COUNTING INTEGER MATRICES WITH SQUARE-FREE DETERMINANTS

ALINA OSTAFE AND IGOR E. SHPARLINSKI

Abstract. We consider the set $\mathcal{M}_n(\mathbb{Z};H)$ of $n\times n$-matrices with integer elements of size at most H and obtain an asymptotic formula for the number of matrices from $\mathcal{M}_n(\mathbb{Z};H)$ with square-free determinants. We also use our approach with some further enhancements, to obtain an asymptotic formula for the sums of the Euler function with determinants of matrices from $\mathcal{M}_n(\mathbb{Z};H)$.

Contents

2020 *Mathematics Subject Classification.* 11C20, 11L07, 15B36, 15B52.
Key words and phrases. Matrices, determinants, square-freeness.

1. Introduction

1.1. **Motivation results.** For a positive integer n, we use $\mathcal{M}_n(\mathbb{Z})$ to denote the set of all $n \times n$ matrices with integer elements. Furthermore, for an integer $H \geqslant 1$ we use $\mathcal{M}_n(\mathbb{Z}; H)$ to denote the set of matrices

$$A = (a_{ij})_{i,j=1}^{n} \in \mathcal{M}_n(\mathbb{Z})$$

with integer entries of size $|a_{ij}| \leqslant H$. In particular, $\mathcal{M}_n(\mathbb{Z}; H)$ is of cardinality $\#\mathcal{M}_n(\mathbb{Z}; H) = (2H+1)^{n^2}$.

Recently there has been quite active interest in investigating arithmetic properties of matrix determinants and minors, see [13, 14]. For example, Kotsovolis and Woo [13] obtained an asymptotic formula for the number of matrices (counted by an slightly different norm) with prime determinants. The methods of homogeneous dynamics, underlying the approach of [13], do not allow to get strong bounds on the error terms of this asymptotic formula. Motivated by this work, and also by work of Kovaleva [14] on square-free minors, we obtain an asymptotic formula for the number $S_n(H)$ of matrices $A \in \mathcal{M}_n(\mathbb{Z}; H)$ with a square-free determinant, that is, matrices for which $\det A$ is not divisible by a square of any prime. While investigating square-free values is typically easier than investigating prime values, our goal is to get strong bounds on the error term of our asymptotic formula.

We also remark that treating the determinant as a generic polynomial over $\mathbb{Z}$ in n^2 variables and of degree n, is not going to bring any results as at the present time all results on square-free values of polynomials of high degree are conditional on the celebrated *abc*-conjecture, see [15, 16], or require an exponentially large (compared to the degree) number of variables [4].

It is natural to ask whether our results extend to arbitrary multilinear polynomials. Unfortunately the answer is negative as our arguments rely on the special structure of determinants, for example, on its invariance with respect to standard row operations used in the proof of Lemma 3.3, and homogeneity with respect to the variables from the same row, used in the proof of Lemma 3.4. Furthermore, there is no analogue of Lemma 2.2 for arbitrary multivariate polynomials.

1.2. **Main results.** Our asymptotic formula gives a power saving in the error term, exceeding 1/2, which is the limit of approaches based on the use of the Weil bound.

In fact, using the standard inclusion-exclusion principle together with Lemmas 2.1 and 2.2 below one can already get a power saving in the error term. However we go beyond this and get a stronger bound.

Theorem 1.1. *We have*

$$S_n(H) = 2^{n^2}\mathfrak{S}_n H^{n^2} + O\left(H^{n^2-\gamma_n}\right),$$

where

$$\mathfrak{S}_n = \prod_{p\ \mathit{prime}} \prod_{j=2}^{n+1} \left(1 - p^{-j}\right)$$

and

$$\gamma_n = \frac{1}{2} + \frac{n-1}{2\left(n^3+3n^2-n+1\right)}.$$

Note that

$$\mathfrak{S}_n = \prod_{j=2}^{n+1} \zeta(j)^{-1},$$

where $\zeta(s)$ is the Riemann zeta-function.

Our approach is based on new bounds on exponential sums along determinant hypersurfaces, which we believe could be of independent interest.

Remark 1.2. Note that the bounds based on algebraic geometry, such as in [7,11], do not apply to rational exponential sums modulo p^2, where p is prime, which is our principal case. Moreover, even in the case of exponential sums modulo p, our bounds are stronger that those which can be derived from, for example, results of Katz [10]. This is due to the high dimension of the singularity locus of the determinant variety over $\mathbb{F}_p$ (which is the set of matrices of $n \times n$ matrices over $\mathbb{F}_p$ of rank at most $n-2$, and thus a variety of dimension n^2-4, see [1]), affecting very adversely the strength of the algebraic geometry approach.

Remark 1.3. It is also interesting to note that Browning, Sawin and Wang [3] have also used bounds on exponential sums with matrices over $\mathbb{F}_p$ to establish some new results on matrices with integer entries. However the exponential sums which arise in [3] and the techniques employed are very different from ours.

We emphasise that the main feature of Theorem 1.1 is that $\gamma_n > 1/2$ since with

$$\gamma_n = n^2/(2n^2+2) < 1/2 \tag{1.1}$$

it can be derived via the aforementioned elementary argument, avoiding the use of exponential sums.

Next, to illustrate other possible applications of our results, in particular, to obtaining asymptotic formulas for certain sums with multiplicative functions with determinants, we consider the following sum

$$\varPhi_n(H) = \sum_{\substack{A \in \mathcal{M}_n(\mathbb{Z};H) \\ \det A \neq 0}} \frac{\varphi\left(|\det A|\right)}{|\det A|},$$

where $\varphi(k)$ is the Euler function. Our results certainly apply to sums of many other multiplicative functions.

In fact in this case we are able to introduce further enhancements to the argument underlying the proof of Theorem 1.1 and obtain the following result.

Theorem 1.4. *We have*

$$\varPhi_n(H) = 2^{n^2}\sigma_n H^{n^2} + O\left(H^{n^2-\vartheta_n+o(1)}\right),$$

where

$$\sigma_n = \prod_{p \ prime}\left(1-\frac{1}{p}\right)\left(1+\frac{1}{p}\prod_{j=2}^{n}\left(1-p^{-j}\right)\right)$$

and

$$\vartheta_n = 1 - \frac{1}{n^3+1}.$$

Remark 1.5. Our proof of Theorem 1.4 takes advantage of stronger bounds of exponential sums with square-free denominators with so-called monomial linear forms, see Lemma 3.7 below. We have not been able to establish a bound of similar strength in the case of denominators, which are squares of square-free integers, see, however, Lemma 3.8.

1.3. **Notation and conventions.** We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are equivalent to $|U| \leqslant cV$ for some positive constant c, which throughout this work, may depend only on n.

We also write $U = V^{o(1)}$ if for any fixed ε we have $V^{-\varepsilon} \leqslant |U| \leqslant V^{\varepsilon}$ provided that V is large enough.

For a finite set $\mathcal{S}$ we use $\#\mathcal{S}$ to denote its cardinality.

For a positive integer m, we use $\mathbb{Z}_m$ to denote the residue ring modulo m, which we assume to be represented by the set $\{0, \ldots, m-1\}$, and use $\mathbb{Z}_m^*$ for its group of units.

The letter p always denotes a prime number.

We also freely alternate between the language of residue rings $\mathbb{Z}_p$ modulo p and finite fields $\mathbb{F}_p$ of p elements. Similarly, we also alternate, where convenient, between the language of residue rings $\mathbb{Z}_m$ and congruences modulo m.

For an integer $k \neq 0$ we denote by $\tau(k)$ the number of positive integer divisors of k, for which we very often use the well-known bound

$$\tau(k) = |k|^{o(1)} \tag{1.2}$$

as $|k| \to \infty$, see [9, Equation (1.81)].

We also use the convention that if A is an $n \times n$ matrix defined over $\mathbb{Z}_m$ or $\mathbb{F}_p$, then by $\det A = 0$ we mean $\det A \equiv 0 \bmod m$ or $\det A \equiv 0 \bmod p$, respectively, which should be clear from the context. When A has entries in an interval $[-H, H]$, then any condition on the determinant modulo a positive integer m or prime p will be clearly indicated.

2. Preliminaries

2.1. Matrices with determinants with a divisibility condition.

Let $N_n(m)$ denote the number of $n \times n$ matrices A over $\mathbb{Z}_m$ for which $\det A = 0$.

The following exact formula is a very special case of a much more general result of Brent and McKay [2, Corollary 2.2] combined with the classical Chinese Remainder Theorem.

Lemma 2.1. *For any square-free integer $d \geqslant 1$, we have*

$$N_n(d) = d^{n^2} \prod_{p \mid d} \left(1 - \prod_{j=1}^{n} \left(1 - p^{-j}\right)\right)$$

and

$$N_n(d^2) = d^{2n^2} \prod_{p \mid d} \left(1 - \prod_{j=2}^{n+1} \left(1 - p^{-j}\right)\right).$$

2.2. Matrices with fixed determinants.

We need a bound on the number of matrices $A \in \mathcal{M}_n(\mathbb{Z}; H)$ with prescribed value of the determinant $\det A = d$. We recall that Duke, Rudnick and Sarnak [6], if $d \neq 0$, and Katznelson [11], when $d = 0$, have obtained asymptotic formulas (with the main terms of orders H^{n^2-n} and $H^{n^2-n} \log H$, respectively) for the number of such matrices when d is fixed. However this is too restrictive for our purpose because we need a uniform with respect to d results, while in [6] the dependency on d is not specified. Hence we use a uniform with respect to d upper bound which is a special case of [17, Theorem 4].

Lemma 2.2. *Uniformly over $a \in \mathbb{Z}$, there are at most $O\left(H^{n^2-n}\log H\right)$ matrices $A \in \mathcal{M}_n(\mathbb{Z}; H)$ with $\det A = a$.*

In principle, as we have mentioned, a combination of Lemmas 2.1 and 2.2 is already enough to prove a version of Theorem 1.1 with γ_n given by (1.1). However, to get the desired bound on the error term we also need to count matrices $A \in \mathbb{Z}_{d^2}^{n\times n}$ with entries in incomplete intervals in $\mathbb{Z}_{d^2}$ such that $\det A = 0$. This is done in Section 3 via bounds of exponential sums.

3. Exponential sums along determinant congruences

3.1. Set-up.

Given a linear form

$$L(\mathbf{X}) = \sum_{i,j=1}^{n} a_{ij}x_{ij} \in \mathbb{Z}[\mathbf{X}] \tag{3.1}$$

in n^2 variables $\mathbf{X} = (x_{ij})_{i,j=1}^{n}$ and an integer m, we define the exponential sums

$$S_m(L) = \sum_{\det \mathbf{X} \equiv 0 \bmod m} \mathbf{e}_m\left(L(\mathbf{X})\right)$$

where $\mathbf{e}_m(u) = \exp(2\pi i u/m)$, along solutions to the congruence $\det \mathbf{X} = 0$ in $\mathbf{X} \in \mathbb{Z}_m^{n\times n}$.

We are only interested in the sums $S_m(L)$ when the modulus $m = d$ or $m = d^2$ for a square-free integer $d \geqslant 1$. Thus we start with reduction to sums modulo p or p^2. Namely, by the Chinese Remainder Theorem, we have the following decomposition, see [9, Equation (12.21)].

Lemma 3.1. *For any square-free integer $d \geqslant 1$ and a linear form $L(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$, we have*

$$S_d(L) = \prod_{p\mid d} S_p(b_{d,p}L) \qquad \text{and} \qquad S_{d^2}(L) = \prod_{p\mid d} S_{p^2}(b_{d,p}L),$$

for some integers $b_{d,p}$ with $\gcd(b_{d,p}, p) = 1$.

Hence we now concentrate on the sums $S_p(L)$ and $S_{p^2}(L)$.

3.2. **Linear sections of the variety of singular matrices.** Let K be an arbitrary field and let $\mathcal{V}_n$ be the variety of $n \times n$ singular matrices over K.

Lemma 3.2. *The variety $\mathcal{V}_n$ is not contained in any hyperplane.*

Proof. Assume that $\mathcal{V}_n$ is contained in a hyperplane $\mathcal{H}$, which is given by the equation

$$\sum_{i,j=1}^{n} a_{ij} x_{ij} = a_0$$

with at least one non-zero coefficient, say $a_{k,m} \neq 0$. Considering matrices with zero-entries everywhere, except at the (k, m) position, which are clearly singular, we see that $a_{k,m} x_{k,m} = a_0$ for all $x_{k,m} \in K$, which is clearly impossible for $a_{k,m} \neq 0$. □

We write $n \times n$ matrices over $\mathbb{F}_p$ as $(\mathbf{z} \mid \mathbf{Z})$ for a vector $\mathbf{z} \in \mathbb{F}_p^n$ and an $n \times (n-1)$ matrix $\mathbf{Z} \in \mathbb{F}_p^{n\times(n-1)}$. We also recall that $N_n(p)$ denotes the number of $n \times n$ matrices A over $\mathbb{F}_p$ for which $\det A = 0$.

Lemma 3.3. *Let $\ell(\mathbf{z})$ be a nontrivial linear form over $\mathbb{F}_p$. Then the system of equations*

$$\det(\mathbf{z} \mid \mathbf{Z}) = \ell(\mathbf{z}) = 0, \qquad (\mathbf{z}, \mathbf{Z}) \in \mathbb{F}_p^n \times \mathbb{F}_p^{n\times(n-1)},$$

has $p^{n(n-1)} + (p^{n-1} - 1)p^{n-1} N_{n-1}(p)$ solutions.

Proof. We fix a vector $\mathbf{z} \in \mathbb{F}_p^n$ with $\ell(\mathbf{z}) = 0$. Clearly if $\mathbf{z} = \mathbf{0}$ is the zero-vector, then for any $\mathbf{Z} \in \mathbb{F}_p^{n\times(n-1)}$ we have $\det(\mathbf{0} \mid \mathbf{Z}) = 0$. Hence there are $p^{n(n-1)}$ such solutions.

Now, let $\mathbf{z} \neq \mathbf{0}$. Without loss of generality, we can assume that $\mathbf{z} = (z_1, z_2, \ldots, z_n)$ with $z_1 \neq 0$. Using elementary row operations, we can reduce the equation $\det(\mathbf{z} \mid \mathbf{Z}) = 0$ to an equation $\det(\mathbf{z}_0 \mid \mathbf{U}) = 0$ for some matrix $\mathbf{U}$ and with $\mathbf{z}_0 = (z_1, 0, \ldots, 0)$. It is now obvious that $\det(\mathbf{z}_0 \mid \mathbf{U}) = 0$ holds for $p^{n-1} N_{n-1}(p)$ matrices $\mathbf{U} \in \mathbb{F}_p^{n\times(n-1)}$ with an arbitrary top row and an arbitrary singular $(n-1)\times(n-1)$ matrix over $\mathbb{F}_p$ on the other positions. Observe that row operations are invertible, and so, for a given $\mathbf{z}$, each matrix $\mathbf{U} \in \mathbb{F}_p^{n\times(n-1)}$ corresponds to a unique matrix $\mathbf{Z} \in \mathbb{F}_p^{n\times(n-1)}$. Since there are $p^{n-1} - 1$ choices for $\mathbf{z} \neq \mathbf{0}$ with $\ell(\mathbf{z}) = 0$, there are $(p^{n-1} - 1)p^{n-1} N_{n-1}(p)$ such solutions. □

3.3. **Bounding $S_p(L)$.** Combining Lemma 3.2 with bounds of exponential sums along algebraic varieties, see, for example, [7, Proposition 1.2], one can immediately derive

$$S_p(L) \ll p^{n^2-3/2} \tag{3.2}$$

for any nonvanishing linear form $L(\mathbf{X}) \in \mathbb{F}_p[\mathbf{X}]$.

We prove now stronger results, and we start with the case when $L(\mathbf{X})$ depends only on the first column of $\mathbf{X}$.

Lemma 3.4. *For any nonvanishing linear form $\ell(\mathbf{z}) \in \mathbb{F}_p[\mathbf{z}]$, with $L(\mathbf{X}) = \ell(\mathbf{z})$, where $\mathbf{X} = (\mathbf{z} \mid \mathbf{Z})$, we have*

$$S_p(L) \ll p^{n^2-n}.$$

Proof. Using that for any $\lambda \in \mathbb{F}_p^*$, the map $\mathbf{z} \mapsto \lambda\mathbf{z}$ permutes $\mathbb{F}_p^n$, we can write

$$\begin{aligned} S_p(L) &= \sum_{\mathbf{Z} \in \mathbb{F}_p^{n\times(n-1)}} \sum_{\substack{\mathbf{z} \in \mathbb{F}_p^n \\ \det(\mathbf{z}|\mathbf{Z})=0}} \mathbf{e}_p\left(\ell(\mathbf{z})\right) \\ &= \frac{1}{p-1} \sum_{\lambda \in \mathbb{F}_p^*} \sum_{\mathbf{Z} \in \mathbb{F}_p^{n\times(n-1)}} \sum_{\substack{\mathbf{z} \in \mathbb{F}_p^n \\ \det(\lambda\mathbf{z}|\mathbf{Z})=0}} \mathbf{e}_p\left(\ell(\lambda\mathbf{z})\right) \\ &= \frac{1}{p-1} \sum_{\mathbf{Z} \in \mathbb{F}_p^{n\times(n-1)}} \sum_{\substack{\mathbf{z} \in \mathbb{F}_p^n \\ \det(\mathbf{z}|\mathbf{Z})=0}} \sum_{\lambda \in \mathbb{F}_p^*} \mathbf{e}_p\left(\lambda\ell(\mathbf{z})\right). \end{aligned}$$

Hence

$$S_p(L) = \frac{1}{p-1}\left(p\Sigma_1 - \Sigma_2\right), \tag{3.3}$$

where

$$\begin{aligned} \Sigma_1 &= \sum_{\mathbf{Z} \in \mathbb{F}_p^{n\times(n-1)}} \sum_{\substack{\mathbf{z} \in \mathbb{F}_p^n \\ \det(\mathbf{z}|\mathbf{Z})=0 \\ \ell(\mathbf{z})=0}} 1, \\ \Sigma_2 &= \sum_{\mathbf{Z} \in \mathbb{F}_p^{n\times(n-1)}} \sum_{\substack{\mathbf{z} \in \mathbb{F}_p^n \\ \det(\mathbf{z}|\mathbf{Z})=0}} 1. \end{aligned}$$

By Lemma 3.3, we have

$$\Sigma_1 = p^{n(n-1)} + \left(p^{n-1} - 1\right) p^{n-1} N_{n-1}(p), \tag{3.4}$$

and obviously

$$\Sigma_2 = N_n(p). \tag{3.5}$$

We now recall Lemma 2.1, and see that

$$\begin{aligned} N_n(p)/p^{n^2} &= 1 - \prod_{j=1}^{n} \left(1 - p^{-j}\right) \\ &= 1 - \left(1 - N_{n-1}(p)/p^{(n-1)^2}\right)\left(1 - p^{-n}\right) \\ &= \left(1 - p^{-n}\right) N_{n-1}(p)/p^{(n-1)^2} + p^{-n}. \end{aligned}$$

Hence

$$N_n(p) = \left(1 - p^{-n}\right) p^{2n-1} N_{n-1}(p) + p^{n^2-n}.$$

Recalling (3.4) and (3.5), we see that

$$\begin{aligned} p\Sigma_1 - \Sigma_2 = p^{n(n-1)+1} &+ \left(p^{n-1} - 1\right) p^n N_{n-1}(p) \\ &- \left(1 - p^{-n}\right) p^{2n-1} N_{n-1}(p) - p^{n^2-n} \\ = (p-1)p^{n(n-1)} &- (p-1)p^{n-1} N_{n-1}(p). \end{aligned}$$

Since we see from Lemma 2.1, that $N_{n-1}(p) \ll p^{n^2-2n}$ we now conclude that

$$p\Sigma_1 - \Sigma_2 = p^{n(n-1)+1} + O\left(p^{n^2-n}\right),$$

which after substitution in (3.3) concludes the proof. □

We now extend the bound of Lemma 3.4, with a weaker saving but still improving (3.2), to any nontrivial (that is, not vanishing identically) form $L(\mathbf{X})$ over $\mathbb{F}_p$.

Lemma 3.5. *For any nontrivial linear form $L(\mathbf{X}) \in \mathbb{F}_p[\mathbf{X}]$, we have*

$$S_p(L) \ll p^{n^2-(n+1)/2}.$$

Proof. Since the form $L(\mathbf{X}) = \sum_{i,j=1}^{n} a_{ij} x_{ij} \in \mathbb{F}_p[\mathbf{X}]$ is nontrivial, without loss of generality, we may assume $a_{1j} \neq 0$ for some $j = 1, \ldots, n$. We write every matrix $\mathbf{X} \in \mathbb{F}_p^{n\times n}$ as

$$\mathbf{X} = (\mathbf{x} \mid \mathbf{Y})$$

with a column $\mathbf{x} \in \mathbb{F}_p^n$ and a matrix $\mathbf{Y} \in \mathbb{F}_p^{n\times(n-1)}$. Therefore, $L(\mathbf{X})$ can be written in the form

$$L(\mathbf{X}) = \ell(\mathbf{x}) + L^*(\mathbf{Y}),$$

for some linear forms ℓ and L^* in n and $n(n-1)$ variables, respectively, where, by our assumption, ℓ is nontrivial modulo p.

Thus

$$S_p(L) = \sum_{\substack{\mathbf{Y}\in\mathbb{F}_p^{n\times(n-1)} \\ \det(\mathbf{x}|\mathbf{Y})=0}} \sum_{\mathbf{x}\in\mathbb{F}_p^n} \mathbf{e}_p\left(\ell(\mathbf{x}) + L^*(\mathbf{Y})\right)$$
$$= \sum_{\mathbf{Y}\in\mathbb{F}_p^{n\times(n-1)}} \mathbf{e}_p\left(L^*(\mathbf{Y})\right) \sum_{\substack{\mathbf{x}\in\mathbb{F}_p^n \\ \det(\mathbf{x}|\mathbf{Y})=0}} \mathbf{e}_p\left(\ell(\mathbf{x})\right).$$

Taking absolute values, we obtain

$$|S_p(L)| \leqslant \sum_{\mathbf{Y}\in\mathbb{F}_p^{n\times(n-1)}} \left| \sum_{\substack{\mathbf{x}\in\mathbb{F}_p^n \\ \det(\mathbf{x}|\mathbf{Y})=0}} \mathbf{e}_p\left(\ell(\mathbf{x})\right) \right|.$$

By the Cauchy inequality,

$$\begin{aligned} |S_p(L)|^2 &\leqslant p^{n^2-n} \sum_{\mathbf{Y}\in\mathbb{F}_p^{n\times(n-1)}} \left| \sum_{\substack{\mathbf{x}\in\mathbb{F}_p^n \\ \det(\mathbf{x}|\mathbf{Y})=0}} \mathbf{e}_p\left(\ell(\mathbf{x})\right) \right|^2 \\ &= p^{n^2-n} \sum_{\mathbf{Y}\in\mathbb{F}_p^{n\times(n-1)}} \sum_{\substack{\mathbf{x}_1,\mathbf{x}_2\in\mathbb{F}_p^n \\ \det(\mathbf{x}_i|\mathbf{Y})=0,\ i=1,2}} \mathbf{e}_p\left(\ell(\mathbf{x}_1-\mathbf{x}_2)\right). \end{aligned} \tag{3.6}$$

We now make the change of variables

$$\mathbf{x} = \mathbf{x}_1 \qquad \text{and} \qquad \mathbf{z} = \mathbf{x}_1 - \mathbf{x}_2$$

and notice that

$$\det\left(\mathbf{x}_1 \mid \mathbf{Y}\right) = \det\left(\mathbf{x}_2 \mid \mathbf{Y}\right) = 0$$

is equivalent to

$$\det\left(\mathbf{x} \mid \mathbf{Y}\right) = \det\left(\mathbf{x}_1 \mid \mathbf{Y}\right) = 0$$

and

$$\begin{aligned} \det\left(\mathbf{z} \mid \mathbf{Y}\right) &= \det\left(\mathbf{x}_1 - \mathbf{x}_2 \mid \mathbf{Y}\right) \\ &= \det\left(\mathbf{x}_1 \mid \mathbf{Y}\right) - \det\left(\mathbf{x}_2 \mid \mathbf{Y}\right) = 0. \end{aligned}$$

Hence, we see that (3.6) implies

$$|S_p(L)|^2 \leqslant p^{n^2-n} \sum_{\mathbf{Y}\in\mathbb{F}_p^{n\times(n-1)}} \sum_{\substack{\mathbf{x}\in\mathbb{F}_p^n \\ \det(\mathbf{x}|\mathbf{Y})=0}} \sum_{\substack{\mathbf{z}\in\mathbb{F}_p^n \\ \det(\mathbf{z}|\mathbf{Y})=0}} \mathbf{e}_p\left(\ell(\mathbf{z})\right).$$

We now split the summation over $\mathbf{Y} \in \mathbb{F}_p^{n\times(n-1)}$ into two parts depending on whether it is of full rank over $\mathbb{F}_p$ or of rank $\mathrm{rk}_p\,\mathbf{Y} \leqslant n-2$.

We observe that if $\mathrm{rk}_p\,\mathbf{Y} \leqslant n-2$ then for all $\mathbf{z} \in \mathbb{F}_p^n$ we have $\det(\mathbf{z} \mid \mathbf{Y}) = 0$. Hence,

$$\sum_{\substack{\mathbf{z}\in\mathbb{F}_p^n\\ \det(\mathbf{z}|\mathbf{Y})=0}} \mathbf{e}_p(\ell(\mathbf{z})) = \sum_{\mathbf{z}\in\mathbb{F}_p^n} \mathbf{e}_p(\ell(\mathbf{z})) = 0 \tag{3.7}$$

for any nontrivial modulo p linear form $\ell(\mathbf{z})$. Therefore, we obtain

$$|S_p(L)|^2 \leqslant p^{n^2-n} \sum_{\substack{\mathbf{Y}\in\mathbb{F}_p^{n\times(n-1)}\\ \mathrm{rk}_p\,\mathbf{Y}=n-1}} \sum_{\substack{\mathbf{x}\in\mathbb{F}_p^n\\ \det(\mathbf{x}|\mathbf{Y})=0}} \sum_{\substack{\mathbf{z}\in\mathbb{F}_p^n\\ \det(\mathbf{z}|\mathbf{Y})=0}} \mathbf{e}_p(\ell(\mathbf{z})).$$

We note that for $\mathbf{Y} \in \mathbb{F}_p^{n\times(n-1)}$ with $\mathrm{rk}_p\,\mathbf{Y} = n-1$ we have

$$\sum_{\substack{\mathbf{x}\in\mathbb{F}_p^n\\ \det(\mathbf{x}|\mathbf{Y})=0}} 1 = p^{n-1}$$

since it counts the number of solutions to some nontrivial linear congruence. Hence,

$$|S_p(L)|^2 \leqslant p^{n^2-1} \sum_{\substack{\mathbf{Y}\in\mathbb{F}_p^{n\times(n-1)}\\ \mathrm{rk}_p\,\mathbf{Y}=n-1}} \sum_{\substack{\mathbf{z}\in\mathbb{F}_p^n\\ \det(\mathbf{z}|\mathbf{Y})=0}} \mathbf{e}_p(\ell(\mathbf{z})),$$

where, using the identity (3.7), we can add back the terms with $\mathrm{rk}_p\,\mathbf{Y} \leqslant n-2$ and rewrite the above bound as

$$|S_p(L)|^2 \leqslant p^{n^2-1} \sum_{\mathbf{Y}\in\mathbb{F}_p^{n\times(n-1)}} \sum_{\substack{\mathbf{z}\in\mathbb{F}_p^n\\ \det(\mathbf{z}|\mathbf{Y})=0}} \mathbf{e}_p(\ell(\mathbf{z})).$$

Thus, together with Lemma 3.4, we obtain

$$|S_p(L)|^2 \leqslant p^{2n^2-n-1},$$

which concludes the proof. □

3.4. **Bounding $S_{p^2}(L)$.** A variation of some of the arguments from Section 3.3 also allows us to estimate $S_{p^2}(L)$.

Lemma 3.6. *For any linear form $L(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$, which is nonvanishing modulo p, we have*

$$S_{p^2}(L) \ll p^{2n^2-(n+3)/2}.$$

Proof. The argument below has several similarities with that in the proof of Lemma 3.5, however we present it in full detail.

Since in the proof we work with both elements of $\mathbb{Z}_{p^2}$ and of $\mathbb{Z}_p$, we use the language of congruences rather than of equations in the corresponding rings.

Without loss of generality, we can assume that $L(\mathbf{X})$ is nontrivial modulo p with respect to the first column of $\mathbf{X}$.

We write every matrix $\mathbf{X} \in \mathbb{Z}_{p^2}^{n\times n}$ as

$$\mathbf{X} = (\mathbf{x} \mid \mathbf{Y})$$

with a column $\mathbf{x} \in \mathbb{Z}_{p^2}^{n}$ and a matrix $\mathbf{Y} \in \mathbb{Z}_{p^2}^{n\times(n-1)}$.

Thus

$$S_{p^2}(L) = \sum_{\substack{\mathbf{Y}\in\mathbb{Z}_{p^2}^{n\times(n-1)} \\ \det(\mathbf{x}|\mathbf{Y})\equiv 0 \bmod p^2}} \sum_{\mathbf{x}\in\mathbb{Z}_{p^2}^{n}} \mathbf{e}_{p^2}\left(\ell(\mathbf{x}) + L^*(\mathbf{Y})\right)$$

for some linear forms ℓ and L^* in n and $n(n-1)$ variables, respectively, where by our assumption, ℓ is nontrivial modulo p.

Furthermore, we have

$$S_{p^2}(L) = \frac{1}{p^n} \sum_{\mathbf{y}\in\mathbb{Z}_p^n} \sum_{\substack{\mathbf{Y}\in\mathbb{Z}_{p^2}^{n\times(n-1)} \\ \det(\mathbf{x}+p\mathbf{y}|\mathbf{Y})\equiv 0 \bmod p^2}} \sum_{\mathbf{x}\in\mathbb{Z}_{p^2}^{n}} \mathbf{e}_{p^2}\left(\ell(\mathbf{x}+p\mathbf{y}) + L^*(\mathbf{Y})\right).$$

Next, we observe that for $\mathbf{x} \in \mathbb{Z}_{p^2}^n$ and $\mathbf{y} \in \mathbb{Z}_p^n$ we have

$$\ell\left(\mathbf{x}+p\mathbf{y}\right) \equiv \ell(\mathbf{x}) + p\ell(\mathbf{y}) \bmod p^2$$

and

$$\det\left(\mathbf{x}+p\mathbf{y} \mid \mathbf{Y}\right) \equiv \det\left(\mathbf{x} \mid \mathbf{Y}\right) + p\det\left(\mathbf{y} \mid \mathbf{Y}\right) \bmod p^2. \tag{3.8}$$

Note that $\det\left(\mathbf{x}+p\mathbf{y} \mid \mathbf{Y}\right) \equiv 0 \bmod p^2$ implies $\det\left(\mathbf{x} \mid \mathbf{Y}\right) \equiv 0 \bmod p$, which we write as $\det\left(\mathbf{x} \mid \mathbf{Y}\right) = -a_{\mathbf{x},\mathbf{Y}}p$ for some integer $a_{\mathbf{x},\mathbf{Y}}$, which is uniquely defined modulo p. Therefore, from (3.8), we conclude that

$$\det\left(\mathbf{y} \mid \mathbf{Y}\right) \equiv a_{\mathbf{x},\mathbf{Y}} \bmod p.$$

Thus, changing the order of summation, we write

$$S_{p^2}(L) = \frac{1}{p^n} \sum_{\substack{\mathbf{Y}\in\mathbb{Z}_{p^2}^{n\times(n-1)} \\ \det(\mathbf{x}|\mathbf{Y})\equiv 0 \bmod p}} \sum_{\mathbf{x}\in\mathbb{Z}_{p^2}^{n}} \mathbf{e}_{p^2}\left(\ell(\mathbf{x})) + L^*(\mathbf{Y})\right) \sum_{\substack{\mathbf{y}\in\mathbb{Z}_p^n \\ \det(\mathbf{y}|\mathbf{Y})\equiv a_{\mathbf{x},\mathbf{Y}} \bmod p}} \mathbf{e}_p\left(\ell(\mathbf{y})\right),$$

and therefore

$$|S_{p^2}(L)| \leqslant \frac{1}{p^n} \sum_{\substack{\mathbf{Y}\in\mathbb{Z}_{p^2}^{n\times(n-1)} \\ \det(\mathbf{x}|\mathbf{Y})\equiv 0 \bmod p}} \sum_{\mathbf{x}\in\mathbb{Z}_{p^2}^{n}} \left| \sum_{\substack{\mathbf{y}\in\mathbb{Z}_p^n \\ \det(\mathbf{y}|\mathbf{Y})\equiv a_{\mathbf{x},\mathbf{Y}} \bmod p}} \mathbf{e}_p\left(\ell(\mathbf{y})\right) \right|.$$

Clearly,

$$\sum_{\substack{\mathbf{Y}\in\mathbb{Z}_{p^2}^{n\times(n-1)}\\ \det(\mathbf{x}|\mathbf{Y})\equiv 0 \bmod p}} \sum_{\mathbf{x}\in\mathbb{Z}_{p^2}^{n}} 1 \leqslant p^{n^2} \sum_{\substack{\mathbf{X}\in\mathbb{Z}_{p}^{n\times n}\\ \det(\mathbf{X})\equiv 0 \bmod p}} 1 \ll p^{2n^2-1}.$$

Therefore, by the Cauchy inequality

$$\begin{aligned} S_{p^2}(L)^2 &\ll p^{2n^2-2n-1} \sum_{\substack{\mathbf{Y}\in\mathbb{Z}_{p^2}^{n\times(n-1)}\\ \det(\mathbf{x}|\mathbf{Y})\equiv 0 \bmod p}} \sum_{\mathbf{x}\in\mathbb{Z}_{p^2}^{n}} \left| \sum_{\substack{\mathbf{y}\in\mathbb{Z}_{p}^{n}\\ \det(\mathbf{y}|\mathbf{Y})\equiv a_{\mathbf{x},\mathbf{Y}} \bmod p}} \mathbf{e}_p\left(\ell(\mathbf{y})\right) \right|^2 \\ &\ll p^{2n^2-2n-1} \sum_{\substack{\mathbf{Y}\in\mathbb{Z}_{p^2}^{n\times(n-1)}\\ \det(\mathbf{x}|\mathbf{Y})\equiv 0 \bmod p}} \sum_{\mathbf{x}\in\mathbb{Z}_{p^2}^{n}} \sum_{\substack{\mathbf{y}_1\mathbf{y}_2\in\mathbb{Z}_{p}^{n}\\ \det(\mathbf{y}_1|\mathbf{Y})\equiv a_{\mathbf{x},\mathbf{Y}} \bmod p\\ \det(\mathbf{y}_2|\mathbf{Y})\equiv a_{\mathbf{x},\mathbf{Y}} \bmod p}} \mathbf{e}_p\left(\ell(\mathbf{y}_1-\mathbf{y}_2)\right). \end{aligned}$$

Writing $\mathbf{z} = \mathbf{y}_1 - \mathbf{y}_2$, we see that

$$\det(\mathbf{z} \mid \mathbf{Y}) \equiv \det(\mathbf{y}_1 \mid \mathbf{Y}) - \det(\mathbf{y}_2 \mid \mathbf{Y}) \equiv 0 \bmod p.$$

Hence changing the variables we obtain

$$\begin{aligned} S_{p^2}(L)^2 \ll p^{2n^2-2n-1} &\sum_{\substack{\mathbf{Y}\in\mathbb{Z}_{p^2}^{n\times(n-1)}\\ \det(\mathbf{x}|\mathbf{Y})\equiv 0 \bmod p}} \sum_{\mathbf{x}\in\mathbb{Z}_{p^2}^{n}} \sum_{\substack{\mathbf{y}\in\mathbb{Z}_{p}^{n}\\ \det(\mathbf{y}|\mathbf{Y})\equiv a_{\mathbf{x},\mathbf{Y}} \bmod p}} \\ &\sum_{\substack{\mathbf{z}\in\mathbb{Z}_{p}^{n}\\ \det(\mathbf{z}|\mathbf{Y})\equiv 0 \bmod p}} \mathbf{e}_p\left(\ell(\mathbf{z})\right). \end{aligned} \tag{3.9}$$

We now split the summation over $\mathbf{Y} \in \mathbb{Z}_{p^2}^{n\times(n-1)}$ into two parts depending on whether it is of full rank over $\mathbb{Z}_p$ or of rank $\operatorname{rk}_p \mathbf{Y} \leqslant n-2$.

We recall that if $\operatorname{rk}_p \mathbf{Y} \leqslant n-2$ then we have (3.7). Therefore we now derive from (3.9) that

$$S_{p^2}(L)^2 \ll p^{2n^2-2n-1} T, \tag{3.10}$$

where

$$T = \sum_{\substack{\mathbf{Y}\in\mathbb{Z}_{p^2}^{n\times(n-1)}\\ \det(\mathbf{x}|\mathbf{Y})\equiv 0 \bmod p\\ \operatorname{rk}_p \mathbf{Y}=n-1}} \sum_{\mathbf{x}\in\mathbb{Z}_{p^2}^{n}} \sum_{\substack{\mathbf{y}\in\mathbb{Z}_{p}^{n}\\ \det(\mathbf{y}|\mathbf{Y})\equiv a_{\mathbf{x},\mathbf{Y}} \bmod p}} \sum_{\substack{\mathbf{z}\in\mathbb{Z}_{p}^{n}\\ \det(\mathbf{z}|\mathbf{Y})\equiv 0 \bmod p}} \mathbf{e}_p\left(\ell(\mathbf{z})\right).$$

We note that for $\mathbf{Y} \in \mathbb{Z}_{p^2}^{n\times(n-1)}$ with $\operatorname{rk}_p \mathbf{Y} = n-1$ we have

$$\sum_{\substack{\mathbf{x}\in\mathbb{Z}_{p^2}^{n}\\ \det(\mathbf{x}|\mathbf{Y})\equiv 0 \bmod p}} 1 = p^{2n-1} \qquad \text{and} \qquad \sum_{\substack{\mathbf{y}\in\mathbb{Z}_{p}^{n}\\ \det(\mathbf{y}|\mathbf{Y})\equiv a_{\mathbf{x},\mathbf{Y}} \bmod p}} 1 = p^{n-1}$$

(since both count the number of solutions to some nontrivial linear congruences). Hence, we can simplify the formula for T as

$$T = p^{3n-2} \sum_{\substack{\mathbf{Y} \in \mathbb{Z}_{p^2}^{n\times(n-1)} \\ \mathrm{rk}_p \mathbf{Y} = n-1}} \sum_{\substack{\mathbf{z} \in \mathbb{Z}_p^n \\ \det(\mathbf{z}|\mathbf{Y}) \equiv 0 \bmod p}} \mathbf{e}_p(\ell(\mathbf{z})).$$

Next, recalling (3.7), we bring back to T the contribution from the matrices $\mathbf{Y} \in \mathbb{Z}_{p^2}^{n\times(n-1)}$ with $\mathrm{rk}_p \mathbf{Y} \leqslant n-2$. That is, we can drop the condition $\mathrm{rk}_p \mathbf{Y} = n-1$ and write

$$\begin{aligned} T &= p^{3n-2} \sum_{\mathbf{Y} \in \mathbb{Z}_{p^2}^{n\times(n-1)}} \sum_{\substack{\mathbf{z} \in \mathbb{Z}_p^n \\ \det(\mathbf{z}|\mathbf{Y}) \equiv 0 \bmod p}} \mathbf{e}_p(\ell(\mathbf{z})) \\ &= p^{3n-2} \cdot p^{n(n-1)} \sum_{\mathbf{Z} \in \mathbb{Z}_{p}^{n\times(n-1)}} \sum_{\substack{\mathbf{z} \in \mathbb{Z}_p^n \\ \det(\mathbf{z}|\mathbf{Z}) \equiv 0 \bmod p}} \mathbf{e}_p(\ell(\mathbf{z})). \end{aligned}$$

Invoking Lemma 3.4, we obtain

$$T \ll p^{3n-2} \cdot p^{n(n-1)} \cdot p^{n^2-n} = p^{2n^2+n-2}$$

and substituting this bound in (3.10), we derive the desired result. ▭

3.5. **Bounding $S_d(L)$ and $S_{d^2}(L)$.** We first combine Lemma 3.1 with the estimates from Sections 3.3 and 3.4 to derive a bound on $S_d(L)$ for an arbitrary square-free integer d.

For a linear form L as in (3.1) and an integer $m \geqslant 1$, we define $\gcd(L, m)$ as the greatest common divisor of the coefficients of L and m.

We start with an upper bound for $S_d(L)$.

Lemma 3.7. *For any square-free integer $d \geqslant 1$ and a linear form $L(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$, we have*

$$|S_d(L)| \leqslant d^{n^2+o(1)} \begin{cases} (D/d)^n & \text{if } L \text{ is a monomial,} \\ (D/d)^{(n+1)/2} & \text{otherwise,} \end{cases}$$

where $\gcd(L, d) = D$.

Proof. By Lemma 3.1, we have

$$S_d(L) = S_1 S_2, \qquad (3.11)$$

where

$$S_1 = \prod_{p \mid d/D} S_p(b_{d,p} L) \qquad \text{and} \qquad S_2 = \prod_{p \mid D} S_p(b_{d,p} L).$$

Note that if $p \mid d/D$ then $\gcd(L,p)=1$. In this case, if L is a monomial (or in fact depends only on one column), then we apply Lemma 3.4, and the bound on the divisor function (1.2), to obtain

$$|S_1| \leqslant (d/D)^{n^2-n+o(1)}. \tag{3.12}$$

If L has at least two nonzero terms, then we apply Lemma 3.5 to obtain

$$|S_1| \leqslant (d/D)^{n^2-(n+1)/2+o(1)}. \tag{3.13}$$

Next, for S_2, since p divides all coefficients of L, the form L vanishes modulo p, and thus

$$|S_2| = \prod_{p \mid D} p^{n^2} = D^{n^2}. \tag{3.14}$$

Substituting the estimates (3.12), (3.13) and (3.14) in (3.11), we derive the result. □

We proceed, following similar line of proof as above, to give a bound for $S_{d^2}(L)$.

Lemma 3.8. *For any square-free integer $d \geqslant 1$ and a linear form $L(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$, we have*

$$|S_{d^2}(L)| \leqslant d^{2n^2-(n+3)/2+o(1)} e f^{(n+3)/2}$$

for some positive square-free integers e and f with $\gcd(e,f)=1$, which are defined by $\gcd(L,d^2)=ef^2$.

Proof. As in the proof of Lemma 3.7, applying Lemma 3.1, we have

$$S_{d^2}(L) = S_1 S_2 S_3, \tag{3.15}$$

where

$$S_1 = \prod_{p \mid d/(ef)} S_{p^2}(b_{d,p}L), \quad S_2 = \prod_{p \mid e} S_{p^2}(b_{d,p}L), \quad S_3 = \prod_{p \mid f} S_{p^2}(b_{d,p}L).$$

Note that if $p \mid d/(ef)$ then $\gcd(L,p)=1$. Hence, by Lemma 3.6 and the bound on the divisor function (1.2), we obtain

$$|S_1| \leqslant (d/ef)^{2n^2-(n+3)/2+o(1)}. \tag{3.16}$$

Next, for S_2 we again use (1.2) and Lemma 3.5, to derive

$$|S_2| = \prod_{p \mid e} \left(p^{n^2} \left| S_p(b_{d,p}p^{-1}L) \right| \right) \leqslant e^{2n^2-(n+1)/2+o(1)}. \tag{3.17}$$

Finally, for S_3 we obviously have

$$S_3 = f^{2n^2}. \tag{3.18}$$

Substituting the estimates (3.16), (3.17) and (3.18) in (3.15), we derive the result. □

We use Lemma 3.8 in the following simplified form using the trivial bound $ef^{(n+3)/2} \leqslant (ef^2)^{(n+3)/4}$.

Corollary 3.9. *For any square-free integer $d \geqslant 1$ and a linear form $L(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$, we have*

$$|S_{d^2}(L)| \leqslant d^{2n^2+o(1)}(D/d^2)^{(n+3)/4},$$

where $D = \gcd(L, d^2)$.

4. Distribution of matrices

4.1. Discrepancy and the Koksma-Szüsz inequality.

We recall that the *discrepancy* $D(\Gamma)$ of a sequence $\Gamma = (\boldsymbol{\gamma}_k)_{k=1}^K$ of K points in the half-open s-dimensional unit cube $[0, 1)^s$, is defined by

$$D(\Gamma) = \sup_{\mathcal{B}\subseteq[0,1]^s} \left| \frac{A(\mathcal{B})}{K} - (\beta_1 - \alpha_1)\cdots(\beta_s - \alpha_s) \right|,$$

where the supremum is taken over all boxes

$$\mathcal{B} = [\alpha_1, \beta_1] \times \ldots \times [\alpha_s, \beta_s] \subseteq [0, 1)^s,$$

and where $A(\mathcal{B})$ is the number of elements of Γ, which fall in $\mathcal{B}$, and

$$\operatorname{vol}\mathcal{B} = (\beta_1 - \alpha_1)\cdots(\beta_s - \alpha_s)$$

is the volume of $\mathcal{B}$.

One of the basic tools in the uniformity of distribution theory is the celebrated *Koksma–Szüsz inequality* [12, 18] (see also [5, Theorem 1.21]), which links the discrepancy of a sequence of points to certain exponential sums.

Lemma 4.1. *For any integer $M \geqslant 1$, we have*

$$D(\Gamma) \ll \frac{1}{M} + \frac{1}{K} \sum_{0<\|\mathbf{m}\|\leqslant M} \frac{1}{r(\mathbf{m})} \left| \sum_{k=1}^{K} \exp\left(2\pi i\langle \mathbf{m}, \boldsymbol{\gamma}_k\rangle\right) \right|,$$

where $\langle \mathbf{m}, \boldsymbol{\gamma}_k\rangle$ denotes the inner product,

$$\|\mathbf{m}\| = \max_{j=1,\ldots,s} |m_j|, \qquad r(\mathbf{m}) = \prod_{j=1}^{s} \max\{|m_j|, 1\},$$

and the sum is taken over all vectors $\mathbf{m} = (m_1, \ldots, m_s) \in \mathbb{Z}^s$ with $0 < \|\mathbf{m}\| \leqslant M$, and the implied constant depends only on s.

4.2. **Matrices with determinants with a divisibility condition in boxes.** We introduce the following extension of $N_n(m)$ from Section 2.1.

For $H \geqslant 1$, we define

$$N_n(m; H) = \#\{A \in \mathcal{M}_n(\mathbb{Z}; H) : \ \det A \equiv 0 \bmod m\}.$$

We combine the bounds of exponential sums from Lemma 3.7 and Corollary 3.9, respectively, with Lemma 4.1 to derive asymptotic formulas for $N_n(m; H)$ in the cases when $m = d$ and $m = d^2$ for a square-free integer $d \geqslant 1$.

Lemma 4.2. *For any square-free integer $d \geqslant 1$ and any integer $H \geqslant 1$*

$$N_n(d; H) = N_n(d)\frac{(2H+1)^{n^2}}{d^{n^2}} + O\left(d^{n^2-2+1/n+o(1)}\right).$$

Proof. Let $m \geqslant 1$ be an integer and let $\mathbf{H} = (H_{ij})_{i,j=1}^n$ with some positive integers $H_{ij} < m/2$ (below we set $m = d$). We extend the definition of $N_n(m; H)$ to $N_n(m; \mathbf{H})$ which is the number of $n \times n$ matrices with

$$A = (a_{ij})_{i,j=1}^n \in \mathcal{M}_n(\mathbb{Z}), \qquad |a_{ij}| \leqslant H_{ij}, \ i, j = 1, \ldots, n,$$

and such that $\det A \equiv 0 \bmod m$.

Clearly, to establish the desired result, it is enough to show that

$$N_n(d; \mathbf{H}) = N_n(d)\frac{1}{d^{n^2}}\prod_{i,j=1}^{n}(2H_{ij}+1) + O\left(d^{n^2-2+1/n+o(1)}\right). \tag{4.1}$$

In fact we only need it when each H_{ij} is either d or H, but this does not simplify the argument.

To derive (4.7), we treat the problem of counting $N_n(d; \mathbf{H})$ as the discrepancy problem for the points $(x_{ij}/d)_{i,j=1}^n \in (\mathbb{R}/\mathbb{Z})^{n^2}$ with

$$\det (x_{ij})_{i,j=1}^n \equiv 0 \bmod d, \qquad x_{ij} \in \mathbb{Z}_d, \ i, j = 1, \ldots, n,$$

embedded in the n^2-dimensional unit torus $(\mathbb{R}/\mathbb{Z})^{n^2}$. In particular, our argument relies on Lemma 4.1, applied with $K = N_n(d)$ and with some $M \geqslant 1$, to be chosen later.

For a positive integer $M \geqslant 1$, it is convenient to define $\mathcal{L}(M)$ as the set of all nonzero linear forms $L(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$ of the form (3.1) and with coefficients in the interval $[-M, M]$.

Furthermore for L as in (3.1), we denote

$$\rho(L) = \prod_{i,j=1}^{n} \max\{|a_{ij}|, 1\}.$$

Hence, splitting each interval $[0, H_{ij})$ into intervals of length d, and applying Lemma 4.1 to count points in incomplete boxes on the boundary, we have

$$N_n(d;\mathbf{H}) = N_n(d)\frac{1}{d^{n^2}}\prod_{i,j=1}^{n}(2H_{ij}+1) + O\left(M^{-1}N_n(d)+R\right),$$

where

$$R = \sum_{L\in\mathcal{L}(M)}\frac{1}{\rho(L)}\left|S_d(L)\right|.$$

We note that Lemma 2.1 implies that

$$N_n(d) \leqslant d^{n^2}\prod_{p\mid d}\left(p^{-1}+O\left(p^{-2}\right)\right) = d^{n^2-1+o(1)}. \tag{4.2}$$

Therefore, we have

$$N_n(d;\mathbf{H}) = N_n(d)\frac{1}{d^{n^2}}\prod_{i,j=1}^{n}(2H_{ij}+1) + O\left(d^{n^2-1+o(1)}M^{-1}+R\right). \tag{4.3}$$

Next for each positive divisor $D \mid d$ we collect together the terms with $\gcd(L,d) = D$. Since $L \in \mathcal{L}(M)$, we can assume that $D \leqslant M$. We also write

$$R = R_{\mathrm{mon}} + R_{\text{non-mon}}, \tag{4.4}$$

where R_{mon} and $R_{\text{non-mon}}$ are contributions to R from monomial and non-monomial linear forms L.

Since $L \in \mathcal{L}(M)$ is a nonzero linear form, the condition $\gcd(L,d) = D$ implies that each of its non-zero coefficients is a non-zero multiple of D. It is now easy to see that

$$\sum_{\substack{L\in\mathcal{L}_d(M)\\ L \text{ monomial}\\ \gcd(L,d)=D}}\frac{1}{\rho(L)} \ll D^{-1}\log d.$$

By Lemma 3.7 and also using (1.2), this leads to the bound

$$R_{\mathrm{mon}} = d^{n^2-n+o(1)}\sum_{\substack{D\mid d\\ D\leqslant M}}D^n\sum_{\substack{L\in\mathcal{L}_d(M)\\ L \text{ monomial}\\ \gcd(L,d)=D}}\frac{1}{\rho(L)} \leqslant d^{n^2-n+o(1)}M^{n-1}. \tag{4.5}$$

Furthermore, since non-monomial linear forms have at least two non-zero coefficients, each of which is a non-zero multiple of D, we see that

$$\sum_{\substack{L\in\mathcal{L}_d(M)\\ L \text{ non-monomial}\\ \gcd(L,d)=D}}\frac{1}{\rho(L)} \ll D^{-2}(\log d)^{n^2}.$$

(the power of $\log d$ can easily be reduced). Hence, by Lemma 3.7 and (1.2) again,

$$R_{\text{non-mon}} = d^{n^2-(n+1)/2+o(1)} \sum_{\substack{D\mid d\\ D\leqslant M}} D^{(n+1)/2} \sum_{\substack{L\in\mathcal{L}_d(M)\\ L \text{ non-monomial}\\ \gcd(L,d)=D}} \frac{1}{\rho(L)} \leqslant d^{n^2-(n+1)/2+o(1)} \left(M^{(n-3)/2}+1\right). \tag{4.6}$$

Substituting the bounds (4.5) and (4.6) in (4.4) and the recalling (4.3) we arrive to

$$N_n(d;\mathbf{H}) = N_n(d)\frac{1}{d^{n^2}}\prod_{i,j=1}^{n}(2H_{ij}+1) + O\left(d^{n^2+o(1)}\mathscr{E}\right),$$

where

$$\mathscr{E} = d^{-1}M^{-1} + d^{-n}M^{n-1} + d^{-(n+1)/2}M^{(n-3)/2} + d^{-(n+1)/2}.$$

Comparing to potentially optimal values

$$M = d^{(n-1)/n} \qquad \text{and} \qquad M = d,$$

we see that the first one leads to the stronger bound

$$\mathscr{E} \ll d^{-(2n-1)/n} + d^{-(5n-3)/(2n)} + d^{-(n+1)/2} \ll d^{-(2n-1)/n} + d^{-(n+1)/2} \ll d^{-(2n-1)/n}.$$

Hence we now derive (4.1) and thus conclude the proof. □

Lemma 4.3. *For any square-free integer $d \geqslant 1$ and any integer $H \geqslant 1$*

$$N_n(d^2;H) = N_n(d^2)\frac{(2H+1)^{n^2}}{d^{2n^2}} + O\left(d^{2n^2-4(n+1)/(n+3)+o(1)}\right).$$

Proof. We follow the same path as in the proof of Lemma 4.2. In particular, we continue to use the notations $\mathbf{H} = (H_{ij})_{i,j=1}^{n}$ and $N_n(m;\mathbf{H})$ (with $m = d^2$) and observe that it is enough to show that

$$N_n(d^2;\mathbf{H}) = N_n(d^2)\frac{1}{d^{2n^2}}\prod_{i,j=1}^{n}(2H_{ij}+1) + O\left(d^{2n^2-4(n+1)/(n+3)+o(1)}\right) \tag{4.7}$$

(this time we only need it when each H_{ij} is either d^2 or H).

As in the proof of Lemma 4.2, with some $M \geqslant 1$, to be chosen later, by Lemma 4.1 we have,

$$N_n(d^2;\mathbf{H}) = N_n(d^2)\frac{1}{d^{2n^2}}\prod_{i,j=1}^{n}(2H_{ij}+1) + O\left(M^{-1}N_n(d^2) + R\right),$$

where

$$R = \sum_{L \in \mathcal{L}(M)} \frac{1}{\rho(L)} \left|S_{d^2}(L)\right|.$$

This time, instead of (4.2), Lemma 2.1 yields

$$N_n(d^2) \leqslant d^{2n^2} \prod_{p \mid d} \left(p^{-2} + O\left(p^{-3}\right)\right) \leqslant d^{2n^2-2+o(1)}. \tag{4.8}$$

Therefore, we have

$$N_n(d^2;\mathbf{H}) = N_n(d^2)\frac{1}{d^{2n^2}} \prod_{i,j=1}^{n} (2H_{ij}+1) + O\left(M^{-1}d^{2n^2-2+o(1)} + R\right). \tag{4.9}$$

Next for each positive divisor $D \mid d^2$ we collect together the terms with $\gcd(L, d^2) = D$. Since $L \in \mathcal{L}(M)$, we can assume that $D \leqslant M$.

Together with Corollary 3.9 this leads to the bound

$$R = d^{2n^2-(n+3)/2+o(1)} \sum_{\substack{D \mid d^2\\ D \leqslant M}} D^{(n+3)/4} \sum_{\substack{L \in \mathcal{L}_{d^2}(M)\\ \gcd(L,d^2)=D}} \frac{1}{\rho(L)}.$$

Since $L \in \mathcal{L}(M)$ is a nonzero linear form, the condition $\gcd(L, d^2) = D$ implies that each of its non-zero coefficients is a non-zero multiple of D. It is now easy to see that

$$\sum_{\substack{L \in \mathcal{L}(M)\\ \gcd(L,d^2)=D}} \frac{1}{\rho(L)} \ll D^{-1} (\log d)^{n^2}.$$

Again, we note that one can certainly get a more precise bound here by classifying forms by the number $\nu \geqslant 1$ of non-zero coefficients but this does not affect the final result.

Hence, by (1.2),

$$R = d^{2n^2-(n+3)/2+o(1)} \sum_{\substack{D \mid d^2\\ D \leqslant M}} D^{(n-1)/4} \leqslant M^{(n-1)/4} d^{2n^2-(n+3)/2+o(1)}.$$

Recalling (4.9), we see that

$$N_n(d^2;\mathbf{H}) = N_n(d^2)\frac{1}{d^{2n^2}} \prod_{i,j=1}^{n} (2H_{ij}+1) + O\left(M^{-1}d^{2n^2-2+o(1)} + M^{(n-1)/4} d^{2n^2-(n+3)/2+o(1)}\right).$$

Choosing $M = d^{2(n-1)/(n+3)}$, we derive (4.7) and thus conclude the proof. □

5. Proof of Theorem 1.1

5.1. **Initial split.** Let $\mu(m)$ denote the *Möbius* function, that is, we have $\mu(m) = 0$ if m is not square-free, while otherwise $\mu(m) = (-1)^s$ where s is the number of distinct prime divisors of m.

Then, by the inclusion-exclusion principle, we have

$$S_n(H) = \sum_{1 \leqslant d \leqslant \sqrt{n! H^n}} \mu(d) N_n(d^2; H).$$

In the above sum we can certainly limit the range of d via the Hadamard inequality, but this is not important for us.

We now choose a parameter Δ and split the above sums as

$$S_n(H) = \mathscr{M} + \mathscr{E}, \tag{5.1}$$

where

$$\mathscr{M} = \sum_{1 \leqslant d \leqslant \Delta} \mu(d) N_n(d^2; H) \qquad \text{and} \qquad \mathscr{E} = \sum_{\Delta < d \leqslant \sqrt{n! H^n}} \mu(d) N_n(d^2; H).$$

5.2. **Main term.** For the main term $\mathscr{M}$ we use Lemma 4.3 and write

$$\begin{aligned}\mathscr{M} &= \sum_{1 \leqslant d \leqslant \Delta} \mu(d) \left(N_n(d^2) \frac{(2H+1)^{n^2}}{d^{2n^2}} + O\left(d^{2n^2 - 4(n+1)/(n+3) + o(1)}\right)\right) \\ &= (2H+1)^{n^2} \sum_{1 \leqslant d \leqslant \Delta} N_n(d^2) \frac{\mu(d)}{d^{2n^2}} + O\left(\Delta^{2n^2 - (3n+1)/(n+3) + o(1)}\right).\end{aligned}$$

Using the bound (4.8), and extending the summation in the above sum over all $d \geqslant 1$, we obtain

$$\begin{aligned}\mathscr{M} &= (2H+1)^{n^2} \sum_{d=1}^{\infty} N_n(d^2) \frac{\mu(d)}{d^{2n^2}} \\ &\qquad + O\left(H^{n^2} \sum_{d > \Delta} d^{-2+o(1)} + \Delta^{2n^2 - (3n+1)/(n+3) + o(1)}\right) \\ &= (2H+1)^{n^2} \sum_{d=1}^{\infty} N_n(d^2) \frac{\mu(d)}{d^{2n^2}} \\ &\qquad + O\left(H^{n^2} \Delta^{-1+o(1)} + \Delta^{2n^2 - (3n+1)/(n+3) + o(1)}\right).\end{aligned}$$

Using the muliplicativity of $\mu(d)$ and $N_n(d^2)/d^{2n^2}$, and Lemma 2.1, we derive

$$\begin{aligned}\sum_{d=1}^{\infty} N_n(d^2)\frac{\mu(d)}{d^{2n^2}} &= \prod_p \left(1 - N_n(p^2)/p^{2n^2}\right)\\ &= \prod_p \left(1 - \left(1 - \prod_{j=2}^{n+1}\left(1-p^{-j}\right)\right)\right)\\ &= \prod_p \prod_{j=2}^{n+1}\left(1-p^{-j}\right) = \mathfrak{S}_n.\end{aligned}$$

Therefore,

$$\begin{aligned}\mathscr{M} &= \mathfrak{S}_n(2H+1)^{n^2}\\ &\qquad + O\left(H^{n^2}\Delta^{-1+o(1)} + \Delta^{2n^2-(3n+1)/(n+3)+o(1)}\right).\end{aligned} \tag{5.2}$$

5.3. **Error term.** To estimate the error term $\mathscr{E}$, we write

$$|\mathscr{E}| \leqslant \sum_{\Delta < d \leqslant \sqrt{n!H^n}} N_n(d^2;H),$$

and notice that

$$N_n(d^2;H) \leqslant \sum_{|a|\leqslant n!H^n/d^2} \#\left\{A \in \mathcal{M}_n(\mathbb{Z};H) :\ \det A = ad^2\right\}.$$

Hence, by Lemma 2.2 we have

$$N_n(d^2;H) \leqslant H^{n^2-n+o(1)} \sum_{|a|\leqslant n!H^n/d^2} 1 \leqslant H^{n^2+o(1)}/d^2.$$

We therefore derive

$$|\mathscr{E}| \leqslant H^{n^2+o(1)} \sum_{\Delta < d \leqslant \sqrt{n!H^n}} d^{-2} \leqslant H^{n^2+o(1)}\Delta^{-1}. \tag{5.3}$$

5.4. **Final optimisation.** Substituting (5.2) and (5.3) in (5.1), we obtain

$$S_n(H) = 2^{n^2}\mathfrak{S}_n H^{n^2} + O\left(H^{n^2}\Delta^{-1+o(1)} + \Delta^{2n^2-(3n+1)/(n+3)+o(1)} + H^{n^2-1}\right),$$

which after choosing

$$\Delta = H^{n^2(n+3)/(2n^2(n+3)-2n+2)}$$

implies the desired result.

6. Proof of Theorem 1.4

6.1. **Initial split.** We proceed similarly to the proof of Theorem 1.1. We recall the formula

$$\varphi(m) = m \sum_{d \mid m} \frac{\mu(d)}{d},$$

where, as before, $\mu(d)$ denotes the *Möbius* function, see, for example, [8, Equation (16.1.3) and Section 16.3]. Therefore, we obtain

$$\Phi_n(H) = \sum_{1 \leqslant d \leqslant \sqrt{n!H^n}} \frac{\mu(d)}{d} N_n(d; H).$$

In the above sum we can certainly limit the range of d via the Hadamard inequality, but this is not important for us.

This time instead of (5.1), for some parameter Δ, we write

$$\Phi_n(H) = \mathscr{M} + \mathscr{E}, \tag{6.1}$$

where

$$\mathscr{M} = \sum_{1 \leqslant d \leqslant \Delta} \frac{\mu(d)}{d} N_n(d; H) \qquad \text{and} \qquad \mathscr{E} = \sum_{\Delta < d \leqslant n!H^n} \frac{\mu(d)}{d} N_n(d; H).$$

6.2. **Main term.** For the main term $\mathscr{M}$ we use Lemma 4.2 and write

$$\begin{aligned} \mathscr{M} &= \sum_{1 \leqslant d \leqslant \Delta} \mu(d) \left(N_n(d) \frac{(2H+1)^{n^2}}{d^{n^2+1}} + O\left(d^{n^2-2+1/n+o(1)}\right)\right) \\ &= (2H+1)^{n^2} \sum_{1 \leqslant d \leqslant \Delta} N_n(d) \frac{\mu(d)}{d^{n^2+1}} + O\left(\Delta^{n^2-1+1/n+o(1)}\right). \end{aligned}$$

Using the bound (4.2), and extending the summation in the above sum over all $d \geqslant 1$, we obtain

$$\begin{aligned} \mathscr{M} &= (2H+1)^{n^2} \sum_{d=1}^{\infty} N_n(d) \frac{\mu(d)}{d^{n^2+1}} \\ &\qquad\qquad + O\left(H^{n^2} \sum_{d > \Delta} d^{-2+o(1)} + \Delta^{n^2-1+1/n+o(1)}\right) \\ &= (2H+1)^{n^2} \sum_{d=1}^{\infty} N_n(d) \frac{\mu(d)}{d^{n^2+1}} + O\left(H^{n^2} \Delta^{-1+o(1)} + \Delta^{n^2-1+1/n+o(1)}\right). \end{aligned}$$

Using the muliplicativity of $\mu(d)$ and $N_n(d)/d^{n^2+1}$, and Lemma 2.1, we derive

$$\begin{aligned}\sum_{d=1}^{\infty} N_n(d)\frac{\mu(d)}{d^{n^2+1}} &= \prod_p \left(1 - N_n(p)/p^{n^2+1}\right)\\ &= \prod_p \left(1 - \frac{1}{p}\left(1 - \prod_{j=1}^{n}\left(1-p^{-j}\right)\right)\right)\\ &= \prod_p \left(1-\frac{1}{p}\right)\left(1+\frac{1}{p}\prod_{j=2}^{n}\left(1-p^{-j}\right)\right) = \sigma_n.\end{aligned}$$

Therefore,

$$\mathscr{M} = \sigma_n(2H+1)^{n^2} + O\left(H^{n^2}\Delta^{-1+o(1)} + \Delta^{n^2-1+1/n+o(1)}\right). \qquad (6.2)$$

6.3. **Error term.** As in Section 5.3, using that by Lemma 2.2 we have

$$N_n(d;H) \leqslant H^{n^2-n+o(1)} \sum_{|a|\leqslant n!H^n/d} 1 \leqslant H^{n^2+o(1)}/d,$$

we derive

$$|\mathscr{E}| \leqslant H^{n^2+o(1)} \sum_{\Delta<d\leqslant n!H^n} d^{-2} \leqslant H^{n^2+o(1)}\Delta^{-1}. \qquad (6.3)$$

6.4. **Final optimisation.** Substituting (6.2) and (6.3) in (6.1), we obtain

$$\varPhi_n(H) = 2^{n^2}\sigma_n H^{n^2} + O\left(H^{n^2}\Delta^{-1+o(1)} + \Delta^{n^2-1+1/n+o(1)} + H^{n^2-1}\right),$$

which after choosing

$$\Delta = H^{n^3/(n^3+1)}$$

implies the desired result.

Acknowledgement

The authors would like to thank Alan Haynes for pointing out at a recurring oversight in the initial version of this paper and also the referees for the very careful reading and helpful comments.

This work was supported, in part, by the Australian Research Council Grants DP200100355 and DP230100530. A.O. gratefully acknowledges the hospitality and support of the Max Planck Institute for Mathematics and Institut des Hautes Études Scientifiques, where her work has been carried out.

References

[1] S. S. Abhyankar, 'Combinatoire des tableaux de Young, variétés déterminantielles et calcul de fonctions de Hilbert', *Rend. Sem. Mat. Univ. Politec. Torino*, **42** (1984), 65–88. 3

[2] R. P. Brent and B. D. McKay, 'Determinants and ranks of random matrices over $\mathbb{Z}_m$', *Discrete Math.*, **66** (1987), 35–49. 5

[3] T. Browning, W. Sawin, V. Wang, 'Pairs of commuting integer matrices', *Math. Ann.*, **393** (2025), 1863–1880. 3

[4] K. Destagnol and E. Sofos, 'Rational points and prime values of polynomials in moderately many variables', *Bull. Sci. Math.*, **156** (2019), Art. 102794. 2

[5] M. Drmota and R. F. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997. 16

[6] W. Duke, Z. Rudnick and P. Sarnak, 'Density of integer points on affine homogeneous varieties', *Duke Math. J.*, **71** (1993), 143–179. 5, 6

[7] E. Fouvry, 'Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums', *Isr. J. Math.*, **120** (2000), 81–96. 3, 7

[8] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979. 23

[9] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004. 5, 6

[10] N. M. Katz, 'Estimates for "singular" exponential sums', *Intern. Math. Res. Notices*, **1999** (1999), 875–899. 3

[11] Y. R. Katznelson, 'Singular matrices and a uniform bound for congruence groups of $\mathrm{SL}_n(\mathbb{Z})$', *Duke Math. J.*, **69** (1993), 121–136. 3, 5

[12] J. F. Koksma, 'Some theorems on Diophantine inequalities', *Math. Centrum Scriptum no. 5*, Amsterdam, 1950. 16

[13] G. Kotsovolis and K. Woo, 'Prime number theorems for polynomials from homogeneous dynamic', *Geom. Func. Analysis*, **35** (2025), 1169–1221. 2

[14] V. Kovaleva, 'On the distribution of equivalence classes of random symmetric p-adic matrices', *Mathematika*, **69** (2023), 903–933. 2

[15] B. Poonen, 'Squarefree values of multivariable polynomials', *Duke Math. J.*, **118** (2003), 353–373. 2

[16] T. Reuss, Power-free values of polynomials. *Bull. London Math. Soc.*, **47** (2015), 270–284. 2

[17] I. E. Shparlinski, 'Some counting questions for matrices with restricted entries', *Lin. Algebra Appl.*, **432** (2010), 155–160. 6

[18] P. Szüsz, 'On a problem in the theory of uniform distribution', *Comptes Rendus Premier Congrès Hongrois*, Budapest, 1952, 461–472 (in Hungarian). 16

School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia

Email address: alina.ostafe@unsw.edu.au

School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia

Email address: igor.shparlinski@unsw.edu.au