

Counting finite index subrings of \mathbb{Z}^n

by

STANISLAV ATANASOV (New York, NY), NATHAN KAPLAN (Irvine, CA),
BENJAMIN KRAKOFF (Ann Arbor, MI) and
JULIA H. MENZEL (Cambridge, MA)

1. Introduction. The main goal of this paper is to study the number of subrings of \mathbb{Z}^n of given index. We begin by reviewing an easier problem, counting subgroups of \mathbb{Z}^n of given index.

1.1. Counting subgroups of \mathbb{Z}^n . The *zeta function* of an infinite group G is defined by

$$\zeta_G(s) = \sum_{\substack{H \leq G \\ [G:H] < \infty}} [G:H]^{-s} = \sum_{k=1}^{\infty} a_k(G) k^{-s},$$

where s is a complex variable and $a_k(G)$ is the number of subgroups of G of index k . We can think of $\zeta_G(s)$ as a generating function that gives the number of subgroups H of G of each finite index.

We focus on the case $G = (\mathbb{Z}^n, +)$. A finite index subgroup of \mathbb{Z}^n is a sublattice, and every sublattice of \mathbb{Z}^n is the column span of a unique matrix A in Hermite normal form. The index of the lattice spanned by A is $\det(A)$. Let $M_n(\mathbb{Z})$ denote the set of all $n \times n$ matrices with entries in \mathbb{Z} . We have

$$a_k(\mathbb{Z}^n) = \#\{A \in M_n(\mathbb{Z}) : A \text{ is in Hermite normal form and } \det(A) = k\}.$$

Throughout this paper, p always represents a prime number, and \prod_p denotes a product over all primes. The zeta function of a finitely generated nilpotent group G has an Euler product [16, Proposition 1.3], so we can write

$$\zeta_{\mathbb{Z}^n}(s) = \prod_p \zeta_{\mathbb{Z}^n, p}(s), \quad \text{where} \quad \zeta_{\mathbb{Z}^n, p}(s) = \sum_{k=0}^{\infty} a_{p^k}(\mathbb{Z}^n) p^{-ks}.$$

2020 *Mathematics Subject Classification*: Primary 20E07; Secondary 11H06, 11M41.

Key words and phrases: subrings, lattices, multiplicative lattices, zeta functions of groups and rings.

Received 1 February 2018; revised 4 May 2020.

Published online 9 November 2020.

A matrix $A \in M_n(\mathbb{Z})$ in Hermite normal form with $\det(A) = p^k$ has diagonal $(p^{i_1}, \dots, p^{i_n})$ where $i_j \geq 0$ for each j and $\sum_{j=1}^n i_j = k$. It is not difficult to compute the number of $n \times n$ matrices in Hermite normal form with given diagonal. This computation implies that

$$(1.1) \quad \zeta_{\mathbb{Z}^n, p}(s) = (1 - p^{-s})^{-1} (1 - p^{-(s-1)})^{-1} \cdots (1 - p^{-(s-(n-1))})^{-1},$$

and therefore

$$(1.2) \quad \zeta_{\mathbb{Z}^n}(s) = \zeta(s) \zeta(s-1) \cdots \zeta(s-(n-1)).$$

See the book of Lubotzky and Segal [20] for five proofs of this fact. We review one of these arguments in Section 2.1, as it forms the basis for the approach to counting subrings that we explain in Section 2.2.

The function in (1.2) has meromorphic continuation to the entire complex plane. Its rightmost pole is located at $s = n$ and is simple. A standard Tauberian theorem gives an asymptotic formula for the number of sublattices of \mathbb{Z}^n of bounded index. We have

$$(1.3) \quad \begin{aligned} N_n(X) &:= \#\{\text{sublattices of } \mathbb{Z}^n \text{ of index } < X\} = \sum_{k < X} a_k(\mathbb{Z}^n) \\ &= \frac{\zeta(n)\zeta(n-1)\cdots\zeta(2)}{n} X^n + O(X^{n-1} \log(X)) \end{aligned}$$

as $X \rightarrow \infty$.

In Section 2.1 we see that for fixed n and e , $a_{p^e}(\mathbb{Z}^n)$ is a polynomial in p that is not difficult to compute. In fact, $a_{p^e}(\mathbb{Z}^n)$ is equal to the p -binomial coefficient $\binom{n-1+e}{e}_p$ [30, Section 1.8]. Therefore, the problems of counting sublattices of \mathbb{Z}^n of given index, and of asymptotically counting sublattices of bounded index, are well-understood.

1.2. Counting subrings of \mathbb{Z}^n . We study the function analogous to $a_k(\mathbb{Z}^n)$ that counts subrings of \mathbb{Z}^n . We use the term *subring* to mean a multiplicatively closed sublattice containing the multiplicative identity $(1, \dots, 1)$. Let $f_n(k)$ denote the number of subrings of \mathbb{Z}^n of index k . Define the *subring zeta function* of \mathbb{Z}^n by

$$\zeta_{\mathbb{Z}^n}^R(s) = \sum_{k=1}^{\infty} f_n(k) k^{-s}.$$

As we saw with $\zeta_{\mathbb{Z}^n}(s)$, this zeta function has an Euler product

$$\zeta_{\mathbb{Z}^n}^R(s) = \prod_p \zeta_{\mathbb{Z}^n, p}^R(s), \quad \text{where} \quad \zeta_{\mathbb{Z}^n, p}^R(s) = \sum_{k=0}^{\infty} f_n(p^k) p^{-ks}.$$

Equivalently, $\zeta_{\mathbb{Z}^n, p}^R(s) = \zeta_{\mathbb{Z}_p^n}^R(s)$ where \mathbb{Z}_p denotes the ring of p -adic integers and $\zeta_{\mathbb{Z}_p^n}^R(s)$ is the zeta function that counts finite index \mathbb{Z}_p -subalgebras of \mathbb{Z}_p^n .

QUESTION 1.1. For fixed n and e , how does $f_n(p^e)$ behave as a function of p ?

Liu uses a strategy similar to the one outlined in Section 1.1 to compute $f_n(p^e)$ for $e \leq 5$ and any n . (There is a small error in the computation of $f_n(p^5)$ that we correct here. More specifically, the constant terms in the coefficients of $\binom{n}{6}$ and $\binom{n}{7}$ are corrected to 141 and 371, respectively.)

PROPOSITION 1.2 ([19, Proposition 1.1]). *We have*

$$\begin{aligned}
 f_n(1) &= 1, \\
 f_n(p) &= \binom{n}{2}, \\
 f_n(p^2) &= \binom{n}{2} + \binom{n}{3} + 3\binom{n}{4}, \\
 f_n(p^3) &= \binom{n}{2} + (p+1)\binom{n}{3} + 7\binom{n}{4} + 10\binom{n}{5} + 15\binom{n}{6}, \\
 f_n(p^4) &= \binom{n}{2} + (3p+1)\binom{n}{3} + (p^2+p+10)\binom{n}{4} + (10p+21)\binom{n}{5} \\
 &\quad + 70\binom{n}{6} + 105\binom{n}{7} + 105\binom{n}{8}, \\
 f_n(p^5) &= \binom{n}{2} + (4p+1)\binom{n}{3} + (7p^2+p+13)\binom{n}{4} \\
 &\quad + (p^3+p^2+41p+31)\binom{n}{5} + (15p^2+35p+141)\binom{n}{6} \\
 &\quad + (105p+371)\binom{n}{7} + 910\binom{n}{8} + 1260\binom{n}{9} + 945\binom{n}{10}.
 \end{aligned}$$

The main theorem of this paper extends Proposition 1.2 to all $e \leq 8$. For consistency with Liu's results, we state our formulas as linear combinations of binomial coefficients $\binom{n}{i}$ with coefficients that are polynomials in p . This also allows one to quickly identify the main term of each function when n is fixed and p varies.

THEOREM 1.3. *We have*

$$\begin{aligned}
 f_n(p^6) &= \binom{n}{2} + (p^2+4p+1)\binom{n}{3} + (p^3+14p^2+p+16)\binom{n}{4} \\
 &\quad + (p^4+11p^3+2p^2+81p+41)\binom{n}{5} + (p^4+p^3+131p^2+111p+226)\binom{n}{6} \\
 &\quad + (21p^3+56p^2+616p+743)\binom{n}{7} + (210p^2+770p+2639)\binom{n}{8} \\
 &\quad + (1260p+6958)\binom{n}{9} + 14175\binom{n}{10} + 17325\binom{n}{11} + 10395\binom{n}{12},
 \end{aligned}$$

$$\begin{aligned}
f_n(p^7) = & \binom{n}{2} + (3p^2 + 4p + 1)\binom{n}{3} + (10p^3 + 12p^2 + p + 19)\binom{n}{4} \\
& + (15p^4 + 21p^3 + 16p^2 + 121p + 51)\binom{n}{5} \\
& + (p^6 + p^5 + 17p^4 + 17p^3 + 392p^2 + 206p + 326)\binom{n}{6} \\
& + (p^5 + 22p^4 + 288p^3 + 379p^2 + 1618p + 1219)\binom{n}{7} \\
& + (28p^4 + 84p^3 + 2324p^2 + 3640p + 5279)\binom{n}{8} \\
& + (378p^3 + 1638p^2 + 11298p + 18600)\binom{n}{9} + (3150p^2 + 15750p + 58800)\binom{n}{10} \\
& + (17325p + 143605)\binom{n}{11} + 252945\binom{n}{12} + 270270\binom{n}{13} + 135135\binom{n}{14}, \\
f_n(p^8) = & \binom{n}{2} + (4p^2 + 4p + 1)\binom{n}{3} + (p^4 + 26p^3 + 9p^2 + p + 22)\binom{n}{4} \\
& + (p^5 + 77p^4 - 13p^3 + 52p^2 + 161p + 61)\binom{n}{5} \\
& + (16p^6 + 31p^5 + 22p^4 + 187p^3 + 702p^2 + 301p + 441)\binom{n}{6} \\
& + (p^8 + p^7 + 2p^6 + 23p^5 + 339p^4 + 1080p^3 + 1206p^2 + 3074p + 1800)\binom{n}{7} \\
& + (29p^6 + 29p^5 + 652p^4 + 1093p^3 + 9374p^2 + 9073p + 8933)\binom{n}{8} \\
& + (36p^5 + 498p^4 + 6420p^3 + 15324p^2 + 39810p + 37201)\binom{n}{9} \\
& + (630p^4 + 3150p^3 + 46200p^2 + 103320p + 148551)\binom{n}{10} \\
& + (6930p^3 + 41580p^2 + 243705p + 510730)\binom{n}{11} \\
& + (51975p^2 + 329175p + 1474165)\binom{n}{12} \\
& + (270270p + 3258255)\binom{n}{13} + 5045040\binom{n}{14} + 4729725\binom{n}{15} + 2027025\binom{n}{16}.
\end{aligned}$$

1.3. Motivation: Counting subrings and orders of bounded index. Bhargava has asked about the asymptotic growth rate of $f_n(k)$ [19]. We would like to have an asymptotic formula for the number of subrings of \mathbb{Z}^n analogous to (1.3). Expressions for $\zeta_{\mathbb{Z}^n}^R(s)$ analogous to (1.2) would lead to such results. However, such formulas are only known for $n \leq 4$.

THEOREM 1.4. *We have*

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

The computation for $n = 2$ is elementary. The $n = 3$ result is originally due to Datskovsky and Wright [8], and for $n = 4$ to Nakagawa [25]. Liu gives combinatorial proofs of these results [19]; his $A_n(p, p^{-s})$ is $\zeta_{\mathbb{Z}^n, p}^R(s)$.

Kaplan, Marcinek, and Takloo-Bighash study the problem of counting subrings of bounded index in \mathbb{Z}^n and prove the following.

THEOREM 1.5 ([18, Theorem 6]). *Let*

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

(1) *Let $n \leq 5$. There is a positive real number C_n such that*

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

as $X \rightarrow \infty$.

(2) *Suppose $n \geq 6$. Then for any $\epsilon > 0$ we have*

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

The authors of [18] derive the asymptotic order of growth for $N_5^R(X)$ up to a constant factor, despite not having a formula for $\zeta_{\mathbb{Z}^5}^R(s)$ analogous to those of Theorem 1.4. The main idea is to find the location and order of the rightmost pole of $\zeta_{\mathbb{Z}^n}^R(s)$ by computing $f_n(p^e)$ exactly for small e and giving estimates for larger e . A major motivation for the computations of the present paper is to try to prove stronger versions of Theorem 1.5. For $n \geq 6$ we do not even know of a conjecture for the asymptotic growth rate of $N_n^R(X)$.

One of the main problems in the field of arithmetic statistics is to count finite extensions of a number field and the orders that they contain. For example, it is an old conjecture that the number of isomorphism classes of degree n extensions K of \mathbb{Q} with $|\text{disc}(K)| < X$ is asymptotic to a constant depending on n times X . One can also ask about the number of isomorphism classes of orders contained in these fields with discriminant at most X in absolute value. Bhargava has proven breakthrough results counting quartic and quintic fields by first counting all isomorphism classes of orders in these fields and then sieving for the maximal ones [2, 3].

Bhargava, Malle, and others have made conjectures on counting finite extensions with bounded discriminant and specified Galois group [1, 23, 24]. Problems about counting orders contained in field extensions of given degree with bounded discriminant have received less attention. Recall that if K is a number field with ring of integers \mathcal{O}_K , then an order $\mathcal{O} \subseteq \mathcal{O}_K$ is a subring of \mathcal{O}_K with identity that is a \mathbb{Z} -module of rank n . If $\mathcal{O} \subseteq \mathcal{O}_K$ is an order, then $\text{disc}(\mathcal{O}) = [\mathcal{O}_K : \mathcal{O}]^2 \cdot \text{disc}(\mathcal{O}_K)$.

QUESTION 1.6. Let $B_n(X)$ denote the number of isomorphism classes of orders \mathcal{O} in all degree n number fields such that $|\text{disc}(\mathcal{O})| < X$. How does $B_n(X)$ grow as a function of X ?

It follows from work of Davenport and Heilbronn [9] for $n = 3$, and Bhargava [2, 3] for $n = 4, 5$, that $B_n(X)$ is asymptotic to a constant c_n times X . For $n \geq 6$ we do not know of a conjecture for the asymptotic growth rate of this function.

One approach to this problem is to count orders contained in a fixed field K of bounded index, and take a sum over all K of fixed degree.

QUESTION 1.7. Let K be a number field and let $N_K(X)$ denote the number of orders \mathcal{O} contained in K with $|\text{disc}(\mathcal{O})| < X$. How does $N_K(X)$ grow as a function of X ?

Kaplan, Marcinek, and Takloo-Bighash study Question 1.7 by investigating analytic properties of the subring zeta function of \mathcal{O}_K . Let

$$\zeta_{\mathcal{O}_K}^R(s) = \sum_{\mathcal{O} \subseteq \mathcal{O}_K} [\mathcal{O}_K : \mathcal{O}]^{-s}$$

where the sum is taken over all orders in \mathcal{O}_K .

In the statement of the theorem below, $n = [K : \mathbb{Q}]$ and r_2 is an explicitly computable positive integer that depends on the Galois group of the normal closure of K/\mathbb{Q} ; see [18] for details.

THEOREM 1.8 ([18, Theorem 2]).

(1) *For $n \leq 5$, there is a constant $C_K > 0$ such that*

$$N_K(X) \sim C_K X^{1/2} (\log X)^{r_2-1} \quad \text{as } X \rightarrow \infty.$$

(2) *For any $n \geq 6$ and any $\epsilon > 0$,*

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

When $[K : \mathbb{Q}] \geq 6$, we do not know of a conjecture for the asymptotic growth rate of $N_K(X)$.

The subring zeta function of \mathcal{O}_K has an Euler product indexed by rational primes p , and its local factors satisfy $\zeta_{\mathcal{O}_K, p}^R(s) = \zeta_{\mathcal{O}_K \otimes \mathbb{Z}_p}^R(s)$, where this zeta function counts finite index \mathbb{Z}_p -subalgebras. When p splits completely in \mathcal{O}_K , $\mathcal{O}_K \otimes \mathbb{Z}_p \cong \mathbb{Z}_p^n$, so

$$\zeta_{\mathcal{O}_K, p}^R(s) = \zeta_{\mathbb{Z}_p^n}^R(s) = \zeta_{\mathbb{Z}^n, p}^R(s).$$

The $n = 3$ case of Theorem 1.8 follows from work of Datskovsky and Wright [8], who compute $\zeta_{\mathcal{O}_K}^R(s)$ for any cubic field K . The $n = 4$ case follows from Nakagawa's [25] computation for any quartic field K of $\zeta_{\mathcal{O}_K, p}^R(s)$ at all unramified primes p .

The authors of [18] suggest that among all unramified primes, those that split completely may control the asymptotic growth rate of $N_K(X)$. This suggests that the growth rate of the simpler function $N_n^R(X)$ along with the Galois group of the normal closure of K may determine the growth rate of $N_K(X)$. For more information, see the discussion following [18, Theorem 4].

We hope that more precise results on the growth of $f_n(p^e)$ will lead not only to improved asymptotic estimates for counting subrings of \mathbb{Z}^n of bounded index, like those of Theorem 1.5, but may also help to understand asymptotic formulas for counting orders of bounded index in a fixed number field, like those of Theorem 1.8.

In Section 4 we give lower bounds for $f_n(p^e)$ that are analogous to lower bounds for $N_K(X)$ due to Brakenhoff [5], suggesting a closer connection between these counting problems.

1.4. Motivation: Uniformity of subring zeta functions. Zeta functions of infinite groups, rings, and algebras have been studied extensively from both a combinatorial and an analytic point of view [14, 26, 27, 32]. A common question is how local factors of zeta functions vary with p .

DEFINITION 1.9. A zeta function $\zeta_G(s) = \prod_p \zeta_{G,p}(s)$ is *finitely uniform* if there are finitely many rational functions $W_i(X, Y) \in \mathbb{Q}(X, Y)$, $i \in I$, a finite index set, such that for every prime p there exists an $i = i(p)$ such that $\zeta_{G,p}(s) = W_i(p, p^{-s})$. We say that $\zeta_G(s)$ is *uniform* if it is finitely uniform for $|I| = 1$.

Definition 1.9 can be extended in the obvious way to subring zeta functions.

EXAMPLE 1.10. (1) In (1.1) we saw that $\zeta_{\mathbb{Z}^n,p}(s)$ is given by a single rational function in p and p^{-s} . That is, $\zeta_{\mathbb{Z}^n}(s)$ is uniform.

(2) When K is a number field of degree at most 4 with ring of integers \mathcal{O}_K , then $\zeta_{\mathcal{O}_K}^R(s)$ is finitely uniform. For $[K : \mathbb{Q}] = 3, 4$, $\zeta_{\mathcal{O}_K,p}^R(s)$ depends on the decomposition of the ideal generated by p in \mathcal{O}_K [8, 25].

In order to understand how $f_n(p^e)$ varies with p , we want to know how the local factors $\zeta_{\mathbb{Z}^n,p}^R(s)$ vary. Grunewald, Segal, and Smith build on work of Denef [10, 11], and Igusa [17], to prove the following result.

THEOREM 1.11 ([16, Theorem 3.5]). *For each positive integer n and each prime p there exist polynomials $\Phi_{n,p}(X), \Psi_{n,p}(X) \in \mathbb{Z}[x]$ such that*

$$\zeta_{\mathbb{Z}^n,p}^R(s) = \frac{\Phi_{n,p}(p^{-s})}{\Psi_{n,p}(p^{-s})}.$$

Moreover, the degrees of $\Phi_{n,p}$ and $\Psi_{n,p}$ are bounded independently of p .

When n is fixed, we want to understand how these rational functions vary with p .

QUESTION 1.12 ([31, Question 3.7]). Is the zeta function $\zeta_{\mathbb{Z}^n}^R(s)$ uniform? Is it finitely uniform?

Expanding the rational functions of Theorem 1.11 as power series and computing individual coefficients shows that $\zeta_{\mathbb{Z}^n}^R(s)$ is uniform if and only if

for each fixed $e \geq 1$, $f_n(p^e)$ is a polynomial in p . Therefore, the first part of Question 1.12 is equivalent to the following question.

QUESTION 1.13. For fixed $n \geq 2$ and $e \geq 1$, is $f_n(p^e)$ a polynomial in p ?

Proposition 1.2 shows that for fixed n and $e \leq 5$, $f_n(p^e)$ is a polynomial in p . Theorem 1.3 extends this to $e \leq 8$ and provides some evidence for a positive answer to Questions 1.12 and 1.13. We will see how the proof of Theorem 1.3 involves counting \mathbb{F}_p -points on certain varieties. We will see that the variety V in 5-dimensional affine space over \mathbb{F}_p defined by

$$(x^2 - x) - (u^2 - u)c' = (y^2 - y) - (v^2 - v)c' = xy - uvc' = 0$$

plays an important role in the proof of Lemma 3.10. A computation in Magma shows that V is 2-dimensional, with seven irreducible components, and suggests that $\#V(\mathbb{F}_p) = 7p^2 - 6p + 6$. We verify this formula in the proof of Lemma 3.10. It is not difficult to imagine how for larger values of e , more complicated varieties may play a role in the formula for $f_n(p^e)$.

1.5. Outline of the paper. In Section 2 we follow the method of Liu and give a bijection between subrings of \mathbb{Z}^n and matrices of a specific form. This transforms the question of counting subrings of prime power index into a problem of counting matrices with entries satisfying certain divisibility conditions. We then review Liu's notion of irreducible subrings. Let $g_n(k)$ be the number of irreducible subrings of \mathbb{Z}^n of index k . We recall in Proposition 2.8 a recurrence due to Liu relating $g_n(k)$ and $f_n(k)$. Our $g_n(k)$ is denoted by $g_{n-1}(k)$ in [19].

In Section 3 we express $g_n(p^e)$ as a sum over irreducible subrings with fixed diagonal entries. Possible diagonals are in bijection with compositions of e into $n-1$ parts. We verify that for $n \leq 9$ and $e \leq 8$ each of the functions counting irreducible subring matrices with a fixed diagonal is given by a polynomial in p . We use these results along with the recurrence of [19] to compute $f_n(p^e)$ for $e \leq 8$, proving Theorem 1.3. In Section 4 we give lower bounds for $g_n(p^e)$ analogous to results of Brakenhoff for orders in a fixed number field [5]. We end with questions for further study.

Computations related to this project were carried out in Sage, Magma, and Mathematica [4, 29]. Some programs are available at the second author's website: https://www.math.uci.edu/~nckaplan/research_files/subrings.

2. Subring matrices and irreducible subring matrices. In our analysis of $f_n(k)$ we employ techniques developed in [19], where Liu gives a bijection between subrings \mathbb{Z}^n and a class of integer matrices. This reduces the problem of counting subrings of index k in \mathbb{Z}^n to the problem of counting *subring matrices*, which can be understood as compositions of yet simpler *irreducible subring matrices*.

2.1. Counting matrices in Hermite normal form. We begin by giving a proof of (1.1) due to Bushnell and Reiner [20, Section 15.2].

DEFINITION 2.1. A matrix $A \in M_n(\mathbb{Z})$ with entries a_{ij} is in *Hermite normal form* if:

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

There is a bijection between sublattices of \mathbb{Z}^n of index p^k and matrices $A \in M_n(\mathbb{Z})$ in Hermite normal form with $\det(A) = p^k$. The diagonal entries of such a matrix are of the form $(p^{i_1}, \dots, p^{i_n})$, where $i_j \geq 0$ for each j and $\sum_{j=1}^n i_j = k$.

DEFINITION 2.2. A *weak composition* of an integer k is a list of non-negative integers $(\alpha_1, \dots, \alpha_n)$ where $\sum_{i=1}^n \alpha_i = k$. Each α_i is a *part* of the weak composition, and n is the *length* or *number of parts*. A weak composition in which every part is positive is called a *composition* of k .

The possible diagonals of an $n \times n$ matrix in Hermite normal form with determinant p^k are in bijection with weak compositions of k of length n .

The number of $n \times n$ matrices in Hermite normal form with diagonal $(p^{i_1}, \dots, p^{i_n})$ is $p^{(n-1)i_1} p^{(n-2)i_2} \dots p^{i_{n-1}}$. Taking the sum of these terms over all weak compositions of k into n parts gives a polynomial formula for $a_{p^k}(\mathbb{Z}^n)$. We have

$$\begin{aligned} \zeta_{\mathbb{Z}^n, p}(s) &= \sum_{k=0}^{\infty} a_{p^k}(\mathbb{Z}^n) p^{-ks} = \sum_{i_1=0}^{\infty} \dots \sum_{i_n=0}^{\infty} p^{-(i_1+\dots+i_n)s} p^{(n-1)i_1} p^{(n-2)i_2} \dots p^{i_{n-1}} \\ &= \left(\sum_{i_1=0}^{\infty} p^{-(s-(n-1))i_1} \right) \dots \left(\sum_{i_{n-1}=0}^{\infty} p^{-(s-1)i_{n-1}} \right) \left(\sum_{i_n=0}^{\infty} p^{-si_n} \right) \\ &= (1 - p^{-s})^{-1} (1 - p^{-(s-1)})^{-1} \dots (1 - p^{-(s-(n-1))})^{-1}, \end{aligned}$$

completing the proof of (1.1).

2.2. Counting subrings via Liu's bijection. Liu adapts the argument of Section 2.1 to count subrings of \mathbb{Z}^n . For column vectors $u = (u_1, \dots, u_n)$ and $w = (w_1, \dots, w_n)$ we write $u \circ w$ for the column vector given by the componentwise product $(u_1 w_1, \dots, u_n w_n)$.

PROPOSITION 2.3 ([19, Propositions 2.1 and 2.2]). *Let k be a positive integer. There is a bijection between subrings with identity $L \subset \mathbb{Z}^n$ of index k and matrices $A \in M_n(\mathbb{Z})$ in Hermite normal form with $\det(A) = k$ such that:*

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

DEFINITION 2.4. (1) A lattice $L \subset \mathbb{Z}^n$ for which $u, w \in L$ implies $u \circ w \in L$ is *multiplicatively closed*.

(2) A matrix that satisfies the conditions of Proposition 2.3 is a *subring matrix*.

A subring matrix A is required to be in Hermite normal form, therefore $(1, \dots, 1)^T$ is in the column span of A if and only if the final column of A is $(1, \dots, 1)^T$.

For fixed n , we may calculate $f_n(k)$ by counting the corresponding subring matrices. Since $f_n(k)$ is weakly multiplicative, it suffices to consider $k = p^e$ for p prime. This restricts our attention to subring matrices with diagonal entries $(p^{\alpha_1}, \dots, p^{\alpha_n})$ such that $(\alpha_1, \dots, \alpha_n)$ is a weak composition of e of length n .

Liu notes that there is a natural correspondence between subrings of \mathbb{Z}_p^n and subrings of \mathbb{Z}^n with index a power of p [19, p. 283]. Liu defines *irreducible subrings* of \mathbb{Z}_p^n , but for notational convenience we prefer to give the corresponding notion for subrings of \mathbb{Z}^n with index equal to a power of p .

DEFINITION 2.5. A subring $L \subset \mathbb{Z}^n$ with index equal to a power of p is *irreducible* if for each $(x_1, \dots, x_n) \in L$, $x_1 \equiv \dots \equiv x_n \pmod{p}$.

THEOREM 2.6 ([19, Theorem 3.4]). *A subring $L \subset \mathbb{Z}^n$ of index equal to a power of p can be written uniquely as a direct sum of irreducible subrings $L_i \subset \mathbb{Z}^n$.*

It is easy to see if a subring is irreducible by considering the corresponding subring matrix.

PROPOSITION 2.7 ([19, Proposition 3.1]). *An $n \times n$ subring matrix represents an irreducible subring if and only if its first $n-1$ columns contain only entries divisible by p , and its final column equals the identity $(1, \dots, 1)^T$.*

Recall that $g_n(k)$ is the number of irreducible subrings of \mathbb{Z}^n of index k . In Section 3, we give formulas for $g_n(p^e)$ for each $e \leq 8$. We recall the following recurrence due to Liu. We again emphasize that $g_n(p^e)$ is given by $g_{n-1}(p^e)$ in [19]. Define $f_0(1) = 1$ and $f_0(p^e) = 0$ for $e > 0$.

PROPOSITION 2.8 ([19, Proposition 4.4]). *The following recurrence holds for $n > 0$:*

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

In order to show for fixed n and e that $f_n(p^e)$ is a polynomial in p , it is enough to show that $f_j(p^k)$ is a polynomial in p for each fixed $j \leq n-1$ and $k \leq e$, and that $g_j(p^i)$ is a polynomial in p for each fixed $j \leq n$ and $i \leq e$.

3. Computing $f_n(p^6)$, $f_n(p^7)$, and $f_n(p^8)$. In this section we compute $f_n(p^6)$, $f_n(p^7)$, and $f_n(p^8)$, proving Theorem 1.3. We do this by computing $g_n(p^e)$ for any n and fixed $e \leq 8$ and then applying Proposition 2.8.

3.1. Statement of results. In this subsection, we state the main results that lead to the proof of Theorem 1.3. Recall that for fixed e , $g_n(p^e) = 0$ for all but finitely many n . Note that $g_1(1) = 1$ and $g_1(p^e) = 0$ for $e \geq 1$.

PROPOSITION 3.1 ([19, Proposition 4.3]). *For all $n \geq 2$, we have $g_n(p^e) = 0$ for $e < n - 1$, $g_n(p^{n-1}) = 1$, and $g_n(p^n) = (p^{n-1} - 1)/(p - 1)$.*

Proposition 1.2 gives Liu's polynomial formulas for $f_n(p^e)$ for $e \leq 5$ [19, Proposition 1.1]. We note that there is a slight error in Liu's computation for $e = 5$, so we have stated the corrected result.

It is easy to see that $g_2(p^e) = 1$ for all $e \geq 1$. Although they are not written explicitly, Liu gives polynomial formulas for $g_n(p^e)$ for $n = 3, 4$ [19, Propositions 6.2 and 6.3]. We record the values of $g_3(p^e)$ for $e \in \{4, 5, 6, 7, 8\}$ and of $g_4(p^e)$ for $e \in \{5, 6, 7, 8\}$ since these values are used in the proof of Theorem 1.3:

Table 1. Values of $g_n(p^e)$ for $n = 3, 4$ and $e \leq 8$

$g_3(p^4)$	$3p + 1$
$g_3(p^5)$	$4p + 1$
$g_3(p^6)$	$p^2 + 4p + 1$
$g_3(p^7)$	$3p^2 + 4p + 1$
$g_3(p^8)$	$4p^2 + 4p + 1$
$g_4(p^5)$	$7p^2 + p + 1$
$g_4(p^6)$	$p^3 + 14p^2 + p + 1$
$g_4(p^7)$	$10p^3 + 12p^2 + p + 1$
$g_4(p^8)$	$p^4 + 26p^3 + 9p^2 + p + 1$

Combining Propositions 1.2 and 2.8 with an induction argument gives polynomial formulas for $f_n(p^e)$ for all $e \leq 5$ and all n . Theorem 1.3 follows from Proposition 1.2, the data in Table 1, and the following result.

THEOREM 3.2. *We have the following values of $g_n(p^e)$:*

Table 2. Values of $g_n(p^e)$ for $n = 5, 6, 7$ and $e \leq 8$

$g_5(p^6)$	$p^4 + 11p^3 + 2p^2 + p + 1$
$g_5(p^7)$	$15p^4 + 21p^3 + 6p^2 + p + 1$
$g_5(p^8)$	$p^5 + 77p^4 - 13p^3 + 12p^2 + p + 1$
$g_6(p^7)$	$p^6 + p^5 + 17p^4 + 2p^3 + 2p^2 + p + 1$
$g_6(p^8)$	$16p^6 + 31p^5 + 22p^4 + 22p^3 + 2p^2 + p + 1$
$g_7(p^8)$	$p^8 + p^7 + 2p^6 + 23p^5 + 3p^4 + 2p^3 + 2p^2 + p + 1$

3.2. Strategy of the proof of Theorem 3.2. In the rest of this section we explain the strategy of the proof of Theorem 3.2. Recall that the last column of any irreducible subring matrix is $(1, \dots, 1)^T$ and that every other entry is divisible by p . The possible diagonals of an $n \times n$ irreducible subring matrix of determinant p^e are in bijection with compositions of e of length $n - 1$.

DEFINITION 3.3. Let $\mathcal{C}_{n,e}$ denote the set of compositions of e into $n - 1$ parts. For a composition α of length $n - 1$ let $g_\alpha(p)$ denote the number of $n \times n$ irreducible subring matrices with diagonal entries $(p^{\alpha_1}, p^{\alpha_2}, \dots, p^{\alpha_{n-1}}, 1)$.

It is a standard fact that $|\mathcal{C}_{n,e}| = \binom{e-1}{n-2}$.

Combining these definitions shows that for any positive integers n and e ,

$$(3.1) \quad g_n(p^e) = \sum_{\alpha \in \mathcal{C}_{n,e}} g_\alpha(p).$$

The following result shows that when computing $g_n(p^e)$ for the values of n, e of Theorem 3.2 we do not have to compute $g_\alpha(p)$ for every $\alpha \in \mathcal{C}_{n,e}$.

LEMMA 3.4. *Let $\alpha = (1, \alpha_2, \dots, \alpha_k)$ be a composition of a positive integer e and $\alpha' = (\alpha_2, \dots, \alpha_k)$. We have $g_\alpha(p) = g_{\alpha'}(p)$.*

Proof. An irreducible subring matrix with a p as its first diagonal entry has first row equal to $(p, 0, \dots, 0, 1)$ since every entry $a_{1,j}$ with $j \notin \{1, n\}$ satisfies $0 \leq a_{1,j} < p$ and $a_{1,j} \equiv 0 \pmod{p}$. The conditions derived from taking products of pairs of columns are identical in both cases. ■

Let $\mathcal{C}'_{n,e}$ denote the set of compositions of e into $n - 1$ parts where the first part is larger than 1. Lemma 3.4 implies that

$$(3.2) \quad g_n(p^e) = g_{n-1}(p^{e-1}) + \sum_{\alpha \in \mathcal{C}'_{n,e}} g_\alpha(p).$$

Using this idea, the formula for $g_5(p^6)$ follows from computing $g_\alpha(p)$ for $\alpha \in \{(3, 1, 1, 1), (2, 2, 1, 1), (2, 1, 2, 1), (2, 1, 1, 2)\}$.

There are some particular classes of compositions for which we can explicitly compute $g_\alpha(p)$. We defer the proofs of the following two lemmas to Section 3.3.

LEMMA 3.5. *Let $n \geq 2$ and $\alpha = (\beta, 1, \dots, 1)$ be a composition of length $n - 1$.*

- (1) *If $\beta = 2$, then $g_\alpha(p) = p^{n-2}$.*
- (2) *If $\beta \geq 3$, then $g_\alpha(p) = (n - 1)p^{n-2}$.*

The first part of this lemma together with Lemma 3.4 shows that

$$g_n(p^n) = g_{(2,1,\dots,1)}(p) + g_{(1,2,1,\dots,1)}(p) + \dots + g_{(1,\dots,1,2)}(p) = p^{n-2} + p^{n-3} + \dots + 1,$$

which proves the formula given in Proposition 3.1.

LEMMA 3.6. *Let $n \geq 3$ and $\alpha = (2, 1, \dots, 1, \beta, 1, \dots, 1)$ be a composition of length $n - 1$ where the β is in the k th position. Set $r = n - 1 - k$, i.e., the number of parts equal to 1 following β .*

(1) *If $\beta = 2$, then*

$$g_\alpha(p) = p^{n-3+r} + (r+1)p^{n-3}(p-1).$$

(2) *If $\beta \geq 3$, then*

$$g_\alpha(p) = (r+1)(p^{n-3+r} + p^{n-3}(p-1)).$$

Applying Lemmas 3.5 and 3.6 gives the following corollary.

COROLLARY 3.7. *For any $n \geq 1$ we have*

$$g_n(p^{n+1}) = \frac{2p^{2n-3} + (n^2 - n)p^{n+1} - (n^2 - n)p^n - (n^2 - n + 2)p^{n-1} + (n^2 - n - 2)p^{n-2} + 2}{2(p-1)^2(p+1)}.$$

Proof. By (3.2) we have

$$\begin{aligned} g_n(p^{n+1}) &= g_{n-1}(p^n) + g_{(3,1,\dots,1)}(p) + g_{(2,2,1,\dots,1)}(p) + g_{(2,1,2,\dots,1)}(p) + g_{(2,1,\dots,1,2)}(p). \end{aligned}$$

Lemma 3.5 implies that $g_{(3,1,\dots,1)}(p) = (n-1)p^{n-2}$. The first part of Lemma 3.6 implies that

$$\begin{aligned} g_{(2,2,1,\dots,1)}(p) + g_{(2,1,2,\dots,1)}(p) + \dots + g_{(2,1,\dots,1,2)}(p) &= p^{n-3} + p^{n-3+1} + \dots + p^{n-3+n-3} + p^{n-3}(p-1)(1 + \dots + (n-2)) \\ &= p^{n-3} \left(\frac{p^{n-2} - 1}{p-1} + (p-1) \binom{n-1}{2} \right). \end{aligned}$$

We argue by induction, first noting that $g_1(p^2) = 0$ and

$$g_2(p^3) = \frac{2p + 2p^3 - 2p^2 - 4p + 2}{2(p-1)^2(p+1)} = 1.$$

The induction hypothesis along with some algebraic simplification shows that

$$\begin{aligned} g_n(p^{n+1}) - g_{n-1}(p^n) &= (n-1)p^{n-2} + p^{n-3} \left(\frac{p^{n-2} - 1}{p-1} + (p-1) \binom{n-1}{2} \right), \end{aligned}$$

completing the proof. ■

Note that the formula of Corollary 3.7 matches the expressions for $g_5(p^6)$, $g_6(p^7)$, and $g_7(p^8)$ given in Theorem 3.2. The following result together with Lemmas 3.4, 3.5 and 3.6 and the formula for $g_4(p^6)$ given in Table 1 implies the formula for $g_5(p^7)$ given in Theorem 3.2.

THEOREM 3.8. *We have*

Table 3. Values of $g_\alpha(p)$ for some $\alpha \in \mathcal{C}'_{5,7}$

$g_{(2,2,2,1)}(p)$	$3p^4 + 2p^3 - 4p^2$
$g_{(2,2,1,2)}(p)$	$p^4 + 2p^3 - 2p^2$
$g_{(2,1,2,2)}(p)$	$2p^3 - p^2$
$g_{(3,2,1,1)}(p)$	$7p^4 - 6p^3 + 6p^2$
$g_{(3,1,2,1)}(p)$	$p^4 + 5p^3 - 2p^2$
$g_{(3,1,1,2)}(p)$	$3p^3$

Again we defer the proof to Section 3.3.

In order to compute $g_5(p^8)$ and $g_6(p^8)$, we must work significantly harder. The following result together with the results above implies the formulas for $g_5(p^8)$ and $g_6(p^8)$ given in Theorem 3.2.

THEOREM 3.9. *We have*

Table 4. Values of $g_\alpha(p)$ for some $\alpha \in \mathcal{C}'_{5,8}$

$g_{(2,1,2,3)}(p)$	$2p^3 - p^2$	$g_{(3,1,2,2)}(p)$	$p^4 + 2p^3 - p^2$
$g_{(2,1,3,2)}(p)$	p^4	$g_{(3,1,3,1)}(p)$	$2p^4 + 6p^3 - 2p^2$
$g_{(2,2,1,3)}(p)$	$p^4 + 2p^3 - 2p^2$	$g_{(3,2,1,2)}(p)$	$5p^4 - 4p^3 + 2p^2$
$g_{(2,2,2,2)}(p)$	$2p^4 - p^2$	$g_{(3,2,2,1)}(p)$	$p^5 + 8p^4 - 8p^3 + 4p^2$
$g_{(2,2,3,1)}(p)$	$4p^4 + 2p^3 - 4p^2$	$g_{(3,3,1,1)}(p)$	$15p^4 - 9p^3 + 3p^2$
$g_{(2,3,1,2)}(p)$	$3p^4 - p^2$	$g_{(4,1,1,2)}(p)$	$p^4 + 2p^3$
$g_{(2,3,2,1)}(p)$	$10p^4 - 11p^3 + 4p^2$	$g_{(4,1,2,1)}(p)$	$5p^4 - p^3 - 2p^2$
$g_{(3,1,1,3)}(p)$	$3p^3$	$g_{(4,2,1,1)}(p)$	$16p^4 - 21p^3 + 6p^2$

and

Table 5. Values of $g_\alpha(p)$ for some $\alpha \in \mathcal{C}'_{6,8}$

$g_{(2,1,1,2,2)}(p)$	$2p^4 - p^3$
$g_{(2,1,2,1,2)}(p)$	$p^5 + 2p^4 - 2p^3$
$g_{(2,1,2,2,1)}(p)$	$3p^5 + 2p^4 - 4p^3$
$g_{(2,2,1,1,2)}(p)$	$p^6 + 3p^4 - 3p^3$
$g_{(2,2,1,2,1)}(p)$	$2p^6 + 2p^5 + 2p^4 - 7p^3 + 2p^2$
$g_{(2,2,2,1,1)}(p)$	$4p^6 + 7p^5 - 16p^4 + 12p^3 - 6p^2$
$g_{(3,1,1,1,2)}(p)$	$4p^4$
$g_{(3,1,1,2,1)}(p)$	$p^5 + 8p^4 - 4p^3$
$g_{(3,1,2,1,1)}(p)$	$8p^5 - 3p^4 + 3p^3$
$g_{(3,2,1,1,1)}(p)$	$5p^6 + 6p^5 - 14p^4 + 16p^3$

We do not give the details of the computations that go into the proof of Theorem 3.9. They are similar to the computations for Theorem 3.8, but more extensive.

3.3. $f_n(p^7)$ and $f_n(p^8)$: details. In this section we give the proofs of Lemmas 3.5 and 3.6, and Theorem 3.8.

We first make some observations that will be useful throughout this section. For the rest of this section, we write v_1, \dots, v_n for the columns of an $n \times n$ matrix A . We write $\text{col}(A)$ for the set of integer linear combinations of the columns of A . If A is a matrix in Hermite normal form with $\det(A) \neq 0$ then for any i it is clear that $v_i \circ v_i \in \text{col}(A)$. If A is an irreducible subring matrix then its last column is $v_n = (1, \dots, 1)^T$ and for any i it is clear that $v_i \circ v_n \in \text{col}(A)$.

Proof of Lemma 3.5. An irreducible subring matrix A that has diagonal $(p^\beta, p, \dots, p, 1)$ is of the form

$$\begin{pmatrix} p^\beta & a_1p & a_2p & \cdots & a_{n-2}p & 1 \\ 0 & p & 0 & \cdots & 0 & 1 \\ 0 & 0 & \ddots & \cdots & \vdots & 1 \\ 0 & 0 & 0 & \ddots & \vdots & 1 \\ 0 & 0 & 0 & 0 & p & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

where $0 \leq a_i \leq p^\beta - 1$ for each $1 \leq i \leq n-2$. If $v_i \circ v_i \in \text{col}(A)$, then $p^\beta \mid (a_i^2 - a_i)p^2$. If $v_i \circ v_j \in \text{col}(A)$ for $2 \leq i < j \leq n-1$, then $p^\beta \mid a_i a_j p^2$. Therefore, irreducible subring matrices with diagonal $(p^\beta, p, \dots, p, 1)$ are in bijection with solutions (a_1, \dots, a_{n-2}) to

$$\begin{aligned} a_i(a_i - 1) &\equiv 0 \pmod{p^{\beta-2}}, \\ a_i a_j &\equiv 0 \pmod{p^{\beta-2}}, \end{aligned}$$

where we have one congruence of the first type for each $2 \leq i \leq n-1$, and one congruence of the second type for each $2 \leq i < j \leq n-1$.

When $\beta = 2$, any choice of (a_1, \dots, a_{n-2}) gives an irreducible subring matrix. There are p choices for each a_i , completing the proof in this case.

Suppose that $\beta \geq 3$. Clearly $a_i(a_i - 1) \equiv 0 \pmod{p^{\beta-2}}$ implies that $a_i \equiv 0 \pmod{p^{\beta-2}}$ or $a_i - 1 \equiv 0 \pmod{p^{\beta-2}}$. There are p choices for a_i with $a_i \equiv 0 \pmod{p^{\beta-2}}$ and p choices for a_i with $a_i - 1 \equiv 0 \pmod{p^{\beta-2}}$. If $i \neq j$ and $a_i - 1 \equiv a_j - 1 \equiv 0 \pmod{p^{\beta-2}}$, then $a_i a_j \not\equiv 0 \pmod{p^{\beta-2}}$, and (a_1, \dots, a_{n-2}) does not give an irreducible subring matrix.

We see that (a_1, \dots, a_{n-2}) gives an irreducible subring matrix if and only if either $a_i \equiv 0 \pmod{p^{\beta-2}}$ for each i , or there exists a unique j with $a_j - 1 \equiv 0 \pmod{p^{\beta-2}}$ and $a_i \equiv 0 \pmod{p^{\beta-2}}$ for every $i \neq j$. This leads to $p^{n-2} + (n-2)p^{n-2} = (n-1)p^{n-2}$ total irreducible subring matrices. ■

The next argument is similar, but more complicated.

Proof of Lemma 3.6. An irreducible subring matrix A that has diagonal $(p^2, p, \dots, p, p^\beta, p, \dots, p, 1)$, where the p^β is in the k th column, is of the form

$$\begin{pmatrix} p^2 & a_1p & a_2p & \cdots & a_{k-1}p & \cdots & \cdots & a_{n-2}p & 1 \\ 0 & p & 0 & \cdots & 0 & \cdots & \cdots & 0 & 1 \\ 0 & 0 & p & \cdots & \vdots & \cdots & \cdots & \vdots & 1 \\ 0 & \cdots & 0 & \ddots & \vdots & \cdots & \cdots & \vdots & 1 \\ 0 & \cdots & \cdots & 0 & p^\beta & b_1p & \cdots & b_rp & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & p & \cdots & \cdots & 1 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & \ddots & \cdots & 1 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & p & 1 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix},$$

where $0 \leq a_i \leq p-1$ for each $1 \leq i \leq n-2$, and $0 \leq b_j \leq p^\beta-1$ for each $1 \leq j \leq r$. It is easy to see that if $\min(i, j) \leq k$, then $v_i \circ v_j \in \text{col}(A)$.

For any $1 \leq m \leq r$, $v_{k+m} \circ v_{k+m} \in \text{col}(A)$ if and only if the following two congruences are satisfied:

$$\begin{aligned} b_m(b_m - 1) &\equiv 0 \pmod{p^{\beta-2}}, \\ a_{k-1}b_m(b_m - 1) &\equiv 0 \pmod{p^{\beta-1}}. \end{aligned}$$

For any $1 \leq i < j \leq r$, we have $v_{k+i} \circ v_{k+j} \in \text{col}(A)$ if and only if the following two congruences are satisfied:

$$\begin{aligned} b_i b_j &\equiv 0 \pmod{p^{\beta-2}}, \\ a_{k-1} b_i b_j &\equiv 0 \pmod{p^{\beta-1}}. \end{aligned}$$

We see that $a_1, \dots, a_{k-2}, a_k, \dots, a_{n-2}$ do not play a role in these congruences. Therefore, the number of irreducible subring matrices with diagonal $(p^2, p, \dots, p, p^\beta, p, \dots, p, 1)$ is equal to p^{n-3} times the number of solutions $(a_{k-1}, b_1, \dots, b_r)$ to this collection of congruences.

We split the count into two pieces. First suppose that $a_{k-1} \not\equiv 0 \pmod{p}$. We count solutions to

$$\begin{aligned} b_m(b_m - 1) &\equiv 0 \pmod{p^{\beta-1}}, \\ b_i b_j &\equiv 0 \pmod{p^{\beta-1}}, \end{aligned}$$

where we have one inequality of the first type for each $1 \leq m \leq r$, and one inequality of the second type for each $1 \leq i < j \leq r$. Since $0 \leq b_m \leq p^{\beta-1}-1$, there is a unique b_m with $b_m \equiv 0 \pmod{p^{\beta-1}}$, and a unique b_m with $b_m - 1 \equiv 0 \pmod{p^{\beta-1}}$. If $i \neq j$ and $b_i - 1 \equiv b_j - 1 \equiv 0 \pmod{p^{\beta-1}}$, then $b_i b_j \not\equiv 0 \pmod{p^{\beta-1}}$, and we do not get a solution to these congruences. So, as in the proof of the previous lemma, we get $p^{n-3}(r+1)(p-1)$ irreducible subring matrices with $a_{k-1} \not\equiv 0 \pmod{p}$.

Now suppose that $a_{k-1} \equiv 0 \pmod{p}$. We count solutions to

$$\begin{aligned} b_m(b_m - 1) &\equiv 0 \pmod{p^{\beta-2}}, \\ b_i b_j &\equiv 0 \pmod{p^{\beta-2}}, \end{aligned}$$

where we have one inequality of the first type for each $1 \leq m \leq r$, and one inequality of the second type for each $1 \leq i < j \leq r$. We are now in the exact same setting as in the proof of the previous lemma. When $\beta = 2$, any of the p^r choices of (b_1, \dots, b_r) gives a solution to these congruences. This gives p^{n-3+r} total irreducible subrings matrices. When $\beta \geq 3$, there are $(r+1)p^r$ solutions (b_1, \dots, b_r) to these inequalities, which gives $(r+1)p^{n-3+r}$ total irreducible subrings with $a_{k-1} \equiv 0 \pmod{p}$. ■

We next prove each of the formulas given in Theorem 3.8. We give one case in detail and note that the remaining arguments are similar, but significantly easier.

LEMMA 3.10. *We have $g_{(3,2,1,1)}(p) = 7p^4 - 6p^3 + 6p^2$.*

Proof. This is an easy computation when $p = 2$, so for the rest of the proof suppose $p \geq 3$.

An irreducible subring matrix A with diagonal $(p^3, p^2, p, p, 1)$ is of the form

$$\begin{pmatrix} p^3 & cp & xp & yp & 1 \\ 0 & p^2 & up & vp & 1 \\ 0 & 0 & p & 0 & 1 \\ 0 & 0 & 0 & p & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

where $0 \leq c, x, y \leq p^2 - 1$ and $0 \leq u, v \leq p - 1$.

If $v_2 \circ v_2 \in \text{col}(A)$, then

$$\begin{pmatrix} c^2 p^2 \\ p^4 \end{pmatrix} = p^2 \begin{pmatrix} cp \\ p^2 \end{pmatrix} + \lambda \begin{pmatrix} p^3 \\ 0 \end{pmatrix}$$

for some $\lambda \in \mathbb{Z}$. This implies $p^3 \mid (c^2 p^2 - cp^3)$, so $p \mid c$. Define c' by $c = pc'$ where $0 \leq c' \leq p - 1$.

Taking $v_3 \circ v_3$ or $v_4 \circ v_4$ and applying an argument like the one for $v_2 \circ v_2$ gives

$$(3.3) \quad (x^2 - x) - (u^2 - u)c' \equiv 0 \pmod{p},$$

$$(3.4) \quad (y^2 - y) - (v^2 - v)c' \equiv 0 \pmod{p}.$$

Taking $v_3 \circ v_4$ gives

$$(3.5) \quad xy - uvc' \equiv 0 \pmod{p}.$$

These congruences depend only on x and y modulo p , rather than their particular values, so any solution (x, y, u, v, c') to these three congruences

gives p^2 irreducible subring matrices. Therefore, we need only count those solutions to equations (3.3)–(3.5) for which $0 \leq x, y \leq p - 1$.

If $c' = 0$, then equations (3.3) and (3.4) imply that $x, y \in \{0, 1\}$. By (3.5) we cannot have $x = y = 1$. Any choices of u and v now satisfy these equations. This gives $3p^2$ choices for (x, y, u, v, c') and $3p^4$ irreducible subring matrices.

For the rest of the proof suppose $c' \neq 0$. We consider cases based on u and x . Equation (3.3) implies that $u \in \{0, 1\}$ if and only if $x \in \{0, 1\}$.

CLAIM 1. *Suppose that $c' \neq 0$. The following table gives the number of solutions to equations (3.3)–(3.5) with specified values of u and x :*

u	x	number of solutions
0	0	p^2
1	0	$2(p - 1)$
0	1	$2(p - 1)$
1	1	$2(p - 1)$
$\notin \{0, 1\}$	$\notin \{0, 1\}$	$3(p - 2)^2$

We further divide up the last case of this claim.

CLAIM 2. *Suppose that $c' \neq 0$ and $u, x \notin \{0, 1\}$. There are $(p - 2)^2$ solutions with $v = 0$. When $v \neq 0$, there are $(p - 1)(p - 2)$ solutions with $x = u$ and $(p - 2)(p - 3)$ solutions with $x \neq u$.*

Once these claims are established, we count

$$3p^4 + p^2(p^2 + 6(p - 1) + 3(p - 2)^2) = 7p^4 - 6p^3 + 6p^2$$

total irreducible subrings, completing the proof.

We now prove Claim 1.

CASE 1: $u = x = 0$. We need only count solutions to (3.4). If $v \in \{0, 1\}$, then for any of the $p - 1$ choices for c' there are two solutions y , namely $y \in \{0, 1\}$, for a total of $4(p - 1)$ solutions. Suppose $v \notin \{0, 1\}$. For any $y \notin \{0, 1\}$ there exists a unique value of c' that gives a solution to this equation. If $y \in \{0, 1\}$, then we get no solutions. Adding these cases together gives $4(p - 1) + (p - 2)^2 = p^2$ solutions.

CASE 2: $u = 1, x = 0$. Equation (3.5) implies $uv c' = 0$, and since u and c' are non-zero, we must have $v = 0$. Equation (3.4) implies $y \in \{0, 1\}$, so accounting for the $p - 1$ possible values of c' gives $2(p - 1)$ solutions.

CASE 3: $u = 0, x = 1$. Equation (3.5) implies $y = 0$. Equation (3.4) gives $v \in \{0, 1\}$, so accounting for the $p - 1$ possible values of c' gives $2(p - 1)$ solutions.

CASE 4: $u = 1, x = 1$. Equation (3.5) gives $y \equiv vc' \pmod{p}$. Substituting this into (3.4) gives $(c'^2 - c')v^2 \equiv 0 \pmod{p}$. If $c' = 1$ we have p choices for v . If $c' \neq 1$ then $v = 0$. This gives $p + p - 2 = 2(p - 1)$ solutions.

For the rest of the proof suppose that $c' \neq 0$ and $x, u \notin \{0, 1\}$. We consider two further subcases.

CASE 5: $v = 0$. Equation (3.5) implies $y = 0$. Setting $c' = \frac{x^2-x}{u^2-u}$ for any choice of x, u gives a valid solution. This gives $(p-2)^2$ solutions.

CASE 6: $v \neq 0$. Equations (3.3) and (3.5) imply that

$$c' \equiv \frac{x(x-1)}{u(u-1)} \equiv \frac{xy}{uv} \pmod{p}.$$

This implies $v \equiv \frac{y(u-1)}{x-1} \pmod{p}$. By assumption $v \neq 0$, so equation (3.5) implies $y \neq 0$. Substituting this expression for v into equation (3.4) and dividing by y gives

$$(3.6) \quad y(1 - c'(u-1)^2/(x-1)^2) + c' \frac{u-1}{x-1} - 1 \equiv 0 \pmod{p}.$$

We need only count solutions to equation (3.6).

Equation (3.6) is linear in y . The coefficient of y is 0 precisely when $c' \equiv \frac{(x-1)^2}{(u-1)^2} \pmod{p}$. Since $c' \equiv \frac{x(x-1)}{u(u-1)} \pmod{p}$ by equation (3.3), this is equivalent to $\frac{x}{u} \equiv \frac{x-1}{u-1} \pmod{p}$. This implies $x \equiv u \pmod{p}$.

Suppose that $x = u$. For any of the $p-2$ possible choices for x , any choice of y gives a solution to (3.6), except that $y = 0$ implies $v = 0$ by (3.5), a case we have already considered. Therefore, this case gives $(p-1)(p-2)$ solutions.

When $x \neq u$, for any of the $(p-2)(p-3)$ choices of x and u there are unique choices of y and c' such that (3.6) holds. This gives $(p-2)(p-3)$ solutions.

This completes the proofs of the two claims, hence of Lemma 3.10. ■

Proof of Theorem 3.8.

CASE 1: $g_{(2,2,2,1)}(p) = 3p^4 + 2p^3 - 4p^2$. We count irreducible subring matrices A of the form

$$\begin{pmatrix} p^2 & ap & bp & cp & 1 \\ 0 & p^2 & dp & ep & 1 \\ 0 & 0 & p^2 & fp & 1 \\ 0 & 0 & 0 & p & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

where $0 \leq a, b, c, d, e, f \leq p-1$. Taking pairwise products of columns shows that we get an irreducible subring matrix if and only if

$$\begin{cases} ad \equiv 0 \pmod{p}, \\ d(f^2 - f) \equiv 0 \pmod{p}, \\ b(f^2 - f) + a(e^2 - e) \equiv 0 \pmod{p}. \end{cases}$$

If $f \in \{0, 1\}$, these congruences become $ad \equiv 0 \pmod{p}$ and $a(e^2 - e) \equiv 0 \pmod{p}$. If $p \mid a$, then any values of b, c, d, e give an irreducible subring. If $p \nmid a$ we must have $p \mid d$ and $e \in \{0, 1\}$. If $f \notin \{0, 1\}$ then we have $p \mid d$ and our final remaining condition is $b(f^2 - f) + a(e^2 - e) \equiv 0 \pmod{p}$. For any choice of a and e , there is a unique value of b that satisfies this equation. Therefore,

$$g_{(2,2,2,1)}(p) = 2p^4 + 4(p-1)p^2 + (p-2)p^3 = 3p^4 + 2p^3 - 4p^2.$$

CASE 2: $g_{(2,2,1,2)}(p) = p^4 + 2p^3 - 2p^2$. We count irreducible subring matrices A of the form

$$\begin{pmatrix} p^2 & ap & bp & cp & 1 \\ 0 & p^2 & dp & ep & 1 \\ 0 & 0 & p & 0 & 1 \\ 0 & 0 & 0 & p^2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

where $0 \leq a, b, c, d, e \leq p-1$. Taking pairwise products of columns shows that we get an irreducible subring matrix if and only if

$$\begin{cases} ae \equiv 0 \pmod{p}, \\ a(d^2 - d) \equiv 0 \pmod{p}. \end{cases}$$

There are p^4 solutions with $p \mid a$, and $2p^2(p-1)$ with $p \nmid a$.

CASE 3: $g_{(2,1,2,2)}(p) = 2p^3 - p^2$. We count irreducible subring matrices A of the form

$$\begin{pmatrix} p^2 & ap & bp & cp & 1 \\ 0 & p & 0 & 0 & 1 \\ 0 & 0 & p^2 & dp & 1 \\ 0 & 0 & 0 & p^2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

where $0 \leq a, b, c, d \leq p-1$. Taking pairwise products of columns shows that we get an irreducible subring matrix if and only if $bd \equiv 0 \pmod{p}$. There are $2p-1$ choices for the pair (b, d) and any such pair gives p^2 irreducible subrings.

CASE 4: $g_{(3,1,2,1)}(p) = p^4 + 5p^3 - 2p^2$. We count irreducible subring matrices A of the form

$$\begin{pmatrix} p^3 & ap & bp & cp & 1 \\ 0 & p & 0 & 0 & 1 \\ 0 & 0 & p^2 & dp & 1 \\ 0 & 0 & 0 & p & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

where $0 \leq a, b, c \leq p^2 - 1$ and $0 \leq d \leq p-1$. If $v_3 \circ v_3 \in \text{col}(A)$, then $p \mid b$.

Let $bp = b'p^2$ where $0 \leq b' \leq p - 1$. Taking pairwise products of columns shows that we get an irreducible subring matrix if and only if

$$\begin{cases} a^2 - a \equiv 0 \pmod{p}, \\ ac \equiv 0 \pmod{p}, \\ (c^2 - c) - b'(d^2 - d) \equiv 0 \pmod{p}. \end{cases}$$

These congruences only depend on a, c modulo p , so we count solutions modulo p and then multiply by p^2 . First suppose that $p \mid a$. It is easy to see that there are $2(3p-2)+(p-2)^2$ solutions to $(c^2 - c) - b'(d^2 - d) \equiv 0 \pmod{p}$. If $p \nmid a$ then $p \mid c$ and we need only note that there are $3p - 2$ solutions to $b'(d^2 - d) \equiv 0 \pmod{p}$. Combining these observations completes the proof.

CASE 5: $g_{(3,1,1,2)}(p) = 3p^3$. We count irreducible subring matrices A of the form

$$\begin{pmatrix} p^3 & ap & bp & cp & 1 \\ 0 & p & 0 & 0 & 1 \\ 0 & 0 & p & 0 & 1 \\ 0 & 0 & 0 & p^2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

where $0 \leq a, b, c \leq p^2 - 1$. If $v_4 \circ v_4 \in \text{col}(A)$, then $p \mid c$. Let $cp = c'p^2$ where $0 \leq c' \leq p - 1$. Taking pairwise products of columns shows that we get an irreducible subring matrix if and only if

$$\begin{cases} a^2 - a \equiv 0 \pmod{p}, \\ b^2 - b \equiv 0 \pmod{p}, \\ ab \equiv 0 \pmod{p}. \end{cases}$$

These congruences are satisfied if and only if $(a, b) \pmod{p} \in \{(0,0), (0,1), (1,0)\}$. This gives $3p^3$ total irreducible subrings. ■

We do not give details for the $g_\alpha(p)$ computations of Theorem 3.9. They are similar in spirit to the computations of this section but the details are significantly more extensive.

4. Lower bounds on $g_n(p^e)$. We now give a lower bound on $g_n(p^e)$ when $n - 1 \leq e \leq 2(n - 1)$. We do this by giving a lower bound on $g_\alpha(p^e)$ for a particular composition α of e of length $n - 1$. These lower bounds on $g_n(p^e)$ together with Proposition 2.8 give lower bounds on $f_n(p^e)$.

PROPOSITION 4.1. *Let $\alpha = (2, \dots, 2, 1, \dots, 1)$ be a composition of length $n - 1$ with r entries equal to 2 and s entries equal to 1. Then $g_\alpha(p) \geq p^{rs}$.*

Note that $r + s = n - 1$ and $2r + s = e$. Solving for r and s in terms of n and e gives $(r, s) = (e - (n - 1), 2(n - 1) - e)$.

Proof of Proposition 4.1. Let A be an upper triangular matrix with columns v_1, \dots, v_n where the diagonal entry of columns v_1, \dots, v_r is p^2 , the diagonal entry of columns v_{r+1}, \dots, v_{r+s} is p , and the final column is $(1, \dots, 1)^T$. Suppose that every non-diagonal entry in the first $n-1$ columns of this matrix is zero except possibly in the first r rows of columns v_{r+1}, \dots, v_{r+s} . In each of these rs entries there are p integers $a_{i,j}$ satisfying $0 \leq a_{i,j} \leq p^2 - 1$ and $a_{i,j} \equiv 0 \pmod{p}$. This gives p^{rs} total matrices. It is easy to check that each one is an irreducible subring matrix. ■

The proof of this proposition comes from producing a set of irreducible subring matrices with diagonal $(p^2, \dots, p^2, p, \dots, p, 1)$ that have many entries equal to 0. Not all irreducible subring matrices with this diagonal have all of these entries equal to 0, so the lower bound of Proposition 4.1 is not actually equal to $g_\alpha(p)$. For example, Lemma 3.6 implies that $g_{(2,2,1,1)}(p) = p^4 + 3p^2(p-1)$, larger than the lower bound of p^4 from Proposition 4.1.

Proposition 4.1 gives a lower bound on $g_n(p^e)$ for every pair (n, e) with $n-1 \leq e \leq 2(n-1)$. For a fixed value of e , we now determine which n gives the largest lower bound. That is, for fixed e we look for the non-negative integer n maximizing the function $h(e, n) = (e - (n-1))(2(n-1) - e)$. It is easy to check that $h(e, n+1) \geq h(e, n)$ if and only if $n \leq (3e+2)/4$. This gives the following lower bound.

COROLLARY 4.2. *Let e be a positive integer. We have*

$$\max_n g_n(p^e) \geq \begin{cases} p^{e^2/8} & \text{if } e \equiv 0 \pmod{4}, \\ p^{(e^2-1)/8} & \text{if } e \equiv 1 \pmod{4}, \\ p^{(e^2-4)/8} & \text{if } e \equiv 2 \pmod{4}, \\ p^{(e^2-1)/8} & \text{if } e \equiv 3 \pmod{4}. \end{cases}$$

In Section 3 we saw that for each $e \leq 8$ and each n , $g_n(p^e)$ was given by a polynomial in p . For each e , the maximum over all n of the degree of this polynomial is equal to the degree of the monomial on the right hand side of the expression given in Corollary 4.2. For example,

$$g_7(p^8) = p^8 + p^7 + 2p^6 + 23p^5 + 3p^4 + 2p^3 + 2p^2 + p + 1,$$

a polynomial of degree $8^2/8 = 8$. It is unclear whether for larger values of e these lower bounds will continue to grow at a rate similar to the growth of $\max_n g_n(p^e)$.

The lower bounds of this section are related to Brakenhoff's lower bounds for orders of bounded index in the ring of integers of a number field.

PROPOSITION 4.3 ([5, Lemma 5.10]). *Let \mathcal{O}_K be the ring of integers of a number field K . Every additive subgroup G of \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.*

The subrings R described in the proof of Proposition 4.1 do indeed satisfy $\mathbb{Z} + p^2\mathbb{Z}^n \subset R \subset \mathbb{Z} + p\mathbb{Z}^n$, where the first \mathbb{Z} is interpreted as integer multiples of the multiplicative identity $(1, \dots, 1)$. Brakenhoff gives a lower bound for the number of additive subgroups satisfying the hypothesis of Proposition 4.3 and derives a lower bound for the number of orders of index at most X in the ring of integers of a degree n number field K . This requires an easy optimization along the lines of Corollary 4.2. In this way, our lower bounds for $g_n(p^e)$ are analogous to the lower bounds from [5, Theorem 5.1].

5. Further questions

5.1. Uniformity of $\zeta_{\mathbb{Z}^n}^R(s)$ and varieties over finite fields. Questions 1.12 and 1.13 are about how counting functions vary with p . Theorem 1.11 gives information on how $f_n(p^e)$ behaves for fixed n and p .

We recall a theorem of du Sautoy and Grunewald [13] about the behavior of local factors of zeta functions of rings as we vary the prime. This result follows from the machinery of [13], suitably modified for the requirement that subrings must contain the multiplicative identity. We use the notation of [33, Theorem A].

THEOREM 5.1. *Let L be a ring of additive rank n containing a multiplicative identity. Then there are smooth projective varieties V_t , $t \in \{1, \dots, m\}$, defined over \mathbb{Q} , and rational functions $W_t(X, Y) \in \mathbb{Q}(X, Y)$ such that for almost all primes p the following holds: Denoting by $b_t(p)$ the number of \mathbb{F}_p -rational points of $\overline{V_t}$, the reduction modulo p of V_t , we have*

$$\zeta_{L,p}^R(s) = \sum_{t=1}^m b_t(p) W_t(p, p^{-s}).$$

Not much is known about the types of varieties that can appear in these zeta functions as we vary over different rings. See the paper of du Sautoy [12] and Voll's survey [32, Section 2.1] for more information.

In case $\zeta_{\mathbb{Z}^n}^R(s)$ is not uniform it would be interesting to see what kinds of varieties arise in the formulas of Theorem 5.1. The conditions for the columns of an $n \times n$ matrix to generate a multiplicatively closed sublattice of \mathbb{Z}^n define many equations in the matrix entries. For examples for $n = 4$ and 5, see [18, Lemmas 12 and 13]. It is possible that once n and e are large enough, varieties V_t occur for which the functions $b_t(p)$ in Theorem 5.1 are not polynomials in p , and that these functions occur in formulas for $f_n(p^e)$.

5.2. Coefficients of $f_n(p^e)$ and $g_n(p^e)$. For small fixed values of n and e , the function $g_n(p^e)$ is a polynomial in p with non-negative coefficients. However, this is not true for $g_5(p^8) = p^5 + 77p^4 - 13p^3 + 12p^2 + p + 1$. As far as we know, there has been no previous study of the positivity of coefficients

of $g_n(p^e)$ or $f_n(p^e)$. These questions are motivated by analogous work related to Hall polynomials.

DEFINITION 5.2. (1) Let $\lambda = (\lambda_1, \dots, \lambda_k)$, where $\lambda_1 \geq \dots \geq \lambda_k > 0$. A finite abelian p -group G is of *type* λ if

$$G \cong \mathbb{Z}/p^{\lambda_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{\lambda_k}\mathbb{Z}.$$

(2) A subgroup of H of G is of *cotype* ν if G/H is of type ν .

(3) Let $g_{\mu\nu}^{\lambda}(p)$ be the number of subgroups H of a finite abelian p -group G of type λ such that H has type μ and cotype ν .

Hall proved that $g_{\mu\nu}^{\lambda}(p)$ is a polynomial in p with integer coefficients. Several other authors have studied these coefficients. For example, Butler and Hales [7] give a characterization of types λ for which all of the associated Hall polynomials have non-negative coefficients.

Maley [22] shows that the expansion of any $g_{\mu\nu}^{\lambda}(p)$ in terms of powers of $p-1$ has non-negative coefficients. In all cases that we have computed, the same property holds for $g_n(p^e)$. This is stronger than the observation that $g_n(1)$ is a non-negative integer.

QUESTION 5.3. When $g_n(p^e)$ is expanded in terms of powers of $p-1$, are the coefficients positive?

For an example of non-negativity questions like this for zeta functions associated to graphs, see the recent work of Rossmann and Voll [28, Section 1.9]. Evseev [15] has studied the substitution $p=1$ in the form of the *reduced zeta function*. The $p \rightarrow 1$ behavior of local factors of zeta functions is related to the corresponding topological zeta function [26]. It would be interesting to undertake a more detailed study of the coefficients of $f_n(p^e)$ and $g_n(p^e)$. For more background on Hall polynomials and connections to counting subgroups of finite abelian groups, see the books of Macdonald [21] and Butler [6].

Acknowledgements. We thank the mathematics department at Yale University and the Summer Undergraduate Research at Yale (SUMRY) program for providing the opportunity to conduct this research. SUMRY is supported in part by NSF grant CAREER DMS-1149054. The second author was supported by NSF Grant DMS 1802281, NSA Young Investigator Grant H98230-16-10305 and an AMS-Simons Travel Grant.

We thank Franco Williams for his active involvement throughout this project and for many helpful conversations. We thank Christopher Voll and Tobias Rossmann for many extremely helpful comments. We would also like to extend our gratitude to Sam Payne, Sam Kimport, and José González for helping to organize SUMRY. The second author thanks Kelly Isham and Robert Lemke Oliver for helpful conversations and computational assistance.

We thank the referee for many helpful comments that greatly improved the paper. Lastly, we thank the Yale Center for Research Computing for High Performance Computing resources.

References

- [1] M. Bhargava, *Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants*, Int. Math. Res. Notices 2007, no. 17, art. rnm052, 20 pp.
- [2] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) 162 (2005), 1031–1063.
- [3] M. Bhargava, *The density of discriminants of quintic rings and fields*, Ann. of Math. (2) 172 (2010), 1559–1591.
- [4] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.
- [5] J. F. Brakenhoff, *Counting problems for number rings*, doctoral thesis, Leiden Univ., 2009.
- [6] L. Butler, *Subgroup lattices and symmetric functions*, Mem. Amer. Math. Soc. 112 (1994), no. 539, vi+160 pp.
- [7] L. Butler and A. Hales, *Nonnegative Hall polynomials*, J. Algebraic Combin. 2 (1993), 125–135.
- [8] B. Datskovsky and D. J. Wright, *Density of discriminants of cubic extensions*, J. Reine Angew. Math. 386 (1988), 116–138.
- [9] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A 322 (1971), no. 1551, 405–420.
- [10] J. Denef, *The rationality of the Poincaré series associated to the p -adic points on a variety*, Invent. Math. 77 (1984), 1–23.
- [11] J. Denef, *On the degree of Igusa’s local zeta function*, Amer. J. Math. 109 (1987), 991–1008.
- [12] M. P. F. du Sautoy, *Zeta functions of groups and rings: uniformity*, Israel J. Math. 86 (1994), 1–23.
- [13] M. P. F. du Sautoy and F. Grunewald, *Analytic properties of zeta functions and subgroup growth*, Ann. of Math. (2) 152 (2000), 793–833.
- [14] M. P. F. du Sautoy and L. Woodward, *Zeta Functions of Groups and Rings*, Lecture Notes in Math. 1925, Springer, Berlin, 2008, xii+208 pp.
- [15] A. Evseev, *Reduced zeta functions of Lie algebras*, J. Reine Angew. Math. 633 (2009), 197–211.
- [16] F. J. Grunewald, D. Segal and G. C. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. 93 (1988), 185–223.
- [17] J.-I. Igusa, *Some observations on higher degree characters*, Amer. J. Math. 99 (1977), 393–417.
- [18] N. Kaplan, J. Marcinek and R. Takloo-Bighash, *Distribution of orders in number fields*, Res. Math. Sci. 2 (2015), art. 6, 57 pp.
- [19] R. I. Liu, *Counting subrings of \mathbb{Z}^n of index k* , J. Combin. Theory Ser. A 114 (2007), 278–299.
- [20] A. Lubotzky and D. Segal, *Subgroup Growth*, Progr. Math. 212, Birkhäuser, Basel, 2003, xxii+453 pp.

- [21] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd ed., Oxford Math. Monogr., Clarendon Press, New York, 1995, x+475 pp.
- [22] F. Maley, *The Hall polynomial revisited*, J. Algebra 184 (1996), 363–371.
- [23] G. Malle, *On the distribution of Galois groups*, J. Number Theory 92 (2002), 315–329.
- [24] G. Malle, *On the distribution of Galois groups. II*, Experiment. Math. 13 (2004), 129–135.
- [25] J. Nakagawa, *Orders of a quartic field*, Mem. Amer. Math. Soc. 122 (1996), no. 583, viii+75 pp.
- [26] T. Rossmann, *Computing topological zeta functions of groups, algebras, and modules II*, J. Algebra 444 (2015), 567–605.
- [27] T. Rossmann, *Computing local zeta functions of groups, algebras, and modules*, Trans. Amer. Math. Soc. 370 (2018), 4841–4879.
- [28] T. Rossmann and C. Voll, *Groups, graphs and hypergraphs: average sizes of kernels of generic matrices with support constraints*, arXiv:1908.09589 (2019).
- [29] SageMath, The Sage Mathematics Software System (Version 8.3), The Sage Developers, 2019, <https://www.sagemath.org>.
- [30] R. Stanley, *Enumerative Combinatorics*, Vol. 1, 2nd ed., Cambridge Stud. Adv. Math. 49, Cambridge Univ. Press, Cambridge, 2012.
- [31] C. Voll, *Zeta functions of groups and rings—recent developments*, in: Groups St Andrews 2013, London Math. Soc. Lecture Note Ser. 422, Cambridge Univ. Press, Cambridge, 2015, 469–492.
- [32] C. Voll, *A newcomer’s guide to zeta functions of groups and rings*, in: Lectures on Profinite Topics in Group Theory, London Math. Soc. Student Texts 77, Cambridge Univ. Press, Cambridge, 2011, 99–144.
- [33] C. Voll, *Functional equations for zeta functions of groups and rings*, Ann. of Math. (2) 172 (2010), 1181–1218.

Stanislav Atanasov
 Department of Mathematics
 Columbia University
 Room 408, MC4406
 2990 Broadway
 New York, NY 10027, U.S.A.
 E-mail: stanislav@math.columbia.edu

Benjamin Krakoff
 Department of Mathematics
 University of Michigan
 East Hall B723
 530 Church Street
 Ann Arbor, MI 48109, U.S.A.
 E-mail: bkrakoff@umich.edu

Nathan Kaplan
 Department of Mathematics
 University of California, Irvine
 340 Rowland Hall
 Irvine, CA 92697, U.S.A.
 E-mail: nckaplan@math.uci.edu

Julia H. Menzel
 Program in History, Anthropology,
 and Science, Technology, and Society
 MIT
 Room E51-163
 77 Massachusetts Avenue
 Cambridge, MA 02139, U.S.A.
 E-mail: julimen@mit.edu