $M'_{n,0}$ is written as a union of sets $A'_u(\mathbb{Z})$ consisting only of matrices with primitive rows all orthogonal to a (primitive) vector u. Letting $L'_u(\mathbb{Z})$ be the set of primitive vectors orthogonal to u, we can identify $A'_u(\mathbb{Z})$ with $(L'_u(\mathbb{Z}))^n$. Möbius inversion is used to count elements in each of the sets $L'_u(\mathbb{Z})$. For $n=3$, the error term given by the Möbius inversion results in convergence problems when summing over all $A'_u(\mathbb{Z})$, which is the reason for the slightly worse error term in the final asymptotic formula.

Chapter 2

Preliminaries

Let us review the tools we will need. In chapter 3, we prove Theorem 1.1. This can be reduced to a problem of counting lattice points. We will therefore need some background in lattices (section 2.3). Translation invariance is an important property of lattices. A function counting lattice points therefore constitutes a translation invariant measure. A general principle when counting lattice points is that the number of lattice points inside a "nice" domain is roughly equal to the measure of the domain itself. One therefore wants to have a translation invariant measure on the ambient space. This is precisely what a Haar measure is. For an n-dimensional lattice in $\mathbb{R}^n$ this is simpler stated as (see also Lemma 2.17): the number of lattice points inside a convex domain is roughly equal to the volume of the domain.

In chapter 4, we investigate the density D_n. This is reduced to a finite problem and plays out largely combinatorially. Our counting functions will turn out to be multiplicative, and some theory of Dirichlet convolutions will be needed.

2.1 Notation and definitions

The **special linear group** $\mathrm{SL}_n(R)$ is the group of invertible $n \times n$-matrices with determinant 1 over the ring R (with matrix multiplication as group operation). In this thesis, we will only be concerned with the groups $\mathrm{SL}_n(\mathbb{Z})$ and $\mathrm{SL}_n(\mathbb{R})$. Note that $\mathrm{SL}_n(\mathbb{Z}) = M_{n,1}$. The **special orthogonal group** $\mathrm{SO}_n(\mathbb{R})$ is the group of orthogonal real $n \times n$-matrices with determinant 1.

The notation $f(T) \sim g(T)$ means that $f(T)/g(T) \to 1$ as $T \to \infty$.

We denote by μ the Möbius function; its definition is given in in section 2.5. The **Riemann zeta function** ζ is given by

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - 1/p^s}$$

for $\operatorname{Re} s > 1$, where we use the convention that when an index p is used in a sum or product, it ranges over the set of primes.

2.2 The Haar measure

Let G be a **locally compact separable (topological) group** G. This means that G is simultaneously a topological space and a group, such that the group operations $(a, b) \mapsto ab$ and $a \mapsto a^{-1}$ are continuous, and such that it is locally compact and separable as a topological space. We recall briefly the following facts from topology and measure theory. That G is **locally compact** means that each point in G has a compact neighborhood, and that it is **separable** means that there are disjoint neighborhoods about any two points of G. The collection of **Borel sets** of G is the smallest collection of subsets of G which contains all the open subsets of G (or equivalently, all closed subsets of G) that is closed under set differences and countable unions. In a topological group, we will interpret the map $x \mapsto gx$ as a **(left) translation** by $g \in G$, and we will refer to the sets $gS := \{gx : x \in S\}$ for $g \in G$ as **translates** of G. By the continuity of translations, the translate gS of S is a Borel set for any Borel set S and any $g \in G$. A **Borel measure** on G is a measure defined on the Borel sets of G. In the following we will simply call the Borel sets **measurable sets** and a Borel measure on G a **measure on** G.

A Borel measure ν on a topological group G is said to be **left invariant** if for any Borel set $S \subseteq G$ and for any $g \in G$, the measure of S and its left translate gS are equal, that is, $\nu(gS) = \nu(S)$. Similarly one can define **right invariant** measures. If a measure is both left- and right invariant, we say that it is **bi-invariant**.

The fundamental fact about Haar measures is the following.

Lemma 2.1 ([Coh], Theorems 9.2.1 and 9.2.3)**.** *Given any locally compact separable group G there exists a unique (up to multiplication by a constant) left invariant Borel measure ν which is not identically zero and which assigns a finite measure to all compact sets. This measure is called the **(left) Haar measure** of G.*

Similarly, one can define a **right Haar measure**. If ν is a left Haar measure, then $\nu^{-1}(S) := \nu(S^{-1})$ defines a right Haar measure, and conversely. In the following, we will denote the Haar measure of G by ν_G, or simply by ν when there is no confusion as to what G is. The Haar measure is ambiguous up to a scalar multiple, but this will not matter to us once the measure is fixed.

One defines as in the general theory of integration an integral with respect to the Haar measure, which is called the **Haar integral**. If f is an integrable function, we will denote its integral over a measurable set S by

$$\int_S f(x)d\nu(x).$$

By the left invariance of the Haar measure, we have for any $g \in G$ that

$$\int f(gx)d\nu(x) = \int f(x)d\nu(x),$$

with the integral taken over all of G.

Example 2.2 ($(\mathbb{R}^n, +)$)**.** The real line $\mathbb{R}$ with the Euclidean topology (and more generally, Euclidean space $\mathbb{R}^n$), regarded as a group under addition, is a locally compact separable group. The ordinary Lebesgue measure ν on $\mathbb{R}$ is a Haar measure. Since $\nu(S) = \int_S dx$ for measurable $S \subseteq \mathbb{R}$, a common (abuse of) notation is $dx := \nu$ for the measure on $\mathbb{R}$.

By the translation invariance of dx, we get the familiar identity

$$\int f(a + x)\, dx = \int f(x)\, dx$$

for all real a and integrable f, with the integral taken over all of $\mathbb{R}$.

Example 2.3 ($(\mathbb{R}^*, \cdot)$)**.** The nonzero real numbers $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ with the Euclidean topology, regarded as a group under multiplication, is a locally compact separable group. Its Haar measure is given by $\nu(S) = \int_S dx\,/|x|$, and one usually writes $dx\,/|x| := \nu$. For all real a and integrable f, we have, by a change of variables, that

$$\int f(ax)\frac{dx}{|x|} = \int f(x)\frac{dx}{|x|}.$$

Example 2.4 (Discrete groups)**.** Any group G equipped with the discrete topology is a locally compact separable group. Its Haar measure is the counting measure $S \mapsto |S| = \sum_{x\in S} 1$. For all $a \in G$ and integrable f, we have

$$\sum_{x\in G} f(ax) = \sum_{x\in G} f(x).$$

Example 2.5 ($\mathrm{GL}_n(\mathbb{R})$)**.** Consider the general linear group $\mathrm{GL}_n(\mathbb{R})$ equipped with the Euclidean topology. It is an open subset of $M_n(\mathbb{R})$ (it is the inverse image of the open set $\mathbb{R}^*$ under the (continuous) determinant function). The space $M_n(\mathbb{R})$ is by definition homeomorphic to $\mathbb{R}^{n^2}$ via the map $(x_{ij}) \mapsto (x_{11}, \ldots, x_{nn}) : M_n(\mathbb{R}) \to \mathbb{R}^{n^2}$, and $\mathbb{R}^{n^2}$ is separable and locally compact. Therefore $\mathrm{GL}_n(\mathbb{R})$ is separable and locally compact. The Haar measure of $\mathrm{GL}_n(\mathbb{R})$ is $dX\,/|\det X|$, where $dX := dx_{11} \cdots dx_{nn}$ is the ordinary Euclidean measure on the space of $n \times n$-matrices $X = (x_{ij})$. For any $A \in \mathrm{GL}_n(\mathbb{R})$ and integrable f, we have (by a change of variables)

$$\int f(AX) \frac{dX}{|\det X|} = \int f(X) \frac{dX}{|\det X|}.$$

Example 2.6 ($\mathrm{SL}_n(\mathbb{R})$)**.** Let us finally consider the special linear group $\mathrm{SL}_n(\mathbb{R})$ under the Euclidean topology. It is a closed subset of $\mathrm{GL}_n(\mathbb{R})$ because it is the inverse image of 1 under the determinant function restricted to $\mathrm{GL}_n(\mathbb{R})$. Therefore $\mathrm{SL}_n(\mathbb{R})$ is separable and locally compact. A Haar measure ν can be constructed on $\mathrm{SL}_n(\mathbb{R})$ in various ways. Perhaps the simplest is the following, given in [Sie2]. Let vol be the Euclidean measure on $M_n(\mathbb{R})$. We define a subset S of $\mathrm{SL}_n(\mathbb{R})$ to be measurable if the cone

$$[0,1] \cdot S = \{t \cdot X : t \in [0,1], X \in S\}$$

is measurable as a subset of $M_n(\mathbb{R})$, and define the measure of S to be $\nu(S) := \mathrm{vol}([0,1] \cdot S)$, that is,

$$\nu(S) = \int_{[0,1]\cdot S} dX\,.$$

Changing the variable by a left- or right multiplication by a matrix $A \in \mathrm{SL}_n(\mathbb{R})$ gives rise to the Jacobian $|(\det A)^n| = 1$, so ν is bi-invariant. This fact is important to us, so we will state this in a lemma.

Lemma 2.7. *The Haar measure of* $\mathrm{SL}_n(\mathbb{R})$ *is bi-invariant.*

We give now an explicit expression for the Haar measure on $\mathrm{SL}_2(\mathbb{R})$.

Proposition 2.8. *The Haar measure of* $\mathrm{SL}_2(\mathbb{R})$ *is (up to a multiplicative constant)*

$$\nu(S) = \int_S \frac{dx\,dy\,dz}{|x|},$$

where we use the parametrization $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ *for matrices in* $\mathrm{SL}_2(\mathbb{R})$*.*

Proof. For $X \in \mathrm{SL}_2(\mathbb{R})$, write $\nu(S) = \int_{X \in S} d\nu(X)$ for the Haar measure of $\mathrm{SL}_2(\mathbb{R})$. We make the ansatz $d\nu(X) =: f(X)\,dx\,dy\,dz$, where $X = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ and dx, dy, dz are the usual Lebesgue measures with respect to x, y, z respectively, and $w = (1 + yz)/x$ (this follows from $1 = \det X = xw - yz$). For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$, we have (by the left invariance of the measure; recall that it is bi-invariant by Lemma 2.7)

$$\nu(AS) = \int_{X \in AS} d\nu(X) = \int_{A^{-1}X \in S} d\nu(AA^{-1}X) =$$
$$\int_{Y \in S} d\nu(AY) = \int_{X \in S} d\nu(AX) = \int_{X \in S} f(AX)\,dx\,dy\,dz\,.$$

We change variables to x', y', z' where

$$X' := \begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix} := AX = \begin{pmatrix} ax+bz & az+bw \\ cx+dz & cz+dw \end{pmatrix}.$$

We get the Jacobian matrix (we omit writing out the starred entries)

$$\begin{pmatrix} \frac{\partial x'}{\partial x} & \frac{\partial x'}{\partial z} & \frac{\partial x'}{\partial y} \\ \frac{\partial z'}{\partial x} & \frac{\partial z'}{\partial z} & \frac{\partial z'}{\partial y} \\ \frac{\partial y'}{\partial x} & \frac{\partial y'}{\partial z} & \frac{\partial y'}{\partial y} \end{pmatrix} = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ * & * & a+bz/x \end{pmatrix},$$

with determinant $(\det A)(ax+bz)/x = \pm(ax+bz)/x$. So we get that

$$\nu(AS) = \int_{X \in S} f(AX) \left| \frac{ax+bz}{x} \right| dx\, dy\, dz,$$

which agrees with $\nu(S)$ if $f(X) = 1/|x|$.

Thus the Haar measure of $\mathrm{SL}_2(\mathbb{R})$ is

$$\frac{dx\, dy\, dz}{|x|}. \qquad \square$$

Remark 2.9. Not all Haar measures are bi-invariant. An example is given by the group G of matrices $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ for all $x > 0$ and all $y \in \mathbb{R}$ (with matrix multiplication as the group operation). It can be shown that

$$\frac{dx\, dy}{x^2} \quad \text{and} \quad \frac{dx\, dy}{x}$$

are left- and right Haar measures of G, respectively, but certainly, these are not scalar multiples of each other.

2.3 Lattices

Let G be a topological group. A **lattice** Γ in G is a discrete subgroup of G (that is, the topology of G restricted to Γ is the discrete topology). We will assume that G is locally compact and separable (so that it has a Haar measure), as well as second countable (recall that a topological space is **second countable** if it has a countable base). The classical example is the square lattice $\mathbb{Z}^2$ in $\mathbb{R}^2$ (seen as a group under addition). In this thesis, we consider the lattice $\mathrm{SL}_n(\mathbb{Z})$ in $\mathrm{SL}_n(\mathbb{R})$.

A **(left) fundamental domain** relative to Γ is a set $F \subseteq G$ such that F is a Borel set (and hence measurable), and G is the disjoint union of all translates $F\gamma$ of F for $\gamma \in \Gamma$. For a fixed fundamental domain F, we will call the translates $F\gamma$ of F for $\gamma \in \Gamma$ **tiles**.

We will now prove that a fundamental domain always exists (the proof is adapted from the one in the article [Sie1]), and that all fundamental domains relative to any given lattice have the same *right* Haar measure.

Let G be a topological group and let Γ be a lattice in G. We say that $B \subseteq G$ is a **subdomain** (relative to Γ) if the translates $B\gamma_1$ and $B\gamma_2$ of B are disjoint for all $\gamma_1 \neq \gamma_2$ in Γ.

Lemma 2.10. *Let Γ be a lattice in a topological group G. Given any point $g \in G$, there exists an open subdomain B containing g.*

Proof. Let U be a neighborhood of the identity element e of G, containing no other point of Γ. Set $f(x,y) := x^{-1}y$. By the continuity of f, there exists a neighborhood W about (g,g) such that $f(x,y) \in U$ whenever $(x,y) \in W$. By the definition of the product topology of $G \times G$, there exist open sets $V_0, V_1 \subseteq G$ such that $(g,g) \in V_0 \times V_1 \subseteq W$. Let $B := V_0 \cap V_1$. Let $x, y \in B$. It remains to prove that if $y = x\gamma$ for some $\gamma \in \Gamma$, then $\gamma = e$. Since $(x,y) \in W$, we have $f(x,y) = x^{-1}y \in U$, and thus $x^{-1}y \neq \gamma$ for all $\gamma \neq e$ in Γ and therefore $y \neq x\gamma$. □

Lemma 2.11. *Let Γ be a lattice in a topological group G. Suppose there exists a (countable) cover $B_1, B_2, \ldots$ of G consisting only of open subdomains relative to Γ. Then F is a fundamental domain relative to Γ, where*

$$F_1 := B_1, \quad F_m := B_m \setminus (B_1 \cup \cdots \cup B_{m-1})\Gamma$$
$$F := \bigcup F_i.$$

Proof. Each point of Γ belongs to at most one set B_i, so Γ is countable, so $F_m = B_m \setminus (B_1 \cup \cdots \cup B_{m-1})\Gamma = B_m \setminus \bigcup_{\gamma\in\Gamma}(B_1\gamma \cup \cdots \cup B_{m-1}\gamma)$ is a Borel set and hence F too is a Borel set.

Since $F_i\Gamma = B_i\Gamma \setminus (B_1\Gamma \cup \cdots \cup B_{i-1}\Gamma)$, we have $(F_1 \cup \cdots \cup F_m)\Gamma = F_1\Gamma \cup \cdots \cup F_m\Gamma = B_1\Gamma \cup \cdots \cup B_m\Gamma$, so $F\Gamma = \bigcup B_i\Gamma \supseteq \bigcup B_i = G$. So G is the union of the translates $F\gamma$ for $\gamma \in G$.

Let $g_1, g_2 \in F$, and suppose that $g_1 = g_2\gamma$ for some $\gamma \in \Gamma$. Since the sets $F_i\Gamma$ are pairwise disjoint, g_1 and g_2 must belong to the same such set, and since they are both in F, they must both be in F_i for some i. But F_i is a subdomain, so $\gamma = e$ is the identity element, and $g_1 = g_2$. Thus all translates of F are disjoint. □

A countable cover $B_1, B_2, \ldots$ of open subdomains is guaranteed to exist if G is second countable. Indeed, given any countable basis $A_1, A_2, \ldots$ of G, we may take our sequence $\{B_m\}$ to consist of only those A_i which are contained in some subdomain relative to Γ (different A_i may be contained in different subdomains). We have thus established:

Corollary 2.12. *Let G be second countable. Then there exists a fundamental domain F relative to Γ.*

Lemma 2.13. *Assume G has a right Haar measure ν and G is second countable. Let E and F be two fundamental domains relative to Γ in G. Then $\nu(E) = \nu(F)$.*

Proof. As stated in the proof of Lemma 2.11, Γ is countable. Then, using countable additivity of measures, we get

$$\begin{aligned} \nu(F) &= \nu\left(\bigcup_{\gamma} E\gamma \cap F\right) = \sum_{\gamma} \nu(E\gamma \cap F) \\ &= \sum_{\gamma} \nu\left((E\gamma \cap F)\gamma^{-1}\right) = \sum_{\gamma} \nu\left(E \cap F\gamma^{-1}\right) \\ &= \nu\left(\bigcup_{\gamma}\left(E \cap F\gamma^{-1}\right)\right) = \nu\left(E \cap \bigcup_{\gamma} F\gamma^{-1}\right) = \nu(E). \qquad \square \end{aligned}$$

One may therefore define the **covolume** of Γ to be the right Haar measure of F, for any fundamental domain F of Γ.[*] Each point x in a fundamental domain F belongs to exactly one orbit $x\Gamma$ in the quotient set $G/\Gamma = \{x\Gamma : x \in G\}$, and for this reason, one often denotes (somewhat improperly) the covolume of Γ by $\nu_G(G/\Gamma)$.

2.4 Lattice point counting

Consider the following general lattice point counting problem. Let G be a topological group that is locally compact, separable and second countable, and let ν be a right Haar measure on G. Let Γ be a lattice in G and let F be a fundamental domain relative to Γ. Given a subset B of G, we ask how many lattice points are contained in B. Assume that this number, $|B \cap \Gamma|$, is finite. Then B can be covered by a finite number of tiles. Let B^+ be the union of all tiles intersecting B, and let B^- be the union of all tiles contained in B. Since each tile contains exactly one lattice point, we get the inequality

$$\frac{\nu(B^-)}{\nu(F)} \leq |B \cap \Gamma| \leq \frac{\nu(B^+)}{\nu(F)},$$

and thus we get the approximation

$$|B \cap \Gamma| \approx \frac{\nu(B)}{\nu(F)},$$

which is valid if the difference $(\nu(B^+) - \nu(B^-))/\nu(F)$ is small.

To be precise, let B_T be a family of subsets of G, parametrized by T, such that $\nu(B_T) < \infty$ for all T and $\nu(B_T^+ \setminus B_T^-)/\nu(B_T) \to 0$ as $T \to \infty$. Then it follows that

$$|B_T \cap \Gamma| \sim \frac{\nu(B_T)}{\nu(F)}. \tag{2.14}$$

[*] Some authors require lattices by definition to have finite covolume.

Asymptotic formulae such as (2.14) are generally the best we can hope for due to the discontinuous nature of the counting function $T \mapsto |B_T \cap \Gamma|$, and one's interest is directed towards the derivation of tight error terms.

It is common practice to **normalize** the Haar measure when working with a lattice of finite covolume: that is, we choose the Haar measure ν_G of G such that $\nu_G(F) = 1$. Noting that the counting measure $\nu_\Gamma(S) := |S|$ is a Haar measure on Γ, we can rewrite the asymptotic formula (2.14) in the beautiful form

$$\nu_\Gamma(B_T \cap \Gamma) \sim \nu_G(B_T \cap G).$$

Example 2.15 (Gauss's circle problem)**.** We ask how many integer points $(l, m) \in \mathbb{Z}^2$ are inside the disc B_T of radius T in $\mathbb{R}^2$. A Haar measure on $G = \mathbb{R}^2$ is the Lebesgue measure. A fundamental domain relative to $\Gamma = \mathbb{Z}^2$ in G is the unit square $F = [0, 1)^2$, with measure 1. The tiles inside B_T, B_T^-, cover the disc of radius $T - \sqrt{2}$, and the tiles intersecting B_T, B_T^+, are contained in the disc of radius $T + \sqrt{2}$. Thus

$$\pi(T - \sqrt{2})^2 \leq |B_T \cap \mathbb{Z}^2| \leq \pi(T + \sqrt{2})^2.$$

Since $(T \pm \sqrt{2})^2 - T^2 = \pm 2\sqrt{2}T + 2 = O(T)$, we get

$$|B_T \cap \mathbb{Z}^2| = \pi T^2 + O(T)$$

as $T \to \infty$.

Remark 2.16. Better error terms for Gauss's circle problem are known — for example $O(T^{2/3})$ which was proved by for example Sierpinski and van der Corput in the early 20th century. Hardy conjectured that the error term is $O(T^{1/2+\varepsilon})$, for any $\varepsilon > 0$ (it is known that $O(T^{1/2})$ is too small). To date, the best known error term is $O(T^{131/208})$ $(131/208 \approx 0.6298\ldots)$, due to Huxley.

The asymptotic formula we obtained for Gauss's circle problem is a special case of the following.

Lemma 2.17. *Let Γ be a fixed n-dimensional lattice in $\mathbb{R}^n$, and let F be a fundamental domain relative to Γ. Let B_T be the (closed) ball of radius T centered at the origin, given any norm on $\mathbb{R}^n$, and let $B = B_1$ be the unit ball. Then the number of lattice points inside B_T is*

$$|B_T \cap \Gamma| = \frac{\operatorname{vol}(B)}{\operatorname{vol}(F)} T^n + O(T^{n-1}).$$

Proof. The Haar measure on $\mathbb{R}^n$ (regarded as a group under vector addition) is the Lebesgue measure, that is, the standard volume. It is easy to show that $\operatorname{vol}(B_T) = T^n \operatorname{vol}(B)$. Since the covolume $\operatorname{vol}(F)$ does not depend on F, we may without loss of generality assume F is the parallelotope[†] spanned by

[†] The n-dimensional generalization of the parallelepiped and parallelogram

some basis for Γ. Let d be the diameter of F (d is finite since F is bounded). Then $B_T^+ \subseteq B_{T+d}$ and $B_{T-d} \subseteq B_T^-$, so the error term in the expression 2.14 is

$$\nu(B_T^+ \setminus B_T^-) \leq \nu(B_{T+d} \setminus B_{T-d}) = \nu(B_{T+d}) - \nu(B_{T-d}) = \\ (\operatorname{vol} B)(T+d)^n - (\operatorname{vol} B)(T-d)^n = O(T^{n-1}). \qquad \square$$

To obtain the asymptotics of the primitive circle problem, and its generalization to n dimensions, one uses Möbius inversion on the formula obtained in Lemma 2.17. We do this in Appendix A.

In this thesis, we are interested in the lattice $\mathrm{SL}_n(\mathbb{Z})$ in $\mathrm{SL}_n(\mathbb{R})$, and the following result will be crucial.

Theorem 2.18 ([DRS], Theorem 10)**.** *Let B_T be the ball of radius T in the space $M_n(\mathbb{R})$ of real $n \times n$-matrices under the Euclidean norm $\|A\| = \sqrt{\operatorname{tr}(A^tA)}$. Let ν be the Haar measure of $\mathrm{SL}_n(\mathbb{R})$, and let F be an arbitrary fundamental domain relative to $\mathrm{SL}_n(\mathbb{Z})$. Then*

$$|B_T \cap \mathrm{SL}_n(\mathbb{Z})| \sim \frac{\nu(B_T \cap \mathrm{SL}_n(\mathbb{R}))}{\nu(F)},$$

and more specifically,

$$|B_T \cap \mathrm{SL}_n(\mathbb{Z})| = C_1 T^{n(n-1)} + O(T^{n(n-1)-1/(n+1)+\varepsilon})$$

for all $\varepsilon > 0$, where

$$C_1 = \frac{1}{\zeta(2)\cdots\zeta(n)} \frac{\pi^{n^2/2}}{\Gamma\left(\frac{n}{2}\right)\Gamma\left(\frac{n(n-1)}{2}+1\right)}.$$

Actually, a slightly more general statement can be made. We can replace the balls B_T in Theorem 2.18 with balls under any norm on $M_n(\mathbb{R})$, and the asymptotics will still hold, save for a slighty increased error term.

Theorem 2.19 ([GN], Corollary 2.3)**.** *Let $\|\cdot\|'$ be any norm on the vector space $M_n(\mathbb{R})$, and let G_T be the ball of radius T in $M_n(\mathbb{R})$ under this norm. Let ν be the Haar measure of $\mathrm{SL}_n(\mathbb{R})$, and let F be an arbitrary fundamental domain relative to $\mathrm{SL}_n(\mathbb{Z})$. Then*

$$|G_T \cap \mathrm{SL}_n(\mathbb{Z})| = \frac{\nu(G_T \cap \mathrm{SL}_n(\mathbb{R}))}{\nu(F)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon})$$

for all $\varepsilon > 0$.

We will be interested in a particular special case of Theorem 2.19. Let $A \in M_{n,k}$. It's easy to check that $\|X\|' := \|A^{-1}X\|$ defines a norm on $M_n(\mathbb{R})$, and that the ball of radius T in $M_n(\mathbb{R})$ under the norm $\|\cdot\|'$ is AB_T.

Corollary 2.20. *Let $A \in M_{n,k}$. Using the notation from Theorem 2.18, it holds that*

$$|AB_T \cap \mathrm{SL}_n(\mathbb{Z})| = \frac{\nu(AB_T \cap \mathrm{SL}_n(\mathbb{R}))}{\nu(F)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon})$$

for all $\varepsilon > 0$.

2.5 Dirichlet convolutions

We review some basic theory on Dirichlet convolutions. A more comprehensive treatment is given in [Apo].

A function $f : \mathbb{N}^* \to \mathbb{C}$ defined on the positive integers $\mathbb{N}^* := \{1, 2, \ldots\}$ is said to be an **arithmetic function**. Given any arithmetic functions f and g, we define their **(Dirichlet) convolution** $f * g$ by

$$(f * g)(k) := \sum_{ab=k} f(a)g(b) = \sum_{d|k} f(d)g\left(\frac{k}{d}\right),$$

where the first sum ranges over all nonnegative integers a and b such that $ab = k$, and the second sum ranges over all positive divisors d of k. It is easy to verify that convolution is an associative and commutative operation, with identity

$$I(k) := \begin{cases} 1, & k = 1, \\ 0, & k > 1. \end{cases}$$

The convolution of multiple functions $f_1, \ldots, f_n$ can be written as

$$(f_1 * \cdots * f_n)(k) = \sum_{d_1 \cdots d_n = k} f_1(d_1) \cdots f_n(d_n).$$

If f is an arithmetic function with $f(1) \neq 0$, there exists a unique **Dirichlet inverse** f^{*-1} of f which satisfies $f * f^{*-1} = f^{*-1} * f = I$. This inverse can be calculated by recursively solving for $f^{*-1}(k)$ in the equations

$$\begin{aligned} 1 &= f(1)f^{*-1}(1), \\ 0 &= f^{*-1}(k)f(1) + \cdots + f^{*-1}(1)f(k), \end{aligned}$$

for increasing k.

An arithmetic function f is **multiplicative** if f is not identically zero and $f(ab) = f(a)f(b)$ for all coprime integers a and b.[‡] A multiplicative function always satisfies $f(1) = 1$, and consequently has a Dirichlet inverse.

The proof of the following assertions may be found in [Apo].

[‡] Note that this differs from the concept of a **completely multiplicative** function, which is an arithmetic function f such that $f(ab) = f(a)f(b)$ for all a and b.

Lemma 2.21 ([Apo]). *Let f and g be multiplicative functions. Then $f \cdot g$ and $f * g$ are multiplicative. If f has a Dirichlet inverse f^{*-1}, then f^{*-1} is multiplicative.*

An important example of a multiplicative function is the **Möbius function** μ, defined by $\mu(k) := (-1)^m$ if k is a product of m distinct prime factors (that is, k is **square-free**), and $\mu(k) := 0$ otherwise. Let 1 denote the function that is identically 1 (that is, $1(k) = 1$ for all k). The functions 1 and μ are each other's Dirichlet inverses: $1 * \mu = I$. This yields in particular (for $s > 1$)

$$\sum_{m=1}^{\infty} \frac{1}{m^s} \sum_{k=1}^{\infty} \frac{\mu(k)}{k^s} = \sum_{i=1}^{\infty} \frac{(1 * \mu)(i)}{i^s} = 1,$$

so

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^s} = \frac{1}{\zeta(s)}. \tag{2.22}$$

If F and G are arithmetic functions, and α is an arithmetic function with a Dirichlet inverse α^{*-1}, then $F = \alpha * G$ is equivalent to $\alpha^{*-1} * F = G$. Written differently: if

$$F(x) = \sum_{m|x} \alpha(m) G(x/m),$$

then

$$G(x) = \sum_{m|x} \alpha^{*-1}(m) F(x/m).$$

Similar sums often arise in number theory, where F and G are not necessarily arithmetic functions, but there exists a generalization of Dirichlet inversion in this case:

Lemma 2.23 (Generalized inversion formula [Apo]). *Let F and G be complex valued functions defined on $(0, \infty)$ which are 0 on $(0, 1)$. If α is an arithmetic function with a Dirichlet inverse α^{*-1}, and*

$$F(x) = \sum_{m \leq x} \alpha(m) G(x/m),$$

then

$$G(x) = \sum_{m \leq x} \alpha^{*-1}(m) F(x/m)$$

for all $x \in (0, \infty)$.

Chapter 3

Number of matrices with primitive rows

In the present chapter, we will derive the asymptotics of $N'_{n,k}(T)$. Since $M'_{n,k}$ is not a group, a direct application of the lattice point counting method does not work. However, as we will show, $M'_{n,k}$ can be decomposed into a finite disjoint union of sets $A\,\mathrm{SL}_n(\mathbb{Z})$ with $A \in M'_{n,k}$, and the number of lattice points in each of these is a multiple of the number of lattice points in the same ball in $\mathrm{SL}_n(\mathbb{Z})$, which is a lattice in $\mathrm{SL}_n(\mathbb{R})$. Counting the lattice points in each such set, and summing, gives us the counting function for $N'_{n,k}(T)$.

Lemma 3.1. *The greatest common divisor of each row in an integer $n \times n$-matrix A is preserved under multiplication on the right by any matrix $X \in \mathrm{SL}_n(\mathbb{Z})$.*

Proof. If y is a row vector of AX, then $y = rX$ for a row vector r of A. If λ divides each element in r, then λ divides each element in y. Conversely, if λ divides each element in y, then λ divides each element in $r = yX^{-1}$, since yX^{-1} is an integer vector (recall that $X^{-1} \in \mathrm{SL}_n(\mathbb{Z})$, and so is an integer matrix). Thus r and y have the same divisors. □

In particular, if each row of A is primitive, then each row of AX is primitive, for any $X \in \mathrm{SL}_n(\mathbb{Z})$. So we get:

Corollary 3.2. *If $A \in M'_{n,k}$ then $AX \in M'_{n,k}$ for all $X \in \mathrm{SL}_n(\mathbb{Z})$. Thus $A\,\mathrm{SL}_n(\mathbb{Z}) \subseteq M'_{n,k}$.*

Consequently $M'_{n,k}$ may be written as a union of orbits of $\mathrm{SL}_n(\mathbb{Z})$:

$$M'_{n,k} = \bigcup_{A \in \mathcal{A}} A\,\mathrm{SL}_n(\mathbb{Z}),$$

for properly chosen subsets $\mathcal{A}$ of $M'_{n,k}$ (one may for example take $\mathcal{A} = M'_{n,k}$). In fact, as we will show in the following, the number of orbits is finite, and so we may take $\mathcal{A}$ to be finite.

Definition 3.3. An integer $n \times n$-matrix is said to be in **Hermite normal form** if it is lower triangular, each diagonal entry is strictly positive and is the strictly largest entry on each row, and all other entries are at nonnegative.

In other words,

$$C := \begin{pmatrix} c_{11} & & & \\ c_{21} & c_{22} & & \\ & & \ddots & \\ c_{n1} & \cdots & c_{n(n-1)} & c_{nn} \end{pmatrix}$$

is in Hermite normal form if and only if $0 \leq c_{ij} < c_{ii}$ for all $j < i$ (we require $0 < c_{11}$).

Lemma 3.4. *Assume $k > 0$. Given an arbitrary matrix $A \in M_{n,k}$, the orbit $A\,\mathrm{SL}_n(\mathbb{Z})$ contains a unique matrix C in Hermite normal form.*

Proof of existence. By multiplying A on the right by elementary matrices in $\mathrm{SL}_n(\mathbb{Z})$ we may add an integer multiple of any column to any other. We will show that a sequence of such column additions produces a matrix in Hermite normal form.

Suppose by induction that we have "completed" the first $(m-1)$ rows: that is to say, for all rows up to the $(m-1)$th, the diagonal entry is strictly positive, the entries to the left of it are strictly smaller but at least zero, and the entries to the right of it are all zero. Allowing $m = 1$ gives us a trivial base case.

We will now complete the mth row. Adding a multiple of column $i \geq m$ to any other column $j \neq i$ leaves the first $(m-1)$ rows unchanged, and adds a multiple of the ith entry to entry j on the mth row. Let us now only consider the mth row. Some entry $i \geq m$ is nonzero (or the matrix would be singular). If it is negative we may add a sufficiently large multiple (negative or positive) of it to another entry $j \geq m$ such that entry j is positive (there must be some other such entry since otherwise we would have $i = m = n$, and we would have a lower triangular matrix with a negative determinant). We may now add a sufficiently large multiple of entry j to all other entries on the row to make sure that all entries on the row are at least 0.

We perform Euclid's algorithm on entries m to n: that is, iteratively subtract the smallest nonzero entry from all other entries until only one nonzero (positive) entry remains. We may move this entry to the diagonal position (the mth entry), if it is not already there, by first adding it to the diagonal position and then subtracting it from its original position.

Finally, we iteratively subtract the diagonal entry from each entry to the left of it until the diagonal entry is the (strictly) largest on the row. This completes the row, and continuing the induction up to $m = n$ finishes the proof. □

Proof of uniqueness. Assume that the orbit $A\,\mathrm{SL}_n(\mathbb{Z})$ contains two such lower triangular matrices C, C'. Then $C = XC'$ for some $X \in \mathrm{SL}_n(\mathbb{Z})$.

$$\begin{pmatrix} c_{11} & & \\ c_{21} & c_{22} & \\ & & \ddots \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} & \\ x_{21} & x_{22} & \\ & & \ddots \end{pmatrix} = \begin{pmatrix} c'_{11} & & \\ c'_{21} & c'_{22} & \\ & & \ddots \end{pmatrix}.$$

We have $(c_{11}, 0, \ldots) \cdot (x_{11}, x_{21}, \cdots) = c'_{11}$, so $x_{11} = c'_{11}/c_{11}$. Therefore c_{11} divides c'_{11}. By symmetry it must also hold that c'_{11} divides c_{11}. Since they are both positive, we must have $c_{11} = c'_{11}$ and hence $x_{11} = 1$. Since $(c_{11}, 0, \ldots) \cdot (x_{1j}, x_{2j}, \ldots) = 0$ for all $j > 1$, we must have $x_{1j} = 0$ for all $j > 1$.

$$\begin{pmatrix} c_{11} & & \\ c_{21} & c_{22} & \\ & & \ddots \end{pmatrix} \begin{pmatrix} 1 & 0 & \cdots \\ x_{21} & x_{22} & \\ & & \ddots \end{pmatrix} = \begin{pmatrix} c_{11} & & \\ c'_{21} & c'_{22} & \\ & & \ddots \end{pmatrix}.$$

We have $(c_{21}, c_{22}, 0, \ldots) \cdot (0, x_{22}, \ldots) = c'_{22}$, so $x_{22} = c'_{22}/c_{22}$, and by the same argument as above we get $c_{22} = c'_{22}$ and $x_{22} = 1$. Similarly, we also get $x_{2j} = 0$ for all $j > 2$. Since $(c_{21}, c_{22}, 0, \ldots) \cdot (1, x_{21}, \ldots) = c'_{21}$ we get $c'_{21} = c_{21} + x_{21}c_{22}$, so c_{21} and c'_{21} differ by a multiple of c_{22}. We must have $x_{21} = 0$, or else c'_{21} falls outside the range $0 \leq c'_{21} < c_{22}$.

$$\begin{pmatrix} c_{11} & & \\ c_{21} & c_{22} & \\ & & \ddots \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ & & \ddots & \end{pmatrix} = \begin{pmatrix} c_{11} & & \\ c_{21} & c_{22} & \\ & & \ddots \end{pmatrix}.$$

Continuing like this shows that $C = C'$ (and $X = I$), as desired. □

Let M be either of $M_{n,k}$ or $M'_{n,k}$. We let $\mathrm{SL}_n(\mathbb{Z})$ act on M by right multiplication. The **quotient set** $M/\mathrm{SL}_n(\mathbb{Z})$ is defined as the set of orbits $A\,\mathrm{SL}_n(\mathbb{Z})$ for $A \in M$. If $|M/\mathrm{SL}_n(\mathbb{Z})| =: m$ is finite, we may choose one representative matrix A_i from each orbit, and write M as a finite disjoint union of the orbits of A_i:

$$M = \bigcup_{i=1}^{m} A_i\,\mathrm{SL}_n(\mathbb{Z}).$$

Proposition 3.5. *Let $k > 0$. Then*

$$|M_{n,k}/\mathrm{SL}_n(\mathbb{Z})| = \sum_{d_1 \cdots d_n = k} d_1^0 d_2^1 \cdots d_n^{n-1},$$

where the sum ranges over all positive integer tuples $(d_1, \ldots, d_n)$ such that $d_1 \cdots d_n = k$.

Proof. By Lemma 3.4, we need only count the number of matrices in Hermite normal form with determinant $k > 0$. First we choose the diagonal entries $d_1, \ldots, d_n$ such that $d_1 \cdots d_n = k$. For each row, there are precisely d_i^{i-1} ways to choose the remaining $i-1$ row elements such that they are all nonnegative and less than d_i. □

Since $M'_{n,k}$ is a subset of $M_{n,k}$, we know that $M'_{n,k}$ can be covered by the orbits in $M_{n,k}/\operatorname{SL}_n(\mathbb{Z})$, and hence that $|M'_{n,k}/\operatorname{SL}_n(\mathbb{Z})|$ is finite. We would like to calculate this number. This is done using inclusion/exclusion.

Proposition 3.6. *Let $k > 0$. Then*

$$|M'_{n,k}/\operatorname{SL}_n(\mathbb{Z})| = \sum_{d_1 \cdots d_n = k} \prod_{i=1}^{n} \sum_{g | d_i} \mu(g) \left(\frac{d_i}{g}\right)^{i-1}$$

where the first sum ranges over all positive integer tuples $(d_1, \ldots, d_n)$ such that $d_1 \cdots d_n = k$.

(Note that $d_1 = 1$ in all nonzero terms above.)

Proof. We want to count exactly those matrices in Hermite normal form which are in $M'_{n,k}$, that is, $n \times n$-matrices in Hermite normal form with determinant k and all rows primitive. The number of such matrices is

$$\left|M'_{n,k}/\operatorname{SL}_n(\mathbb{Z})\right| = \sum_{d_1 \cdots d_n = k} \prod_{i=1}^{n} v_i(d_i),$$

where $v_i(d)$ is the number of primitive vectors $(x_1, \ldots, x_{i-1}, d)$ with $0 \leq x_1, \ldots, x_{i-1} < d$.

There is a bijective correspondence between the vectors $(x_1, \ldots, x_{i-1}, d)$ and the vectors $y = (y_1, \ldots, y_{i-1})$ such that $1 \leq y_1, \ldots, y_{i-1} \leq d$ and $\gcd(y)$ is coprime to d. Let $d = p_1^{a_1} \cdots p_j^{a_j}$ be the prime factorization of d. The number of vectors y which are divisible by some set of primes $P \subseteq \{p_1, \ldots, p_j\}$ is

$$\left(\frac{d}{\prod P}\right)^{i-1},$$

so by the principle of inclusion/exclusion (see, for instance, Stanley [Sta]), we have

$$\begin{aligned} v_i(d) &= \sum_{P \subseteq \{p_1, \ldots, p_j\}} (-1)^{|P|} \left(\frac{d}{\prod P}\right)^{i-1} \\ &= \sum_{g | p_1 \cdots p_j} (-1)^{\#\text{ prime factors of } g} \left(\frac{d}{g}\right)^{i-1} \\ &= \sum_{g | p_1 \cdots p_j} \mu(g) \left(\frac{d}{g}\right)^{i-1} = \sum_{g | d} \mu(g) \left(\frac{d}{g}\right)^{i-1}. \end{aligned}$$

□

We are now ready to derive the asymptotics of $N'_{n,k}(T)$.

From the heuristic

$$|B_T \cap \Gamma| \sim \frac{\nu(B_T)}{\nu(F)},$$

we expect that changing the shape of the ball B_T should change the asymptotics by a constant factor corresponding to the volume change in B_T. Thus, we expect $|AB_T \cap \mathrm{SL}_n(\mathbb{Z})| \sim c|B_T \cap \mathrm{SL}_n(\mathbb{Z})|$ for some constant c for all $A \in M_{n,k}$.

Lemma 3.7. *Given any nonsingular matrix $A \in M_{n,k}$, we have as $T \to \infty$ that*

$$|B_T \cap A\,\mathrm{SL}_n(\mathbb{Z})| = \frac{1}{(\det A)^{n-1}}|B_T \cap \mathrm{SL}_n(\mathbb{Z})| + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon}),$$

for all $\varepsilon > 0$.

Proof. In the following, $f(T) \sim g(T)$ will be shorthand for the statement that

$$f(T) = g(T) + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon})$$

for all $\varepsilon > 0$. We will be using Theorem 2.18 and Corollary 2.20 multiple times. For convenience we will normalize the Haar measure ν on $\mathrm{SL}_n(\mathbb{R})$ such that $\nu(F) = 1$, where F is the fundamental domain relative to $\mathrm{SL}_n(\mathbb{Z})$. We also use the bi-invariance of ν (Lemma 2.7) and the fact that $A/k^{1/n} \in \mathrm{SL}_n(\mathbb{R})$. The assertion in the lemma then follows from the calculation

$$\begin{gathered}
|B_T \cap A\,\mathrm{SL}_n(\mathbb{Z})| = \left|A(A^{-1}B_T \cap \mathrm{SL}_n(\mathbb{Z}))\right| = \\
\left|A^{-1}B_T \cap \mathrm{SL}_n(\mathbb{Z})\right| \sim \nu\left(A^{-1}B_T \cap \mathrm{SL}_n(\mathbb{R})\right) = \\
\nu\left(\frac{A}{k^{1/n}}\left(A^{-1}B_T \cap \mathrm{SL}_n(\mathbb{R})\right)\right) = \nu\left(k^{-1/n}B_T \cap \frac{A}{k^{1/n}}\,\mathrm{SL}_n(\mathbb{R})\right) = \\
\nu\left(B_{T/k^{1/n}} \cap \mathrm{SL}_n(\mathbb{R})\right) \sim |B_{T/k^{1/n}} \cap \mathrm{SL}_n(\mathbb{R})| \sim \\
C_1\frac{T^{n(n-1)}}{k^{n-1}} \sim \frac{1}{k^{n-1}}|B_T \cap \mathrm{SL}_n(\mathbb{Z})|.
\end{gathered}$$

□

Proposition 3.8. *Let M be a set which can be written as a finite disjoint union $\bigcup_{i=1}^m A_i\,\mathrm{SL}_n(\mathbb{Z})$, where $\det A_i = k$ for each i. Then as $T \to \infty$,*

$$|B_T \cap M| = |M/\,\mathrm{SL}_n(\mathbb{Z})|\frac{C_1}{k^{n-1}}T^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon})$$

for all $\varepsilon > 0$.

Proof. Let $m := |M/\,\mathrm{SL}_n(\mathbb{Z})|$. Again, we will use $f(T) \sim g(T)$ as a shorthand for the statement that

$$f(T) = g(T) + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon})$$

for all $\varepsilon > 0$. Then by Lemma 3.7,

$$|B_T \cap M| = \left| B_T \cap \bigcup_{i=1}^{m} A_i \operatorname{SL}_n(\mathbb{Z}) \right| =$$
$$\sum_{i=1}^{m} |B_T \cap A_i \operatorname{SL}_n(\mathbb{Z})| \sim \sum_{i=1}^{m} \frac{1}{k^{n-1}} |B_T \cap \operatorname{SL}_n(\mathbb{Z})| =$$
$$m \frac{1}{k^{n-1}} N_{n,1}(T) \sim m \frac{C_1}{k^{n-1}} T^{n(n-1)}. \qquad \square$$

Finally, we apply the above proposition to our special case, and we have proved Theorem 1.1, which we state again here.

For all $n \geq 2$ and $k > 0$ we have as $T \to \infty$ that

$$\begin{aligned} N_{n,k}(T) &= c_{n,k} T^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon}) \\ N'_{n,k}(T) &= c'_{n,k} T^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon}) \end{aligned}$$

for all $\varepsilon > 0$, for the constants

$$\begin{aligned} c_{n,k} &:= \frac{C_1}{k^{n-1}} \sum_{d_1 \cdots d_n = k} d_1^0 d_2^1 \cdots d_n^{n-1} \\ c'_{n,k} &:= \frac{C_1}{k^{n-1}} \sum_{d_1 \cdots d_n = k} \prod_{i=1}^{n} \sum_{g | d_i} \mu(g) \left(\frac{d_i}{g} \right)^{i-1}, \end{aligned}$$

where the sum $\sum_{d_1 \cdots d_n = k}$ ranges over all integer tuples $(d_1, \ldots, d_n)$ such that $d_1 \cdots d_n = k$, and C_1 is the constant from Theorem 2.18.

3.1 Another approach

We will demonstrate another method of deriving $N'_{n,k}(T)$, using Dirichlet inversion.

Throughout this section, $f(T) \sim g(T)$ will be shorthand for the statement that

$$f(T) = g(T) + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon})$$

for all $\varepsilon > 0$ as $T \to \infty$.

Let $M'_{n,k,(d_1,\ldots,d_n)}$ be the set of integer $n \times n$-matrices $A = (r_1, \ldots, r_n)^t$ with nonzero determinant $k \in \mathbb{Z}$, such that $\gcd(r_i) = d_i$, and let

$$N'_{n,k,(d_1,\ldots,d_n)}(T) := |B_T \cap M'_{n,k,(d_1,\ldots,d_n)}|.$$

We are interested in estimating the number of matrices with primitive rows, $N'_{n,k}(T) = N'_{n,k,(1,\ldots,1)}(T)$.

Given $A \in M'_{n,k,(d_1,\dots,d_n)}$, denote by $r_1, \dots, r_n$ its rows, and and let $r'_i := r_i/d_i$ as well as $A' := (r'_1, \dots, r'_n)^t$. Then A' has primitive rows and

$$k = \det A = (d_1 \cdots d_n) \det A',$$

so $d_1 \cdots d_n$ divides k, and $\det A' = k/(d_1 \cdots d_n)$.

Let D be the diagonal matrix with diagonal entries $d_1, \dots, d_n$. Then $A = DA'$, so

$$M'_{n,k,(d_1,\dots,d_n)} = DM'_{n,\frac{k}{d_1 \cdots d_n}}.$$

Therefore by Lemma 3.7 we get

$$N'_{n,k,(d_1,\dots,d_n)}(T) = |B_T \cap M_{n,k,(d_1,\dots,d_n)}| =$$
$$|B_T \cap DM'_{n,\frac{k}{d_1 \cdots d_n}}| \sim \frac{1}{(d_1 \cdots d_n)^{n-1}} |B_T \cap M'_{n,\frac{k}{d_1 \cdots d_n}}| =$$
$$\frac{1}{(d_1 \cdots d_n)^{n-1}} N'_{n,\frac{k}{d_1 \cdots d_n}}(T).$$

We have

$$N_{n,k}(T) = \sum_{d_1 \cdots d_n | k} N'_{n,k,(d_1,\dots,d_n)}(T) \sim$$
$$\sum_{d_1 \cdots d_n | k} \frac{1}{(d_1 \cdots d_n)^{n-1}} N'_{n,\frac{k}{d_1 \cdots d_n}}(T) =$$
$$\sum_{d|k} \tau_n(d) \frac{1}{d^{n-1}} N'_{n,k/d}(T) = \sum_{d|k} \underbrace{\frac{\tau_n(d)}{d^{n-1}}}_{f_n(d)} N'_{n,k/d}(T),$$

where $\tau_n(d) := \sum_{d_1 \cdots d_n = d} 1$ is the number of ways to write d as a product of n positive integers.

It is easy to verify that f_n as defined above is a multiplicative function (but not completely multiplicative[*]). Moreover, since $f_n(1) \neq 0$, it has a Dirichlet inverse f_n^{*-1}. Applying the generalized Dirichlet inversion formula 2.23, we get

$$N'_{n,k}(T) \sim \sum_{d|k} f_n^{*-1}(d) N_{n,k/d}(T).$$

(We do not need to worry about increasing the error term, because we are only summing a finite number of terms.) Recall that (by Theorem 2.18)

$$N_{n,k}(T) \sim C_1 g_n(k) T^{n(n-1)},$$

where

$$g_n(k) := \frac{1}{k^{n-1}} \sum_{d_1 \cdots d_n = k} d_1^0 \cdots d_n^{n-1}.$$

[*] $f_2(4) \neq f_2(2) f_2(2)$

We observe that g_n is a multiplicative function (but not completely multiplicative[†]). We get

$$N'_{n,k}(T) \sim C_1 T^{n(n-1)} \sum_{d|k} f_n^{*-1}(d) g_n(k/d).$$

The coefficients $C_1(f_n^{*-1} * g_n)(k)$ of the main term are rather unwieldy, but they can in principle be calculated. For square-free numbers, we may obtain a simple expression as follows.

Since g_n is multiplicative and f_n^{*-1} is multiplicative (because f_n is), we have, if k is square-free, that

$$\sum_{d|k} f_n^{*-1}(d) g_n(k/d) = \prod_{p|k} (f_n^{*-1}(p) + g_n(p)),$$

where the product ranges over primes (the identity can be verified by expanding out the product on the right side).

We calculate $f_n^{*-1}(p)$ and $g_n(p)$ for primes p. We have

$$g_n(p) = \sum_{d_1 \cdots d_n = p} \frac{p}{d_1 \cdots d_n^n} = p \sum_{i=1}^{n} \frac{1}{p^i} = 1 + \frac{1}{p} + \cdots + \frac{1}{p^{n-1}} = \frac{1-p^{-n}}{1-p^{-1}}$$

and

$$0 = \sum_{ab=p} f_n^{*-1}(a) f_n(b) = f_n^{*-1}(p) f_n(1) + f_n^{*-1}(1) f(p),$$

so $f_n^{*-1}(p) = -f_n(p) = -d_n(p)/p^{n-1} = -n/p^{n-1}$.

We have thus established, for k a square-free number,

$$\begin{aligned} N'_{n,k}(T) &\sim C_1 T^{n(n-1)} \prod_{p|k} \left(\frac{1-p^{-n}}{1-p^{-1}} - \frac{n}{p^{n-1}} \right) \\ &= \frac{C_1}{k^{n-1}} T^{n(n-1)} \prod_{p|k} \left(\frac{p^n - 1}{p-1} - n \right). \end{aligned}$$

[†] $g_3(4) \neq g_3(2) g_3(2)$

Chapter 4

Density of matrices with primitive rows

Wigman [Wig] showed that the density of matrices with primitive rows in $M_{n,k}$ for $k = 0$ is (provided that $n \geq 3$)

$$D_n(0) = \lim_{T \to \infty} \frac{N'_{n,0}(T)}{N_{n,0}(T)} = \frac{c'_{n,0}}{c_{n,0}} = \frac{1}{\zeta(n-1)^n}.$$

This is what we would intuitively expect, as all rows in a singular $n \times n$-matrix belong to a single $(n-1)$-dimensional subspace of $\mathbb{R}^n$, and the density of primitive vectors in $\mathbb{R}^{n-1}$ is $1/\zeta(n-1)$ (see Appendix A). We note also that this density converges to 1 as $n \to \infty$: that is, almost all matrices in $M_{n,k}$ have primitive rows for large n, which makes intuitive sense because for large n, almost all vectors in $\mathbb{Z}^n$ are primitive.

We would like to calculate the density of matrices with primitive rows in $M_{n,k}$ for $k \neq 0$,

$$D_n(k) = \lim_{T \to \infty} \frac{N'_{n,k}(T)}{N_{n,k}(T)} = \frac{c'_{n,k}}{c_{n,k}} = \frac{|M'_{n,k}/\operatorname{SL}_n(\mathbb{Z})|}{|M_{n,k}/\operatorname{SL}_n(\mathbb{Z})|}.$$

We cannot hope for the density $D_n(k)$ to be equal to the density $D_n(0)$: in particular, the former is always rational, whereas the latter is transcendental for all odd n. However, we will discover perhaps somewhat surprisingly that $D_n(k_i) \to D_n(0)$ as $i \to \infty$ if $(k_1, k_2, \ldots)$ is totally divisible.

We prove theorems 1.4, 1.5, 1.6 and 1.8 in section 4.2. We begin here by calculating $D_n(k)$ in a few simple cases.

The case $k = \pm 1$. When the determinant of a matrix is ± 1, all its rows are primitive (Lemma 3.1), so $M_{n,k} = M'_{n,k}$ and thus $D_n(\pm 1) = 1$.

The case $k = p$. Let $k = p$ be a prime. Then

$$|M_{n,k}/\operatorname{SL}_n(\mathbb{Z})| = \sum_{i=1}^{n} p^{i-1} = \frac{p^n - 1}{p - 1}$$

and

$$|M'_{n,k}/\operatorname{SL}_n(\mathbb{Z})| = \sum_{i=1}^{n}(\mu(1)p^{i-1} + \mu(p)) = \sum_{i=1}^{n}(p^{i-1} - 1) = \frac{p^n - 1}{p - 1} - n,$$

so

$$D_n(p) = 1 - n\frac{p-1}{p^n - 1}.$$

We see that this density converges to 1 if either $n \to \infty$ or $k = p \to \infty$.

The case $k = p_1 \cdots p_j$. Let k be a square-free number. It can be shown that $c_{n,k}$ and $c'_{n,k}$ are multiplicative[*] (we will show this in the next section) as functions of k, so

$$D_n(k) = \frac{c'_{n,k}}{c_{n,k}} = \prod_{p|k}\left(1 - n\frac{p-1}{p^n - 1}\right),$$

which converges to 1 if either $n \to \infty$ or $\min(p_1, \ldots, p_j) \to \infty$.

4.1 Convolutions

We will use the notation of this section throughout the rest of the chapter.

Set

$$\begin{aligned} a_n(k) &:= |M_{n,k}/\operatorname{SL}_n(\mathbb{Z})| = \sum_{d_1 \cdots d_n = k} d_1^0 \cdots d_n^{n-1}, \\ a'_n(k) &:= |M'_{n,k}/\operatorname{SL}_n(\mathbb{Z})| = \sum_{d_1 \cdots d_n = k} \prod_{i=1}^{n} \sum_{g|d_i} \mu(g)\left(\frac{d_i}{g}\right)^{i-1}. \end{aligned}$$

Then $D_n(k) = c'_{n,k}/c_{n,k} = a'_n(k)/a_n(k)$ for $k > 0$. We may write

$$a_n = (\cdot)^{n-1} * \cdots * (\cdot)^0,$$

where $(\cdot)^i : x \mapsto x^i$.

Similarly, since

$$\sum_{g|d_i} \mu(g)\left(\frac{d_i}{g}\right)^{i-1} = \left(\mu * (\cdot)^{i-1}\right)(d_i),$$

[*] But not completely multiplicative!

we have

$$a_n' = \sum_{d_1\cdots d_n=k}\prod_{i=1}^{n}(\mu * (\cdot)^{i-1}) = (\mu * (\cdot)^{n-1}) * \cdots * (\mu * (\cdot)^0),$$

so by the commutativity and associativity of the Dirichlet convolution we have

$$a_n' = \mu * (\cdot)^{n-1} * \cdots * \mu * (\cdot)^0 = \mu^{*n} * a_n,$$

where $\mu^{*n} := \mu * \cdots * \mu$ denotes the convolution of μ with itself n times (so that $\mu^{*1} = \mu$). Since the Dirichlet inverse of μ is the function 1, and since

$$1^{*n}(k) = \prod_{d_1\cdots d_n=k} 1 =: \tau_n(k)$$

is the number of ways to write k as a product of n positive integers (order matters), we have also

$$a_n = 1^{*n} * a_n' = \tau_n * a_n.$$

Since $(\cdot)^i$ and μ are multiplicative functions, so are a_n, a_n' and $D_n = a_n'/a_n$. We state this in a proposition.

Proposition 4.1. *The functions $D_n = a_n'/a_n$, a_n and a_n' are multiplicative and the following relations hold:*

$$a_n' = \mu^{*n} * a_n,$$
$$a_n = \tau_n * a_n'.$$

4.2 Asymptotics

In this section we derive the asymptotics of $D_n(k)$ and prove theorems 1.4, 1.5, 1.6 and 1.8. The proof of the converse of Theorem 1.6 in the case $n = 3$ is given in Appendix C.

Since D_n, a_n, and a_n' are multiplicative we need only understand their behavior for prime powers $k = p^m$.

The following formula (which could also be derived directly from the identity $a_n' = \mu^{*n} * a_n$, but we will benefit from the inclusion/exclusion interpretation of the present proof) gives us a convenient formula for calculating values of $a_n'(k)$.

Lemma 4.2. *The functions a_n' and a_n are connected via the identity*

$$a_n'(p^m) = \sum_{i=0}^{m}(-1)^i \binom{n}{i} a_n(p^{m-i})$$

for primes p and $m \geq 0$.

Proof. $a_n(p^m)$ counts the number of $n \times n$-matrices in Hermite normal form with determinant p^m, whereas $a'_n(p^m)$ counts the number of such with primitive rows. If A is a matrix that $a_n(p^m)$ counts which $a'_n(p^m)$ does not, then some set of rows, indexed by $S \subseteq [n] := \{1, \ldots, n\}$ (where $|S| \leq m$), are divisible by p. The number of such matrices is $a_n(p^{m-|S|})$, and thus by the inclusion/exclusion principle,

$$a'_n(p^m) = \sum_{\substack{S \subseteq [n] \\ |S| \leq m}} (-1)^{|S|} a_n(p^{m-|S|}) = \sum_{i=0}^{m} (-1)^i \binom{n}{i} a_n(p^{m-i}). \qquad \square$$

Lemma 4.3. *For any prime p and for all $m \geq 0$,*

$$(p^m)^{n-1} \leq a_n(p^m) \leq (m+1)^n (p^m)^{n-1}.$$

Proof. We have

$$a_n(p^m) = \sum_{d_1 \cdots d_n = p^m} d_1^0 \cdots d_n^{n-1}.$$

The largest value that $d_1^0 \cdots d_n^{n-1}$ attains is $(p^m)^{n-1}$, when $d_1 = \cdots = d_{n-1} = 1$ and $d_n = p^m$. The number of terms in the sum is $\sum_{d_1 \cdots d_n = p^m} 1 \leq (m+1)^n$, since each d_i takes on one of the $(m+1)$ values $1, p, \ldots, p^m$. Thus it follows that

$$(p^m)^{n-1} \leq \sum_{d_1 \cdots d_n = p^m} d_1^0 \cdots d_n^{n-1} \leq (m+1)^n (p^m)^{n-1}. \qquad \square$$

Lemma 4.4. *For any prime p and $m \geq 1$,*

$$a_n(p^m) = p^{n-1} a_n(p^{m-1}) + a_{n-1}(p^m),$$

or written differently:

$$a_n(p^{m-1}) = \frac{a_n(p^m) - a_{n-1}(p^m)}{p^{n-1}}.$$

Proof. We split the sum

$$a_n(p^m) = \sum_{d_1 \cdots d_n = p^m} d_1^0 \cdots d_n^{n-1}$$

into two parts, one part where d_n is divisible by p, and another part where it is not (so that $d_n = 1$). The terms corresponding to $d_n = 1$ sum to $a_{n-1}(p^m)$. Where d_n is divisible by p, we can write $d_n =: pe_n$ for some e_n. Let $e_i := d_i$ for all $i < n$. Thus,

$$\sum_{\substack{d_1 \cdots d_n = p^m \\ p | d_n}} d_1^0 \cdots d_n^{n-1} = \sum_{e_1 \cdots e_n = p^{m-1}} e_1^0 \cdots (e_n/p)^{n-1} = \frac{1}{p^{n-1}} a_n(p^{m-1}).$$

Adding the two parts gives us $a_n(p^m) = p^{n-1} a_n(p^{m-1}) + a_{n-1}(p^m)$. $\square$

Lemma 4.5. *Let n and p be fixed, where $n \geq 3$ and p is a prime. Then, as $m \to \infty$,*

$$a_n(p^{m-i}) = \frac{1}{(p^{n-1})^i} a_n(p^m) + O((p^m)^{n-2}(m+1)^{n-1})$$

for $1 \leq i \leq n$.

Proof. This follows from repeated application (at most n times) of the following formula, which we get by using the expression for $a_n(p^{m-1})$ in Lemma 4.4 and using the bounds in Lemma 4.3:

$$\begin{aligned} a_n(p^{m-1}) &= \frac{1}{p^{n-1}}(a_n(p^m) - a_{n-1}(p^m)) \\ &= \frac{1}{p^{n-1}} a_n(p^m) + O((p^m)^{n-2}(m+1)^{n-1}). \end{aligned}$$ □

Lemma 4.6. *Let n and p be fixed, where $n \geq 3$ and p is a prime. Then*

$$D_n(p^m) \to \left(1 - \frac{1}{p^{n-1}}\right)^n$$

as $m \to \infty$.

Proof. We may assume m to be larger than n. The sum in Lemma 4.2 then extends up to $i = n$ (because the terms $\binom{n}{i}$ vanish for larger i), so

$$a'_n(p^m) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_n(p^{m-i}).$$

Combining this with the asymptotics of Lemma 4.5, we get

$$a'_n(p^m) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} \frac{1}{(p^{n-1})^i} a_n(p^m) + O((p^m)^{n-2}(m+1)^{n-1}).$$

We divide by $a_n(p^m)$ on both sides and use the fact that $a_n(p^m) \geq p^m$, so that

$$\begin{aligned} D_n(p^m) &= \sum_{i=0}^{n} (-1)^i \binom{n}{i} \frac{1}{(p^{n-1})^i} + O\left(\frac{(p^m)^{n-2}(m+1)^{n-1}}{(p^m)^{n-1}}\right) \\ &= \sum_{i=0}^{n} \binom{n}{i} \left(\frac{-1}{p^{n-1}}\right)^i + O\left(\frac{(m+1)^{n-1}}{p^m}\right) \\ &= \left(1 - \frac{1}{p^{n-1}}\right)^n + O\left(\frac{(m+1)^{n-1}}{p^m}\right). \end{aligned}$$

As $m \to \infty$, the second term on the right vanishes. □

Lemma 4.7. *For any prime p and for all $m \geq 0$,*

$$1 - \frac{n}{p^{n-1}} \leq D_n(p^m).$$

Proof. By the inclusion/exclusion principle, the first two terms of

$$a'_n(p^m) = \sum_{i=0}^{m} (-1)^i \binom{n}{i} a_n(p^{m-i}),$$

exceed $a'_n(p^m)$, that is,

$$a'_n(p^m) \geq a_n(p^m) - n a_n(p^{m-1}).$$

Applying Lemma 4.4, we get

$$\begin{aligned} a'_n(p^m) &\geq a_n(p^m) - n a_n(p^{m-1}) \\ &= a_n(p^m) - \frac{n}{p^{n-1}}(a_n(p^m) - a_{n-1}(p^m)) \\ &\geq a_n(p^m)\left(1 - \frac{n}{p^{n-1}}\right) + \frac{n}{p^{n-1}} a_{n-1}(p^m) \\ &\geq a_n(p^m)\left(1 - \frac{n}{p^{n-1}}\right), \end{aligned}$$

and the conclusion follows. □

Lemma 4.8. *For any prime p and for all $m \geq 1$,*

$$D_n(p^m) \leq 1 - \frac{1}{p^{n-1}}.$$

Proof. Let M be the set of $n \times n$-matrices in Hermite normal form with determinant p^m. Let $a^*_n(p^m)$ be the number of matrices in M whose last diagonal element is divisible by p. Then $a^*_{n-i}(p^m)$ is the number of matrices in M whose diagonal element on row $n-i$ is divisible by p, and the diagonal elements on rows $n-i+1$ to n are 1. We have

$$a_n(p^m) = a^*_n(p^m) + \cdots + a^*_1(p^m).$$

Now, $a^*_{n-i}(p^m)/p^{(n-i)-1}$ counts the matrices in M whose $(n-i)$th row is divisible by p and whose diagonal elements on row $n-i+1$ to n are 1. Thus

$$\frac{a^*_n(p^m)}{p^{n-1}} + \cdots + \frac{a^*_1(p^m)}{p^{1-1}}$$

counts only matrices with not all of their rows primitive (no matrix is counted twice). So

$$\begin{aligned} a'_n(p^m) &\leq a_n(p^m) - \left(\frac{a_n^*(p^m)}{p^{n-1}} + \cdots + \frac{a_1^*(p^m)}{p^{1-1}} \right) \\ &\leq a_n(p^m) - \frac{1}{p^{n-1}} \left(a_n^*(p^m) + \cdots + a_1^*(p^m) \right) \\ &= a_n(p^m) \left(1 - \frac{1}{p^{n-1}} \right), \end{aligned}$$

wherefore

$$D_n(p^m) \leq 1 - \frac{1}{p^{n-1}}. \qquad \square$$

Theorem 1.4. *Let k be an integer (possibly 0). Then*

$$D_n(k) \to 1$$

uniformly as $n \to \infty$.

Proof. Assume $k \neq 0$. As $D_n(k) = D_n(-k)$, we may assume $k > 0$. By Lemma 4.7 and the multiplicativity of D_n, $D_n(k)$ is bounded below by

$$\prod_p \left(1 - \frac{n}{p^{n-1}} \right),$$

where the product ranges over the primes p. As $n \to \infty$, this lower bound converges to 1, and as $D_n(k)$ is trivially bounded by 1, $D_n(k) \to 1$.

Now assume $k = 0$. We have due to [Wig] that $D_n(0) = 1/\zeta(n-1)^n$. Since $(1 - 1/p^{n-1})^n \geq 1 - n/p^{n-1}$ for all primes p, we get

$$D_n(0) = \frac{1}{\zeta(n-1)^n} = \prod_p \left(1 - \frac{1}{p^{n-1}} \right)^n \geq \prod_p \left(1 - \frac{n}{p^{n-1}} \right),$$

which is the same lower bound as for $k \neq 0$. Thus $D_n(k) \to 1$ for all k. □

Recall that a sequence $(k_1, k_2, \ldots)$ is rough if and only if its terms eventually have no divisors smaller than m (except for 1), for any m.

Theorem 1.5. *Let $n \geq 3$ be fixed. Then*

$$D_n(k_i) \to 1$$

as $i \to \infty$ if and only if the sequence $(k_1, k_2, \ldots)$ is rough.

Proof. We may assume $k_i \geq 0$ for all i.

Assume $(k_1, k_2, \ldots)$ is rough. Take N such that k_i is not divisible by any prime $p < N$. By Lemma 4.7 and the multiplicativity of D_n, $D_n(k_i)$ is bounded below by

$$\prod_{p \geq N} \left(1 - \frac{n}{p^{n-1}}\right),$$

which is an absolutely convergent infinite product because $\sum_{p \geq N} n/p^{n-1}$ is an absolutely convergent series with no terms equal to 1 (for sufficiently large N). By the definition of convergence for infinite products,

$$\prod_{p \geq N} \left(1 - \frac{n}{p^{n-1}}\right) \to 1$$

as $N \to \infty$. As $D_n(k_i)$ is also bounded above by 1, this proves that $D_n(k_i) \to 1$ as $i \to \infty$.

To demonstrate the only if-part, we assume instead that $(k_1, k_2, \ldots)$ is not rough. Then there is a prime p_0 such that infinitely many k_i are divisible by p_0. Since D_n is multiplicative, we can write $D_n(k_i)$ as a product of factors $D_n(p^m)$ (p is a prime), all of which are at most 1. Fix a k_i such that k_i is divisible by p_0. Using Lemma 4.8, we can write for some $m \geq 1$,

$$D_n(k_i) \leq D_n(p_0^m) \leq 1 - \frac{1}{p_0^{n-1}}.$$

Since infinitely many $D_n(k_i)$ are bounded by $1 - 1/p_0^{n-1} < 1$, we cannot have $D_n(k_i) \to 1$ as $i \to \infty$. □

Recall that a sequence $(k_1, k_2, \ldots)$ is totally divisible if and only if its terms are eventually divisible by all positive integers smaller than m, for any m.

Theorem 1.6. *Let $n \geq 3$ be fixed. Then*

$$D_n(k_i) \to \frac{1}{\zeta(n-1)^n}$$

as $i \to \infty$ if the sequence $(k_1, k_2, \ldots)$ is totally divisible.

Proof. We have $D_n(0) = 1/\zeta(n-1)^n$ exactly due to [Wig]. We may thus assume $k_i > 0$ for all i.

Assume that $(k_1, k_2, \ldots)$ is totally divisible. Write $k_i =: \prod_p p^{m_p(i)}$ (where all but finitely many of the $m_p(i)$ are zero) as a product extending over all primes p. Then $m_p(i) \to \infty$ as $i \to \infty$ for all p. We have

$$D_n(k_i) = \prod_p D_n(p^{m_p(i)}) = \prod_p (1 - b_p(i)),$$

where $b_p(i) := 1 - D_n(p^{m_p(i)}) \geq 0$. By Lemma 4.8, $b_p(i) \leq 1 - (1 - 1/p^{n-1}) = 1/p^{n-1}$, so $\sum_p b_p(i)$ is absolutely and uniformly convergent by the Weierstrass M-test, for which reason $\prod_p (1 - b_p(i))$ is uniformly convergent (with respect to i). We may thus interchange limits, so that

$$\lim_{i\to\infty} D_n(k_i) = \prod_p \lim_{i\to\infty} D_n(p^{m_p(i)}) = \prod_p \left(1 - \frac{1}{p^{n-1}}\right)^n = \frac{1}{\zeta(n-1)^n},$$

where we have used Lemma 4.6. □

Proposition 1.8. *Let $n = 2$. Then*

$$D_2(k_i) \to 0$$

if and only if $\lim_{i\to\infty} \sum_{p|k_i} 1/p \to \infty$. *Moreover,*

$$D_2(k_i) \to 1$$

if and only if $\lim_{i\to\infty} \sum_{p|k_i} 1/p \to 0$. *The sums are taken over all primes p which divide k_i.*

Proof. If $m = 0$, we have $D_n(p^m) = 1$. Assume $m > 0$. The 2×2-matrices in Hermite normal form with determinant p^m and primitive rows are of the form $\begin{pmatrix} 1 & 0 \\ x & p^m \end{pmatrix}$ where $0 \leq x < p^m, p \nmid x$. Thus $a_2'(p^m) = p^m(1 - 1/p)$. Moreover,

$$a_2(p^m) = \sum_{d_1 d_2 = p^m} d_2 = \sum_{i+j=m} p^i = \sum_{i=0}^{m} p^i = \frac{p^{m+1} - 1}{p - 1} = \frac{1 - 1/p^{m+1}}{1 - 1/p},$$

so $D_2(p^m) = (1 - 1/p)^2/(1 - 1/p^{m+1})$. Therefore

$$\left(1 - \frac{1}{p}\right)^2 \leq D_2(p^m) \leq 1 - \frac{1}{p}.$$

Since D_2 is multiplicative, we get

$$\left[\prod_{p|k} \left(1 - \frac{1}{p}\right)\right]^2 \leq D_2(k) \leq \prod_{p|k} \left(1 - \frac{1}{p}\right).$$

The left and right sides diverge to 0 if and only if $\lim_{i\to\infty} \sum_{p|k_i} 1/p \to \infty$, and they converge to 1 if and only if $\lim_{i\to\infty} \sum_{p|k_i} 1/p \to 0$. □

Appendix A

Density of primitive vectors in Euclidean space

Lemma A.1 (The primitive circle problem). *Let $n \geq 2$. The number of primitive vectors in $\mathbb{Z}^n$ of length at most T as $T \to \infty$ is*

$$\frac{\pi T^n}{\zeta(n)} + O(T^{n-1}).$$

Since the total number of vectors in $\mathbb{Z}^n$ is $\pi T^n + O(T^{n-1})$, we can formulate this in terms of density as:

Corollary A.2. *The density of primitive vectors in $\mathbb{Z}^n$ is $1/\zeta(n)$.*

Proof of Lemma A.1. Let $\widehat{N}_n(T)$ be the number of vectors in $\mathbb{Z}^n$ of length at most T, and let $\widehat{N}'_n(T)$ be the number of primitive vectors in $\mathbb{Z}^n$ of length at most T.

Every vector in $\mathbb{Z}^n$ is a positive integer multiple of a unique primitive vector, so

$$\widehat{N}_n(T) = \sum_{m=1}^{\lfloor T \rfloor} \widehat{N}'_n(T/m),$$

and we can apply the generalized inversion formula from Lemma 2.23 and the identity 2.22 to get

$$\begin{aligned}
\widehat{N}_n'(T) &= \sum_{m=1}^{\lfloor T\rfloor} \mu(m)\widehat{N}_n(T/m) = \sum_{m=1}^{\lfloor T\rfloor} \mu(m)(\pi(T/m)^n + O((T/m)^{n-1})) \\
&= \pi T^n \sum_{m=1}^{\lfloor T\rfloor} \frac{\mu(m)}{m^n} + O(T^{n-1}) \sum_{m=1}^{\lfloor T\rfloor} \frac{1}{m^{n-1}} \\
&= \pi T^n \sum_{1}^{\infty} \frac{\mu(m)}{m^n} - \pi T^n \sum_{\lfloor T\rfloor+1}^{\infty} \frac{\mu(m)}{m^n} + O(T^{n-1}) \sum_{m=1}^{\lfloor T\rfloor} \frac{1}{m^{n-1}} \\
&=: \frac{\pi T^n}{\zeta(n)} + E(T),
\end{aligned}$$

where $E(T)$ is an error term which we calculate as follows. For $n \geq 3$ we get

$$\begin{aligned}
|E(T)| &\leq \pi T^n \int_T^\infty \frac{dm}{m^n} + O(T^{n-1}) \sum_1^\infty \frac{1}{m^{n-1}} \\
&= T^n O(1/T^{n-1}) + O(T^{n-1})O(1) \\
&= O(T) + O(T^{n-1}) = O(T^{n-1}).
\end{aligned}$$

This estimation fails for $n = 2$ as $\sum_{m=1}^{\lfloor T\rfloor} 1/m^{n-1}$ is $O(\log T)$ (by integral comparison) and not $O(1)$ as above, yielding the slightly worse error term $E(T) = O(T \log T)$. However, this can be fixed by starting with a better error term for $N_2(T)$ (from Gauss's circle problem), see remark 2.16. Using $N_2(T) = \pi T^2 + O(T^\alpha)$ for any $1/2 < \alpha < 1$ (for example $\alpha = 2/3$) and repeating the proof above *mutatis mutandis*, will yield exactly the error term $E(T) = O(T)$ for $n = 2$. □

Appendix B

Counting singular 2×2-matrices with primitive row vectors

Proposition B.1. *The number of singular* 2×2*-matrices with primitive row vectors and Euclidean norm at most* T *as* $T \to \infty$ *is*

$$N_2'(T) = \frac{\pi T^2}{\zeta(2)} + O(T).$$

Proof. The singular matrices with primitive rows are of the form $\begin{pmatrix} v \\ \alpha v \end{pmatrix}$ where v is a primitive vector and α is nonzero. Since αv is an integer vector, α cannot be irrational, so we can write $\alpha = n/m$ where $m > 0$ and n is coprime to m. Since m must divide every element of the primitive vector v, we must have $m = 1$. Further, for $\alpha v = nv$ to be primitive, we must have $n = \pm 1$. So the singular matrices with primitive row vectors are precisely the matrices $\begin{pmatrix} v \\ v \end{pmatrix}$ and $\begin{pmatrix} v \\ -v \end{pmatrix}$ for primitive v. The Euclidean norm of $\begin{pmatrix} v \\ \pm v \end{pmatrix}$ is $\sqrt{2}\|v\| \leq T$, or equivalently $\|v\| \leq T/\sqrt{2}$. Thus, the number of integer 2×2-matrices with primitive rows and norm at most T is twice the number of primitive vectors $v \in \mathbb{Z}^2$ with norm at most $T/\sqrt{2}$, and an application of Lemma A.1 gives us our asymptotic formula. □

Appendix C

Proof recipe for the lower bound on density

This appendix is concerned with the conjectured lower bound

$$D_n(p^m) > \left(1 - \frac{1}{p^n}\right)^n \tag{$\star$}$$

for all $n \geq 3$, primes p and $m \geq 0$ (for $n = 2$ this inequality is false and the lower bound is actually 0, as proved in Theorem 1.8). Actually, something stronger should be true: $D_n(p^m)$ decreases strictly as m increases (when n and p are held fixed).

For us, the lower bound ($\star$) would be sufficient to prove Conjecture 1.7 and the converse (the "only if"-part) of Theorem 1.6. For small n, ($\star$) can be proved using the following *ad hoc* method. We fix n and rewrite ($\star$) as a polynomial inequality, and observe that it holds for all sufficiently large m (independent of p), leaving us with only a finite number of cases to check by hand. For small n, it is feasible to do this. This has been done for $n = 3$ and $n = 4$ and a full proof of the case $n = 3$ is given with Proposition C.1. We prove that ($\star$) holds for all but finitely many (p, m) in Proposition C.3 for any given fixed n.

Proposition C.1. *Fix $n = 3$. For all primes p and for all $m \geq 0$,*

$$D_3(p^m) > \left(1 - \frac{1}{p^2}\right)^3.$$

Proof sketch. Using the formulae from Proposition 3.5 and Lemma 4.2, we may explicitly calculate

$$\begin{aligned} a_3(p^m) &= \frac{\left(p^{m+1} - 1\right)\left(p^{m+2} - 1\right)}{(p-1)\left(p^2 - 1\right)} \\ a_3'(p^m) &= \frac{(p-1)^2(p+1)p^{m-3}\left(2p^{m+1} + p^{m+2} + p^m - p\right)}{p^2 - 1}, \qquad m \geq 3. \end{aligned}$$

Thus for $m \geq 3$, we can explicitly write out $D_3(p^m)$. Then $D_3(p^m) > (1 - p^{-2})^3$ is equivalent to (after multiplying by the denominators on both sides, and some rearranging)

$$p^{m+1} \underbrace{(3p^6 - 3p^5 - 5p^4 + 4p^3 + 3p^2 - p + 1)}_{q(p)} > (p^2 - 1)^3.$$

It can be verified that the polynomial q is strictly positive.[*] Since $q(p)$ is integer valued for all primes p, $q(p) \geq 1$ for all p. Therefore the inequality holds for $m+1 \geq 6$, since then $p^{m+1} > (p^2-1)^3$. The remaining cases $m \leq 4$ are treated separately. In each case, we explicitly write out $D_n(p^m)$ and rearrange ($\star$) to a polynomial inequality. The polynomials we get which we need to prove are positive are the following.

$$\begin{aligned} 3p^7 - 2p^5 - p^4 - p^3 - p^2 + p + 1 &\qquad (m = 4) \\ 3p^6 - 2p^4 - 2p^3 - p^2 + p + 1 &\qquad (m = 3) \\ 3p^5 - 3p^3 - 2p^2 + p + 1 &\qquad (m = 2) \\ 3p^4 - 3p^2 + 1 &\qquad (m = 1) \end{aligned}$$

It is easy to see that this is true, for the leading coefficient is the largest in each case, and thus the leading term dominates in each polynomial when substituting $p \geq 2$. □

In the proof below, we will use without proof the fact that $a_n(p^m)$ can be written as a Gaussian binomial coefficient (a p-analogue of the binomial coefficient)

$$a_n(p^m) = \binom{m+n-1}{n-1}_p = \frac{(p^{m+1}-1)\cdots(p^{m+n-1}-1)}{(p-1)\cdots(p^{n-1}-1)}. \tag{C.2}$$

Proposition C.3. *Fix $n \geq 3$. Then*

$$D_n(p^m) > \left(1 - \frac{1}{p^{n-1}}\right)^n$$

holds for all but finitely many (p, m), where p is prime and $m \geq 0$.

Proof. The inequality

$$\frac{a_n'(p^m)}{a_n(p^m)} > \frac{(p^{n-1}-1)^n}{(p^{n-1})^n}$$

[*] By computing its roots numerically by computer and observing there are no real roots, or more rigorously by bounding the absolute value of its roots ($|p| < 3$ is an upper bound as the leading term dominates for $p \geq 3$), and then checking a finite number of cases (here, only $p = 2$).

is equivalent to

$$p^{(n-1)n}a'_n(p^m) - (p^{n-1}-1)^n a_n(p^m) > 0, \tag{C.4}$$

where the left side is a polynomial in p. We have

$$a_n(p^m) = \sum_{m_1+\cdots+m_n=m} p^{0m_1+\cdots+(n-1)m_n} = p^{m(n-1)} + \beta p^{m(n-1)-1} + \cdots$$

for some $\beta > 0$ (depending on m), where here and throughout the rest of the proof, an ellipsis denotes terms of smaller degree. Hence

$$\begin{aligned} a'_n(p^m) &= a_n(p^m) - \binom{n}{1} a_n(p^{m-1}) + \cdots \\ &= (p^{m(n-1)} + \beta p^{m(n-1)-1} + \cdots) - n(p^{(m-1)(n-1)-1} + \cdots) \\ &= p^{m(n-1)} + \beta p^{m(n-1)-1} + \cdots . \end{aligned}$$

Thus since

$$(p^{n-1}-1)^n = p^{(n-1)n} - np^{(n-1)n-1} + \cdots ,$$

the left side of (C.4) becomes

$$\begin{gathered} (p^{(n-1)n+m(n-1)} + \beta p^{(n-1)n+m(n-1)-1} + \cdots) - \\ (p^{(n-1)n} - np^{(n-1)n-1} + \cdots)(p^{m(n-1)} + \beta p^{m(n-1)-1} + \cdots) = \\ (\beta + n - \beta)p^{(n-1)n+m(n-1)-1} + \cdots , \end{gathered}$$

the leading coefficient of which is n.

It follows from the product formula (C.2) and the fact that

$$a'_n(p^m) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_n(p^{m-i})$$

for $m \geq n$ that (C.4) can be written in the form

$$p^{sm}q_s(p) + p^{(s-1)m}q_{s-1}(p) + \cdots + p^m q_1(p) + q_0(p) > 0, \tag{C.5}$$

for some fixed s, where each q_i denotes some fixed polynomial in p (independent of m).

Actually, $s = n-1$, and $q_s(p) \geq 1$ since we proved that the leading term is $np^{(n-1)m}p^{(n-1)n-1}$. It is easy to see that the inequality (C.5) holds for all sufficiently large m (independent of p), as well as that for any fixed m, it holds for all sufficiently large p. □

Appendix D

The Katznelson measure

In [Kat] the asymptotics

$$N_{n,0}(T) = \frac{n-1}{\zeta(n)} w(B) T^{n(n-1)} \log T + O(T^{n(n-1)})$$

are given, where w is a particular measure and B is the unit ball in $M_n(\mathbb{R})$. It is not difficult to calculate $w(B)$, and this is what we will do in this section.

The measure w on $M_n(\mathbb{R})$ is defined in [Kat] as follows. Let $A_u := \{A \in M_n(\mathbb{R}) : Au = 0\} = \{(r_1, \ldots, r_n)^t : r_i \cdot u = 0\} = (u^\perp)^n$ be the space of matrices annihilating the nonzero vector $u \in \mathbb{R}^n \setminus \{0\}$. We define for (Lebesgue measurable) subsets $E \subseteq M_n(\mathbb{R})$ the measure $w_u(E) := \mathrm{vol}(E \cap A_u(\mathbb{R}))$ where vol is the standard $n(n-1)$-dimensional volume on $A_u(\mathbb{R})$, and define the measure $w(E) := (1/2) \int_{\mathrm{S}^{n-1}} w_u(E)\, d\nu(u)$, where ν is the standard Euclidean surface measure on the $(n-1)$-dimensional sphere S^{n-1}.

The volume of the unit ball $B \cap A_u(\mathbb{R})$ in the $n(n-1)$-dimensional vector space $A_u(\mathbb{R})$ is equal to the volume of the unit ball in $\mathbb{R}^{n(n-1)}$, which we will denote by $V_{n(n-1)}$. So $w_u(B) = V_{n(n-1)}$, independently of $u \neq 0$, and

$$w(B) = V_{n(n-1)} \frac{1}{2} \int_{\mathrm{S}^{n-1}} d\nu(u) = \frac{V_{n(n-1)} S_{n-1}}{2},$$

where S_{n-1} is the surface area of the sphere S^{n-1}. The volume and surface area of the unit ball is of course well known, and we may explicitly calculate

$$C_0 = w(B) = \frac{\pi^{n^2/2}}{\Gamma\left(\frac{n}{2}\right) \Gamma\left(\frac{n(n-1)}{2} + 1\right)}.$$

We recognize the similarity of this expression to that of C_1 given in Theorem 2.18, and see that

$$C_1 = \frac{1}{\zeta(2) \cdots \zeta(n)} C_0.$$

Bibliography

[Apo] Tom M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York, 1976. Undergraduate Texts in Mathematics.

[Coh] Donald L. Cohn. *Measure theory*. Birkhäuser Boston, Mass., 1980.

[DRS] W. Duke, Z. Rudnick, and P. Sarnak. Density of integer points on affine homogeneous varieties. *Duke Math. J.*, 71(1):143–179, 1993.

[GG] Henri Gillet and Daniel R. Grayson. Volumes of symmetric spaces via lattice points. *Doc. Math.*, 11:425–447 (electronic), 2006.

[GN] Alexander Gorodnik and Amos Nevo. *The ergodic theory of lattice subgroups*, volume 172 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2010.

[Kat] Y. R. Katznelson. Singular matrices and a uniform bound for congruence groups of $\mathrm{SL}_n(\mathbb{Z})$. *Duke Math. J.*, 69(1):121–136, 1993.

[Lia] Ming Liao. *Lévy processes in Lie groups*, volume 162 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2004.

[LP] Peter D. Lax and Ralph S. Phillips. The asymptotic distribution of lattice points in Euclidean and non-Euclidean spaces. *J. Funct. Anal.*, 46(3):280–350, 1982.

[Sie1] Carl Ludwig Siegel. Discontinuous groups. *Ann. of Math. (2)*, 44:674–689, 1943.

[Sie2] Carl Ludwig Siegel. A mean value theorem in geometry of numbers. *Ann. of Math. (2)*, 46:340–347, 1945.

[Sie3] Carl Ludwig Siegel. *Lectures on the geometry of numbers*. Springer-Verlag, Berlin, 1989. Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter, With a preface by Chandrasekharan.

[Sta] Richard P. Stanley. *Enumerative combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

[Wig] Igor Wigman. Counting singular matrices with primitive row vectors. *Monatsh. Math.*, 144(1):71–84, 2005.

Index