A uniform formula on the number of integer matrices with given determinant and height

Muhammad (Afif) Afifurrahman

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

Universitas Gadjah Mada, Yogyakarta, Indonesia, 3 February 2025

Counting integer matrices

- Consider a set of matrices $\mathcal{M}$. We would like to count the *arithmetic statistics* of $\mathcal{M}$; e.g. the number of matrices in $\mathcal{M}$ with a given rank, determinant, or characteristic polynomial.
- There have been a lot of works on the *arithmetic statistics* of matrices in $\mathcal{M}_n(\mathbb{Z}; H)$, the set of $n \times n$ integer matrices with entries bounded by H in absolute value.
- For general n, Katznelson (1993), Duke-Rudnick-Sarnak (1994), and Shparlinski (2010) gave bounds on the number of matrices in $\mathcal{M}_n(\mathbb{Z}; H)$ with a given determinant Δ.
- However, only Shparlinski's result is uniform with respect of H and Δ.
- We will present a uniform improvement for the last result in the case $n = 2$.

Notes on notations

- We are interested in obtaining the main term of the formulae.
- We use the notation

$$U = O(V) \iff |U| \leq cV$$

for some positive constant c. Also,

$$U = O(V) \quad \text{and} \quad V = O(U) \iff U \asymp V.$$

- We also write $U = V^{o(1)}$ if, for a fixed $\varepsilon > 0$, $V^{-\varepsilon} \leq U \leq V^{\varepsilon}$ for sufficiently big V.

Previous results: general n

$$D_n(H, \Delta) = \#\{A \in \mathcal{M}_n(\mathbb{Z}; H) \mid \det A = \Delta\}.$$

Katznelson (1993) and Duke-Rudnick-Sarnak (1994)'s results imply that, asymptotically,

$$D_n(H, \Delta) \asymp \begin{cases} H^{n^2-n}, & \text{if } \Delta \neq 0, \\ H^{n^2-n} \log H, & \text{if } \Delta = 0. \end{cases}$$

However, their results were in a different setting (the matrices are ordered according to ℓ_2 norm).
Thus, their results are not uniform with respect of H.
The best uniform bound (for "any" Δ) is from Shparlinski, who proved

$$D_n(H, \Delta) = O(H^{n^2-n} \log H).$$

The main obstacle: there are n^2 variables.

For $n = 2$, we only have four variables, with corresponding equation

$$ad - bc = \Delta,$$

with $0 \leq |a|, |b|, |c|, |d| \leq H$. More results are known in this case for particular values of Δ.
For $\Delta = 0$, a quick corollary from Ayyad-Cochrane-Zhang (1996) can be used to obtain

$$D_2(H, 0) = \frac{96}{\pi^2} H^2 \log H + CH^2 + O(H^{19/13} \log^{7/13} H),$$

with C an explicit constant.
The asymptotics for $\Delta = 1$ is known to Selberg and Newman. Then, Bulinski and Shparlinski (2022) prove

$$D_2(H, 1) = \frac{96}{\pi^2} H^2 + O(H^{5/3+o(1)}).$$

In fact, they proved results on the cardinalities of intersections between modular subgroups of $SL_2(\mathbb{Z})$ with $\mathcal{M}_2(\mathbb{Z}; H)$.

The main result

We now consider the problem for general Δ, uniformly.

MA (2024+)

Fix an integer $\Delta \neq 0$. As $H \to \infty$, we have

$$D_2(H, \Delta) = \frac{96}{\pi^2} H^2 \frac{\sigma(|\Delta|)}{|\Delta|} + O(H^{5/3+o(1)}),$$

where $\sigma(n)$ denotes the sum of all positive divisors of n.

We actually proved a stronger result for a fixed Δ and H. The main steps:

- Algebraic manipulations and case divisions.
- A result from Ustinov (2009) on counting points on a modular hyperbola.
- New lemmas on some summations.

Preliminary algebraic manipulation

After some algebraic manipulations, we may instead count the number of integer solutions to

$$ad - b\mathbf{c} = \Delta,$$

with $0 < a, |b|, c, d \leq H$ and a fixed $\Delta > 0$. In particular, all variables are nonzero and, except b, positive.
If we fix $c \in [1, H]$, the problem is equivalent to

$$ad \equiv \Delta \pmod{\mathbf{c}},$$

with a, d, and $\frac{ad - \Delta}{c} = b$ bounded. This problem is closely related to counting points on a **modular hyperbola**.

Counting points on a modular hyperbola

For a function f and integers U, V, K, $q \geq 1$, we would like to count the number of integer solutions (u, v) of

$$uv \equiv K \pmod{q}$$

with $U < u \leq U + X$ and $0 < v \leq f(u)$. This is the problem of counting points on a **modular hyperbola** defined by the function f.

Ustinov provides a general result for $T_f(K, q; U, X)$, the number of solutions of $uv \equiv K \pmod{q}$, with $U < u \leq U + X$ and $0 < v \leq f(u)$.

Ustinov (2009)

Assume f's second derivative satisfies some bounds. We have

$$T_f(K, q; U, X) = \frac{1}{q} \sum_{r|K} \sum_{\substack{U<u\leq U+X \\ \gcd(u,q)=r}} rf(u) - \frac{X\delta_q(K)}{2} + E,$$

where

$$|E| \leq q^{o(1)}(XL^{-1/3} + q^{-1}D^{1/2}L^{1/2} + q^{1/2} + D),$$

with $D = \gcd(K, q)$.

If f is a constant function, the corresponding region is a **modular rectangle**, for which we have better results.

Case divisions

We need to count the number of integral points of

$$ad \equiv \Delta \pmod{c},$$

with $0 < a, d \leq H$ and

$$-H \leq \frac{ad - \Delta}{c} \leq H \iff \frac{\Delta - Hc}{a} \leq d \leq \frac{\Delta + Hc}{a}.$$

Hence, d needs to satisfy two different inequalities. There are four possible intervals of d, depending on the size of a and c.
Thus we have four cases: small a large c, small a small c, large a large c and large a small c.

From determinant to modular hyperbola

One of the cases is the "large a, large c" case: counting the number of integral points of

$$ad \equiv \Delta \pmod{c},$$

with $\Delta/H + c < a \leq H$, $\Delta/H < c \leq H$. In this case, we have

$$\frac{\Delta - Hc}{a} < 0 < d \leq \frac{\Delta + Hc}{a} < H \implies 0 < d \leq \frac{\Delta + Hc}{a}.$$

Hence, our case is equivalent to counting the integral points on a modular hyperbola defined by the function $f_+(x) = \dfrac{\Delta + Hc}{x}$.

Applying Ustinov's result, the number of solutions of $ad \equiv \Delta \pmod{c}$ for a fixed c with $\Delta/H + c < a \leq H$, $0 < d \leq f_+(a)$ is

$$\frac{cH+\Delta}{c}\sum_{r|\Delta}\sum_{\substack{\Delta/H+c<a\leq H\\ \gcd(a,c)=r}}\frac{r}{a} - \left(H - \frac{\Delta}{H} - c\right)\frac{\delta_c(\Delta)}{2} + E_3(c),$$

for some error term $E_3(c)$.
Hence, adding all possible values of c with $\Delta/H < c \leq H$, the number of solutions of $ad \equiv \Delta \pmod{c}$ in the interval $\Delta/H + c < a \leq H$, $\Delta/H < c \leq H$ is

$$H\sum_{r|\Delta}\sum_{\substack{\Delta/H+c<a\leq H\\ \Delta/H<c\leq H\\ \gcd(a,c)=r}}\frac{r}{a} + \Delta\sum_{r|\Delta}\sum_{\substack{\Delta/H+c<a\leq H\\ \Delta/H<c\leq H\\ \gcd(a,c)=r}}\frac{r}{ac} + O(H^{5/3+o(1)}).$$

We repeat these calculations for other possible intervals of a and c. The corresponding region in each case can be modular rectangle, modular hyperbola, or some union of them. We add all terms from these cases to conclude the division.

Back to the original equation

Adding over all possible intervals of a and c, the number of integer solutions (a, b, c, d) to

$$ad - bc = \Delta$$

with $0 < a, |b|, c, d \le H$ is

$$H \sum_{r|\Delta} \left[\sum_{\substack{0<a\le c+\Delta/H \\ 0<c\le H \\ \gcd(a,c)=r}} \frac{r}{c} + \sum_{\substack{\Delta/H+c<a\le H \\ 0<c\le H \\ \gcd(a,c)=r}} \frac{r}{a} + \sum_{\substack{0<a\le H \\ 0<c\le \Delta/H \\ \gcd(a,c)=r}} \frac{r}{a} \right] + O\left(\Delta \sum_{r|\Delta} \sum_{\substack{0<a,c\le H \\ \gcd(a,c)=r}} \frac{r}{ac} \right) + O(H^{5/3+o(1)})$$

How to simplify these four summations?

A new summation result

MA (2024+)

Let $X, Y \geq 0$ and r be a positive integer. We have

$$\sum_{\substack{0<y<x+Y \\ 0<x\leq X \\ \gcd(x,y)=r}} \frac{r}{x} = \frac{6}{\pi^2}\left(\frac{X}{r} + \frac{Y}{r}\log\frac{X}{r}\right) + O\left(\frac{Y}{r}\right) + O\left(\log^2\frac{X}{r}\right).$$

Sketch of proof: substituting $x = rx', y = ry'$, switching the order of summations, and using the asymptotic

$$\sum_{0<x\leq X} \frac{\varphi(x)}{x} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

We also have similar results for the other summations in the previous slide, proven similarly.

Applying the summation lemmas

For a fixed H and $\Delta \neq 0$, as $H, \Delta \to \infty$, the number of integer solutions (a, b, c, d) to

$$ad - bc = \Delta$$

with $0 < a, |b|, c, d \leq H$ is

$$\frac{12}{\pi^2} H^2 \sum_{\substack{r|\Delta \\ r \leq H}} \frac{1}{r} + O(H^{o(1)} \max(H^{5/3}, \Delta)).$$

To complete the proof of the main result, we consider the other signs of a, c, d and count them accordingly.

MA (2024+)

Fix integers H, $\Delta \neq 0$. As $H, \Delta \to \infty$, we uniformly have

$$D_2(H,\Delta) = \frac{96}{\pi^2}\frac{\sigma(|\Delta|)}{|\Delta|}H^2 + O(H^{o(1)}\max(H^{5/3},\Delta)),$$

where $\sigma(n)$ denotes the sum of all positive divisors of n.

The last result gives a uniform formula of $D_2(H,\Delta)$ if $0 < |\Delta| \leq H^{2-\varepsilon}$, for every $\varepsilon > 0$. If $|\Delta| > H^{2-\varepsilon}$, the result only implies

$$D_2(H,\Delta) = O(H^{2+o(1)}),$$

which is already known from Shparlinski.

Other work for general Δ

With more sophisticated tools from automorphic froms and character sums, Guria and Ganguly (2024+) prove

$$D_2(H,\Delta) = \frac{96}{\pi^2}\frac{\sigma(|\Delta|)}{|\Delta|}H^2 + \begin{cases} O(H^{3/2+7/64+o(1)}), & \text{if } 0 < |\Delta| \ll H^{1/3}, \\ O(H^{5/3} + o(1)), & \text{if } H^{1/3} < |\Delta| \ll H^{5/3}. \end{cases}$$

Compared to our result, they have better error bounds, but smaller intervals of $|\Delta|$.
Also, their methods can be used for giving results on counting 2×2 integer matrices with other restrictions, such as when some of the entries are primes or the matrices have fixed characteristic polynomials.

Further with more variables

Another extension of this problem is to consider the equation

$$x_1 x_2 \dots x_n - y_1 y_2 \dots y_n = \Delta,$$

with $|x_i|, |y_i| \leq H$. For the case $\Delta = 0$, we have results for Munsch-Shparlinski (2015). Another direction for the case $\Delta = 0$ is to count the number of solutions of

$$x_1 x_2 = x_3 x_4 = \cdots = x_{2n-1} x_{2n}$$

with $|x_i| \leq H$. Mastrostefano (2021, unpublished) obtained the correct order of this quantity.

These two equations may be generalised further as follows: Let $k, m > 1$ be integer, and consider the equation

$$x_{1,1} \ldots x_{1,m} = \cdots = x_{k,1} \ldots x_{k,m} \tag{1}$$

A recent work of MA with fellow PhD student in UNSW, Chandler C. Corrigan, provides a new bound for counting solutions to this equation.

MA-Corrigan (2025+)

Let $E(H)$ be number of integer solutions to (1) with $0 < x_{i,j} \leq H$. As $H \to \infty$, we have

$$E(H) = q_{m,k} H^m (\log H)^{m^k - (m-1)k - 1} + H^m P_{m,k}(\log H) + o(H^{m - \vartheta_{m,k}}),$$

with $P_{m,k}$ is a polynomial of degree not exceeding $m^k - (m-1)k - 2$, $\vartheta_{m,k} > 0$ and

$$q_{m,k} = V_{m,k} \prod_p (1 - p^{-1})^{m^k} \sum_{n \geqslant 0} \frac{1}{p^n} \binom{n + m - 1}{m - 1}^k,$$

where $V_{m,k}$ is the volume of a m^k-dimensional box.

Thank you

M. Afifurrahman, 'A uniform formula on the number of integer matrices with given determinant and height', *Preprint*, 2024, available from `https://arxiv.org/abs/2407.08191`.

M. Afifurrahman, C. C. Corrigan 'Solutions to multiplicative Diophantine equations in orthotopes', *Preprint*, 2025, available from `https://arxiv.org/abs/2501.15372`.