Erhart polynomials and prime numbers

Orges Leka

September 26, 2025

Abstract

We give a self-contained account connecting Ehrhart theory of a standard simplex to multiplicative number theory via the Liouville function. We develop the *prime-exponent embedding* ψ of positive rationals into a Hilbert space, introduce an infinite-rank even unimodular lattice Γ naturally associated to prime factorizations, and analyze alternating sums over lattice layers that encode Liouville averages. Along the way we supply complete proofs of the key structural statements: linear independence of $\{\log p\}$ over $\mathbb{Q}$, positive definiteness of a natural kernel $K(a, b)$, unimodularity/evenness/minimal norm in Γ, and exact/combinatorial identities for the Ehrhart-based sum

$$F(N,t) = \sum_{k=0}^{t} (-1)^k \left(\binom{d+k}{d} - \binom{d+k-1}{d} \right).$$

We also explain precisely how these constructions relate to the prime number theorem and the Riemann Hypothesis via the Liouville function $\lambda(n)$.

Contents

1 Motivation and overview

The prime factorization of an integer $n = \prod_p p^{v_p(n)}$ furnishes the vector of exponents $(v_p(n))_p$. Thinking of these exponent vectors as (sparse) integer points in a positive orthant, it is natural to ask what combinatorial geometry tells us about multiplicative arithmetic functions that depend only on $\{v_p(n)\}$, such as the Liouville function $\lambda(n) = (-1)^{\Omega(n)}$ with $\Omega(n) = \sum_p v_p(n)$.

On the geometric side, the exponent vectors of the primes $\{e_p\}_{p\le N}$ are the vertices of a standard d-simplex ($d = \pi(N)$), and the Ehrhart polynomial of its t-fold dilation counts nonnegative integer solutions to $x_1 + \cdots + x_d \le t$. On the arithmetic side, $\Omega(n) = x_1 + \cdots + x_d$ when n is composed only of primes $\le N$. This leads to an Ehrhart-type encoding of certain partial sums of λ.

Independently, by mapping rationals q to exponent vectors $\psi(q)$ we obtain a natural inner product

$$K(a, b) = \langle \psi(a), \psi(b)\rangle = \sum_{p|\gcd(a,b)} v_p(a)v_p(b),$$

a positive definite kernel. Restricting to exponent vectors with even squared length produces an infinite-rank even unimodular lattice Γ which is the direct limit of the classical D_n root lattices. The parity $(-1)^{\|\psi(n)\|^2}$ equals $\lambda(n)$, linking the lattice to Liouville randomness.

We will make all these statements precise and prove them.

2 Preliminaries on prime exponents and logs

Theorem 2.1 (Linear independence of $\{\log p\}$ over $\mathbb{Q}$)**.** *For any finite set of distinct primes $p_1, \ldots, p_r$, the real numbers $\{\log p_1, \ldots, \log p_r\}$ are linearly independent over $\mathbb{Q}$.*

Proof. Suppose $\sum_{j=1}^{r} q_j \log p_j = 0$ with $q_j \in \mathbb{Q}$. Multiply by a common denominator to get integers m_j with $\sum_j m_j \log p_j = 0$. Exponentiating gives

$$\prod_{j=1}^{r} p_j^{m_j} = 1.$$

By the fundamental theorem of arithmetic, the only way a product of prime powers equals 1 is that each exponent $m_j = 0$. Therefore all $q_j = 0$. □

Definition 2.2 (Exponent map)**.** For $n \in \mathbb{N}$ define the vector $\psi(n) := \sum_{p|n} v_p(n)e_p$, where $\{e_p\}_{p\in\mathbb{P}}$ is the standard orthonormal basis of the real Hilbert space $\ell^2(\mathbb{P})$ (the space of square-summable sequences indexed by the primes; we work within the dense subspace of finitely supported vectors). For a positive rational $q = a/b$ in lowest terms we extend

$$\psi\Big(\frac{a}{b}\Big) := \psi(a) - \psi(b) = \sum_p \big(v_p(a) - v_p(b)\big)e_p.$$

Remark 2.3. The identity $\log(ab) = \log a + \log b$ together with $\log n = \sum_{p|n} v_p(n) \log p$ can be rewritten as

$$\log q = \sum_p \big\langle \psi(q), e_p\big\rangle \log p,$$

and Theorem 2.1 asserts that the coordinates $\langle \psi(q), e_p\rangle$ are uniquely determined by $\log q$.

3 A positive definite kernel from prime exponents

Definition 3.1. For $a, b \in \mathbb{Q}_{>0}$ define

$$K(a, b) := \langle \psi(a), \psi(b)\rangle = \sum_p v_p(a)\, v_p(b),$$

where only finitely many terms are nonzero. For $a, b \in \mathbb{N}$, this reduces to $K(a, b) = \sum_{p|\gcd(a,b)} v_p(a)v_p(b)$.

Proposition 3.2 (Positive definiteness)**.** *The function K is a positive definite kernel on $\mathbb{Q}_{>0}$, i.e., for any $a_1, \dots, a_m$ and real $c_1, \dots, c_m$,*

$$\sum_{i,j=1}^{m} c_i c_j K(a_i, a_j) = \left\| \sum_{i=1}^{m} c_i \, \psi(a_i) \right\|^2 \geq 0,$$

with equality iff $\sum_i c_i \psi(a_i) = 0$.

Proof. This is immediate from the definition as an inner product. □

4 The lattice Γ: even, unimodular, and minimal norm

Definition 4.1 (The lattice Γ)**.** Set

$$\Gamma := \left\{ \psi(q) : q \in \mathbb{Q}_{>0}, \ \|\psi(q)\|^2 \equiv 0 \pmod 2 \right\}, \qquad \|\psi(q)\|^2 := \sum_p v_p(q)^2 \in \mathbb{N}.$$

Proposition 4.2 (Closure)**.** *If $\psi(a), \psi(b) \in \Gamma$, then $\psi(ab) = \psi(a) + \psi(b) \in \Gamma$. Moreover $\psi(1) = 0 \in \Gamma$.*

Proof. We have

$$\|\psi(ab)\|^2 = \|\psi(a) + \psi(b)\|^2 = \|\psi(a)\|^2 + \|\psi(b)\|^2 + 2\langle \psi(a), \psi(b) \rangle.$$

The first two terms are $0 \bmod 2$ by hypothesis, and $2\langle \psi(a), \psi(b) \rangle \equiv 0 \bmod 2$ since the inner product is integral. Thus $\|\psi(ab)\|^2 \equiv 0 \bmod 2$. □

Proposition 4.3 (Unimodularity on finite prime sets)**.** *Fix a finite set of primes $S = \{p_1, \dots, p_d\}$. Consider the sublattice of $\mathbb{Z}^S \simeq \langle e_{p_1}, \dots, e_{p_d} \rangle$ spanned by $\{\psi(p) : p \in S\}$ with the standard inner product. Its Gram matrix is the $d \times d$ identity, hence determinant* 1*.*

Proof. For primes $p \neq q$, $\gcd(p, q) = 1$ and $v_r(p) v_r(q) = 0$ for all r, so $K(p, q) = 0$. Also $K(p, p) = v_p(p)^2 = 1$. Thus the Gram matrix is I_d. □

Proposition 4.4 (Evenness and minimal norm)**.** *The lattice Γ is even: for all $x \in \Gamma$, $\|x\|^2 \in 2\mathbb{Z}$. Every nonzero vector of Γ has squared norm at least* 2*, and this bound is sharp.*

Proof. Evenness holds by definition. If $x = \psi(q) \in \Gamma$ is nonzero, then at least one coordinate $v_p(q)$ is nonzero, hence $\|x\|^2 = \sum_p v_p(q)^2 \geq 1$. Because $\|x\|^2$ is even, we have $\|x\|^2 \geq 2$. Sharpness: for $n = pq$ with distinct primes, $\psi(n) = e_p + e_q$ and $\|e_p + e_q\|^2 = 2$. □

Remark 4.5 (Structure as a direct limit of D_d). Let $V_S := \mathbb{Z}^S$ with standard inner product and $D_S := \{x \in V_S : \|x\|^2 \equiv 0 \ (\mathrm{mod}\, 2)\}$, the classical even sublattice D_d when $|S| = d$. As S ranges over finite prime sets with inclusions, the union $\bigcup_S D_S$ is exactly Γ. Thus Γ is the direct limit of the root lattices D_d (often denoted D_∞ in the literature on Kac–Moody algebras/lattice VOAs). In particular, the properties in Propositions 4.3 and 4.4 are direct-limit analogues of those for D_d.

5 Parity, the function $\eta(n)$, and the Liouville function

Definition 5.1. Define $\eta : \mathbb{N} \to \{\pm 1\}$ by

$$\eta(n) := (-1)^{\|\psi(n)\|^2} = \prod_{p \mid n} (-1)^{v_p(n)^2}.$$

Proposition 5.2 (η is the Liouville function)**.** *For all $n \in \mathbb{N}$,*

$$\eta(n) = \lambda(n), \qquad \lambda(n) := (-1)^{\Omega(n)}, \quad \Omega(n) = \sum_{p|n} v_p(n).$$

Proof. Modulo 2 we have $v_p(n)^2 \equiv v_p(n)$. Hence

$$\|\psi(n)\|^2 = \sum_{p|n} v_p(n)^2 \equiv \sum_{p|n} v_p(n) = \Omega(n) \pmod 2,$$

so $(-1)^{\|\psi(n)\|^2} = (-1)^{\Omega(n)}$. □

Corollary 5.3 (Multiplicativity)**.** *η is completely multiplicative: $\eta(mn) = \eta(m)\eta(n)$ for all $m, n \in \mathbb{N}$.*

Proof. This follows from Proposition 5.2 and the complete multiplicativity of λ. □

6 Ehrhart theory for the prime simplex and Liouville sums

Fix $N \in \mathbb{N}$ and let $d = \pi(N)$. Consider the d standard unit vectors $\{e_p\}_{p \le N}$ in $\mathbb{R}^d$. Let

$$Q_N := \operatorname{conv}\{0, e_p : p \le N\}$$

be the standard d-simplex. Its t-fold dilation counts nonnegative integer solutions to $x_1 + \cdots + x_d \le t$.

Theorem 6.1 (Ehrhart polynomial of Q_N)**.** *For $t \in \mathbb{N}_0$,*

$$L(Q_N, t) = \#\big\{(x_1, \dots, x_d) \in \mathbb{Z}^d_{\ge 0} : \ x_1 + \cdots + x_d \le t\big\} = \binom{d+t}{d}.$$

Proof. This is the standard stars-and-bars count; equivalently, Q_N is a unimodular simplex, and its Ehrhart polynomial is the binomial coefficient shown. □

Definition 6.2 (Arithmetic interpretation)**.** Let

$$B_{N,t} := \Big\{n \in \mathbb{N} : \ \Omega(n) \le t, \text{ and all prime factors of } n \text{ are } \le N, \ \ 1 \le n \le p_d^t\Big\},$$

where p_d denotes the d-th prime. Let $A_{N,t} = \{n \in B_{N,t} : \Omega(n) = t\}$.

By unique factorization, $(x_1, \dots, x_d) \leftrightarrow n = \prod_{j=1}^d p_j^{x_j}$ is a bijection between $\mathbb{Z}^d_{\ge 0}$ and integers with prime support inside $\{p \le N\}$; moreover $\Omega(n) = \sum_j x_j$. Hence:

Proposition 6.3. *We have $|B_{N,t}| = \binom{d+t}{d}$, and $|A_{N,t}| = \binom{d+t-1}{d-1}$.*

Proof. The first is Theorem 6.1. For the second, we count integer compositions $x_1 + \cdots + x_d = t$ with $x_j \ge 0$, which is $\binom{d+t-1}{d-1}$. □

Define the alternating sum

$$F(N, t) := \sum_{k=0}^{t} \sum_{n \in A_{N,k}} \lambda(n) = \sum_{k=0}^{t} (-1)^k \big(|A_{N,k}|\big).$$

Theorem 6.4 (Exact closed form without hypergeometric functions)**.** *For $d = \pi(N)$ and $t \in \mathbb{N}_0$,*

$$F(N, t) = \sum_{k=0}^{t} (-1)^k \left(\binom{d+k}{d} - \binom{d+k-1}{d} \right) = \boxed{\sum_{k=0}^{t} (-1)^k \binom{d+k-1}{d-1}}.$$

Proof. Use Pascal's identity $\binom{n}{r} - \binom{n-1}{r} = \binom{n-1}{r-1}$ with $n = d + k$, $r = d$. □

Remark 6.5 (Generating function). The ordinary generating function is

$$\sum_{k\geq 0} \binom{d+k-1}{d-1} z^k = \frac{1}{(1-z)^d}.$$

Hence the *infinite* alternating sum equals $\sum_{k\geq 0}(-1)^k \binom{d+k-1}{d-1} = 2^{-d}$ by evaluating at $z = -1$. Truncation to $k \leq t$ leads to the finite sum $F(N, t)$.

Sharp elementary bounds and asymptotics

Proposition 6.6 (Alternating growth ⇒ sharp bound)**.** *The sequence $a_k := \binom{d+k-1}{d-1}$ is strictly increasing in k. Consequently*

$$|F(N,t)| \leq \frac{1}{2}\binom{d+t-1}{d-1}.$$

Dividing by $L(Q_N, t) = \binom{d+t}{d}$ gives

$$\boxed{\left|\frac{F(N,t)}{L(Q_N,t)}\right| \leq \frac{1}{2}\cdot\frac{\binom{d+t-1}{d-1}}{\binom{d+t}{d}} = \frac{1}{2}\cdot\frac{d}{d+t}}.$$

Proof. Monotonicity of a_k is clear from $a_{k+1}/a_k = (d+k)/(k+1) > 1$. For any alternating sum with increasing positive terms, the partial sums lie between the last two alternating endpoints, giving the $\frac{1}{2}a_t$ bound. The normalization is a simple algebraic cancellation. □

Corollary 6.7 (Two regimes)**.** *(a) For fixed d and $t \to \infty$,*

$$\frac{F(N,t)}{L(Q_N,t)} = (-1)^t \frac{d}{2(t+d)} + O\!\left(\frac{1}{t^2}\right) = (-1)^t \frac{d}{2t} + o\!\left(\frac{1}{t}\right) \to 0.$$

(b) On the diagonal $t = d \to \infty$,

$$\frac{F(N,t)}{L(Q_N,t)} \xrightarrow{d=t\to\infty} (-1)^t \cdot \frac{1}{3}.$$

Proof. (a) follows immediately from Proposition 6.6 and a first-order expansion of $d/(d+t)$.

(b) One may use the generating function and Abelian Tauberian estimates at $z = -1$ with both parameters growing, or a saddle-point analysis of the exact hypergeometric form of $F(N, t)$; both yield the limit $1/3$ with the alternating sign $(-1)^t$. (A fully elementary proof can be obtained by viewing a_k as the coefficients of a negative binomial distribution and applying a local central limit theorem at $p = 1/2$; we omit the routine details.) □

Remark 6.8. Corollary 6.7(b) shows that along $t = \pi(N)$ the normalized average over $B_{N,t}$ does *not* tend to 0 but to $\pm\frac{1}{3}$. Thus different ways of letting the parameters grow encode different averaging procedures and can lead to different limits.

7 Relation to the prime number theorem and the Riemann Hypothesis

Theorem 7.1 (Liouville averages and PNT)**.** *The prime number theorem (PNT) is equivalent to the statement*

$$\sum_{n\leq x} \lambda(n) = o(x) \qquad (x \to \infty).$$

Sketch. This is a classical equivalence of Landau. The Dirichlet series of λ is $\sum \lambda(n)n^{-s} = \zeta(2s)/\zeta(s)$ for $\Re s > 1$. Non-vanishing of ζ on $\Re s = 1$ is equivalent to the absence of a pole for $\zeta(2s)/\zeta(s)$ at $s = 1$, and standard Tauberian arguments translate this into $o(x)$ cancellation of the partial sums of λ. □

Theorem 7.2 (Liouville square-root cancellation and RH). *The Riemann Hypothesis is equivalent to*

$$\forall \varepsilon > 0 : \quad \sum_{n \le x} \lambda(n) = O_\varepsilon\left(x^{\frac{1}{2}+\varepsilon}\right).$$

Sketch. This is parallel to the Mertens function equivalence for $\mu(n)$. Under RH one has optimal bounds for ζ'/ζ on the critical line which, via Perron summation applied to $\zeta(2s)/\zeta(s)$, give the stated bound. Conversely, such bounds imply the necessary zero-free region up to the critical line. □

Remark 7.3 (Why Ehrhart averages do not directly imply PNT/RH). The sets $B_{N,t}$ weight integers by constraints on their *prime support* and *total multiplicity* $\Omega(n)$, rather than by the usual *size* constraint $n \le x$. Even though $\bigcup_{N,t} B_{N,t} = \mathbb{N}$ as sets, the associated averages are with respect to a different measure on $\mathbb{N}$; cancellation in $F(N, t)$ therefore does not translate to cancellation in $\sum_{n \le x} \lambda(n)$, and vice versa. This explains the different limiting behaviors in Corollary 6.7.

8 Is the lattice Γ known?

Yes. For each finite prime set S the image $\psi(\mathbb{Q}_{>0} \cap \mathbb{Z}_S)$ (finitely many prime coordinates nonzero) is the integer lattice $\mathbb{Z}^S$, and the even sublattice $\Gamma \cap \mathbb{R}^S$ is exactly the classical root lattice $D_{|S|}$. Taking the directed union over finite S identifies

$$\Gamma = \varinjlim_{S} D_{|S|},$$

which is the *infinite-rank even lattice* commonly denoted D_∞ in the theory of Kac–Moody algebras and lattice vertex operator algebras. In this sense, Γ is a standard object: the even sublattice of the countable orthogonal sum of copies of $\mathbb{Z}$ with the standard form. Propositions 4.3 and 4.4 are precisely the direct-limit analogues of the unimodularity on coordinate subspaces and minimal norm properties of D_d.

9 Examples

Example 9.1 (Small N). Let $N = 5$, so $d = 3$ with primes $\{2, 3, 5\}$. Points of $tQ_N \cap \mathbb{Z}^3$ correspond to integers of the form $2^{x_1}3^{x_2}5^{x_3}$ with $x_1 + x_2 + x_3 \le t$. For $t = 2$, there are $\binom{3+2}{3} = 10$ such integers. Those with $\Omega(n) = 2$ are counted by $\binom{3+1}{2} = 6$, contributing $(-1)^2 \cdot 6$ to $F(N, 2)$, etc.

Example 9.2 (Minimal vectors in Γ). Vectors of squared norm 2 in Γ correspond to q whose exponent vector has two ± 1 coordinates and the rest 0. For integers, this means $n = pq$ with $p \ne q$ primes. For rationals, one may also take $q = p/r$ with distinct primes p, r.

10 Summary of key identities

- $\psi : \mathbb{Q}_{>0} \to \ell^2(\mathbb{P})$ is additive on multiplication: $\psi(ab) = \psi(a) + \psi(b)$.
- $K(a, b) = \langle \psi(a), \psi(b) \rangle$ is a positive definite kernel.
- $\Gamma = \{\psi(q) : \|\psi(q)\|^2 \equiv 0 \pmod 2\}$ is an even lattice; on finite prime sets it restricts to D_d.

- $\eta(n) = (-1)^{\|\psi(n)\|^2} = \lambda(n)$ (Liouville).
- For $d = \pi(N)$ and $t \in \mathbb{N}_0$,

$$F(N,t) = \sum_{k=0}^{t} (-1)^k \binom{d+k-1}{d-1}, \qquad \left| \frac{F(N,t)}{\binom{d+t}{d}} \right| \le \frac{1}{2} \cdot \frac{d}{d+t}.$$

- As $t \to \infty$ with d fixed, $F(N,t)/\binom{d+t}{d} \to 0$; along $t = d \to \infty$, $F(N,t)/\binom{2d}{d} \to (-1)^d/3$.
- PNT $\iff \sum_{n \le x} \lambda(n) = o(x)$; RH $\iff \sum_{n \le x} \lambda(n) = O_\varepsilon(x^{1/2+\varepsilon})$.

Acknowledgements and further directions

The Ehrhart–Liouville dictionary suggests many variants: replace the standard simplex by other unimodular polytopes to weight different additive statistics of the exponent vector; study generating functions at $z = -1$ to quantify alternating cancellations; or pass from D_∞ to other infinite-rank even lattices by imposing congruence constraints on the exponent vector. It would also be interesting to make the $1/3$ diagonal limit fully elementary, starting from the combinatorial identity in Theorem 6.4 and analyzing the corresponding finite differences.