Counting Subrings of $\mathbb{Z}^n$

Nathan Kaplan

University of California, Irvine
New York Number Theory Seminar

January 28, 2021
I. Main Questions
Some Definitions

Definition

- A sublattice $\Lambda \subseteq \mathbb{Z}^n$ is a finite index subgroup of $\mathbb{Z}^n$.

- Let $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n) \in \mathbb{Z}^n$. Define $v \circ w = (v_1w_1, \ldots, v_nw_n)$.

- A sublattice $\Lambda \subseteq \mathbb{Z}^n$ is a multiplicative sublattice if $v, w \in \Lambda$ implies $v \circ w \in \Lambda$.

- A subring $R \subseteq \mathbb{Z}^n$ is a multiplicatively closed sublattice that contains $(1, 1, \ldots, 1)$.

- Let $a_k(\mathbb{Z}^n)$ be the number of sublattices $\Lambda \subseteq \mathbb{Z}^n$ with $[\mathbb{Z}^n: \Lambda] = k$.

- Let $f_n(k)$ be the number of subrings $R \subseteq \mathbb{Z}^n$ with $[\mathbb{Z}^n: R] = k$.

- It is not difficult to show that the number of subrings of $\mathbb{Z}^{n+1}$ of index $k$ equals the number of multiplicative sublattices of $\mathbb{Z}^n$ of index $k$. 

Kaplan (UCI) Counting Subrings of $\mathbb{Z}^n$ January 28, 2021 3 / 29
Main Questions

Question

1. Can we give a formula for $a_k(\mathbb{Z}^n)$?

2. Let

$$N_n(X) = \#\{\text{sublattices of } \mathbb{Z}^n \text{ of index } \leq X\} = \sum_{k \leq X} a_k(\mathbb{Z}^n).$$

Can we give an asymptotic formula for $N_n(X)$ as $X \to \infty$?

Question

1. Can we give a formula for $f_n(k)$?

2. Let

$$N_n^R(X) = \#\{\text{subrings of } \mathbb{Z}^n \text{ of index } \leq X\} = \sum_{k \leq X} f_n(k).$$

Can we give an asymptotic formula for $N_n^R(X)$ as $X \to \infty$?
Every finite index subgroup of $\mathbb{Z}$ is $k\mathbb{Z}$ for some positive integer $k$.

$a_k(\mathbb{Z}) = 1$ for each $k \geq 1$.

$N_1(X) = \lfloor X \rfloor$.

**Theorem**

For $n \geq 2$,

$$N_n(X) = \# \{ \text{sublattices of } \mathbb{Z}^n \text{ of index } \leq X \}$$

$$= \frac{\zeta(n)\zeta(n-1)\cdots\zeta(2)}{n} X^n + O(X^{n-1} \log(X)).$$

**Example**

$$N_2(X) \sim \frac{\pi^2}{12} X^2.$$
Counting Subrings

Theorem (Datskovsky-Wright 3, Nakagawa 4, K.-Marcinek-Takloo-Bighash ≥ 5)

1. For $n \in \{2, 3, 4, 5\}$ there exists a $C_n > 0$ such that

$$N_n^R(X) \sim C_nX(\log X)^{\binom{n}{2}-1}.$$ 

2. Suppose $n \geq 6$. For any $\epsilon > 0$ we have

$$X(\log X)^{\binom{n}{2}-1} \ll N_n^R(X) \ll \epsilon X^{\frac{n}{2}-\frac{7}{6}+\epsilon}.$$ 

Theorem (Isham)

Fix $n > 1$ and let

$$a(n) = \max_{0 \leq d \leq n-1} \left( \frac{d(n - 1 - d)}{n - 1 + d} + \frac{1}{n - 1 + d} \right).$$

Then $X^{a(n)} \ll N_n^R(X)$.

- As $n \to \infty$, $a(n) \approx 0.17n$.
- This result builds on work of Brakenhoff.
II. Counting Sublattices
Counting Matrices in Hermite Normal Form

- Every sublattice of \( \mathbb{Z}^n \) is the column span of a unique matrix in Hermite normal form.
- The index of the sublattice is the determinant of the matrix.

**Definition**

An \( n \times n \) integer matrix \( A \) is in **Hermite normal form** if:

1. \( A \) is upper triangular, and
2. \( 0 \leq a_{ij} < a_{ii} \) for \( 1 \leq i < j \leq n \).

\[
\begin{pmatrix}
1 & 2 & 0 \\
-3 & 3 & 0 \\
2 & 0 & 1
\end{pmatrix} \rightarrow \begin{pmatrix}
3 & 2 & 0 \\
0 & 3 & 0 \\
0 & 0 & 1
\end{pmatrix}
\]

**Question**

1. How many \( n \times n \) matrices in Hermite normal form have determinant \( k \)?
2. How many \( n \times n \) matrices in Hermite normal form have a given diagonal?
The Zeta Function of $\mathbb{Z}^n$

**Definition**

$$\zeta_{\mathbb{Z}^n}(s) = \sum_{\Lambda \subseteq \mathbb{Z}^n} \left[ \mathbb{Z}^n : \Lambda \right]^{-s} = \sum_{k=1}^{\infty} a_k(\mathbb{Z}^n) k^{-s}.$$  

**Example**

$$\zeta_{\mathbb{Z}}(s) = \sum_{k=1}^{\infty} \left[ \mathbb{Z} : k\mathbb{Z} \right]^{-s} = \sum_{k=1}^{\infty} k^{-s} = \zeta(s).$$

If $\gcd(k_1, k_2) = 1$ then $a_{k_1 k_2}(\mathbb{Z}^n) = a_{k_1}(\mathbb{Z}^n) a_{k_2}(\mathbb{Z}^n)$. Therefore,

$$\zeta_{\mathbb{Z}^n}(s) = \prod_p \zeta_{\mathbb{Z}^n,p}(s),$$

where

$$\zeta_{\mathbb{Z}^n,p}(s) = \sum_{e=0}^{\infty} a_p^e(\mathbb{Z}^n) p^{-es}. $$
Example

\[
\begin{pmatrix}
p^{a} & x & y \\
0 & p^{b} & z \\
0 & 0 & p^{c}
\end{pmatrix}
\]

There are \(p^{a}\) choices for \(x\), \(p^{a}\) choices for \(y\), and \(p^{b}\) choices for \(z\).

\[
\zeta_{\mathbb{Z}^{3},p}(s) = \sum_{a=0}^{\infty} \sum_{b=0}^{\infty} \sum_{c=0}^{\infty} p^{2a+b} \cdot p^{-(a+b+c)s}
\]

\[
= \left( \sum_{a=0}^{\infty} p^{a(2-s)} \right) \left( \sum_{b=0}^{\infty} p^{b(1-s)} \right) \left( \sum_{c=0}^{\infty} p^{-sc} \right)
\]

\[
= \left( 1 - p^{-(s-2)} \right)^{-1} \left( 1 - p^{-(s-1)} \right)^{-1} \left( 1 - p^{-s} \right)^{-1}.
\]
Theorem

\[ \zeta_{\mathbb{Z}^n}(s) = \zeta(s)\zeta(s - 1) \cdots \zeta(s - (n - 1)). \]

- Analytic properties of \( \zeta_{\mathbb{Z}^n}(s) \) give information about \( N_n(X) \).
- More specifically, \( \zeta_{\mathbb{Z}^n}(s) \) has meromorphic continuation to the entire complex plane. Its right-most pole is at \( s = n \). It is a simple pole.
- Calculating the residue and applying a Tauberian theorem gives

\[ N_n(X) \sim \frac{\zeta(n)\zeta(n - 1) \cdots \zeta(2)}{n} X^n. \]

Subgroup Growth by Lubotzky and Segal gives 5 different proofs of this result. (This one is attributed to Bushnell and Reiner.)
III. The Subring Zeta Function of $\mathbb{Z}^n$
When does a matrix give a multiplicatively closed sublattice?

Proposition

Let $A$ be an $n \times n$ matrix Hermite normal form with columns $v_1, \ldots, v_n$. The column span $\Lambda$ of $A$ is a multiplicative sublattice of $\mathbb{Z}^n$ if and only if $v_i \circ v_j \in \Lambda$ for all $1 \leq i \leq j \leq n$.

Consider $A = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$.

\[
\begin{align*}
v_1 \circ v_1 &= \begin{pmatrix} x^2 \\ 0 \end{pmatrix} = x \cdot v_1 + 0 \cdot v_2. \\
v_1 \circ v_2 &= \begin{pmatrix} xy \\ 0 \end{pmatrix} = y \cdot v_1 + 0 \cdot v_2. \\
v_2 \circ v_2 &= \begin{pmatrix} y^2 \\ z^2 \end{pmatrix} = \begin{pmatrix} y^2 - yz \\ 0 \end{pmatrix} + z \cdot v_2.
\end{align*}
\]

The sublattice spanned by this matrix is multiplicative if and only if $x \mid (y^2 - yz)$, or equivalently, if $\frac{y^2 - yz}{x} \in \mathbb{Z}$. 
Definition

\[ \zeta^n_R(s) = \sum_{k=1}^{\infty} f_n(k)k^{-s}. \]

As we saw with \( \zeta^n(s) \), this zeta function has an Euler product

\[ \zeta^n_R(s) = \prod_p \zeta^n_{p}(s), \text{ where } \zeta^n_{p}(s) = \sum_{e=0}^{\infty} f_n(p^e)p^{-es}. \]

Theorem (Datskovsky-Wright)

We have

\[ \zeta^n_2(s) = \zeta(s), \]
\[ \zeta^n_3(s) = \frac{\zeta(3s-1)\zeta(s)^3}{\zeta(2s)^2}. \]
The Subring Zeta Function of $\mathbb{Z}^n$ for Small $n$

**Theorem (Nakagawa)**

We have

$$
\zeta_{\mathbb{Z}^4}(s) = \prod_p \frac{1}{(1 - p^{-s})^2(1 - p^2 p^{-4s})(1 - p^3 p^{-6s})} \left(1 + 4p^{-s} + 2p^{-2s} + (4p - 3)p^{-3s} + (5p - 1)p^{-4s} + (p^2 - 5p)p^{-5s} + (3p^2 - 4p)p^{-6s} - 2p^2 p^{-7s} - 4p^2 p^{-8s} - p^2 p^{-9s}\right).
$$

**Theorem (Datskovsky-Wright, Nakagawa, K.-Marcinek-Takloo-Bighash)**

For $n \in \{2, 3, 4, 5\}$ there exists a $C_n > 0$ such that

$$N^R_n(X) \sim C_n X (\log X)^{\binom{n}{2} - 1}.$$

**Idea for $n = 5$:** Count subrings of ‘small index’ and show that there are not ‘too many’ subrings of ‘large index’. Show that $\zeta_{\mathbb{Z}^5}(s)$ has a pole at $s = 1$ of order $\binom{5}{2}$ and that there are no poles to the right of $s = 1$. 
Conjecture

Let $A_n(X)$ denote the number of isomorphism classes of degree $n$ number fields $K$ such that $|\text{disc}(K)| < X$.

There exists a real number $c_n > 0$ such that

$$A_n(X) \sim c_n X.$$ 

- $n = 3$, Davenport-Heilbronn.
- $n = 4, 5$, Bhargava.

Idea: Count all orders in degree $n$ fields then sieve for the maximal orders.

Question

Let $B_K(X)$ denote the number of isomorphism classes of orders $\mathcal{O}$ contained in $K$ such that $|\text{disc}(\mathcal{O})| < X$.

How does $B_K(X)$ grow as a function of $X$?

- If $\mathcal{O} \subseteq \mathcal{O}_K$ is an order, then $\text{disc}(\mathcal{O}) = [\mathcal{O}_K : \mathcal{O}]^2 \text{disc}(\mathcal{O}_K)$. 
Motivation: Counting Orders in Number Fields II

- Let $K$ be a degree $n$ number field.
- The subring zeta function $\zeta^{R}_{\mathcal{O}_K}(s)$ has an Euler product.
- The local factor $\zeta^{R}_{\mathcal{O}_K,p}(s)$ depends on how $p$ decomposes in $K$.
- If $p$ splits completely in $K$ the local factor at $p$ is $\zeta^{\mathbb{Z}^n,p}(s)$.

**Idea:** Primes that split completely should contribute ‘the most’ orders.

**Question**

*Does the growth rate of $N_n(X)$ determine the growth rate of $B_K(X)$?*
IV. Counting Subrings of $\mathbb{Z}^n$ of ‘Small Index’
Proposition (Liu)

For any positive integer $n$

\begin{align*}
  f_n(1) &= 1, \\
  f_n(p) &= \binom{n}{2}, \\
  f_n(p^2) &= \binom{n}{2} + \binom{n}{3} + 3\binom{n}{4}, \\
  f_n(p^3) &= \binom{n}{2} + (p+1)\binom{n}{3} + 7\binom{n}{4} + 10\binom{n}{5} + 15\binom{n}{6}, \\
  f_n(p^4) &= \binom{n}{2} + (3p+1)\binom{n}{3} + (p^2 + p + 10)\binom{n}{4} + (10p + 21)\binom{n}{5} \\
  &\quad + 70\binom{n}{6} + 105\binom{n}{7} + 105\binom{n}{8}.
\end{align*}

- Liu also gives a formula for $f_n(p^5)$. 
Atanasov-K.-Krakoff-Menzel: Give formulas for $f_n(p^e)$ for $e \in \{6, 7, 8\}$.

$$f_n(p^8) = \binom{n}{2} + (4p^2 + 4p + 1)\binom{n}{3} + (p^4 + 26p^3 + 9p^2 + p + 22)\binom{n}{4}$$
$$+ (p^5 + 77p^4 - 13p^3 + 52p^2 + 161p + 61)\binom{n}{5}$$
$$+ (16p^6 + 31p^5 + 22p^4 + 187p^3 + 702p^2 + 301p + 441)\binom{n}{6}$$
$$+ (p^8 + p^7 + 2p^6 + 23p^5 + 339p^4 + 1080p^3 + 1206p^2 + 3074p + 1800)\binom{n}{7}$$
$$+ (29p^6 + 29p^5 + 652p^4 + 1093p^3 + 9374p^2 + 9073p + 8933)\binom{n}{8}$$
$$+ (36p^5 + 498p^4 + 6420p^3 + 15324p^2 + 39810p + 37201)\binom{n}{9}$$
$$+ (630p^4 + 3150p^3 + 46200p^2 + 103320p + 148551)\binom{n}{10}$$
$$+ (6930p^3 + 41580p^2 + 243705p + 510730)\binom{n}{11}$$
$$+ (51975p^2 + 329175p + 1474165)\binom{n}{12}$$
$$+ (270270p + 3258255)\binom{n}{13} + 5045040\binom{n}{14} + 4729725\binom{n}{15} + 2027025\binom{n}{16}. $$
**Irreducible Subrings**

**Definition (Liu)**
- A subring $R \subseteq \mathbb{Z}^n$ with index equal to a power of $p$ is **irreducible** if for each $(x_1, \ldots, x_n) \in R$, $x_1 \equiv \cdots \equiv x_n \pmod{p}$.
- Let $g_n(p^e)$ be the number of irreducible subrings of $\mathbb{Z}^n$ of index $p^e$.

**Proposition (Liu)**

For $n > 0$, 

$$f_n(p^e) = \sum_{i=0}^{e} \sum_{j=1}^{n} \binom{n-1}{j-1} f_{n-j}(p^{e-i}) g_j(p^i).$$

**Idea:** Compute $f_n(p^e)$ by computing $f_j(p^k)$ for all $j \leq n - 1$ and $k \leq e$ and $g_j(p^i)$ for all $j \leq n$ and $i \leq e$. 
Irreducible Subring Matrices

**Proposition (Liu)**

There is a bijection between subrings of \( \mathbb{Z}^n \) of index \( k \) and \( n \times n \) *subring matrices* \( A \) in Hermite normal form with \( \text{det}(A) = k \) such that:

1. the identity element \((1, \ldots, 1)^T\) is in the column span of \( A \), and
2. for each \( i, j \in [1, n] \), \( v_i \circ v_j \) is in the lattice spanned by the column vectors \( v_1, \ldots, v_n \).

An \( n \times n \) subring matrix represents an irreducible subring, and is called an *irreducible subring matrix*, if and only if

1. its first \( n - 1 \) columns contain only entries divisible by \( p \),
2. its final column is equal the identity \((1, \ldots, 1)^T\).

**Question**

*How many irreducible subring matrices have a given diagonal?*
Consider
\[
\begin{pmatrix}
  p^3 & cp & xp & yp & 1 \\
  0 & p^2 & up & vp & 1 \\
  0 & 0 & p & 0 & 1 \\
  0 & 0 & 0 & p & 1 \\
  0 & 0 & 0 & 0 & 1 \\
\end{pmatrix}
\]
where \(0 \leq c, x, y \leq p^2 - 1\), and \(0 \leq u, v \leq p - 1\).

- If \(v_2 \circ v_2\) is in the column span,
  \[
  \begin{pmatrix} c^2p^2 \\ p^4 \end{pmatrix} = p^2 \begin{pmatrix} cp \\ p^2 \end{pmatrix} + \lambda \begin{pmatrix} p^3 \\ 0 \end{pmatrix}
  \]
  for some \(\lambda \in \mathbb{Z}\). This implies \(p \mid c\), so we let \(c = pc'\).

- The number of irreducible subring matrices of this form is \(p^2\) times the number of \(\mathbb{F}_p\)-points of the variety \(V\) in 5-dimensional affine space defined by
  \[
  (x^2 - x) - (u^2 - u)c' = (y^2 - y) - (v^2 - v)c' = xy - uvc' = 0.
  \]

- \(V\) has 7 irreducible components and \(#V(\mathbb{F}_p) = 7p^2 - 6p + 6\).
What happens when we try to count irreducible subring matrices with more complicated diagonals?

Fixing the diagonal leads to solving a collection of polynomial equations modulo powers of $p$.
How complicated can the geometry of the underlying varieties become?

For fixed $n, e$, is $f_n(p^e)$ always a polynomial in $p$?

It is known that $\zeta_{\mathbb{Z}^n, p}^R(s)$ is a rational function in $p$ and $p^{-s}$.
How do these rational functions vary with $p$?
V. Further Questions
Lower Bounds for Subrings and Orders

Every matrix of the form

\[
\begin{pmatrix}
p^2 & 0 & xp & yp & 1 \\
0 & p^2 & up & vp & 1 \\
0 & 0 & p & 0 & 1 \\
0 & 0 & 0 & p & 1 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix},
\]

where \(0 \leq x, y, u, v < p\), is an irreducible subring matrix.

Idea: Find special classes of matrices for which the multiplicative closure conditions are always satisfied.

**Proposition (Brakenhoff)**

Every additive subgroup \(G\) of \(O_K\) that satisfies

\[
\mathbb{Z} + m^2 O_K \subseteq G \subseteq \mathbb{Z} + mO_K
\]

for some integer \(m\) is a subring.

**Question**

Do ‘most’ orders satisfy this condition for some \(m\)?
Quotients of Random Sublattices

Question

1. Let $\Lambda \subseteq \mathbb{Z}^n$ be a sublattice with $[\mathbb{Z}^n : \Lambda] = k$. Then $\mathbb{Z}^n / \Lambda$ is a finite abelian group of order $k$ and rank at most $n$. How often is $\mathbb{Z}^n / \Lambda$ cyclic?

2. What is the following limit?

$$\lim_{X \to \infty} \frac{\#\{\Lambda \subseteq \mathbb{Z}^n : [\mathbb{Z}^n : \Lambda] \leq X \text{ and } \mathbb{Z}^n / \Lambda \text{ is cyclic}\}}{\#\{\Lambda \subseteq \mathbb{Z}^n : [\mathbb{Z}^n : \Lambda] \leq X\}}$$

Theorem (Nguyen-Shparlinski)

The probability that $\mathbb{Z}^n / \Lambda$ is cyclic is

$$\prod_p \left(1 + \frac{p^{n-1} - 1}{p^{n+1} - p^n} \right) \frac{\zeta(n) \zeta(n-1) \cdots \zeta(2)}{\zeta(n)}.$$

- Chinta-K.-Koplewitz: ‘Probability that $\mathbb{Z}^n / \Lambda$ has rank $m$’.
Consider the limit
\[
\lim_{X \to \infty} \frac{\#\{R \subseteq \mathbb{Z}^n \text{ is a subring: } [\mathbb{Z}^n : R] \leq X \text{ and } \mathbb{Z}^n / R \text{ is cyclic}\}}{\#\{R \subseteq \mathbb{Z}^n \text{ is a subring: } [\mathbb{Z}^n : R] \leq X\}}.
\]

A result of Brakenhoff implies that for \( n \) large enough, \( \mathbb{Z}^n / R \) should not be cyclic ‘very often’.

**Question**

*Why is this behavior different?*

**Question**

*What does a random subring of \( \mathbb{Z}^n \) ‘look like’?*
Chimni studies the number of subrings of $\mathbb{Z}[x]/(x^n)$ for small $n$.

- It seems that this ring has ‘more’ subrings than $\mathbb{Z}^n$ does.
- It also seems that $(\mathbb{Z}[x]/(x^n))/R$ is very often cyclic.