Mathematical Proceedings of the Cambridge Philosophical Society

VOL. 181 JULY 2026 PART 1

Math. Proc. Camb. Phil. Soc. (2026), **181**, 743–750

doi: 10.1017/S0305004126101881

First published online 25 March 2026

Counting 2×2 matrices with fixed determinant and bounded coefficients†

BY KAVITA DHANDA, ALAN HAYNES AND SILMI PRASALA

Department of Mathematics, University of Houston, Houston, TX, United States

e-mails: kkavita@cougarnet.uh.edu, haynes@math.uh.edu, szprasal@cougarnet.uh.edu

(*Received* 24 *September* 2025*; revised* 15 *January* 2026*; accepted* 15 *January* 2026)

Abstract

Recent work by M. Afifurrahman established the first asymptotic estimates with error terms for the number of 2×2 matrices with fixed non-zero determinant $n \in \mathbb{N}$, and with coefficients bounded in absolute value by X. In this paper we present a new proof of this result, which also gives an improved error term as $X \to \infty$. Similar to Afifurrahman's result, our error term is uniform in both n and X, and our estimates are significant for X as small as $n^{1/2+\delta}$. To complement this, we also demonstrate that the exponent $1/2 + \delta$ in this statement cannot be reduced, by establishing a result which gives a different asymptotic main term when n is either a prime or the square of a prime, and when $X = n^{1/2}$.

2020 Mathematics Subject Classification: 11D45 (Primary); 11D04, 11N45 (Secondary)

1. *Introduction*

It is a well-studied problem to estimate the number $S_{k,\|\cdot\|}(n, X)$ of $k \times k$ matrices A with integer coefficients, $\det(A) = n$, and $\|A\| \leq X$, where $k \geq 2$, $n \in \mathbb{Z}$, $X \geq 1$, and $\|\cdot\|$ is a prescribed norm. For the Euclidean norm $\|\cdot\|_2$, a famous result of Selberg from the 1970's

†Research supported by a Summer Undergraduate Research Fellowship (SURF) from the University of Houston.

on the hyperbolic circle problem (see Selberg's unpublished notes [17, p. 5 of document 3]) gives that

$$S_{2,\|\cdot\|_2}(1,X) = 6X^2 + O_\epsilon\left(X^{4/3+\epsilon}\right),$$

for any $\epsilon > 0$.

In 1993 Duke, Rudnick and Sarnak published a landmark paper on the density of integer points on affine homogeneous varieties [6]. As one application of their results they proved (theorem 1.10 in their paper) that, for any $k \geq 2$ and for any $n \neq 0$,

$$S_{k,\|\cdot\|_2}(n,X) = c_{k,n}X^{k^2-k} + O_{n,\epsilon}\left(X^{k^2-k-1/(k+1)+\epsilon}\right), \tag{1·1}$$

for any $\epsilon > 0$, where $c_{k,n}$ is a constant determined by values of the gamma function, the Riemann zeta function, and the prime power divisors of n.

Analogous results for the case when $n = 0$ were established by Katznelson in [11] (cf. [12]). These types of problems were further investigated, using tools from ergodic theory, by Eskin, Mozes and Shah [7, 18], who proved asymptotic formulas for numbers of matrices with bounded Euclidean norm and specified characteristic polynomial.

Surprisingly, the asymptotic behavior of $S_{k,\|\cdot\|_\infty}(n,X)$, where $\|\cdot\|_\infty$ is the sup-norm, has been less well studied, even in the case when $k = 2$, until recently. The above mentioned work of Selberg, Duke, Rudnick and Sarnak relies on the rotational invariance of the Euclidean norm, and therefore does not apply to this problem. Asymptotic formulae for $S_{2,\|\cdot\|_\infty}(0,X)$ (with second order asymptotics) can be derived from work of Ayyad, Cochrane and Zhang [2]. There is an asymptotic formula for $S_{2,\|\cdot\|_\infty}(1,X)$ due to Roettger [16] (who also considers an analogous problem over rings of integers of algebraic number fields), as well as more recent work of Bulinski and Shparlinski [3], which leads to an improved error term (see [1, equation (1·4)]). A 'smoothed' version of the sup-norm problem for $k = 2$ and arbitrary n (actually for 2×2 matrices with a fixed characteristic polynomial) is considered in [9], however adding smooth weights in the count does change the problem.

Significant progress on this problem was made by M. Afifurrahman, who in July 2024 published a preprint containing a proof of the following result.

THEOREM [1, theorem 1·1]. *For $n \in \mathbb{N}$,*

$$S_{2,\|\cdot\|_\infty}(n,X) = \frac{96\sigma_{-1}(n)}{\pi^2}X^2 + O\left(X^{o(1)}\max\left\{X^{5/3}, n\right\}\right), \tag{1·2}$$

as $X, n \to \infty$.

In the statement of the theorem, $\sigma_s(n)$ denotes the sum of the sth powers of the positive divisors of n. One important feature of this result is that, in contrast to (1·1), the dependence on n of the error term here is made explicit, so that both X and n may tend to infinity as functions of one another. This is necessary for some applications (cf. [19, theorem 4], [15, section 2·2]), and the theorem is significant for X even as small as $n^{1/2+\delta}$. For the case of large X, a preprint of Ganguly and Guria [8] improves the error term in this theorem to $\ll_\epsilon n^\theta X^{3/2+\epsilon}$ (where θ is a non-negative constant), in the range where $X \gg n^3$.

Our first aim in this paper is to give a short proof of the following theorem.

THEOREM 1. *Let $\epsilon > 0$. Then, for $n \in \mathbb{N}$ and $X \geq 1$ we have that*

$$S_{2,\|\cdot\|_\infty}(n,X) = \frac{96\sigma_{-1}(n)}{\pi^2}X^2 + O_\epsilon\left(\sigma_0(n)X\log X + nX^\epsilon\right).$$

https://doi.org/10.1017/S0305004126101881 Published online by Cambridge University Press

The bound in our theorem recovers the error term from (1·2) when X is small compared to n, but it gives a significant power savings (over both that result and the one in [8]) when $X \gg n$. To understand the dependence of the error term on n, note that

$$\limsup_{n\to\infty} \frac{\log \sigma_0(n)}{\log n/\log\log n} = \log 2,$$

while

$$\sum_{n\le N} \sigma_0(n) = N\log N + O(N).$$

In other words, $\sigma_0(n)$ behaves on average like $\log n$, but it can also sometimes be larger than $2^{\xi \log n/\log\log n}$, for any $\xi < 1$ (see [10, theorems 317, 320]).

As in Afifurraman's result, our error term allows one to obtain significant estimates for X as small as $n^{1/2+\delta}$. It turns out that this is the threshold of what one could hope for in the exponent, as demonstrated by our second result.

THEOREM 2. *For all prime numbers p we have that*

$$S_{2,\|\cdot\|_\infty}(p, p^{1/2}) = 4\left(\frac{12}{\pi^2} - 1\right)p + O\big(p^{1/2}\log p\big),$$

and that

$$S_{2,\|\cdot\|_\infty}(p^2, p) = 4\left(\frac{12}{\pi^2} - 1\right)p^2 + O\left(p\log p\right).$$

Note that the constant on the main term in these formulas is different from that in Theorem 1. This shows, in particular, that the main term in Theorem 1 does not give a correct asymptotic estimate, as $n\to\infty$, with $X = n^{1/2}$. As pointed out to us by one of the referees, this theorem is also related to the problem of counting directions determined by subsets of a finite field, as discussed in [14]. In particular, Theorem 2 significantly improves the error term in [14, theorem 1·11] in the special case, in the statement of that theorem, when $\lambda = 1$.

Results similar to Theorem 2 for higher powers of primes do not seem to follow from the same types of arguments given in our proof. This is a direction for further investigation, which was the initial motivation for the research leading to the results in this paper, and which is closely related to a natural analogue of the 'minimal denominator problem' in the setting of p-adic numbers (see [5, 13, 20]).

Notation. We use O and $\ll$ to denote the standard big-oh and Vinogradov notations. If a and q are integers then we write (a, q) for the gcd of a and q. The symbols φ, μ, ω, and ζ denote the Euler phi, Möbius, prime omega, and Riemann zeta functions, respectively. For $n\in\mathbb{N}$, $\sum_{d|n}$ denotes a sum over positive divisors d of n. For $x\in\mathbb{R}$, we write $\lfloor x\rfloor$ for the greatest integer less than or equal to x and $\{x\} = x - \lfloor x\rfloor$ for the fractional part of x.

2. *Proof of Theorem 1*

To understand the general strategy, our proof can be divided into 3 elementary steps:

(i) make use of symmetry in the variables a, b, q, and r, in the equation

$$ar - bq = n, \tag{2·1}$$

https://doi.org/10.1017/S0305004126101881 Published online by Cambridge University Press

to reduce the problem to solving the equation under the additional constraint that $|r| \leq |q|$. Although this is close to trivial, it paves the way for one of the most important steps in the proof later on;

(ii) separate out consideration of the resulting sums, depending on the gcd of q and n. This allows us to more carefully count solutions of the linear Diophantine equation (2·1), with variables in the prescribed ranges;

(iii) evaluate the final summations using results from elementary analytic number theory. One of the key steps here is the exact formula for the inner sum in (2·5), which is a direct result of the symmetry imposed in step (i).

First note that it is sufficient to prove the theorem for $X \in \mathbb{N}$, since interpolating between integers in the main term adds an error of at most $O(\sigma_{-1}(n)X)$. For $n \in \mathbb{Z}$ and $X \in \mathbb{N}$, write:

$$\begin{aligned} S(n,X) &= S_{2,\|\cdot\|_\infty}(n,X); \\ S_{leq}(n,X) &= \left\{(a,b,q,r) \in \mathbb{Z}^4 : |a|,|b|,|q| \leq X, |r| \leq |q|, ar - bq = n\right\}; \text{and} \\ S_{eq}(n,X) &= \left\{(a,b,q,r) \in \mathbb{Z}^4 : |a|,|b|,|q| \leq X, |r| = |q|, ar - bq = n\right\}. \end{aligned}$$

Then:

$$\begin{aligned} &S(n,X) = S(-n,X), S_{leq}(n,X) = S_{leq}(-n,X); \text{and} \\ &S(n,X) = S_{leq}(n,X) + S_{leq}(-n,X) - S_{eq}(n,X) \\ &\qquad = 2S_{leq}(n,X) - S_{eq}(n,X). \end{aligned} \tag{2·2}$$

For $n \in \mathbb{N}$ we have that

$$S_{leq}(n,X) = \sum_{d|n} S_d,$$

where

$$S_d = \sum_{\substack{|q| \leq X \\ (q,n)=d}} \sum_{\substack{|a|,|b| \leq X \\ |r| \leq |q| \\ ar-bq=n}} 1.$$

For the remainder of the proof we will simplify notation by writing $q_d = q/d, n_d = n/d, X_d = X/d$, and so on. First of all we have that

$$S_d = \sum_{\substack{|q_d| \leq X_d \\ (q_d,n_d)=1}} \sum_{\substack{|a|,|b| \leq X \\ |r| \leq d|q_d| \\ ar-bdq_d=n}} 1. \tag{2·3}$$

Note that, in order to have $ar - bq = n$, it is necessary that $(a,q)|n$, which implies that $(a,q)|d$. Furthermore, if $(a,q) = e$, for some $e|d$, then it must be the case that $\frac{d}{e}|r$. This means that (2·3) is equal to

$$\sum_{\substack{|q_d| \leq X_d \\ (q_d,n_d)=1}} \sum_{e|d} \sum_{\substack{|a| \leq X \\ (a,q)=e}} \sum_{\substack{|r| \leq |q| \\ \frac{d}{e}|r}} \sum_{\substack{|b| \leq X \\ a_e r_{d/e} - bq_d = n_d}} 1.$$

https://doi.org/10.1017/S0305004126101881 Published online by Cambridge University Press

The condition that $(a, q) = e$ guarantees that $(a_e, q_d) = 1$. Once q, a, and r are chosen in the sums above, the equation $a_e r_{d/e} - bq_d = n_d$ will have a solution $|b| \le X$ (which obviously then must be unique) if and only if $r_{d/e} = n_d a_e^{-1} \bmod q_d$ and

$$\left| \frac{a_e r_{d/e} - n_d}{q_d} \right| \le X. \tag{2·4}$$

Therefore

$$S_d = \sum_{\substack{|q_d| \le X_d \\ (q_d, n_d)=1}} \sum_{e|d} \sum_{\substack{|a_e| \le X_e \\ (a_e, q_e)=1}} \sum_{\substack{|r_{d/e}| \le |q_{d/e}| \\ r_{d/e} = n_d a_e^{-1} \bmod q_d \\ (2·4) \text{ holds}}} 1.$$

Now let us consider the effect of removing condition (2·4) from the inner sum. First, note that the conditions $|a_e| \le X_e$ and $|r_{d/e}| \le |q_{d/e}|$ already guarantee that

$$\frac{a_e r_{d/e} - n_d}{|q_d|} \le X.$$

For the other inequality, suppose that q_d and e are chosen, that $r_{d/e} = n_d a_e^{-1} \bmod q_d$, and that

$$\frac{a_e r_{d/e} - n_d}{|q_d|} < -X.$$

Then we have that $a_e r_{d/e} = n_d \bmod q_d$ and that

$$-|q_d| X \le a_e r_{d/e} < -|q_d| X + n_d.$$

Using the assumption that $X \in \mathbb{N}$, we have that the number of choices for the integer $c = a_e r_{d/e}$ is equal to $\lfloor n_d / |q_d| \rfloor$. For each such integer c the number of different values of a_e and $r_{d/e}$ with $c = a_e r_{d/e}$ is at most

$$\sigma_0(c) \ll_\epsilon (|q_d| X)^\epsilon .$$

Therefore

$$S_d = M_d + E_d,$$

with

$$M_d = \sum_{\substack{|q_d| \le X_d \\ (q_d, n_d)=1}} \sum_{e|d} \sum_{\substack{|a_e| \le X_e \\ (a_e, q_e)=1}} \sum_{\substack{|r_{d/e}| \le |q_{d/e}| \\ r_{d/e} = n_d a_e^{-1} \bmod q_d}} 1 \tag{2·5}$$

$$= \sum_{\substack{|q_d| \le X_d \\ (q_d, n_d)=1}} \sum_{e|d} 2e \left(\frac{2X_e \varphi(q_e)}{|q_e|} + O\big(2^{\omega(q_e)}\big) \right) \tag{2·6}$$

$$= 4X \sum_{e|d} \sum_{\substack{|q| \le X \\ (q,n)=d}} \frac{\varphi(q/e)}{|q/e|} + O\left(\sum_{e|d} e \sum_{\substack{|q| \le X \\ (q,n)=d}} 2^{\omega(q/e)} \right) \tag{2·7}$$

https://doi.org/10.1017/S0305004126101881 Published online by Cambridge University Press

and

$$E_d \ll_\epsilon \sum_{\substack{|q_d|\le X_d \\ (q_d,n_d)=1}} \sum_{e|d} \frac{n_d}{|q_d|} (|q_d|X)^\epsilon \ll_\epsilon \frac{\sigma_0(d)}{d^{1+\epsilon}} \left(nX^{2\epsilon}\right). \tag{2·8}$$

To be clear, we are using the fact that the inner sum in (2·5) is exactly equal to $2e$, and in (2·6)-(2·8) we are also using standard asymptotic estimates for arithmetical functions. Now we consider the sum of these quantities over divisors of n. For the main term in (2·7) we have that

$$\begin{aligned}\sum_{d|n} \left(4X \sum_{e|d} \sum_{\substack{|q|\le X \\ (q,n)=d}} \frac{\varphi(q/e)}{|q/e|} \right) &= 4X \sum_{e|n} \sum_{\substack{|q|\le X \\ e|q}} \frac{\varphi(q/e)}{|q/e|} \\ &= 4X \sum_{e|n} \sum_{|q_e|\le X_e} \frac{\varphi(q_e)}{|q_e|} \\ &= \frac{48\sigma_{-1}(n)}{\pi^2} X^2 + O\left(\sigma_0(n) X \log X\right).\end{aligned}$$

For the error term in (2·6) we have that

$$\sum_{d|n} \sum_{e|d} e \sum_{\substack{|q|\le X \\ (q,n)=d}} 2^{\omega(q/e)} = \sum_{e|n} e \sum_{|q_e|\le X_e} 2^{\omega(q_e)} \ll \sigma_0(n) X \log X.$$

For the sum of the E_d error terms, adjusting the choice of ϵ above and the corresponding constant, we obtain

$$\sum_{d|n} E_d \ll_\epsilon nX^\epsilon.$$

Finally, it is easy to show that $S_{eq}(n, X) \ll \sigma_0(n)X$. Combining these estimates in formula (2·2) completes the proof of the theorem.

3. *Proof of Theorem 2*

First consider the following basic lemma.

LEMMA 3. *Let p be prime and suppose that $n = p$ or that $n = p^2$. For every integer c satisfying $0 \le c < n$, there exist integers a and q satisfying $|a| \le n^{1/2}$, $0 < q < n^{1/2}$, and*

$$aq^{-1} = c \bmod n.$$

Proof. Let

$$\mathcal{A} = \left\{(b, r) : 0 \le b \le n^{1/2}, 0 \le r < n^{1/2}\right\}.$$

It is easy to check that, whether $n = p$ or p^2,

$$|\mathcal{A}| \ge n + 1.$$

https://doi.org/10.1017/S0305004126101881 Published online by Cambridge University Press

Therefore, by the Dirichlet pigeonhole principle, there are distinct $(a_1, q_1), (a_2, q_2) \in \mathcal{A}$ with

$$a_1 - q_1 c = a_2 - q_2 c \bmod n.$$

Take $a = a_1 - a_2$ and $q = q_1 - q_2$ and assume without loss of generality, by switching the signs if necessary, that $q \geq 0$. If $q = 0 \bmod p$ then, since $q < n^{1/2} \leq p$, it must be the case that $q = 0$. Since $|a| \leq n^{1/2}$, this forces $a = 0$ as well, which is a contradiction. Therefore $q > 0$, and it is invertible modulo n, which completes the proof of the lemma.

Let us continue to write $n = p$ or p^2, depending on which of the two cases in the statement of Theorem 2 is being considered. Define $\Omega \in \mathbb{Z}^2$ by

$$\Omega = \left\{(a, q) \in \mathbb{Z}^2 : |a| \leq n^{1/2}, 0 < q < n^{1/2}, (a, q) = 1\right\},$$

and define $T : \Omega \to (\mathbb{Z}/n\mathbb{Z})$ by

$$T(a, q) = aq^{-1} \bmod n.$$

It is easy to see from Lemma 3 that the map T is surjective. Distinct points $(a, q), (b, r) \in \Omega$ will have the same image under T if and only if $ar - bq = \pm n$. It follows from this that every point in $\mathbb{Z}/n\mathbb{Z}$ is the image of either one or two points in the domain, and that

$$n = |\Omega| - \#\{((a, q), (b, r)) \in \Omega \times \Omega : ar - bq = n\}.$$

Finally, by considering the maps $(a, q) \leftrightarrow (-a, -q)$ and $(b, r) \leftrightarrow (-b, -r)$ (which require also mapping n to $-n$, but do not change the quantities we are counting), and by subtracting off contributions along the boundaries of the regions, we have that

$$\begin{aligned} S_{2,\|\cdot\|_\infty}(n, \sqrt{n}) &= 4\#\{((a, q), (b, r)) \in \Omega \times \Omega : ar - bq = n\} + O\left(n^{1/2}\right) \\ &= 4\left(|\Omega| - n\right) + O(n^{1/2}) \\ &= 4\left(\frac{12}{\pi^2} - 1\right) n + O(n^{1/2} \log n). \end{aligned}$$

This completes the proof of the theorem.

Acknowledgements. We would like to thank the anonymous referees for their careful reading of this paper and their suggestions for improvements. We would also like to mention that, a few days after our paper was first made public on arxiv.org, a similar collection of results was posted by Chapman and Mudgal [4].

REFERENCES

[1] M. Afifurrahman. A uniform formula on the number of integer matrices with given determinant and height. *J. Number Theory* **281** (2026), 741–770.
[2] A. Ayyad, T. Cochrane and Z. Zheng. 'The congruence $x_1x_2 = x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$, and mean values of character sums'. *J. Number Theory* **59** (1996), 398–413.
[3] K. Bulinski, I. E. Shparlinski. Counting elements of the congruence subgroup. *Canad. Math. Bull.* **67**(4) (2024), 955–969.
[4] J. Chapman, A. Mudgal. Counting 2×2 integer matrices with a given determinant. *Preprint*: arxiv:2509.20259.
[5] H. Chen and A. K. Haynes. Expected value of the smallest denominator in a random interval of fixed radius. *Int. J. Number Theory* **19**(6) (2023), 1405–1413.

https://doi.org/10.1017/S0305004126101881 Published online by Cambridge University Press

[6] W. D. DUKE, Z. RUDNICK and P. C. SARNAK. Density of integer points on affine homogeneous varieties. *Duke Math. J.* **71**(1) (1993), 143–179.
[7] A. ESKIN, S. MOZES and N. A. SHAH. Unipotent flows and counting lattice points on homogeneous varieties. *Ann. of Math.* (2) **143**(2) (1996), 253–299.
[8] S. GANGULY and R. GURIA. Lattice points on determinant surfaces and the spectrum of the automorphic Laplacian. 4, *Preprint*: arXiv:2410.04637.
[9] R. GURIA. Counting 2×2 integer matrices with fixed trace and determinant. *J. Ramanujan Math. Soc.* **39**(3) (2024), 219–224.
[10] G. H. HARDY and E. M. WRIGHT. *An introduction to the theory of numbers*, sixth edition, Oxford Univ. Press, Oxford, 2008.
[11] Y. R. KATZNELSON. Singular matrices and a uniform bound for congruence groups of $SL_n(\mathbf{Z})$. *Duke Math. J.* **69**(1) (1993), 121–136.
[12] Y. R. KATZNELSON. Integral matrices of fixed rank. *Proc. Amer. Math. Soc.* **120**(3) (1994), 667–675.
[13] J. MARKLOF. Smallest denominators. *Bull. London Math. Soc.* **56**(6) (2024), 1920–1938.
[14] G. G. MARTIN, E. P. WHITE and C. H. YIP. Asymptotics for the number of directions determined by $[n] \times [n]$ in $\mathbb{F}_p^2$. *Mathematika* **68**(2) (2022), 511–534.
[15] A. OSTAFE, I. E. SHPARLINSKI. Counting integer matrices with square free determinants. *Preprint*: arXiv:2503.13768v1, (2025).
[16] C. ROETTGER. Counting invertible matrices and uniform distribution. *J. Théor. Nombres Bordeaux* **17**(1) (2005), 301–322.
[17] A. SELBERG. Equidistribution in discrete groups and the spectral theory of automorphic forms, unpublished note. Available at: http://publications.ias.edu/selberg/section/2491 (1970s).
[18] N. A. SHAH. Counting integral matrices with a given characteristic polynomial. *Sankhya Ser. A* **62**(3) (2000), 386–412.
[19] I. E. SHPARLINSKI. Some counting questions for matrices with restricted entries. *Linear Algebra Appl.* **432**(1) (2010), 155–160.
[20] I. E. SHPARLINSKI. Rational numbers with small denominators in short intervals. *Arch. Math. (Basel)* **122**(6) (2024), 629–637.