Journal of Number Theory 234 (2022) 363–390

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

# Lower bounds for the number of subrings in $\mathbb{Z}^n$

Kelly Isham

*University of California, Irvine, 410R Rowland Hall, Irvine, 92697, CA, USA*

ARTICLE INFO

*Article history:*
Received 12 February 2021
Received in revised form 16 June 2021
Accepted 18 June 2021
Available online 22 July 2021
Communicated by L. Smajlovic

*MSC:*
11M41
20E07

*Keywords:*
Zeta functions of rings
Subrings
Orders in number fields
Lattices

ABSTRACT

Let $f_n(k)$ be the number of subrings of index $k$ in $\mathbb{Z}^n$. We show that results of Brakenhoff imply a lower bound for the asymptotic growth of subrings in $\mathbb{Z}^n$, improving upon lower bounds given by Kaplan, Marcinek, and Takloo-Bighash. Further, we prove two new lower bounds for $f_n(p^e)$ when $e \geq n-1$. Using these bounds, we study the divergence of the subring zeta function of $\mathbb{Z}^n$ and its local factors. Lastly, we apply these results to the problem of counting orders in a number field.



## 1. Introduction

A *subring* of $\mathbb{Z}^n$ is a sublattice that contains the multiplicative identity $(1, 1, \ldots, 1)$ and is closed under componentwise multiplication. Let $f_n(k)$ denote the number of subrings of $\mathbb{Z}^n$ of finite index $k$. The *subring zeta function* of $\mathbb{Z}^n$ is given by

$$\zeta^R_{\mathbb{Z}^n}(s) = \sum_{\substack{S \text{ subring of} \\ \text{finite index in } \mathbb{Z}^n}} [\mathbb{Z}^n : S]^{-s} = \sum_{k=1}^{\infty} f_n(k) k^{-s}.$$

*E-mail address:* ishamk@uci.edu.

https://doi.org/10.1016/j.jnt.2021.06.026

There is a wider class of zeta functions for groups or rings, which are defined in [7]. For an extensive survey about these zeta functions, see [6]. Let $\prod_p$ denote the product over all primes. The subring zeta function has an Euler product

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

with local factors

$$\zeta^R_{\mathbb{Z}^n,p}(s) = \sum_{e=0}^{\infty} f_n(p^e)p^{-es}.$$

Let $\mathbb{Z}_p$ denote the $p$-adic integers. Note that $\zeta^R_{\mathbb{Z}^n,p}(s) = \zeta^R_{\mathbb{Z}_p^n}(s)$ where the $p^{-es}$ coefficient in the latter zeta function is the number of $\mathbb{Z}_p$-subalgebras of index $p^e$ in $\mathbb{Z}_p^n$.

When $n \leq 4$, there are explicit closed formulas for $\zeta^R_{\mathbb{Z}^n}(s)$, which we summarize in the following theorem.

**Theorem 1.1.** *We have*

$$\begin{aligned}
\zeta^R_{\mathbb{Z}^2}(s) &= \zeta(s)\\
\zeta^R_{\mathbb{Z}^3}(s) &= \frac{\zeta(3s-1)\zeta(s)^3}{\zeta(2s)^s}\\
\zeta^R_{\mathbb{Z}^4}(s) &= \prod_p \frac{1}{(1-p^{-s})^2(1-p^{2-4s})(1-p^{3-6s})}\Big(1+4p^{-s}\\
&\quad + 2p^{-2s} + (4p-3)p^{-3s} + (5p-1)p^{-4s} + (p^2-5p)p^{-5s}\\
&\quad + (3p^2-4p)p^{-6s} - 2p^{2-7s} - 4p^{2-8s} - p^{2-9s}\Big).
\end{aligned}$$

The case $n = 2$ follows from the fact that $f_2(k) = 1$ for all positive integers $k$. The case $n = 3$ is originally due to Datskovsky and Wright [5] and $n = 4$ is due to Nakagawa [10]. Liu [9] gives combinatorial proofs of these formulas.

In this paper, we are motivated by three broad questions. These questions have been actively studied by several other authors and we summarize some known results below.

**Question 1.2.** *For each fixed $n$ and $e$, what is $f_n(p^e)$ as a function of $p$?*

For each fixed $n \leq 4$ and $e \geq 0$, comparing the $p^{-es}$ coefficients of the expression in Theorem 1.1 shows that $f_n(p^e)$ is a polynomial in $p$. Liu [9] gives explicit formulas for $f_n(p^e)$ for fixed $e \leq 5$ and $n > 0$, which are all polynomial in $p$. His formula for $e = 5$ has a small error that Atanasov, Kaplan, Krakoff, and Menzel [1] correct. Further, the authors extend Liu's work by giving explicit polynomial formulas for $f_n(p^e)$ when $e \in \{6, 7, 8\}$ and $n > 0$. These are the only exact formulas that are known; it is not even

known if $f_n(p^e)$ will always be polynomial in $p$. In this paper, we discuss known and new results about lower bounds for $f_n(p^e)$.

**Question 1.3.** *What is the asymptotic growth of the number of subrings in $\mathbb{Z}^n$ of index at most $B$?*

For each fixed $n$, let

$$N_n(B) = \#\{S \subset \mathbb{Z}^n \,:\, S \text{ is a subring and } [\mathbb{Z}^n : S] \leq B\} = \sum_{k \leq B} f_n(k).$$

This function counts the number of subrings of index at most $B$ in $\mathbb{Z}^n$. In [8], Kaplan, Marcinek, and Takloo-Bighash give the asymptotic growth of $N_n(B)$ when $n \leq 5$. The cases $n \leq 4$ follow from Theorem 1.1 after applying a Tauberian theorem (see e.g. the appendix of [4]). It is important to note that these authors were able to prove an asymptotic formula when $n = 5$ even though no closed formula for $\zeta^R_{\mathbb{Z}^5}(s)$ is known. There is not even a conjecture about the asymptotic growth of $N_n(B)$ for $n \geq 6$. To make progress toward an answer to Question 1.3 when $n \geq 6$, Kaplan, Marcinek, and Takloo-Bighash give upper and lower bounds for the asymptotic behavior of $N_n(B)$.

**Theorem 1.4.** *[8, Theorem 6]*

1. *Let $n \leq 5$. There exists a constant $C_n$ so that*

$$N_n(B) \sim C_n B (\log B)^{\binom{n}{2}-1}$$

   *as $B \to \infty$.*
2. *Let $n > 5$. For any $\epsilon > 0$,*

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

   *as $B \to \infty$.*

The authors obtain the lower bound in Theorem 1.4(2) by computing the rightmost pole of the simpler Euler product $\prod_p (1 + f_n(p)p^{-s})$ and then applying a Tauberian theorem. In this paper, we show that the results of Brakenhoff [2] lead to a new asymptotic lower bound for $N_n(B)$ that improves upon Theorem 1.4(2).

Observe that Theorem 1.4 implies that $\zeta^R_{\mathbb{Z}^n}(s)$ diverges for all $s \in \mathbb{C}$ such that $\Re(s) \leq 1$. Thus the strategy Kaplan, Marcinek, and Takloo-Bighash employ also gives a partial answer to the question: what is the abscissa of convergence of $\zeta^R_{\mathbb{Z}^n}(s)$? Recall that the *abscissa of convergence* of a Dirichlet series $D(s)$ is the unique $\sigma \in \mathbb{R} \cup \{\pm\infty\}$ so that $D(s)$ diverges for all $s$ with $\Re(s) < \sigma$ and converges for all $s$ with $\Re(s) > \sigma$. We will show that results of Brakenhoff [2] improve upon the lower bound for the abscissa of convergence of $\zeta^R_{\mathbb{Z}^n}(s)$.

**Table 1**
Values of $a(n)$ for small $n$.

| $n$ | 6 | 7 | 8 | 9 | 10 | 20 | 50 | 100 |
|---|---|---|---|---|---|---|---|---|
| $a(n)$ | 1 | $\frac{9}{8}$ | $\frac{13}{10}$ | $\frac{16}{11}$ | $\frac{21}{13}$ | $\frac{89}{27}$ | $\frac{581}{69}$ | $\frac{2379}{140}$ |

**Question 1.5.** *What is the abscissa of convergence of* $\zeta^R_{\mathbb{Z}^n,p}(s)$*?*

If $\zeta^R_{\mathbb{Z}^n}(s)$ converges, so do each of the local factors. Therefore the abscissa of convergence for $\zeta^R_{\mathbb{Z}^n}(s)$ gives an upper bound for the abscissa of convergence for $\zeta^R_{\mathbb{Z}^n,p}(s)$ for each prime $p$. However, not much is known about lower bounds. We will provide a lower bound for the abscissa of convergence of $\zeta^R_{\mathbb{Z}^n,p}(s)$.

### *1.1. Main results*

In this paper, we give partial results to the three broad questions asked in Section 1. First, we provide a new lower bound for the asymptotic growth of $N_n(B)$ that improves upon [8] for all $n \geq 7$ (see Table 1). The main elements in the proof of this theorem come from interpreting results of Brakenhoff [2].

**Theorem 1.6.** *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* $B^{a(n)} \ll N_n(B)$ *as* $B \to \infty$.

Next, we study two different techniques for bounding the number of subrings in $\mathbb{Z}^n$ of index $p^e$. The first technique is an extension of Brakenhoff's [2] results and holds more generally for the function that counts subrings of the ring of integers $\mathcal{O}_K$ in a fixed number field $K$ of degree $n$. We find a lower bound by showing that a special set of subgroups of $\mathcal{O}_K$ are subrings and then bounding the number of such subgroups. This is detailed in Section 2. The second technique is based off Liu's [9] work; we bound subrings by counting the number of $n \times n$ matrices with certain properties, see Sections 3 and 4.

We summarize our main results, which give partial answers to Questions 1.2 and 1.5. First, we provide new lower bounds for $f_n(p^e)$ that hold for all $e \geq n-1$. We use the first technique to obtain Theorem 1.8. The other two theorems follow from the second technique.

**Remark 1.7.** Unless otherwise stated, $\max_{A \leq x \leq B}$ means the maximum over all integers $x$ in the range $[A, B]$.

**Theorem 1.8.** *Fix integers* $n > 1$ *and* $e \geq n-1$. *For each* $t$, *set* $k = e - t(n-1)$, $c = \lceil \frac{e}{t} \rceil - (n-1)$ *and* $b = \lfloor \frac{e}{t} \rfloor - (n-1)$. *Set*

$$h(e,n) = \max_{\lceil \frac{e}{2(n-1)} \rceil \leq t \leq \lfloor \frac{e}{n-1} \rfloor} \left( k(n-1) - c^2(k+t-ct) - b^2(ct-k) \right).$$

*Then* $f_n(p^e) \geq p^{h(e,n)}$.

**Theorem 1.9.** *Suppose that* $e \geq n-1$. *Let*

$$b(n,e) = \max_{0 \leq d \leq n-1} \left\lfloor \frac{e}{n-1+d} \right\rfloor \cdot d(n-1-d).$$

*Then* $f_n(p^e) \geq p^{b(n,e)}$.

The lower bounds from Theorem 1.9 and the work in Section 5 lead to a lower bound for the abscissa of convergence of $\zeta^R_{\mathbb{Z}^n,p}(s)$.

**Theorem 1.10.** *Fix* $n > 1$. *Let*

$$c_7(n) = \max_{0 \leq d \leq n-1} \frac{d(n-1-d)}{n-1+d}.$$

*Then* $\zeta^R_{\mathbb{Z}^n,p}(s)$ *diverges for all* $s$ *such that*

$$\Re(s) \leq c_7(n).$$

### *1.2. Outline of the paper*

In the rest of this paper, we discuss lower bounds for various functions related to subrings in $\mathbb{Z}^n$ including $f_n(p^e)$, $N_n(B)$, and the abscissa of convergence of $\zeta^R_{\mathbb{Z}^n,p}(s)$. In Section 2, we summarize results from Brakenhoff [2] and then show how these results lead to better asymptotic lower bounds for $N_n(B)$. Brakenhoff gives a lower bound for $f_n(p^e)$, when $e \in [(n-1), 2(n-1)]$. We extend his method to obtain a lower bound for $f_n(p^e)$ for all $e \geq n-1$. In Section 3, we introduce Liu's method of counting subrings in $\mathbb{Z}^n$ by counting matrices in Hermite normal form with certain conditions. We then provide an algorithmic method for counting such matrices. In Section 4, we prove new lower bounds for $f_n(p^e)$ using the method discussed in Section 3. In Section 5, we prove a lower bound for the abscissa of convergence of $\zeta^R_{\mathbb{Z}^n,p}(s)$. In Section 6, we connect the results in this paper to the problem of counting orders in a number field. Finally, in Section 7 we discuss further questions.

## 2. Extending results of Brakenhoff

In his 2009 PhD thesis [2], Brakenhoff studies similar questions to those asked in Section 1. Let $\mathrm{Nf}_n$ be the set of number fields of degree $n$. For $K \in \mathrm{Nf}_n$, let $\mathcal{O}_K$ be the ring of integers of $K$. Brakenhoff considers the function

$$f(n,m) = \max_{K \in \mathrm{Nf}_n} \#\{R \subset \mathcal{O}_K \,:\, R \text{ is a subring of index } m\}.$$

An *order* in $\mathcal{O}_K$ is a finite index subring of $\mathcal{O}_K$ that contains the multiplicative identity. Since we assume that all subrings contain the multiplicative identity, the function $f(n,m)$ is also counting orders.

**Lemma 2.1.** *[2, Lemma 5.10] Every additive subgroup $G \subset \mathcal{O}_K$ that satisfies $\mathbb{Z}+m^2\mathcal{O}_K \subset G \subset \mathbb{Z}+m\mathcal{O}_K$ for some integer $m$ is a subring.*

Using Lemma 2.1, Brakenhoff finds a lower bound for $f(n,p^e)$ when $e \in [n-1, 2(n-1)]$. First we recall a definition.

**Definition 2.2.** Let $q$ be a prime power. The $q$-binomial coefficient is given by

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}.$$

**Proposition 2.3.** *[2, Page 42] Fix integers $n > 0$ and $d \in [0, n-1]$. Then*

$$f(n, p^{n-1+d}) \geq \begin{bmatrix} n-1 \\ d \end{bmatrix}_p.$$

**Remark 2.4.** It is important to note that $\begin{bmatrix} n-1 \\ d \end{bmatrix}_p$ is a polynomial in $p$ of degree $d(n-1-d)$.

**Remark 2.5.** Note that Lemma 2.1 is still true for each fixed number field $K$. Further, it is still true if we replace $\mathcal{O}_K$ with $\mathbb{Z}^n$. Therefore the bound in Proposition 2.3 is also a lower bound for $f_n(p^{n-1+d})$ when $d$ is an integer in $[0, n-1]$.

In Section 2.2, we extend Proposition 2.3 by providing a lower bound for $f_n(p^e)$ when $e \geq n-1$. This extended lower bound holds for all $K \in \mathrm{Nf}_n$. In Section 4, we provide a different technique for bounding $f_n(p^e)$.

### *2.1. Asymptotic lower bounds using Brakenhoff's results*

We now show that Proposition 2.3 leads to new a lower bound for the asymptotic growth of subrings in $\mathbb{Z}^n$. The main theorem in this section (Theorem 1.6) does not appear in [2].

**Lemma 2.6.** *Fix $n \geq 0$ and $e \geq 0$. Suppose there exists a constant $c_n > 0$ and positive integer $a$ so that $f_n(p^e) \geq c_n p^a$. Then $\zeta^R_{\mathbb{Z}^n}(s)$ diverges for all $s$ such that $\Re(s) \leq \frac{a+1}{e}$.*

The following corollary was not stated in Brakenhoff's thesis.

**Corollary 2.7.** *Fix $n > 1$. Then $\zeta^R_{\mathbb{Z}^n}(s)$ diverges for all $s$ such that*

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

**Proof.** By Remarks 2.4 and 2.5, for each fixed $n > 0$ and for each integer $d \in [0, n-1]$,

$$f_n(p^{n-1+d}) \geq p^{d(n-1-d)}.$$

Applying Lemma 2.6 gives the result. □

**Proof of Theorem 1.6.** This follows from Corollary 2.7 and standard Tauberian theorem. □

Theorem 1.6 is an improvement upon Theorem 1.4 for all $n \geq 7$.

### *2.2. Extending Brakenhoff's lower bound for $f_n(p^e)$*

We begin by sketching the proof of Proposition 2.3, which relies on Lemma 2.1. Take $m = p$ in Lemma 2.1 and consider the following set

$$\{G \subset \mathcal{O}_K \,:\, \mathbb{Z} + p^2\mathcal{O}_K \subset G \subset \mathbb{Z} + p\mathcal{O}_K \text{ and } \dim_{\mathbb{F}_p}\left(G/(\mathbb{Z} + p^2\mathcal{O}_K)\right) = d\},$$

which is a subset of the set of subrings in $\mathcal{O}_K$ of index $p^{n-1+d}$. Note that there is a small typo on page 42 of [2]; he writes $\dim_{\mathbb{F}_p}(G/(\mathbb{Z} + p\mathcal{O}_K)) = d$. Brakenhoff proves that the cardinality of this set is exactly $\begin{bmatrix} n-1 \\ d \end{bmatrix}_p$ by showing the set is in bijection with the set of $\mathbb{F}_p$-vector spaces in $\mathbb{F}_p^{n-1}$ of dimension $d$.

We now generalize this lower bound by relating subgroups satisfying the condition in Lemma 2.1 to subgroups in $(\mathbb{Z}/m\mathbb{Z})^{n-1}$. Let $K$ be a number field of degree $n$ and consider the set

$$\{G \subset \mathcal{O}_K \,:\, \mathbb{Z} + m^2\mathcal{O}_K \subset G \subset \mathbb{Z} + m\mathcal{O}_K\}.$$

By Lemma 2.1, every finite index subgroup in this set is a subring of $\mathcal{O}_K$. Since $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n$, $\mathcal{O}_K$ is additively isomorphic to $\mathbb{Z}^n$. Let $\{1, v_1, \ldots, v_{n-1}\}$ be a basis for $\mathcal{O}_K$. There is a bijection between sublattices of $\mathbb{Z}^{n-1}$ and subgroups of $\mathcal{O}_K$ that contain $\mathbb{Z}$.

**Proposition 2.8.** *Let $K$ be a degree $n$ number field and let $\{1, v_1, \ldots, v_{n-1}\}$ be a basis for $\mathcal{O}_K$. For any $m \geq 1$, $\mathbb{Z} + m^2\mathcal{O}_K \subset G \subset \mathbb{Z} + m\mathcal{O}_K$ if and only if $G$ contains the sublattice of $\mathbb{Z}^{n-1}$ spanned by $m^2v_1, \ldots, m^2v_{n-1}$ and $G$ is contained in the sublattice of $\mathbb{Z}^{n-1}$ spanned by $mv_1, \ldots, mv_{n-1}$.*

**Proof.** Observe that $\mathbb{Z} + m^2\mathcal{O}_K$ is the subgroup corresponding to the sublattice of $\mathbb{Z}^{n-1}$ spanned by $m^2v_1, \ldots, m^2v_{n-1}$. Therefore $\mathbb{Z} + m^2\mathcal{O}_K \subset G$ if and only if $G$ contains all basis elements of $\mathbb{Z} + m^2\mathcal{O}_K$. The second condition follows from the fact that $\mathbb{Z} + m\mathcal{O}_K$ corresponds to the sublattice spanned by $mv_1, \ldots, mv_{n-1}$. □

**Theorem 2.9.** *Let $K$ be a degree $n$ number field. Fix some $k \in \mathbb{N}$. The number of subgroups $G$ of index $m^{n-1}k$ such that $\mathbb{Z} + m^2\mathcal{O}_K \subset G \subset \mathbb{Z} + m\mathcal{O}_K$ is equal to the number of subgroups of order $k$ in $(\mathbb{Z}/m\mathbb{Z})^{n-1}$.*

**Proof.** By the Lattice Isomorphism Theorem for groups, there is a bijection between subgroups $G \subset \mathbb{Z}^{n-1}$ such that $m^2\mathbb{Z}^{n-1} \subset G \subset m\mathbb{Z}^{n-1}$ and subgroups $G' \subset m\mathbb{Z}^{n-1}/m^2\mathbb{Z}^{n-1} \cong (\mathbb{Z}/m\mathbb{Z})^{n-1}$. Fix some $G \subset \mathbb{Z}^{n-1}$ satisfying the conditions. Then

$$[\mathbb{Z}^{n-1} : G] = [\mathbb{Z}^{n-1} : m\mathbb{Z}^{n-1}][m\mathbb{Z}^{n-1} : G] = m^{n-1}[m\mathbb{Z}^{n-1} : G].$$

Set $k = [m\mathbb{Z}^{n-1} : G]$. Let $G'$ be the subgroup of $(\mathbb{Z}/m\mathbb{Z})^{n-1}$ corresponding to $G$. Then $k = [m\mathbb{Z}^{n-1} : G] = [(\mathbb{Z}/m\mathbb{Z})^{n-1} : G']$. Finally, observe that the number of subgroups of index $k$ in $(\mathbb{Z}/m\mathbb{Z})^{n-1}$ is equal to the number of subgroups of order $k$ in $(\mathbb{Z}/m\mathbb{Z})^{n-1}$. □

In order to find a lower bound for $f_n(p^e)$, it now suffices to count the number of subgroups in $(\mathbb{Z}/m\mathbb{Z})^{n-1}$. Specifically, we will set $m = p^t$ for some $t > 0$.

**Definition 2.10.** Let $\lambda = (\lambda_1, \ldots, \lambda_r)$ be a partition. A finite abelian $p$-group has *type* $\lambda$ if $G \cong \mathbb{Z}/p^{\lambda_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\lambda_r}\mathbb{Z}$.

Let $\lambda'$ denote the conjugate partition of $\lambda$. We use the notation $\nu \subseteq \lambda$ if $\nu_i \leq \lambda_i$ for all $i = 1, \ldots, r$.

**Theorem 2.11.** *[11, Page 1] Let $\nu \subseteq \lambda$ be partitions. Let $\nu'$ be the conjugate partition of $\nu$ and $\lambda'$ be the conjugate partition of $\lambda$. The number of subgroups of type $\nu$ in a finite abelian $p$-group of type $\lambda$ is equal to*

$$\prod_{j \geq 1} p^{\nu'_{j+1}(\lambda'_j - \nu'_j)} \begin{bmatrix} \lambda'_j - \nu'_{j+1} \\ \nu'_j - \nu'_{j+1} \end{bmatrix}_p.$$

Using this theorem, we can give an exact formula for the number of subgroups of type $\nu$ in a finite abelian $p$-group of type $\lambda = (t, t, \ldots, t)$.

**Corollary 2.12.** *The number of subgroups of type $\nu$ in $(\mathbb{Z}/p^t\mathbb{Z})^{n-1}$ is equal to*

$$\prod_{j \geq 1} p^{\nu'_{j+1}((n-1) - \nu'_j)} \begin{bmatrix} (n-1) - \nu'_{j+1} \\ \nu'_j - \nu'_{j+1} \end{bmatrix}_p.$$

**Proof.** Set $\lambda = (t, \dots, t)$ with the $t$ repeated $n-1$ times. Observe that $\lambda' = (n-1, \dots, n-1)$ where the term $n-1$ is repeated $t$ times. Then apply Theorem 2.11. □

**Proposition 2.13.** *The expression in Corollary 2.12 is a polynomial in $p$ of degree*

$$\sum_{j=1}^{t} \nu'_j(n-1-\nu'_j).$$

**Proof.** The degree of $\begin{bmatrix} n \\ k \end{bmatrix}_p$ is equal to $k(n-k)$. Therefore the degree of each term in the product is

$$\nu'_{j+1}(n-1-\nu'_j) + (n-1-\nu'_{j+1} - (\nu'_j - \nu'_{j+1}))(\nu'_j - \nu'_{j+1}).$$

Simplifying and then adding all terms together gives the result. □

**Theorem 2.14.** *Fix $n > 1$ and let $\lambda = (t, \dots, t)$ be the type of the group $G = (\mathbb{Z}/p^t\mathbb{Z})^{n-1}$. Let $k \in [0, t(n-1)]$. Set $b = \lfloor \frac{k}{t} \rfloor$ and $c = \lceil \frac{k}{t} \rceil$. Then the number of subgroups of $G$ of order $p^k$ is a polynomial in $p$ with degree*

$$k(n-1) - c^2(k+t-ct) - b^2(ct-k).$$

**Proof.** By Proposition 2.13, for each $\nu \subseteq \lambda = (t, t, \dots, t)$, the degree of the polynomial that counts the number of subgroups of type $\nu$ is

$$\sum_{j=1}^{t} \nu'_j(n-1-\nu'_j).$$

The number of subgroups of type $\nu \subseteq \lambda$ is equal to the number of subgroups of type $\nu' \subseteq \lambda'$. Therefore we seek to maximize the degree of the polynomials counting subgroups of order $p^k$ in $(\mathbb{Z}/p^t\mathbb{Z})^{n-1}$ by considering the subgroups of type $\nu' \subseteq \lambda' = (n-1, \dots, n-1)$ where the $n-1$ is repeated $t$ times subject to the constraint $\sum_{j=1}^{t} \nu'_j = k$. Observe that the degree is as large as possible when $\sum_{j=1}^{t} (\nu'_j)^2$ is minimized subject to the constraint that $\sum_{j=1}^{t} \nu'_j = k$. Over $\mathbb{R}$, this function is minimized when $\nu'_j = \frac{k}{t}$ for all $j = 1, \dots t$. However, each $\nu'_j$ must be an integer. Thus take $i$ of the $\nu'_j = \lfloor \frac{k}{t} \rfloor$ and the rest equal to $\lceil \frac{k}{t} \rceil$ subject to the constraint $i\lfloor \frac{k}{t} \rfloor + (t-i)\lceil \frac{k}{t} \rceil = k$. Then

$$\sum_{j=1}^{t} (\nu'_j)^2 = i \left\lfloor \frac{k}{t} \right\rfloor^2 + (t-i) \left\lceil \frac{k}{t} \right\rceil^2.$$

Solving the constraint for $i$ gives $i = t\lceil \frac{k}{t} \rceil - k$. The result follows. □

Theorem 2.14 gives the degree of the polynomial that counts the number of subgroups of order $p^k$ in $(\mathbb{Z}/p^t\mathbb{Z})^{n-1}$ for each $k \in [0, t(n-1)]$. Applying Theorem 2.9 and Theorem 2.14 gives a lower bound for the number of subrings of index $p^{t(n-1)+k}$ in $\mathbb{Z}^n$ for each $k \in [0, t(n-1)]$. We can now state a lower bound for subrings of index $p^e$ based on these results. Moreover, our result holds for the function that counts subrings in $\mathcal{O}_K$ of index $p^e$; however for consistency throughout this paper, we state the result for the function $f_n(p^e)$, which counts subrings in $\mathbb{Z}^n$ of index $p^e$.

**Corollary 2.15.** *Fix integers $n > 1$ and $e \geq n-1$. Fix an integer $t$ so that $t(n-1) \leq e \leq 2t(n-1)$. Let $k = e - t(n-1)$. Set $b = \lfloor \frac{e}{t} \rfloor - (n-1)$ and $c = \lceil \frac{e}{t} \rceil - (n-1)$. Then*

$$f_n(p^e) \geq p^{k(n-1)-c^2(k+t-ct)-b^2(ct-k)}.$$

**Remark 2.16.** The bound in Corollary 2.15 is as large as possible when $t \mid e$. Observe that the exponent of the bound reduces in this case. We find that if $t(n-1) \leq e \leq 2t(n-1)$ and $t \mid e$, then

$$f_n(p^e) \geq p^{(e-t(n-1))(2(n-1)-\frac{e}{t})}.$$

Finally, we prove Theorem 1.8.

**Proof of Theorem 1.8.** This theorem follows from Corollary 2.15, taking a maximum over all $t$ so that $t(n-1) \leq e \leq 2t(n-1)$. □

## 3. A method for counting subring matrices

We now introduce a combinatorial method for counting subrings due to Liu [9]. In Section 4, we will use this method to find a different bound for subrings of prime power index in $\mathbb{Z}^n$. In this section, we begin by describing Liu's method for counting subrings and we then describe a simpler algorithm for counting subrings based on row reduction.

**Definition 3.1.** A $n \times n$ matrix with entries in $\mathbb{Z}$ is in *Hermite normal form* if $A = (a_{ij})_{i,j}$ is upper triangular and $0 \leq a_{ij} < a_{ii}$ for all $1 \leq i < j \leq n$.

**Definition 3.2.** An $n \times n$ matrix $A$ in Hermite normal form is a *subring matrix* of index $k$ if

1. $\det(A) = k$.
2. The identity $(1, 1, \ldots, 1)^T$ is in the column span of $A$.
3. For all $1 \leq i \leq j \leq n$, if $v_i = (v_1, v_2, \ldots, v_n)^T$ and $v_j = (w_1, w_2, \ldots, w_n)^T$ are columns of $A$, then $v_i \circ v_j = (v_1 w_1, v_2 w_2, \ldots, v_n w_n)^T$ is in the column span of $A$.

A subring matrix $A$ is *irreducible* if $\det(A) = p^e$, every element in the first $n-1$ columns is divisible by $p$, and the last column is $(1, 1, \ldots, 1)^T$. A subring in $\mathbb{Z}^n$ of index $p^e$ is *irreducible* if for every $(v_1, \ldots, v_n) \in \mathbb{Z}^n$, $v_1 \equiv v_2 \equiv \cdots \equiv v_n \pmod{p}$.

Liu justifies the terminology "irreducible subring" by showing that any subring $S$ of index $p^e$ in $\mathbb{Z}^n$ can be written uniquely as a direct sum of irreducible subrings $S_i$ in $\mathbb{Z}^{n_i}$, see [9, Theorem 3.4].

In [9], Liu shows that there is a bijection between subrings in $\mathbb{Z}^n$ of index $k$ and subring matrices with determinant $k$. He also shows that there is a bijection between irreducible subrings of $\mathbb{Z}^n$ of index $p^e$ and irreducible subring matrices with determinant $p^e$.

Let $g_n(k)$ be the number of irreducible subrings of index $k$ in $\mathbb{Z}^n$. Observe that $g_n(k)$ is denoted $g_{n+1}(k)$ in [9].

**Proposition 3.3.** *[9, Proposition 4.4] There is a recurrence relation*

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

By the above recurrence relation, to understand $f_n(p^e)$, it suffices to understand $g_j(p^i)$ for each prime $p$, $j \leq n$ and $i \leq e$. In particular, we study the number of irreducible subring matrices of index $p^e$. These matrices have the following form

$$A = \begin{pmatrix} p^{e_1} & pa_{12} & pa_{13} & \cdots & pa_{1(n-1)} & 1 \\ & p^{e_2} & pa_{23} & \cdots & pa_{2(n-1)} & 1 \\ & & p^{e_3} & \cdots & pa_{3(n-1)} & 1 \\ & & & \ddots & \vdots & \vdots \\ & & & & p^{e_{n-1}} & 1 \\ & & & & & 1 \end{pmatrix}$$

where $0 \leq a_{ij} < p^{e_i - 1}$ for each $1 \leq i < j \leq n-1$.

**Definition 3.4.** We say that the matrix $A$ as written above has *diagonal* $(p^{e_1}, \ldots, p^{e_{n-1}}, 1)$.

Let $C_{n,e}$ denote the number of compositions of $e$ into $n-1$ parts. The diagonals corresponding to irreducible subring matrices with determinant $p^e$ are in bijection with the compositions in $C_{n,e}$. If a matrix has diagonal $(p^{e_1}, \ldots, p^{e_{n-1}}, 1)$, abusing notation we also say the matrix has diagonal $\alpha = (e_1, \ldots, e_{n-1}) \in C_{n,e}$. Let $g_\alpha(p)$ be the number of irreducible matrices with diagonal $\alpha \in C_{n,e}$. Then

$$g_n(p^e) = \sum_{\alpha \in C_{n,e}} g_\alpha(p).$$

The authors of [9] and [1] prove that $f_n(p^e)$ is polynomial in $p$ when $e \leq 8$ and $n > 0$ by providing exact formulas for the number of irreducible subrings with each possible diagonal and then using the recurrence relation from Proposition 3.3.

Let $\mathrm{Col}(A)$ denote the $\mathbb{Z}$-column span of the matrix $A$. For each $\alpha \in C_{n,e}$, the authors of [9] and [1] determine formulas for $g_\alpha(p)$ by considering all closure conditions $v_i \circ v_j \in \mathrm{Col}(A)$ explicitly in order to find conditions on the variables $a_{ij}$. In general, finding all the closure conditions for a given diagonal can be complicated.

**Example 3.5.** [1, Page 19] Let $\alpha = (3, 2, 1, 1)$. The corresponding matrix is

$$\begin{pmatrix} p^3 & pa_{12} & pa_{13} & pa_{14} & 1 \\ & p^2 & pa_{23} & pa_{24} & 1 \\ & & p & 0 & 1 \\ & & & p & 1 \\ & & & & 1 \end{pmatrix}$$

with $a_{1j} \in [0, p^2)$ for $j = 2, 3, 4$ and $a_{2j} \in [0, p)$ for $j = 3, 4$. Atanasov et al. illustrate their method for finding the closure conditions. For example, consider $v_2 \circ v_2 = (p^2a_{12}^2, p^4, 0, 0, 0)^T$. They note that $v_2 \circ v_2$ must be a linear combination of the first two columns, so it suffices to understand how to write $(p^2a_{12}^2, p^4)^T$ as a linear combination of $(p^3, 0)^T$ and $(pa_{12}, p^2)^T$. We must take $p^2$ times this second column, so we obtain

$$\begin{pmatrix} p^2a_{12}^2 \\ p^4 \end{pmatrix} = \lambda \begin{pmatrix} p^3 \\ 0 \end{pmatrix} + p^2 \begin{pmatrix} pa_{12} \\ p^2 \end{pmatrix} \tag{1}$$

for some $\lambda \in \mathbb{Z}$. In order for Equation (1) to hold, $p^3 \mid p^2a_{12}$ and thus $p \mid a_{12}$. Thus the closure condition corresponding to $v_2 \circ v_2$ is $a_{12} \equiv 0 \pmod{p}$. Atanasov et al. compute the closure conditions for other pairs of columns using similar methods and noting that the equations are simpler when they replace $a_{12}$ with $pa'_{12}$. The final conditions are

$$\begin{aligned} &(a_{13}^2 - a_{13}) - (a_{23}^2 - a_{23})a'_{12} \equiv 0 \pmod{p} \\ &(a_{14}^2 - a_{14}) - (a_{24}^2 - a_{24})a'_{12} \equiv 0 \pmod{p} \\ &a_{13}a_{14} - a_{23}a_{24}a'_{12} \equiv 0 \pmod{p}. \end{aligned}$$

We show that by using the method of row reduction, we can find these conditions in an algorithmic way. This method has two advantages. First, it simplifies proofs about counting the number of irreducible subrings with a given diagonal. Second, since it is algorithmic, it is easily implementable in a computer algebra system.

Recall that the closure conditions are of the form $v_i \circ v_j \in \mathrm{Col}(A)$ for each $1 \leq i \leq j \leq n$. These conditions are satisfied if and only if $A\vec{x}_{i,j} = v_i \circ v_j$ has a solution $\vec{x}_{i,j} \in \mathbb{Z}^n$ for every $1 \leq i \leq j \leq n$. By basic linear algebra, a solution $\vec{x}_{i,j}$ exists if and only if the last column in the reduced echelon form of the matrix $[A\ v_i \circ v_j]$ has integer entries. We illustrate the row reducing steps below. Note that we omit the column $(1, 1, \ldots, 1)^T$

corresponding to the identity in $\mathbb{Z}^n$ since it is clear that $v_i \circ (1, 1, \ldots, 1)^T$ is in the $\mathbb{Z}$-column span of $A$ for all $1 \leq i \leq n$ and if $i, j \neq n$, then the $n^{th}$ entry in $v_i \circ v_j$ is 0. Suppose we have a matrix

$$A = \begin{pmatrix} p^{e_1} & pa_{12} & pa_{13} & \cdots & pa_{1(n-1)} & x_1 \\ & p^{e_2} & pa_{23} & \cdots & pa_{2(n-1)} & x_2 \\ & & p^{e_3} & \cdots & pa_{3(n-1)} & x_3 \\ & & & \ddots & & \vdots \\ & & & & p^{e_{n-1}} & x_{n-1} \end{pmatrix}$$

where the last column contains the first $n-1$ entries of the vector $v_i \circ v_j = (x_1, x_2, \ldots, x_{n-1}, x_n)^T$ for some pair $(i, j)$ so that $1 \leq i \leq j \leq n-1$. We begin by dividing each row $i$ by $p^{e_i}$ in order to make every diagonal entry equal to 1, obtaining the matrix

$$A \to \begin{pmatrix} 1 & \frac{pa_{12}}{p^{e_1}} & \frac{pa_{13}}{p^{e_1}} & \cdots & \frac{pa_{1(n-1)}}{p^{e_1}} & \frac{x_1}{p^{e_1}} \\ & 1 & \frac{pa_{23}}{p^{e_2}} & \cdots & \frac{pa_{2(n-1)}}{p^{e_2}} & \frac{x_2}{p^{e_2}} \\ & & 1 & \cdots & \frac{pa_{3(n-1)}}{p^{e_3}} & \frac{x_3}{p^{e_3}} \\ & & & \ddots & & \vdots \\ & & & & 1 & \frac{x_{n-1}}{p^{e_{n-1}}} \end{pmatrix}.$$

Observe that since the matrix is upper triangular, it is not necessary to make any more divisions. From here, we row reduce and we note that finding conditions on $a_{ij}$ so that $v_i \circ v_j$ is in the $\mathbb{Z}$-span of the first $n-1$ columns is equivalent to finding conditions on $a_{ij}$ so that the entries in the last column are in $\mathbb{Z}$. Thus, for each fixed $v_i \circ v_j$, we are counting the number of solutions to expressions of the form

$$h_{ij}^{(c)} = \frac{f_{ij}^{(c)}(\vec{a_{ij}})}{p^r} \in \mathbb{Z} \tag{2}$$

where $f_{ij}^{(c)}$ is a multivariate polynomial with coefficients in $\mathbb{Z}$, $1 \leq c \leq n-1$, and $r$ is an integer depending on $i, j$, and $c$. Note that for this fixed $v_i \circ v_j$, $x_{i+1} = x_{i+2} = \cdots = x_{n-1} = 0$. This allows us to use the row reduction process on the smaller $i \times (i+1)$ matrix formed by taking the first $i$ columns of $A$, augmenting $v_i \circ v_j$, and then removing the rows $i+1, \ldots, n-1$. We will make use of this simplification in Section 4.

Let $p^r$ be the largest denominator that occurs in all expressions $h_{ij}^{(c)}$ in Equation (2). Then the rational functions $h_{ij}^{(c)}$ are in $\mathbb{Z}$ if and only if the numerators $f_{ij}^{(c)} \equiv 0 \mod p^r$. Thus counting the simultaneous system $h_{ij}^{(c)} \in \mathbb{Z}$ is essentially the same as counting points to a simultaneous vanishing of the polynomials $f_{ij}^{(c)}$ modulo $p^r$. Note that these problems are not exactly the same as the variables $a_{ij}$ live in the range $[0, p^{e_i - 1})$ and we may have $e_i - 1 > r$. However, since all expressions have denominator at worst $p^r$, then

the congruence conditions for the variables only matter modulo $p^r$. For any $e_i - 1 > r$, we can simply multiply the point count for the variety by $p^{e_i-1-r}$. Thus up to polynomial factors, it is sufficient to understand the varieties defined over $\mathbb{Z}/p^r\mathbb{Z}$ defined by the polynomials $f_{ij}^{(c)}$.

**Remark 3.6.** In general, counting points on varieties over a ring is a difficult problem. It is easier to consider varieties over $\mathbb{F}_p$, however these denominators that occur are often larger than $p$. Sometimes it is possible to reduce the denominators to all be $p$ by using clever substitution. In these cases, we can say more about the point counts of the varieties.

We summarize the method described in this section as follows.

**Algorithm 3.7.** *Input a diagonal* $(e_1, \ldots, e_{n-1})$ *with integers* $e_i \geq 0$ *for all* $1 \leq i \leq n-1$.

1. *Create the matrix*

$$A = \begin{pmatrix} p^{e_1} & pa_{12} & pa_{13} & \cdots & pa_{1(n-1)} & 1 \\ & p^{e_2} & pa_{23} & \cdots & pa_{2(n-1)} & 1 \\ & & p^{e_3} & \cdots & pa_{3(n-1)} & 1 \\ & & & \ddots & \vdots & \vdots \\ & & & & p^{e_{n-1}} & 1 \\ & & & & & 1 \end{pmatrix}$$

   *in the variables* $a_{ij}$ *for* $1 \leq i < j \leq n-1$. *If* $e_i = 0$ *or 1, set* $a_{ij} = 0$ *for all* $i < j \leq n-1$.
2. *For each* $v_i \circ v_j$ *with* $1 \leq i \leq j \leq n-1$, *row reduce* $[A\, v_i \circ v_j]$ *to* $A'$ *over* $\mathbb{Q}$. *Add the entries of the rightmost column of* $A'$ *to a list.*
3. *Return the list formed in Step 2. All elements in this list are of the form* $\frac{f_{ij}(\vec{a}_{ij})}{p^r}$ *for some* $r \geq 0$.

## 4. A new lower bound for $f_n(p^e)$ via irreducible subring matrices

We now provide a lower bound for the number of subrings in $\mathbb{Z}^n$ of index $p^e$ using techniques from Section 3. That is, we find a lower bound for $f_n(p^e)$ by bounding the number of *irreducible* subrings of index $p^e$ in $\mathbb{Z}^n$. These results will lead to a new lower bound for the abscissa of convergence of $\zeta^R_{\mathbb{Z}^n,p}(s)$, which will be discussed in Section 5.

### *4.1. Bounding the number of irreducible subring matrices*

Fix an integer $d \in [0, n-1]$ and let $k, \ell$ be positive integers so that $\ell \geq \lceil \frac{k}{2} \rceil$. Let $C_{n,d,k,\ell}$ denote the set of compositions of $kd + \ell(n-1-d)$ into $n-1$ parts that contain exactly $d$ terms equal to $k$ and $n-1-d$ terms equal to $\ell$. In other words, each $\alpha \in C_{n,d,k,\ell}$ is

a permutation of the composition $(k, k, \dots, k, \ell, \ell, \dots, \ell)$ with $k$ appearing $d$ times and $\ell$ appearing $n-1-d$ times.

**Proposition 4.1.** *Let $n > 1$. Fix an integer $d \in [0, n-1]$ and let $k, \ell$ be positive integers so that $\ell \geq \lceil \frac{k}{2} \rceil$. For a fixed $\alpha \in C_{n,d,k,\ell}$, let $A_\alpha$ be a matrix in Hermite normal form with diagonal $\alpha$ that satisfies the following conditions for each pair $1 \leq i < j \leq n-1$:*

1. *if $a_{ii} = p^k$ and $a_{jj} = p^\ell$, then $a_{ij} \equiv 0 \pmod{p^{\lceil \frac{k}{2} \rceil}}$*
2. *otherwise, $a_{ij} = 0$.*

*Then $A_\alpha$ is an irreducible subring matrix.*

**Proof.** Let $A_\alpha$ be as described in the statement of the proposition. We must show that $v_i \circ v_j \in \mathrm{Col}(A_\alpha)$ for all $1 \leq i \leq j \leq n$. Let $r_1, \dots, r_d$ be the columns containing $p^k$. There are three cases to consider.

First, suppose that $i = r_m$ for some integer $m \in [1, d]$. Then $v_i = (0, \cdots, 0, p^k, 0, \cdots, 0)^T$. Fix some integer $j \in [1, n]$. Suppose the $i^{th}$ entry of $v_j$ is equal to $x$. Then $v_i \circ v_j = x v_i \in \mathrm{Col}(A_\alpha)$. Notice that we made no assumption about the entries of $v_j$.

Second, suppose the $i^{th}$ entry of $v_i$ is $p^\ell$ and let $j > i$ such that $j \notin \{r_1, \dots, r_d\}$. The only possible nonzero entries in $v_i \circ v_j$ are in the rows $\{i_1, \dots, i_d\}$. Therefore $v_i \circ v_j \in \mathrm{Col}(A_\alpha)$ if and only if $v_i \circ v_j$ is a linear combination of $v_{r_1}, \dots, v_{r_d}$. By applying the technique established in Section 3, we need to understand whether the following augmented matrix has integer solutions

$$A'_\alpha = \begin{pmatrix} p^k & 0 & \cdots & 0 & p^{2\lceil \frac{k}{2} \rceil} a_{r_1 i} a_{r_1 j} \\ & p^k & \cdots & 0 & p^{2\lceil \frac{k}{2} \rceil} a_{r_2 i} a_{r_2 j} \\ & & \ddots & \vdots & \vdots \\ & & & p^k & p^{2\lceil \frac{k}{2} \rceil} a_{r_d i} a_{r_d j} \end{pmatrix}.$$

Observe that $v_i \circ v_j \in \mathrm{Col}(A_\alpha)$ if and only if

$$v = (p^{2\lceil \frac{k}{2} \rceil} a_{r_1 i} a_{r_1 j}\, ,\, p^{2\lceil \frac{k}{2} \rceil} a_{r_2 i} a_{r_2 j}\, ,\, \cdots\, ,\, p^{2\lceil \frac{k}{2} \rceil} a_{r_d i} a_{r_d j})^T \in \mathrm{Col}(A'_\alpha).$$

By applying the row reduction technique, we see that $v \in \mathrm{Col}(A'_\alpha)$ if and only if

$$p^k \mid p^{2\lceil \frac{k}{2} \rceil} a_{r_m i} a_{r_m j}$$

for each integer $m \in [1, d]$. This condition holds for all $m \in [1, d]$.

Finally, suppose that $v_i$ has a $p^\ell$ in the $i^{th}$ entry and consider $v_i \circ v_i$. Then $v_i \circ v_i \in \mathrm{Col}(A_\alpha)$ if and only if $v_i \circ v_i$ is a linear combination of $v_i$ and $v_{r_1}, \dots, v_{r_d}$. Consider the matrix

$$A'_\alpha = \begin{pmatrix} p^k & 0 & \cdots & 0 & p^{\lceil \frac{k}{2} \rceil} a_{r_1 i} & p^{2\lceil \frac{k}{2} \rceil} a_{r_1 i}^2 \\ & p^k & \cdots & 0 & p^{\lceil \frac{k}{2} \rceil} a_{r_2 i} & p^{2\lceil \frac{k}{2} \rceil} a_{r_2 i}^2 \\ & & \ddots & \vdots & \vdots & \vdots \\ & & & p^k & p^{\lceil \frac{k}{2} \rceil} a_{r_d i} & p^{2\lceil \frac{k}{2} \rceil} a_{r_d i}^2 \\ & & & & p^\ell & p^{2\ell} \end{pmatrix}.$$

After applying the row reduction method, $v_i \circ v_i \in \mathrm{Col}(A_\alpha)$ if and only if

$$p^k \mid \left( p^{2\lceil \frac{k}{2} \rceil} a_{r_m i}^2 - p^{\ell + \lceil \frac{k}{2} \rceil} a_{r_m i} \right)$$

for all integers $m \in [1, d]$. This holds for all possible choices of $a_{r_m i}$ since $\ell \geq \lceil \frac{k}{2} \rceil$. □

**Example 4.2.** Let $\alpha = (2, 1, 2, 1, 2)$. The matrix $A_\alpha$ corresponding to Proposition 4.1 has the form

$$\begin{pmatrix} p^2 & pa_{12} & 0 & pa_{14} & 0 & 1 \\ & p & 0 & 0 & 0 & 1 \\ & & p^2 & pa_{34} & 0 & 1 \\ & & & p & 0 & 1 \\ & & & & p^2 & 1 \\ & & & & & 1 \end{pmatrix}.$$

There are exactly $p^3$ irreducible subring matrices of this form since $A_\alpha$ is a subring matrix for any choice of $a_{12}, a_{14}, a_{34} \in [0, p)$.

**Example 4.3.** Let $\alpha = (3, 5, 3, 3, 5)$. Setting $k = 5$, we have $\lceil \frac{k}{2} \rceil = 3$. The matrix $A_\alpha$ corresponding to Proposition 4.1 has the form

$$\begin{pmatrix} p^3 & 0 & 0 & 0 & 0 & 1 \\ & p^5 & p^3 a_{23} & p^3 a_{24} & 0 & 1 \\ & & p^3 & 0 & 0 & 1 \\ & & & p^3 & 0 & 1 \\ & & & & p^5 & 1 \\ & & & & & 1 \end{pmatrix}.$$

When $i = 2$, $a_{ij} \in [0, p^2)$. There are exactly $p^4$ such irreducible subrings matrices.

We now discuss a method for computing the number of subring matrices that have the form given in Proposition 4.1.

**Definition 4.4.** A *north-east lattice path* $P$ is a path in $\mathbb{Z}^2$ starting at the origin and ending at $(u, v)$ so that every step in the path is either a step one unit to the north or one unit to the east.

The *area* of a path is the area enclosed by the path, the $x$- and $y$-axes, and the line $x = u$. Denote the area by $\mathrm{Area}(P)$.

Fix $\alpha \in C_{n,d,k,\ell}$ and let $A_\alpha$ be a matrix as in Proposition 4.1. Let $P_\alpha$ denote the lattice path from $(0,0)$ to $(n-1-d,d)$ so that the $i^{th}$ step in the path is a northerly step if the $i^{th}$ entry of $\alpha$ is $k$ and is an easterly step if the $i^{th}$ entry of $\alpha$ is $\ell$.

**Theorem 4.5.** *Let $\alpha \in C_{n,d,k,\ell}$ and let $A_\alpha$ be as in Proposition 4.1. Then the number of such matrices $A_\alpha$ is equal to $p^{(k-\lceil \frac{k}{2} \rceil)\cdot Area(P_\alpha)}$.*

**Proof.** Observe that a non-diagonal element $a_{ij} \in A_\alpha$ is nonzero if and only if $i < j$ and $\alpha_i = k, \alpha_j = \ell$. In this case any choice of $a_{ij} \in [0, p^{k-\lceil \frac{k}{2} \rceil})$ leads to an irreducible subring matrix. By the definition of $P_\alpha$, we see that

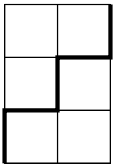
$$\text{Area}(P_\alpha) = \#\{i < j \,:\, \alpha_i = k \text{ and } \alpha_j = \ell\}.$$

Therefore the number of irreducible subring matrices $A_\alpha$ satisfying the conditions in Proposition 4.1 is

$$\left(p^{(k-\lceil \frac{k}{2} \rceil)}\right)^{\text{Area}(P_\alpha)}. \quad \square$$

**Corollary 4.6.** *For each $\alpha \in C_{n,d,k,\ell}$, we have $g_\alpha(p) \geq p^{(k-\lceil \frac{k}{2} \rceil)\cdot Area(P_\alpha)}$.*

**Example 4.7.** Let $\alpha = (2,1,2,1,2)$. The north-east lattice path $P_\alpha$ goes from $(0,0)$ to $(2,3)$, following the steps: north, east, north, east, north. This path is depicted below.



The area of this path is equal to 3 and $k - \lceil \frac{k}{2} \rceil = 1$, verifying our claim in Example 4.2 that there are exactly $p^3$ irreducible subring matrices that have diagonal $\alpha$ and satisfy the properties listed in Proposition 4.1.

**Remark 4.8.** For each $\alpha \in C_{n,d,k,\ell}$ let $A_\alpha$ be a matrix satisfying Proposition 4.1. Let $P_\alpha$ be the corresponding north-east lattice path. Set $\gamma = (k,k,\ldots,k,\ell,\ldots,\ell) \in C_{n,d,k,\ell}$. Observe that $\text{Area}(P_\gamma) \geq \text{Area}(P_\alpha)$ for all $\alpha \in C_{n,d,k,\ell}$. Therefore the degree of the main term in our bound is always equal $(k - \lceil \frac{k}{2} \rceil)\text{Area}(P_\gamma)$.

**Corollary 4.9.** *Set $\gamma = (k,\ldots,k,\ell,\ldots,\ell)$. Then $g_\gamma(p) \geq p^{(k-\lceil \frac{k}{2} \rceil)d(n-1-d)}$.*

**Proof.** The north-east lattice path $P_\gamma$ is a rectangle with vertices $(0,0), (n-1-d,0), (n-d-1,d)$, and $(0,d)$. This rectangle has area $d(n-1-d)$. The result follows from Theorem 4.5. $\square$

To conclude this section, we show that the method of counting subrings recovers the bound for $f_n(p^{n-1+d})$ when $d \in [0, n-1]$ given in Proposition 2.3, thus giving a different proof of this proposition.

**Lemma 4.10.** *[3, Page 116] Let $\mathcal{P}$ be the set of north-east lattice paths from $(0,0)$ to $(u,v)$ and let $q$ be a prime power. Then*

$$\sum_{P \in \mathcal{P}} q^{Area(P)} = \begin{bmatrix} u+v \\ v \end{bmatrix}_q.$$

**Corollary 4.11.** *Fix integers $n > 1$ and $d \in [0, n-1]$. Then $g_n(p^{n-1+d}) \geq \begin{bmatrix} n-1 \\ d \end{bmatrix}_p$.*

**Proof.** Recall that $g_n(p^e) = \sum_{\alpha \in C_{n,e}} g_\alpha(p)$. We can bound $g_n(p^{n-1+d})$ from below by counting the number of irreducible subrings with diagonal $\alpha \in C_{n,d,2,1}$. The set $C_{n,d,2,1}$ is in bijection with the set of north-east lattice paths from $(0,0)$ to $(d, n-1-d)$. Fix some $\alpha \in C_{n,d,2,1}$. By Theorem 4.5, for the corresponding lattice path $P_\alpha$, $g_\alpha(p) \geq p^{\text{Area}(P_\alpha)}$. By Lemma 4.10,

$$g_n(p^{n-1+d}) \geq \sum_{\alpha \in C_{n,d,2,1}} g_\alpha(p) \geq \begin{bmatrix} n-1 \\ d \end{bmatrix}_p. \quad \square$$

Since $f_n(p^e) \geq g_n(p^e)$ for all $e \geq 0$, $f_n(p^{n-1+d}) \geq \begin{bmatrix} n-1 \\ d \end{bmatrix}_p$. Thus this method of bounding subrings in $\mathbb{Z}^n$ gives exactly the same bound as Proposition 2.3.

### *4.2. Optimizing the bound for $g_n(p^e)$*

In this section, we optimize the exponent $(k - \lceil \frac{k}{2} \rceil) d(n-1-d)$. Fixing $n$, Corollary 4.9 implies that

$$f_n(p^e) \geq g_n(p^e) \geq p^{(k - \lceil \frac{k}{2} \rceil) d(n-1-d)}$$

for each $0 \leq d \leq n-1$ and $k, \ell \in \mathbb{Z}_{\geq 1}$ so that $\ell \geq \frac{k}{2}$ and $e \leq kd + \ell(n-1-d)$. It is important that $k, \ell \geq 1$; if $e < n-1$, then $g_n(p^e) = 0$. In order to obtain the best possible bound for $f_n(p^e)$ in terms of $n$ and $e$, we optimize the exponent $(k - \lceil \frac{k}{2} \rceil) d(n-1-d)$ over $\mathbb{Z}$.

**Proof of Theorem 1.9.** The term $k - \lceil \frac{k}{2} \rceil$ is maximized when $k = 2j$ for some $j \in \mathbb{N}$. Recall that we are subject to the constraint $kd + \ell(n-1-d) \geq e$ for some $\ell \geq \lceil \frac{k}{2} \rceil$. Therefore $j \leq \lfloor \frac{e}{d+(n-1)} \rfloor$. Set $j = \lfloor \frac{e}{d+(n-1)} \rfloor$ so that it is as large as possible.

Then $(k - \lceil \frac{k}{2} \rceil) d(n-1-d) \geq \lfloor \frac{e}{d+(n-1)} \rfloor \cdot d(n-1-d)$. Taking a maximum over all $0 \leq d \leq n-1$ gives the result. $\square$

The above proposition gives the best possible bound for $(k - \lceil \frac{k}{2} \rceil) d(n-1-d)$ subject to the constraints that $\ell \geq \lceil \frac{k}{2} \rceil$ and $kd + \ell(n-1-d) \geq e$. We now give a weakening of Theorem 1.9, which will be helpful later. The benefit of the following proposition is that the maximum is taken over real numbers rather than integers.

**Proposition 4.12.** *Suppose that $e \geq n-1$. Let*

$$c(n,e) = \max_{0 \leq C \leq 1} \left( e \left( \frac{C - C^2}{C+1}(n-1) + \frac{C-1}{C+1} \right) - \left( (C-C^2)(n-1)^2 + (C-1)(n-1) \right) \right)$$

*where the maximum is taken over $\mathbb{R}$. Then $f_n(p^e) \geq p^{c(n,e)}$.*

**Proof.** For any fixed integer $d \in [0, n-1]$, $d = \lfloor C(n-1) \rfloor$ for some real number $C \in [0,1]$. Starting from the bound given in Theorem 1.9, for any $C \in [0,1]$,

$$\begin{aligned}
&\left(k - \lceil \frac{k}{2} \rceil\right) d\,(n-1-d) \\
&\geq \left\lfloor \frac{e}{\lfloor C(n-1) \rfloor + (n-1)} \right\rfloor \cdot \lfloor C(n-1) \rfloor \cdot (n-1-\lfloor C(n-1) \rfloor) \\
&\geq \left( \frac{e}{\lfloor C(n-1) \rfloor + (n-1)} - 1 \right) (C(n-1)-1)(1-C)(n-1) \\
&\geq \left( \frac{e}{(C+1)(n-1)} - 1 \right) (C(n-1)-1)(1-C)(n-1) \\
&= \left( \frac{e}{(C+1)(n-1)} - 1 \right) \left( (C-C^2)(n-1)^2 + (C-1)(n-1) \right) \\
&= e \left( \frac{C-C^2}{C+1}(n-1) + \frac{C-1}{C+1} \right) - \left( (C-C^2)(n-1)^2 + (C-1)(n-1) \right).
\end{aligned}$$

Taking a maximum over all real numbers $C \in [0,1]$ gives the result. □

### *4.3. Comparison of Theorems 1.8 and 1.9*

Consider the bounds from Theorems 1.8 and 1.9. We compared these lower bounds for various values of $n$ and $e$ in Sage and found that they grow at very similar rates. The bound from Theorem 1.8 seems to be slightly better than the bound from Theorem 1.9 for each fixed $n$ and for sufficiently large $e$. Let $h(n,e)$ be the bound from Theorem 1.8 and let $b(n,e)$ be the bound from Theorem 1.9. We provide Table 2 summarizing some of this data.

Next, we show that there are subrings that are counted using one of the two techniques, but not the other.

**Table 2**
Values of the bounds from Theorems 1.8 and 1.9.

| $n$ | $e$ | $\log_p h(n,e)$ | $\log_p b(n,e)$ |
|---|---|---|---|
| 6 | 10 | 0 | 6 |
| 6 | 20 | 16 | 12 |
| 6 | 30 | 24 | 24 |
| 6 | 300 | 256 | 252 |
| 6 | 1000 | 856 | 852 |
| 10 | 10 | 8 | 8 |
| 10 | 20 | 16 | 20 |
| 10 | 30 | 36 | 40 |
| 10 | 300 | 460 | 460 |
| 10 | 1000 | 1538 | 1520 |

**Example 4.13.** Let $n = 3$ and $e = 7$. Consider the following matrix.

$$A = \begin{pmatrix} p^3 & p^2 & 1 \\ 0 & p^4 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

This is an irreducible subring matrix with diagonal $\alpha = (3, 4)$. The matrix $A$ satisfies Proposition 4.1. Therefore our technique from Section 4 counts the matrix $A$ in the lower bound for $f_3(p^7)$.

Let $G$ be the subgroup generated by the columns of $A$. Then $G$ does not satisfy the condition $\mathbb{Z} + p^4\mathbb{Z}^3 \subset G \subset \mathbb{Z} + p^2\mathbb{Z}^3$ since $(0, p^4, 0)^T$ is not in the $\mathbb{Z}$-column span of $A$. Therefore our technique from Section 2.2 does not count the subgroup corresponding to $A$.

**Example 4.14.** Let $n = 4$. Let $G$ be the subgroup generated by $(1, 1, 1, 1)$, $(p^3, 0, 0, 0)$, $(p^2, p^3, 0, 0)$, and $(0, 0, p^2, 0)$. Then $\mathbb{Z} + p^4\mathbb{Z}^4 \subset G \subset \mathbb{Z} + p^2\mathbb{Z}^4$.

The subgroup $G$ corresponds to the matrix

$$A = \begin{pmatrix} p^3 & p^2 & 0 & 1 \\ 0 & p^3 & 0 & 1 \\ 0 & 0 & p^2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Our technique from Section 2.2 includes $G$ in the lower bound for $f_4(p^8)$. However, our technique from Section 4 does not since $A$ violates the conditions in the statement of Proposition 4.1.

It is not too difficult to give conditions on when the columns of a subring matrix satisfying Proposition 4.1 will generate a subgroup $G$ satisfying Lemma 2.1. We state this below in Proposition 4.15. However, it is much more difficult to determine when a subgroup $G$ satisfying Lemma 2.1 corresponds to a subring matrix $M_G$ satisfying Proposition 4.1. The main obstacle here is that the closure conditions to determine whether $M_G$ is a subring matrix are complicated.

**Proposition 4.15.** *Let $A$ be a subring matrix satisfying Proposition 4.1 with columns $v_1, \dots, v_{n-1}, (1, \dots, 1)^T$. Let $G$ be the subgroup generated by $v_1^T, \dots, v_{n-1}^T$, and $(1, \dots, 1)$. Then there exists an $r$ such that $\mathbb{Z} + p^{2r}\mathbb{Z}^n \subset G \subset \mathbb{Z} + p^r\mathbb{Z}^n$ if and only if*

$$\ell = \begin{cases} \frac{k}{2} & 2 \mid k \\ \frac{k+1}{2} \text{ or } \frac{k+3}{2} & 2 \nmid k. \end{cases}$$

**Proof.** Let $w_1 = (1, 0, \dots, 0)$, $w_2 = (0, 1, \dots, 0), \dots, w_{n-1} = (0, \dots, 0, 1, 0)$, and $w_n = (1, \dots, 1)$ be a basis for $\mathbb{Z}^n$. By Proposition 2.8, it suffices to understand conditions on $r, k$, and $\ell$ so that $p^{2r}w_i$ is contained in the lattice spanned by $G$ and $v_i$ is contained in the lattice $L$ spanned by $\{p^r w_1, \dots, p^r w_{n-1}\}$ for all $1 \leq i \leq n-1$.

Observe that $v_i$ is in $L$ if and only if

$$r \leq \min\left(\left\lceil \frac{k}{2} \right\rceil, k, \ell\right) = \left\lceil \frac{k}{2} \right\rceil.$$

By applying the row reduction method, $p^{2r}w_i$ is in the lattice spanned by $G$ if and only if the following three conditions hold:

1. $k \leq 2r$
2. $\ell \leq 2r$
3. $k \leq 2r - \ell + \lceil \frac{k}{2} \rceil$.

We can simplify the four conditions to the following:

1. $r = \lceil \frac{k}{2} \rceil$
2. $\lceil \frac{k}{2} \rceil \leq \ell \leq 3\lceil \frac{k}{2} \rceil - k$. □

Finally, we demonstrate an upper bound for each of our lower bounds, which can be derived as corollaries of Theorems 1.8 and 1.9 respectively.

**Corollary 4.16.** *Let $h(n, e)$ be the exponent of the lower bound from Theorem 1.8. Then $h(n, e) \leq (3 - 2\sqrt{2})(n-1)e$.*

**Proof.** By Remark 2.16, for each fixed $t \in [\frac{e}{2(n-1)}, \frac{e}{n-1}]$, we have

$$h(n, e) \leq (e - t(n-1))(2(n-1) - \frac{e}{t}).$$

Taking a maximum over all $t$ in this range over $\mathbb{R}$ gives the result. □

**Corollary 4.17.** *Let $b(n, e)$ be the exponent of the lower bound from Theorem 1.9. Then $b(n, e) \leq (3 - 2\sqrt{2})(n-1)e$.*

**Proof.** Removing the floor function and optimizing over $\mathbb{R}$ gives the result. □

It is interesting to note that our two different methods lead to lower bounds that are very close asymptotically.

## 5. Divergence of local factors

In this section, we use the lower bounds for $f_n(p^e)$ from Section 4 to find lower bounds for the abscissa of convergence of $\zeta^R_{\mathbb{Z}^n,p}(s)$. It is less clear how to use the bound from Theorem 1.8 to derive a result about the divergence of $\zeta^R_{\mathbb{Z}^n,p}(s)$ since the exponent is quadratic in $e$. While some results are known about the divergence of $\zeta^R_{\mathbb{Z}^n}(s)$, not much is known about the divergence of the local factors. We fill this gap and also provide a partial answer to Question 1.5.

For each lower bound $p^B$ of $f_n(p^e)$ given in Section 4, we can determine the poles of the series $\sum_{e\geq n-1} p^B p^{-es}$. Since $f_n(p^e) \geq p^B$ whenever $e \geq n-1$, then $\zeta^R_{\mathbb{Z}^n,p}(s) \geq \sum_{e\geq n-1} p^B p^{-es}$. Therefore $\zeta^R_{\mathbb{Z}^n,p}(s)$ diverges whenever the simpler series diverges.

First, let

$$b(n,e) = \left\lfloor \frac{e}{n-1+d} \right\rfloor \cdot d(n-1-d)$$

as in Theorem 1.9. In order to simplify the geometric series, we set

$$F(d,e,n) = \frac{ed(n-1-d)}{n-1+d} - d(n-1-d)$$

and note that $b(n,e) \geq F(d,e,n)$

**Lemma 5.1.** *Fix $n > 1$. Then $\sum_{e\geq n-1} p^{F(d,e,n)} p^{-es}$ diverges for all $s$ such that $\Re(s) \leq \frac{d(n-1-d)}{n-1+d}$.*

**Proof.** Consider

$$\sum_{e\geq n-1} p^{F(d,e,n)} p^{-es} = p^{-d(n-1-d)} \sum_{e\geq n-1} \left(p^{\frac{d(n-1-d)}{n-1+d} - s}\right)^e.$$

This series diverges for all $s$ such that $\Re(s) \leq \frac{d(n-1-d)}{n-1+d}$. □

**Lemma 5.2.** *Let $n > 1$ and*

$$G(C,e,n) = e\left(\frac{C-C^2}{C+1}(n-1) + \frac{C-1}{C+1}\right) - \left((C-C^2)(n-1)^2 + (C-1)(n-1)\right).$$

*Then $\sum_{e\geq n-1} p^{G(C,e,n)} p^{-es}$ diverges for all $s$ such that $\Re(s) \leq \left(\frac{C-C^2}{C+1}(n-1) + \frac{C-1}{C+1}\right)$.*

**Proof.** Consider

$$\sum_{e\geq n-1} p^{G(C,e,n)}p^{-es} = p^{-((C-C^2)(n-1)^2+(C-1)(n-1))} \sum_{e\geq n-1} p^{e\left(\frac{C-C^2}{C+1}(n-1)+\frac{C-1}{C+1}\right)}p^{-es}$$
$$= p^{-((C-C^2)(n-1)^2+(C-1)(n-1))} \sum_{e\geq n-1} \left(p^{\left(\frac{C-C^2}{C+1}(n-1)+\frac{C-1}{C+1}-s\right)}\right)^e$$

The series diverges for all $s$ such that $\Re(s) \leq \frac{C-C^2}{C+1}(n-1)+\frac{C-1}{C+1}$. □

Consider the bound $G(C,e,n)$ used in Lemma 5.2. In order to maximize $G(C,e,n)$ as a function in $n$, consider $\max_{0\leq C\leq 1} \frac{C-C^2}{C+1} = 3-2\sqrt{2}$. The maximum occurs when $C=\sqrt{2}-1$. Plugging in this value of $C$, we obtain the following corollary.

**Corollary 5.3.** *Let $n>1$ and let $G(C,e,n)$ be as in Lemma 5.2. Setting $C=\sqrt{2}-1$, we find that $\sum_{e\geq n-1} p^{G(1-\sqrt{2},n)}p^{-es}$ diverges for all $s$ such that $\Re(s) \leq (3-2\sqrt{2})(n-1)+1-\sqrt{2}$.*

Lemma 5.1 and Corollary 5.3 combined give the proof of Theorems 1.10. Recall that

$$\sum_{e\geq 0} f_n(p^e)p^{-es} \geq \sum_{e\geq n-1} p^B p^{-es}$$

for each choice of bound $B$ as above. Therefore the previous lemmas give regions where the local factors of $\zeta^R_{\mathbb{Z}^n}(s)$ diverge. Observe that $f_n(p^e) \geq p^{F(d,e,n)}$ for all integers $d \in [0,n-1]$ and $f_n(p^e) \geq p^{G(C,e,n)}$ for all real numbers $C \in [0,1]$, so we can take a maximum over all $d$ in Lemma 5.1 or over all $C$ in Lemma 5.2 to find the largest possible regions of divergence for these geometric series.

It is possible that there are poles further to the right of the ones found above in the given geometric series. Consider the bound in Lemma 5.1. When $s > c_7(n)$, $\zeta^R_{\mathbb{Z}^n}(s)$ diverges if

$$\sum_p p^{-d(n-1-d)} \cdot \frac{p^{\frac{d(n-1-d)(n-1)}{n-1+d}-(n-1)s}}{1-p^{\frac{d(n-1-d)}{n-1+d}-s}}$$

diverges for all $0 \leq d \leq n-1$. It is a simple computation to show that this series converges on $s > c_7(n)$. Similar computations show that we cannot find a larger region of divergence for the local factors by using Lemma 5.2 and Corollary 5.3 either. Thus Theorem 1.10 gives the best possible lower bound for the abscissa of convergence of $\zeta^R_{\mathbb{Z}^n,p}(s)$ given our lower bounds for $f_n(p^e)$.

**Proof of Theorem 1.10.** Set

$$b(n,e) = \left\lfloor \frac{e}{n-1+d} \right\rfloor d(n-1-d)$$

and

$$F(d,e,n) = \frac{ed(n-1-d)}{n-1+d} - d(n-1-d).$$

By Theorem 1.9, $f_n(p^e) \geq p^{b(n,e)} \geq p^{F(d,e,n)}$ for each $e \geq n-1$. Therefore

$$\zeta^R_{\mathbb{Z}^n,p}(s) = \sum_{e\geq 0} f_n(p^e)p^{-es} \geq \sum_{e\geq n-1} p^{F(d,e,n)}p^{-es}.$$

By Lemma 5.1, the simpler geometric series diverges for all $s$ such that $\Re(s) \leq \frac{d(n-1-d)}{n-1+d}$ and thus $\zeta^R_{\mathbb{Z}^n,p}(s)$ diverges on the same region. Taking a maximum over all integers $d \in [0, n-1]$ and applying a Tauberian theorem gives the result. □

The following proposition is strictly worse than Theorem 1.10 – it comes from choosing a specific value of $C \in [0,1]$ – but is easier to use directly.

**Proposition 5.4.** *Fix $n > 1$. Then $\zeta^R_{\mathbb{Z}^n,p}(s)$ diverges for all $s$ such that*

$$\Re(s) \leq (3-2\sqrt{2})(n-1) + 1 - \sqrt{2}.$$

**Proof.** The proof is similar to that of Theorem 1.10, replacing Lemma 5.1 with Corollary 5.3. □

## 6. Orders in a number field

We now study a related zeta function and use results from previous sections to find new lower bounds for the number of orders in a number field. Let $K$ be a number field of degree $n$ with ring of integers $\mathcal{O}_K$. Let

$$F_K(k) = \#\{\mathcal{O} \subset \mathcal{O}_K \,:\, \mathcal{O} \text{ is a order of } \mathcal{O}_K \text{ and } |\mathrm{disc}(\mathcal{O})| = k\}.$$

Recall that there is a relation between $\mathrm{disc}(\mathcal{O})$ and $\mathrm{disc}(\mathcal{O}_K)$ given by

$$\mathrm{disc}(\mathcal{O}) = \mathrm{disc}(\mathcal{O}_K)[\mathcal{O}_K : \mathcal{O}]^2.$$

Consider the order zeta function

$$\eta_K(s) = \sum_{\mathcal{O} \text{ order of } \mathcal{O}_K} |\mathrm{disc}(\mathcal{O})|^{-s} = \sum_{k=1}^{\infty} F_K(k)k^{-s}.$$

This zeta function is closely related to the zeta function

$$\tilde{\eta}_K(s) = \sum_{\mathcal{O} \text{ order of } \mathcal{O}_K} [\mathcal{O}_K : \mathcal{O}]^{-s}$$

by the relation $\eta_K(s) = |\mathrm{disc}(\mathcal{O}_K)|^{-s}\tilde{\eta}_K(2s)$.

Notice that $\tilde{\eta}_K(s)$ also has an Euler product $\prod_p \tilde{\eta}_{K,p}(s)$ indexed over the rational primes where

$$\tilde{\eta}_{K,p}(s) = \sum_{\mathcal{O} \text{ order of } \mathcal{O}_K} [\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p : \mathcal{O}]^{-s}.$$

If $p$ splits completely, then $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathbb{Z}_p^n$. Therefore for all primes $p$ that split completely,

$$\tilde{\eta}_{K,p}(s) = \zeta^R_{\mathbb{Z}_p^n}(s) = \zeta^R_{\mathbb{Z}^n,p}(s).$$

Let $N_K(B) = \sum_{X \leq B} F_K(X)$. The following theorem is due to Kaplan, Marcinek, and Takloo-Bighash [8]; see their paper for details on $r_2$, which is a constant that depends on the Galois group of the normal closure of $K/\mathbb{Q}$.

**Theorem 6.1.** *[8, Theorem 2]*

1. *Let $n \leq 5$. Then there exists a constant $C_K > 0$ so that*

$$N_K(B) \sim C_K B^{\frac{1}{2}} (\log B)^{r_2 - 1}$$

   *as $B \to \infty$.*
2. *Let $n > 5$. Then for every $\epsilon > 0$,*

$$B^{\frac{1}{2}} (\log B)^{r_2-1} \ll N_K(B) \ll_\epsilon B^{\frac{n}{4} - \frac{7}{12} + \epsilon}$$

   *as $B \to \infty$.*

We can use Theorem 1.6 along with a Tauberian theorem to obtain an improvement on the lower bound in Theorem 6.1(2).

**Theorem 6.2.** *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 $B^{\frac{1}{2}a(n)} \ll N_K(B)$ as $B \to \infty$.*

As a consequence of Theorem 1.10 and Proposition 5.4, we can also bound the abscissa of convergence of $\tilde{\eta}_{K,p}(s)$.

**Theorem 6.3.** *Let $n > 1$ be an integer and let $K$ be a degree $n$ number field. Then*

1. *The zeta function $\tilde{\eta}_{K,p}(s)$ diverges for all $s$ such that $\Re(s) \leq \frac{c_7(n)}{2}$.*

2. *The zeta function* $\tilde{\eta}_{K,p}(s)$ *diverges for all* $s$ *such that*

$$\Re(s) \leq \frac{(3-2\sqrt{2})(n-1)+1-\sqrt{2}}{2}.$$

## 7. Further questions

In this process of bounding $f_n(p^e)$ by counting irreducible subrings, we made a few assumptions. First, we only considered compositions $\alpha \in C_{n,d,k,\ell}$. Second, we set several entries in the matrix with diagonal $\alpha$ equal to 0 and the rest equal to $p^{\lceil \frac{k}{2} \rceil} a_{ij}$ for some $a_{ij} \in [0, p^{k-\lceil \frac{k}{2} \rceil})$. Lastly, we bounded $f_n(p^e)$ by $g_n(p^e)$. These simplifications lead to the following questions.

**Question 7.1.** *Let* $d \in [0, n-1]$ *be an integer and let* $k, \ell$ *be positive integers so that* $\ell \geq \lceil \frac{k}{2} \rceil$. *Let* $\alpha \in C_{n,d,k,\ell}$.

1. *Does the main term of* $g_n(p^e)$ *always come from* $g_\alpha(p)$ *for some* $\alpha \in C_{n,d,k,\ell}$*?*
2. *Is* $p^{(k-\lceil \frac{k}{2} \rceil) Area(P_\alpha)}$ *always the main term of* $g_\alpha(p)$*?*
3. *Do* $f_n(p^e)$ *and* $g_n(p^e)$ *always have the same main terms?*

The answer to Question 7.1(1) is no. For example, Atanasov et al. [1] show that $g_5(p^7)$ is a polynomial of degree 4, with the main term coming from the compositions $(3,2,1,1)$ and $(2,3,1,1)$. It is unclear how often pairs $n$ and $e$ are counterexamples to Question 7.1(1). It is also unknown how far off the main term of $g_n(p^e)$ can be from the main term of $\max_\alpha g_\alpha(p)$ where the maximum is taken over all $\alpha$ of the form above.

It may be the case that a composition of the form $\alpha \in C_{n,d,k,\ell}$ leads to the main term of $g_n(p^e)$, but our lower bound for the number of irreducible subring matrices with diagonal corresponding to $\alpha$ does not give the main term. While the answer to Question 7.1(2) is not understood for most pairs $n$ and $e$, we give a partial answer. First, we state some necessary propositions.

**Proposition 7.2.** *[9, Proposition 4.3] Fix* $n > 1$. *Then*

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

Corollary 3.7 in [1] gives an exact formula for $g_n(p^{n+1})$. To save space, we rewrite their corollary in terms of the degree of $g_n(p^{n+1})$.

**Corollary 7.3.** *[1, Corollary 3.7] Let* $n \geq 4$. *The function* $g_n(p^{n+1})$ *is a polynomial in* $p$ *of degree* $2n-6$.

**Example 7.4.** Let $\alpha \in C_{n,d,2,1}$. Observe that $e = n-1+d$.

When $d = 0$, $e = n - 1$. Proposition 7.2 shows that $g_n(p^{n-1}) = 1$, which matches the bound from Theorem 1.9. We see that $g_n(p^{n-1}) = \begin{bmatrix} n-1 \\ 0 \end{bmatrix}_p$.

When $d = 1$, $e = n$. The second part of Proposition 7.2 shows that the main term of $g_n(p^n)$ is $p^{n-2}$. This agrees with Theorem 1.9. Further, $g_n(p^n) = \frac{p^{n-1}-1}{p-1} = \begin{bmatrix} n-1 \\ 1 \end{bmatrix}_p$, so our method counts all possible irreducible subrings of index $p^n$.

When $d = 2$, $e = n + 1$. By Corollary 7.3, the main term of $g_n(p^{n+1})$ is $p^{2n-6}$, which matches the main term in Theorem 1.9. In this case, our lower bound $g_n(p^{n+1}) \geq \begin{bmatrix} n-1 \\ 2 \end{bmatrix}_p$ is strictly smaller than the actual formula for $g_n(p^{n+1})$, but the main term is the same. In fact,

$$g_n(p^{n+1}) - \begin{bmatrix} n-1 \\ 2 \end{bmatrix}_p = \binom{n}{2} p^{n-2}.$$

Lastly, we provide a partial answer to Part 3 of Question 7.1. We do not understand the relationship between the main term of $f_n(p^e)$ and the main term of $g_n(p^e)$ for each fixed $n$ and $e \geq n - 1$. In fact, there are classes of examples for which the main term for $f_n(p^e)$ is greater than the main term of $g_n(p^e)$.

**Example 7.5.** Let $e = n - 1$. By Proposition 7.2, $g_n(p^{n-1}) = 1$ for all $n \geq 2$. However, the term $f_1(p^0)g_{n-1}(p^{n-1})$ appears in the recurrence relation stated in Proposition 3.3. Proposition 7.2 implies that $g_{n-1}(p^{n-1})$ is a polynomial in $p$ with main term $p^{n-3}$. Therefore $f_n(p^{n-1}) \geq p^{n-3}$ whereas $g_n(p^{n-1}) = 1$.

In some cases we are likely not capturing the highest order term of $f_n(p^e)$ by using the bound $f_n(p^e) \geq g_n(p^e)$. However, this is currently the best known approach for counting subrings via subring matrices.

In this paper, we give two new lower bounds for $f_n(p^e)$. Data suggests that the lower bound for $f_n(p^e)$ that comes from counting irreducible subring matrices is slightly worse than the lower bound that comes from counting subgroups. Both of these lower bounds are at most $p^{(3-2\sqrt{2})e(n-1)}$. In order to improve upon the lower bounds given in this paper using these techniques, it seems necessary to answer Questions 7.1(2) and 7.1(3) or to find other related sets of subgroups that are also subrings. Improvements of the lower bounds for $f_n(p^e)$ would likely lead to better lower bounds for the asymptotic growth of subrings in $\mathbb{Z}^n$ or orders in a fixed number field.

## Acknowledgments

The author thanks Nathan Kaplan for suggesting the problem and for many helpful conversations. The author also thanks the anonymous referee for their helpful comments. This work was supported by the NSF grant DMS 1802281.

## References

[1] S. Atanasov, N. Kaplan, B. Krakoff, J.H. Menzel, Counting finite index subrings of $\mathbb{Z}^n$, Acta Arith. 197 (2021) 221–246.
[2] J. Brakenhoff, Counting problems for number rings, Ph.D. thesis, Leiden University, 2009.
[3] P.J. Cameron, Notes on Counting: An Introduction to Enumerative Combinatorics, Australian Mathematical Society Lecture Series, Cambridge University Press, 2017.
[4] A. Chambert-Loir, Y. Tschinkel, Fonctions zêta des hauteurs des espaces fibrés, in: E. Peyre, Y. Tschinkel (Eds.), Rational Points on Algebraic Varieties, Springer Basel, 2001, pp. 71–115.
[5] B. Datskovsky, D.J. Wright, Density of discriminants of cubic extensions, J. Reine Angew. Math. 386 (1988) 116–138, http://eudml.org/doc/153019.
[6] M. du Sautoy, L. Woodward, Zeta Functions of Groups and Rings, Lecture Notes in Mathematics, vol. 1925, Springer-Verlag, 2008.
[7] F.J. Grunewald, D. Segal, G.C. Smith, Subgroups of finite index in nilpotent groups, Invent. Math. 93 (1988) 185–223.
[8] N. Kaplan, J. Marcinek, R. Takloo-Bighash, Distribution of orders in number fields, Res. Math. Sci. 2 (2015), https://doi.org/10.1186/s40687-015-0027-8.
[9] R. Liu, Counting subrings of $\mathbb{Z}^n$ of index $k$, J. Comb. Theory, Ser. A 114 (2007) 278–299, https://doi.org/10.1016/j.jcta.2006.05.002.
[10] J. Nakagawa, Orders of a quartic field, Mem. Am. Math. Soc. 583 (1996).
[11] T. Stehling, On computing the number of subgroups of a finite Abelian group, Combinatorica 12 (1992) 475–479, https://doi.org/10.1007/BF013052392.