Kaplan *et al. Research in the Mathematical Sciences* (2015) 2:6
DOI 10.1186/s40687-015-0027-8

Research in the Mathematical Sciences
a SpringerOpen Journal

RESEARCH Open Access

Distribution of orders in number fields

Nathan Kaplan[1], Jake Marcinek[2] and Ramin Takloo-Bighash[3*]

*Correspondence: rtakloo@uic.edu
[3]Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, 851 S Morgan St (M/C 249), 60607, Chicago, IL, USA
Full list of author information is available at the end of the article

Abstract
In this paper, we study the distribution of orders of bounded discriminants in number fields. We use the zeta functions introduced by Grunewald, Segal, and Smith. In order to carry out our study, we use p-adic and motivic integration techniques to analyze the zeta function. We give an asymptotic formula for the number of orders contained in the ring of integers of a quintic number field. We also obtain non-trivial bounds for higher degree number fields.

AMS Subject Classification: Primary 11M41; 11R29; secondary 11S40

Keywords: Orders; *p*-adic and motivic integration; Subring zeta function

Introduction

Let $K/\mathbb{Q}$ be an extension of degree n with ring of integers $\mathcal{O}_K$. An order $\mathcal{O}$ is a subring of $\mathcal{O}_K$ with identity that is a $\mathbb{Z}$-module of rank n. Set

$$N_K(B) := |\{\mathcal{O} \subseteq \mathcal{O}_K; \mathcal{O} \text{ an order }, |\text{disc}\,\mathcal{O}| \leq B\}|\,.$$

In this paper, we study the asymptotic growth of $N_K(B)$ as B grows.

Results

Our first theorem, which is a consequence of the motivic framework used here, is the following result:

Theorem 1. *There is* $\alpha_K \in \mathbb{Q}_{>0}, \beta_K \in \mathbb{N}, C_K \in \mathbb{R}_{>0}$ *such that*

$$N_K(B) \sim C_K B^{\alpha_K} (\log B)^{\beta_K - 1}$$

as $B \to \infty$.

Let $E/\mathbb{Q}$ be the normal closure of K with Galois group $G = \text{Gal}\,(E/\mathbb{Q})$. Then G has a natural embedding in S_n as a transitive subgroup. Let V_2 be the vector space whose basis is the set of 2-element subsets of $\{1, \cdots, n\}$. The group G has a natural action on V_2. Let r_2 be the dimension of the space of G fixed vectors in V_2. Then, we have the following theorem:

Theorem 2. *Let* $K/\mathbb{Q}$ *number field of degree* n.

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

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

as $B \to \infty$;

Springer

© 2015 Kaplan et al.; licensee Springer. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Table 1 Transitive subgroups up to conjugation

n	Order	Group name	Generators	r_2
3	3	$\mathbb{Z}/3\mathbb{Z}$	$(1\ 2\ 3)$	1
3	6	S_3	$(1\ 2), (1\ 3)$	1
4	4	$\mathbb{Z}/4\mathbb{Z}$	$(1\ 2\ 3\ 4)$	2
4	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$(1\ 2)(3\ 4), (1\ 4)(2\ 3)$	3
4	8	D_4	$(1\ 2\ 3\ 4), (1\ 3)$	2
4	12	A_4	$(1\ 2\ 4), (2\ 3\ 4)$	1
4	24	S_4	$(1\ 2), (1\ 3), (1\ 4)$	1
5	5	$\mathbb{Z}/5\mathbb{Z}$	$(1\ 2\ 3\ 4\ 5)$	2
5	10	D_5	$(1\ 2\ 3\ 4\ 5), (1\ 4)(2\ 3)$	2
5	20	$\mathrm{AGL}(1,5)$	$(1\ 2\ 3\ 4\ 5), (2\ 3\ 5\ 4)$	2
5	60	A_5	$(1\ 2\ 4), (3\ 4\ 5), (2\ 3\ 5)$	1
5	120	S_5	$(1\ 2), (1\ 3), (1\ 4), (1\ 5)$	1

2. *For any $n > 5$,*

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

Table 1 lists the transitive subgroups of S_n for small n and the corresponding r_2 values. The reference for the list of subgroups up to conjugation is ([9], section 2.9). For the computation of r_2, see section 'Some remarks on r_2'.

In order to study the behavior of $N_K(B)$, we form the counting zeta function

$$\eta_K(s) = \sum_{\mathcal{O}\text{order}} \frac{1}{|\mathrm{disc}\,\mathcal{O}|^s},$$

where $\mathcal{O}_K$ is the ring of integers of K and $\mathcal{O}$ is an order. This series converges absolutely for $\Re s$ large, and in its domain of absolute convergence we have

$$\eta_K(s) = |\mathrm{disc}\,\mathcal{O}_\mathrm{K}|^{-s}\tilde{\eta}_K(2s)$$

where

$$\tilde{\eta}_K(s) = \sum_{\mathcal{O}\text{ order}} \frac{1}{[\mathcal{O}_K : \mathcal{O}]^s}.$$

The zeta function $\tilde{\eta}_K$ has an Euler product of the form

$$\tilde{\eta}_K(s) = \prod_p \tilde{\eta}_{K,p}(s)$$

where

$$\tilde{\eta}_{K,p}(s) = \sum_{\mathcal{O}} \frac{1}{[\mathcal{O}_K \otimes_\mathbb{Z} \mathbb{Z}_p : \mathcal{O}]^s}$$

and the summation in the last expression is over full rank sublattices of $\mathcal{O}_K \otimes_\mathbb{Z} \mathbb{Z}_p$ that are subrings with identity. We define the coefficients $a_i(p)$ by

$$\tilde{\eta}_{K,p}(s) = 1 + \sum_{i=1}^{\infty} \frac{a_i(p)}{p^{is}}.$$

The number $a_i(p)$ is what in section 'Our method' is denoted by $a^{1,<}_{\mathcal{O}_K}(p^i)$.

The proof of Theorem 2 has two main steps. The first step which is arithmetic is the following theorem:

Theorem 3 (Arithmetic Step). *The Euler product*

$$f(s) = \prod_{p \text{unramified}} \left(1 + a_1(p)p^{-s}\right)$$

converges absolutely for $\Re s$ large, and it has an analytic continuation to a meromorphic function on an open set containing $\Re s \geq 1$ with a unique pole at $s = 1$ of order r_2.

Remark 1. It is reasonable to conjecture that for n small the function $\tilde{\eta}_K(s)$ is holomorphic for $\Re s > 1$, and has an analytic continuation to a domain containing $\Re s \geq 1$ with a unique pole of order r_2 at $s = 1$. If this is true, then there is a nonzero constant C_K such that

$$N_K(B) = C_K B^{1/2} (\log B)^{r_2 - 1}(1 + o(1))$$

as $B \to \infty$. The conjecture is true for $n \leq 5$ by Theorem 2. The results of Brakenhoff [3], summarized in section 'Comparison with previous results' below, show that for $n \geq 8$ there is a pole to the right of $\Re s = 1$.

The second step of the proof of the main theorem is geometric. Since by Lemma 4.15 of [10] the finitely many bad primes do not contribute to the main pole, part 1 of Theorem 2 is a consequence of the following theorem:

Theorem 4 (Geometric Step for small n). *Let $n \leq 5$. There is a finite set S of primes such that the series*

$$\sum_{p \notin S} \sum_{i=2}^{\infty} \frac{a_i(p)}{p^{i\sigma}}$$

converges for any real $\sigma > 19/20$.

We give heuristic reasoning for why this result should hold in the case $n = 5$. Let $b_i(p)$ be the number of subrings with identity of $\mathbb{Z}_p^5$, i.e., orders, whose index is p^i. It is reasonable to expect that

$$a_i(p) \leq b_i(p) \tag{1}$$

for all i and p. It is then a consequence of Theorem 14 that the series

$$\sum_{p \text{odd prime}} \sum_{i=2}^{\infty} \frac{b_i(p)}{p^{i\sigma}}$$

converges for $\sigma > 19/20$. Alas, we have not been able to prove (1) - even though we are confident it is true. Here, we employ an alternative method based on p-adic integration.

Part 2 of Theorem 2 is a consequence of the following theorem and Lemma 4.15 of [10]:

Theorem 5 (Geometric step for large n). *Let $n > 5$. There is a finite set S of primes such that the series*

$$\sum_{p \notin S} \sum_{i=2}^{\infty} \frac{a_i(p)}{p^{i\sigma}}$$

converges for any real $\sigma > \frac{n}{2} - \frac{7}{6}$.

Remark 2. Note that by Theorem 1.5 of [10], the zeta function $\eta_K(s)$ has an analytic continuation to a domain of the form $\Re s > \alpha - \epsilon$ with $\alpha > 0$ the abscissa of convergence and $\epsilon > 0$.

Remark 3. A byproduct of our methods, stated as Corollary 4 and Corollary 5 in section 'The proof of Theorems 1 and 2', is an improvement of the upper bounds obtained by Brakenhoff [3], Theorem 5.1 and Theorem 8.1.

Remark 4. It would be interesting to obtain information about the constant C_K. For the cubic case, the results of [6] stated below give precise values for C_K. Corollary 1 of Nakagawa [24] gives the value of C_K in terms of certain Euler products, but it is not clear if these Euler products have any conceptual meaning. For higher degree extensions, we know nothing about the constants C_K.

More generally if $L = \prod_i K_i$ is an étale $\mathbb{Q}$-algebra with K_i's number fields, we define $\mathcal{O}_L = \prod_i \mathcal{O}_{K_i}$. Clearly, $\mathcal{O}_L$ is $\mathbb{Z}$-algebra which is free as a $\mathbb{Z}$-module of rank $d = \sum_i [K_i : \mathbb{Q}]$. We define an order $\mathcal{O}$ in $\mathcal{O}_L$ to be a subring with identity of $\mathcal{O}_L$ which is of $\mathbb{Z}$-rank d. Again, we set

$$\widetilde{\eta}_L(s) = \sum_{\mathcal{O} \text{ order}} \frac{1}{[\mathcal{O}_L : \mathcal{O}]^s}.$$

As usual, knowing the analytic properties of $\widetilde{\eta}_L(s)$ via Tauberian arguments, e.g., Theorem 9, gives us information about the function

$$\widetilde{N}_L(B) := |\{\mathcal{O} \subset \mathcal{O}_L; \mathcal{O}\text{an order}, [\mathcal{O}_L : \mathcal{O}] \le B\}|.$$

Our methods give an asymptotic formula for $\widetilde{N}_L(B)$ whenever $[L : \mathbb{Q}] \le 5$.

Let us explain the simplest possible case. For $d \in \mathbb{N}$, we set $N_d(B) := \widetilde{N}_{\mathbb{Q}^d}(B)$. Given $k \in \mathbb{N}$, we define $f_d(k)$ to be the number of orders in $\mathbb{Z}^d$ of index equal to k. Clearly, $N_d(B) = \sum_{k \le B} f_d(k)$. It is easy to see that the function $f_d(k)$ is multiplicative, i.e., if k_1, k_2 are coprime integers then $f_d(k_1k_2) = f_d(k_1)f_d(k_2)$.

This is the prototype of the problem that we study in this paper:

Problem 1.1. *Let $d \in \mathbb{N}$. Study the function $N_d(B)$ as $B \to \infty$.*

Despite its innocent appearance, this is a very difficult problem, and prior to our work, the only cases for which an asymptotic formula is known for $N_d(B)$ are $d = 2, 3, 4$ [19]. Here, we obtain an asymptotic formula for $N_5(B)$, and give non-trivial bounds for $N_d(B)$ when $d > 5$.

Definition 1. Let $d, k \in \mathbb{N}$. We define $a^{<}_{\mathbb{Z}^d}(k)$ to be number of subrings S of $\mathbb{Z}^d$, not necessarily with identity, such that $[\mathbb{Z}^d : S] = k$.

A subring S in $\mathbb{Z}^d$ which is of finite index as an additive group will necessarily be a free $\mathbb{Z}$-module of rank d. Such subrings are called *multiplicative sublattices* in [19]. An elementary proposition in [19] states that for any $d, k \in \mathbb{N}$, $d \ge 2$, we have

$$f_d(k) = a^{<}_{\mathbb{Z}^{d-1}}(k).$$

As a result, with the notation of section 'Our method'

$$\tilde{\eta}_{\mathbb{Q}^d}(s) = \zeta^{<}_{\mathbb{Z}^{d-1}}(s).$$

Determining the asymptotic behavior of $N_1(B)$ and $N_2(B)$ is trivial. In this paper, we will use the method of p-adic integration as in section 'Our method' to prove the following theorem:

Theorem 6. *1. Let $d \leq 5$. There is a positive real number C_d such that*

$$N_d(B) \sim C_d B(\log B)^{\binom{d}{2}-1}$$

as $B \to \infty$.

2. Suppose $d \geq 6$. Then for any $\epsilon > 0$ we have

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

as $B \to \infty$.

We actually prove a more precise statement and give error estimates; see Theorems 12, 13, and 14. We include the $d = 3$ case to illustrate our method in a simple case. Our results for $d \geq 5$ are new.

Theorem 6 is more than just a prototype of the type of result we can prove. The computations in section 'Orders of $\mathbb{Z}^5$' form the backbone of the proof of Theorem 2. In fact, Theorem 8 shows that, essentially, whatever estimate we obtain for the volumes of the sets considered in section 'Orders of $\mathbb{Z}^5$' works in general.

We expect the asymptotic formula in Part 1 of Theorem 6 to be valid for $d < 8$. The formalism of p-adic integration shows that $N_d(B)$ has an asymptotic formula of the form $CB^a(\log B)^{b-1}$, for a rational number a and a natural number b, but for $d \geq 8$ it is not clear what the numbers a, b should be.

We finish this introduction with the following conjecture:

Conjecture 1. *Let $K/\mathbb{Q}$ be a number field of degree d. Then with the notation of Theorem 1, we have*

$$\alpha_K = \frac{1}{2}\lim_{B\to\infty}\frac{\log N_d(B)}{\log B}.$$

In particular, α_K only depends on the extension degree of K over $\mathbb{Q}$.

Comparison with previous results

If we write

$$\zeta_{\mathbb{Z}^n}(s) := \sum_{\Lambda\subset\mathbb{Z}^n}\frac{1}{[\mathbb{Z}^n : \Lambda]^s},$$

where Λ is a sublattice of $\mathbb{Z}^n$, it can be seen that for $\Re(s) > n$, we have

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

As a result, $\zeta_{\mathbb{Z}^d}(s)$ has a pole of order 1 at $s = n$ with residue $\zeta(n)\zeta(n-1)\cdots\zeta(2)$. Consequently,

$$|\{\Lambda \leq \mathbb{Z}^n \mid \Lambda \text{sublattice}, [\mathbb{Z}^n : \Lambda] \leq B\}| \sim \frac{\zeta(n)\zeta(n-1)\cdots\zeta(2)}{d}B^n$$

as $B \to \infty$. The book [20] contains five distinct proofs of this fact.

Since in this work we are counting sublattices with additional structure, we expect slower asymptotic growth. Theorem 2 is trivial for a quadratic field as the counting zeta function is simply the Riemann zeta function $\zeta(s)$. For K a cubic or quartic extension of $\mathbb{Q}$, Theorem 2 is due to Datsovsky-Wright [6] for the cubic case, and Nakagawa [24] for the quartic case.

In the cubic setting, there is a bijection between the set of equivalence classes of integral binary cubic forms and the set of orders of cubic fields. Then it follows from Shintani's theory of zeta functions associated to the prehomogeneous vector space of binary cubic forms combined with a theorem of [6] that

$$\tilde{\eta}_K(s) = \frac{\zeta_K(s)}{\zeta_K(2s)}\zeta(2s)\zeta(3s-1).$$

In the quartic setting, Nakagawa explicitly computes the local factors of the zeta function $\tilde{\eta}_K$ using an intricate combinatorial argument involving counting the number of solutions of some very complicated congruences. Due to computational difficulties at the prime 2, Nakagawa's theorem assumes some mild ramification conditions. Under these conditions, he shows that the zeta function $\tilde{\eta}_K(s)$ has an analytic continuation to $\Re s > 2/3$. Nakagawa's explicit local computations can also be used to prove Theorem 6 for $d = 4$. The paper [19] contains a different approach to Theorem 6 using combinatorial arguments. Here, too, the local Euler factors of the counting zeta function are explicitly computed, though the proof follows from elegant recursive formulas, c.f. Propositions 6.2 and 6.3 of [19].

In a series of spectacular papers, Bhargava studies orders in quintic fields. In [1], he shows that there is a canonical bijection between the set of orbits of $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ on the space $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ and the set of isomorphism classes of pairs (R, S) with R a quintic ring and S a sextic resolvent ring of R. An impressive theorem of Bhargava [2] which is proved using the above bijection says that

$$\sum_{K \text{quintic}} N_K(B) \sim cB$$

as $B \to \infty$. Bhargava's methods do not identify the contribution of each $N_K(B)$ to the sum.

The thesis [3] contains an array of interesting results on the distribution of orders in number fields. In keeping with our notation below, for a number field K, we let

$$a^{1,<}_{\mathcal{O}_K}(m) = |\{\mathcal{O} \subset \mathcal{O}_K; \mathcal{O} \text{ an order}, [\,\mathcal{O}_K : \mathcal{O}] = m\}|\,.$$

We then let

$$a^{1,<}(n,m) = \max_{K/\mathbb{Q} \text{extension of degree } n} a^{1,<}_{\mathcal{O}_K}(m).$$

Theorem 5.1 of [3] is the statement that

$$c_7(n) \le \limsup_{m\to\infty} \frac{\log a^{1,<}(n,m)}{\log m} \le c_8(n)$$

with $c_7(n) = \max_{0\le d\le n-1} \frac{d(n-1-d)}{n-1+d}$ and $c_8(n)$ given by the following Table 2:

Table 2 Values of $c_8(n)$

n	2	3	4	5	6	7	8	9	10	11	12	13	≥ 14
$c_8(n)$	0	$\frac{1}{3}$	1	$\frac{20}{11}$	$\frac{29}{11}$	$\frac{186}{53}$	$\frac{49}{11}$	$\frac{119}{22}$	$\frac{70}{11}$	$\frac{388}{53}$	$\frac{440}{53}$	$\frac{492}{53}$	$n-\frac{8}{3}$

Furthermore,

$$\liminf_{n\to\infty} \frac{1}{n} \limsup_{m\to\infty} \frac{\log a^{1,<}(n,m)}{\log m} \geq 3 - 2\sqrt{2}$$

and

$$\limsup_{n\to\infty} \frac{1}{n} \limsup_{m\to\infty} \frac{\log a^{1,<}(n,m)}{\log m} \leq 1.$$

One can compute the values of $c_7(n)$ explicitly as follows:

$$c_7(n) = \begin{cases} \frac{k(2k-1)}{4k-1} & n = 3k; \\ \frac{k}{2} & n = 3k+1; \\ \frac{k(k+1)}{2k+1} & n = 3k+2. \end{cases}$$

In particular, for $n \geq 8$, $c_7(n) > 1$.

Theorem 8.1 of [3], which is used in [2], is the following result: If $K/\mathbb{Q}$ is a quintic field, then for any prime p

$$\sum_{k=1}^{\infty} \frac{a^{1,<}_{\mathcal{O}_K}\left(p^k\right)}{p^{2k}} = O\left(1/p^2\right).$$

We improve the upper bounds in these theorems in section 'The proof of Theorems 1 and 2', Corollary 4 and Corollary 5.

Our method

Given a ring R whose additive group is isomorphic to $\mathbb{Z}^d$ for some $d \in \mathbb{N}$, we define

$$a^<_R(k) := \left|\left\{S \text{subring of } R \mid [R:S] = k\right\}\right|.$$

For any $k \in \mathbb{N}$, $a^<_R(k)$ is finite. We define the *subring zeta function of R* by

$$\zeta^<_R(s) := \sum_{k=1}^{\infty} \frac{a^<_R(k)}{k^s} = \sum_{S \leq R} \frac{1}{[R:S]^s}.$$

We view $\zeta^<_R(s)$ not just as a formal series, but as a series converging on some non-trivial subset of the complex numbers. The idea is that the analytic properties of the resulting complex function have consequences for the distribution of subrings of finite index in R. In particular, by various Tauberian theorems, e.g., Theorem 9, the location of poles and their orders gives information about the function $s^<_R(B)$ defined by

$$s^<_R(B) := \sum_{k \leq B} a^<_R(k) = \left|\left\{S \text{subring of } R \mid [R:S] \leq B\right\}\right|.$$

Similar constructions can be made for subgroups of finitely generated groups and ideals in rings, but in this introduction, we only consider subring zeta functions. We have the following theorem which is a summary of results from [10,14]

Theorem 7. *1. The series $\zeta^<_R(s)$ converges in some right half plane of $\mathbb{C}$. The abscissa of convergence $\alpha^<_R$ of $\zeta^<_R(s)$ is a rational number. There is a $\delta > 0$ such that $\zeta^<_R(s)$ can be meromorphically continued to the domain $\{s \in \mathbb{C} \mid \Re(s) > \alpha^<_R - \delta\}$. Furthermore, the line $\Re(s) = \alpha^<_R$ contains at most one pole of $\zeta^<_R(s)$ at the point $s = \alpha^<_R$.*

1. *There is an Euler product decomposition*

$$\zeta_R^{<}(s) = \prod_p \zeta_{R,p}^{<}(s)$$

with the local Euler factor given by

$$\zeta_{R,p}^{<}(s) = \sum_{l=0}^{\infty} \frac{a_R^{<}\left(p^l\right)}{p^{ls}}.$$

This local factor is a rational function of p^{-s}*; there are polynomials* $P_p, Q_p \in \mathbb{Z}[x]$ *such that* $\zeta_R^{<}(s) = P_p\left(p^{-s}\right)/Q_p\left(p^{-s}\right)$*. The polynomials* P_p, Q_p *can be chosen to have bounded degree as* p *varies. The local Euler factors satisfy functional equations.*

The functional equation mentioned in the theorem is proved in [27]; also see Chapter 4 of [13]. A corollary of this theorem is that the asymptotic behavior of the function $s_R^{<}(B)$ is of the form $c_R^{<} B^{\alpha_R^{<}} (\log B)^{b_R^{<}-1}$ as $B \to \infty$. Here, $b_R^{<}$ is the order of pole of $\zeta_R^{<}(s)$ at $s = \alpha_R^{<}$. It is known that $b_R^{<} \geq 1$. It is a fundamental problem in the subject to relate the numbers $\alpha_R^{<}, b_R^{<}, c_R^{<} \in \mathbb{R}$ to structure of R.

The paper [14] introduced a p-adic formalism to study the local Euler factors $\zeta_R^{<}(s)$. Fix a $\mathbb{Z}$-basis for R and identify R with $\mathbb{Z}^d$. The multiplication in R is given by a bi-additive map

$$\beta : \mathbb{Z}^d \times \mathbb{Z}^d \to \mathbb{Z}^d$$

which extends to a bi-additive map

$$\beta_p : \mathbb{Z}_p^d \times \mathbb{Z}_p^d \to \mathbb{Z}_p^d$$

giving $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ the structure of a $\mathbb{Z}_p$-algebra.

Definition 2. Let $\mathcal{M}_p(\beta)$ be the subset of the set of $d \times d$ lower triangular matrices M with entries in $\mathbb{Z}_p$ such that if the rows of $M = (x_{ij})_{1 \leq i,j \leq d}$ are denoted by $v_1, \ldots, v_d$, then for for all i, j satisfying $1 \leq i, j \leq d$, there are p-adic integers $c_{ij}^1, \ldots, c_{ij}^d$ such that

$$\beta(v_i, v_j) = \sum_{k=1}^{d} c_{ij}^k v_k.$$

Let dM be the normalized additive Haar measure on $\mathrm{T}_d(\mathbb{Z}_p)$, the set of $n \times n$ lower triangular matrices with entries in $\mathbb{Z}_p$. Proposition 3.1 of [14] says:

$$\zeta_{R,p}^{<}(s) = \left(1 - p^{-1}\right)^{-d} \int_{\mathcal{M}_p(\beta)} |x_{11}|^{s-d} |x_{22}|^{s-d+1} \cdots |x_{dd}|^{s-1}\, dM. \tag{2}$$

Most of the statements of Theorem 7 are proved using this p-adic formulation. The integral appearing in (2) is an example of a *cone integral*. The beauty of Equation (2) is that it allows us to express the number of subrings of a given index in terms of volumes of certain p-adic domains.

Let $D = (f_0, g_0, f_1, g_1, \cdots, f_l, g_l)$ be polynomials in the variables $x_1, \ldots, x_m$ with rational coefficients. We call D the *cone integral data*. For a prime number p, we define

$$\mathcal{M}_p(D) := \{x \in \mathbb{Z}_p^m \mid v_p(f_i(x)) \leq v_p(g_i(x)), \text{ for all } 1 \leq i \leq l\},$$

and we define the *cone integral* associated to the cone integral data D by

$$Z_D(s,p) = \int_{\mathcal{M}_p(D)} |f_0(x)|_p^s |g_0(x)|_p \, dx$$

with dx is the normalized additive Haar measure. The study of such integrals in special cases was started by Igusa [16,17]. Igusa's original method was based on the resolution of singularities. Igusa's approach was generalized by Denef [7] and du Sautoy and Grunewald [10]. Denef [7] also introduced the use of elimination of quantifiers in $\mathbb{Q}_p$ as an alternative approach. For surveys on cone integrals and their applications to zeta functions of groups and rings, as well as references and examples, see [11,13,28]. In general, calculating cone integrals is difficult and requires explicit desingularizations of highly singular varieties. For a 'simple' example, see [12].

There is a modification of this formalism to treat subrings with identity. Again, let R be a ring with identity whose additive group is isomorphic to $\mathbb{Z}^d$ and for simplicity assume that the identity of R is sent to $(1, 1, \ldots, 1)$ under this isomorphism. For $k \in \mathbb{N}$, let

$$a_R^{1,<}(k) := |\{S \text{ subring with identity of } R \mid [\, R : S] = k\}|.$$

Now define the unitary subring zeta function of R by

$$\zeta_R^{1,<}(s) := \sum_{k=1}^{\infty} \frac{a_R^{1,<}(k)}{k^s}.$$

As before, we have an Euler product expansion

$$\zeta_R^{1,<}(s) = \prod_p \zeta_{R,p}^{1,<}(s).$$

We let

$$s_R^{1,<}(B) := \sum_{k \le B} a_R^{1,<}(k) = \left|\left\{S \text{ unitary subring of } R \mid [\, R : S] \le B\right\}\right|.$$

Again suppose after identifying R with $\mathbb{Z}^d$, the multiplication on R is given by a bi-additive map

$$\beta : \mathbb{Z}^d \times \mathbb{Z}^d \to \mathbb{Z}^d$$

which extends to a bi-linear map

$$\beta_p : \mathbb{Z}_p^d \times \mathbb{Z}_p^d \to \mathbb{Z}_p^d.$$

Definition 3. Let $\mathcal{M}_p^1(\beta)$ be the subset of $\mathcal{M}_p(\beta)$ whose rows generate a unitary subring.

Then it is not hard to see that

$$\zeta_{R,p}^{1,<}(s) = \left(1 - p^{-1}\right)^{-d} \int_{\mathcal{M}_p^1(\beta)} |x_{11}|^{s-d} |x_{22}|^{s-d+1} \cdots |x_{dd}|^{s-1} \, dM. \tag{3}$$

This integral too is a cone integral as we will see in section 'The proof of Theorems 1 and 2'. As a result, the asymptotic behavior of $s_R^{<}(B)$ is of the form $c_R^{<} B^{\alpha_R^{<}} (\log B)^{b_R^{<}-1}$ as $B \to \infty$. Again, we use the expression (3) to write the number of unitary subrings of a given index in terms of volumes of certain p-adic sets.

In our problems of interest, the ring R is a product of rings of integers of number fields. The two usual methods to study the cone integrals coming from subring zeta functions are resolution of singularities and elimination of quantifiers. Neither of these methods, however, can be applied in any obvious fashion to the problem of counting subrings of such R. This is due to the fact that our cone integrals are too complicated (see sections 'Orders of $\mathbb{Z}^4$' and 'Orders of $\mathbb{Z}^5$'). In general, there is no effective algorithm to eliminate quantifiers for a complicated p-adic domain, and resolution of singularities, while in principle computationally tractable, is dreadful for domains of the type considered here. For example, the domain needed to study $\mathbb{Z}^d$ would involve about d^3 inequalities of the form $v_p(f(\underline{x})) \leq v_p(g(\underline{x}))$ with $\underline{x}$ a vector of variables of length about d^2, and f, g ranging over polynomials with integer coefficients of degrees 2 to d.

In this paper, inspired by [26], we propose a different approach. So far as the determination of the fundamental quantities $\alpha_R^<, b_R^<$ is concerned, we do not need explicit computations of the local integrals. Instead, in favorable circumstances such as those under consideration here, we can accomplish this by computing the first two terms of the Euler factors and estimating the rest of the terms. It is precisely for this reason that our method can be applied to more cases that what was treated in the earlier papers [6,19,24]. Here, the difficulty lies in estimating volumes of certain p-adic sets that arise in the split situation of $\mathbb{Z}^d$, see section 'Orders of $\mathbb{Z}^4$', 'Orders of $\mathbb{Z}^5$', and 'Orders of $\mathbb{Z}^d$ for $d > 5$'. Once this has been accomplished, we will use the results of section 'Application to some volume computations' to show that the volume estimates obtained for the $\mathbb{Z}^n$ setting automatically extend to an arbitrary R of the sort considered here.

Organization of the paper

The rest of the paper is organized as follows. In section 'Geometry and p-adic integrals', we recall results by Denef [8], and use them to prove Theorem 8. We prove Theorem 3 in section 'The proof of Theorem 3', using the outline explained in section 'Outline of the proof of Theorem 3'. Section 'Tauberian theorem' contains the statements of the Tauberian theorems we use in this work. We discuss the values of r_2 in section 'Some remarks on r_2'. The proof of Theorem 6 is presented in section 'The proof of Theorem 6'. The outline of the proof is sketched in section 'Outline of the proof of Theorem 6' and details are postponed to later sections. In section 'General facts about volumes', we collect several lemmas used in estimating volumes. Section 'Orders of $\mathbb{Z}^3$' contains the treatment of the simple case of $\mathbb{Z}^3$. We include this simple case to illustrate the method. In sections 'Orders of $\mathbb{Z}^4$' and 'Orders of $\mathbb{Z}^5$', we give bounds for the volumes of our domains for $n = 4$ and $n = 5$, respectively. These bounds are then used in Sections 'Counting orders of $\mathbb{Z}^4$' and' Counting orders of $\mathbb{Z}^5$' to establish Theorems 12, 13, and 14 which imply the first part of Theorem 6. The proof of the second part of Theorem 6 is presented in section 'Orders of $\mathbb{Z}^d$ for $d > 5$'. The paper ends with the proof of Theorem 2 in section 'The proof of Theorems 1 and 2'.

Notation

In this paper, a ring R is an additive group with a bi-additive multiplication such that the underlying additive group is finitely generated. We write $S \leq R$ if S is a subring of R. The number $[R : S]$ is defined to be the index of S in R as an additive subgroup. Throughout this paper, p is a prime number. When p is used as the index of a sum or product, we will always understand that it ranges through the primes. The symbols $\mathbb{Q}_p$ and $\mathbb{Z}_p$ are the field of p-adic numbers and its ring of integers, respectively. We let U_p denote the group of units of $\mathbb{Z}_p$. We normalize the additive Haar measure on $\mathbb{Q}_p$ such that $\mathrm{vol}(\mathbb{Z}_p) = 1$, and the volume of a subset of $\mathbb{Q}_p$ is always with respect to this measure. For example, if $P(x)$ is a statement about a p-adic number x, the volume of $x \in \mathbb{Q}_p$ such that $P(x)$ means the normalized Haar measure of the set $\{x \in \mathbb{Q}_p; P(x)\}$. The measure on $\mathbb{Q}_p^r$ for any $r > 0$ is normalized similarly. The function $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ is the p-adic valuation. If $f : S \to \mathbb{C}$ and $g : S \to \mathbb{R}_+$ are functions defined on a set S to the set of positive real numbers $\mathbb{R}_+$ and $\mathbb{C}$, respectively, the notation $f(x) = O(g(x))$ means there is a constant $C > 0$ such that for all $x \in S$ we have $|f(x)| \leq Cg(x)$; this is also sometimes denoted by $f(x) \ll g(x)$. If S, T are sets, and $f : S \to \mathbb{C}$ and $g : S \times T \to \mathbb{R}_+$ are functions, the notation $f(x) = O_y(g(x, y))$ means that for every $y \in T$, there is a constant $C(y) > 0$ such that for every $x \in S$ we have $|f(x)| \leq C(y)g(x, y)$.

If $f(x), g(x) : \mathbb{R}_+ \to \mathbb{R}_+$, we say that $f(x) \sim g(x)$ as $x \to +\infty$ if $\lim_{x\to+\infty} f(x)/g(x) = 1$. For a complex number s, $\Re(s)$, usually denoted by σ, is the real part of s. We will, without explicit mention, repeatedly use the fact that $\sum_{p\,\text{prime}} p^{a-bs}$, with a, b real numbers, converges for $\Re(s) > (a + 1)/b$. The collection of $n \times n$ matrices with entries in a ring R is denoted by $\mathrm{M}_n(R)$. The set of lower triangular matrices in $\mathrm{M}_n(R)$ is written $\mathrm{T}_n(R)$. A finite extension $K/\mathbb{Q}$ is called a number field, and its absolute discriminant is denoted by $\mathrm{disc}_{\mathrm{K}}$. The ring of integers of K is written $\mathcal{O}_K$. A subring with identity of $\mathcal{O}_K$ which is a $\mathbb{Z}$-module of rank equal to the $\mathbb{Z}$-rank of $\mathcal{O}_K$ is called an order. We write $\zeta(s)$ for the Riemann zeta function. If ψ is a property of integers, and f an arithmetic function, $\sum_{p\ \psi} f(p)$ means the sum of the values of f over all prime numbers p which satisfy ψ; for example, if S is a set of integers, $\sum_{p\notin S} f(p)$ means the sum is over all those prime numbers which are not in S.

Geometry and *p*-adic integrals

In this section, we study a multivariable version of the Igusa zeta integral following the method of [8] and [10]. We start with some geometric preparation.

Resolutions with good reduction

We recall the the material of Section 2 of [8]. In this section, K is an arbitrary field of characteristic zero, R a discrete valuation subring of K with field of fractions K, P unique maximal ideal, and residue field $\overline{K}$ which we assume to be perfect. Let $f(\underline{X}) \in K[\underline{X}]$, $\underline{X} = (X_1, \cdots, X_m)$ be a nonzero polynomial. Let $\mathcal{X} = \mathit{Spec}\, K[\underline{X}]$, $\tilde{\mathcal{X}} = \mathit{Spec}\, R[\underline{X}]$, $\overline{\mathcal{X}} = \mathit{Spec}\, \overline{K}[\underline{X}]$, and

$$\mathcal{D} = \mathit{Spec}\, \left(K[\underline{X}]\,/(f)\right) \subset \mathcal{X}.$$

A resolution $(\mathcal{Y}, h)$ for f over K consists of a closed integral subscheme $\mathcal{Y}$ of $\mathbb{P}^k_{\mathcal{X}}$ for some k, and the morphism $h : \mathcal{Y} \to \mathcal{X}$ which is the restriction of the projective morphism $\mathbb{P}^k_{\mathcal{X}} \to \mathcal{X}$ such that:

1. $\mathcal{Y}$ is smooth over $\mathit{Spec}\, K$;
2. The restriction $h : \mathcal{Y} \setminus h^{-1}(\mathcal{D}) \to \mathcal{X} \setminus \mathcal{D}$ is an isomorphism;
3. The reduced scheme $(h^{-1}(\mathcal{D}))_{red}$ associated to $h^{-1}(\mathcal{D})$ has only normal crossings.

Let $\mathcal{E}_i$, $i \in T$, be the irreducible components of $(h^{-1}(\mathcal{D}))_{red}$. For $i \in T$, we define N_i to be the multiplicity of $\mathcal{E}_i$ in the divisor of $div\,(f \circ h)$ on $\mathcal{Y}$, and let $\nu_i - 1$ be the multiplicity of $\mathcal{E}_i$ in the divisor of $h^*(dx_1 \wedge \cdots \wedge dx_m)$. We have $N_i, \nu_i \geq 1$ for all $i \in T$.

We think of $\mathbb{P}^k_{\mathcal{X}}$ as an open subscheme of $\mathbb{P}^k_{\tilde{\mathcal{X}}}$. If $\mathcal{Z}$ is a closed subscheme of $\mathbb{P}^k_{\mathcal{X}}$, we define $\tilde{\mathcal{Z}}$ to be the scheme theoretic closure of $\mathcal{Z}$ in $\mathbb{P}^k_{\tilde{\mathcal{X}}}$. We also set $\overline{\mathcal{Z}} = \tilde{\mathcal{Z}} \times_R Spec\,\overline{K}$, and we call it the reduction of $\mathcal{Z}$ mod P.

Let $\tilde{h} : \tilde{\mathcal{Y}} \to \tilde{\mathcal{X}}$ be the restriction to $\tilde{\mathcal{Y}}$ of the projective morphism $\mathbb{P}^k_{\tilde{\mathcal{X}}} \to \tilde{\mathcal{X}}$, and $\bar{h} : \overline{\mathcal{Y}} \to \overline{\mathcal{X}}$ be obtained from $\tilde{h}$ by base extension. We say $(\mathcal{Y}, h)$ has good reduction mod P if the following two conditions are satisfied:

1. $\overline{\mathcal{Y}}$ is smooth over $Spec\,\overline{K}$;
2. $\bar{\mathcal{E}}_i$ is smooth over $Spec\,\overline{K}$, for all $i \in T$, and $\cup_i \bar{\mathcal{E}}_i$ has only normal crossings; and
3. for $i \neq j$, $\bar{\mathcal{E}}_i$ and $\bar{\mathcal{E}}_j$ have no common irreducible components.

Let K' be a field containing K, R' a discrete valuation subring of K' who fraction field is K', and which contains R, with maximal ideal P' containing P, and with perfect residue field. Suppose $(\mathcal{Y}, h)$ be a resolution of f over K as above. Let $\mathcal{Y}' = \mathcal{Y} \times_K Spec\,K'$ and $h' : \mathcal{Y}' \to \mathcal{X}' = Spec\,K'[\underline{X}]$ be obtained from h by base extension. Proposition 2.3 of [8] says that then $(\mathcal{Y}', h')$ is a resolution of f over K'. Moreover, if $(\mathcal{Y}, h)$ is a resolution with good reduction mod P, $(\mathcal{Y}', h')$ has good reduction mod P'.

In the arithmetic case, let F be a number field, and $\mathcal{O}_F$ its ring of integers. Let $f(\underline{X}) \in F[\underline{X}]$, $\underline{X} = (X_1, \cdots, X_m)$. Let $(\mathcal{Y}, h)$ be a resolution for f. For any maximal ideal $\mathfrak{p}$, we consider the discrete valuation ring $\mathcal{O}_{F,\mathfrak{p}}$ with maximal ideal $\mathfrak{p}\mathcal{O}_{F,\mathfrak{p}}$. Note that the field of fractions of $\mathcal{O}_{F,\mathfrak{p}}$ is F. Theorem 2.4 of [8] then states that for almost all $\mathfrak{p}$, $(\mathcal{Y}, h)$ is a resolution with good reduction mod $\mathfrak{p}\mathcal{O}_{F,\mathfrak{p}}$. As a corollary, if $F_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic completion of F, and $\mathcal{O}_{\mathfrak{p}}$ its ring of integers, and by abuse of notation $\mathfrak{p}$ its unique prime ideal, then $(\mathcal{Y}, h)$ is a resolution of f over $F_{\mathfrak{p}}$ with good reduction mod $\mathfrak{p}$ for almost all $\mathfrak{p}$.

Multivariable cone integral

For a finite extension F of $\mathbb{Q}_p$, we let be $\mathcal{O}_F$ its ring of integers, $\mathfrak{p}$ the maximal ideal, $|.|_F$ its normalized absolute value, and v_F the corresponding discrete valuation. Let q be the size of $\overline{F}$, the residue field of F.

Let $f_1, \cdots, f_l$ and $g_1, \cdots, g_l$ be polynomials in the variables $\underline{X} = (X_1, \cdots, X_m)$ with rational coefficients. We denote by $\psi_F(\underline{X})$ the first order formula

$$v_F(f_i(\underline{X})) \leq v_F(g_i(\underline{X})), \quad i = 1, \ldots, l.$$

As before we call the formula $\psi_F(\underline{X})$ a cone condition, and the polynomials f_i, g_i, $1 \leq i \leq l$, the cone data.

We define

$$V_{F,\psi} = \{\underline{x} \in \mathcal{O}_F^m; \psi(\underline{x})\}.$$

If $h_0, h_1, \ldots, h_k$ are polynomials in $\underline{X}$ with rational coefficients, we define the cone integral in k complex variables $\underline{s} = (s_1, \cdots, s_k) \in \mathbb{C}^k$ with respect to ψ by

$$Z_\psi(\underline{s}; F) = \int_{V_{F,\psi}} |h_0(\underline{x})| \cdot |h_1(\underline{x})|^{s_1} \cdots |h_k(\underline{x})|^{s_k} \cdot |d\underline{x}|.$$

Our first goal here is to find an explicit formula for Z_ψ for p outside a finite set of primes. In this section, following the method of [10] closely, we will find an explicit formula for our multivariable cone integral which depends on the numerical invariants of a resolution.

Let $(\mathcal{Y}_{\mathbb{Q}}, h_{\mathbb{Q}})$ be a resolution of the polynomial $\Phi = \prod_i h_i. \prod_j f_j g_j$ over $\mathbb{Q}$, and assume that the prime p is such that $(\mathcal{Y}_{\mathbb{Q}}, h_{\mathbb{Q}})$ has good reduction mod p, and $\Phi \not\equiv 0 \mod p$. Let $(\mathcal{Y}, h)$ be the resolution of Φ over F obtained by base extension. Then $(\mathcal{Y}, h)$ has good reduction mod $\mathfrak{p}$.

Let $a \in \overline{\mathcal{Y}}(\overline{F})$. Since $\overline{\mathcal{Y}}$ is a closed subscheme of $\widetilde{\mathcal{Y}}$, a is a closed point of $\widetilde{\mathcal{Y}}$. Let

$$T_a = \{i \in T, a \in \overline{\mathcal{E}}_i\} = \{i \in T, a \in \widetilde{\mathcal{E}}_i\}.$$

Let $r = |T_a|$ and write $T_a = \{i_1, \cdots, i_r\}$. Then in the local ring $\mathcal{O}_{\widetilde{\mathcal{Y}},a}$, we write

$$\Phi \circ \tilde{h} = u c_1^{N_{i_1}} \ldots c_r^{N_{i_r}}$$

where $c_j \in \mathcal{O}_{\widetilde{\mathcal{Y}},a}$ generates the ideal of $\widetilde{\mathcal{E}}_{i_j}$ and u a unit in $\mathcal{O}_{\widetilde{\mathcal{Y}},a}$. Since f_i, g_i, h_i divide Φ, we can also write

$$f_i \circ \tilde{h} = u(f_i) c_1^{N_{i_1}(f_i)} \ldots c_r^{N_{i_r}(f_i)}$$

$$g_i \circ \tilde{h} = u(g_i) c_1^{N_{i_1}(g_i)} \ldots c_r^{N_{i_r}(g_i)}$$

$$h_i \circ \tilde{h} = u(h_i) c_1^{N_{i_1}(h_i)} \ldots c_r^{N_{i_r}(h_i)}.$$

We define vectors $\underline{w}_j$, $1 \le j \le r$, by

$$\underline{w}_j = (N_{i_j}(h_1), \ldots, N_{i_j}(h_k)) \in \mathbb{N}^k.$$

Define an integral $J_{a,\psi}(\underline{s}, F)$ by the following expression:

$$J_{a,\psi}(\underline{s}; F) = \int_{\theta^{-1}(a) \cap h^{-1}(V_{F,\psi})} |h_0 \circ h| \cdot |h_1 \circ h|^{s_1} \cdots |h_k \circ h|^{s_k} \cdot |h^*(dx_1 \wedge \cdots \wedge dx_m)|.$$

Here, the function θ is defined as follows: Let $H = \{b \in \mathcal{Y}(F), h(b) \in \mathcal{O}_F^m\}$. A point $b \in H \subset \mathcal{Y}(F)$ can be represented by its coordinates $(x_1, \cdots, x_m, y_0, \cdots, y_k) \in F^m \times \mathbb{P}^k_{\mathcal{X}}(F)$ where $(x_1, \cdots, x_m) \in \mathcal{O}_F^m$ and $(y_0, \ldots, y_k)$ are homogeneous coordinates that are chosen to satisfy $\min_i v_F(y_i) = 0$. We define $\theta(b) = (\overline{x_1}, \cdots, \overline{x_m}, \overline{y_0}, \cdots, \overline{y_k}) \in \overline{\mathcal{Y}}(\overline{F})$. The next step is to calculate each integral $J_{a,\psi}$. We have

$$J_{a,\psi}(\underline{s}; F) = \int_{\theta^{-1}(a) \cap h^{-1}(V_{F,\psi})} |c_1|^{\underline{w}_1 \cdot \underline{s} + N_{i_1}(h_0) + v_{i_1} - 1} \cdots |c_r|^{\underline{w}_r \cdot \underline{s} + N_{i_r}(h_0) + v_{i_r} - 1} |dc_1 \wedge \cdots \wedge dc_m|.$$

Since $\bar{c}_1, \ldots, \bar{c}_m$ are in the maximal ideal of $\mathcal{O}_{\overline{\mathcal{Y}},a}$, we have that $c_1(b), \ldots, c_m(b) \in \mathfrak{p}$ for all $b \in \theta^{-1}(a)$, and the map $c : \theta^{-1}(a) \to \mathfrak{p}^m$ given by

$$b \mapsto (c_1(b), \ldots, c_m(b)).$$

is a bijection. Consequently,

$$J_{a,\psi}(\underline{s}; F) = \int_{V'_{F,\psi}} |c_1|^{\underline{w}_1 \cdot \underline{s} + N_{i_1}(h_0) + v_{i_1} - 1} \cdots |c_r|^{\underline{w}_r \cdot \underline{s} + N_{i_r}(h_0) + v_{i_r} - 1} |dc_1 \wedge \cdots \wedge dc_m|$$

where $V'_{F,\psi}$ is the set of all $y = (y_1, \ldots, y_m) \in \mathfrak{p}^m$ such that for each i satisfying $1 \le i \le l$

$$\sum_{j=1}^{r} N_{i_j}(f_i) v_F(y_j) \le \sum_{j=1}^{r} N_{i_j}(g_i) v_F(y_j).$$

Let $\underline{A}_{j,a} = w_j$ and $B_{j,a} = N_{i_j}(h_0) + \nu_{i_j}$ for $1 \le j \le r$ and $\underline{A}_{j,a} = \underline{0}$ and $B_{j,a} = 1$ for $j > r$. Then

$$J_{a,\psi}(\underline{s}; F) = \sum_{(k_1,\ldots,k_m)\in\Lambda} q^{-\sum_{j=1}^m k_j\left(\underline{A}_{j,a}\cdot\underline{s}+B_{j,a}-1\right)} \left(q^{-k_1} - q^{-k_1-1}\right)\ldots\left(q^{-k_m} - q^{-k_m-1}\right)$$

$$= (1-q^{-1})^m \sum_{(k_1,\ldots,k_m)\in\Lambda} q^{-\sum_{j=1}^m k_j\left(\underline{A}_{j,a}\cdot\underline{s}+B_{j,a}\right)},$$

where

$$\Lambda = \left\{ (k_1,\ldots,k_m) \in \mathbb{N}^m; \sum_{j=1}^r N_{i_j}(f_i)k_j \le \sum_{j=1}^r N_{i_j}(g_i)k_j, 1 \le i \le l \right\}.$$

The set Λ is the intersection of $\mathbb{N}^m$ with a rational polyhedral cone C in $\mathbb{R}^m$. Write this cone as a disjoint union of simplicial cones $C_1, \ldots, C_t$ with

$$C_i = \{\alpha_1 v_{i1} + \cdots + \alpha_{m_i} v_{im_i}; \alpha_j \in \mathbb{R}_{>0}, 1 \le j \le m_i\}$$

where $\{v_{i1}, \ldots, v_{im_i}\}$ is a linearly independent set of vectors in $\mathbb{R}^m$.

Then Λ is the disjoint union of the following sets

$$\Lambda_i = \{l_1 v_{i1} + \cdots + l_{m_i} v_{im_i}; l_j \in \mathbb{N}, 1 \le j \le m_i\}.$$

Now $v_{jk} = (q_{jk1}, \ldots, q_{jkm}) \in \mathbb{R}^m_{>0}$ for $1 \le k \le m_j$. Hence

$$J_{a,\psi}(\underline{s}; F) = (1-q^{-1})^m \sum_{i=1}^t \prod_{u=1}^{m_i} \frac{q^{-\underline{A}_{i,u,a}\cdot\underline{s}-B_{i,u,a}}}{1-q^{-\underline{A}_{i,u,a}\cdot\underline{s}-B_{i,u,a}}}$$

with $\underline{A}_{i,u,a} = \sum_{j=1}^m q_{iuj}\underline{A}_{j,a}$ and $B_{i,u,a} = \sum_{j=1}^m q_{iuj}B_{j,a}$.

For each $I \subset T$ define

$$c_{F,I} = \left|\{a \in \overline{\mathcal{Y}}(\overline{F}); a \in \overline{\mathcal{E}}_i \text{if and only if } i \in I\}\right|,$$

and put $\underline{A}_{i,u,I} = \underline{A}_{i,u,a}$ and $B_{i,u,I} = B_{i,u,a}$ for any $a \in \{x \in \overline{\mathcal{Y}}(\overline{F}); x \in \overline{\mathcal{E}}_i \text{if and only if } i \in I\}$.

Clearly,

$$Z_\psi\left(\underline{s}; F\right) = \sum_{a\in\overline{\mathcal{Y}}(\overline{F})} J_{a,\psi}\left(\underline{s}; F\right).$$

Putting everything together

$$Z_\psi\left(\underline{s}; F\right) = \left(1-q^{-1}\right)^m \sum_{I\subset T} c_{F,I} \sum_{i=1}^{t_I} \prod_{u=1}^{m_i} \frac{q^{-\underline{A}_{i,u,I}\cdot\underline{s}-B_{i,u,I}}}{1-q^{-\underline{A}_{i,u,I}\cdot\underline{s}-B_{i,u,I}}}.$$

The absolute convergence of the integral is guaranteed if

$$\underline{A}_{i,u,I}\cdot\Re\underline{s} + B_{i,u,I} > 0$$

for all $I \subset T$, $1 \le i \le t$, and $1 \le u \le m_i$, where

$$\Re\underline{s} = (\Re s_1, \ldots, \Re s_k).$$

We note that the domain of the absolute convergence depends only on the geometry of our data, and not on the particular choice of the field F.

As in [10], we derive another expression for the integral. Set

$$\overline{D_T} = \left\{ (x_1, \ldots, x_t) \in \mathbb{R}^t_{\geq 0}; \sum_{j=1}^{t} N_j(f_i)x_j \leq \sum_{j=1}^{t} N_j(g_i)x_j, 1 \leq i \leq l \right\}$$

where $t = |T|$. This is a closed cone. This cone is a disjoint union of open simplicial pieces called R_k, $0 \leq k \leq w$. We assume that the fundamental region for the lattice points of R_k has no lattice points in its interior. We will assume that $R_0 = (0, \ldots, 0)$ and that $R_1, \ldots, R_q$ are all the open one-dimensional edges of the cone $\overline{D_T}$. Write

$$R_k = \left\{ \alpha \underline{e}_k = \alpha(q_{k1}, \ldots, q_{kt}); \alpha > 0 \right\}.$$

For any $0 \leq k \leq w$, there is a subset $M_k \subset \{1, \ldots, q\}$ such that

$$R_k = \left\{ \sum_{j \in M_k} \alpha_j \underline{e}_j, \forall j \in M_k \right\}.$$

Let $m_k := |M_k| \leq t$. For each $I \subset T$ set

$$D_I = \left\{ (k_1, \ldots, k_t) \in \overline{D_T}; k_i > 0, \forall i \in I, k_i = 0, \forall i \in T \setminus I \right\}$$

$$\Delta_I = D_I \cap \mathbb{N}^t.$$

We also set $\overline{D_T} = \overline{\Delta_T}$. For each $I \subset T$, there is a subset $W_I \subset \{0, \ldots, w\}$ such that

$$D_I = \bigcup_{k \in W_I} R_k.$$

Suppose $a \in \overline{\mathcal{Y}}(\overline{F})$ is such that $a \in \overline{\mathcal{E}}_i$ if and only if $i \in I$. Then we have

$$J_{a,\psi}\left(\underline{s}; F\right) = p^{-(m-|I|)} \int_{V'_F} \prod_{i \in I} |z_i|^{N_i(h_1)s_1 + \cdots + N_i(h_k)s_k + N_i(h_0) + \nu_i - 1} \prod_{i \in I} |dz_i|$$

with V'_F the set of all $(z_i)_{i \in I} \in \mathfrak{p}^{|I|}$ satisfying for $1 \leq j \leq l$

$$\sum_{i \in I} N_i(f_j)\nu_F(z_i) \leq \sum_{i \in I} N_i(g_j)\nu_F(z_i).$$

Then

$$\begin{aligned} J_{a,\psi}\left(\underline{s}; F\right) &= p^{-(m-|I|)}(1-p^{-1})^{|I|} \sum_{(k_1,\ldots,k_t) \in \Delta_I} q^{-\sum_{j=1}^{t} k_j (N_i(h_1)s_1 + \cdots + N_i(h_k)s_k + N_i(h_0) + \nu_i)} \\ &= \sum_{k \in W_I} p^{-(m-|I|)}(1-p^{-1})^{|I|} \sum_{(k_1,\ldots,k_t) \in R_k \cap \mathbb{N}^t} q^{-\sum_{j=1}^{t} k_j (N_j(h_1)s_1 + \cdots + N_j(h_k)s_k + N_j(h_0) + \nu_j)} \end{aligned}$$

as $D_I = \cup_{k \in W_I} R_k$. As

$$R_k \cap \mathbb{N}^t = \left\{ \sum_{j \in M_k} \alpha_j \underline{e}_j; \alpha_j \in \mathbb{N}, \forall j \in M_k \right\}$$

we have

$$J_{a,\psi}\left(\underline{s}; F\right) = \sum_{k \in W_I} p^{-(m-|I|)}(1-p^{-1})^{|I|} \prod_{j \in M_k} \frac{q^{-(\underline{A_j} \cdot \underline{s} + B_j)}}{1 - q^{-(\underline{A_j} \cdot \underline{s} + B_j)}}$$

with

$$\underline{A}_j = \sum_{i=1}^{t} q_{ji}\underline{N}_i$$

$$B_j = \sum_{i=1}^{t} q_{ji}(N_i(h_0) + \nu_i),$$

and

$$\underline{N}_i = (N_i(h_1), \ldots, N_i(h_k)).$$

So if we set $c_{F,k} = c_{F,I}$ and $I_k = I$ if $k \in W_I$, for every non-archimedean local field F where the resolution has good reduction, we have

$$Z_\psi(\underline{s}; F) = \sum_{k=0}^{w} (q-1)^{|I_k|} q^{-m} c_{F,k} \prod_{j \in M_k} \frac{q^{-(\underline{A_j}.\underline{s}+B_j)}}{1 - q^{-(\underline{A_j}.\underline{s}+B_j)}}.$$

In the situation where the resolution is not necessarily of good reduction, following the argument of Proposition 3.3 of [10], one proves that there exists a finite set B_F such that for every $b \in B_F$ there is an associated subset $I_b \subset T$ and an integer e_b such that

$$Z_\psi(\underline{s}; F) = \sum_{b \in B_F} \sum_{k \in W_{I_b}} (q-1)^{|I_b|} q^{-m} \prod_{j \in M_k} \frac{q^{-e_b\left(\underline{A_j}.\underline{s}+B_j\right)}}{1 - q^{-\left(\underline{A_j}.\underline{s}+B_j\right)}}. \tag{4}$$

Application to some volume computations

Let F be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_F$ and $|.|_F$ its normalized absolute value. We fix a uniformizer ϖ_F for F. Let q be the size of the residue field of F. For $\underline{x} = (x_1, \cdots, x_n) \in (F^\times)^n$, and $\underline{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{R}^n$, we define $\nu_F(\underline{x}) = (\nu_F x_1, \ldots, \nu_F x_n)$, and $|\underline{x}|_F^{\underline{\alpha}} = \prod_i |x_i|_F^{\alpha_i}$. We define vol_F and vol_{F^n}, to be the normalized Haar measure on F, and on F^n, respectively. If $\underline{k} = (k_1, \ldots, k_n) \in \mathbb{Z}^n$, and $\alpha \in F$ is nonzero, we set $\alpha^{\underline{k}} = \left(\alpha^{k_1}, \ldots, \alpha^{k_n}\right)$; in particular, $\varpi_F^{\underline{k}} = \left(\varpi_F^{k_1}, \ldots, \varpi_F^{k_n}\right)$.

Let $\underline{X} = (X_1, \cdots, X_n)$ and $\underline{Y} = (Y_1, \cdots, Y_m)$, and let $f_i, g_i \in \mathbb{Z}[\underline{X}; \underline{Y}]$, $1 \le i \le k$, be polynomials. For each $\underline{x} \in \mathcal{O}_F^n$, define a set

$$V_F(\underline{x}) = \{\underline{y} \in \mathcal{O}_F^m; \nu_F(f_i(\underline{x}; \underline{y})) \le \nu_F(g_i(\underline{x}; \underline{y})), 1 \le i \le k\}.$$

We will assume that $V_F(\underline{x})$ is F-*round* in that it is invariant under the action of units of the local field, i.e., $V_F(\underline{x}) = V_F(\underline{x}')$ if $\nu_F(\underline{x}) = \nu_F(\underline{x}')$. With abuse of language, when we say V, we mean the assignment that takes an extension F of $\mathbb{Q}_p$ and an element $\underline{x} \in \mathcal{O}_F^n$, and returns the set $V_F(\underline{x})$. We will call V *round* if for all F, $V_F(\underline{x})$ is F-round.

Definition 4. Let $\underline{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{R}^n$, $\ell \in \mathbb{N}$, and $P \in \mathbb{R}[X_1, \ldots, X_n]$ with positive coefficients. We say V is $(\ell, \underline{\alpha}, P, F)$-narrow, if for all $\underline{x} \in (\mathcal{O}_F \setminus \{0\})^n$ we have

$$vol_{F^m}(V_F(\underline{x})) \le P(\nu_F(\underline{x})) q^{-\ell} |\underline{x}|_F^{\underline{\alpha}}.$$

Now, here is the theorem:

Theorem 8. *Suppose there is* $\underline{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{R}^n$, $\ell \in \mathbb{N}$, $P \in \mathbb{R}[X_1, \ldots, X_n]$ *with positive coefficients, and an infinite set of primes* $\mathcal{P}$ *such that for all* $p \in \mathcal{P}$ *the set* V *is* $(\ell, \underline{\alpha}, P, \mathbb{Q}_p)$*-narrow. Then* V *is* $(\ell, \underline{\alpha}, P, \mathbb{Q}_p)$*-narrow for almost all primes* p.

In the statement of the theorem 'almost all' means all but possibly finitely many.

Proof. Let $F = \mathbb{Q}_p$ for $p \in \mathcal{P}$. In order to prove the theorem, we consider the following integral:

$$Z_V(\underline{s}) = \int_{\mathcal{O}_F^n} vol_{F^m}(V_F(\underline{x}))|\underline{x}|^{\underline{s}}\, dx$$
$$= \left(1-p^{-1}\right)^n \sum_{\underline{k}\in\mathbb{Z}_{\geq 0}^m} vol_{F^m}\left(V_F\left(\underline{\varpi_F^k}\right)\right)p^{-|\underline{k}|}p^{-\underline{k}.\underline{s}}.$$

On the other hand, we write

$$Z_V(\underline{s}) = \int_{\mathcal{O}_F^{m+n};v(f_i(\underline{x};\underline{y}))_F\leq v(g_i(\underline{x};\underline{y}))_F,1\leq i\leq k} |x_1|^{s_1}\dots|x_n|^{s_n}\,|d\underline{x}|\,|d\underline{y}|.$$

This is a multivariable cone integral.

Since the set $\mathcal{P}$ is infinite, we may assume that p is good in the sense of section 'Resolutions with good reduction'. By section 'Multivariable cone integral', we have

$$Z_V(\underline{s}) = \sum_{k=0}^{w}(p-1)^{|I_k|}p^{-m-n}c_{F,k}\prod_{j\in M_k}\frac{p^{-(\underline{A_j}.\underline{s}+B_j)}}{1-p^{-(\underline{A_j}.\underline{s}+B_j)}}$$

with non-negative integer vectors $\underline{A_j}$ and non-negative integers B_j. Regrouping terms gives

$$Z_V(\underline{s}) = \sum_{\underline{k}}p^{-\underline{k}.\underline{s}}\sum_{i=0}^{w}(p-1)^{|I_i|}p^{-m-n}c_{F,i}\left(\prod_{j\in M_i}\sum_{\alpha_j=1}^{+\infty}\right)_{\sum_j\alpha_j\underline{A_j}=\underline{k}} p^{-\alpha_jB_j}$$

where the notation

$$\left(\prod_{j\in M_i}\sum_{\alpha_j=1}^{+\infty}\right)_{\sum_j\alpha_j\underline{A_j}=\underline{k}}$$

means we have only considered those α_j's that satisfy $\sum_j\alpha_j\underline{A_j} = \underline{k}$. Comparing the two expressions for Z_V gives

$$vol_{F^m}\left(V_F\left(\underline{\varpi_F^k}\right)\right) = \left(1-p^{-1}\right)^{-n}p^{|\underline{k}|}\sum_{i=0}^{w}(p-1)^{|I_i|}p^{-m-n}c_{F,i}\left(\prod_{j\in M_i}\sum_{\alpha_j=1}^{+\infty}\right)_{\sum_j\alpha_j\underline{A_j}=\underline{k}} p^{-\alpha_jB_j}$$
$$= \sum_{i=0}^{w}c_{F,i}\left(1-p^{-1}\right)^{-n}p^{|\underline{k}|}(p-1)^{|I_i|}p^{-m-n}\left(\prod_{j\in M_i}\sum_{\alpha_j=1}^{+\infty}\right)_{\sum_j\alpha_j\underline{A_j}=\underline{k}} p^{-\alpha_jB_j}.$$

We note that if $|I_i| > m+n$, then $c_{F,i} = 0$. As a result, we may write

$$vol_{F^m}\left(V_F\left(\underline{\varpi_F^k}\right)\right) = \sum_{i=0}^{w}c_{F,i}\left(1-p^{-1}\right)^{-n}p^{|\underline{k}|}(p-1)^{|I_i|}p^{-m-n}P_{i,\underline{k}}\left(p^{-1}\right)$$

with $P_{i,\underline{k}}(X)$ a polynomial with positive integral coefficients which depends only on i and $\underline{k}$, and not on the choice of the field F. Furthermore, the number of terms of $P_{i,\underline{k}}$ depends on $\underline{k}$ in a polynomial fashion. In particular, there are no cancellations between the terms. These observations imply that V is $(\underline{\alpha},F)$-narrow if and only if for each $i = 0,\dots,w$, we have some polynomial with positive coefficients P such that

$$c_{F,i}\left(1-p^{-1}\right)^{-n}p^{|\underline{k}|}(p-1)^{|I_i|}p^{-m-n}P_{i,\underline{k}}\left(p^{-1}\right) \leq P(k_1,\dots,k_n)p^{-\ell}p^{-\alpha_1k_1-\dots-\alpha_nk_n}.$$

This is true if and only if

$$c_{F,i}p^{|\underline{k}|}p^{|I_i|-m-n}P_{i,\underline{k}}\left(p^{-1}\right) \leq P(k_1,\ldots,k_n)p^{-\ell}p^{-\alpha_1 k_1-\cdots-\alpha_n k_n}.$$

Proposition 4.9 combined with Proposition 4.13 of [10] implies that, after letting $\mathcal{P}$ become larger in $\mathfrak{p}$, this inequality is true if and only if

$$p^{m+n-|I_i|}p^{|\underline{k}|}p^{|I_i|-m-n}P_{i,\underline{k}}\left(p^{-1}\right) \leq P(k_1,\ldots,k_n)p^{-\ell}q^{-\alpha_1 k_1-\cdots-\alpha_n k_n},$$

which is equivalent to

$$p^{|\underline{k}|}P_{i,\underline{k}}\left(p^{-1}\right) \leq P(k_1,\ldots,k_n)p^{-\ell}p^{-\alpha_1 k_1-\cdots-\alpha_n k_n}.$$

Since $\mathfrak{p}$ is infinite, we can let $p \to \infty$, and as a result, an inequality of this nature is valid if and only if it is true for degree reasons. The theorem now follows. □

Remark 5. Here is a variation of the above theorem which may be useful in other contexts. There is a finite set S of primes such that every $p \notin S$ has the following property: If there is $\alpha \in \mathbb{R}^n$, $\ell \in \mathbb{N}$, and $P \in \mathbb{R}[X_1,\ldots,X_n]$ such V is $(\ell,\underline{\alpha},P,F)$-narrow for every F finite extension of $\mathbb{Q}_p$, then for all $q \notin S$, V is $(\ell,\underline{\alpha},E)$-narrow for every E finite extension of $\mathbb{Q}_q$.

The proof of Theorem 3

Tauberian theorem

We will use the Tauberian theorem of [5], Appendix A, in the following form:

Theorem 9. *Let*

$$F(s) = \sum_{n=1}^{\infty}\frac{a_n}{n^s}$$

be a Dirichlet series with an Euler product

$$F(s) = \prod_p F_p(s).$$

Suppose each Euler factor is of the form

$$F_p(s) = 1 + \sum_{l\geq 1}\frac{a_l(p)}{p^{ls}}$$

where $a_1(p) = k$, a positive integer independent of p, and $a_l(p)$ are non-negative real numbers. Suppose there is a δ_0 satisfying $\frac{1}{2} \leq \delta_0 < 1$ such that for $\sigma > \delta_0$, we have

$$\sum_p \sum_{l\geq 2}\frac{a_l(p)}{p^{\sigma}} < +\infty.$$

Then there is a polynomial P of degree $k-1$ such that for all $\epsilon > 0$

$$\sum_{n\leq B} a_n = BP(\log B) + O_\epsilon\left(B^{\delta_0+\epsilon}\right)$$

as $B \to \infty$.

Outline of the proof of Theorem 3

If p is unramified in K, we write

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r,$$

where each $\mathfrak{p}_i$ is a prime ideal in $\mathcal{O}_K$, and let

$$f_i = f(\mathfrak{p}_i/p)$$

denote the residue degree of the prime $\mathfrak{p}_i$.

Then

$$\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p = \prod_i \mathcal{O}_{\mathfrak{p}_i}$$

where $\mathcal{O}_{\mathfrak{p}_i}$ is the ring of integers of the completion of K at the prime $\mathfrak{p}_i$, and the isomorphism class of $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is determined by the multi-set $f_p = \{f_1, \cdots, f_r\}$, called the *type* of p. The type of a prime is always a partition of n. We typically write the type of an unramified prime p in the form $f_p = 1^v 2^w r_1^{e_1} \cdots r_k^{e_k}$, where $1 < 2 < r_1 < \cdots < r_k$ are the distinct residue degrees, and $v, w, e_1, \cdots, e_k$ are the number of times each of these appears.

The starting point of the proof of the theorem is the following proposition:

Proposition 1. *If p is an unramified prime of type $f_p = 1^v 2^w r_1^{e_1} \cdots r_k^{e_k}$, then*

$$a_1(p) = w + \binom{v}{2};$$

in particular, $a_1(p)$ depends only on the type f_p.

We will present the proof of this proposition in section 'Proof of Proposition 1'. Given a partition f as above, we let

$$a(f) = w + \binom{v}{2}.$$

Then we observe that the condition that p has type $1^u 2^w r_1^{e_1} \cdots r_k^{e_k}$ is Chebotarev condition in $G = \mathrm{Gal}\,(E/\mathbb{Q})$ in the sense that there are a number of conjugacy classes $\mathcal{C}_i \subset G$, $1 \leq i \leq t$, such that p has type $1^u 2^w r_1^{e_1} \cdots r_k^{e_k}$ if and only if

$$\left(\frac{E/\mathbb{Q}}{p}\right) = \mathcal{C}_i$$

for some i. Here, $\left(\frac{E/\mathbb{Q}}{p}\right)$ is the Frobenius conjugacy class of p in G. Next, we use the following fact:

Proposition 2. *Let L/K be a Galois extension of number fields with Galois group $H = Gal\,(L/K)$. Let $\mathcal{C} \subset H$ be a conjugacy class and define*

$$F_{\mathcal{C}}(s) = \prod_{\substack{p \text{ unramified} \\ \left(\frac{L/K}{p}\right) = C}} (1 - N(p)^{-s})^{-1}.$$

Then $F_{\mathcal{C}}(s)$ converges absolutely for $\Re s > 1$. Furthermore, $F_{\mathcal{C}}(s)^{|H|}$ has an analytic continuation to a meromorphic function on an open set containing $\Re s \geq 1$ with a unique pole of order $|\mathcal{C}|$ at $s = 1$.

We will present the proof of this proposition in section 'Proof of Proposition 2'. Now, suppose a partition f of n is given. On the one hand, f can be type of a prime p, and on the other hand, p determines a conjugacy class in S_n. It is a well-known fact that if p has type f in $K/\mathbb{Q}$, then $\left(\frac{E/\mathbb{Q}}{p}\right)$ has cycle type f. Given a type f, we define $b(f)$ be the number of elements of G of cycle type f in S_n. Combining everything done so far, one concludes that the function $f(s)$ in the statement of Theorem 3 has a pole at $s = 1$ of order

$$r := \frac{1}{|G|} \sum_{f \text{type}} a(f) b(f). \tag{5}$$

We finally have the following statement:

Lemma 1 (B. Srinivasan)**.** *We have* $r = r_2$.

Proof of Lemma. We define a function α on G as follows. If g is of cycle decomposition type f, we set $\alpha(g) = a(f)$. We note that the expression on the right is equal to $\langle \alpha, \psi \rangle$ where ψ is the trivial character of G, and $\langle , \rangle$ is the inner product on the space of class functions of G. The function α is character of the permutation representation π of G on the set of 2-element subsets of $\{1, 2, \ldots, n\}$. In fact, if g is of type f as above, then it is clear that it fixes $\binom{u}{2} + w$ 2-element sets. Then the expression on the right-hand side of (5) is equal to the multiplicity of the trivial representation in π. For every orbit of G on the set of 2-element subsets of $\{1, 2, \ldots, n\}$, we get a copy of the trivial representation in π, and these are the only copies of the trivial representation in π. It is easily seen that if G is transitive the number of such orbits is equal to r_2. $\square$

Theorem 3 now follows from a standard Tauberian argument.

Proof of Proposition 1

We first give an overview of the proof of Proposition 1. A result of [14] shows that determining $a_1(p)$ is equivalent to a counting problem about certain lower-triangular matrices. By Lemma 5.18 of [3] $\mathcal{O}_p := \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is a $\mathbb{Z}_p$-module of rank n. By choosing a special type of basis for $\mathcal{O}_p$ and then applying elementary row operations, the lower-triangular matrices we consider will be of a relatively simple form. We then break up the overall computation of $a_1(p)$ into a few parts depending on the type of p. The proof of Proposition 1 depends on the following lemmas.

Lemma 2. *Let $L/\mathbb{Q}_p$ be an extension of degree n. If $n > 2$, the ring of integers $\mathcal{O}_L$ of L does not have any multiplicatively closed sublattices of index p that are $\mathbb{Z}_p$ modules of rank n.*

This result shows that in order to determine $a_1(p)$ in general, we need only determine primes of a restricted type.

Lemma 3. *Let p be a prime of type* $f_p = 1^v 2^w r_1^{e_1} \cdots r_k^{e_k}$, *and let q be a prime of type* $f_q = 1^v 2^w$. *Then* $a_1(p) = a_1(q)$.

We will determine $a_1(p)$ for primes of this type by considering primes of type 1^v and primes of type 2^w separately. The next lemma follows directly from [19] Proposition 1.1.

Lemma 4. *Let p be a prime of type* $f_p = 1^v$. *Then* $a_1(p) = \binom{v}{2}$.

Lemma 5. *Let p be a prime of type* $f_p = 2^w$. *Then* $a_1(p) = w$.

The proof of Proposition 1 will follow from combining these results in the following way.

Lemma 6. *Let p be a prime of type* $f_p = 1^v 2^w$. *Then* $a_1(p) = \binom{v}{2} + w$.

We now explain how to interpret $a_1(p)$ in terms of a counting problem about lower-triangular matrices. The first observation is that $a_1(p)$ depends only on $\mathcal{O}_p$ and not on K. We choose any ordered basis of this ring, $\{v_1, \ldots, v_n\}$ and represent a subring L of $\mathcal{O}_p$ by a matrix M where the ith column corresponds to v_i and L is generated by the rows of M. The entries of this matrix are in $\mathbb{Z}_p$. By elementary linear algebra, a version of Gauss-Jordan elimination over $\mathbb{Z}_p$, we are free to suppose that M is lower triangular. Multiplying a row of M by a unit in $\mathbb{Z}_p$ does not change the subring generated by M. Therefore, we may suppose that the (i, i) entry of M is equal to p^{k_i} for some $k_i \geq 0$.

Let $\mathcal{M}(p)$ denote the set of all lower triangular matrices whose rows generate a subring of $\mathcal{O}_p$ with respect to this ordered basis. We can now present a slight modification of a proposition of Grunewald, Segal and Smith [14].

Proposition 3. *For every prime p,*

$$\eta_{K,p}(s) = \left(1 - p^{-1}\right)^{-n} \int_{M \in \mathcal{M}(p)} |x_{11}|^{s-n} |x_{22}|^{s-(n-1)} \cdots |x_{nn}|^{s-1} |dv|,$$

where $|dv|$ *is the additive Haar measure of the p-adic lower triangular matrices.*

The index of a subring $L \subseteq \mathcal{O}_p$ is the determinant of any matrix $M \in \mathcal{M}(p)$ generating L. By definition, $a_1(p)$ is equal to the p^{-s} coefficient of the integral in this proposition. We therefore need only consider matrices $M \in \mathcal{M}(p)$ where exactly one x_{ii} is equal to p and all others are equal to 1.

Suppose the rows of M generate a subring of $\mathcal{O}_p$ of index p and suppose that $x_{jj} = 1$ for some j. By adding multiples of the jth row of M to its other rows, we can set each of the nondiagonal entries in column j to 0 without changing the subring generated by this matrix. In fact, by applying a version of Gauss-Jordan elimination, we can simultaneously accomplish this for each column which has its diagonal entry equal to 1. This gives a matrix that is diagonal except for a single column that may have nonzero entries below the diagonal. We give an example below:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & p & 0 & 0 \\ 0 & 0 & a_1 & 1 & 0 \\ 0 & 0 & a_2 & 0 & 1 \end{pmatrix}.$$

Suppose the rows of M generate a subring of $\mathcal{O}_p$ of index p, $x_{jj} = p$ for some j, and every other column of M has a single 1 on the diagonal and is 0 otherwise. Let $\{a_0, a_1, a_2, \ldots, a_{p-1}\}$ be some choice of representatives for $\mathbb{Z}_p/p\mathbb{Z}_p$ with $a_0 = 0$ and $a_1 = 1$. By adding multiples of row j to the rows below it, we may suppose that the entries $x_{j+1,j}, x_{j+2,j}, \ldots, x_{n,j}$ are all elements of $\{a_0, \ldots, a_{p-1}\}$. These representatives are uniquely defined by the subring, but the elements of a matrix generating this subring can be changed by an arbitrary element of $p\mathbb{Z}_p$. We note that the normalized volume of $p\mathbb{Z}_p$ is p^{-1}.

This reduction gives a map from subrings of $\mathcal{O}_p$ of index p given by a matrix M with $x_{jj} = p$ and all other diagonal entries equal to 1 to tuples $\left(x_{j+1,j}, x_{j+2,j}, \ldots, x_{n,j}\right)$ where each $x_{i,j} \in \{a_0, \ldots, a_{p-1}\}$. Let $a_1(p,j)$ be the size of the image of this map. In the case $j = n$, if the matrix M with diagonal entries all equal to 1 except for $x_{n,n} = p$ and all other entries equal to 0 generates a subring of $\mathcal{O}_p$ of index p, then we define $a_1(p,n) = 1$. Otherwise, $a_1(p,n) = 0$. This description along with Proposition 3 shows the following.

Lemma 7. *We have* $a_1(p) = \sum_{j=1}^{n} a_1(p,j)$.

The particular basis that we choose for $\mathcal{O}_p$ has a major effect on the multiplication of rows of the matrix generating a subring. Our next goal is to pick a convenient basis for this module.

Suppose that p is an unramified prime of type $f_p = 1^v 2^w r_1^{e_1} \cdots r_k^{e_k}$ where the r_i are distinct and greater than 2. Each residue degree r_i that occurs contributes r_i basis elements. We choose these basis elements for $\mathcal{O}_p/f\mathcal{O}_p$ to be $1, y, y^2, \ldots, y^{r_i-1}$, where $f(y)$ is an irreducible polynomial of degree r_i over $\mathbb{Z}_p$. We get e_i such groups of r_i basis elements for each r_i, including w blocks of two basis elements $\{1, y\}$ coming from primes of residue degree 2, and v basis elements $\{1\}$ corresponding to primes of residue degree 1. We choose these basis elements to be orthogonal to each other unless they correspond to the same irreducible polynomial.

The ordering of the basis elements has a large effect on the form of the lower triangular matrices in $\mathcal{M}(p)$. We order this basis so that elements corresponding to a single irreducible polynomial are given left to right by increasing powers of y. The e_i sets of r_i columns corresponding to the primes of residue degree r_i are ordered so that they occur in adjacent blocks. We order these groups of e_i blocks of r_i columns from left to right by decreasing values of r_i, except that we switch the positions of the block of v columns corresponding to primes of residue degree 1, and the w pairs of columns corresponding to primes of residue degree 2. We give an example for a lower triangular matrix corresponding to a prime of type $1^2 2^1 3^1$. The first three columns correspond to basis elements corresponding to an irreducible cubic, followed by two columns corresponding to linear polynomials, and finally by a pair of columns from an irreducible quadratic. In the picture below, variable names are chosen to emphasize the grouping of columns:

$$\begin{pmatrix} a_{1,1} & 0 & 0 & 0 & 0 & 0 & 0 \\ a_{2,1} & a_{2,2} & 0 & 0 & 0 & 0 & 0 \\ a_{3,1} & a_{3,2} & a_{3,3} & 0 & 0 & 0 & 0 \\ a_{4,1} & a_{4,2} & a_{4,3} & b_{4,4} & 0 & 0 & 0 \\ a_{5,1} & a_{5,2} & a_{5,3} & b_{5,4} & b_{5,5} & 0 & 0 \\ a_{6,1} & a_{6,2} & a_{6,3} & b_{6,4} & b_{6,5} & c_{6,6} & 0 \\ a_{7,1} & a_{7,2} & a_{7,3} & b_{7,4} & b_{7,5} & c_{7,6} & c_{7,7} \end{pmatrix}.$$

We now briefly explain how to take the product of two rows of such a matrix. A row vector corresponds to a linear combination of basis elements. We can take two vectors, take the product of the corresponding elements in $\mathcal{O}_p$ and then express the result as a linear combination of our chosen basis. We denote the product corresponding to rows v and w by $v \circ w$.

We now give the proof of Lemma 2 on the non-existence of certain kinds of multiplicatively closed sublattices.

Proof of Lemma 2. Let R be a multiplicatively closed sublattice of $\mathcal{O}_L$ of index p. Then clearly $p\mathcal{O}_L \subset R$, and consequently

$$p\mathcal{O}_L \subset R \subset \mathcal{O}_L.$$

This means $(R/p\mathcal{O}_L) \subset (\mathcal{O}_L/p\mathcal{O}_L)$. Now, $\mathcal{O}_L/p\mathcal{O}_L$ is a field of order p^n, and $R/p\mathcal{O}_L$ is a subring, not necessarily with a multiplicative identity, of $\mathcal{O}_L/p\mathcal{O}_L$. It is also clear that $R/p\mathcal{O}_L$ is multiplicatively closed. Any multiplicatively closed subset of a finite field does contain the identity element because the multiplicative group of the field is cyclic, so $R/p\mathcal{O}_L$ is also a field.

Since the index is of R in $\mathcal{O}_L$ is p the number of elements of $R/p\mathcal{O}_L$ is p^{n-1}. Thus, if $\mathbb{F}_{p^k}$ is the finite field with p^k elements, we have $\mathbb{F}_{p^{n-1}} \subset \mathbb{F}_{p^n}$. This implies either $n-1=0$ or $n-1$ divides n. In the first case, we get $n=1$ and in the second case, we get $n=2$. Any larger value of n gives a contradiction. □

Corollary 1. *Let p be a prime of type $f_p = r$ with $r \geq 3$. Then $a_1(p) = 0$.*

These previous two lemmas allow us to compute $a_1(p)$ by considering a much smaller class of lower triangular matrices.

Proof of Lemma 3. We choose the ordered basis of $\mathcal{O}_p$ described above. Suppose that column j corresponds to a basis element coming from a prime of residue degree $k > 2$. We claim that the diagonal element of this column must be equal to 1.

We argue by contradiction. Suppose that $x_{jj} = p$. By row-reducing, we may suppose that the only nonzero elements of this matrix off the diagonal are in column j. Basis elements that do not correspond to the same irreducible polynomial are orthogonal. Suppose that the columns corresponding to the same irreducible polynomial as the basis element of column j are labeled by $c_1, \ldots, c_k$ and let $v_1, \ldots, v_k$ be the rows containing the diagonal entries of these columns. The only nonzero entries of the vector $v_i \circ v_j$ are in positions corresponding to the columns $c_1, \ldots, c_k$. Therefore, $v_i \circ v_j$ is a linear combination of the rows $v_1, \ldots, v_k$. Taking the span of these rows and projecting onto the coordinates corresponding to the columns $c_1, \ldots, c_k$ gives a multiplicatively closed sublattice of a ring corresponding to a degree k extension of $\mathbb{Q}_p$, which is impossible by the argument of Lemma 2.

Therefore, every column corresponding to a basis element coming from a prime of residue degree greater than 2 has its diagonal entry equal to 1 and does not contribute to $a_1(p)$. □

Proof of Lemma 5. A subring of $\mathcal{O}_p$ of index p is generated by a lower triangular matrix M with exactly one diagonal element equal to p and all others equal to 0. We choose the basis of $\mathcal{O}_p$ so that columns occur in pairs with each pair corresponding to two basis elements $\{1, y\}$ of $\mathcal{O}_p/f\mathcal{O}_p$ where $f(y)$ is an irreducible quadratic polynomial over $\mathbb{F}_p$ and the column corresponding to 1 occurs first. When $p \neq 2$, we can choose $f(y) = y^2 - b$ with b a positive integer which is not a square modulo p. We focus on this case but note that for $p = 2$, we can take $f(y) = y^2 + y + 1$ and the rest of the argument is similar. Basis elements occurring in distinct pairs are orthogonal to each other.

We will first show that it is not possible that the column with diagonal entry p corresponds to a basis element 1 for some quadratic polynomial. Suppose that it is and let the row which contains this diagonal element be v_1. Let v_2 be the row which has diagonal element in the column corresponding to the basis element y for the same polynomial. Suppose the entry in row v_2 in the column with diagonal entry p is $a \in \mathbb{Z}_p$.

We will now give a first example of an argument that will be important throughout the rest of this section. Suppose M spans a sublattice of index p and has diagonal entries equal to 1 except for a single column in which the corresponding entry is p. We note that all vectors in the lattice spanned by M that are zero except in this entry must lie in $p\mathbb{Z}_p$ since otherwise we could row reduce M and see that the index of this lattice is actually 1. We will use this fact to show that certain columns cannot have the single diagonal entry equal to p.

We see that $v_2 \circ v_2$ has two nonzero entries: $2a$ in the column corresponding to y and a $b + a^2$ corresponding to 1, since y^2 is b modulo $f(y)$. Since M generates a multiplicatively closed sublattice, and all other entries in the column with diagonal entry in the row v_2 are 0, and so $v_2 \circ v_2 - 2av_2$ must be in the row span of v_1. So there must exist some $\alpha_1 \in \mathbb{Z}_p$ such that

$$p\alpha_1 = b + a^2 - 2a^2 = b - a^2.$$

This implies that $b - a^2 \in p\mathbb{Z}_p$, contradicting the fact that b is a nonsquare modulo p. Therefore, we may suppose that for each column corresponding to 1 for a quadratic polynomial, the diagonal entry is 1.

There are w columns which correspond to basis elements y for distinct irreducible quadratic polynomials. We will show that if the diagonal element of such a column is equal to p then all other entries of this column are in $p\mathbb{Z}_p$. Applying elementary row operations together with Lemma 7 completes the proof.

We suppose that row v_1 has its diagonal entry equal to p and that this column corresponds to a basis element y for some irreducible quadratic polynomial. Let v_2 denote the row with diagonal entry corresponding to the basis element 1 for the same quadratic polynomial. Note that v_2 is above v_1 in this matrix and has a single nonzero entry equal to 1. We will show that it is not possible for there to be a row u with an entry that is a unit in the column with diagonal entry p.

Suppose that there is such a row with an entry $a \in U_p$ in this column and consider $u \circ v_1$. This has a single nonzero entry equal to a in the column corresponding to the diagonal entry p. The argument above shows that such a matrix actually generates $\mathcal{O}_p$ and not a subring of index p, which is a contradiction. We have shown that there are no units in the column with diagonal entry p, completing the proof. □

Proof of Lemma 6. We continue with the notation of the previous proof. Again, we consider $p \neq 2$ and note that when $p = 2$ we choose $f(y) = y^2 + y + 1$ for our irreducible quadratic polynomials and the argument is very similar.

We choose the basis elements of $\mathcal{O}_p$ so that the first v columns correspond to primes of residue degree 1 and the last $2w$ columns occur in pairs and correspond to primes of residue degree 2. The proof of the previous lemma shows that matrices with diagonal entry equal to p in a column corresponding to a prime of residue degree 2 contribute w to $a_1(p)$. We now focus only on the entries of the columns of this matrix which correspond to primes of residue degree 1.

Suppose $x_{jj} = p$ and that this column corresponds to a prime of residue degree 1. Since L is a subring and not just a multiplicative sublattice, it must contain the identity element of $\mathcal{O}_p$, and we see that there must be some entry in this column that is a unit. In fact, we will show that there must be a unique entry in this column that is a unit. Each of the $v - j$ rows directly below this diagonal entry can contain any unit in $1 + p\mathbb{Z}_p$, but no other units can occur. Applying Lemma 7 shows that $a_1(p) = w + \sum_{j=1}^{v}(v - j) = w + \binom{v}{2}$, completing the proof.

We first note that we cannot have two units in rows corresponding to primes of degree 1 in the column with diagonal entry equal to p. If we did, taking $v_1 \circ v_2$ for these two rows would give a vector with a single nonzero entry which is a unit in the column with diagonal entry p. This is a contradiction.

Suppose there is a row with diagonal entry corresponding to an irreducible quadratic polynomial which has a unit entry in the column with diagonal entry p. Let v_1 be the row corresponding to the basis element 1 for this polynomial and v_2 be the row corresponding to the basis element y. Suppose the entry in the column with diagonal entry p is a in row v_1 and c in row v_2. By assumption, at least one of a, c is a unit. We show that this is a contradiction.

We see that $v_1 \circ v_1 - v_1$ has an entry of $a^2 - a$ in the column with diagonal entry p and every other entry of this vector is zero. So either $a \in p\mathbb{Z}_p$ or $a \in 1 + p\mathbb{Z}_p$. We see that $v_2 \circ v_2 - bv_1$ has an entry $c^2 - ab$ in the column with diagonal entry p and every other entry is zero. If $a \in 1 + p\mathbb{Z}_p$ then since b is not a square modulo p, we get a contradiction. If $a \in p\mathbb{Z}_p$, then we have $c^2 \in p\mathbb{Z}_p$, which is also a contradiction. $\square$

Combining Lemma 3 and Lemma 6 completes the proof of Proposition 1.

Proof of Proposition 2

To fix notation, we give a quick review of basic class field theory [25]. Let K be a number field, and let J_K be the free group generated by the finite primes of K. There is a natural map $\iota : K^\times \to J_K$. A modulus, called a cycle in [25], is a finite formal product of primes of K with non-negative exponents $\prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$. If $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$ is a modulus, and $x \in K$, we write $x \equiv 1 \mod \mathfrak{m}$ to mean:

- For each finite $\mathfrak{p}|\mathfrak{m}$, $x \equiv 1 \mod \mathfrak{p}^{n_\mathfrak{p}}$;
- for each real prime $v|\mathfrak{m}$, we have $x_v > 0$.

If S is a finite set of primes, we let J_K^S be the subgroup of J generated by the primes not in S. For a modulus $\mathfrak{m}$, we let $J_K^\mathfrak{m}$ be J_K^S where S is the set of finite primes that divide $\mathfrak{m}$. Set

$$K^\mathfrak{m} := \iota^{-1}\left(J_K^\mathfrak{m}\right)$$

and

$$K_1^\mathfrak{m} := \{x \in K^\mathfrak{m}; x \equiv 1 \mod \mathfrak{m}\}.$$

Let $P_K^{\mathfrak{m}} = \iota\left(K_1^{\mathfrak{m}}\right)$ and define

$$\mathcal{C}_K^{\mathfrak{m}} = J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}.$$

This class group is finite. A congruence subgroup modulo $\mathfrak{m}$ is a subgroup $H^{\mathfrak{m}}$ of $J_K^{\mathfrak{m}}$ which contains $P_K^{\mathfrak{m}}$. We recall the following two main theorems of class field theory:

Theorem 10 (Artin Reciprocity Law)**.** *For L/K an Abelian extension of number fields, there is a modulus $\mathfrak{m}$ divisible by all the ramified primes of L/K such that the sequence*

$$1 \to P_K^{\mathfrak{m}}.N_{L/K}\left(J_L^{\mathfrak{m}}\right) \hookrightarrow J_K^{\mathfrak{m}} \to Gal\,(L/K) \to 1$$

is exact.

Theorem 11. *For any congruence subgroup $H^{\mathfrak{m}}$, there is a unique Abelian extension L/K such that L is the class field of K of the congruence class group $J_K^{\mathfrak{m}}/H^{\mathfrak{m}}$.*

We have the following lemma:

Lemma 8. *Let K be a number field, $\mathfrak{m}$ a modulus, and $H^{\mathfrak{m}}$ a congruence subgroup. If C is a coset of $J_K^{\mathfrak{m}}/H^{\mathfrak{m}}$, we set*

$$f_C(s) = \prod_{p \in C} (1 - N(p)^{-s})^{-1}.$$

Then $f_C(s)$ is holomorphic for $\Re s > 1$. Furthermore, then $g_C(s) = f_C(s)^r$, $r = |J_K^{\mathfrak{m}}/H^{\mathfrak{m}}|$, has an analytic continuation to an open set containing $\Re s = 1$ with a unique pole at $s = 1$. Assuming GRH, $s = 1$ is the only pole for $\Re s > 1/2$.

We do not need the additional convergence provided but assuming GRH to prove Proposition 2, but include this statement to give a better idea of the analytic behavior of this function.

Proof. Let $G = J_K^{\mathfrak{m}}/H^{\mathfrak{m}}$. Then

$$\begin{aligned}\log g_C(s) &= |G| \log f_C(s)\\ &= -|G| \sum_{p \in C} \log(1 - N(p)^{-s})\\ &= |G| \sum_{p \in C} N(p)^{-s} + |G| \sum_{p \in C} \sum_{m \geq 2} \frac{1}{m} N(p)^{-ms}.\end{aligned}$$

Write

$$h(s) = |G| \sum_{p \in C} \sum_{m \geq 2} \frac{1}{m} N(p)^{-ms}.$$

This is holomorphic for $\Re s > 1/2$. We then write

$$\begin{aligned}\log g(s) - h(s) &= \sum_{p} \sum_{\chi \in Hom(G,S^1)} \chi(p)\chi\left(C^{-1}\right) N(p)^{-s}\\ &= \sum_{\chi \in Hom(G,S^1)} \chi\left(C^{-1}\right) \sum_{p} \chi(p) N(p)^{-s}\end{aligned}$$

$$= \sum_{\chi\in Hom(G,S^1)} \chi(C^{-1}) \left(\log \prod_p (1-\chi(p)N(p)^{-s}) - \sum_p \sum_{m\geq 2} \frac{1}{m}\chi(p)^m N(p)^{-ms} \right)$$

$$= \log \left(\prod_{\chi\in Hom(G,S^1)} L(s,\chi)^{\chi(C^{-1})} \right) + H(s)$$

with $H(s)$ a function that is holomorphic for $\Re s > 1/2$. Hence

$$g_C(s) = \prod_{\chi\in Hom(G,S^1)} L(s,\chi)^{\chi(C^{-1})} e^{H(s)+h(s)}.$$

The lemma now follows from results on zero free regions of L-functions, e.g., Ch. 2 of [23]. $\square$

Next, we can prove Proposition 2:

Proof of Proposition 2. If L/K is Abelian, this follows from the above lemma and class field theory. In general, let $\sigma \in C$, and let $H = \langle\sigma\rangle$. Let $M = L^H$. Note that L/M is an Abelian Galois extension. Let

$$F_H(s) = \prod_{p\in S} (1 - N_M(p)^{-s})^{-1}$$

where S is the set of primes of L^H satisfying

- $\left(\frac{L/M}{p}\right) = \sigma$;
- $f(p/p\cap \mathcal{O}_K) = e(p/p\cap\mathcal{O}_K) = 1$.

We will also consider

$$F'_H(s) = \prod_{p\in S'} (1 - N_M(p)^{-s})^{-1}$$

where S' is the set of primes p of M such that $\left(\frac{L/M}{p}\right) = \sigma$. We know from what we proved before that $F'_H(s)^{|H|}$ has a simple pole at $s = 1$. By the computations of Ch. V, (section 6 of [25]), we know that $F'_H(s)/F_H(s)$ is holomorphic for $\Re s > 1/2$. Thus $F_H(s)^{|H|}$ has a simple pole at $s = 1$ and otherwise holomorphic in an open set containing $\Re s \geq 1$.

Next, it follows from the reduction step of the proof of the Chebotarev density theorem, Theorem 6.4 of [25], that

$$F_H(s) = \left(\prod_{\substack{p \text{prime of } K \\ \left(\frac{L/K}{p}\right)=C}} (1 - N(p)^{-s})^{-1} \right)^{\frac{|G|}{|C|\cdot|H|}}$$

$$= (F_C(s))^{\frac{|G|}{|C|\cdot|H|}}.$$

The proposition is now immediate. $\square$

Some remarks on r_2

Suppose we have a finite group G acting on a finite set A. Let $O_1, \ldots, O_r$ be the distinct orbits of the action of G. Then G has an induced representation on the vector space

$$V = \oplus_{a\in A}\mathbb{C}.$$

We skip the proof of the following elementary lemma:

Lemma 9. *We have*

$$\dim V^G = r.$$

The lemma has the following consequence:

Proposition 4. *We have*

1. *for* $n \geq 3$, $r_2(S_n) = r_2(A_n) = 1$;
2. $r_2(C_n) = r_2(D_n) = \lfloor n/2 \rfloor$.

Proof. For the first part, we show that A_n acts transitively on the two element subsets of $\{1, \ldots, n\}$. For this, we notice that for three distinct elements a, b, c, the even permutation $(a\ c)(b\ a)$ maps the set $\{a, b\}$ to the set $\{b, c\}$.

For C_n and D_n, write $n = 2k$ or $n = 2k + 1$, depending on the parity of n. Suppose $C_n = \langle (1\ 2\ \ldots\ n) \rangle$. It is easy to see that for each $1 \leq i \leq k$, the set

$$O_i = \{\{a, b\}; 1 \leq a, b \leq n, b - a \equiv i \mod n\}$$

is an orbit of the action of C_n on the set of two element subsets of $\{1, \ldots, n\}$. Furthermore, these are all the possible orbits. To see the result for D_n, we consider the generators $(1\ 2\ \ldots\ n), \sigma$, with

$$\sigma = (1\ n)(2\ n-1) \ldots (k\ k+1).$$

We observe that each orbit O_i is invariant under the action of σ. □

For the case where n is a prime number, we have the following proposition:

Proposition 5. *Let G be a transitive subgroup of S_p, p prime. Then one of the following two possibilities occurs:*

1. *G is doubly transitive and $r_2(G) = 1$;*
2. *G is solvable in which case $p \mid |G|$ and $r_2(G) = \gcd\left(\frac{|G|}{p}, \frac{p-1}{2}\right)$.*

Proof. A theorem of Burnside [4,22] says that a transitive subgroup of S_p is either doubly transitive or solvable. If the action of G is doubly transitive, then $r_2(G) = 1$. If G is solvable, a classical theorem of Galois ([15], p. 163)[1] asserts that G contains a unique normal subgroup C of order p, and is contained in the normalizer of C. Furthermore, G/C is a cyclic group of order dividing $p - 1$. Up to conjugation, we may assume that $C = \langle (1\ 2\ \ldots\ p) \rangle$. The normalizer of C is the split extension of the group C by the cyclic group Z of order $p - 1$ consisting of the elements σ_k, $1 \leq k \leq p - 1$ identified by

$$\sigma_k(x) \equiv kx \mod p,$$

for $x \in \{1, \ldots, n\}$; that the group Z is cyclic is the theorem of the primitive root in elementary number theory. Let σ_g be a generator of Z. Since G is transitive, G is equal to $C \ltimes \langle \sigma_g^j \rangle$

for some $j|p-1$. By the description of orbits of C on the two element subsets of $\{1,\ldots,p\}$, we just need to know the number of orbits of $\langle\sigma_g^j,\sigma_g^{\frac{p-1}{2}}\rangle$ on $(\mathbb{Z}/p\mathbb{Z})^*$. The latter is equal to

$$\frac{|(\mathbb{Z}/p\mathbb{Z})^*|}{|\langle\sigma_g^j,\sigma_g^{\frac{p-1}{2}}\rangle|}=\frac{p-1}{|\langle\sigma_g^{\gcd\left(j,\frac{p-1}{2}\right)}\rangle|}=\gcd\left(j,\frac{p-1}{2}\right).$$

□

The proof of Theorem 6

Outline of the proof of Theorem 6

Let $d\in\mathbb{N}$, and let $R=\mathbb{Z}^d$ equipped with componentwise addition and multiplication. Namely for $v=(v_1,\ldots,v_d), w=(w_1,\ldots,w_d)\in\mathbb{Z}^n$, we set

$$v+w=(v_1+w_1,\ldots,v_d+w_d),$$

$$\beta(v,w):=v\circ w=(v_1w_1,\ldots,v_dw_d).$$

To emphasize the dependence of $\mathcal{M}_p(\beta)$ from Definition 2 on d, we write it as $\mathcal{M}_d(p)$. For $d=2,3,4$, we will give an explicit description of $\mathcal{M}_d(p)$ in sections 'Orders of $\mathbb{Z}^3$', 'Orders of $\mathbb{Z}^4$', and 'Orders of $\mathbb{Z}^5$'.

Definition 5. If $\underline{k}=(k_1,\ldots,k_d)$ is a d-tuple of non-negative integers, we set

$$\mathcal{M}_d(p;\underline{k})=\left\{M=\begin{pmatrix}p^{k_1}&0&\ldots&0\\x_{21}&p^{k_2}&0&\vdots\\\vdots&\vdots&\ddots&0\\x_{d1}&\ldots&x_{d\,d-1}&p^{k_d}\end{pmatrix}\in\mathcal{M}_d(p)\right\}.$$

We define $\mu_p(\underline{k})$ to be the $\frac{d(d-1)}{2}$-dimensional volume of $\mathcal{M}_d(p;\underline{k})$.

It is easy to see that

$$\zeta^{<}_{\mathbb{Z}^d,p}(s)=\sum_{\substack{\underline{k}=(k_1,\ldots,k_d)\\k_i\geq 0,\forall i}}p^{\sum_{i=1}^d(d-i)k_i}p^{-s\sum_{i=1}^d k_i}\mu_p(\underline{k}). \tag{6}$$

Intuitively, what this means is that we have multiplied the rows by units to make the diagonal entries a p-power. We note that this does not change the lattice generated by the rows.

Warning. The volume of $\mathcal{M}_d(p;\underline{k})$ are used to count *subrings* of finite index in $\mathbb{Z}^d$, and *orders* of finite index in $\mathbb{Z}^{d+1}$. The reader should be careful about the distinction between subrings and orders.

We have the following lemma which is equivalent to Lemma 4 given during the proof of Proposition 1.

Lemma 10. *We have*

$$a^{<}_{\mathbb{Z}^d}(p)=\binom{d+1}{2}.$$

For a proof, see [19] Proposition 1.1. The quantity $a^{<}_{\mathbb{Z}^d}(p)$ is equal to $f_{d+1}(p)$ of that reference. By Theorem 9, Theorem 6 is proved if we can show the following statement: there is an $\epsilon > 0$ such that for $\Re(s) = \sigma > 1 - \epsilon$ we have

$$\sum_p \sum_{k=2}^{\infty} \frac{a^{<}_{\mathbb{Z}^d}(p^k)}{p^{k\sigma}} < \infty.$$

Since by Equation (6)

$$a^{<}_{\mathbb{Z}^d}(p^k) = \sum_{\substack{\underline{k}=(k_1,\ldots,k_d)\\ \sum_i k_i = k}} p^{\sum_i (d-i)k_i} \mu_p(\underline{k}),$$

in order to prove the lemma, we need to estimate $\mu_p(\underline{k})$. The relevant computations are performed in sections 'Orders of $\mathbb{Z}^3$', 'Orders of $\mathbb{Z}^4$', and 'Orders of $\mathbb{Z}^5$'.

The results are stated in Theorems 12, 13, and 14. These theorems form part 1 of Theorem 6.

The proof of part 2 of Theorem 6 appears in section 'Orders of $\mathbb{Z}^d$ for $d > 5$'.

General facts about volumes

We begin with some lemmas that allow us to bound the volumes of certain sets that arise in our volume computations. Let U_p denote the set of units of $\mathbb{Z}_p$ and $v_p(\cdot)$ be the p-adic valuation. Recall that for $\alpha, \beta \in \mathbb{Z}_p$, if $v_p(\alpha) \neq v_p(\beta)$ then $v_p(\alpha - \beta) = \min\{v_p(\alpha), v_p(\beta)\}$.

Proposition 6. *For fixed $y, z \in \mathbb{Z}_p$, $k \geq 0$, the volume of $x \in \mathbb{Z}_p$ such that $v_p(xy - z) \geq k$ is at most $p^{-(k - v_p(y))}$.*

Proof. We first note that for $y = 1$, the volume of x such that $v_p(x - z) \geq k$ is p^{-k}, since we are just fixing the first k digits in the p-adic expansion of x to coincide with those of z. Similarly, for any unit $u \in U_p$, the volume of x such that $v_p(ux - z) \geq k$ is p^{-k}.

We see that if $v_p(z) < k$ and $v_p(y) > v_p(z)$, then clearly $v_p(xy - z) = v_p(z) < k$ for any value of x. If $v_p(z) \geq k$, then $v_p(xy - z) \geq k$ if and only if $v_p(xy) \geq k$ which holds if and only if $v_p(x) \geq k - v_p(y)$. This holds on a set of volume at most $p^{-(k - v_p(y))}$ if $k \geq v_p(y)$ and on a set of volume 1 if $v_p(y) \geq k$.

Now, if $v_p(z) < k$ and $v_p(y) \leq v_p(z)$ then we can write $y = p^{v_p(y)}u$ for some unique unit $u \in U_p$, and $z = p^{v_p(y)}z'$ for some unique $z' \in \mathbb{Z}_p$. We have $v_p(xy - z) \geq k$ if and only if $v_p(xu - z') \geq k - v_p(y)$, which holds on a set of volume at most $p^{-(k - v_p(y))}$. $\square$

Proposition 7. *For fixed $z \in \mathbb{Z}_p$, the combined volume of $x, y \in \mathbb{Z}_p^2$ such that $v_p(xy - z) \geq k$ is at most $(k+1)p^{-k}$.*

Proof. If $v_p(y) \geq k$, then there are two cases. Either $v_p(z) \geq k$ in which case any x will work or $v_p(z) < k$ in which case no x works. So assume $0 \leq v_p(y) < k$. Then given y with $l = v_p(y)$, we need x such that $x \in p^{-l}(p^k\mathbb{Z}_p + z)$. So the total volume is

$$\sum_{l=0}^{k-1} p^{-l} \mathrm{vol}\,(p^{-l}(p^k\mathbb{Z}_p + z)) \leq kp^{-k}.$$

$\square$

Proposition 8. *For any fixed $z \in \mathbb{Z}_p$, the combined volume of $x, y \in \mathbb{Z}_p^2$ such that $v_p(x(y-z)) \geq k$ is at most $(k+1)p^{-k}$.*

Proof. This proposition is very similar to the previous one. We have $v_p(x) \geq k$ on a set of volume p^{-k}. Suppose that this does not hold and set $v_p(x) = m$. We see that for any fixed z, the volume of y such that $v_p(y-z) \geq k-m$ is $p^{-(k-m)}$. Summing over the k possible values of m gives the result. □

Proposition 9. *Suppose $z \in \mathbb{Z}_p$, $k, l \geq 0$ are given. Then the volume of $x \in \mathbb{Z}_p$ such that*

$$v_p\left(x\left(x-p^l\right)-z\right) \geq k$$

is bounded by $2p^{-\lceil k/2 \rceil}$.

Proof. If there is no such x, then the volume is zero and there is nothing to prove. Assume that the volume is nonzero. For simplicity of notation, let $y = p^l$. If $v_p(t) \geq k$ and $v_p(x(x-y)-z) \geq k$, then $x+t$ also satisfies the same inequality.

Given y and z modulo p^k, we must determine the number of x modulo p^k such that $x(x-y)-z \equiv 0 \mod p^k$. If this number is N, the volume of our domain is $N \cdot p^{-k}$. Suppose $X, X+u$ are both solutions of the congruence

$$x(x-y) \equiv z \mod p^k.$$

This implies that u satisfies the congruence

$$u^2 + u(2X-y) \equiv 0 \mod p^k.$$

We count the number of nonzero solutions u of this congruence equation.

If $2X - y \equiv 0 \mod p^k$, then $u^2 \equiv 0 \mod p^k$. This implies any solution u is of the form

$$a_{\lceil \frac{k}{2} \rceil} p^{\lceil \frac{k}{2} \rceil} + a_{r+1}p^{r+1} + \cdots + a_{k-1}p^{k-1}.$$

There are at most $p^{k-\lceil k/2 \rceil}$ choices for u. If not, then we write $2X - y \equiv p^s q \mod p^k$ with $s < k$ and $(q,p) = 1$.

We write $u = p^r m \mod p^k$. By assumption, $(m,p) = 1$ and $r < k$. Since

$$u\left(u + (2X-y)\right) \equiv 0 \mod p^k, \tag{7}$$

we have $u + (2X-y) \equiv 0 \mod p^{k-r}$.

If $2r \geq k$, then $r \geq \lceil \frac{k}{2} \rceil$, and as above there are at most $p^{k-\lceil k/2 \rceil}$ choices for u.

If $2r < k$, then $s = r$ and Equation 7 implies that u and $2X - y$ match up in the first $k - r \geq \lceil \frac{k}{2} \rceil$ digits of their p-adic expansions. This gives at most $p^{k-\lceil \frac{k}{2} \rceil} \leq p^{\lceil \frac{k}{2} \rceil}$ choices for u. Multiplication by p^{-k} gives the result. □

We point out that in the most general possible case, it is not possible to improve this result by more than a factor of 2. Suppose $l \geq \lceil k/2 \rceil$. Then $v_p(x) + v_p\left(x - p^l\right) \geq k$ if and only if $v_p(x) \geq \lceil k/2 \rceil$, which holds on a set of volume at most $p^{-\lceil k/2 \rceil}$. However, in some cases, we can say something stronger.

Proposition 10. *Suppose $z \in \mathbb{Z}_p$, $k, l \geq 0$ are given. Then there is a constant C, which for odd p may be taken to be 6, such that the volume of $x \in \mathbb{Z}_p$ satisfying*

$$v_p\left(x\left(x-p^l\right)-z\right) \geq k$$

is bounded by $Cp^{-(k-l)}$ except when $p=2$ and $v_2(z)=2l-2<k$. In this exceptional situation:

1. *If $v_2\left(z+2^{2l-2}\right) \geq k$, the volume is bounded by $2^{-\lceil k/2 \rceil}$, and this is the best bound possible.*
2. *If $v_2\left(z+2^{2l-2}\right) < k$ is odd, the volume is zero.*
3. *If $v_2\left(z+2^{2l-2}\right) < k$, the volume is bounded by*

   $$8\left|z+2^{2l-2}\right|_2^{-1/2} 2^{-k},$$

   where $|\,.\,|_2$ is the 2-adic absolute value on $\mathbb{Q}_2$.

Proof. The proposition will have no content unless $l < k$. First, we consider the case where p is odd. We recognize two basic cases:

1. If $v_p(z) \geq k$, then we have $v_p\left(x\left(x-p^l\right)\right) \geq k$. We consider two cases, when $v_p(x)=l$ and when $v_p(x) \neq l$. In the first case $v_p\left(x-p^l\right) \geq k-l$, and in the second case, we have $v_p(x) \geq k-l$. In either case, the volume is bounded by $p^{-(k-l)}$.

2. If $v_p(z) < k$, then our inequality can be valid only when $v_p\left(x\left(x-p^l\right)\right)=v_p(z)$. Since $v_p(z)<k$, we write $z=\zeta p^u$ with $u<k$. We are looking for solutions to

$$v_p\left(x\left(x-p^l\right)-\zeta p^u\right) \geq k$$

that satisfy $v_p(x)+v_p\left(x-p^l\right)=u$.

- If $v_p(x) > l$, then we must have $v_p(x)+l=u$, and as a result $u-l>l$ which means $u>2l$. Write $x=\epsilon p^{u-l}$. Then we need

  $$v_p\left(\epsilon p^{u-l}\left(\epsilon p^{u-l}-p^l\right)-\zeta p^u\right) \geq k.$$

  This implies $v_p(\epsilon(\epsilon p^{u-2l}-1)-\zeta) \geq k-u$. This is a quadratic equation in ϵ with at most two solutions modulo p. Hensel's lemma says that the volume of ϵ satisfying this last inequality is at most $2p^{-(k-u)}$. The volume for x is then at most $2p^{-(u-l)} \cdot p^{-(k-u)}$ $=2p^{-(k-l)}$.
- (*) If $v_p(x) < l$, then $2v_p(x)=u$, which means u is even and $u<2l$. Write $x=\epsilon p^{u/2}$. Then we need $v_p\left(\epsilon p^{u/2}\left(\epsilon p^{u/2}-p^l\right)-\zeta p^u\right) \geq k$ which gives $v_p\left(\epsilon\left(\epsilon-p^{l-u/2}\right)-\zeta\right) \geq k-u$. By Hensel's lemma, the volume of such ϵ is at most $2p^{-(k-u)}$. The volume of x is then bounded by $2p^{-(k-u)} \cdot p^{-u/2}=2p^{-k+u/2}<2p^{-k+l}$ which is what we want.
- If $v_p(x)=l$, then $x=\epsilon p^l$, and we have $2l+v_p(\epsilon-1)=u$. This means $u \geq 2l$. Then we need $v_p\left(\epsilon\left(\epsilon-1\right)-\zeta p^{u-2l}\right) \geq k-2l$. An application of Hensel's lemma then says that the volume of ϵ satisfying this inequality is at most $2p^{-(k-2l)}$. Since $x=p^l\epsilon$, the volume of x is at most $2p^{-(k-l)}$.

Now, we examine the situation for $p = 2$. Except for the step marked (*) every other step of the proof works verbatim. The argument (*) can be adjusted as follows. We let $r = l - \frac{u}{2}$ and $s = k - u$. Then $r \geq 1$ and we are trying to determine the volume of $\epsilon \in U_p$ such that

$$\nu_2(\epsilon(\epsilon - 2^r) - \zeta) \geq s.$$

for a given unit ζ. Rewrite this inequality as

$$\nu_2\left(\left(\epsilon - 2^{r-1}\right)^2 - \left(\zeta + 2^{2r-2}\right)\right) \geq s.$$

First, we consider the situation for $r \geq 2$. In this case, both $\epsilon - 2^{r-1}$ and $\zeta + 2^{2r-2}$ are still units, and without loss of generality, we may assume that our inequality has the form

$$\nu_2(\epsilon^2 - \zeta) \geq s$$

with ϵ, ζ units. Fix an ϵ that satisfies the inequality, and we determine for what values of τ, $\epsilon + \tau$ also satisfies the inequality. The volume of such τ is the volume of ϵ. We have

$$\nu_2((\epsilon + \tau)^2 - \zeta) = \nu_2((\epsilon^2 - \zeta) + \tau(\tau + 2\epsilon)).$$

This implies that

$$\nu_2(\tau(\tau + 2\epsilon)) \geq s.$$

This immediately implies that $\nu_2(\tau) \geq s - 1$ or $\nu_2(\tau + 2\epsilon) \geq s - 1$. Consequently, the volume of ϵ is bounded by $2 \cdot 2^{-(s-1)} = 4 \cdot 2^{-(k-u)}$. The rest of the argument works as before.

Now, we consider the case where $r = 1$. In this case, the inequality becomes

$$\nu_2((\epsilon - 1)^2 - (\zeta + 1)) \geq s.$$

There are two cases to consider:

Case I. $\nu_2(\zeta + 1) \geq s$. In this case, we see that $\nu_2(\epsilon - 1) \geq \lceil s/2 \rceil$ and as a result, the volume is $2^{-\lceil s/2 \rceil}$. The volume of x is then seen to be bounded by $2^{-\lceil k/2 \rceil}$.

Case II. $\nu_2(\zeta + 1) < s$. We have $2\nu_2(\epsilon - 1) = \nu_2(\zeta + 1)$, so we can write $\zeta + 1 = \gamma 2^{2t}$, with γ a unit. Then we have $\nu_2(\epsilon - 1) = t$, and write $\epsilon - 1 = \omega 2^t$. This implies

$$\nu_2(\omega^2 - \gamma) \geq s - 2t.$$

As above, the volume of such ω is bounded by $4 \cdot 2^{-s+2t}$. The volume of ϵ then is bounded by $4 \cdot 2^{-s+t}$. The volume of x is then bounded by $4 \cdot 2^{-k+l} \cdot 2^t$. $\square$

Orders of $\mathbb{Z}^3$

Volume estimates for $\mathbb{Z}^3$

First, we give a description of $\mathcal{M}_2(p)$.

Lemma 11. *The set $\mathcal{M}_2(p)$ is the collection of matrices*

$$M = \begin{pmatrix} x_{11} & 0 \\ x_{21} & x_{22} \end{pmatrix},$$

with entries in $\mathbb{Z}_p$ such that

$$\nu_p(x_{21}(x_{21} - x_{22})) \geq \nu_p(x_{11}).$$

Proof. Let v_1 and v_2 be the first and the second rows of M, respectively. Then since entries are in $\mathbb{Z}_p$, it is clear that $v_1 \circ v_1$ and $v_1 \circ v_2$ are integral linear combinations of v_1, v_2. Now we need $v_2 \circ v_2 = \alpha_1 v_1 + \alpha_2 v_2$ with $\alpha_1, \alpha_2 \in \mathbb{Z}_p$. So $x_{22}^2 = \alpha_2 x_{22}$, which implies $\alpha_2 = x_{22}$. Then $\alpha_1 x_{11} + x_{22}x_{21} = x_{21}^2$, and $\alpha_1 = x_{11}^{-1}\left(x_{21}^2 - x_{21}x_{22}\right)$. Therefore, α_1 is in $\mathbb{Z}_p$ if and only if $v_p(x_{11}) \le v_p\left(x_{21}^2 - x_{21}x_{22}\right)$. □

We note that the sublattice corresponding to a matrix M as above has finite index if and only if $\det M \neq 0$.

Counting orders of $\mathbb{Z}^3$

We now prove the following theorem:

Theorem 12. *There is a polynomial P_3 of degree 2 such that for all $\epsilon > 0$*

$$N_3(B) = BP_3(\log B) + O\left(B^{\frac{1}{2}+\epsilon}\right)$$

as $B \to \infty$.

Proof. By Theorem 9 and Lemma 10, it suffices to prove the following statement: If $\sigma > \frac{1}{2}$, the series

$$\sum_p \sum_{k+l \ge 2} p^k p^{-k\sigma - l\sigma} \mu_p(k,l) \tag{8}$$

converges. Here, $\mu_p(k,l)$ is as in Definition 5.

We divide the series (8) into three subseries:

Case I. $k \ge 0, l \ge 2$. Then by Proposition 9

$$\mu_p(k,l) \le 2p^{-k/2}.$$

Our subseries is then majorized by

$$\sum_p \sum_{k \ge 0} \sum_{l \ge 2} p^{k/2} p^{-k\sigma - l\sigma}$$

which converges for $\sigma > \frac{1}{2}$.

Case II. $k \ge 2, l = 0$. Then by the proof of Proposition 9

$$\mu_p(k,0) \le 2p^{-k}$$

and as a result, our subseries is majorized by

$$\sum_p \sum_{k \ge 2} p^{-k\sigma}$$

which converges for $\sigma > \frac{1}{2}$.

Case III. $k = 1, l = 1$. By Proposition 9

$$\mu_p(1,1) \le 2p^{-1}$$

and our subseries is majorized by

$$\sum_p p^{-2\sigma}.$$

This converges for $\sigma > \frac{1}{2}$.

For the second assertion in the statement of the theorem, we observe that

$$f_3(k) = N_3(k) - N_3(k-1).$$

□

Orders of $\mathbb{Z}^4$

Volume estimates for $\mathbb{Z}^4$

Lemma 12. *The domain $\mathcal{M}_3(p)$ is the collection of 3×3 lower triangular matrices*

$$\begin{pmatrix} x_{11} & & \\ x_{21} & x_{22} & \\ x_{31} & x_{32} & x_{33} \end{pmatrix}$$

with entries in $\mathbb{Z}_p$ such that the following inequalities hold:

[4-1] $v_p(x_{11}) \le v_p\left(x_{21}^2 - x_{21}x_{22}\right)$

[4-2] $v_p(x_{11}) \le v_p(x_{21}(x_{31} - x_{32}))$

[4-3] $v_p(x_{22}) \le v_p\left(x_{32}^2 - x_{32}x_{33}\right)$

[4-4] $v_p(x_{11}) + v_p(x_{22}) \le v_p\left(x_{22}\left(x_{31}^2 - x_{31}x_{33}\right) - x_{21}\left(x_{32}^2 - x_{32}x_{33}\right)\right).$

Proof. We want to determine the conditions on matrices

$$M = \begin{pmatrix} x_{11} & 0 & 0 \\ x_{21} & x_{22} & 0 \\ x_{31} & x_{32} & x_{33} \end{pmatrix},$$

such that $x_{11}, x_{21}, x_{22}, x_{31}, x_{32}, x_{33} \in \mathbb{Z}_p$ and for $1 \le i,j \le 3$, there exist $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_p$ with $v_i \circ v_j = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3$, where v_i is the ith row of the matrix M.

The condition that $v_2 \circ v_2 = \alpha_1 v_1 + \alpha_2 v_2$ gives the same condition that we had for the case $n = 3$. That is, $v_p(x_{11}) \le v_p\left(x_{21}^2 - x_{21}x_{22}\right)$.

We have

$$v_2 \circ v_3 = (x_{21}x_{31}, x_{22}x_{32}, 0) = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3.$$

Clearly, $\alpha_3 = 0$. We have $\alpha_2 x_{22} = x_{32}x_{22}$, so $\alpha_2 = x_{32}$. So we have $\alpha_1 x_{11} + x_{32}x_{21} = x_{21}x_{31}$. This implies

$$\alpha_1 = x_{11}^{-1}(x_{21}x_{31} - x_{21}x_{32}).$$

Therefore, $v_p(x_{11}) \le v_p(x_{21}(x_{31} - x_{32}))$.

Next, consider

$$v_3 \circ v_3 = \left(x_{31}^2, x_{32}^2, x_{33}^2\right) = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3.$$

We must have $\alpha_3 = x_{33}$. So $\alpha_2 x_{22} + x_{33}x_{32} = x_{32}^2$. This implies

$$\alpha_2 = x_{22}^{-1}\left(x_{32}^2 - x_{32}x_{33}\right).$$

Therefore, $v_p(x_{22}) \le v_p\left(x_{32}^2 - x_{32}x_{33}\right)$.

We also have $\alpha_1 x_{11} + x_{22}^{-1}\left(x_{32}^2 - x_{32}x_{33}\right)x_{21} + x_{33}x_{31} = x_{31}^2$. This implies

$$\begin{aligned} \alpha_1 &= x_{11}^{-1}\left(x_{31}^2 - x_{31}x_{33} - x_{22}^{-1}x_{21}\left(x_{32}^2 - x_{32}x_{33}\right)\right) \\ &= x_{11}^{-1}x_{22}^{-1}(x_{22}(x_{31}^2 - x_{31}x_{33}) - x_{21}(x_{32}^2 - x_{32}x_{33})). \end{aligned}$$

So $v_p(x_{11}) + v_p(x_{22}) \le v_p\left(x_{22}\left(x_{31}^2 - x_{31}x_{33}\right) - x_{21}\left(x_{32}^2 - x_{32}x_{33}\right)\right)$. □

Suppose that $v_p(x_{11}) = k$, $v_p(x_{22}) = l$ and $v_p(x_{33}) = r$. By multiplying by appropriate units, we can suppose that $x_{11} = p^k$, $x_{22} = p^l$, and $x_{33} = p^r$. Note that this does not change the lattice generated by the rows. Then we can define $\mu_p(k;l;r)$ as in Definition 5.

Proposition 11. *Suppose that $k, l, r \geq 0$. Then*

$$\mu_p(k;l;r) \leq 8p^{-7k/6}p^{-l/6}. \tag{9}$$

Proof. We divide the proof into three steps. We give two different bounds on $\mu_p(k;l;r)$ and then take an average.

Step I. By Proposition 9, the volume of x_{32} satisfying inequality [4-3] is at most $2p^{-l/2}$. By Proposition 9, the volume of x_{21} satisfying inequality [4-1] is at most $2p^{-k/2}$, and for fixed x_{21}, x_{32}, Proposition 9 implies that the volume of x_{31} satisfying inequality [4-4] is at most $2p^{-k/2}$. Multiplication gives:

$$\mu_p(k;l;r) \leq 8p^{-k}p^{-l/2}.$$

Step II. By one of the steps of the proof of Proposition 10 the volume of x_{21} satisfying inequality [4-1] is at most $2p^{-k+l}$. By Proposition 9 the volume of x_{32} satisfying inequality [4-3] is at most $2p^{-l/2}$. By Proposition 9 the volume of x_{31} satisfying inequality [4-4] is at most $2p^{-k/2}$. Multiplication gives

$$\mu_p(k;l;r) \leq 8p^{-3k/2}p^{l/2}.$$

Step III. We now consider an appropriate average. The idea is that if $\mu \leq A$ and $\mu \leq B$, with $\mu, A, B > 0$, then for all m, n positive integers

$$\mu \leq (A^m B^n)^{\frac{1}{m+n}}.$$

The bounds from steps I and II give

$$\begin{aligned}\mu_p &\leq \left\{ \left(8p^{-k}p^{-l/2}\right)^2 \left(8p^{-3k/2}p^{l/2}\right) \right\}^{1/3} \\ &= 8p^{-7k/6}p^{-l/6}.\end{aligned}$$

□

Remark 6. This is not the best possible bound one can prove. In fact, using a more complicated argument similar to the proof of step I of Theorem 15, we can prove a bound of $Cp^{-9k/8}p^{-l/2}$ in step I of the above theorem. This leads to the bound $\mu_p \leq Cp^{-5k/4}p^{-l/2}$ after averaging. This, however, will not improve the bound in Theorem 13 unless one has an analogue of Theorem 17 for $r = 1$. Such a theorem is easy to prove, but the resulting estimate would still not be as good as the one obtained in [19]. For this reason, we decided to include only the simplest non-trivial estimate.

Proposition 12. *Let p be odd. If $r = 0$ and $k, l \geq 1$, then*

$$\mu_p(k;l;0) \leq 24p^{-3k/2-l}.$$

Proof. Proposition 9 implies that inequality [4-1] holds on a set of x_{21} of volume at most $2p^{-\lceil k/2 \rceil}$. Proposition 10 implies that inequality [4-3] holds on a set of x_{32} of volume at most $2p^{-l}$. For fixed x_{21}, x_{32}, Proposition 10 implies that inequality [4-4] holds on a set of x_{31} of volume at most $6p^{-k}$.

We see that our total volume is bounded by $24p^{-k-l-\lceil k/2 \rceil}$. □

Proposition 13. *Let p be odd. Then*

$$\mu_p(0; l; 0) \leq 2p^{-l}$$

and

$$\mu_p(k; 0; 0) \leq 3p^{-2k}.$$

Proof. If $k = r = 0$, then inequality [4-3] and Proposition 10 give the result. Now suppose $l = r = 0$. Then we have

$$v_p(x_{21}) + v_p(x_{21} - 1) \geq k$$

which determines two possibilities for x_{21}:

1. $v_p(x_{21}) \geq k$. In this case, inequality [4-4] says

$$v_p(x_{31}) + v_p(x_{31} - 1) \geq k.$$

The volume of such x_{31} is $2p^{-k}$. As a result, the whole volume is at most $2p^{-2k}$.

2. $v_p(x_{21}) = 0$ and $v_p(x_{21} - 1) \geq k$. Then inequality [4-2] gives

$$v_p(x_{31} - x_{32}) \geq k$$

and the two-dimensional volume of (x_{31}, x_{32}) satisfying this inequality is at most p^{-k}. This gives a bound on the entire volume of p^{-2k}.

Adding up gives the result.

□

Counting orders of $\mathbb{Z}^4$

In this section, we prove the following theorem:

Theorem 13. *There is a polynomial P_4 of degree 5 such that for all $\epsilon > 0$*

$$N_4(B) = BP_4(\log B) + O\left(B^{\frac{11}{12}+\epsilon}\right)$$

as $B \to \infty$.

Proof. By Theorem 9, it suffices to prove the following statement: the expression

$$\sum_p \sum_{k+l+r \geq 2} p^{2k+l-k\sigma-l\sigma-r\sigma} \mu_p(k; l; r) \tag{10}$$

converges whenever $\sigma > \frac{11}{12}$.

We write the sum (10) as

$$\sum_{k+l+r \geq 2} 2^{2k+l-k\sigma-l\sigma-r\sigma} \mu_2(k; l; r) + \sum_{p \text{odd}} \sum_{k+l+r \geq 2} p^{2k+l-k\sigma-l\sigma-r\sigma} \mu_p(k; l; r).$$

By Proposition 11, the first piece is majorized by

$$\sum_{k,l,r\geq 0} 2^{2k+l-k\sigma-l\sigma-r\sigma} 2^{-7k/6} 2^{-l/6}$$

which converges for $\sigma > 5/6$.

We now consider the second piece of the sum. We consider three cases.

Case I. $r \geq 2$. By Proposition 11, the relevant sum is bounded by

$$\sum_{p\text{odd}} \sum_{r\geq 2} \sum_{k,l\geq 0} p^{2k+l-k\sigma-l\sigma-r\sigma} p^{-7k/6} p^{-l/6} = \sum_{p \text{ odd}} \sum_{r\geq 2} \sum_{k,l\geq 0} p^{\left(\frac{5}{6}-\sigma\right)(k+l)-r\sigma}.$$

This sum is equal to

$$\sum_{p\text{odd}} \sum_{r\geq 2} \sum_{m\geq 0} (m+1) p^{\left(\frac{5}{6}-\sigma\right)m-r\sigma}.$$

This sum is converges for $\sigma > \frac{5}{6}$.

Case II. $r = 1$. From the previous computation, the corresponding sum converges if the sum

$$\sum_{p\text{odd}} \sum_{m\geq 1} p^{\left(\frac{5}{6}-\sigma\right)m-\sigma}$$

converges. If $\sigma > \frac{5}{6}$, the series converges if the series

$$\sum_{p\text{odd}} p^{\left(\frac{5}{6}-\sigma\right)-\sigma}$$

converges. The latter converges for $\sigma > 11/12$.

Case III. $r = 0$. We write the corresponding sum as

$$\sum_{p\text{odd}} \sum_{k+l\geq 2} p^{2k+l-k\sigma-l\sigma} \mu_p(k;l;0) = \sum_{p \text{ odd}} \sum_{l\geq 2} p^{l-l\sigma} \mu_p(0;l;0)$$

$$+ \sum_{p\text{odd}} \sum_{k\geq 2} p^{2k-k\sigma} \mu_p(k;0;0) + \sum_{p\text{odd}} \sum_{k,l\geq 1} p^{2k+l-k\sigma-l\sigma} \mu_p(k;l;0).$$

By Proposition 13, we have

$$\sum_{p\text{odd}} \sum_{l\geq 2} p^{l-l\sigma} \mu_p(0;l;0) \ll \sum_{p \text{ odd}} \sum_{l\geq 2} p^{-l\sigma}$$

and this is convergent for $\sigma > 1/2$. Again, by Proposition 13

$$\sum_{p\text{odd}} \sum_{k\geq 2} p^{2k-k\sigma} \mu_p(k;0;0) \ll \sum_{k\geq 2} p^{-k\sigma}$$

which converges for $\sigma > 1/2$. Finally, by Proposition 12

$$\sum_{p\text{odd}} \sum_{k,l\geq 1} p^{2k+l-k\sigma-l\sigma} \mu_p(k;l;0) \ll \sum_{p \text{ odd}} \sum_{k,l\geq 1} p^{\left(\frac{1}{2}-\sigma\right)k-l\sigma}.$$

If $\sigma > \frac{1}{2}$, this last series converges if the series

$$\sum_{p\text{odd}} p^{\left(\frac{1}{2}-\sigma\right)-\sigma}$$

converges. This last series converges for $\sigma > \frac{3}{4}$. □

Remark 7. The bounds obtained by Liu [19] for $f_3(k)$ and $f_4(k)$ are better than what we have obtained here. Liu proves $f_3(k) = O\left(k^{1/3}\right)$ and $f_4(k) = O_\epsilon\left(k^{1/2+\epsilon}\right)$.

Orders of $\mathbb{Z}^5$

Volume estimates for $\mathbb{Z}^5$

We will begin with the set of inequalities defining our region of integration.

Lemma 13. *$\mathcal{M}_4(p)$ is the collection of matrices with entries in $\mathbb{Z}_p$*

$$\begin{pmatrix} x_{11} & & & \\ x_{21} & x_{22} & & \\ x_{31} & x_{32} & x_{33} & \\ x_{41} & x_{42} & x_{43} & x_{44} \end{pmatrix}$$

whose entries satisfy:

$$\begin{aligned}
&[5\text{-}1] \quad v_p(x_{11}) \le v_p\left(x_{21}^2 - x_{21}x_{22}\right)\\
&[5\text{-}2] \quad v_p(x_{11}) \le v_p(x_{21}(x_{31} - x_{32}))\\
&[5\text{-}3] \quad v_p(x_{22}) \le v_p(x_{32}^2 - x_{32}x_{33})\\
&[5\text{-}4] \quad v_p(x_{11}) + v_p(x_{22}) \le v_p\left(x_{22}\left(x_{31}^2 - x_{31}x_{33}\right) - x_{21}\left(x_{32}^2 - x_{32}x_{33}\right)\right)\\
&[5\text{-}5] \quad v_p(x_{11}) \le v_p(x_{21}(x_{41} - x_{42}))\\
&[5\text{-}6] \quad v_p(x_{22}) \le v_p(x_{32}(x_{42} - x_{43}))\\
&[5\text{-}7] \quad v_p(x_{11}) + v_p(x_{22}) \le v_p(x_{22}x_{31}(x_{41} - x_{43}) - x_{21}x_{32}(x_{42} - x_{43}))\\
&[5\text{-}8] \quad v_p(x_{33}) \le v_p\left(x_{43}^2 - x_{43}x_{44}\right)\\
&[5\text{-}9] \quad v_p(x_{22}) + v_p(x_{33}) \le v_p(x_{33}x_{42}(x_{42} - x_{44}) - x_{32}x_{43}(x_{43} - x_{44}))\\
&[5\text{-}10] \quad v_p(x_{11}) + v_p(x_{22}) + v_p(x_{33}) \le v_p(x_{22}x_{33}x_{41}(x_{41} - x_{44}) - x_{22}x_{31}x_{43}(x_{43} - x_{44})\\
&\qquad\qquad - x_{21}x_{33}x_{42}(x_{42} - x_{44}) + x_{21}x_{32}x_{43}(x_{43} - x_{44})).
\end{aligned}$$

The proof of this lemma is very similar to the proof of Lemma 12.

By multiplying by appropriate units, we can suppose that $x_{11} = p^k,\ x_{22} = p^l,\ x_{33} = p^r$, and $x_{44} = p^t$. We define $\mu_p(k; l; r; t)$ as in Definition 5.

We start with a lemma:

Lemma 14. *Let p be a prime. Then there is a polynomial with positive coefficients $R \in \mathbb{R}[x]$ such that*

$$\mu_p(k; l; r; t) \le R(k)p^{-2k-l}.$$

Proof. In this proof, we will suppress the dependence of $R(k)$ on k, and will simply write R. The value of the polynomial R does not affect the convergence of the sum we consider, so we do not compute it. The key to our argument will be that once our other variables are fixed, there are several different bounds available to us for the volume of x_{31} such that inequalities [5-4] and [5-10] hold.

More specifically, we use Proposition 9 to give a bound on the volume of the possible set of x_{32}, then give a bound on the set of possible x_{43}. Once these two values are fixed, we again use Proposition 9 to give a bound on the set of x_{42}, which then bounds the set of possible x_{21}. Finally, we combine a few different possible bounds for the set of x_{31} so that these inequalities simultaneously hold.

Proposition 9 implies that inequality [5-3] holds on a set of x_{32} of volume at most $2p^{-l/2}$.

Suppose that $v_p(x_{43}(x_{43} - x_{44})) = r + z$. Inequality [5-8] implies that $z \geq 0$. This inequality holds on a set of x_{43} of volume at most $2p^{-r/2-z/2}$. Fix such an x_{43}.

Now for fixed x_{32}, x_{43}, Proposition 9 implies that inequality [5-9] holds on a set of x_{42} of volume at most $2p^{-l/2}$.

We now consider inequality [5-5]. For fixed x_{42}, Proposition 8 implies that the total volume of x_{21}, x_{41} such that this inequality holds is at most $(k + 1)p^{-k}$.

Finally, we consider x_{31}. We begin with inequality [5-10]. For fixed values of $x_{21}, x_{32}, x_{41}, x_{42}, x_{43}$, we can write this as

$$k + l + r \leq v_p(x_{31}x_{22}y - \tau),$$

where $y, \tau \in \mathbb{Z}_p$ with $v_p(y) = r + z$. We see that this holds on a set of x_{31} of volume at most $p^{-(k-z)}$.

Consider inequality [5-4]. By Proposition 9, this holds on a set of x_{31} of volume at most $2p^{-k/2}$.

Using $2p^{-(k-z)}$ as our bound for the volume of x_{31} gives a bound on our total volume of

$$R_1p^{-2k-l-(r-z)/2},$$

for some polynomial R_1. This is enough for our result if $r \geq z$. Suppose that this is not the case.

By the proof of Proposition 10, we see that the total volume of x_{31} such that

$$v_p(x_{31}(x_{31} - x_{33}) - z) \geq k,$$

is at most $6p^{-(k-r)}$ unless $p = 2$, $v_p(x_{31}) = r - 1$ and $v_p(z) = 2r - 2 < k$. If we are not in this exceptional situation, the total volume is at most $R_2p^{-2k-l-(z/2-r/2)}$. Since $r < z$, this is at most Rp^{-2k-l}, completing the proof.

Suppose that we are in the situation where $p = 2$, $v_p(x_{31}) = r-1$ and $v_p(z) = 2r-2 < k$.

First, suppose that $v_p(x_{31}) \neq v_p(x_{32})$. Then $v_p(x_{31} - x_{32}) \leq v_p(x_{31}) = r - 1$. Inequality [5-2] now holds on a set of x_{21} of volume at most $p^{-(k-r)}$. Using this bound for the volume of x_{21}, $2p^{-l/2}$ for the volume of x_{32} and $2p^{-k/2}$ for the volume of x_{31}, gives the total bound

$$R_3p^{-2k-l-(z-r)/2},$$

which is at most Ap^{-2k-l} for some polynomial A, since $z \geq r$.

Now suppose $v_p(x_{32}) = v_p(x_{31}) = r-1$. Then $v_p(x_{32}(x_{32}-x_{33})) = 2r-2$, and we must have $v_p(x_{21}) = l$. Now consider inequality [5-7]. We write $x_{21} = \alpha p^l$, $x_{31} = \beta p^{r-1}$, and $x_{32} = \gamma p^{r-1}$ for units α, β, γ. Factoring out p^{l+r-1}, the inequality is now

$$v_p(\beta x_{41} - \alpha\gamma x_{42} + (\alpha\gamma - \beta)x_{43}) \geq k - r + 1.$$

For fixed values of $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$, this holds on a set of x_{41} of volume at most $p^{-(k-r)}$. Using $2p^{-k/2}$ as our bound for x_{21} and x_{31}, this gives total bound

$$R_4p^{-2k-l-(z-r)/2},$$

which is at most Rp^{-2k-l}, completing the proof. □

Proposition 14. *Let p be any prime. Suppose that $k, l, r, t \geq 0$. Then for a polynomial $A \in \mathbb{R}[x]$ with positive coefficients, we have*

$$\mu_p(k; l; r; t) \leq A(k)p^{-(2+\frac{1}{34})k-(1+\frac{1}{34})l-\frac{r}{17}+\frac{16t}{17}}.$$

Proof. The value of the polynomial A does not affect the convergence of the sum we will consider so we do not compute it. For example in the collection of Equations (11), (12), and (13), the polynomials A will not be the same.

We have two steps:

Step I. Here, we show that the following three inequalities hold:

$$\mu_p(k; l; r; t) \leq Ap^{-3k/2-3l/2+t} \tag{11}$$

$$\mu_p(k; l; r; t) \leq Ap^{-2k-l-r+3t} \tag{12}$$

$$\mu_p(k; l; r; t) \leq Ap^{-5k/2-l+r+3t}. \tag{13}$$

We proceed as follows. Inequality [5-1] holds on a set x_{21} of volume at most the minimum of $2p^{-k/2}$ and $2p^{-(k-l)}$. Inequality [5-3] holds on a set x_{32} of volume at most the minimum of $2p^{-l/2}$ and $2p^{-(l-r)}$. Inequality [5-8] holds on a set of x_{43} of volume at most $2p^{-(r-t)}$.

When $p \neq 2$, we can use Proposition 10 for the remaining three variables (see the proof of Theorem 15 for details). For $p = 2$, some care is required. By Proposition 9, we always have the following. For any fixed x_{21} and x_{32}, inequality [5-4] holds on a set of x_{31} of volume at most $2p^{-k/2}$. For any fixed x_{32}, x_{43}, inequality [5-9] holds on a set of x_{42} of volume at most $2p^{-l/2}$. For any fixed $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$, inequality [5-10] holds on a set of x_{41} of volume at most $2p^{-k/2}$.

Inequality (11) follows from taking $2p^{-k/2}$ for the volume of x_{21}, x_{31}, x_{41}, taking $2p^{-(l-r)}$ for the volume of x_{32}, taking $2p^{-l/2}$ for the volume of x_{42}, and taking $2p^{-(r-t)}$ for the volume of x_{43}.

For inequality (12), we take $2p^{-k/2}$ as our bound for the volume of x_{21} and x_{31}, $2p^{-l/2}$ as the bound for x_{32} and x_{42}, and $2p^{-(r-t)}$ as the bound for the volume of x_{43}. We must now show that when all other variables are fixed, the total volume of x_{41} satisfying our inequalities is at most $Ap^{-(k-2t)}$.

Suppose we are not in the special case in which we cannot apply Proposition 10. We have that the volume of x_{41} satisfying inequality [5-10] is at most $6p^{-(k-t)}$, completing this case.

We can write inequality [5-10] as

$$\begin{aligned} v_p(x_{11}) + v_p(x_{22}) + v_p(x_{33}) \leq v_p(&x_{22}x_{33}x_{41}(x_{41} - x_{44}) - (x_{22}x_{31}x_{43}(x_{43} - x_{44}) \\ &+x_{21}(x_{33}x_{42}(x_{42} - x_{44}) - x_{32}x_{43}(x_{43} - x_{44})))). \end{aligned}$$

Inequality [5-8] implies that we can write $x_{43}(x_{43} - x_{44}) = p^r\alpha$, with $\alpha \in \mathbb{Z}_p$. Inequality [5-9] implies that we can write

$$x_{33}x_{42}(x_{42} - x_{44}) - x_{32}x_{43}(x_{43} - x_{44}) = p^{l+r}\beta,$$

with $\beta \in \mathbb{Z}_p$.

Our inequality is now

$$k \leq v_p(x_{41}(x_{41} - x_{44}) - (x_{31}\alpha + x_{21}\beta)).$$

We can apply Proposition 10, giving our bound, unless $v_p(x_{41}) = t-1$ and $v_p(x_{31}\alpha + x_{21}\beta) = 2t-2$.

First, suppose that $v_p(x_{21}) \le 2t$. Then for fixed x_{21}, x_{42}, inequality [5-5] holds on a set of x_{41} of volume at most $p^{-(k-2t)}$, which completes this case. Now suppose that $v_p(x_{31}) \le 2t$. Proposition 6 now implies that for fixed $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$, inequality $[5-7]$ holds on a set of x_{41} of volume at most $p^{-(k-v_p(x_{31}))} \le p^{-(k-2t)}$. This is enough for our bound, so we suppose that $v_p(x_{21}) \ge 2t$ and $v_p(x_{31}) \ge 2t$. This implies that $v_p(x_{31}\alpha + x_{21}\beta) \ge 2t > 2t-2$, so we can apply Proposition 10, completing this case.

Inequality (13) will be proved in a few steps. First, we suppose that we are in the case where we can apply Proposition 10 to inequality [5-4] and conclude that the volume of x_{31} satisfying this inequality is at most $6p^{-(k-r)}$. As above, we see that either one of x_{21}, x_{31} has valuation at most $2t$, giving a bound of $p^{-(k-2t)}$, or both have valuation at least $2t$, in which case we can apply Proposition 10 and conclude that the total volume of x_{41} is at most $6p^{-(k-t)}$. Using $2p^{-k/2}$ as our bound for x_{21}, $2p^{-l/2}$ as our bound for x_{32} and x_{42}, and $2p^{-(r-t)}$ as our bound for x_{43}, we get total volume

$$Ap^{-5k/2-l+3t},$$

completing this case.

Now suppose that we are in the case where we cannot apply Proposition 10 to inequality [5-4]. Then $v_p(x_{31}) = r-1$. We now consider two subcases. First, suppose that $v_p(x_{31}) \neq v_p(x_{32})$. Then inequality [5-2] implies that $v_p(x_{21}) \ge k - v_p(x_{31}) > k-r$, which holds on a set of x_{21} of volume at most $p^{-(k-r)}$. We use $2p^{-k/2}$ as the bound for the volume of x_{31} satisfying inequality [5-4]. Now using the same argument given above, the volume of x_{41} satisfying these inequalities is at most $6p^{-(k-2t)}$. Combining these estimates gives total volume bounded by

$$Ap^{-5k/2-l+3t},$$

completing this case.

Finally, suppose that $v_p(x_{31}) = v_p(x_{32}) = r-1$. Now for fixed x_{32}, x_{43}, the total volume of x_{42} satisfying inequality [5-6] is at most $p^{-(l-r)}$. We use $2p^{-(k-l)}$ as the bound on the volume of x_{21} satisfying inequality [5-1], $2p^{-k/2}$ as the bound on the volume of x_{31}, $2p^{-(r-l)}$ as our bound on the volume of x_{32}, and $2p^{-(r-t)}$ as the bound on the volume of x_{43}. Using the same argument given above, we can use $6p^{-(k-2t)}$ as our bound on the volume of x_{41}. This gives total bound

$$Ap^{-5k/2-l+r+3t},$$

completing step I.

Step II. Here, we consider an appropriate average of the previous inequalities to prove the theorem. The constants attached to these inequalities do not affect the convergence of the sums we consider so we will suppress them. By Lemma 14 and step I, we have

$$\mu_p \le p^{-2k-l},$$

$$\mu_p \le p^{-3k/2-3l/2+t},$$

$$\mu_p \le p^{-2k-l-r+3t},$$

and

$$\mu_p \le p^{-5k/2-l+r+3t}.$$

This means for all $n \geq 1$

$$\begin{aligned}\mu_p \leq & \left\{ \left(p^{-3k/2-3l/2+t}\right) \left(p^{-2k-l-r+3t}\right)^3 \left(p^{-5k/2-l+r+3t}\right)^2 \left(p^{-2k-l}\right)^n \right\}^{1/(n+6)} \\ = & p^{-\left(2+\frac{1}{2(n+6)}\right)k-\left(1+\frac{1}{2(n+6)}\right)l-\frac{r}{n+6}+\frac{16t}{n+6}}.\end{aligned}$$

Setting $n = 11$ gives the result. □

We now state several results for odd primes p.

Proposition 15. *Let p be odd. Suppose that $k, l, r, t \geq 0$. Then there is a polynomial $B \in \mathbb{R}[x]$ with positive coefficients such that*

$$\mu_p(k;l;r;t) \leq B(k)p^{-(2+\frac{1}{20})k-(1+\frac{1}{20})l-\frac{r}{20}+\frac{9t}{20}}.$$

Proof. We have two steps:

Step I. Here, we show that the following three inequalities hold:

$$\mu_p(k;l;r;t) \leq Bp^{-2k-3l/2-r+3t},$$

$$\mu_p(k;l;r;t) \leq Bp^{-3k-l+r+3t},$$

and

$$\mu_p(k;l;r;t) \leq Bp^{-5k/2-3l/2+3t}. \tag{14}$$

We will use (14) in the proof of Theorem 17. We proceed as follows. Inequality [5-1] holds on a set x_{21} of volume at most the minimum of $2p^{-k/2}$ and $2p^{-(k-l)}$. Inequality [5-3] holds on a set x_{32} of volume at most the minimum of $2p^{-l/2}$ and $2p^{-(l-r)}$. Inequality [5-8] holds on a set of x_{43} of volume at most $2p^{-(r-t)}$. For any fixed x_{21} and x_{32}, inequality [5-4] holds on a set of x_{31} of volume at most the minimum of $2p^{-k/2}$ and $6p^{-(k-r)}$. For any fixed x_{32}, x_{43} inequality [5-9] holds on a set of x_{42} of volume at most $6p^{-(l-t)}$. For any fixed $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$, inequality [5-10] holds on a set of x_{41} of volume at most $6p^{-(k-t)}$. Hence the total volume is bounded by

$$Bp^{-(k-t)} \cdot p^{-(l-t)} \cdot p^{-(r-t)} \cdot p^{-k/2} \cdot p^{-l/2} \cdot p^{-k/2},$$

by

$$Bp^{-(k-t)} \cdot p^{-(l-t)} \cdot p^{-(r-t)} \cdot p^{-(k-l)} \cdot p^{-(l-r)} \cdot p^{-(k-r)},$$

and by

$$Bp^{-(k-t)} \cdot p^{-(l-t)} \cdot p^{-(r-t)} \cdot p^{-k/2} \cdot p^{-l/2} \cdot p^{-(k-r)}.$$

Simplification gives the result.

Step II. Here, we consider an appropriate average of the previous inequalities to prove the theorem. As constants play no role, we ignore them. By Lemma 14 and step I, we have

$$\mu_p \leq p^{-2k-l},$$

$$\mu_p \leq p^{-2k-3l/2-r+3t},$$

and

$$\mu_p \leq p^{-3k-l+r+3t}.$$

This means for all $n \geq 1$

$$\begin{aligned}\mu_p \leq & \left\{ \left(p^{-2k-3l/2-r+3t}\right)^2 \left(p^{-3k-l+r+3t}\right) \left(p^{-2k-l}\right)^n \right\}^{1/(n+3)} \\ = & p^{-(2+\frac{1}{n+3})k-(1+\frac{1}{n+3})l-\frac{r}{n+3}+\frac{9t}{n+3}}.\end{aligned}$$

Setting $n = 17$ gives the result. □

Proposition 16. *Let p be odd. Then for any k, l, r, with $k + l + r \geq 2$, we have*

$$\mu_p(k; l; r; 0) \leq Cp^{-(2+\frac{1}{7})k-(1+\frac{1}{7})l-\frac{r}{7}-\frac{8}{7}}$$

for some constant $C > 0$.

Proof. We have two basic steps:

Step I. Here, we will show that $\mu_p \leq Cp^{-2k-l-2}$ whenever $k + l + r \geq 2$. We first note that Proposition 10 implies that inequality [5-8] holds on a set of x_{43} of volume at most $2p^{-(r-t)} = 2p^{-r}$. Inequality [5-3] holds on a set of x_{32} of volume at most $2p^{-\lceil l/2 \rceil}$.

Proposition 9 implies that inequality [5-1] holds on a set of x_{21} of volume at most $2p^{-\lceil k/2 \rceil}$. For fixed x_{21}, x_{32}, Proposition 9 implies that the total volume of x_{31} satisfying inequality [5-4] is at most $2p^{-\lceil k/2 \rceil}$.

For fixed $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$, inequality [5-10] can be written as

$$k + l + r \leq v_p(x_{22}x_{33}x_{41}(x_{41} - x_{44}) - z),$$

for some $z \in \mathbb{Z}_p$. Proposition 10 implies that this holds on a set of x_{41} of volume at most $6p^{-k}$.

Therefore, our total volume is at most

$$Cp^{-k-2\lceil k/2 \rceil - l - \lceil l/2 \rceil - r},$$

for some $C > 0$. If $r + \lceil l/2 \rceil \geq 2$, we are done. Therefore, suppose $r = 0$ and $l \in \{0, 1, 2\}$ or $r = 1$ and $l = 0$.

First, suppose $r = 0$. Then Proposition 10 implies that inequality [5-3] holds on a set of x_{32} of volume at most $2p^{-l}$. For fixed x_{21}, x_{32}, Proposition 10 implies that inequality [5-4] holds on a set of x_{31} of volume at most $6p^{-k}$. Using the above bounds for x_{42} and x_{41}, our total volume is now bounded by

$$Cp^{-2k-\lceil k/2 \rceil - 2l}.$$

Since $k + l \geq 2$, we have $\lceil k/2 \rceil + l \geq 2$ unless $l = 0$ and $k = 2$. In this case, we use $2p^{-k}$ as a bound for the volume of x_{21} satisfying inequality $[5 - 1]$, which completes this case.

Now suppose $r = 1$ and $l = 0$. Proposition 10 implies that the volume of x_{21} satisfying inequality $[5 - 1]$ is at most $2p^{-k}$. For fixed x_{21}, x_{32}, Proposition 9 implies that the total volume of x_{31} satisfying inequality $[5 - 4]$ is at most $2p^{-\lceil k/2 \rceil}$. We use the same bounds for the volume of x_{43} and x_{41}. Our total volume is now bounded by

$$Cp^{-2k-\lceil k/2 \rceil - 1}.$$

Since $k + l + r \geq 2$, we have $k \geq 1$ and our bound is at most Cp^{-2k-2}, completing the proof.

Step II. This step is very similar to the last step of the proof of Theorem 15. We have by the above and the second step of the proof of Theorem 15

$$\mu_p \le p^{-2k-l-2},$$

$$\mu_p \le p^{-2k-3l/2-r},$$

and

$$\mu_p \le p^{-3k-l+r}.$$

This means for all $n \ge 1$

$$\begin{aligned}\mu_p \le & \left\{ \left(p^{-2k-3l/2-r}\right)^2 \left(p^{-3k-l+r}\right) \left(p^{-2k-l-2}\right)^n \right\}^{1/(n+3)} \\ = & p^{-\left(2+\frac{1}{n+3}\right)k-\left(1+\frac{1}{n+3}\right)l-\frac{r}{n+3}-\frac{2n}{n+3}}.\end{aligned}$$

Setting $n = 4$ gives the result. □

We can similarly handle the case where $t = 1$.

Proposition 17. *Let p be odd. Then for any k, l, r with* $k + l + r \ge 1$*, we have*

$$\mu_p(k; l; r; 1) \le Dp^{-(2+\frac{1}{18})k-(1+\frac{1}{9})l-\frac{r}{9}-\frac{1}{9}},$$

for some constant $D > 0$*.*

Proof. We have two main steps:

Step I. Here, we will show that the volume is bounded by

$$Dp^{-2k-l-1}.$$

We recall that inequality [5-1] holds on a set of x_{21} of volume at most the minimum of $2p^{-\lceil k/2\rceil}$ and $2p^{-(k-l)}$. Similarly, inequality [5-3] holds on set x_{32} of volume at most the minimum of $2p^{-\lceil l/2\rceil}$ and $2p^{-(l-r)}$. We also have that inequality [5-8] holds on a set of x_{43} of volume at most the minimum of $2p^{-\lceil r/2\rceil}$ and $2p^{-(r-t)} = 2p^{-(r-1)}$.

For any fixed values of x_{21}, x_{32}, we see that inequality [5-4] holds on a set of x_{31} of volume at most the maximum of $2p^{-\lceil k/2\rceil}$ and $6p^{-(k-r)}$. For any fixed values of x_{32}, x_{43}, we see that inequality [5-9] holds on a set of x_{42} of volume at most the maximum of $2p^{-\lceil l/2\rceil}$ and $6p^{-(l-1)}$. For any fixed values of $x_{21}, x_{31}, x_{32}, x_{42}, x_{43}$, we can write inequality [5-10] as $k \le v_p(x_{41}(x_{41} - x_{44}) - z)$, for some $z \in \mathbb{Z}_p$. This holds on a set of x_{41} of volume at most the maximum of $2p^{-\lceil k/2\rceil}$ and $6p^{-(k-1)}$.

We now combine these inequalities to get bounds on the total volume satisfying inequalities [5-1] through [5-10]. Note that if $k - l \ge \lceil k/2\rceil$ and $l - r \ge \lceil l/2\rceil$, then $k - r \ge \lceil k/2\rceil$. By using $2p^{-\lceil k/2\rceil}$ as the bound for the volume of x_{21} and x_{31}, and $2p^{-(l-r)}$ as the bound for x_{32}, we see that our total volume is bounded by

$$Dp^{-k-2l-2\lceil k/2\rceil+3}.$$

Therefore, we are done if $l \ge 4$, or if $l \ge 3$ and k is odd. Suppose that this is not the case.

Suppose that $l \le 3$. Using $2p^{-\lceil l/2\rceil}$ instead of $2p^{-(l-r)}$ as our bound for the volume of x_{32}, our total bound is now

$$Dp^{-k-2\lceil k/2\rceil-l-\lceil l/2\rceil-r+3}.$$

Therefore, we are done if $\lceil l/2 \rceil + r \geq 4$, or $\lceil l/2 \rceil + r \geq 3$ and k is odd. Suppose that these conditions do not hold.

First, suppose that $l = 3$. Then $r \leq 1$. We can use $2p^{-\lceil r/2 \rceil}$ as a bound for the total volume of x_{43} satisfying inequality [5-8] instead of $2p^{-(r-1)}$. We use $2p^{-(l-r)}$ as our bound for the volume of x_{32} satisfying inequality [5-3]. We see that our total volume is bounded by

$$Dp^{-k-2\lceil k/2 \rceil -3-3+r-\lceil r/2 \rceil +2} = Dp^{-k-2\lceil k/2 \rceil -4+r-\lceil r/2 \rceil}.$$

Since $r \leq 1$, this is at most $Dp^{-2k-l-1}$, completing this case.

Now suppose that $l \leq 2$. For fixed x_{32}, x_{43}, Proposition 9 implies that the total volume of x_{42} satisfying inequality [5-9] is at most $2p^{-\lceil l/2 \rceil}$. We use this bound instead of $6p^{-(l-1)}$. Our total volume is now bounded by

$$Dp^{-k-2\lceil k/2 \rceil -2\lceil l/2 \rceil -r+2},$$

and we are done unless $r \leq 2$. In this case $\lceil r/2 \rceil \geq r-1$, so we use $2p^{-\lceil r/2 \rceil}$ as our bound for the volume of x_{43} satisfying inequality [5-8]. Now our bound is

$$Dp^{-k-2\lceil k/2 \rceil -2\lceil l/2 \rceil -\lceil r/2 \rceil +1}.$$

First, suppose $r = 2$. Then if l is odd or k is odd, we are done. If $l = 0$, then we can use $2p^{-k}$ as our bound for the volume of x_{21} satisfying inequality [5-1], giving

$$Dp^{-2k-\lceil k/2 \rceil},$$

as our bound. Therefore, we are done unless $k = 0$. In this case, $k = l = 0$, we have that the total volume is at most the total volume of x_{43} satisfying inequality [5-9], which is at most $2p^{-1}$, which completes this case.

Now, suppose $r = l = 2$. This is the most difficult case to consider. If k is odd then $2\lceil k/2 \rceil = k+1$, and we are done. If $k \geq 6$, then we can use $2p^{-(k-l)}$ as our bound for x_{21}, which is enough to complete this case. If $k = 0$, then we use 1 as our bound for x_{41} instead of $6p^{-(k-1)}$, and our total bound is Dp^{-l-1}, completing this case. We now must consider $k = 2$ and $k = 4$.

First, suppose $k = 2$. We need a bound of Dp^{-7}. Using $2p^{-\lceil k/2 \rceil}$ as our bound for x_{21}, x_{31}, x_{41}, $2p^{-\lceil l/2 \rceil}$ as our bound for x_{32} and x_{42}, and $2p^{-\lceil r/2 \rceil}$ as our bound for x_{43}, we get a bound of Dp^{-6}. Since $l = k = 2$ inequality [5-1] becomes $2v_p(x_{21}) \geq 2$ and inequality [5-3] becomes $2v_p(x_{32}) \geq 2$. If either of these variables has valuation greater than 1, then we will have the upper bound that we need. Therefore, we need only consider the case where $v_p(x_{21}) = v_p(x_{32}) = 1$. Inequality [5-2] now implies that $v_p(x_{31} - x_{32}) \geq 1$. Therefore, $v_p(x_{31}) \geq 1$, and we note that if $v_p(x_{32}) \geq 2$, we will have our bound. Therefore, we suppose that $v_p(x_{31}) = 1$. Finally, we consider inequality [5-4]. We have $v_p\left(x_{22}\left(x_{31}^2 - x_{31}x_{33}\right)\right) = 4 = k + l$, but $v_p\left(x_{21}\left(x_{32}^2 - x_{32}x_{33}\right)\right) = 3 < k + l$, so this case cannot occur.

When $k = 4$ we will argue similarly. We need a bound of Dp^{-11}. Using $2p^{-\lceil k/2 \rceil}$ as our bound for x_{21} and x_{31}, $6p^{-(k-1)}$ as our bound for x_{41}, $2p^{-\lceil l/2 \rceil}$ as our bound for x_{32} and x_{42}, and $2p^{-\lceil r/2 \rceil}$ as our bound for x_{43}, we get a bound of Dp^{-10}. Since $l = r = 2$, inequality [5-8] becomes $2v_p(x_{43}) \geq 2$ and inequality [5-3] becomes $2v_p(x_{32}) \geq 2$. If either of these variables has valuation greater than 1, then we will have the bound that we need. Therefore, we need only consider the case where $v_p(x_{43}) = v_p(x_{32}) = 1$. Inequality [5-6] now implies that $v_p(x_{42} - x_{43}) \geq 1$. Therefore, $v_p(x_{42}) \geq 1$, and we note that if $v_p(x_{42}) \geq 2$, we will have our bound. Therefore, we suppose that $v_p(x_{42}) = 1$. Finally, we consider inequality [5-9]. We have $v_p\left(x_{33}\left(x_{42}^2 - x_{42}x_{43}\right)\right) = 4 = l+r$, but $v_p\left(x_{32}\left(x_{43}^2 - x_{43}x_{44}\right)\right) = 3 < l + r$, so this case cannot occur.

Next, suppose $l \leq 2$ and $r = 1$. We have the bound

$$Dp^{-k-2\lceil k/2\rceil-2\lceil l/2\rceil}.$$

If $l = 1$, we are done. Suppose $l = 2$. Then we can use $2p^{-l}$ as our bound for the volume of x_{32} satisfying inequality [5-3], and we are done. If $l = 0$, then we can use $2p^{-k}$ as the bound for x_{21} satisfying inequality [5-1], and our bound is

$$Dp^{-2k-\lceil k/2\rceil},$$

which completes this case unless $k = 0$. If $k = l = 0$ and $r = t = 1$, then our total volume is at most the volume of x_{43} satisfying inequality [5-8], which is $2p^{-1}$, and we are done.

Finally, suppose $r = 0$ and $l \leq 2$. We can use $2p^{-l}$ as our bound for the volume of x_{32} satisfying inequality [5-3], and for fixed x_{21}, x_{32}, we use $6p^{-k}$ as our bound for the volume of x_{31} satisfying inequality [5-4]. We also use $2p^{-\lceil k/2\rceil}$ as our bound for the volume of x_{41} satisfying inequality [5-10]. Our total volume is now bounded by

$$Dp^{-2k-\lceil k/2\rceil-l-\lceil l/2\rceil}.$$

Since $k + l + r \geq 1$, we are done.

Step II. Again, we do an averaging. We have the inequalities

$$\mu_p \leq p^{-2k-l-1},$$

$$\mu_p \leq p^{-2k-3l/2-r+3},$$

and

$$\mu_p \leq p^{-5k/2-3l/2+3}.$$

The last two inequalities are from step II of the proof of Theorem 15 for $t = 1$. This means for all $n \geq 1$

$$\begin{aligned}\mu_p \leq & \left\{\left(p^{-2k-3l/2-r+3}\right)\left(p^{-5k/2-3l/2+3}\right)\left(p^{-2k-l-1}\right)^n\right\}^{1/(n+2)} \\ =& p^{-\left(2+\frac{1}{2(n+2)}\right)k-\left(1+\frac{1}{n+2}\right)l-\frac{r}{n+2}+\frac{6-n}{n+2}}.\end{aligned}$$

We set $n = 7$ to get the result. □

Remark 8. The case by case analysis of the small values of parameters in the proofs of Theorems 16 and 17 can be avoided if instead one uses the results of [19] for $f_n\left(p^k\right)$ for small k. In [19], these values are worked out for k up to 5. This is not sufficient for our purposes, but computing the missing data is not difficult using the results of Liu. Here, we chose instead to present the above elementary treatment to make the argument self-contained.

Remark 9. The choices of the parameter n in the proofs of Theorems 14, 15, 16, and 17 are made to optimize the error estimate in Theorem 14.

Counting orders of $\mathbb{Z}^5$

In this section, we prove the following theorem:

Theorem 14. *There is a polynomial P_5 of degree 9 such that for all $\epsilon > 0$*

$$N_5(B) = BP_5(\log B) + O\left(B^{\frac{33}{34}+\epsilon}\right)$$

as $B \to \infty$.

Proof. By Theorem 9, it suffices to prove the following statement: for $\sigma > \frac{33}{34}$ the expression

$$\sum_p \sum_{m\geq 2} \frac{a^{<}_{\mathbb{Z}^4}(p^m)}{p^{m\sigma}}$$

converges.

In our analysis, we will ignore all constants as they will have no bearing on convergence. We write

$$\sum_p \sum_{m\geq 2} \frac{a^{<}_{\mathbb{Z}^4}(p^m)}{p^{m\sigma}} = \sum_{m\geq 2} \frac{a^{<}_{\mathbb{Z}^4}(2^m)}{2^{m\sigma}} + \sum_{p\text{odd}} \sum_{m\geq 2} \frac{a^{<}_{\mathbb{Z}^4}(p^m)}{p^{m\sigma}}.$$

If we use Proposition 14, we see very easily that the first piece converges for $\sigma > \frac{33}{34}$. So we concentrate on the sum corresponding to the odd primes. We will show that for $m \geq 2$ and p odd, we have

$$a^{<}_{\mathbb{Z}^4}(p^m) \leq A(m)p^{-1+\frac{19}{20}m} \tag{15}$$

for a polynomial $A(m)$.

It is clear that this will be sufficient for the proof of the theorem. In order to prove (15), we write

$$\begin{aligned}
a^{<}_{\mathbb{Z}^4}(p^m) &= \sum_{k+l+r+t=m} p^{3k+2l+r}\mu_p(k;l;r;t) \\
&= \sum_{t=2}^{m} \sum_{k+l+r=m-t} p^{3k+2l+r}\mu_p(k;l;r;t) \\
&\quad + \sum_{k+l+r=m-1,t=1} p^{3k+2l+r}\mu_p(k;l;r;t) \\
&\quad + \sum_{k+l+r=m,t=0} p^{3k+2l+r}\mu_p(k;l;r;t) \\
&\leq \sum_{t=2}^{m} \sum_{k+l+r=m-t} p^{3k+2l+r}p^{-(2+1/20)k-(1+1/20)l-r/20+9t/20} \\
&\quad + \sum_{k+l+r=m-1} p^{3k+2l+r}p^{-(2+1/18)k-(1+1/9)l-r/9-1/9} \\
&\quad + \sum_{k+l+r=m,t=0} p^{3k+2l+r}p^{-(2+1/7)k-(1+1/7)l-r/7-8/7}
\end{aligned}$$

by Propositions 15, 16, 17, after ignoring some polynomials in terms of k, l, r, t as coefficients. Next,

$$
\begin{aligned}
a^{<}_{\mathbb{Z}^4}(p^m) &\leq \sum_{t=2}^{m} p^{9t/20} p^{(1-1/20)(m-t)} \sum_{k+l+r=m-t} 1 \\
&\quad + p^{-1/9} p^{(1-1/18)(m-1)} \sum_{k+l+r=m-1} 1 + p^{-8/7} p^{(1-1/7)m} \sum_{k+l+r=m} 1 \\
&\leq p^{-1+(1-1/20)m} + p^{-19/18+(1-1/18)m} + p^{-8/7+(1-1/7)m}
\end{aligned}
$$

after ignoring some polynomials. Now, the result follows. □

The following statement is a consequence of the inequality (15):

Corollary 2. *For each* $\epsilon > 0$

$$f(k) \ll_\epsilon k^{\frac{33}{34}+\epsilon} \prod_{p|k} p^{-1}.$$

If k is odd, then for each $\epsilon > 0$*,*

$$f(k) \ll_\epsilon k^{\frac{19}{20}+\epsilon} \prod_{p|k} p^{-1}.$$

Remark 10. Using Proposition 14 for odd primes instead of Proposition 15 in the proof of Theorem 14 would have produced a weaker error term.

Orders of $\mathbb{Z}^d$ for $d > 5$

In this section, we prove part 2 of Theorem 6. The idea is to find non-trivial volume bounds for $\mathcal{M}_5(p)$, and then use an inductive argument to obtain bounds for $\mathcal{M}_d(p)$ for $d > 5$.

We begin by defining $\mathcal{M}_5(p)$.

Lemma 15. *$\mathcal{M}_5(p)$ is the collection of 5×5 lower triangular matrices with entries in $\mathbb{Z}_p$*

$$
\begin{pmatrix}
x_{11} & & & & \\
x_{21} & x_{22} & & & \\
x_{31} & x_{32} & x_{33} & & \\
x_{41} & x_{42} & x_{43} & x_{44} & \\
x_{51} & x_{52} & x_{53} & x_{54} & x_{55}
\end{pmatrix}
$$

whose entries satisfy:

[6-1] $\quad v_p(x_{11}) \leq v_p(x_{21}(x_{21} - x_{22}))$

[6-2] $\quad v_p(x_{11}) \leq v_p(x_{21}(x_{31} - x_{32}))$

[6-3] $\quad v_p(x_{22}) \leq v_p(x_{32}(x_{32} - x_{33}))$

[6-4] $\quad v_p(x_{11}) + v_p(x_{22}) \leq v_p(x_{22}x_{31}(x_{31} - x_{33}) - x_{21}x_{32}(x_{32} - x_{33}))$

[6-5] $\quad v_p(x_{11}) \leq v_p(x_{21}(x_{41} - x_{42}))$

[6-6] $\quad v_p(x_{22}) \leq v_p(x_{32}(x_{42} - x_{43}))$

[6-7] $\quad v_p(x_{11}) + v_p(x_{22}) \leq v_p(x_{22}x_{31}(x_{41} - x_{43}) - x_{21}x_{32}(x_{42} - x_{43}))$

[6-8] $\quad v_p(x_{33}) \leq v_p(x_{43}(x_{43} - x_{44}))$

[6-9] $\quad v_p(x_{22}) + v_p(x_{33}) \leq v_p(x_{33}x_{42}(x_{42} - x_{44}) - x_{32}x_{43}(x_{43} - x_{44}))$

[6-10] $\quad v_p(x_{11}) + v_p(x_{22}) + x_{33} \leq v_p(x_{22}x_{33}x_{41}(x_{41} - x_{44}) - x_{22}x_{31}x_{43}(x_{43} - x_{44}) - x_{21}x_{33}x_{42}(x_{42} - x_{44}) + x_{21}x_{32}x_{43}(x_{43} - x_{44}))$

[6-11] $\quad v_p(x_{11}) \leq v_p(x_{21}(x_{51} - x_{52}))$

[6-12] $v_p(x_{22}) \le v_p(x_{32}(x_{52} - x_{53}))$
[6-13] $v_p(x_{11}) + v_p(x_{22}) \le v_p(x_{22}x_{31}(x_{51} - x_{33}) - x_{21}x_{32}(x_{52} - x_{53}))$
[6-14] $v_p(x_{33}) \le v_p(x_{43}(x_{53} - x_{54}))$
[6-15] $v_p(x_{22}) + v_p(x_{33}) \le v_p(x_{33}x_{42}(x_{52} - x_{54}) - x_{32}x_{43}(x_{53} - x_{54}))$
[6-16] $v_p(x_{11}) + v_p(x_{22}) + x_{33} \le v_p(x_{22}x_{33}x_{41}(x_{51} - x_{54}) - x_{22}x_{31}x_{43}(x_{53} - x_{54}) - x_{21}x_{33}x_{42}(x_{52} - x_{54}) + x_{21}x_{32}x_{43}(x_{53} - x_{54}))$
[6-17] $v_p(x_{44}) \le v_p(x_{54}(x_{54} - x_{55}))$
[6-15] $v_p(x_{33}) + v_p(x_{44}) \le v_p(x_{44}x_{53}(x_{53} - x_5) - x_{43}x_{54}(x_{54} - x_{55})$
[6-19] $v_p(x_{22}) + v_p(x_{33}) + x_{44} \le v_p(x_{33}x_{44}x_{52}(x_{52} - x_{55}) - x_{33}x_{42}x_{54}(x_{54} - x_{55}) - x_{32}x_{44}x_{53}(x_{53} - x_{55}) + x_{32}x_{43}x_{54}(x_{54} - x_{55}))$
[6-20] $v_p(x_{11}) + v_p(x_{22}) + v_p(x_{33}) + v_p(x_{44}) \le v_p(x_{22}x_{33}x_{44}x_{51}(x_{51} - x_{55}) - x_{22}x_{33}x_{41}x_{54}(x_{54} - x_{55}) - x_{22}x_{31}x_{44}x_{53}(x_{53} - x_{55}) + x_{22}x_{31}x_{43}x_{54}(x_{54} - x_{55}) - x_{21}x_{33}x_{44}x_{52}(x_{52} - x_{55}) - x_{21}x_{33}x_{42}x_{54}(x_{54} - x_{55}) - x_{21}x_{32}x_{44}x_{53}(x_{53} - x_{55}) + x_{21}x_{32}x_{43}x_{54}(x_{54} - x_{55}))$

We omit the proof.

As usual, after multiplying by appropriate units, we can assume that $x_{11} = p^{k_1}$, $x_{22} = p^{k_2}$, $x_{33} = p^{k_3}$, $x_{44} = p^{k_4}$, and $x_{55} = p^{k_5}$.

We now give a bound for $\mu_p(k_1, k_2, k_3, k_4, k_5)$.

Proposition 18. *For odd prime p,*

$$\mu_p(k_1, k_2, k_3, k_4, k_5) \le c \cdot p^{-(\frac{5}{2}+\frac{1}{6})k_1-(\frac{3}{2}+\frac{1}{6})k_2-(\frac{1}{2}+\frac{1}{6})k_3-(\frac{1}{2}-\frac{2}{6})k_4+\frac{2}{6}k_5}$$

where c is a polynomial in $k_1, \ldots, k_5$.

Proof. First, we show the following three inequalities:

$$\mu_p \le c_1 \cdot p^{-3k_1-\frac{3}{2}k_2-k_3+k_5} =: A \tag{16}$$

$$\mu_p \le c_2 \cdot p^{-\frac{5}{2}k_1-\frac{3}{2}k_2-\frac{1}{2}k_3-\frac{1}{2}k_4} =: B \tag{17}$$

$$\mu_p \le c_3 \cdot p^{-\frac{5}{2}k_1-2k_2-\frac{1}{2}k_3} =: C \tag{18}$$

where c_1, c_2, c_3 are polynomials in $k_1, \ldots, k_5$.

To show (1), we see that inequality [6-1] holds on a set of x_{21} of volume at most $2p^{-k_1/2}$ by Proposition 9. We see that [6-4] holds on a set of x_{31} of volume at most $2p^{-k_1/2}$ by Proposition 9. The combined volume of x_{41} and x_{54} satisfying [6-16] is at most $(k_1+1)p^{-k_1}$ by Proposition 8. The volume of x_{51} satisfying [6-20] is at most $6p^{-k_1+k_5}$ by Proposition 10. The volume of x_{32} satisfying [6-3] is at most $2p^{-k_2/2}$ by Proposition 9. The volume of x_{42} satisfying [6-9] is at most $2p^{-k_2/2}$ by Proposition 9. The volume of x_{52} satisfying [6-19] is at most $2p^{-k_2/2}$ by Proposition 9. The volume of x_{43} satisfying [6-8] is at most $2p^{-k_3/2}$ by Proposition 9. The volume of x_{53} satisfying [6-18] is at most $2p^{-k_3/2}$ by Proposition 9. Multiplication gives@

$$\mu_p \le c_1 \cdot p^{-3k_1-\frac{3}{2}k_2-k_3+k_5} = A.$$

To show (2), we see that inequality [6-1] holds on a set of x_{21} of volume at most $2p^{-k_1/2}$ by Proposition 9. The combined volume of x_{31} and x_{43} satisfying [6-7] is at most $(k_1 + 1)p^{-k_1}$ by Proposition 7. The volume of x_{41} satisfying [6-10] is at most $2p^{-k_1/2}$ by Proposition 9. The volume of x_{51} satisfying [6-20] is at most $2p^{-k_1/2}$ by Proposition 9.

The volume of x_{32} satisfying [6-3] is at most $2p^{-k_2/2}$ by Proposition 9. The volume of x_{42} satisfying [6-9] is at most $2p^{-k_2/2}$ by Proposition 9. The volume of x_{52} satisfying [6-19] is at most $2p^{-k_2/2}$ by Proposition 9. The volume of x_{53} satisfying [6-18] is at most $2p^{-k_3/2}$ by Proposition 9. The volume of x_{54} satisfying [6-17] is at most $2p^{-k_4/2}$ by Proposition 9. Multiplication gives

$$\mu_p \le c \cdot p^{-\frac{5}{2}k_1 - \frac{3}{2}k_2 - \frac{1}{2}k_3 - \frac{1}{2}k_4} = B.$$

To show (3), we see that inequality [6-1] holds on a set of x_{21} of volume at most $2p^{-k_1/2}$ by Proposition 9. The volume of x_{31} satisfying [6-4] is at most $2p^{-k_1/2}$ by Proposition 9. The combined volume of x_{41} and x_{54} satisfying [6-16] is at most $(k_1+1)p^{-k_1}$ by Proposition 8. The volume of x_{51} satisfying [6-20] is at most $2p^{-k_1/2}$ by Proposition 9. The combined volume of x_{32} and x_{43} satisfying [6-6] is at most $(k_2+1)p^{-k_2}$ by Proposition 8. The volume of x_{42} satisfying [6-9] is at most $2p^{-k_2/2}$ by Proposition 9. The volume of x_{52} satisfying [6-19] is at most $2p^{-k_2/2}$ by Proposition 9. The volume of x_{53} satisfying [6-18] is at most $2p^{-k_3/2}$ by Proposition 9. Multiplication gives

$$\mu_p \le c \cdot p^{-\frac{5}{2}k_1 - 2k_2 - \frac{1}{2}k_3} = C.$$

Lastly, we note that $\mu_p \le \min\{A, B, C\}$ implies that

$$\mu_p \le (ABC)^{1/3} = c \cdot p^{-(\frac{5}{2}+\frac{1}{6})k_1 - (\frac{3}{2}+\frac{1}{6})k_2 - (\frac{1}{2}+\frac{1}{6})k_3 - (\frac{1}{2}-\frac{2}{6})k_4 + \frac{2}{6}k_5}$$

giving the result. □

Proposition 19. *Suppose $n \ge 5$. Then there is $C \in \mathbb{R}[k_1, \ldots, k_5]$ such that*

$$\mu_p(k_1, \ldots, k_d) \le Cp^{-A_d(p) - \sum_{j=6}^{d}(d-j)\left\lceil \frac{k_j}{2} \right\rceil}$$

with

$$A_d(p) = \left(\frac{d}{2}+\frac{1}{6}\right)k_1 + \left(\frac{d-2}{2}+\frac{1}{6}\right)k_2 + \left(\frac{d-4}{2}+\frac{1}{6}\right)k_3 + \left(\frac{d-4}{2}-\frac{1}{6}\right)k_4 + \left(\frac{d-5}{2}-\frac{2}{6}\right)k_5$$

for p odd, and

$$A_d(p) = \left(\frac{d}{2}+\frac{1}{34}\right)k_1 + \left(\frac{d-2}{2}+\frac{1}{34}\right)k_2 + \left(\frac{d-4}{2}+\frac{1}{17}\right)k_3 + \left(\frac{d-4}{2}-\frac{16}{17}\right)k_4 + \left(\frac{d-5}{2}\right)k_5$$

for $p = 2$.

Proof. The proof is by induction on d. Since C will not affect the convergence of the sums, we consider we do not compute it. The lemma will follow from Theorem 14 and Theorem 15 if we show that

$$\mu_p(k_1; \ldots; k_d) \le 2^{d-1} p^{-\sum_{j=1}^{d-1}\left\lceil \frac{k_j}{2} \right\rceil} \mu_p(k_1, \ldots, k_{d-1}). \tag{19}$$

In order to see this inequality, observe that if

$$M = \begin{pmatrix} p^{k_1} & 0 & \ldots & 0 \\ x_{21} & p^{k_2} & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 \\ x_{d1} & \ldots & \ldots & p^{k_d} \end{pmatrix} \in \mathcal{M}_d(p; k_1, \ldots, k_d)$$

then for the matrix obtained by removing the last row

$$M' = \begin{pmatrix} p^{k_1} & 0 & \dots & 0 \\ x_{21} & p^{k_2} & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 \\ x_{d-1\,1} & \dots & \dots & p^{k_{d-1}} \end{pmatrix} \in \mathcal{M}_{d-1}(p; k_1, \dots, k_{d-1}).$$

The inequality (19) will follow if we show that the fibers of the map $M \mapsto M'$ have volume bounded by

$$2^{d-1} p^{-\sum_{j=1}^{d-1} \left\lceil \frac{k_j}{2} \right\rceil}.$$

As usual, we set

$$v_j = (x_{j1}, \dots, x_{jj}, 0, \dots, 0).$$

Suppose $v_1, \dots, v_{d-1}$ are the rows of M'. We now bound the volume of the set of vectors v_d with $x_{dd} = p^{k_d}$ such that

$$v_d \circ v_d = c_1 v_1 + \dots + c_d v_d$$

with $c_i \in \mathbb{Z}_p$. It is clear that $c_d = x_{dd}$. We then see that for $1 \le j \le d-1$

$$x_{dj}^2 - x_{dd} x_{dj} = c_j x_{jj} + \sum_{k=j+1}^{d-1} c_k x_{kj}.$$

If c_k, x_{kj} are given for $j+1 \le k \le d$, then the existence of such a a c_j is equivalent to

$$v_p \left(x_{dj}^2 - x_{dd} x_{dj} - \sum_{k=j+1}^{d-1} c_k x_{kj} \right) \ge k_j.$$

Proposition 9 implies that the volume of x_{dj} is bounded by $2p^{-\lceil k_j/2 \rceil}$. Induction will give the result. □

We can now prove part 2 of Theorem 6:

Proof. We will prove this theorem for $\mathbb{Z}^{d+1}$. We will show that the abscissa of convergence of $\zeta^{<}_{\mathbb{Z}^d}(s)$ is less than or equal to $\frac{d-1}{2} - \frac{1}{6}$. Recall

$$\zeta^{<}_{\mathbb{Z}^d}(s) = \prod_p \sum_{k_1, \dots, k_d \ge 0} p^{\sum_{j=1}^d (d-j) k_j} p^{-s \sum_{j=1}^d k_j} \mu_p(k_1, \dots, k_d).$$

It is not hard to see that by Lemma 19 the factor corresponding to $p = 2$ converges for $\sigma = \Re(s) > \frac{d-1}{2} - \frac{1}{6}$. For the remainder of this proof, we will write $\sum_p$ for $\sum_{p \text{odd}}$. It remains to prove the convergence of the series

$$\begin{aligned} &\sum_p \sum_{k_1 + \dots + k_d \ge 1} p^{\sum_{j=1}^d (d-j) k_j} p^{-\sigma \sum_{j=1}^d k_j} \mu_p(k_1, \dots, k_d) \\ =&\sum_p \sum_{k_1 + \dots + k_d = 1} p^{\sum_{j=1}^d (d-j) k_j} p^{-\sigma \sum_{j=1}^d k_j} \mu_p(k_1, \dots, k_d) \\ &+ \sum_{p \text{odd}} \sum_{k_1 + \dots + k_d \ge 2} p^{\sum_{j=1}^d (d-j) k_j} p^{-\sigma \sum_{j=1}^d k_j} \mu_p(k_1, \dots, k_d). \end{aligned}$$

By Lemma 10

$$\sum_{k_1+\ldots+k_d=1} p^{\sum_{j=1}^d (d-j)k_j} p^{-\sigma\sum_{j=1}^d k_j} \mu_p(k_1,\ldots,k_d) = \binom{d+1}{2} p^{-\sigma}.$$

and $\sum_p \binom{d+1}{2} p^{-\sigma}$ converges for all $\sigma > 1$. By Theorem 18, we see that the other summand is bounded by

$$\begin{aligned}
&\sum_p \sum_{k_1+\ldots+k_d\geq 2} p^{\sum_{j=1}^d (d-j)k_j} p^{-\sigma\sum_{j=1}^d k_j} \mu_p(k_1,\ldots,k_d) \\
&\quad\leq \sum_p \sum_{k_1+\ldots+k_d\geq 2} p^{\sum_{j+1}^d (d-j)k_j} p^{-\sigma\sum_{j=1}^d k_j} p^{-A_d-\sum_{j=5}^d (d-j)\left\lceil \frac{k_j}{2}\right\rceil} \\
&\quad\leq \sum_p \sum_{k_1+\ldots+k_d\geq 2} p^{B_d+\frac{1}{2}\sum_{j=5}^d (d-j)k_j} p^{-\sigma\sum_{j=1}^d k_j}
\end{aligned}$$

where

$$B_d = \left(\frac{d}{2}-1-\frac{1}{6}\right)(k_1+k_2+k_3) + \left(\frac{d}{2}-2+\frac{1}{6}\right)k_4 + \left(\frac{d}{2}-2-\frac{1}{6}\right)k_5.$$

Our series is now bounded by

$$\begin{aligned}
&\sum_p \sum_{k_1+\ldots+k_d\geq 2} p^{\left(\frac{d}{2}-1-\frac{1}{6}-\sigma\right)\sum_{j=1}^{d-1} k_j} p^{-\sigma k_d} \\
&\quad= \sum_p \sum_{m+k_d\geq 2} C_d(m) p^{\left(\frac{d}{2}-1-\frac{1}{6}-\sigma\right)m} p^{-\sigma k_d}
\end{aligned}$$

where $C_d(m)$ is the number of solutions to $\sum_{j=1}^{d-1} k_j = m$ for $m \geq 0$. Since $C_d(m)$ is a polynomial in m, this series converges if and only if

$$\sum_p \sum_{m+k_d\geq 2} p^{\left(\frac{d}{2}-1-\frac{1}{6}-\sigma\right)m} p^{-\sigma k_d}$$

converges. The subseries consisting of $m=0, k_d \geq 2$ converges if $\sigma > \frac{1}{2}$. If $k_d = 0, m \geq 2$, the series converges for $\sigma > \frac{d-1}{2} - \frac{1}{6}$. If $m, k_d \geq 1$ then the series converges if $\sigma > \frac{d}{4} - \frac{1}{12}$. The theorem is now immediate. □

We state the following corollary of the proof for future reference.

Corollary 3. *Let $d \geq 6$. There is a polynomial D such that for all primes p and all natural numbers l we have*

$$a_{\mathbb{Z}^d}^{1,<}\left(p^l\right) \leq D(l) p^{\left(\frac{d}{2}-\frac{5}{3}\right)l}.$$

Consequently, for each $\epsilon > 0$, we have

$$a_{\mathbb{Z}^d}^{1,<}(k) \ll_\epsilon k^{\frac{d}{2}-\frac{5}{3}+\epsilon}.$$

The proof of Theorems 1 and 2

In this section, we present a proof of Theorems 4 and 5 which finish the proof of our main result, Theorem 2. Let $K/\mathbb{Q}$ be an arbitrary extension of degree n which we assume to be

$K = \mathbb{Q}(\alpha)$ for α a root of an irreducible polynomial $f(x) \in \mathbb{Z}[x]$. We want to find a finite set S of primes and $\sigma_0(n) \in \mathbb{R}$ such that the double series

$$\sum_{p \notin S} \sum_{k \geq 2} \frac{a^{1,<}(p^k)}{p^{k\sigma}}$$

converges for $\sigma > \sigma_0(n)$. We show that $\sigma_0(5) = 19/20$ works, and for $n > 5$, $\sigma_0(n) = n/2 - 7/6$ works.

We choose an integral basis for $K/\mathbb{Q}$ which we will fix throughout; in particular, this basis provides an integral basis for $K \otimes \mathbb{Q}_p$ over $\mathbb{Q}_p$. By Equation (3) we have

$$\zeta^{1,<}_{\mathcal{O}_K \otimes \mathbb{Z}_p, p}(s) = (1 - p^{-1})^{-n} \int_{\mathcal{M}^1_p(K)} |x_{11}|^{s-n} |x_{22}|^{s-n+1} \cdots |x_{nn}|^{s-1} \, dM. \tag{20}$$

where we have written $\mathcal{M}^1_p(K)$ instead of the relevant $\mathcal{M}^1_p(\beta)$.

Definition 6. If $\underline{k} = (k_1, \ldots, k_n)$ is a n-tuple of non-negative integers, we set

$$\mathcal{M}^1_p(K; \underline{k}) = \left\{ M = \begin{pmatrix} p^{k_1} & 0 & \ldots & 0 \\ x_{21} & p^{k_2} & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 \\ x_{n1} & \ldots & x_{n\,n-1} & p^{k_n} \end{pmatrix} \in \mathcal{M}^1_p(K) \right\}.$$

We define $\mu^1_p(K, \underline{k})$ to be the $\frac{n(n-1)}{2}$-dimensional volume of $\mathcal{M}^1_p(K; \underline{k})$.

The basic observation is that $\mathcal{M}^1_p(K, \underline{k})$ is given by a cone condition. The set $\mathcal{M}_p(K; \underline{k})$ is given by cone conditions. To define the set $\mathcal{M}^1_p(K, \underline{k})$, we have to add the condition that the sublattice generated by the rows contains the identity element. Let $e \in \mathbb{Z}_p^n$ be the image of the identity element of $\mathcal{O}_K \otimes \mathbb{Z}_p$ under the identification of the latter with $\mathbb{Z}_p^n$. Write

$$M = \begin{pmatrix} p^{k_1} & 0 & \ldots & 0 \\ x_{21} & p^{k_2} & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 \\ x_{n1} & \ldots & x_{n\,n-1} & p^{k_n} \end{pmatrix}$$

and let the rows of the matrix M be $v_1, \ldots, v_n$. Then $M \in \mathcal{M}^1_p(K; \underline{k})$ if there are $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_p^n$ such that $\sum_i \alpha_i v_i = e$. This is equivalent to saying

$$(\alpha_1, \cdots, \alpha_n) M = e,$$

or what is the same

$$e.M^{-1} \in \mathbb{Z}_p^n.$$

Since M is a lower triangular matrix, this last statement is equivalent to a collection of p-adic inequalities of the form considered in section 'Application to some volume computation'.

Let S be a large finite set of primes containing all primes lying above 2 and all ramified primes; after enlarging S if necessary, we may assume that any $p \notin S$ is good in the sense of section 'Resolutions with good reduction'. Let $\mathfrak{p}$ be the set of primes $p \notin S$ which are split in the number field K. Clearly, $\mathfrak{p}$ is an infinite set of primes.

It is easy to see that

$$\zeta^{1,<}_{\mathcal{O}_K\otimes\mathbb{Z}_p,p}(s) = \sum_{\substack{\underline{k}=(k_1,\ldots,k_n)\\ k_i\geq 0,\forall i}} p^{\sum_{i=1}^n (n-i)k_i} p^{-s\sum_{i=1}^n k_i} \mu^1_p(K,\underline{k}). \tag{21}$$

Let $p \in \mathfrak{p}$. For each m

$$a^{1,<}_{\mathcal{O}_K\otimes\mathbb{Z}_p}(p^m) = \sum_{\substack{\underline{k}=(k_1,\ldots,k_n)\\ k_i\geq 0,\forall i,\sum_i k_i=m}} p^{\sum_{i=1}^n (n-i)k_i} \mu^1_p(K,\underline{k}).$$

First, we consider $n = 5$. We start with the observation that by Equation (15) for $m \geq 0$

$$a^{1,<}_{\mathbb{Z}_p^5}(p^m) = a^{<}_{\mathbb{Z}_p^4}(p^m) \leq A(m)p^{-1+19m/20}$$

for a polynomial $A(m)$. On the other hand, since

$$a^{1,<}_{\mathbb{Z}_p^5}(p^m) = \sum_{k+l+r+t+u=m} p^{4k+3l+2r+t}\mu^1_p(k;l;r;t;u)$$

we have

$$p^{4k+3l+2r+t}\mu^1_p(k;l;r;t;u) \leq A(k,l,r,t,u)p^{-1+19(k+l+r+t+u)/20}$$

whenever $k + l + r + t + u \geq 2$, for some polynomial $A(k,l,r,t,u)$. Thus,

$$\mu^1_p(k,l,r,t,u) \leq A(k,l,r,t,u)p^{-1}p^{-(3+1/20)k-(2+1/20)l-(1+1/20)r-t/20+19u/20}.$$

In the terminology of section 'Application to some volume computations', this means that $\mathcal{M}^1_p(K)$ is $(1,\underline{\alpha},A)$-narrow with

$$\underline{\alpha} = (3 + 1/20, 2 + 1/20, 1 + 1/20, 1/20, -19/20)$$

and some polynomial A. Now, Theorem 8 implies that there is a finite set T of primes such that for $p \notin T$ the set $\mathcal{M}^1_p(K)$ is $(1,\alpha,A)$-narrow. Reversing the process, we get

$$a^{1,<}_{\mathcal{O}_K}(p^m) \leq B(m)p^{-1+19m/20} \tag{22}$$

for some polynomial $B(m)$. Clearly, this implies that

$$\sum_{p\notin T}\sum_{m\geq 2}\frac{a^{1,<}_{\mathcal{O}_K}(p^m)}{p^{m\sigma}}$$

converges for $\sigma > 19/20$. This shows that $\sigma_0(5) = 19/20$ works. The proof of the statement that $\sigma_0(n) = n/2 - 7/6$ works for $n \geq 6$ follows the same reasoning, except that we use Corollary 3. This finishes the proof of the theorem.

The following corollary is immediate from Equation (22). This is an improvement of Theorem 8.1 of [3].

Corollary 4. *For any quintic field K and any prime number p, we have*

$$\sum_{m\geq 1}\frac{a^{1,<}_{\mathcal{O}_K}(p^m)}{p^{2m}} = O\left(\frac{1}{p^{2+\frac{1}{20}}}\right).$$

As in the introduction, we set

$$a^{1,<}(n,m) = \max_{K/\mathbb{Q}\text{extension of degree } n} a^{1,<}_{\mathcal{O}_K}(m).$$

We have the following corollary:

Corollary 5. *We have*

$$\limsup_{m\to\infty} \frac{\log a^{1,<}(5,m)}{\log m} \leq \frac{19}{20}.$$

For $n \geq 6$, *we have*

$$\limsup_{m\to\infty} \frac{\log a^{1,<}(n,m)}{\log m} \leq \frac{n}{2} - \frac{5}{3}.$$

In particular,

$$\limsup_{n\to\infty} \frac{1}{n} \limsup_{m\to\infty} \frac{\log a^{1,<}(n,m)}{\log m} \leq \frac{1}{2}.$$

Endnote

[1] We learned Galois' theorem from a question posted by Chandan Singh Dalawat on `mathoverflow`, and comments by Matt Emerton, Jack Chapman, and Jack Schmidt.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

This work owes a great deal of intellectual debt to Ricky Liu's paper [19]. This paper has its genesis in the Princeton senior thesis [18]. The first author wishes to acknowledge support from a National Science Foundation Graduate Research Fellowship. The second author wishes to acknowledge support from the National Science Foundation (Award number DMS-0701753), a grant from the National Security Agency (Award number 111011), and a Collaboration Grant from the Simons Foundation (Award number 245977). In the course of the preparation of this work, we benefited from conversations with Nir Avni, Manjul Bhargava, Alice Medvedev, Alireza Salehi-Golsefidi, and Christopher Voll. We wish to thank Bhama Srinivasan for useful conversations, and especially for her crucial observation Lemma 1, and Eun Hye Lee for numerical computations on UIC's Argo cluster to provide support for Equation (1). Thanks are also due to the referee for reading the paper very carefully, and for pointing out errors and inconsistencies that have led to the improvement of the paper.

Author details

[1]Department of Mathematics, Yale University, PO Box 208283, 06520-8283, New Haven, CT, USA. [2]Department of Mathematics, California Institute of Technology, 1200 East California Blvd, 91125, Pasadena, CA, USA. [3]Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, 851 S Morgan St (M/C 249), 60607, Chicago, IL, USA.

Received: 14 August 2014 Accepted: 15 April 2015
Published online: 10 June 2015

References

1. Bhargava, M: Higher composition laws. IV. The parametrization of quintic rings. Ann. Math. **167**(1), 53–94 (2008)
2. Bhargava, M: The density of discriminants of quintic rings and fields. Ann. Math. **172**(3), 1559–1591 (2010)
3. Brakenhoff, JF: Counting problems for number rings. pp. 116. Thesis (Ph.D.)-Leiden University. (2009). Available at. [http://www.math.leidenuniv.nl/scripties/proefschrift-brakenhoff.pdf]
4. Burnside, W: Theory of groups of finite order. 2nd ed., Dover Publications, Inc., xxiv+512 pp (1955)
5. Chambert-Loir, A, Tschinkel, Y: Fonctions zêta des hauteurs des espaces fibrés. Rational points on algebraic varieties. Progr. Math. Birkhä, user Basel. **199**, 71–115 (2001)
6. Datskovsky, B, Wright, DJ: The adelic zeta function associated with the space of binary cubic forms. II: Local theory. J. Reine Angew. Math. **367**, 27–75 (1986)
7. Denef, J: The rationality of the Poincaré, series associated to the p-adic points on a variety. Invent. Math. **77**, 1–23 (1984)
8. Denef, J: On the degree of Igusa's local zeta function. Amer. J. Math. **109**(6), 991–1008 (1987)
9. Dixon, JD, Mortimer, B: Permutation groups Graduate Texts in Mathematics. 163. Springer-Verlag, New York (1996). xii+346 pp
10. du Sautoy, M, Grunewald, F: Analytic properties of zeta functions and subgroup growth. Ann. Math. **152**(3), 793–833 (2000)
11. du Sautoy, M, Grunewald, F: Zeta functions of groups and rings. In: International Congress of Mathematicians. Vol. II, pp.131–149. Eur. Math. Soc., Zürich (2006)
12. du Sautoy, M, Taylor, G: The zeta function of $\mathfrak{sl}_2$ and resolution of singularities. Math. ProcCamb. Phil. Soc. **132**(1), 57–73 (2002)
13. du Sautoy, M, Woodward, L: Zeta functions of groups and rings. Lecture Notes in Mathematics, 1925. Springer-Verlag, Berlin, xii+208 pp (2008)
14. Grunewald, FJ, Segal, D, Smith, GC: Subgroups of finite index in nilpotent groups. Invent. Math. **93**, 185–223 (1988)
15. Huppert, B: Endliche Gruppen I. pp. xii+793. Springer-Verlag, Berlin-New York (1967)

16. Igusa, J-I: Some observations on higher degree characters. Amer. J. Math. **99**(2), 393–417 (1977)
17. Igusa, J-I: An introduction to the theory of local zeta functions. AMS/IP Stud. Adv. Math. 14, Amer. Math. Soc., Providence, RI, International Press, Cambrigde, MA (2002)
18. Kaplan, N: P-adic integration and subrings of $\mathbb{Z}^n$. Princeton University, Department of Mathematics, Princeton, NJ (2007)
19. Liu, R: Counting subrings of $\mathbb{Z}^n$ of index k. J. Combin. Theory Ser. A. **114**(2), 278–299 (2007)
20. Lubotzky, A, Segal, D: Subgroup growth. In: Progress in Mathematics, 212. pp. xxii+453. Birkhäuser Verlag, Basel (2003)
21. Macintyre, A: On definable subsets of p-adic fields. J. Symbolic Logic. **41**(3), 605–610 (1976)
22. Mueller, P: Permutation groups of prime degree, a quick proof of Burnsides theorem. Archiv der Mathematik. **85**(1), 15–17 (2005)
23. Murty, MR, Murty, VK: Non-vanishing of L-functions and applications. Progress in Mathematics, 157. pp. xii+196. Birkhäuser Verlag, Basel 1997
24. Nakagawa, J: Orders of a quartic field. Mem. Amer. Math. Soc. **122**(583), viii+75 pp (1996)
25. Neukirch, J: Class field theory. Grundlehren der Mathematischen Wissenschaften, 280. pp. viii+140 Springer-Verlag, Berlin 1986
26. Shalika, J, Takloo-Bighash, R, Tschinkel, Yu: Rational points on compactifications of semi-simple groups. J. Amer. Math. Soc. **20**(4), 1135–1186 (2007)
27. Voll, C: Functional equations for zeta functions of groups and rings. Ann. Math. **172**(2), 1181–1218 (2010)
28. Voll, C: A newcomer's guide to zeta functions of groups and rings. Lectures on profinite topics in group theory, 99-144, London Math. Soc. Stud. Texts, 77. Cambridge Univ. Press, Cambridge 2011

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Immediate publication on acceptance
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com