hexagon:2611.00436v1

Subrings and cotypes of truncated polynomial rings

Sarthak Chimni Ramin Takloo-Bighash

November 13, 2026

Abstract

We study unital finite-index subrings of $R_n = \mathbb{Z}[t]/(t^n)$. We compute the cubic cotype function and the quartic total and cocyclic functions at every prime, including the exceptional factors at 2, and prove the corresponding global counting theorems in degrees three, four, and five. Explicit Hermite sums with determinantal weights give full cotype formulas for $n = 4, 5$, without an asserted closed rational evaluation. We extend these calculations by a linear lifting recursion for every degree and by a two-parameter description of every cocyclic subring for $n \geq 4$. The latter gives $2 - 2/(n-1) \leq \alpha_n^{\mathrm{cc}} \leq 2$ for the global cocyclic convergence abscissa, and hence $\alpha_n^{\mathrm{cc}} \to 2$. An exact quadratic family of quintic diagonal counts gives absolute convergence of the residual Dirichlet series for $\mathrm{Re}\, s > 19/13$. All asymptotics are obtained by elementary summation and absolutely convergent convolution.

Contents

1 Introduction **2**
1.1 Main results and organization . . . 2

2 Lattice and summation preliminaries **2**
2.1 Cotypes and local lattices . . . 2
2.2 Triangular bases and local decomposition . . . 3
2.3 Smith invariants and congruence measures . . . 4
2.4 Elementary analytic tools . . . 5

3 The cubic cotype function **5**

4 Quartic local factors and counting functions **9**
4.1 All subrings . . . 9
4.2 Cocyclic subrings . . . 11
4.3 Asymptotics by absolutely convergent convolution . . . 13

5 Quintic counting functions **14**
5.1 Quintic closure in Hermite normal form . . . 15
5.2 A uniform bound for all quintic diagonal types . . . 17
5.3 The finite exceptional calculation . . . 19
5.3.1 A quadratic diagonal family . . . 20
5.3.2 Extraction of the global factors . . . 23
5.4 Exact enumeration of quintic cocyclic subrings . . . 24
5.4.1 A cyclic quotient parametrization . . . 24
5.4.2 Coefficients and rational functions . . . 25

5.5 Elementary passage to the counting functions 26

6 Cotype refinements in degrees four and five **27**
6.1 The normalized cotype integral 29

7 Lifting through the last annihilator **30**

8 Two parameters for cocyclic subrings in every degree **31**

A Finite comparisons and coefficient checks **33**
A.1 Supplementary checks 35

1 Introduction

1.1 Main results and organization

For $n \geq 2$, let $A_n(B)$ count the unital subrings of $R_n = \mathbb{Z}[t]/(t^n)$ of index at most B, and let $A_n^{\mathrm{cc}}(B)$ count those whose additive quotient is cyclic. The leading terms are summarized below; all constants displayed in the table are positive.

n	$A_n(B)$	$A_n^{\mathrm{cc}}(B)$	Result
3	$C_3 B(\log B)^2$	$D_3 B(\log B)^2$	Theorem 3.4
4	$K_4 B^{3/2}$	$K_4^{\mathrm{cc}} B^{3/2}$	Theorem 4.4
5	$C_5 B^{3/2}(\log B)^2$	$D_5 B^{3/2} \log B$	Theorems 5.1 and 5.2

Here $C_3 = 1/(12\zeta(2))$ and $D_3 = \frac{1}{12}\prod_p(1 - 3p^{-2} + 2p^{-3})$. The cited theorems give the other constants and the error terms. The proportion of cocyclic subrings has a positive limit in degrees three and four, but tends to zero in degree five.

Section 2 supplies the lattice and summation tools. Sections 3 and 4 treat degrees three and four. Section 5 contains the entire quintic argument, including the separate character calculation for cocyclic quotients. Sections 6 and 7 give exact cotype sums and a coefficient recursion in every degree. Section 8 describes every cocyclic local subring by two polynomial congruences and proves $2-2/(n-1) \leq \alpha_n^{\mathrm{cc}} \leq 2$, hence $\alpha_n^{\mathrm{cc}} \to 2$, for the global convergence abscissae. The rational evaluation of the full cotype sums and sharp asymptotics in degrees at least six are left open. Appendix A prints the complete finite enumeration used in the quintic convergence proof.

The authors thank Nathan Kaplan, Tobias Rossmann, and Christopher Voll for useful convervastions. We originally learned about this problem from [1]. The second author is partially supported by a collaboration grant from the Simons Foundation. The bulk of this work was included in the first author's doctoral thesis at the University of Illinois at Chicago. The work was further developed with assistance from ChatGPT. Access to ChatGPT 6 Astra was provided through OpenAI's ChatGPT for Academic Researchers program via Julius Ross, whom the authors thank.

2 Lattice and summation preliminaries

2.1 Cotypes and local lattices

Throughout, a subring contains the identity of the ambient ring. A *cocyclic* subring is one whose additive quotient is cyclic; the trivial quotient is included. A full lattice is an additive submodule

of finite index. For $n \geq 2$ put $R_n = \mathbb{Z}[t]/(t^n)$, $d = n-1$, and $N_{n,p} = t\mathbb{Z}_p[t]/(t^n)$. If $S \subset R_n$ has finite index, its additive quotient has uniquely determined invariant factors

$$R_n/S \cong \bigoplus_{i=1}^{d} \mathbb{Z}/\alpha_i(S)\mathbb{Z}, \qquad \alpha_{i+1}(S) \mid \alpha_i(S).$$

Trivial factors are included. There is a further trivial factor from the identity, which we suppress. Define

$$\mathcal{Z}_n(s_1, \ldots, s_d) = \sum_S \prod_{i=1}^{d} \alpha_i(S)^{-s_i}, \qquad Z_n(s) = \mathcal{Z}_n(s, \ldots, s).$$

Write $Z_n^{\mathrm{cc}}(s)$ for the same sum over subrings with cyclic additive quotient, and $a_n(q), a_n^{\mathrm{cc}}(q)$ for the respective coefficients. The quotient is only an additive group; no ideal condition on S is being imposed. Its *corank* is the minimum number of additive generators, equivalently the number of nontrivial invariant factors.

We use $v_p(p) = 1$, $v_p(0) = +\infty$, and $|x|_p = p^{-v_p(x)}$. For a residue modulo p^m, a valuation means the minimum of m and the valuation of a lift. The nilpotent algebra $N_{n,p}$ has rank $n-1$, whereas R_n has rank n; the words cubic, quartic, and quintic refer to $n = 3, 4, 5$.

For clarity, we distinguish the ordinary local generating function from the Dirichlet series:

$$\mathsf{Z}_{n,p}(T) = \sum_{m \geq 0} a_n(p^m) T^m, \qquad Z_{n,p}(s) = \mathsf{Z}_{n,p}(p^{-s}),$$

and use the superscript cc for their cocyclic counterparts. The local coefficients count unital $\mathbb{Z}_p$-subalgebras of finite index. The local cotype series $\mathcal{Z}_{n,p}$ is defined by the same invariant-factor weights as the global series.

2.2 Triangular bases and local decomposition

Every local subring with identity is uniquely written as $\mathbb{Z}_p \oplus L$ with L a full lattice in $N_{n,p}$ and $L^2 \subseteq L$. Indeed subtracting the constant coefficient of an element of the subring gives an element of L, and the converse follows by expanding products. Its index and nontrivial Smith invariants are those of $N_{n,p}/L$.

Lemma 2.1 (Row Hermite coordinates)**.** *Fix an ordered basis $e_1, \ldots, e_d$ of $\mathbb{Z}_p^d$. Every full lattice has a unique upper triangular row basis matrix $H = (h_{ij})$ satisfying*

$$h_{ii} = p^{a_i}, \qquad a_i \geq 0, \qquad 0 \leq h_{ij} < p^{a_j} \quad (i < j).$$

Its index is $p^{\sum_i a_i}$. For a fixed diagonal there are $p^{\sum_j (j-1)a_j}$ such lattices. The diagonal valuations need not be ordered.

Proof. The projection of a full lattice onto its first coordinate is a nonzero ideal $p^{a_1}\mathbb{Z}_p$. Choose a vector with first coordinate p^{a_1} and apply induction to the intersection with $\langle e_2, \ldots, e_d \rangle$. Subtract multiples of its successive basis rows, from left to right, to reduce the remaining coordinates of the first vector modulo $p^{a_2}, \ldots, p^{a_d}$. This constructs the asserted basis. The projection ideal and the intersection are intrinsic. Two reduced choices for the first row differ by a vector of the intersection, so successive coordinate comparison forces them to agree. Induction proves uniqueness. Successive reduction also gives unique quotient representatives with ith coordinate between 0 and $p^{a_i} - 1$, proving the index formula. There are $j-1$ freely chosen entries above the jth diagonal entry, proving the count. □

All lattice bases below are recorded as *rows* of their matrices. In the cubic and quartic local calculations we use decreasing powers of t, which gives a lower triangular display. Reversing both the ordered basis and the row order gives the upper triangular convention of Lemma 2.1; index and Smith invariants are unchanged.

The following lemma is well-known.

Lemma 2.2. *Finite-index subrings with identity of R_n correspond bijectively to collections of full lattices $L_p \subset N_{n,p}$ satisfying $L_p^2 \subseteq L_p$, with $L_p = N_{n,p}$ for all but finitely many primes. Consequently*

$$\mathcal{Z}_n(\boldsymbol{s}) = \prod_p \mathcal{Z}_{n,p}(\boldsymbol{s}), \quad Z_n(s) = \prod_p Z_{n,p}(s), \quad Z_n^{\mathrm{cc}}(s) = \prod_p Z_{n,p}^{\mathrm{cc}}(s).$$

These identities hold as coefficient identities and converge absolutely if $\min_i \operatorname{Re} s_i > d$.

2.3 Smith invariants and congruence measures

For $L \subset N_{n,p}$ write its invariant exponents as $\lambda_1 \geq \cdots \geq \lambda_d \geq 0$. We use also the formal notation

$$\mathcal{C}_{n,p}(X_1, \ldots, X_d) = \sum_{\substack{L \subseteq N_{n,p} \text{ full} \\ L^2 \subseteq L}} \prod_{i=1}^{d} X_i^{\lambda_i}; \qquad \mathcal{Z}_{n,p}(\boldsymbol{s}) = \mathcal{C}_{n,p}(p^{-s_1}, \ldots, p^{-s_d}).$$

Each coefficient is finite. The one-variable specialization is obtained by setting every $X_i = T$; the cocyclic specialization sets $X_1 = T$ and $X_2 = \cdots = X_d = 0$, with $0^0 = 1$. More generally, setting $X_{r+1} = \cdots = X_d = 0$ retains the subrings of corank at most r.

Lemma 2.3. *Let M be a full-rank $d \times d$ matrix over $\mathbb{Z}_p$. Set $\delta_0 = 0$ and let δ_j be the minimum valuation of its $j \times j$ minors. Then the decreasing invariant exponents of its row quotient are*

$$\lambda_i = \delta_{d-i+1} - \delta_{d-i} \quad (1 \leq i \leq d).$$

In particular these differences are nonnegative and occur in decreasing order.

Proof. Choose an entry of least valuation, move it to the first diagonal position, and multiply its row by a unit to make it a power of p. It divides every entry, so integral row and column operations clear its column and row. Iterating on the remaining block produces a diagonal matrix with entries $p^{e_1}, \ldots, p^{e_d}$ and $e_1 \leq \cdots \leq e_d$: after each clearing step all remaining entries are still divisible by the previous pivot. These operations are unimodular and preserve the quotient. They also preserve the ideal generated by the j-minors, by multilinearity (or the Cauchy–Binet identity), with equality following from the inverse operations. For the diagonal matrix that ideal is generated by $p^{e_1+\cdots+e_j}$. Hence $\delta_j = e_1 + \cdots + e_j$ and $\lambda_i = e_{d-i+1}$, proving the assertion. □

The same pivot argument applies to rectangular matrices: a matrix of rank r is equivalent, by invertible integral row and column operations, to a rectangular diagonal matrix with nonzero diagonal $p^{e_1}, \ldots, p^{e_r}$. In particular, for a matrix with r rows and rank r, the index of its column module in $\mathbb{Z}_p^r$ is $p^{e_1+\cdots+e_r}$, the power of p generated by its maximal minors. This is the form used for systems of linear congruences.

Normalized additive Haar measure on $\mathbb{Z}_p^k$ assigns measure p^{-ak} to each residue class modulo p^a. Thus a condition depending only on these residues has measure equal to its number of solutions divided by p^{ak}. Invertible integral linear changes preserve this measure. More generally an injective linear map with determinant of valuation b scales it by p^{-b}: Smith reduction reduces this assertion to multiplication of one coordinate by p^e. These facts justify all congruence-measure calculations below.

2.4 Elementary analytic tools

Lemma 2.4 (Absolutely convergent convolution)**.** *Let $b(n)$ be a sequence with summatory function $D(Y) = \sum_{n\le Y} b(n)$, and suppose $\sum_{d\ge 1} |h(d)|d^{-\beta} < \infty$ for some $\beta < \alpha$. Put $f(n) = \sum_{d|n} h(d)b(n/d)$ and $H(\alpha) = \sum_d h(d)d^{-\alpha}$. If $r \ge 1$ is an integer and*

$$D(Y) = cY^{\alpha}(\log Y)^r + O\big(Y^{\alpha}(\log(2Y))^{r-1}\big),$$

then

$$\sum_{n\le B} f(n) = cH(\alpha)B^{\alpha}(\log B)^r + O\big(B^{\alpha}(\log(2B))^{r-1}\big).$$

If instead $D(Y) = cY^{\alpha} + O(Y^{\gamma})$ with $\gamma < \beta < \alpha$, then

$$\sum_{n\le B} f(n) = cH(\alpha)B^{\alpha} + O(B^{\beta}).$$

The constants may depend on the sequences and the stated parameters.

Proof. Finite rearrangement gives $\sum_{n\le B} f(n) = \sum_{d\le B} h(d)D(B/d)$. For every fixed $j \ge 0$,

$$\sum_{d} |h(d)|d^{-\alpha}(\log d)^j < \infty,$$

because $d^{\beta-\alpha}(\log d)^j$ is bounded (with the constant monomial interpreted as 1 when $j = 0$). In the first case the summed error is $O(B^{\alpha}(\log(2B))^{r-1})$. Expanding $(\log B - \log d)^r$ shows that all nonleading terms have this same bound. Extending the leading sum from $d \le B$ to all d costs $O(B^{\beta}(\log B)^r)$, which is absorbed since $\beta < \alpha$. In the second case the summed error is at most

$$B^{\gamma} \sum_{d\le B} |h(d)|d^{-\gamma} \le B^{\beta} \sum_{d} |h(d)|d^{-\beta}.$$

The tail of the main term is bounded by $B^{\alpha}B^{\beta-\alpha}\sum_{d>B} |h(d)|d^{-\beta}$. This proves both assertions. □

3 The cubic cotype function

Separating Hermite forms according to their first determinantal divisor gives the cubic cotype formula. The resulting three elementary sums retain the Smith weights throughout. We write $\mathcal{C}_{3,p}(X, Y)$ for the two-variable series defined in Section 2.

Theorem 3.1 (Cubic cotype formula)**.** *For every prime p,*

$$\mathcal{C}_{3,p}(X, Y) = \frac{1 + X + pX^2 - pX^3Y - p^2X^4Y - p^2X^5Y}{(1 - XY)(1 - pX^2Y)(1 - p^2X^3)}. \tag{1}$$

Thus the local cotype Dirichlet series is obtained by setting $X = p^{-s_1}$ and $Y = p^{-s_2}$ wherever the defining sum converges absolutely.

Proof. The split augmentation $R_3 \otimes \mathbb{Z}_p = \mathbb{Z}_p 1 \oplus (t)$ is useful because subtracting the constant coefficient from an element of a unital subring stays inside that subring. Hence every such subring is $\mathbb{Z}_p 1 \oplus L$, with $L \subset (t)$ a full lattice closed under multiplication, as in Section 2.

In the ordered basis (t^2, t), the unique row Hermite normal form of L has rows

$$p^a t^2, \qquad ut^2 + p^b t, \qquad a, b \ge 0, \quad 0 \le u < p^a.$$

Here the range of u fixes representatives in $\mathbb{Z}_p/p^a\mathbb{Z}_p$. All products involving $p^a t^2$ vanish, whereas $(ut^2 + p^b t)^2 = p^{2b}t^2$. Consequently multiplication is closed if and only if

$$a \le 2b. \tag{2}$$

The index is p^{a+b}. Put $v_p(0) = +\infty$. The first determinantal divisor of the two-by-two matrix has valuation

$$k = \min\{a, b, v_p(u)\}.$$

The determinant has valuation $a + b$. The Smith normal form therefore gives $\lambda_2 = k$ and $\lambda_1 = a + b - k$.

To sum without losing this minimum, write $a = k + r$, $b = k + s$. Condition (2) becomes

$$r \le k + 2s.$$

For fixed k, r, s, the cotype monomial is $X^{k+r+s}Y^k$. If $\min(r, s) = 0$, it suffices that u be divisible by p^k, and there are p^r such residue classes modulo p^{k+r}. If $r, s \ge 1$, its valuation must be exactly k, and there are $(p-1)p^{r-1}$ such classes. These observations give a disjoint partition into $r = 0$, $s = 0 < r$, and $r, s \ge 1$.

The first two contributions are

$$U = \sum_{k,s\ge 0} X^{k+s}Y^k = \frac{1}{(1-X)(1-XY)},$$

$$V = \sum_{r\ge 1}\sum_{k\ge r} p^r X^{k+r}Y^k = \frac{pX^2Y}{(1-XY)(1-pX^2Y)}.$$

For the third contribution substitute $r = R + 1$, $s = S + 1$. Then $0 \le R \le k + 2S + 1$, so the finite geometric sum gives

$$\begin{aligned} W &= (p-1)X^2 \sum_{k,S\ge 0} (XY)^k X^S \sum_{R=0}^{k+2S+1} (pX)^R \\ &= \frac{(p-1)X^2}{1-pX}\left\{\frac{1}{(1-XY)(1-X)} - \frac{p^2X^2}{(1-pX^2Y)(1-p^2X^3)}\right\}. \end{aligned}$$

All rearrangements are valid formally, because only finitely many indices contribute to a prescribed total degree. For completeness, the cancellation in $U + V + W$ uses the polynomial identity

$$\begin{aligned} &(1-pX^3Y)(1-pX)(1-p^2X^3) \\ &\quad + (p-1)X^2\{(1-pX^2Y)(1-p^2X^3) - p^2X^2(1-X)(1-XY)\} \\ &= (1-pX)(1-X)(1+X+pX^2-pX^3Y-p^2X^4Y-p^2X^5Y), \end{aligned}$$

which follows by expansion. Dividing by $(1-pX)(1-X)(1-XY)(1-pX^2Y)(1-p^2X^3)$ proves (1). □

Corollary 3.2. *Let $Z_3(s)$ count all finite-index subrings with identity of R_3, and let $Z_3^{\mathrm{cc}}(s)$ count those with cyclic additive quotient. For* $\operatorname{Re} s > 1$,

$$Z_3(s) = \frac{\zeta(s)\zeta(2s-1)\zeta(3s-2)}{\zeta(4s-2)}, \tag{3}$$

$$Z_3^{\mathrm{cc}}(s) = \zeta(s)\zeta(2s-1)\zeta(3s-2)H(s), \tag{4}$$

$$H(s) = \prod_p \left(1 - p^{-2s} - p^{1-3s} + p^{1-4s} - p^{2-4s} + p^{2-5s}\right). \tag{5}$$

The Euler product defining H has an absolutely convergent Dirichlet-series expansion in $\operatorname{Re} s > 3/4$. *In particular, the number of cocyclic subrings of index p^e is*

$$a_3^{\mathrm{cc}}(p^e) = p^{\lfloor 2e/3 \rfloor} \qquad (e \geq 0). \tag{6}$$

Proof. In Theorem 3.1, put $X = Y = T$ to count by index, and put $X = T$, $Y = 0$ to retain precisely $\lambda_2 = 0$. They give, respectively,

$$\mathsf{Z}_{3,p}(T) = \frac{1 + pT^2}{(1-T)(1-p^2T^3)}, \qquad \mathsf{Z}_{3,p}^{\mathrm{cc}}(T) = \frac{1 + T + pT^2}{1 - p^2T^3}. \tag{7}$$

As a check independent of the cotype cancellation, the first equality also follows directly from

$$\sum_{b \geq 0} \sum_{a=0}^{2b} p^a T^{a+b} = \frac{1}{1-pT} \left(\frac{1}{1-T} - \frac{pT}{1-p^2T^3} \right).$$

The last expression reduces to the first expression in (7). Expanding the second one gives coefficients p^{2j}, p^{2j}, p^{2j+1} in degrees $3j$, $3j+1$, $3j+2$, proving (6).

By Lemma 2.2, the coefficient functions are multiplicative. Their Euler products converge absolutely for $\operatorname{Re} s > 1$: the total factor in (7) is bounded coefficientwise by $((1-T)(1-pT^2)(1-p^2T^3))^{-1}$, whose Euler product is $\zeta(s)\zeta(2s-1)\zeta(3s-2)$ and converges in that half-plane. The cocyclic coefficients are bounded by the total coefficients.

Now $1 + pT^2 = (1-p^2T^4)/(1-pT^2)$ proves (3). For the second factor, direct multiplication gives

$$(1 + T + pT^2)(1-T)(1-pT^2) = 1 - T^2 - pT^3 + (p-p^2)T^4 + p^2T^5.$$

This proves (4)–(5). At a real $\sigma > 3/4$, the sum over primes of the absolute values of the nonconstant local Dirichlet coefficients is bounded by

$$\sum_p (p^{-2\sigma} + p^{1-3\sigma} + (p+p^2)p^{-4\sigma} + p^{2-5\sigma}) < \infty.$$

Each exponent of p is strictly less than -1. The product of the corresponding local absolute sums is therefore finite. Expanding finite Euler products and passing monotonically to the product of absolute sums proves absolute convergence of the Dirichlet series, including the assertion about H. □

The coefficients of the three zeta factors in (3) and (4) are a weighted count of triples. Elementary summation of that count, followed by an absolutely convergent convolution, gives the asymptotics and their error terms.

Lemma 3.3. *Suppose $h(d)$ is a complex sequence with $\sum_{d \geq 1} |h(d)| d^{-\sigma_0} < \infty$ for some $\sigma_0 < 1$. If $f(n)$ are the Dirichlet coefficients of*

$$\zeta(s)\zeta(2s-1)\zeta(3s-2) \sum_{d \geq 1} h(d) d^{-s},$$

then, as $B \to \infty$,

$$\sum_{n \leq B} f(n) = \frac{B(\log B)^2}{12} \sum_{d \geq 1} \frac{h(d)}{d} + O_h(B \log(2B)).$$

Proof. First consider the three zeta factors alone. Their summatory coefficient function is

$$D(B) = \sum_{ab^2c^3 \le B} bc^2 = \sum_{b^2c^3 \le B} bc^2 \left\lfloor \frac{B}{b^2c^3} \right\rfloor .$$

Replacing the floor by its argument gives

$$D(B) = B \sum_{b^2c^3 \le B} \frac{1}{bc} + O\left(\sum_{c \le B^{1/3}} c^2 \sum_{b \le (B/c^3)^{1/2}} b \right).$$

For $Y \ge 1$, $\sum_{b \le Y} b \le Y^2$, so the error is at most $B \sum_{c \le B^{1/3}} 1/c = O(B \log(2B))$. For the main term put $C = B^{1/3}$. Integral comparison gives $\sum_{j \le Y} 1/j = \log Y + O(1)$ for $Y \ge 1$, and hence

$$\begin{aligned} \sum_{b^2c^3 \le B} \frac{1}{bc} &= \sum_{c \le C} \frac{1}{c} \left(\frac{1}{2} \log B - \frac{3}{2} \log c + O(1) \right) \\ &= \frac{1}{2} \log B \log C - \frac{3}{4} (\log C)^2 + O(\log(2B)) \\ &= \frac{1}{12} (\log B)^2 + O(\log(2B)). \end{aligned}$$

Here $\sum_{c \le C} (\log c)/c = \frac{1}{2}(\log C)^2 + O(1)$ also follows by integral comparison (the function is decreasing for $c > e$, with bounded variation on $[1, \infty)$). We have proved

$$D(B) = \frac{1}{12} B (\log B)^2 + O(B \log(2B)).$$

Apply Lemma 2.4 with $\alpha = 1$, $r = 2$, $c = 1/12$, and $\beta = \sigma_0$. This proves the claimed convolution asymptotic. □

Theorem 3.4. *Let $A_3(B)$ and $A_3^{\mathrm{cc}}(B)$ denote the numbers of all unital subrings and cocyclic unital subrings of R_3, respectively, of index at most B. Then*

$$\begin{aligned} A_3(B) &= \frac{1}{12\zeta(2)} B (\log B)^2 + O(B \log(2B)), \\ A_3^{\mathrm{cc}}(B) &= \frac{1}{12} \prod_p (1 - 3p^{-2} + 2p^{-3})\, B (\log B)^2 + O(B \log(2B)). \end{aligned}$$

Consequently the limiting proportion of cocyclic subrings exists and is the strictly positive number

$$\lim_{B \to \infty} \frac{A_3^{\mathrm{cc}}(B)}{A_3(B)} = \zeta(2) \prod_p (1 - 3p^{-2} + 2p^{-3}) = \prod_p \left(1 - \frac{2}{p(p+1)} \right).$$

Proof. For the total count, the correction factor is

$$\frac{1}{\zeta(4s-2)} = \sum_{d \ge 1} \mu(d) d^2 (d^4)^{-s},$$

whose absolute series converges when $\operatorname{Re} s > 3/4$. For the cocyclic count the same convergence was proved for $H(s)$ in Corollary 3.2. Choose any $\sigma_0 \in (3/4, 1)$ and apply Lemma 3.3 to each factorization. The correction factors at $s = 1$ are $1/\zeta(2)$ and $\prod_p (1 - 3p^{-2} + 2p^{-3})$, respectively. Every factor of the latter product is $(1 - p^{-1})^2 (1 + 2p^{-1}) > 0$, and the deviations from 1 are

summable. The product is therefore positive. Dividing the two asymptotics is legitimate. The alternative expression for the ratio follows, prime by prime, from

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

□

4 Quartic local factors and counting functions

Let $\mathsf{Z}_{4,p}(x)$ and $\mathsf{Z}^{\mathrm{cc}}_{4,p}(x)$ count, respectively, all subrings and cocyclic subrings of p-power index, with x recording the exponent of the index. A triangular basis gives explicit closure conditions and a determinantal test for cyclicity. The coefficient 2 in the square of the last basis element requires a separate calculation at the dyadic prime.

Lemma 4.1 (Quartic triangular coordinates)**.** *Every local subring has a unique basis consisting of* 1 *and*

$$v_1 = p^k t^3, \qquad v_2 = at^3 + p^l t^2, \qquad v_3 = ct^3 + bt^2 + p^r t,$$

where $k, l, r \geq 0$, $0 \leq a, c < p^k$, *and* $0 \leq b < p^l$. *The necessary and sufficient multiplicativity conditions are*

$$l \leq 2r, \qquad k \leq l + r, \qquad p^k \mid 2p^r b - p^{2r-l}a. \tag{8}$$

Its index is p^{k+l+r}. *Its additive quotient is cyclic if and only if at least one of*

$$p^{k+l}, \quad p^{k+r}, \quad p^{l+r}, \quad p^k b, \quad p^r a, \quad ab - p^l c \tag{9}$$

is a p*-adic unit.*

Proof. Subtracting the constant coefficient times 1 gives the direct sum of $\mathbb{Z}_p 1$ and a lattice in (t). Apply row Hermite normal form in the ordered basis (t^3, t^2, t); the stated residue ranges are precisely the uniqueness ranges for that form. The determinant gives the index. We have $v_1 v_i = 0$ for all i, $v_2^2 = 0$, and

$$v_2 v_3 = p^{l+r} t^3, \qquad v_3^2 = 2p^r b\, t^3 + p^{2r} t^2.$$

The first nonzero product belongs to the lattice exactly when $k \leq l + r$. For the second, the coefficient of v_3 must vanish, and the coefficient of v_2 is necessarily p^{2r-l}. It is integral exactly when $l \leq 2r$; the remaining t^3 coefficient gives the last condition in (8). These checks cover every product of basis vectors, so they are sufficient as well as necessary. Finally the quotient of a full rank three lattice is cyclic exactly when its matrix has rank at least two modulo p: in Smith normal form, at least two of its three diagonal entries must be units. Its possibly nonzero two-by-two minors are exactly those in (9), up to signs. This proves the last assertion. □

4.1 All subrings

Theorem 4.2. *Define*

$$\begin{aligned} N_p(x) &= 1 + px^2 + p^2x^3 - p^4x^5 - 2p^5x^6 - 2p^6x^7 - p^7x^8 \\ &\qquad + p^9x^{10} + p^{10}x^{11} + p^{11}x^{13}, \\ D_p(x) &= (1-x)(1-p^2x^2)(1-p^3x^3)(1-p^4x^4)(1-p^5x^6). \end{aligned}$$

For odd p,

$$\mathsf{Z}_{4,p}(x) = N_p(x)/D_p(x). \tag{10}$$

At $p = 2$ the answer is

$$\mathsf{Z}_{4,2}(x) = \frac{N_2(x)}{D_2(x)} + \frac{64x^6}{(1-4x^2)(1-8x^3)(1-16x^4)} = \frac{\widetilde{N}_2(x)}{D_2(x)}, \tag{11}$$

where N_2 means specialization of N_p and

$$\begin{aligned}\widetilde{N}_2(x) = 1 + 2x^2 + 4x^3 - 16x^5 - 192x^7 - 128x^8 \\ + 512x^{10} + 1024x^{11} - 2048x^{12} + 4096x^{13}.\end{aligned}$$

Proof. We compare the valuations of the two coefficients in the last condition of (8). On the admissible diagonal cone, write $\epsilon_p = v_p(2)$ and

$$h = \max\{0, k + l - r - \min(l + \epsilon_p, r)\}.$$

The number of bases with this diagonal is exactly

$$p^{2k+l-h}. \tag{12}$$

Here is a direct justification of this count. The homomorphism $(a, b) \mapsto 2p^r b - p^{2r-l}a \pmod{p^k}$ is well defined on $(\mathbb{Z}/p^k) \times (\mathbb{Z}/p^l)$: changing a by p^k changes the image by a multiple of p^k, and changing b by p^l does so because $k \le r + l$. Its image is the ideal modulo p^k generated by $p^{r+\epsilon_p}$ and p^{2r-l}, hence has cardinality p^h. Every fiber has equal cardinality; the free parameter c contributes p^k. This proves (12) without measure normalization.

For odd p, partition the cone into the five disjoint regions below. In the table the summand is $p^{2k+l-h}x^{k+l+r}$.

	region	value of h
F_1	$1 \le l \le r < k \le r + l$	$k - r$
F_2	$0 \le l \le r,\ 0 \le k \le r$	0
F_3	$r < l \le 2r,\ r < k \le r + l$	$k + l - 2r$
F_4	$r < l \le 2r,\ 2r - l < k \le r$	$k + l - 2r$
F_5	$r < l \le 2r,\ 0 \le k \le 2r - l$	0

Every entry is summed by the two elementary identities

$$\sum_{j=A}^{B} y^j = \frac{y^A - y^{B+1}}{1-y}, \qquad \sum_{j=A}^{\infty} y^j = \frac{y^A}{1-y}.$$

For completeness the intermediate differences, before cancelling the finite-geometric denominators, are

$$\begin{aligned}
F_1 &= \frac{px}{(1-px)(1-p^2x^2)}\left(\frac{p^3x^3}{1-p^3x^3} - \frac{p^4x^4}{1-p^4x^4}\right), \\
F_2 &= \frac{1}{(1-p^2x)(1-x)(1-px^2)} - \frac{p^2x}{(1-p^2x)(1-p^2x^2)(1-p^3x^3)}, \\
F_3 &= \frac{p^4x^5}{(1-px)(1-p^3x^3)(1-p^3x^4)} - \frac{p^6x^7}{(1-px)(1-p^4x^4)(1-p^5x^6)}, \\
F_4 &= \frac{p^3x^4}{(1-px)(1-p^3x^3)(1-p^2x^3)} - \frac{p^4x^5}{(1-px)(1-p^3x^3)(1-p^3x^4)}, \\
F_5 &= \frac{p^2x^3}{(1-p^2x)(1-px^2)(1-p^2x^3)} - \frac{p^4x^4}{(1-p^2x)(1-p^3x^3)(1-p^2x^3)}.
\end{aligned}$$

For example, the third region gives $\sum_{r\ge1}(p^2x)^r\sum_{l=r+1}^{2r}x^l\sum_{k=r+1}^{r+l}(px)^k$; applying the displayed finite identity first to k, then to l, and finally the infinite identity to r, gives F_3 above. The other four rows follow in the same order from their explicit bounds. Adding these five displayed rational expressions, putting them over a common denominator, and cancelling yields N_p/D_p. This last operation is a polynomial identity, so the apparently extra denominators $1-px$, $1-p^2x$, $1-px^2$, $1-p^2x^3$, and $1-p^3x^4$ introduce no poles into the answer.

At $p=2$ the value of h changes only on $1\le l<r<k\le l+r$. On this region the odd-prime value $h=k-r$ is replaced by $h=k-r-1$. Thus each such coefficient doubles, and one extra copy of the generic contribution is required. Its sum is

$$\sum_{l\ge1}(px)^l\sum_{r\ge l+1}(px)^r\sum_{k=r+1}^{r+l}(px)^k\Bigg|_{p=2}=\frac{p^6x^6}{(1-p^2x^2)(1-p^3x^3)(1-p^4x^4)}\Bigg|_{p=2}.$$

This proves the first expression in (11). Multiplication by D_2 adds $64x^6(1-x)(1-32x^6)$ to N_2, which gives the stated polynomial $\widetilde{N}_2$. □

4.2 Cocyclic subrings

Theorem 4.3. *For odd p put*

$$M_p(x)=1+x+(p^3-p^2)x^3-p^3x^4-p^4x^5.$$

Then

$$\mathsf{Z}^{\mathrm{cc}}_{4,p}(x)=\frac{M_p(x)}{(1-p^2x^2)(1-p^4x^4)}. \tag{13}$$

At $p=2$,

$$\mathsf{Z}^{\mathrm{cc}}_{4,2}(x)=\frac{\widetilde{M}_2(x)}{(1-4x^2)(1-16x^4)}, \tag{14}$$

where

$$\widetilde{M}_2(x)=1+x+4x^3-16x^4-16x^5+64x^6-64x^7+512x^9.$$

Proof. Impose the determinantal condition of Lemma 4.1 before summing over diagonals. Put $q=1-p^{-1}$. If $k=0$, then $a=c=0$. There is one choice when $l=0$, and p^lq choices when $1\le l\le 2r$, because b must be a unit. If $k>0$ and $l=0$, then $b=0$, $1\le k\le r$, and cyclicity says c is a unit. Thus there are $p^{2k}q$ choices. If $k,l>0$, then $r>0$ and the only potentially unit minor is $ab-p^lc$. Consequently a and b must both be units, and c is arbitrary.

Suppose p is odd. If $l<r$, the expression $2b-p^{r-l}a$ is a unit, so the allowed values are $k\le r$. If $l>r$, the expression $2p^{l-r}b-a$ is a unit, so the allowed values satisfy $k+l\le 2r$. If $l=r$ and $k\le l$, there is no additional constraint. In these three cases the count is $p^{2k+l}q^2$. Finally, when $l=r<k\le 2l$, we need $a\equiv 2b \pmod{p^{k-l}}$. Every unit b has p^l allowed lifts a, all units, so the count is $p^{k+2l}q$. These cases are exhaustive, including the zero diagonals.

Here are their geometric sums, in precisely the order just described:

$$A_1 = \sum_{r\ge 0} x^r + q\sum_{r\ge 1} x^r \sum_{l=1}^{2r}(px)^l = \frac{1+x+px^2}{1-p^2x^3},$$

$$A_2 = q\sum_{r\ge 1} x^r \sum_{k=1}^{r}(p^2x)^k = \frac{p(p-1)x^2}{(1-x)(1-p^2x^2)},$$

$$A_3 = q^2\sum_{r\ge 2} x^r \sum_{l=1}^{r-1}(px)^l \sum_{k=1}^{r}(p^2x)^k$$

$$= \frac{p(p-1)^2x^2}{(1-px)(1-p^2x)}\left(\frac{x^2}{1-x} - \frac{p^4x^4}{1-p^2x^2} - \frac{px^3}{1-px^2} + \frac{p^5x^5}{1-p^3x^3}\right),$$

$$A_4 = q^2\sum_{r\ge 2} x^r \sum_{l=r+1}^{2r-1}(px)^l \sum_{k=1}^{2r-l}(p^2x)^k = \frac{p^3(p-1)^2x^6}{(1-px^2)(1-p^3x^3)(1-p^2x^3)},$$

$$A_5 = q^2\sum_{l\ge 1}(px^2)^l \sum_{k=1}^{l}(p^2x)^k = \frac{p(p-1)^2x^3}{(1-px^2)(1-p^3x^3)},$$

$$A_6 = q\sum_{l\ge 1}(p^2x^2)^l \sum_{k=l+1}^{2l}(px)^k = \frac{p^3(p-1)x^4}{(1-p^3x^3)(1-p^4x^4)}.$$

Each equality is obtained by the finite and infinite geometric identities used above, with the written summation order; no estimate is used. Addition and multiplication by the common denominator show that $\sum A_i = M_p/((1-p^2x^2)(1-p^4x^4))$.

At $p=2$, compare the count with the odd-prime rational expression specialized to 2. The cases $k=0$ and $l=0$ do not change. For positive diagonals with $l \ge r$, $2^{l-r+1}b - a$ is odd; therefore $k+l \le 2r$ is necessary and sufficient. This removes precisely $A_6|_{p=2}$ from the generic expression. For $r \ge l+2$, $2b - 2^{r-l}a$ has valuation one, so one additional diagonal $k = r+1$ is allowed. Its total contribution is

$$G_1 = \sum_{l\ge 1}\sum_{r\ge l+2} 2^{2r+l}x^{2r+l+1} = \frac{128x^8}{(1-8x^3)(1-4x^2)}.$$

Indeed $l = 1+u$, $r = 3+u+v$ makes the summand $128x^8(8x^3)^u(4x^2)^v$. For $r = l+1$, the additional values are $k = l+2+j$, $0 \le j \le l-1$. The congruence is $a \equiv b \pmod{2^j}$. For $j=0$ it places no restriction on the two odd variables, giving 2^{3l+2} choices. For $j \ge 1$, each odd b has 2^{k-j} allowed a, so the count is 2^{3l+3+j}. Their contributions are

$$G_2 = \sum_{l\ge 1} 2^{3l+2}x^{3l+3} = \frac{32x^6}{1-8x^3},$$

$$G_3 = \sum_{j\ge 1}\sum_{l\ge j+1} 2^{3l+3+j}x^{3l+3+j} = \frac{1024x^{10}}{(1-16x^4)(1-8x^3)}.$$

For the last equality take $j = 1+u$, $l = 2+u+v$. There are no further changes. Hence

$$\mathsf{Z}^{\mathrm{cc}}_{4,2}(x) = \frac{M_2(x)}{(1-4x^2)(1-16x^4)} - \frac{8x^4}{(1-8x^3)(1-16x^4)} + G_1 + G_2 + G_3.$$

Here M_2 is the specialization of the polynomial M_p at $p=2$. A common denominator and cancellation of $1-8x^3$ give exactly (14), completing the count at every prime. □

4.3 Asymptotics by absolutely convergent convolution

The leading factor in both Euler products is $\zeta(2s-2)$, and uniformly for $Y \geq 1$,

$$\sum_{m \leq \sqrt{Y}} m^2 = \frac{1}{3} Y^{3/2} + O(Y).$$

Consequently the second part of Lemma 2.4 applies to $\zeta(2s-2)G(s)$ whenever G is absolutely convergent at some $1 < \beta < 3/2$. It gives leading constant $G(3/2)/3$ and error $O(B^{\beta})$.

Theorem 4.4. *Let $A_4(B)$ count all subrings of R_4 of index at most B, let $A_4^{\mathrm{cc}}(B)$ count its cocyclic subrings, and let $A_4^{\mathrm{cc,odd}}(B)$ impose in addition that the index is odd. For every $0 < \varepsilon < 1/6$,*

$$\begin{aligned} A_4(B) &= K_4 B^{3/2} + O_\varepsilon(B^{4/3+\varepsilon}), \\ A_4^{\mathrm{cc}}(B) &= K_4^{\mathrm{cc}} B^{3/2} + O_\varepsilon(B^{4/3+\varepsilon}), \\ A_4^{\mathrm{cc,odd}}(B) &= K_4^{\mathrm{cc,odd}} B^{3/2} + O_\varepsilon(B^{4/3+\varepsilon}), \end{aligned}$$

where the positive constants are

$$\begin{aligned} K_4 &= \frac{314 - 5\sqrt{2}}{768} \zeta(3/2)^2 \zeta(2) \zeta(4) \prod_{p \neq 2} N_p(p^{-3/2}), \\ K_4^{\mathrm{cc}} &= \frac{14 + 5\sqrt{2}}{48} \zeta(2) \prod_{p \neq 2} M_p(p^{-3/2}), \\ K_4^{\mathrm{cc,odd}} &= \frac{1}{8} \zeta(2) \prod_{p \neq 2} M_p(p^{-3/2}). \end{aligned}$$

The all-subring and both cocyclic Dirichlet series have a simple pole at $s = 3/2$ and no other singularity on that vertical line.

Proof. For all subrings the Euler product equals

$$\zeta(2s-2) G_4(s), \qquad G_4(s) = \zeta(s)\zeta(3s-3)\zeta(4s-4)\zeta(6s-5) H_4(s),$$

where $H_4(s) = \widetilde{N}_2(2^{-s}) \prod_{p \neq 2} N_p(p^{-s})$. The polynomial Euler product H_4 has an absolutely convergent Dirichlet expansion for $\Re s > 1$: for each of its finitely many nonconstant monomial types $p^a x^b$, the sum $\sum_p p^{a-b\sigma}$ converges for $\sigma > 1$. The four zeta factors in G_4 have absolutely convergent Dirichlet expansions for $\Re s > 4/3$. Consequently so does their product. For all cocyclic subrings,

$$G_4^{\mathrm{cc}}(s) = \zeta(4s-4) \widetilde{M}_2(2^{-s}) \prod_{p \neq 2} M_p(p^{-s})$$

is the residual factor after removing $\zeta(2s-2)$. The most restrictive monomial in the polynomial product is $p^3 x^3$; it gives absolute convergence for $\sigma > 4/3$. The zeta factor already converges for $\sigma > 5/4$. For odd indices replace $\widetilde{M}_2(2^{-s})$ in this expression by $(1 - 2^{2-2s})(1 - 2^{4-4s})$. This is a Dirichlet polynomial and therefore does not affect absolute convergence. Apply Lemma 2.4 with $\beta = 4/3 + \varepsilon$ to obtain all three estimates.

At $x = 2^{-3/2} = \sqrt{2}/4$, direct substitution gives

$$\widetilde{N}_2(x) = \frac{314 - 5\sqrt{2}}{256}, \qquad \widetilde{M}_2(x) = \frac{14 + 5\sqrt{2}}{16}, \qquad (1 - 4x^2)(1 - 16x^4) = \frac{3}{8}.$$

Inserting these values into $G(3/2)/3$ gives the constants displayed in the theorem. Every numerator Euler factor is positive at $3/2$, because it equals a positive counting series times its positive local denominator. Absolute convergence of the products then makes the products strictly positive. Finally G is holomorphic for $\Re s > 4/3$, and $\zeta(2s-2)$ has only its simple pole at $s = 3/2$ on the line in question. Since $G(3/2) > 0$, that pole does not cancel. □

Remark 4.5 (Dyadic boundaries and index restrictions). The dyadic factors must be calculated from the closure conditions with $v_2(2) = 1$. For example, the only diagonal triples at index 4 are $(k,l,r) = (0,0,2),(1,0,1),(0,1,1)$, contributing $1,4,2$. Thus the coefficient of x^2 in (11) is 7. For the cocyclic count, the case $r = l+1$ permits $k \le 2l+1$. The sums G_2, G_3 above retain this endpoint and treat an empty interval as contributing zero; in particular, (14) has coefficient 128 at x^6. The all-index and odd-index asymptotics differ by the local factor at 2: restricting to odd indices removes that factor from the Euler product. This changes the leading constant while preserving the exponent $3/2$.

Remark 4.6. The cubic and quartic computations above can also be done using Zeta [6]. We have included them here to motivate the method used to compute the quintic zeta functions which are not accessible toe Zeta.

5 Quintic counting functions

We now state the quintic total and cocyclic counting theorems. Their proofs use the closure conditions in Section 5.1, uniform bounds for all diagonal types, and exact counts for the exceptional types. An infinite quadratic family gives the convergence region $\operatorname{Re} s > 19/13$ for the residual total series. Throughout this section $R = R_5 = \mathbb{Z}[t]/(t^5)$; the notation $a_5(n)$, $a_5^{\mathrm{cc}}(n)$, Z_5, and Z_5^{cc} is as in Section 1. The total factorization is proved in Sections 5.2–5.3.2; the cocyclic factors are evaluated in Section 5.4. Section 5.5 completes both asymptotic proofs.

Theorem 5.1. *There is a Dirichlet series $H_5(s)$, absolutely convergent for $\operatorname{Re} s > 19/13$, such that, for $\operatorname{Re} s > 3/2$,*

$$Z_5(s) = \zeta(2s-2)\zeta(4s-5)\zeta(6s-8)H_5(s). \tag{15}$$

The right side extends Z_5 meromorphically to $\operatorname{Re} s > 19/13$. Moreover $H_5(3/2) > 0$. Thus Z_5 has abscissa of convergence $3/2$ and a pole of order three there. If $B \ge 2$, then

$$\sum_{n \le B} a_5(n) = C_5 B^{3/2} (\log B)^2 + O(B^{3/2} \log B), \qquad C_5 = \frac{H_5(3/2)}{144} > 0. \tag{16}$$

In particular,

$$C_5 = \frac{1}{144} \prod_p (1-p^{-1})^3 Z_{5,p}(3/2). \tag{17}$$

Theorem 5.2. *Let x be a formal variable and put*

$$P_p(x) = 1 + x + p^2x^2 + p^3x^3.$$

For $p \neq 5$, let ρ_p be the number of roots of z^2+z-1 in $\mathbb{F}_p$. Thus $\rho_2 = 0$, and $\rho_p = 1 + \left(\frac{5}{p}\right)$ for odd $p \neq 5$. Then

$$\mathsf{Z}_{5,p}^{\mathrm{cc}}(x) = \frac{P_p(x)}{1-p^5x^4} + \frac{(1-p^{-1})\rho_p p^6 x^5}{(1-p^5x^4)(1-p^6x^5)} \qquad (p \neq 5). \tag{18}$$

At $p = 5$ the formula is

$$\mathsf{Z}^{\mathrm{cc}}_{5,5}(x) = \frac{P_5(x) + (1 - 5^{-1})5^6 x^5}{1 - 5^5 x^4}. \tag{19}$$

These are identities of formal power series; substituting $x = p^{-s}$ gives the local Dirichlet series, absolutely convergent for $\operatorname{Re} s > 5/4$. There is a Dirichlet series H^{cc}_5, absolutely convergent for $\operatorname{Re} s > 7/5$, such that, initially for $\operatorname{Re} s > 3/2$,

$$Z^{\mathrm{cc}}_5(s) = \zeta(2s-2)\zeta(4s-5)H^{\mathrm{cc}}_5(s), \qquad H^{\mathrm{cc}}_5(3/2) > 0. \tag{20}$$

The right side extends Z^{cc}_5 meromorphically to $\operatorname{Re} s > 7/5$. The series Z^{cc}_5 has abscissa of convergence $3/2$ and a pole of order two there. Moreover,

$$\sum_{n \le B} a^{\mathrm{cc}}_5(n) = D_5 B^{3/2} \log B + O(B^{3/2}), \quad D_5 = \frac{H^{\mathrm{cc}}_5(3/2)}{12} = \frac{1}{12}\prod_p (1 - p^{-1})^2 Z^{\mathrm{cc}}_{5,p}(3/2) > 0. \tag{21}$$

Corollary 5.3. *The proportion of subrings of index at most B that are cocyclic tends to zero. More precisely, this proportion is asymptotic to*

$$\frac{12 H^{\mathrm{cc}}_5(3/2)}{H_5(3/2)} \frac{1}{\log B}.$$

For $\mathbb{Z}[t]/(t^4)$, the total and cocyclic counts in Section 4 both have growth of order $B^{3/2}$. The extra logarithms in degree five arise from additional low-index local contributions. Uniform control of the remaining diagonal types will isolate these contributions in an absolutely convergent product.

5.1 Quintic closure in Hermite normal form

Triangular division in increasing degree gives the complete closure conditions, by the same method as Lemma 4.1.

Let $N = t\mathbb{Z}_p[t]/(t^5)$. Every finite-index subring of $\mathbb{Z}_p[t]/(t^5)$ containing 1 is uniquely $\mathbb{Z}_p \oplus L$, where L is a full lattice in N satisfying $L^2 \subseteq L$. Its index equals $[N : L]$. There is a unique upper-triangular Hermite basis

$$f_1 = p^a t + u t^2 + v t^3 + w t^4, \qquad f_2 = p^b t^2 + x t^3 + y t^4,$$
$$f_3 = p^c t^3 + z t^4, \qquad f_4 = p^d t^4,$$

where $a, b, c, d \ge 0$ and the representatives satisfy

$$0 \le u < p^b, \quad 0 \le v, x < p^c, \quad 0 \le w, y, z < p^d. \tag{22}$$

Let $A_p(a, b, c, d)$ count the multiplicatively closed lattices of this type, and put $m = a + b + c + d$.

Lemma 5.4. *The necessary and sufficient conditions for multiplicative closure are*

$$b \le 2a, \qquad c \le a+b, \qquad d \le a+c, \qquad d \le 2b, \tag{23}$$

together with the following three congruences. Define

$$T = 2p^a u - p^{2a-b}x.$$

Then

$$T \equiv 0 \pmod{p^c}, \tag{24}$$

$$p^a x + p^b u - p^{a+b-c}z \equiv 0 \pmod{p^d}, \tag{25}$$

$$u^2 + 2p^a v - p^{2a-b}y - (T/p^c)z \equiv 0 \pmod{p^d}. \tag{26}$$

Proof. Only $f_1^2, f_1f_2, f_1f_3, f_2^2$ can be nonzero. The products $f_1f_3 = p^{a+c}t^4$ and $f_2^2 = p^{2b}t^4$ give the last two inequalities in (23). Next,

$$f_1f_2 = p^{a+b}t^3 + (p^a x + p^b u)t^4.$$

Subtracting $p^{a+b-c}f_3$ gives the inequality $c \le a+b$ and (25). Finally,

$$f_1^2 = p^{2a}t^2 + 2p^a u\, t^3 + (u^2 + 2p^a v)t^4.$$

Subtracting $p^{2a-b}f_2$ first requires $b \le 2a$; subtracting $(T/p^c)f_3$ next gives (24) and (26). These calculations also prove sufficiency. □

Here is an exact local expression, valid at every prime:

$$Z_{5,p}(s) = \sum_{\substack{a,b,c,d\ge 0 \\ \text{(23) holds}}} A_p(a,b,c,d)p^{-s(a+b+c+d)}, \tag{27}$$

where A_p is the finite count defined by (22) and (24)–(26).

For the estimates it is more convenient to let all six off-diagonal entries range over $\mathbb{Z}_p$, with normalized Haar measure, and to denote the measure of the three congruences by $\mu_p(a,b,c,d)$. Then

$$A_p(a,b,c,d) = p^{b+2c+3d}\mu_p(a,b,c,d). \tag{28}$$

To justify the measure in (28), fix a Hermite matrix M_0 with the prescribed diagonal and off-diagonal entries $u_0, v_0, w_0, x_0, y_0, z_0$. Every upper-triangular basis matrix with the same diagonal and the same row lattice is uniquely UM_0, where U is upper unitriangular over $\mathbb{Z}_p$. Indeed the change-of-basis matrix is integral and upper triangular, and its diagonal entries are all 1. Conversely every such U preserves the row lattice. Writing the entries of U above the diagonal as q_{ij}, the off-diagonal entries of UM_0 are

$$\begin{aligned} u &= u_0 + p^b q_{12}, & x &= x_0 + p^c q_{23}, \\ v &= v_0 + x_0 q_{12} + p^c q_{13}, & y &= y_0 + z_0 q_{23} + p^d q_{24}, \\ w &= w_0 + y_0 q_{12} + z_0 q_{13} + p^d q_{14}, & z &= z_0 + p^d q_{34}. \end{aligned}$$

This affine map from $\mathbb{Z}_p^6$ to the six off-diagonal coordinates has determinant

$$p^b p^c p^d p^c p^d p^d = p^{b+2c+3d}.$$

Its image therefore has Haar measure $p^{-b-2c-3d}$. These images, as M_0 ranges over Hermite representatives, partition the space of triangular bases with the prescribed diagonal. Multiplicative closure is constant on each image because it depends only on the row lattice. Summing their measures proves (28). This is the elementary lattice-counting form of the p-adic integral formalism of Grunewald–Segal–Smith [2].

5.2 A uniform bound for all quintic diagonal types

We combine two complementary estimates: one counts the linear equations by their minors, and the other bounds the fibers of the remaining quadratic expression. Their minimum controls every relative size of the diagonal entries.

Set

$$\epsilon_p = v_p(2), \qquad e = \min(a+\epsilon_p, 2a-b), \qquad h = \min(d,e).$$

For fixed u, x, z satisfying (24), integration over v, y in (26) has measure $p^{-(d-h)}$ if

$$u^2 - (T/p^c)z \equiv 0 \pmod{p^h}, \tag{29}$$

and has measure zero otherwise. This follows because the image of $(v,y) \mapsto 2p^a v - p^{2a-b}y$ is exactly $p^e\mathbb{Z}_p$.

Lemma 5.5. *Suppose (23) holds. Define*

$$\delta_p = \min\{c+d, c+b, c+a, a+b, d+a+\epsilon_p, d+2a-b,\\ 2a+v_p(3), 2a+b-c+\epsilon_p, 3a-c\}.$$

Then

$$A_p(a,b,c,d) \le p^{b+c+d+\delta_p+h}, \tag{30}$$

$$A_p(a,b,c,d) \le (h+1)p^{b+c+2d+\min(c+h,e)}. \tag{31}$$

Proof. To prove (30), discard (29). The two linear congruences (24) and (25) define the kernel of

$$\mathbb{Z}_p^3 \longrightarrow \mathbb{Z}_p/p^c\mathbb{Z}_p \oplus \mathbb{Z}_p/p^d\mathbb{Z}_p, \quad (u,x,z) \longmapsto (2p^a u - p^{2a-b}x,\ p^b u + p^a x - p^{a+b-c}z).$$

The cokernel has order p^{δ_p}. To see this, adjoin the columns $(p^c,0)^\intercal, (0,p^d)^\intercal$ to obtain

$$\begin{pmatrix} 2p^a & -p^{2a-b} & 0 & p^c & 0 \\ p^b & p^a & -p^{a+b-c} & 0 & p^d \end{pmatrix}.$$

Its nine nonzero 2×2 minors, up to signs, are

$$3p^{2a},\quad 2p^{2a+b-c},\quad p^{3a-c},\quad p^{b+c},\quad 2p^{a+d},\\ p^{a+c},\quad p^{2a-b+d},\quad p^{a+b},\quad p^{c+d}.$$

Their valuations are exactly the nine entries in the minimum defining δ_p. The index of the column module is the greatest common divisor of these minors, by Smith normal form. Thus the kernel measure is $p^{-c-d+\delta_p}$. Combining this with $p^{-(d-h)}$ and (28) gives (30).

For (31), discard (25) instead. A unimodular linear change in u, x writes $T = p^e U$, where U is one of two independent Haar coordinates. If $c > e$, condition (24) requires $U = p^{c-e}U'$ and has measure $p^{-(c-e)}$. If $c \le e$, put $U' = U$. In either case U' is Haar-uniform on $\mathbb{Z}_p$ after imposing (24), and

$$T/p^c = p^{(e-c)_+}U', \qquad q_+ = \max(q,0).$$

For fixed U' and the other coordinate, the measure of z satisfying (29) is at most

$$p^{-\max\{h-(e-c)_+ - v_p(U'),0\}}.$$

This estimate is valid regardless of the dependence of u on U'. For every integer $H \geq 0$,

$$\int_{\mathbb{Z}_p} p^{-\max\{H - v_p(U'),0\}}\, dU' = \sum_{j=0}^{H-1} (1-p^{-1}) p^{-j} p^{-(H-j)} + p^{-H}$$
$$= [1 + H(1-p^{-1})] p^{-H} \leq (H+1) p^{-H}.$$

Taking $H = (h - (e-c)_+)_+$ and using

$$(c-e)_+ + (h - (e-c)_+)_+ = (c+h-e)_+,$$

we see that the joint measure of (24) and (29) is at most

$$(h+1) p^{-(c+h-e)_+}.$$

Multiplication by $p^{-(d-h)} p^{b+2c+3d}$ gives an exponent of

$$b + 2c + 2d + h - (c+h-e)_+ = b + c + 2d + \min(c+h, e),$$

which proves (31). □

Proposition 5.6. *For every prime p and every admissible type of total index exponent $m = a + b + c + d$,*

$$A_p(a,b,c,d) \leq 4(m+2) p^{7m/5}. \tag{32}$$

For odd p, the factor 4 may be omitted. Consequently

$$a_5(p^m) \leq 4(m+2) \binom{m+3}{3} p^{7m/5}. \tag{33}$$

Proof. First suppose p is odd. We bound the exponent in the smaller of (30) and (31); their common prefactor may be enlarged to $h+1$.

If $b \leq a$, then $e = a$ and $h \leq a$. The available exponent bounds include

$$A = a + b + c + 2d, \qquad F = a + 2b + 2c + d, \qquad C = 3a + 2b + d.$$

Here A follows from (31), F from $\delta_p \leq b + c$, and C from $\delta_p \leq 2a + b - c$. If $c \leq a$, then

$$\frac{2}{5}A + \frac{3}{5}F - \frac{7}{5}m = \frac{-2a + b + c}{5} \leq 0.$$

If $c \geq a$, then

$$\frac{2}{5}A + \frac{3}{5}C - \frac{7}{5}m = \frac{4a + b - 5c}{5} \leq 0.$$

The minimum of two bounds is at most their weighted average.

If $b \geq a$, then $e = 2a - b$. The corresponding three bounds are

$$B = 2a + c + 2d, \qquad G = 3a + 2c + d, \qquad J = 5a + d.$$

The last two use $\delta_p \leq a + c$ and $\delta_p \leq 3a - c$. Since $m \geq 2a + c + d$, for $c \leq a$ we have

$$\frac{2}{5}B + \frac{3}{5}G - \frac{7}{5}(2a + c + d) = \frac{c - a}{5} \leq 0,$$

and for $c \geq a$ we have

$$\frac{2}{5}B + \frac{3}{5}J - \frac{7}{5}(2a + c + d) = a - c \leq 0.$$

This proves the exponent bound $7m/5$ at every odd prime, including 3.

At $p = 2$, the bounds in the case $b \leq a$ become $A + 1, F + 1, C + 2$; thus an extra factor at most $2^2 = 4$ suffices. In the case $b \geq a$, the bounds B, G, J remain valid without change. Finally $h + 1 \leq m + 2$. Summing over at most $\binom{m+3}{3}$ diagonal types gives (33). □

In particular each individual local factor is holomorphic for $\operatorname{Re} s > 7/5$. The prime-independent bound in (33) is the estimate needed to control the infinite tail of the global Euler product.

5.3 The finite exceptional calculation

The gap between the uniform local exponent $7/5$ and the global exponent $3/2$ makes a sufficiently long tail summable over primes. We count the remaining initial diagonal types explicitly.

For $p \geq 5$, set

$$\begin{aligned} e_0 &= \min(a, 2a - b), \qquad h_0 = \min(d, e_0), \\ \delta_0 &= \min(c + d, c + b, c + a, a + b, d + a, d + 2a - b, 2a, 2a + b - c, 3a - c), \\ E(a, b, c, d) &= \min\{b + c + d + \delta_0 + h_0, b + c + 2d + \min(c + h_0, e_0)\}. \end{aligned}$$

Lemma 5.5 gives

$$A_p(a, b, c, d) \leq (h_0 + 1)p^{E(a,b,c,d)}. \tag{34}$$

For $1 \leq m \leq 10$, only the following eight types satisfy $E \geq 3m/2 - 1$. Their exact counts are also displayed. Write $\rho_p(j) = \#\{r \bmod p^j : r^2 + r - 1 \equiv 0 \pmod{p^j}\}$.

m	(a, b, c, d)	$A_p(a, b, c, d)$
2	(1,0,1,0)	p^2
3	(1,1,0,1)	p^3
4	(1,1,1,1)	p^5
5	(1,1,1,2)	$p^5\{1 + (p - 1)\rho_p(1)\}$
6	(2,1,1,2)	p^8
6	(2,2,0,2)	p^7
8	(2,2,1,3)	p^{10}
10	(2,2,2,4)	$p^{10}\{p^2 + (p^2 - p)\rho_p(2)\}$

Appendix A gives the exhaustive integer comparison that produces this list.

We verify all eight counts, using the Hermite representatives from (22).

1. For $(1, 0, 1, 0)$, the entries u, w, y, z vanish. The two entries v, x are arbitrary modulo p, giving p^2.

2. For $(1, 1, 0, 1)$, one has $v = x = 0$, and the final congruence reduces modulo p to $u^2 = 0$. Thus $u = 0$, while w, y, z are arbitrary modulo p.

3. For $(1, 1, 1, 1)$, the only nontrivial condition is

   $$u^2 - (2u - x)z = 0 \quad \text{in } \mathbb{F}_p.$$

   If $z = 0$, there are p choices, with $u = 0$ and x arbitrary. If $z \neq 0$, each u determines a unique x, giving $p(p - 1)$ choices. Hence there are p^2 choices for u, x, z and p^3 independent choices for v, y, w.

4. For $(1,1,1,2)$, (25) says $z \equiv x+u \pmod p$. The residual condition is

$$x^2 - ux - u^2 \equiv 0 \pmod p.$$

There are $1+(p-1)\rho_p(1)$ pairs (u,x). Indeed, the pair with $u=0$ must be $(0,0)$; for $u \neq 0$ put $r = -x/u$. For each pair there are p lifts of z, p^2 choices of (v,y) satisfying the final congruence modulo p^2, and p^2 choices of w. The count follows.

5. For $(2,1,1,2)$, (25) forces $u=0$, after which all remaining conditions hold automatically. The entries v,x each have p choices and w,y,z each have p^2 choices.

6. For $(2,2,0,2)$, one has $v=x=0$, and the residual condition is $u^2 \equiv 0 \pmod{p^2}$. Thus u has p choices; w,y,z each have p^2 choices.

7. For $(2,2,1,3)$, (25) first gives $u+x \equiv 0 \pmod p$. The final congruence modulo p forces $u \equiv 0 \pmod p$, hence $x=0$ in its chosen range. Write $u = pU$ with $0 \le U < p$. The residual congruence modulo p^2 is now automatic. Modulo p^3 the final condition is

$$U^2 + 2v - y - 2Uz \equiv 0 \pmod p.$$

There are p^3 choices of (v,y), p^3 of z, p^3 of w, and p of U.

8. For $(2,2,2,4)$, one has $z \equiv x+u \pmod{p^2}$, and the residual condition modulo p^2 is $x^2 - ux - u^2 = 0$. The pairs divisible by p give p^2 solutions. If u is a unit, putting $r = -x/u$ gives $(p^2-p)\rho_p(2)$ solutions. If u is divisible by p, the congruence modulo p forces x to be divisible by p, so this accounts for every pair. There are p^2 lifts of z, p^4 choices of (v,y) satisfying the last congruence, and p^4 choices of w.

The same eight counts in fact hold at 2 and 3 as well, although only $p \ge 5$ is needed in the Euler-product estimate.

5.3.1 A quadratic diagonal family

The exceptional types $(1,1,1,2)$ and $(2,2,2,4)$ belong to a single family controlled by $x^2 - ux - u^2 = 0$. Its third member, $(3,3,3,6)$, will sharpen the estimate for the global remainder.

Proposition 5.7. *For every prime p and integer $k \ge 0$, put*

$$\mathcal{N}_p(k) = \#\{(u,x) \in (\mathbb{Z}/p^k\mathbb{Z})^2 : x^2 - ux - u^2 \equiv 0 \pmod{p^k}\}.$$

Thus $\mathcal{N}_p(0) = 1$. Then

$$A_p(k,k,k,2k) = p^{5k}\mathcal{N}_p(k). \tag{35}$$

Writing

$$\rho_p(j) = \#\{z \bmod p^j : z^2 + z - 1 \equiv 0 \pmod{p^j}\}, \qquad j \ge 1,$$

one has the formula, including $k=0$ with an empty sum,

$$\mathcal{N}_p(k) = p^{2\lfloor k/2 \rfloor} + (1-p^{-1})p^k \sum_{\substack{r \ge 0 \\ 2r<k}} \rho_p(k-2r). \tag{36}$$

In particular,

$$\mathcal{N}_p(k) = \begin{cases} p^k(1 + k(1 - p^{-1})), & p \neq 5 \text{ and } z^2 + z - 1 \text{ has two roots modulo } p, \\ p^{2\lfloor k/2 \rfloor}, & z^2 + z - 1 \text{ has no root modulo } p, \\ p^k, & p = 5. \end{cases} \tag{37}$$

The second case includes $p = 2$. Consequently

$$A_p(k, k, k, 2k) \leq (k + 1)p^{6k} \quad \text{for every } p, k. \tag{38}$$

If X is a formal variable and $Y = p^6X^5$, then

$$\sum_{k \geq 0} A_p(k, k, k, 2k)X^{5k} = \begin{cases} (1 - Y/p)/(1 - Y)^2, & \rho_p(1) = 2, \\ (1 + Y/p)/(1 - Y^2), & \rho_p(1) = 0, \\ (1 - Y)^{-1}, & p = 5. \end{cases} \tag{39}$$

These are contributions of the specified diagonal family to the local factor, rather than formulas for the entire local factor.

Proof. The case $k = 0$ is immediate. Assume $k \geq 1$. In the Hermite basis with $(a, b, c, d) = (k, k, k, 2k)$, the variables u, v, x range modulo p^k, whereas w, y, z range modulo p^{2k}. The congruence (24) is automatic, since $T = p^k(2u - x)$. The congruence (25) is

$$z \equiv x + u \pmod{p^k}.$$

For each pair (u, x) it therefore gives exactly p^k choices of z. Reduction of (26) modulo p^k gives

$$u^2 - (2u - x)(x + u) = x^2 - ux - u^2 \equiv 0 \pmod{p^k}.$$

If this congruence fails, there is no lift. If it holds, fix any of the p^k admissible z and any of the p^k values of v. The unreduced last congruence is

$$p^k y \equiv u^2 + 2p^k v - (2u - x)z \pmod{p^{2k}}.$$

Its right side is divisible by p^k, so it determines y modulo p^k and allows exactly p^k values modulo p^{2k}. Finally, w has p^{2k} arbitrary values. Thus each admissible (u, x) contributes $p^k p^k p^k p^{2k} = p^{5k}$ lattices. This proves (35), without excluding any prime.

To count the quadratic solutions, we stratify by the common valuation of (u, x). This is motivated by the homogeneity of the quadratic form: dividing both coordinates by p^r lowers the required modulus by p^{2r}. The pairs for which both coordinates are divisible by $p^{\lceil k/2 \rceil}$ all satisfy the equation; there are $p^{2\lfloor k/2 \rfloor}$ of them.

Every remaining solution has

$$r = \min\{v_p(u), v_p(x)\} < k/2.$$

Here valuations of residue classes are truncated at k. In this range one necessarily has $v_p(u) = r$: if u/p^r were zero modulo p and x/p^r a unit, the quadratic equation divided by p^{2r} would reduce to a nonzero square modulo p. There are $(1 - p^{-1})p^{k-r}$ choices of u of valuation r. For fixed such u, write $u = p^r u'$ and $x = p^r x'$, with u' a unit modulo p^{k-r}. The change of coordinate

$$z = -x'/u' \pmod{p^{k-r}}$$

is bijective and turns the equation into

$$z^2 + z - 1 \equiv 0 \pmod{p^{k-2r}}.$$

Each root modulo p^{k-2r} has exactly p^r lifts modulo p^{k-r}. Thus this valuation stratum contains

$$(1-p^{-1})p^{k-r}\,p^r\rho_p(k-2r) = (1-p^{-1})p^k\rho_p(k-2r)$$

solutions. The strata are disjoint and exhaustive, proving (36).

For odd $p \neq 5$, the discriminant is 5, so the polynomial has either zero or two roots modulo p. Each root is simple: a common zero with its derivative $2z+1$ would force $5 = 0$ modulo p. For completeness, a root z_j modulo p^j has lifts $z_j + p^j t$, t mod p, and

$$(z_j + p^j t)^2 + (z_j + p^j t) - 1 \equiv z_j^2 + z_j - 1 + p^j t(2z_j + 1) \pmod{p^{j+1}}.$$

The derivative is a unit, so exactly one t gives a root. Thus $\rho_p(j) = \rho_p(1)$ for all $j \geq 1$. At 2 there are no roots modulo 2, hence none modulo any higher power. At 5 the only root modulo 5 is 2, and

$$(2+5t)^2 + (2+5t) - 1 \equiv 5 \pmod{25}.$$

Therefore $\rho_5(1) = 1$ and $\rho_5(j) = 0$ for $j \geq 2$.

In the case of two roots, the sum in (36) is $2\lceil k/2 \rceil$. Substitution, separately for even and odd k, gives the first line of (37). With no roots only the first term remains. At 5, when k is even the sum is empty of nonzero terms and the first term is 5^k; when k is odd there is just the term $r = (k-1)/2$, giving $5^{k-1} + (1-5^{-1})5^k = 5^k$. The bound (38) follows immediately. Finally, summing the first line uses $\sum_{k\geq 0} Y^k = (1-Y)^{-1}$ and $\sum_{k\geq 0} kY^k = Y(1-Y)^{-2}$. In the second line the even terms are Y^{2j} and the odd terms are Y^{2j+1}/p; the last line is geometric. These identities prove (39) as formal power series. □

Lemma 5.8 (Summability of the quintic remainder)**.** *For $p \geq 5$, define the local Dirichlet series*

$$R_p(s) = Z_{5,p}(s) - 1 - p^{2-2s} - p^{5-4s} - p^{8-6s}.$$

It has nonnegative coefficients. For every $\sigma > 19/13$,

$$\sum_{p\geq 5} R_p(\sigma) < \infty.$$

Proof. For $p \geq 5$ the bound (34) applies, and the finite comparison of integer expressions in Appendix A gives

m	11	12	13	14	15	16
# admissible types	108	136	165	202	242	290
$\max E$	15	16	18	19	21	22

At $m = 15$, the maximum 21 is attained only at $(3,3,3,6)$; all other types have $E \leq 20$. Proposition 5.7 improves the bound for this one type to $A_p(3,3,3,6) \leq 4p^{18}$. Thus the maximum sufficient coefficient exponents, after making this replacement, are

$$15, \quad 16, \quad 18, \quad 19, \quad 20, \quad 22 \qquad (11 \leq m \leq 16).$$

All implied constants here are independent of p: there are finitely many types and $h_0 + 1 \leq m + 1$.

For each of the six exponents, summation over primes is justified when $m\sigma - E > 1$, where $\sigma = \operatorname{Re} s$. Their thresholds are

$$\frac{16}{11}, \quad \frac{17}{12}, \quad \frac{19}{13}, \quad \frac{10}{7}, \quad \frac{7}{5}, \quad \frac{23}{16}.$$

Their maximum is $19/13$. For $m \le 10$, the nonexceptional types have maximum threshold $13/9$, by Appendix A. The five nondominant exceptional rows have bounds $O(p^3)$, $O(p^6)$, $O(p^7)$, $O(p^{10})$, and $O(p^{12})$, respectively, because $\rho_p(j) \le 2$ for $p \ge 5$. Their thresholds are at most $7/5 < 13/9$. Thus every retained term with $m \le 10$ is prime-summable for $\sigma > 13/9$, which is weaker than the asserted condition.

It remains to control every larger index. Write $\sigma \ge \sigma_1 > 7/5$. By (33),

$$\begin{aligned}\sum_{m\ge 17} a_5(p^m)p^{-m\sigma} &\le 4\sum_{m\ge 17}(m+2)\binom{m+3}{3}p^{-m(\sigma-7/5)}\\ &\ll_{\sigma_1} p^{-17(\sigma-7/5)}.\end{aligned}$$

Indeed, after removing the first power $p^{-17(\sigma-7/5)}$, the remaining polynomially weighted geometric series is bounded by replacing $p^{-(\sigma-7/5)}$ with $2^{-(\sigma_1-7/5)} < 1$. The prime sum of this bound converges provided

$$\sigma > \frac{7}{5} + \frac{1}{17} = \frac{124}{85} < \frac{19}{13}.$$

The three subtracted monomials are the complete contributions of the diagonal types

$$(1,0,1,0), \qquad (1,1,1,1), \qquad (2,1,1,2),$$

in that order. Thus R_p has nonnegative coefficients. The finite estimates and the tail bound prove the asserted prime summability. □

5.3.2 Extraction of the global factors

For a local series $F(s) = \sum_{m\ge 0} c_m p^{-ms}$, put

$$\|F\|_{p,\sigma} = \sum_{m\ge 0} |c_m| p^{-m\sigma}.$$

This coefficient norm is submultiplicative whenever both norms on the right are finite. Lemma 5.8 gives

$$Z_{5,p}(s) = 1 + p^{2-2s} + p^{5-4s} + p^{8-6s} + R_p(s), \qquad \sum_{p\ge 5} \|R_p\|_{p,\sigma} < \infty \quad (\sigma > 19/13).$$

We prove that

$$H_5(s) = \prod_p (1-p^{2-2s})(1-p^{5-4s})(1-p^{8-6s})Z_{5,p}(s) \tag{40}$$

has an absolutely convergent Dirichlet-series expansion in that half-plane.

Let $H_{5,p}$ denote the pth factor of (40), and set

$$X_1 = p^{2-2s}, \quad X_2 = p^{5-4s}, \quad X_3 = p^{8-6s}, \qquad t_i = \|X_i\|_{p,\sigma}.$$

For $p \ge 5$, we have

$$H_{5,p} = (1-X_1)(1-X_2)(1-X_3)(1+X_1+X_2+X_3+R_p).$$

In the part not involving R_p, the constant term is 1 and all terms of degree one in the X_i cancel. Since $0 < t_i < 1$ for $\sigma > 19/13$, submultiplicativity gives the uniform estimate

$$\|H_{5,p} - 1\|_{p,\sigma} \ll (t_1 + t_2 + t_3)^2 + \|R_p\|_{p,\sigma}. \tag{41}$$

Indeed every remaining polynomial term has degree at least two, and the norm of the coefficient multiplying R_p is at most $\prod_i (1+t_i) \le 8$. The prime sums of t_1^2, t_2^2, t_3^2 converge for $\sigma > 5/4, 11/8, 17/12$, respectively. By $(t_1+t_2+t_3)^2 \le 3\sum_i t_i^2$, all of them are summable in the half-plane under consideration. The two factors at $2, 3$ have finite coefficient norms for $\sigma > 7/5$, by Proposition 5.6.

Write $H_{5,p}(s) = \sum_{m\ge 0} h_p(m) p^{-ms}$, with $h_p(0) = 1$, and define $h(n) = \prod_p h_p(v_p(n))$. The preceding bounds imply

$$\sum_{n\ge 1} |h(n)| n^{-\sigma} = \prod_p \|H_{5,p}\|_{p,\sigma} < \infty \qquad (\sigma > 19/13).$$

The equality follows first for integers supported on a finite set of primes and then by monotone convergence. This proves the asserted absolute Dirichlet-series convergence of H_5.

The remainder estimate and the three displayed monomials show that $\sum_p (Z_{5,p}(\sigma) - 1)$ converges for $\sigma > 3/2$. Consequently (15) first holds by absolutely convergent Euler products in that half-plane and then gives the asserted meromorphic continuation. At $s = 3/2$ each local factor in (40) is $(1-p^{-1})^3 Z_{5,p}(3/2) > 0$. Absolute convergence makes their product nonzero. The three Riemann zeta factors therefore give a pole of order exactly three. The counting asymptotic will be proved in Section 5.5.

5.4 Exact enumeration of quintic cocyclic subrings

A cocyclic lattice is the kernel of a primitive additive character. Multiplicative closure forces that character to be a unit at t, so we normalize its value there to 1. The resulting product equations involve only two free coordinates after elimination.

5.4.1 A cyclic quotient parametrization

Fix $m \ge 1$, and put $A = \mathbb{Z}/p^m\mathbb{Z}$. A cocyclic lattice $L \subset N$ of index p^m is the kernel of a primitive (that is, surjective) $\mathbb{Z}_p$-linear map $N \to A$, unique up to multiplication by a unit of A. If L is closed under multiplication, its image modulo p is a three-dimensional subalgebra of $t\mathbb{F}_p[t]/(t^5)$. That subalgebra must equal $t^2\mathbb{F}_p[t]/(t^5)$. In fact the first four powers of an element with nonzero t coefficient would span the whole four-dimensional algebra. Thus every such kernel has a unique normalized defining map

$$\phi(t) = 1, \quad \phi(t^2) = B, \quad \phi(t^3) = C, \quad \phi(t^4) = D, \qquad B, C, D \in pA. \tag{42}$$

The kernel is generated by $p^m t, t^2 - Bt, t^3 - Ct, t^4 - Dt$. Checking their six possibly nonzero pairwise products gives

$$D - 2BC + B^3 = 0, \tag{43}$$
$$-BD - C^2 + B^2C = 0, \tag{44}$$
$$D(B^2 - C) = 0, \tag{45}$$
$$C(BC - 2D) = 0, \tag{46}$$
$$D(BC - D) = 0, \tag{47}$$
$$BD^2 = 0 \tag{48}$$

in A. Products with $p^m t$ impose no additional condition. The first equation determines $D = 2BC - B^3$, and the second becomes

$$F(B,C) := C^2 + B^2C - B^4 = 0. \tag{49}$$

Modulo F, both (45) and (46) become

$$G(B,C) := 5B^3C - 3B^5 = 0. \tag{50}$$

Lemma 5.9. *The solutions of (43)–(48) are exactly the following two disjoint classes, with $D = 2BC - B^3$:*

1. *$v_p(B) \geq \lceil m/4 \rceil$ and $v_p(C) \geq \lceil m/2 \rceil$;*
2. *$r = v_p(B)$ satisfies*
$$\lceil m/5 \rceil \leq r < m/4,$$
and $C = B^2 z$, where
$$z^2 + z - 1 \equiv 0 \pmod{p^{m-4r}}.$$
Here valuations of residue classes are truncated at m; the parameter z is considered modulo p^{m-2r} in the second class.

Proof. Take lifts of B, C to $\mathbb{Z}_p$, choosing valuation m for a zero residue, and use the lift $D = 2BC - B^3$. Valuation bounds at least m then imply the required congruences. Put $r = v_p(B)$. If $4r \geq m$, equation (49) forces $v_p(C) \geq \lceil m/2 \rceil$: otherwise C^2 has strictly smaller valuation than the other two terms and has valuation less than m. Conversely these two divisibilities imply (49). If $q = \min(v_p(C), 2r)$, then $q \geq m/2$ and $v_p(D) \geq r + q$. Hence (45)–(48) all hold: their terms have valuations at least $r + 2q$, $v_p(C) + r + q$, $2r + 2q$, and $3r + 2q$, respectively, each at least m.

Suppose now that $4r < m$. In (49), comparison of valuations forces $v_p(C) = 2r$. Writing $C = B^2 z$ gives $z^2 + z - 1 \equiv 0 \pmod{p^{m-4r}}$. Equation (50) becomes $B^5(5z - 3) = 0$. If $5r < m$, these two congruences would imply both $z^2 + z - 1 = 0$ and $5z - 3 = 0$ modulo p. This is impossible at every prime because

$$25(z^2 + z - 1) = (5z - 3)(5z + 8) - 1.$$

Thus $5r \geq m$ is necessary. It is also sufficient: after (49), the remaining expressions in (45)–(48) have valuations at least $5r, 5r, 6r, 7r$, respectively. The condition $D \in pA$, as well as $B, C \in pA$, holds in both classes. This proves the lemma. □

5.4.2 Coefficients and rational functions

Lemma 5.9 gives, for every prime and $m \geq 1$,

$$a_5^{\mathrm{cc}}(p^m) = p^{2m - \lceil m/4 \rceil - \lceil m/2 \rceil} + (1 - p^{-1}) \sum_{\lceil m/5 \rceil \leq r < m/4} \rho_p(m - 4r) p^{m+r}. \tag{51}$$

Indeed the first class gives the first term. In the second class there are $(1 - p^{-1})p^{m-r}$ choices of B and $p^{2r}\rho_p(m - 4r)$ choices of C.

The root counts were established in the proof of Proposition 5.7: for $p \neq 5$, $\rho_p(j) = \rho_p$ for all $j \geq 1$, while $\rho_5(1) = 1$ and $\rho_5(j) = 0$ for $j \geq 2$.

Grouping m modulo 4 shows

$$1 + \sum_{m \geq 1} p^{2m - \lceil m/4 \rceil - \lceil m/2 \rceil} x^m = \frac{1 + x + p^2x^2 + p^3x^3}{1 - p^5x^4}. \tag{52}$$

For the second term of (51), write $m = 4r + j$. The range is precisely $1 \le j \le r$, and its generating series is

$$(1-p^{-1})\sum_{r\ge 1}\sum_{j=1}^{r}\rho_p(j)p^{5r+j}x^{4r+j} = \frac{1-p^{-1}}{1-p^5x^4}\sum_{j\ge 1}\rho_p(j)(p^6x^5)^j. \tag{53}$$

Equations (52)–(53) prove (18) and (19).

Define

$$H_5^{\mathrm{cc}}(s) = \prod_p (1-p^{2-2s})(1-p^{5-4s})Z_{5,p}^{\mathrm{cc}}(s).$$

Put $x = p^{-s}$. The part of the adjusted local factor arising from P_p is

$$(1-p^2x^2)P_p(x) = 1 + x + (p^3-p^2)x^3 - p^4x^4 - p^5x^5.$$

For $p \ne 5$, the coefficient norm of the remaining term is at most

$$2(1+p^{2-2\sigma})\frac{p^{6-5\sigma}}{1-p^{6-5\sigma}} \ll_\sigma p^{6-5\sigma} \qquad (\sigma > 7/5).$$

Its prime sum converges. The nonconstant terms in the displayed polynomial are prime-summable already for $\sigma > 4/3$; at 5 the adjusted factor is a polynomial. As in Section 5.3.2, expanding the local factors and using their absolute coefficient norms proves absolute Dirichlet-series convergence of H_5^{cc} for $\operatorname{Re} s > 7/5$. For $\operatorname{Re} s > 3/2$, the original cocyclic series converges because its coefficients are bounded by the total coefficients. Euler multiplication therefore proves (20) in that half-plane. The right side then gives the stated continuation. At $s = 3/2$ every adjusted local factor is positive, so absolute convergence makes the product nonzero. The two zeta factors give a pole of order exactly two.

5.5 Elementary passage to the counting functions

The following elementary sums determine the constants and error terms. Let $b_2(n)$ and $b_3(n)$ be the Dirichlet coefficients of

$$\zeta(2s-2)\zeta(4s-5), \qquad \zeta(2s-2)\zeta(4s-5)\zeta(6s-8),$$

respectively, and put $B_j(Y) = \sum_{n\le Y} b_j(n)$.

Lemma 5.10. *For $Y \ge 1$,*

$$B_2(Y) = \frac{1}{12}Y^{3/2}\log Y + O(Y^{3/2}),$$
$$B_3(Y) = \frac{1}{144}Y^{3/2}(\log Y)^2 + O(Y^{3/2}\log(2Y)).$$

Proof. Using $\sum_{i\le X} i^2 = X^3/3 + O(X^2)$ for $X \ge 1$,

$$B_2(Y) = \sum_{j\le Y^{1/4}} j^5 \sum_{i\le Y^{1/2}/j^2} i^2$$
$$= \frac{Y^{3/2}}{3}\sum_{j\le Y^{1/4}}\frac{1}{j} + O\left(Y\sum_{j\le Y^{1/4}} j\right),$$

which gives the first formula.

Similarly,

$$B_3(Y) = \sum_{j^4k^6\le Y} j^5k^8 \sum_{i\le Y^{1/2}/(j^2k^3)} i^2$$
$$= \frac{Y^{3/2}}{3} \sum_{j^4k^6\le Y} \frac{1}{jk} + O\left(Y \sum_{j^4k^6\le Y} jk^2\right).$$

The error is $O(Y^{3/2}\log(2Y))$, since summing over j bounds it by a constant times $Y^{3/2}\sum_{k\le Y^{1/6}} k^{-1}$. For the main harmonic sum, putting $K = Y^{1/6}$ gives

$$\sum_{j^4k^6\le Y} \frac{1}{jk} = \sum_{k\le K} \frac{1}{k}\left(\frac{1}{4}\log Y - \frac{3}{2}\log k + O(1)\right)$$
$$= \frac{1}{48}(\log Y)^2 + O(\log(2Y)),$$

because $\sum_{k\le K} k^{-1} = \log K + O(1)$ and $\sum_{k\le K}(\log k)/k = \frac{1}{2}(\log K)^2 + O(1)$. This gives the second formula. □

To finish Theorem 5.1, apply Lemma 2.4 to b_3 and the Dirichlet coefficients of H_5, taking $\alpha = 3/2$, $r = 2$, and any $19/13 < \beta < 3/2$. Lemma 5.10 gives $c = 1/144$, so the leading constant is $H_5(3/2)/144$ and the error is $O(B^{3/2}\log B)$. For Theorem 5.2, use b_2, H_5^{cc}, $r = 1$, $c = 1/12$, and $7/5 < \beta < 3/2$. The leading constant is $H_5^{\mathrm{cc}}(3/2)/12$ and the error is $O(B^{3/2})$. These positive asymptotics, together with convergence to the right of $3/2$, prove that both convergence abscissae are exactly $3/2$.

6 Cotype refinements in degrees four and five

We now attach the determinantal weights of Lemma 2.3 to the Hermite parametrizations in Sections 4 and 5.1. Fix a prime p and write $N_n = N_{n,p}$. For a full-rank $r \times r$ matrix H, let $\delta_j(H)$ be the minimum valuation of its $j \times j$ minors, with $\delta_0(H) = 0$. Lemma 2.3 gives

$$\lambda_i = \delta_{r-i+1}(H) - \delta_{r-i}(H) \qquad (1 \le i \le r). \tag{54}$$

Thus Hermite diagonal valuations need not coincide with the invariant exponents used in $\mathcal{C}_{n,p}$.

All the identities below are identities of formal power series. They also hold absolutely when $\min_i \Re s_i > n-2$ locally and when $\min_i \Re s_i > n-1$ in the global Euler product. To justify these sufficient domains, there are at most $\binom{m+r-1}{r-1}p^{(r-1)m}$ lattices of index p^m in rank $r = n-1$, by Lemma 2.1. The number of subrings is no larger. Summing this bound first over m proves local convergence, and then summing the nonconstant local factors over primes proves the stated global convergence. These are sufficient domains, not claims of optimal convergence.

Theorem 6.1 (Explicit quartic cotype sum)**.** *Let*

$$\mathsf{H}_4 = \begin{pmatrix} p^a & u & v \\ 0 & p^b & x \\ 0 & 0 & p^c \end{pmatrix}, \qquad a,b,c \ge 0, \qquad 0 \le u < p^b, \quad 0 \le v,x < p^c.$$

In the following sum retain exactly those matrices satisfying

$$b \le 2a, \qquad c \le a+b, \qquad 2p^a u - p^{2a-b}x \equiv 0 \pmod{p^c}. \tag{55}$$

For each such matrix put $m = a+b+c$ *and*

$$d_1 = \min\{a, b, c, v_p(u), v_p(v), v_p(x)\},$$
$$d_2 = \min\{a+b, a+v_p(x), a+c, v_p(ux-p^b v), c+v_p(u), b+c\}.$$

Then, at every prime,

$$\mathcal{C}_{4,p}(X_1, X_2, X_3) = \sum_{\substack{a,b,c,u,v,x \\ \text{as above}}} X_1^{m-d_2} X_2^{d_2-d_1} X_3^{d_1}. \tag{56}$$

Proof. The rows represent $f_1 = p^a t + ut^2 + vt^3$, $f_2 = p^b t^2 + xt^3$, and $f_3 = p^c t^3$. This is the triangular parametrization of Lemma 4.1, with the powers of t and the basis rows written in increasing order. The only products that can be nonzero are

$$f_1^2 = p^{2a}t^2 + 2p^a u\, t^3, \qquad f_1 f_2 = p^{a+b}t^3.$$

The second lies in the row lattice precisely when $c \le a+b$. Eliminating the t^2 coefficient of the first requires $b \le 2a$; the remaining t^3 coefficient gives the congruence in (55). Bilinearity then proves sufficiency. The displayed d_1 is the minimum of the entry valuations. The six possibly nonzero 2-minors are

$$p^{a+b}, \quad p^a x, \quad p^{a+c}, \quad ux - p^b v, \quad up^c, \quad p^{b+c}.$$

Consequently $d_1 = \delta_1(\mathsf{H}_4)$, $d_2 = \delta_2(\mathsf{H}_4)$, and $\delta_3(\mathsf{H}_4) = m$. Equation (54) proves the claimed weight; uniqueness of Hermite representatives proves that every lattice is counted exactly once. □

Theorem 6.2 (Explicit quintic cotype sum)**.** *Let*

$$\mathsf{H}_5 = \begin{pmatrix} p^a & u & v & w \\ 0 & p^b & x & y \\ 0 & 0 & p^c & z \\ 0 & 0 & 0 & p^d \end{pmatrix},$$

where $a, b, c, d \ge 0$, $0 \le u < p^b$, $0 \le v, x < p^c$, *and* $0 \le w, y, z < p^d$. *Retain precisely the matrices satisfying*

$$b \le 2a, \quad c \le a+b, \quad d \le a+c, \quad d \le 2b,$$
$$T = 2p^a u - p^{2a-b}x \equiv 0 \pmod{p^c},$$
$$p^a x + p^b u - p^{a+b-c} z \equiv 0 \pmod{p^d},$$
$$u^2 + 2p^a v - p^{2a-b} y - (T/p^c) z \equiv 0 \pmod{p^d}.$$

Set $m = a+b+c+d$ *and* $d_j = \delta_j(\mathsf{H}_5)$ *for* $j = 1, 2, 3$. *Then*

$$\mathcal{C}_{5,p}(X_1, X_2, X_3, X_4) = \sum_{\substack{a,b,c,d,u,v,w,x,y,z \\ \text{as above}}} X_1^{m-d_3} X_2^{d_3-d_2} X_3^{d_2-d_1} X_4^{d_1}. \tag{57}$$

The matrix specifies all $\binom{4}{2}^2$ *minors used to compute* d_2. *For a direct computation of* d_3, *its ten possibly nonzero minors are*

$$p^{a+b+c}, \quad p^{a+b}z, \quad p^a(xz - p^c y), \quad uxz - up^c y - p^b vz + p^{b+c}w,$$
$$p^{a+b+d}, \quad p^{a+d}x, \quad p^d(ux - p^b v), \quad p^{a+c+d}, \quad p^{c+d}u, \quad p^{b+c+d}.$$

Proof. The product elimination establishing these conditions is the quintic Hermite calculation above: the only products to check are $f_1^2, f_1f_2, f_1f_3, f_2^2$. For completeness their nonzero coordinates are, respectively,

$$(p^{2a}, 2p^a u, u^2 + 2p^a v), \quad (p^{a+b}, p^a x + p^b u), \quad p^{a+c}, \quad p^{2b},$$

starting in degrees $2, 3, 4, 4$. Eliminating in increasing degree gives exactly the displayed conditions and proves both necessity and sufficiency. Expanding the 3-minors gives the displayed list. Since $\delta_4(\mathsf{H}_5) = m$, equation (54) then gives the weight in (57). □

Setting all $X_i = p^{-s}$ gives the unrestricted local functions. Setting $X_2 = \cdots = X_{n-1} = 0$ retains precisely the cocyclic terms, with the convention $0^0 = 1$. These are exact cotype extensions in degrees four and five. Their evaluation as closed multivariable rational functions remains an open calculation.

6.1 The normalized cotype integral

The p-adic lattice-counting method of Grunewald–Segal–Smith [2] replaces discrete representatives by a domain defined by polynomial divisibility. Splitting off the identity gives the following normalized integral over the nilpotent summand.

In this subsection reset $d = n-1$. Let $\mathscr{M}_{n,p}$ be the set of upper triangular $d \times d$ matrices M over $\mathbb{Z}_p$ with nonzero determinant whose rows, interpreted in the basis $(t, \dots, t^d)$, span a lattice closed under multiplication. Give the triangular entries independent normalized additive Haar measure dM. Write $D_0(M) = 1$ and

$$D_j(M) = \max_{|I|=|J|=j} |\det M_{I,J}|_p \quad (1 \le j \le d).$$

All these quantities are positive on this domain.

Proposition 6.3. *For* $\min_i \operatorname{Re} s_i > d - 1$,

$$\mathcal{Z}_{n,p}(\boldsymbol{s}) = \frac{1}{(1-p^{-1})^d} \int_{\mathscr{M}_{n,p}} \prod_{j=1}^{d} |m_{jj}|_p^{-j} \prod_{i=1}^{d} \left(\frac{D_{d-i+1}(M)}{D_{d-i}(M)} \right)^{s_i} dM.$$

For $n = 4, 5$, the domains of this integral are specified explicitly through their Hermite representatives by the closure conditions in Theorems 6.1 and 6.2. Direct row elimination gives the equivalent conditions for arbitrary nonzero diagonal entries.

Proof. Fix a Hermite representative H with diagonal $p^{a_1}, \dots, p^{a_d}$. All upper triangular integral bases for its row lattice are exactly UH, where U is upper triangular integral with unit diagonal entries. Necessity follows because both H and UH are bases of the same lattice; their change-of-basis matrix and its inverse are integral and upper triangular. Conversely such a U preserves the lattice. This representation is unique.

The linear map $U \mapsto UH$ on the vector space of upper triangular matrices has determinant $\prod_{j=1}^{d} (p^{a_j})^j$: in row i its diagonal factors are $p^{a_i}, \dots, p^{a_d}$. The domain of U has measure $(1-p^{-1})^d$, so this orbit has measure

$$(1-p^{-1})^d p^{-\sum_j j a_j}.$$

On the orbit, $|m_{jj}|_p = p^{-a_j}$, and all determinantal ideals are constant. Lemma 2.3 says that their ratios give $p^{-\lambda_i}$. Thus the normalized integral over this orbit is exactly $\prod_i p^{-s_i \lambda_i}$. The orbits partition the domain. There are at most $\binom{m+d-1}{d-1} p^{(d-1)m}$ Hermite lattices of index p^m; this proves absolute convergence in the asserted local domain and justifies summing the orbit integrals. □

7 Lifting through the last annihilator

The last monomial t^{n-1} annihilates N_n. This turns the passage from degree $n-1$ to degree n into a system of linear congruences.

Let $n \geq 3$, put $r = n-2$, and project $\pi : N_n \longrightarrow N_{n-1}$. Write $e = t^{n-1}$, so that $\ker \pi = \mathbb{Z}_p e$ and $eN_n = 0$. Denote by $\sigma : N_{n-1} \to N_n$ the additive section represented by polynomials of degree at most $n-2$. If $M \subseteq N_{n-1}$ is a closed full lattice with fixed Hermite basis $g_1, \dots, g_r$, uniquely write

$$g_i g_j = \sum_{k=1}^{r} c_{ij,k} g_k \quad \text{in } N_{n-1}, \qquad c_{ij,k} \in \mathbb{Z}_p,$$

and put

$$\gamma_{ij} = [t^{n-1}](\sigma(g_i)\sigma(g_j)) \quad (1 \leq i \leq j \leq r).$$

Thus $C_M = (c_{ij,k})$ is an $r(r+1)/2$ by r matrix, and $\gamma_M = (\gamma_{ij})$ is an explicitly computable column.

Theorem 7.1 (Linear lifting recursion)**.** *Fix M as above and an integer $a \geq 0$. The closed full lattices $L \subseteq N_n$ with*

$$\pi(L) = M, \qquad L \cap \mathbb{Z}_p e = p^a \mathbb{Z}_p e$$

are in bijection with the solutions

$$C_M z \equiv \gamma_M \pmod{p^a}, \qquad z \in (\mathbb{Z}_p/p^a\mathbb{Z}_p)^r. \tag{58}$$

The solution z gives the basis matrix

$$H(M, z, a) = \begin{pmatrix} H_M & \widetilde{z} \\ 0 & p^a \end{pmatrix}, \tag{59}$$

where $\widetilde{z}$ consists of the representatives $0 \leq \widetilde{z}_i < p^a$. Its index is $p^a[N_{n-1} : M]$, and its cotype is obtained from the minors of (59) by (54).

More explicitly, choose Smith matrices P, Q with $PC_MQ = \operatorname{diag}(p^{e_1}, \dots, p^{e_\ell}, 0)$, where $\ell = \operatorname{rank}_{\mathbb{Q}_p} C_M$ and $0 \leq e_1 \leq \cdots \leq e_\ell$; units are absorbed into P, Q. Put $\eta = P\gamma_M$. Solutions exist if and only if

$$\eta_i \equiv 0 \pmod{p^{\min(a,e_i)}} \ (i \leq \ell), \qquad \eta_i \equiv 0 \pmod{p^a} \ (i > \ell). \tag{60}$$

When they exist, their number is

$$p^{a(r-\ell)+\sum_{i=1}^{\ell} \min(a,e_i)}. \tag{61}$$

Proof. For a lattice L with the specified image and intersection, lift each g_i to an element of L. Its difference from $\sigma(g_i)$ is some multiple $z_i e$. Replacing the lift changes z_i by a multiple of p^a and has no other effect. Thus L determines a unique $z \bmod p^a$. Conversely the vectors $\sigma(g_i) + \widetilde{z}_i e$ and $p^a e$ generate a full lattice with precisely that image and intersection. This proves the bijection for lattices before imposing closure and also proves the block matrix and index assertions.

Since $eN_n = 0$, multiplication of two lifted basis vectors is independent of z:

$$(\sigma(g_i) + \widetilde{z}_i e)(\sigma(g_j) + \widetilde{z}_j e) = \sum_k c_{ij,k}\sigma(g_k) + \gamma_{ij} e.$$

Subtracting $\sum_k c_{ij,k}(\sigma(g_k) + \widetilde{z}_k e)$ leaves $(\gamma_{ij} - \sum_k c_{ij,k}\widetilde{z}_k)e$. It lies in L precisely when its coefficient is divisible by p^a. Products with $p^a e$ vanish. Bilinearity therefore makes (58) necessary and sufficient.

Finally $z = Qw$ and multiplication by P give $p^{e_i} w_i \equiv \eta_i \pmod{p^a}$ for $i \leq \ell$ and $0 \equiv \eta_i \pmod{p^a}$ for the remaining rows. The first congruence is soluble exactly under its condition in (60); when soluble it has $p^{\min(a,e_i)}$ solutions. The other $r - \ell$ variables are unrestricted. Multiplication gives (61). □

In particular the unrestricted local function has the coefficientwise recursion, absolutely convergent for $\operatorname{Re} s > n-2$,

$$Z_{n,p}(s) = \sum_{\substack{M \subseteq N_{n-1} \\ M^2 \subseteq M}} [N_{n-1} : M]^{-s} \sum_{a \geq 0} p^{-as} \#\{z \bmod p^a : C_M z = \gamma_M\}.$$

The corresponding cotype recursion assigns the full block-matrix weight to each lift:

$$\mathcal{C}_{n,p}(\boldsymbol{X}) = \sum_{\substack{M \subseteq N_{n-1} \\ M^2 \subseteq M}} \sum_{\text{full } a \geq 0} \sum_{\substack{z \in (\mathbb{Z}/p^a\mathbb{Z})^r \\ C_M z \equiv \gamma_M \pmod{p^a}}} \prod_{i=1}^{n-1} X_i^{\lambda_i(H(M,z,a))}. \tag{62}$$

Here the exponents are obtained from the minors as in (54). For a fixed total index exponent m, only $a \leq m$ and lattices M of index at most p^m are relevant, so each coefficient is computed by a finite calculation. The recursion starts with the zero-multiplication algebra $N_2 = t\mathbb{Z}_p$, whose lattices are $p^b t\mathbb{Z}_p$ and whose cotype series is $(1-X_1)^{-1}$. It retains the multiplication constants and last-degree product coefficients of M in addition to its cotype.

8 Two parameters for cocyclic subrings in every degree

The products $(t^2 - Bt)(t^j - b_j t)$ extend the quintic cyclic-kernel calculation to every degree. They produce a second-order recurrence; an addition identity then checks all the other products at once.

Define polynomials in $\mathbb{Z}[B, C]$ by

$$U_1 = 1, \quad U_2 = B, \qquad U_{j+2} = BU_{j+1} + (C - B^2)U_j \quad (j \geq 1). \tag{63}$$

In particular $U_3 = C$.

Lemma 8.1 (Addition identity)**.** *For all $i, j \geq 1$,*

$$U_{i+j} = U_i U_{j+1} + U_j U_{i+1} - BU_i U_j. \tag{64}$$

Also U_j is homogeneous of weight $j-1$ when B has weight 1 and C has weight 2.

Proof. For fixed j, both sides of (64), viewed as sequences in i, obey the recurrence (63). At $i = 1$ the identity is immediate from $U_1 = 1, U_2 = B$. At $i = 2$ its right side is $BU_{j+1} + (C - B^2)U_j = U_{j+2}$. Induction proves the identity. The weight assertion holds for U_1, U_2 and is preserved by the recurrence, because both summands defining U_{j+2} have weight $j+1$. □

Theorem 8.2. *Let $n \geq 4$, $m \geq 1$, and $A = \mathbb{Z}/p^m\mathbb{Z}$. There is a bijection between the cocyclic unital subrings of $\mathbb{Z}_p[t]/(t^n)$ of index p^m and the pairs*

$$(B, C) \in (pA)^2, \qquad U_n(B, C) = U_{n+1}(B, C) = 0 \quad \text{in } A. \tag{65}$$

For the corresponding nilpotent lattice L, its uniquely normalized defining character is

$$L = \ker \phi, \qquad \phi(t) = 1, \qquad \phi(t^j) = U_j(B, C) \quad (2 \leq j < n).$$

Consequently, with $a_n^{\mathrm{cc}}(p^m)$ denoting the local cocyclic coefficient,

$$a_n^{\mathrm{cc}}(p^m) = \#\{(B, C) \in (pA)^2 : U_n(B, C) = U_{n+1}(B, C) = 0\}. \tag{66}$$

Proof. A lattice with cyclic quotient of order p^m is the kernel of a surjective $\mathbb{Z}_p$-linear map $\phi : N_n \to A$, unique up to multiplication by a unit of A. To normalize it, reduce L modulo p. The resulting subspace $(L + pN_n)/pN_n$ has codimension one in $t\mathbb{F}_p[t]/(t^n)$ and is closed under multiplication. If it contained an element h with nonzero coefficient of t, the vectors $h, h^2, \dots, h^{n-1}$ would lie in it and be a basis: their coefficient matrix is triangular with nonzero diagonal. This is impossible for a codimension-one subspace. It must therefore be $t^2\mathbb{F}_p[t]/(t^n)$. Hence $\phi(t)$ is a unit and the other values lie in pA; there is exactly one normalization with $\phi(t) = 1$.

Write $b_1 = 1$, $b_j = \phi(t^j)$ for $2 \le j < n$, and $b_j = 0$ for $j \ge n$. Put $B = b_2, C = b_3$. The kernel is generated over $\mathbb{Z}_p$ by $p^m t$ and $h_j = t^j - \widetilde{b}_j t$ for $2 \le j < n$, where the tildes are arbitrary lifts. Products with $p^m t$ have character zero automatically. For $2 \le i, j < n$, direct multiplication shows that the remaining closure conditions are exactly

$$b_{i+j} - b_i b_{j+1} - b_j b_{i+1} + B b_i b_j = 0 \quad \text{in } A. \tag{67}$$

Taking $i = 2$ gives $b_{j+2} = Bb_{j+1} + (C - B^2)b_j$ for $2 \le j < n$. Together with $b_1 = 1, b_2 = B, b_3 = C$, the equations for $2 \le j \le n - 3$ determine $b_j = U_j(B, C)$ through degree $n - 1$. This interior range is empty for $n = 4$, where the same assertion already holds by the three initial values. The equation at $j = n - 2$ now says $U_n = 0$; the one at $j = n - 1$ says $U_{n+1} = 0$. This proves necessity.

Conversely take a pair satisfying (65). The recurrence implies $U_j = 0$ in A for every $j \ge n$. For $j \ge 2$, every monomial of U_j has positive weight and contains B or C, so $U_j(B, C) \in pA$. Define ϕ by the indicated values. It is primitive because $\phi(t) = 1$. The addition identity (64), including the vanishing terms in degrees at least n, proves every equation (67). Thus its kernel is closed under multiplication. The unique normalization and the recovery $B = \phi(t^2), C = \phi(t^3)$ prove injectivity as well as surjectivity. □

The first polynomials make the relation with the lower-rank calculations explicit:

$$\begin{aligned} U_4 &= 2BC - B^3, \\ U_5 &= C^2 + B^2C - B^4, \\ U_6 &= 3BC^2 - 2B^3C, \\ U_7 &= C^3 + 3B^2C^2 - 4B^4C + B^6. \end{aligned}$$

For $n = 5$, reduction of U_6 modulo U_5 gives $U_6 \equiv -5B^3C + 3B^5$; these are exactly the two residual quintic equations already solved above. For $n = 6$ the exact coefficient problem consists of the two explicit equations

$$BC(3C - 2B^2) = 0, \qquad C^3 + 3B^2C^2 - 4B^4C + B^6 = 0 \pmod{p^m}.$$

We do not assert an evaluated rational function or a sharp counting asymptotic for this sextic problem.

Corollary 8.3 (Uniform cocyclic bounds and limiting abscissa)**.** *For every $n \ge 4$, every prime p, and $m \ge 1$,*

$$p^{\,2m - \lceil m/(n-1) \rceil - \lceil 2m/(n-1) \rceil} \;\le\; a_n^{\mathrm{cc}}(p^m) \;\le\; p^{2m-2}. \tag{68}$$

If α_n^{cc} is the abscissa of convergence of the global cocyclic Dirichlet series, then

$$2 - \frac{2}{n-1} \le \alpha_n^{\mathrm{cc}} \le 2, \qquad \lim_{n\to\infty} \alpha_n^{\mathrm{cc}} = 2. \tag{69}$$

The coefficients, and consequently the abscissae, are nondecreasing with n.

Proof. There are p^{2m-2} possible pairs in $(pA)^2$, giving the upper bound. For the lower bound take all pairs with

$$v_p(B) \geq \lceil m/(n-1) \rceil, \qquad v_p(C) \geq \lceil 2m/(n-1) \rceil.$$

Here a zero residue has truncated valuation m. Every monomial $B^u C^v$ of U_j has $u + 2v = j - 1$. For these pairs its valuation is at least $(u + 2v)m/(n-1)$. Therefore both U_n and U_{n+1} vanish modulo p^m. The number of the selected pairs is exactly the lower bound in (68).

For real $\sigma > 2$, the upper bound gives

$$\sum_{m \geq 1} a_n^{\mathrm{cc}}(p^m) p^{-m\sigma} \leq \frac{p^{-\sigma}}{1 - p^{2-\sigma}}.$$

Summing over primes is finite, since the denominator is bounded below by $1 - 2^{2-\sigma} > 0$. The Euler product of these nonnegative local series then converges absolutely; the identity with the global series follows from the prime-by-prime lattice correspondence. This proves $\alpha_n^{\mathrm{cc}} \leq 2$.

On the other hand set $m = n - 1$ in the lower bound, giving $a_n^{\mathrm{cc}}(p^{n-1}) \geq p^{2n-5}$. The global series at $\sigma = 2 - 2/(n-1)$ therefore dominates

$$\sum_p p^{2n-5-(n-1)\sigma} = \sum_p \frac{1}{p} = \infty.$$

For clarity, the last divergence follows from Euler's argument: convergence of $\sum_p 1/p$ would make $\prod_p (1 - 1/p)^{-1}$ finite, whereas its partial products dominate the partial sums of the divergent harmonic series. Thus the lower bound for the abscissa follows, and the limit is the squeeze consequence of the two bounds.

Finally the inverse image of a unital subring under $\mathbb{Z}[t]/(t^{n+1}) \to \mathbb{Z}[t]/(t^n)$ has the same additive quotient as that subring. Inverse image is injective and preserves both index and cyclicity. This proves coefficientwise monotonicity and hence monotonicity of the abscissae. The same inverse-image observation preserves all nontrivial cotype factors, adding one trivial factor. □

A Finite comparisons and coefficient checks

The numerical calculations given here are available from

`https://github.com/rtakloo/Chimni`

The quintic argument needs exact maxima over a finite set of diagonal types. This appendix records that entire calculation, so its role in the proof can be checked without an external data file. The loops use only integer arithmetic; they are also an explicit enumeration prescription that can be followed directly. The restrictions $a + b + c + d = m$ and (23) make it finite; every admissible quadruple occurs exactly once. The test uses $2E \geq 3m - 2$ to avoid floating-point arithmetic.

```
from fractions import Fraction

def diagonal_data(m):
    for a in range(m + 1):
        for b in range(min(2*a, m-a) + 1):
            for c in range(min(a+b, m-a-b) + 1):
                d = m-a-b-c
                if not 0 <= d <= min(a+c, 2*b):
                    continue
                e = min(a, 2*a-b)
```

```
                h = min(d, e)
                delta = min(c+d, c+b, c+a, a+b,
                            d+a, d+2*a-b, 2*a,
                            2*a+b-c, 3*a-c)
                E = min(b+c+d+delta+h,
                        b+c+2*d+min(c+h, e))
                yield (a,b,c,d), E

counts = [1, 3, 6, 11, 17, 27, 35, 50, 64, 87]
nexceptional = [0, 1, 1, 1, 1, 2, 0, 1, 0, 1]
thresholds = [(1,1), (1,1), (4,3), (5,4), (7,5),
              (4,3), (10,7), (11,8), (13,9), (7,5)]
exceptional = []
for m in range(1, 11):
    rows = list(diagonal_data(m))
    bad = [typ for typ, E in rows if 2*E >= 3*m-2]
    good = [E for typ, E in rows if 2*E < 3*m-2]
    assert len(rows) == counts[m-1]
    assert len(bad) == nexceptional[m-1]
    assert max(Fraction(E+1, m) for E in good) == \
           Fraction(*thresholds[m-1])
    exceptional.extend(bad)
assert sum(counts) == 301
assert exceptional == [
    (1,0,1,0), (1,1,0,1), (1,1,1,1), (1,1,1,2),
    (2,1,1,2), (2,2,0,2), (2,2,1,3), (2,2,2,4)]
```

For the extended comparison in Lemma 5.8, continue the same script with the following exhaustive integer check.

```
expected_counts = [108, 136, 165, 202, 242, 290]
expected_maxima = [15, 16, 18, 19, 21, 22]
for m in range(11, 17):
    rows = list(diagonal_data(m))
    assert len(rows) == expected_counts[m-11]
    assert max(E for typ, E in rows) == expected_maxima[m-11]
    if m == 15:
        assert [typ for typ, E in rows if E == 21] == [(3,3,3,6)]
        assert max(E for typ, E in rows
                   if typ != (3,3,3,6)) == 20
```

There are 301 admissible types with $1 \le m \le 10$. The following table records their distribution. In its last column, the maximum is taken over the nonexceptional types of the indicated total exponent. Since E is an upper bound for the exponent of p in (34), the number $(E+1)/m$ is the threshold supplied by that estimate for absolute summation over primes.

m	Admissible types	Exceptional types	$\max(E+1)/m$
1	1	0	1
2	3	1	1
3	6	1	4/3
4	11	1	5/4
5	17	1	7/5
6	27	2	4/3
7	35	0	10/7
8	50	1	11/8
9	64	0	13/9
10	87	1	7/5

For coefficient checks in the second class of Lemma 5.9, the following symmetry reduces the number of pairs that must be examined. Fix $m \geq 1$ and put $A = \mathbb{Z}/p^m\mathbb{Z}$. If $\alpha \in A^\times$, the precomposition of the defining character with the automorphism $t \mapsto \alpha t$, followed by normalization at t, sends

$$(B, C, D) \longmapsto (\alpha B, \alpha^2 C, \alpha^3 D).$$

It preserves multiplicative closure of the kernel and is transitive on the choices of B with any fixed valuation $1 \leq r < m$. For each such r, one may therefore set $B = p^r$, enumerate $C \in pA$, put $D = 2BC - B^3$, and test products of the three kernel generators directly in $A[t]/(t^5)$. Multiplying the result by $(p-1)p^{m-r-1}$ accounts for all B of valuation r; the case $B = 0$ is counted separately. For example, (51) gives the first split contribution:

$$a_5^{\mathrm{cc}}(11^5) = 21 \cdot 11^5 = 3382071.$$

The ramified value is $a_5^{\mathrm{cc}}(5^5) = 15625$; here $\rho_5(2) = 0$, whereas $\rho_{11}(1) = \rho_{11}(2) = 2$.

The first coefficients of $Z_{5,p}$, obtained by Hermite enumeration with linear lifting for the last column, are:

$p\backslash m$	0	1	2	3	4	5	6
2	1	1	7	27	115	323	1411
3	1	1	13	76	589	2371	21325
5	1	1	31	306	5431	46681	815431

A.1 Supplementary checks

The program `verify_chimni_20261110_131204_CST.py` available from

`https://github.com/rtakloo/Chimni`

checks finite coefficients independently by multiplying basis rows as truncated polynomials and applying exact triangular division. It also compares the stated cotype weights with integer minors, checks the exceptional diagonal counts, and tests the character and lifting constructions. A separate exact polynomial calculation checks the quartic rational identities after clearing denominators. The programs and their parameter ranges are supplied with the verification record. These supplementary tests can detect arithmetic and implementation errors; the assertions for arbitrary index follow from the proofs in the main text. The proof-critical finite comparisons are the exhaustive listings and tables printed above.

References

[1] S. Atanasov, N. Kaplan, B. Krakoff, and J. Menzel, *Counting finite index subrings of $\mathbb{Z}^n$ and $\mathbb{Z}[x]/(x^n)$*, arXiv:1609.06433v1.

[2] F. J. Grunewald, D. Segal, and G. C. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. **93** (1988), no. 1, 185–223. https://doi.org/10.1007/BF01393692.

[3] V. M. Petrogradsky, *Multiple zeta functions and asymptotic structure of free Abelian groups of finite rank*, J. Pure Appl. Algebra **208** (2007), no. 3, 1137–1158. https://doi.org/10.1016/j.jpaa.2006.05.010.

[4] G. Chinta, N. Kaplan, and S. Koplewitz, *The cotype zeta function of $\mathbb{Z}^d$*, Indag. Math. (N.S.) **34** (2023), no. 3, 643–659. https://doi.org/10.1016/j.indag.2023.01.003.

[5] S. H. Lee and S. Lee, *Cotype zeta functions enumerating subalgebras of R-algebras*, Indag. Math. (N.S.) **37** (2026), no. 6, 2239–2266; arXiv:2504.18908v2. https://doi.org/10.1016/j.indag.2026.06.005.

[6] T. Rossmann, *Zeta: computing zeta functions of groups, algebras, and modules*, SageMath package. https://torossmann.github.io/Zeta/.