Injectivity criteria for smallest prime q congruent to 1 mod (p)-function via linear independence of primes

Orges Leka

November 22, 2025

Abstract

We revisit the partition of the prime numbers into linearly independent and linearly dependent primes, defined in terms of the exponent vectors of $p-1$ in the basis of all primes, and we develop its arithmetic and dynamical consequences for the successor map

$$\Phi(p) := \min\{q \text{ prime} : q \equiv 1 \pmod{p}\}.$$

On the structural side, we show that the image of Φ is exactly the set of linearly independent primes, and that Φ extends multiplicatively to a map $\Phi\colon \mathbb{N} \to \mathbb{N}$ whose image consists precisely of LI-numbers. This leads to a factorisation of the Riemann zeta function

$$\zeta(s) = G(s)H(s),$$

where G and H are Dirichlet series attached to LI- and LD-numbers, respectively, and to a "dynamical" Dirichlet series

$$G_b(s) = \sum_{n\geq 1} \Phi(n)^{-s},$$

whose coefficients encode the multiplicities of Φ on LI-numbers. We give an arithmetical description of the dynamically weighted zeta function $\zeta_b(s) := G_b(s)H(s)$ in terms of the LI/LD–components $\ell_{LI}(n), \ell_{LD}(n)$ of an integer and the associated divisor sums LLD, LLI, and we derive a purely arithmetical injectivity criterion for Φ in terms of $LLD(\Phi(n))$. Using the unimodular "Φ-lattice" we obtain explicit logarithmic representations for $p-1$ when p is LD and introduce an auxiliary operator ψ with terminal value $\psi_\infty(p)$, leading to an infinite descent mechanism via a map α. Finally, we define a class of H-numbers by the growth condition $\Phi(n) \leq \log \Phi(n!)$, prove a quadratic upper bound $\Phi(n) < n^2$ on H-numbers and injectivity of Φ on H-primes, and discuss numerical evidence and a heuristic that suggest the existence of infinitely many H-primes and an "H-dominant" regime for the dynamical zeta function.

Contents

1 Introduction

The Euler product for the Riemann zeta function

$$\zeta(s) \;=\; \prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}}, \qquad \Re s > 1,$$

expresses ζ as an infinite product over all primes $\mathbb{P}$ and provides the starting point for much of analytic number theory. In this paper we refine this product by splitting the primes into two canonical, infinite subsets

$$\mathbb{P} = \mathbb{P}_{LI} \,\dot\cup\, \mathbb{P}_{LD},$$

the *linearly independent* and *linearly dependent* primes, according to linear relations among the exponent vectors of $p-1$ in the basis of all primes. This LI/LD–partition leads simultaneously to a nontrivial filtration of the prime sequence $p_1 = 2 < p_2 = 3 < p_3 = 5 < \ldots$ and to a dynamical picture governed by a successor map on primes.

More precisely, we consider the map

$$\Phi(p) := \min\{q \in \mathbb{P} : q \equiv 1 \pmod p\},$$

the least prime congruent to 1 modulo p. The size of $\Phi(p)$ is a classical object of study in analytic number theory, going back to work on the least prime in an arithmetic progression and bounds for primes in residue classes. Under GRH, explicit bounds of the form $\Phi(p) \ll p^2 \log^2 p$ follow from the work of Bach and Sorenson [4], while unconditional results of Heath–Brown, Wagstaff and Xylouris [5, 6, 7, 8, 9] give successively sharper estimates in the style of Linnik's theorem. On the computational side, tables of least primes in progressions and related sequences (see, for instance, Wilson's data [2] or the entries in OEIS) provide substantial numerical evidence about the typical size and distribution of such least primes.

Our approach to Φ is of a different flavour. Instead of focusing on upper bounds for $\Phi(p)$, we study the *structure* of its image and preimage sets by exploiting linear relations among the vectors of prime exponents in $p-1$. This is reminiscent in spirit of previous work of Bach and Huelsbergen on small generating sets of multiplicative groups modulo m [3], and of the algorithmic viewpoint on primes in residue classes and related computations in Bach and Shallit [1]. Here, however, we work on the level of the integers $p-1$ themselves and use the resulting LI/LD–decomposition to build a "Φ–lattice" which governs the behaviour of the successor map.

The goals of this paper are threefold:

(1) to give a self-contained account of the LI/LD notion for primes and its consequences for the successor map Φ;

(2) to record the resulting factorisation

$$\zeta(s) = G(s)\,H(s) = \prod_{q \in \mathbb{P}_{LI}} \frac{1}{1-q^{-s}} \prod_{p \in \mathbb{P}_{LD}} \frac{1}{1-p^{-s}}, \qquad \Re s > 1,$$

and to reinterpret the Dirichlet series G and H in terms of an LI/LD–decomposition of the integers and a "Φ–lattice";

(3) to introduce a dynamical Dirichlet series

$$G_b(s) := \sum_{n \geq 1} \Phi(n)^{-s},$$

together with an associated zeta function $\zeta_b(s) = G_b(s)H(s)$, and to relate their coefficients to the multiplicities of Φ and to certain divisor sums built from the LI/LD–components of n.

On the dynamical side we show that the image of Φ on primes is precisely $\mathbb{P}_{LI}$, and that each LI-prime admits a unique predecessor under Φ, whereas LD-primes never occur as successors. Extending Φ multiplicatively to $\mathbb{N}$ leads to a natural notion of LI- and LD-numbers and a structural factorisation $\zeta = G \cdot H$ of the Riemann zeta function into LI- and LD-zeta factors. We

then define an auxiliary operator ψ with terminal value $\psi^{\infty}(p)$ and a map α which together provide an infinite descent mechanism in the Φ–lattice, yielding explicit logarithmic representations of $p-1$ in terms of $(r-1)$ for LI-primes $r<p$ when p is LD.

In the final part of the paper we single out a class of integers $n \geq 2$ defined by the growth condition

$$\Phi(n) \leq \log \Phi(n!),$$

which we call H-numbers. For H-numbers we prove a quadratic upper bound $\Phi(n) < n^2$, in strong contrast with the general exponential bounds known for $\Phi(p)$, and we show that Φ is injective on the H-primes. This leads to an "H-dominant" regime for the dynamical zeta function $\zeta_b(s)$ and to a heuristic—supported by numerical data—that there should be infinitely many H-primes.

Throughout the paper we work analytically in the half-plane $\Re s > 1$: all Euler products and Dirichlet series we introduce converge absolutely there, and we do not claim any new analytic continuation or functional equations for G, H, or G_b. The emphasis is on the structural interaction between the LI/LD–decomposition, the successor map Φ, and the induced dynamical Dirichlet series.

2 Linear independence for primes

We briefly recall the definition of LI/LD primes introduced in [13].

2.1 Exponent vectors

Let $(p_i)_{i\geq 1}$ be the increasing sequence of primes:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5, \dots.$$

For each integer $n \geq 2$ we define the (infinite) exponent vector

$$\varphi(n) := \big(v_{p_1}(n-1), v_{p_2}(n-1), v_{p_3}(n-1), \dots\big) \in \prod_{i\geq 1} \mathbb{Z},$$

where $v_{p_i}(\cdot)$ denotes the p_i-adic valuation. Only finitely many coordinates of $\varphi(n)$ are nonzero.

For many arguments it is convenient to truncate these vectors. If $N \geq 2$ is fixed, we set

$$\varphi_N(n) := \big(v_{p_1}(n-1), \dots, v_{p_{\pi(N)}}(n-1)\big) \in \mathbb{Z}^{\pi(N)}.$$

For primes $r \leq N$ we then regard $\varphi_N(r)$ as vectors in the finite-dimensional space $\mathbb{Q}^{\pi(N)}$.

2.2 Definition of LI/LD primes

Definition 2.1 (LI and LD primes)**.** A prime q is called *linearly independent* (LI) if the vector $\varphi(q)$ does not lie in the $\mathbb{Q}$-linear span of the vectors $\varphi(r)$ with r prime and $r < q$. Otherwise q is called *linearly dependent* (LD).

Equivalently, fix some $N \geq q$ and work with the truncated vectors $\varphi_N(r) \in \mathbb{Q}^{\pi(N)}$ for all $r \leq q$. Then q is LI if and only if

$$\varphi_N(q) \notin \operatorname{span}_{\mathbb{Q}}\{\varphi_N(r) : r < q,\ r \text{ prime}\}.$$

This definition produces two disjoint infinite subsets of primes:

$$\mathbb{P}_{\mathrm{LI}} := \{q \in \mathbb{P} : q \text{ LI}\}, \qquad \mathbb{P}_{\mathrm{LD}} := \mathbb{P} \setminus \mathbb{P}_{\mathrm{LI}}.$$

3 The successor map Φ and its extension

3.1 Definition on primes

For a prime p we define its *successor* in the progression $1 \bmod p$ by

$$\Phi(p) := \min\{q \in \mathbb{P} : q \equiv 1 \pmod{p}\}.$$

By Dirichlet's theorem on primes in arithmetic progressions, the set $\{q \in \mathbb{P} : q \equiv 1 \bmod p\}$ is infinite, so $\Phi(p)$ is well-defined for every prime p.

A basic observation, proved in detail in [13], is that $\Phi(p)$ is always LI:

Proposition 3.1 (Minimal primes in $1 \bmod p$ are LI)**.** *Let p be a prime and let $q = \Phi(p)$ be the smallest prime with $q \equiv 1 \pmod{p}$. Then q is linearly independent.*

The proof uses exactly the p-th coordinate of the exponent vectors: $v_p(q-1) \geq 1$, whereas $v_p(r-1) = 0$ for all primes $r < q$ by minimality of q in its residue class.

3.2 Multiplicative extension

We extend Φ to all positive integers by declaring it completely multiplicative.

Definition 3.2 (Multiplicative extension of Φ)**.** We set

$$\Phi(1) := 1,$$

and for any integer $n \geq 2$ with prime factorization $n = \prod_{p^e \| n} p^e$ we define

$$\Phi(n) := \prod_{p^e \| n} \Phi(p)^e.$$

Then Φ is a (completely) multiplicative map $\Phi : \mathbb{N} \to \mathbb{N}$, and Proposition 3.1 implies that

$$\Phi(n) \in \{\text{LI-numbers}\}$$

for all $n \geq 1$. In particular, any prime in the image of Φ is LI.

4 The successor map and surjectivity onto LI primes

In this section we recall the successor map

$$\Phi(p) := \min\{\, q \text{ prime} : q \equiv 1 \pmod{p} \,\},$$

which is well-defined for every prime p by Dirichlet's theorem on primes in arithmetic progressions. We then prove in detail that the image of Φ is *exactly* the set of linearly independent primes.

Throughout we let $(p_k)_{k\geq 1}$ denote the increasing sequence of primes,

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5, \ldots.$$

4.1 Linear independence via valuation vectors

For each integer $n \geq 2$ we consider the exponent vector of $n-1$

$$\varphi(n) := \big(v_{p_1}(n-1), v_{p_2}(n-1), v_{p_3}(n-1), \ldots\big) \in \prod_{i\geq 1} \mathbb{Z},$$

where v_{p_i} is the p_i–adic valuation. Only finitely many coordinates of $\varphi(n)$ are nonzero.

Definition 4.1 (LI and LD primes)**.** A prime q is called *linearly independent* (LI) if $\varphi(q)$ does not lie in the $\mathbb{Q}$–linear span of the vectors $\varphi(r)$ with r prime and $r < q$. Otherwise q is called *linearly dependent* (LD).

Equivalently, if we fix $N \geq q$ and truncate to the first $\pi(N)$ coordinates

$$\varphi_N(n) := \big(v_{p_1}(n-1), \ldots, v_{p_{\pi(N)}}(n-1)\big) \in \mathbb{Z}^{\pi(N)},$$

then q is LI iff $\varphi_N(q)$ is not in the $\mathbb{Q}$–span of $\{\varphi_N(r) : r \text{ prime}, r < q\}$.

4.2 Minimal primes in $1 \bmod p$ are LI

We first show that successors of primes are always LI.

Lemma 4.2 (Minimal primes modulo p are LI)**.** *Let p be a prime, and let q be the smallest prime with*

$$q \equiv 1 \pmod{p}.$$

Then q is linearly independent.

Proof. Since $q \equiv 1 \pmod{p}$ we have $p \mid (q-1)$ and hence

$$v_p(q-1) \ \geq\ 1.$$

Fix $N \geq q$ and consider the truncated vectors $\varphi_N(r)$ in $\mathbb{Q}^{\pi(N)}$. Let $p = p_i$ for some index i. Then the i–th coordinate of $\varphi_N(q)$ is

$$(\varphi_N(q))_i = v_p(q-1) \geq 1.$$

Now let r be any prime with $r < q$. By minimality of q in the progression $1 \bmod p$ there is no such r with $r \equiv 1 \pmod{p}$, so $p \nmid (r-1)$ and thus

$$v_p(r-1) = 0 \qquad \text{for all primes } r < q.$$

Equivalently,

$$(\varphi_N(r))_i = 0 \qquad \text{for all primes } r < q.$$

Suppose for contradiction that $\varphi_N(q)$ lies in the $\mathbb{Q}$–span of $\{\varphi_N(r) : r < q\}$. Then there exist rational numbers c_r (finitely many nonzero) such that

$$\varphi_N(q) = \sum_{r<q} c_r \, \varphi_N(r).$$

Comparing the i–th coordinate on both sides gives

$$v_p(q-1) = (\varphi_N(q))_i = \sum_{r<q} c_r \, (\varphi_N(r))_i = \sum_{r<q} c_r \cdot 0 = 0,$$

a contradiction. Hence $\varphi_N(q)$ is not in the $\mathbb{Q}$–span of $\{\varphi_N(r) : r < q\}$, and q is LI. □

As an immediate consequence we obtain:

Proposition 4.3 (LD primes are never successors)**.** *Let p be a linearly dependent prime. Then p is not in the image of the successor map Φ, i.e. there is no prime r with*

$$\Phi(r) = p.$$

Proof. Suppose, for contradiction, that p is LD and that there exists a prime r with $\Phi(r) = p$. By definition of Φ this means that p is the smallest prime with $p \equiv 1 \pmod{r}$, i.e. p is the minimal prime in the residue class $1 \bmod r$. By Lemma 4.2, p is then LI, contradicting the assumption that p is LD. Hence no LD prime lies in the image of Φ. □

Thus we already know:

$$\mathrm{im}(\Phi) \subseteq \{\text{LI primes}\}.$$

We now prove the converse inclusion.

4.3 The valuation matrix and first occurrence indices

To describe the *predecessor* of an LI prime, we recall the valuation matrix from [13].

For each integer $n \geq 1$ we consider the $n \times n$ matrix

$$E(n) = (e_{i,k})_{1 \leq i,k \leq n}, \qquad e_{i,k} := v_{p_i}(p_k - 1).$$

The k–th column of $E(n)$ is exactly the truncated valuation vector

$$V_k^{(n)} := \begin{pmatrix} v_{p_1}(p_k - 1) \\ v_{p_2}(p_k - 1) \\ \vdots \\ v_{p_n}(p_k - 1) \end{pmatrix} = \varphi_n(p_k) \in \mathbb{Z}^n.$$

Note that if p_i divides $p_k - 1$, then necessarily $p_i < p_k$, so $i < k$. In particular the diagonal entries $e_{k,k} = v_{p_k}(p_k - 1)$ are all zero.

As in [13], linear independence of p_n is equivalent to a rank jump of $E(n)$ when we pass from $n - 1$ to n.

Next we introduce the *first occurrence index* of each prime p_i as a divisor of some $p_k - 1$.

Definition 4.4 (First occurrence index)**.** For each $i \geq 1$ define

$$t(i) := \min\{\, k \geq 1 : v_{p_i}(p_k - 1) \geq 1 \,\},$$

if this set is nonempty, and set $t(i) := \infty$ otherwise.

If $t(i) < \infty$, then $p_i \mid (p_{t(i)} - 1)$ and, as noted above, we automatically have $t(i) \geq i + 1$.

The following rank formula is proved in [13, Prop. 4.2] and we recall it for completeness.

Proposition 4.5 (Rank of the valuation matrix)**.** *For each $n \geq 1$ we have*

$$\operatorname{rank} E(n) = \#\{\, i \in \{1, \ldots, n\} : t(i) \leq n \,\}.$$

Proof. Let

$$I_n := \{\, i \in \{1, \ldots, n\} : t(i) \leq n \,\}, \qquad r(n) := \#I_n.$$

Lower bound. List the elements of I_n as $i_1, \ldots, i_{r(n)}$ in such a way that

$$t(i_1) < t(i_2) < \cdots < t(i_{r(n)}).$$

Consider the $r(n) \times r(n)$ submatrix M of $E(n)$ with rows indexed by $i_1, \ldots, i_{r(n)}$ and columns indexed by $t(i_1), \ldots, t(i_{r(n)})$.

By definition of $t(i_\ell)$, in row i_ℓ all entries in columns $k < t(i_\ell)$ are zero, and the entry in column $t(i_\ell)$ is

$$v_{p_{i_\ell}}\big(p_{t(i_\ell)} - 1\big) \;\geq\; 1.$$

Since $t(i_1) < \cdots < t(i_{r(n)})$, this means that M is (up to permutation of rows or columns) triangular with nonzero diagonal entries. Hence $\det M \neq 0$ and $\operatorname{rank} M = r(n)$. Therefore

$$\operatorname{rank} E(n) \;\geq\; r(n).$$

Upper bound. If $i \notin I_n$, i.e. $t(i) > n$, then by definition $v_{p_i}(p_k - 1) = 0$ for all $k \leq n$. Thus the i–th row of $E(n)$ is identically zero and does not contribute to the rank. Hence the row space of $E(n)$ is spanned by the rows with $i \in I_n$, so

$$\operatorname{rank} E(n) \;\leq\; \#I_n = r(n).$$

Combining both inequalities yields the claimed equality. □

4.4 Every LI prime has a predecessor

We now use Proposition 4.5 to show that every LI prime arises as a successor of a smaller prime.

Lemma 4.6 (First occurrence attached to an LI prime)**.** *Let $q = p_n$ be a linearly independent prime. Then there exists at least one prime p_i dividing $q - 1$ such that*

$$t(i) = n,$$

i.e. q is the first prime for which p_i divides $p_k - 1$.

Proof. Since $q = p_n$ is LI, the vector $V_n^{(n)} = \varphi_n(p_n)$ is not in the $\mathbb{Q}$–span of the previous columns $V_1^{(n)}, \ldots, V_{n-1}^{(n)}$. Equivalently, the rank of $E(n)$ is strictly larger than the rank of the $(n-1) \times (n-1)$ principal submatrix $E(n-1)$:

$$\operatorname{rank} E(n) \;>\; \operatorname{rank} E(n-1).$$

By Proposition 4.5 we have

$$\operatorname{rank} E(n) = \#\{i : t(i) \leq n\}, \qquad \operatorname{rank} E(n-1) = \#\{i : t(i) \leq n-1\}.$$

Thus the strict inequality implies that there exists an index i with

$$t(i) = n.$$

By definition of $t(i)$ this means $v_{p_i}(p_n - 1) \geq 1$, i.e. $p_i \mid (p_n - 1) = q - 1$. □

For such a prime divisor p_i we now identify q as the minimal prime $1 \bmod p_i$.

Lemma 4.7 (Predecessor of an LI prime)**.** *Let $q = p_n$ be linearly independent, and choose a prime $p = p_i$ with $t(i) = n$ as in Lemma 4.6. Then q is the smallest prime with*

$$q \equiv 1 \pmod{p},$$

i.e. by definition

$$\Phi(p) = q.$$

Proof. Since $t(i) = n$, we have $v_{p_i}(p_n - 1) \geq 1$, so $p_i \mid (q-1)$ and hence $q \equiv 1 \pmod{p}_i$.

If there were a smaller prime $r < q$ with $r \equiv 1 \pmod{p}_i$, then $p_i \mid (r-1)$. By the definition of $t(i)$ as the *first* index k with $p_i \mid (p_k - 1)$, we would then have $t(i) \leq \text{index}(r) < n$, contradicting $t(i) = n$.

Thus no smaller prime $r < q$ satisfies $r \equiv 1 \pmod{p}_i$, so q is indeed the minimal prime in the residue class $1 \bmod p_i$. By the definition of the successor map, $\Phi(p_i) = q$. □

Combining Lemma 4.6 and Lemma 4.7 gives:

Proposition 4.8 (Every LI prime is a successor)**.** *For every linearly independent prime q there exists a prime $p < q$ such that*

$$\Phi(p) = q.$$

In particular, every LI prime lies in the image of Φ.

Together with Proposition 4.3 we obtain the following structural description of the successor map.

Corollary 4.9 (Image of Φ)**.** *The image of the successor map Φ is exactly the set of linearly independent primes:*

$$\text{im}(\Phi) = \{\, q \text{ prime} : q \text{ is LI} \}.$$

Equivalently, Φ induces a surjective map from the set of all primes onto the set of LI primes, and no LD prime occurs as a successor.

Remark 4.10. Note that none of the arguments in this section uses Hypothesis (H) or any upper bound of the form $\Phi(p) \ll p^2$. The only input from analytic number theory is Dirichlet's theorem (to guarantee that $\Phi(p)$ is defined for every prime p). All statements above are purely structural and unconditional.

5 LI- and LD-zeta functions and product decomposition

5.1 LI- and LD-zeta functions

We now define Dirichlet series attached to LI- and LD-numbers.

Definition 5.1 (LI- and LD-numbers)**.** A positive integer n is called an LI-number if all its prime divisors lie in $\mathbb{P}_{\mathrm{LI}}$, and an LD-number if all its prime divisors lie in $\mathbb{P}_{\mathrm{LD}}$.

The indicator functions of LI- and LD-numbers are multiplicative, so their Dirichlet series admit Euler products.

Definition 5.2 (LI- and LD-zeta functions)**.** For $\Re s > 1$ we set

$$G(s) := \sum_{\substack{n \geq 1 \\ n \text{ LI}}} \frac{1}{n^s} = \prod_{q \in \mathbb{P}_{\mathrm{LI}}} \frac{1}{1 - q^{-s}},$$

and

$$H(s) := \sum_{\substack{m \geq 1 \\ m \text{ LD}}} \frac{1}{m^s} = \prod_{p \in \mathbb{P}_{\mathrm{LD}}} \frac{1}{1 - p^{-s}}.$$

By absolute convergence of these Euler products for $\Re s > 1$, both G and H are holomorphic in the half-plane $\Re s > 1$.

Since every positive integer n factors uniquely as a product of an LI-number and an LD-number (by the partition $\mathbb{P} = \mathbb{P}_{\mathrm{LI}} \cup \mathbb{P}_{\mathrm{LD}}$ of primes), we obtain an immediate factorization of the Riemann zeta function.

Proposition 5.3 (Product decomposition of ζ)**.** *For $\Re s > 1$ we have*

$$\zeta(s) = G(s)\, H(s).$$

Equivalently,

$$\prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} = \Big(\prod_{q \in \mathbb{P}_{\mathrm{LI}}} \frac{1}{1 - q^{-s}} \Big) \Big(\prod_{p \in \mathbb{P}_{\mathrm{LD}}} \frac{1}{1 - p^{-s}} \Big).$$

Proof. This is immediate from the Euler product for $\zeta(s)$ and the partition of primes into $\mathbb{P}_{\mathrm{LI}}$ and $\mathbb{P}_{\mathrm{LD}}$. Every Euler factor $(1 - p^{-s})^{-1}$ with $p \in \mathbb{P}$ appears exactly once, either in the product over $\mathbb{P}_{\mathrm{LI}}$ or in that over $\mathbb{P}_{\mathrm{LD}}$, and the products converge absolutely for $\Re s > 1$. □

5.2 The dynamical zeta function $\widehat{G}$

The multiplicative extension of Φ leads naturally to another Dirichlet series, which encodes the "successor dynamics":

Definition 5.4 (Dynamical zeta function)**.** For $\Re s > 1$ we define

$$\widehat{G}(s) := \sum_{n \geq 1} \frac{1}{\Phi(n)^s}.$$

Since $\Phi(n) > n$ for all $n \geq 2$, we have $1/\Phi(n)^s \leq 1/n^{\Re s}$, so $\widehat{G}(s)$ converges absolutely for $\Re s > 1$.

Using Proposition **??**, we can rewrite $\widehat{G}(s)$ as a Dirichlet series supported on LI-numbers. For each LI-number m set

$$a(m) := \#\{n \geq 1 : \Phi(n) = m\}.$$

Then

$$\widehat{G}(s) = \sum_{\substack{m \geq 1 \\ m \text{ LI}}} \frac{a(m)}{m^s}, \qquad \Re s > 1.$$

By construction $a(m) \geq 1$ for all LI-numbers m (surjectivity of Φ onto LI), while the original $G(s)$ has coefficients identically equal to 1 on LI-numbers:

$$G(s) = \sum_{\substack{m \geq 1 \\ m \text{ LI}}} \frac{1}{m^s}.$$

Thus the comparison between G and $\widehat{G}$ is equivalent to understanding the *multiplicities* $a(m)$, i.e. how often a given LI-number appears as a successor value $\Phi(n)$.

Remark 5.5 (Injektivity of Φ vs. equality of G and $\widehat{G}$)**.** The map Φ is injective on LI-numbers if and only if $a(m) = 1$ for all LI-numbers m. Equivalently, Φ is injective if and only if

$$\widehat{G}(s) = G(s)$$

for some (and hence every) real $s > 1$, since the coefficients in $\widehat{G}(s) - G(s)$ are nonnegative. At present, the injectivity of Φ is an open problem.

6 Analytic remarks and open questions

We conclude by collecting some analytic observations and questions about G, H and $\widehat{G}$.

6.1 Analytic properties in $\Re s > 1$

By construction:

- $G(s)$, $H(s)$ and $\widehat{G}(s)$ are absolutely convergent Dirichlet series for $\Re s > 1$, with nonnegative coefficients.
- They admit Euler products in $\Re s > 1$:

  $$G(s) = \prod_{q \in \mathbb{P}_{\text{LI}}} (1 - q^{-s})^{-1}, \quad H(s) = \prod_{p \in \mathbb{P}_{\text{LD}}} (1 - p^{-s})^{-1},$$

  and $\widehat{G}(s)$ can be expressed as a Dirichlet series supported on LI-numbers with integer coefficients $a(m) \geq 1$.

- The product identity $\zeta(s) = G(s)H(s)$ holds for $\Re s > 1$, and all three functions are holomorphic in this half-plane.

Since all coefficients are nonnegative, there is no issue of conditional convergence on the real axis; in particular, convergence and absolute convergence coincide for real $s > 1$.

7 An arithmetical description of the dynamical factor

In this section we make the LI/LD–decomposition of $\zeta(s)$ from Sections 5–6 more explicit on the level of integers and Dirichlet coefficients, and we express the dynamical factor $G^\flat(s)$ (Definition 5.4) in purely arithmetical terms.

7.1 LI- and LD-components of an integer

Let $\mathbb{P}$ be the set of all primes, and recall the partition

$$\mathbb{P} \;=\; P_{\mathrm{LI}} \sqcup P_{\mathrm{LD}}$$

into linearly independent and linearly dependent primes (Definition 2.1).

For each integer $n \geq 1$ with prime factorization

$$n \;=\; \prod_{p \in \mathbb{P}} p^{v_p(n)}$$

we define its *LI-* and *LD-component* by

$$\ell_{\mathrm{LI}}(n) \;:=\; \prod_{q \in P_{\mathrm{LI}}} q^{v_q(n)}, \qquad \ell_{\mathrm{LD}}(n) \;:=\; \prod_{p \in P_{\mathrm{LD}}} p^{v_p(n)}.$$

Equivalently,

- $\ell_{\mathrm{LI}}(n)$ is the largest LI-number dividing n;
- $\ell_{\mathrm{LD}}(n)$ is the largest LD-number dividing n.

Lemma 7.1 (Elementary properties of ℓ_{LI} and ℓ_{LD})**.** *For all $n \geq 1$ we have*

$$n \;=\; \ell_{\mathrm{LI}}(n)\,\ell_{\mathrm{LD}}(n), \qquad \gcd\big(\ell_{\mathrm{LI}}(n), \ell_{\mathrm{LD}}(n)\big) = 1,$$

and both ℓ_{LI} and ℓ_{LD} are multiplicative. More precisely:

1. *For a prime r,*

$$\ell_{\mathrm{LI}}(r) = \begin{cases} r, & r \in P_{\mathrm{LI}}, \\ 1, & r \in P_{\mathrm{LD}}, \end{cases} \qquad \ell_{\mathrm{LD}}(r) = \begin{cases} 1, & r \in P_{\mathrm{LI}}, \\ r, & r \in P_{\mathrm{LD}}. \end{cases}$$

The analogous statements hold for prime powers r^k.

2. *If* $\gcd(m,n)=1$, *then*

$$\ell_{\mathrm{LI}}(mn)=\ell_{\mathrm{LI}}(m)\,\ell_{\mathrm{LI}}(n), \qquad \ell_{\mathrm{LD}}(mn)=\ell_{\mathrm{LD}}(m)\,\ell_{\mathrm{LD}}(n).$$

3. *An integer* n *is an LI-number (Definition 5.1) if and only if*

$$\ell_{\mathrm{LI}}(n)=n \quad \textit{(and hence } \ell_{\mathrm{LD}}(n)=1\textit{)},$$

and n *is an LD-number if and only if*

$$\ell_{\mathrm{LD}}(n)=n \quad \textit{(and } \ell_{\mathrm{LI}}(n)=1\textit{)}.$$

Proof. All statements are immediate from the prime factorization of n and the disjoint union $\mathbb{P}=P_{\mathrm{LI}}\sqcup P_{\mathrm{LD}}$. Each prime power $p^{v_p(n)}$ is assigned to exactly one of the two factors, which yields the factorization of n and the coprimality. The formulas for primes and prime powers follow by inspection, and multiplicativity holds because the constructions of ℓ_{LI} and ℓ_{LD} are defined on the level of prime powers and respect disjoint supports of $\gcd(m,n)=1$. Finally, the characterizations of LI/LD-numbers are tautological from Definition 5.1. □

Thus ℓ_{LI} and ℓ_{LD} give a canonical "projection" of any integer onto its LI- and LD-part, in line with the prime level partition used throughout the paper.

7.2 Rewriting $G(s)$ and $H(s)$ via LI/LD-components

The Dirichlet series $G(s)$ and $H(s)$ from Definition 5.2 can now be written in a compact arithmetic form using ℓ_{LI} and ℓ_{LD}.

Let $\mathbf{1}_{\mathcal{E}}(n)$ denote the indicator of a property $\mathcal{E}$ of n. Since an integer n is LI if and only if $\ell_{\mathrm{LD}}(n)=1$, and LD if and only if $\ell_{\mathrm{LI}}(n)=1$, we have, for $\Re s>1$,

$$G(s)=\sum_{\substack{u\geq 1\\ u\ \mathrm{LI}}}\frac{1}{u^s}=\sum_{n\geq 1}\frac{\mathbf{1}_{\{\ell_{\mathrm{LD}}(n)=1\}}}{n^s},$$

$$H(s)=\sum_{\substack{v\geq 1\\ v\ \mathrm{LD}}}\frac{1}{v^s}=\sum_{n\geq 1}\frac{\mathbf{1}_{\{\ell_{\mathrm{LI}}(n)=1\}}}{n^s}.$$

In particular, the Euler product identity $\zeta(s)=G(s)H(s)$ (Proposition 5.3) can be viewed as encoding the unique factorization

$$n=\ell_{\mathrm{LI}}(n)\,\ell_{\mathrm{LD}}(n)$$

at the level of Dirichlet coefficients: each n contributes exactly once to the double sum

$$\Big(\sum_{u\ \mathrm{LI}}\frac{1}{u^s}\Big)\Big(\sum_{v\ \mathrm{LD}}\frac{1}{v^s}\Big)=\sum_{n\geq 1}\frac{1}{n^s}$$

via the pair

$$(u,v)=\big(\ell_{\mathrm{LI}}(n),\ell_{\mathrm{LD}}(n)\big), \qquad uv=n.$$

7.3 The dynamical factor and an arithmetical $\widehat{\zeta}(s)$

Recall the multiplicative extension $\Phi : \mathbb{N} \to \mathbb{N}$ (Definition 3.2) and the dynamical Dirichlet series

$$G^{\flat}(s) \;=\; \sum_{n\geq 1} \frac{1}{\Phi(n)^s}, \qquad \Re s > 1$$

from Definition 5.4. By Corollary 4.9, $\Phi(n)$ is always an LI-number, and every LI prime occurs as $\Phi(p)$ for at least one prime p. Extending multiplicatively, every LI-number m has at least one "predecessor" n with $\Phi(n) = m$.

For each LI-number u we set

$$a(u) \;:=\; \#\{n \geq 1 : \Phi(n) = u\},$$

and $a(u) = 0$ for non-LI u. Then, as observed in Section 5.2,

$$G^{\flat}(s) \;=\; \sum_{\substack{u\geq 1 \\ u \text{ LI}}} \frac{a(u)}{u^s}, \qquad a(u) \geq 1 \text{ for LI } u.$$

In this language it is natural to introduce the "dynamically weighted" zeta function

$$\widehat{\zeta}(s) \;:=\; G^{\flat}(s)\, H(s), \qquad \Re s > 1.$$

Proposition 7.2 (Dirichlet coefficients of $\widehat{\zeta}$)**.** *For $\Re s > 1$ we have an absolutely convergent Dirichlet series*

$$\widehat{\zeta}(s) = \sum_{n\geq 1} \frac{c(n)}{n^s},$$

where the coefficient $c(n)$ is given arithmetically by

$$c(n) \;=\; a\big(\ell_{\mathrm{LI}}(n)\big).$$

Proof. We first expand the product

$$\widehat{\zeta}(s) = \left(\sum_{u \text{ LI}} \frac{a(u)}{u^s}\right)\left(\sum_{v \text{ LD}} \frac{1}{v^s}\right) = \sum_{n\geq 1} \frac{c(n)}{n^s},$$

with

$$c(n) \;=\; \sum_{\substack{uv=n \\ u \text{ LI},\, v \text{ LD}}} a(u).$$

By the uniqueness of the factorization $n = \ell_{\mathrm{LI}}(n)\, \ell_{\mathrm{LD}}(n)$, there is exactly one pair (u, v) with u LI, v LD and $uv = n$, namely

$$u = \ell_{\mathrm{LI}}(n), \qquad v = \ell_{\mathrm{LD}}(n).$$

Thus the sum defining $c(n)$ reduces to a single term, and we obtain

$$c(n) = a\big(\ell_{\mathrm{LI}}(n)\big).$$

□

Since $\ell_{\mathrm{LI}}(n)$ is always an LI-number and $a(u) \geq 1$ for every LI-number u, we immediately get:

Corollary 7.3 (Comparison with $\zeta(s)$)**.** *For all $n \geq 1$ we have*

$$c(n) = a\big(\ell_{\mathrm{LI}}(n)\big) \;\geq\; 1,$$

and hence, for real $s > 1$,

$$\widehat{\zeta}(s) = \sum_{n\geq 1} \frac{c(n)}{n^s} \;\geq\; \sum_{n\geq 1} \frac{1}{n^s} = \zeta(s).$$

Moreover,

$$\widehat{\zeta}(s) - \zeta(s) = \sum_{n\geq 1} \frac{a(\ell_{\mathrm{LI}}(n)) - 1}{n^s}, \qquad a(\ell_{\mathrm{LI}}(n)) - 1 \;\geq\; 0.$$

In summary, the maps ℓ_{LI} and ℓ_{LD} simultaneously:

- encode the canonical LI/LD-factorization $n = \ell_{\mathrm{LI}}(n)\,\ell_{\mathrm{LD}}(n)$,
- index the coefficients of the dynamical factor $G^{\flat}(s)$,
- and organize the coefficient-wise comparison between $\widehat{\zeta}(s)$ and $\zeta(s)$ through the multiplicities $a(\ell_{\mathrm{LI}}(n))$.

8 Elementary properties of the LI/LD–decomposition and an injectivity criterion for Φ

In this section we collect some basic but useful properties of the maps $\ell_{\mathrm{LI}}, \ell_{\mathrm{LD}}$, their divisor sums $L_{\mathrm{LD}}, L_{\mathrm{LI}}$, and the dynamical map Φ. Throughout we assume:

- $\mathbb{P}$ denotes the set of all primes, decomposed as a disjoint union

  $$\mathbb{P} \;=\; \mathbb{P}_{\mathrm{LI}} \sqcup \mathbb{P}_{\mathrm{LD}},$$

  where $\mathbb{P}_{\mathrm{LI}}$ are the LI-primes and $\mathbb{P}_{\mathrm{LD}}$ the LD-primes.
- For each integer $n \geq 1$ with prime factorization

  $$n \;=\; \prod_{p\in\mathbb{P}} p^{v_p(n)}$$

  we define its LI- and LD-components by

  $$\ell_{\mathrm{LI}}(n) \;:=\; \prod_{q\in\mathbb{P}_{\mathrm{LI}}} q^{v_q(n)}, \qquad \ell_{\mathrm{LD}}(n) \;:=\; \prod_{p\in\mathbb{P}_{\mathrm{LD}}} p^{v_p(n)}.$$

  In particular,

  $$n \;=\; \ell_{\mathrm{LI}}(n)\,\ell_{\mathrm{LD}}(n), \qquad \gcd\big(\ell_{\mathrm{LI}}(n), \ell_{\mathrm{LD}}(n)\big) = 1.$$

- $\Phi : \mathbb{N} \to \mathbb{N}$ is completely multiplicative, its image consists only of LI-numbers, and Φ is surjective onto the set of LI-numbers (every LI-number occurs as $\Phi(m)$ for at least one m). Moreover, for $m > 1$ we have $\Phi(m) > m$; this is satisfied by the concrete construction of Φ from the LI/LD-lattice.

We write $\tau(n)$ for the number of positive divisors of n, $\sigma(n)$ for the sum of positive divisors, and $\mu(n)$ for the Möbius function.

8.1 The basic identities (1)–(5)

We begin by recording the elementary identities that express the projector-like nature of ℓ_{LI} and ℓ_{LD} and their interaction with Φ.

Lemma 8.1 (1) $\ell_{\mathrm{LI}}(\Phi(n)) = \Phi(n)$**).** *For all $n \geq 1$ we have*

$$\ell_{\mathrm{LI}}(\Phi(n)) = \Phi(n), \qquad \ell_{\mathrm{LD}}(\Phi(n)) = 1.$$

Proof. By construction and Theorem 4.9 (in the earlier part of the paper) the values of Φ are precisely the LI-numbers. Thus every prime divisor of $\Phi(n)$ lies in $\mathbb{P}_{\mathrm{LI}}$. Hence the LI-component is all of $\Phi(n)$, and there are no LD-prime factors, so the LD-component is 1. □

Lemma 8.2 (2) and 3) idempotence)**.** *For all $n \geq 1$ we have*

$$\ell_{\mathrm{LI}}(\ell_{\mathrm{LI}}(n)) = \ell_{\mathrm{LI}}(n), \qquad \ell_{\mathrm{LD}}(\ell_{\mathrm{LD}}(n)) = \ell_{\mathrm{LD}}(n).$$

Proof. The number $\ell_{\mathrm{LI}}(n)$ has by definition only LI-prime factors, and therefore is itself an LI-number. Applying ℓ_{LI} again leaves it unchanged: $\ell_{\mathrm{LI}}(\ell_{\mathrm{LI}}(n)) = \ell_{\mathrm{LI}}(n)$. Similarly, $\ell_{\mathrm{LD}}(n)$ has only LD-prime factors, hence is an LD-number and is fixed by ℓ_{LD}. □

Lemma 8.3 (4) Preimages of $\ell_{\mathrm{LI}}(n)$ under Φ)**.** *For every $n \geq 1$ there exists $m \in \mathbb{N}$ such that*

$$\ell_{\mathrm{LI}}(n) = \Phi(m) \quad \textit{and} \quad n \geq m.$$

If $n > 1$, then in fact $n > m$.

Proof. By definition $\ell_{\mathrm{LI}}(n)$ is an LI-number. Since Φ is surjective onto the LI-numbers, there exists at least one $m \in \mathbb{N}$ such that

$$\Phi(m) = \ell_{\mathrm{LI}}(n).$$

If $m > 1$, then by the growth property of Φ we have $\Phi(m) > m$, hence

$$m < \Phi(m) = \ell_{\mathrm{LI}}(n) \leq n,$$

because $\ell_{\mathrm{LI}}(n)$ always divides n. This yields $m < n$ whenever $n > 1$. For $n = 1$ we have $\ell_{\mathrm{LI}}(1) = 1$, and choosing $\Phi(1) = 1$ (as is natural for a completely multiplicative map) we can take $m = 1$. Thus the statement holds for all $n \geq 1$. □

Lemma 8.4 (5) Factorization through Φ). *For every $n \geq 1$ there exists $m \in \mathbb{N}$ such that*

$$n = \ell_{\mathrm{LD}}(n)\,\Phi(m) \quad \textit{and} \quad n \geq m,$$

and if $n > 1$ then $n > m$.

Proof. By the definition of ℓ_{LI} and ℓ_{LD} we always have

$$n = \ell_{\mathrm{LI}}(n)\,\ell_{\mathrm{LD}}(n).$$

By the previous lemma there exists an m with $\ell_{\mathrm{LI}}(n) = \Phi(m)$ and $m \leq n$. Substituting gives

$$n = \ell_{\mathrm{LD}}(n)\,\Phi(m),$$

and the inequality properties for m are inherited from Lemma 4. □

8.2 Divisor sums and Möbius inversion (6) and (7)

We now define global divisor sums built from the local components ℓ_{LI} and ℓ_{LD}, and show how to recover the latter from the former.

Definition 8.5. For every $n \geq 1$ we define

$$L_{\mathrm{LD}}(n) := \sum_{d \mid n} \ell_{\mathrm{LD}}(d), \qquad L_{\mathrm{LI}}(n) := \sum_{d \mid n} \ell_{\mathrm{LI}}(d).$$

Proposition 8.6 (Exact factorization of L_{LD} and L_{LI}). *For every $n \geq 1$ we have*

$$L_{\mathrm{LD}}(n) = \tau\big(\ell_{\mathrm{LI}}(n)\big)\,\sigma\big(\ell_{\mathrm{LD}}(n)\big), \qquad L_{\mathrm{LI}}(n) = \tau\big(\ell_{\mathrm{LD}}(n)\big)\,\sigma\big(\ell_{\mathrm{LI}}(n)\big).$$

In particular,

$$L_{\mathrm{LD}}(n) \leq \sigma(n), \qquad L_{\mathrm{LI}}(n) \leq \sigma(n) \quad \textit{for all } n \geq 1.$$

Proof. Write

$$n = \ell_{\mathrm{LI}}(n)\,\ell_{\mathrm{LD}}(n) =: u\,v$$

with $\gcd(u, v) = 1$. Every divisor $d \mid n$ then has a unique factorization

$$d = d_{\mathrm{LI}}\,d_{\mathrm{LD}}, \qquad d_{\mathrm{LI}} \mid u,\ d_{\mathrm{LD}} \mid v.$$

This establishes a bijection

$$\{d \mid n\} \longleftrightarrow \big\{(d_{\mathrm{LI}}, d_{\mathrm{LD}}) : d_{\mathrm{LI}} \mid u,\ d_{\mathrm{LD}} \mid v\big\}, \quad d \mapsto (d_{\mathrm{LI}}, d_{\mathrm{LD}}).$$

For such a divisor we have:

- d_{LI} contains only LI-primes and d_{LD} only LD-primes,

- hence $\ell_{\mathrm{LD}}(d) = \ell_{\mathrm{LD}}(d_{\mathrm{LI}} d_{\mathrm{LD}}) = d_{\mathrm{LD}}$, $\ell_{\mathrm{LI}}(d) = \ell_{\mathrm{LI}}(d_{\mathrm{LI}} d_{\mathrm{LD}}) = d_{\mathrm{LI}}$.

We can therefore compute:

$$L_{\mathrm{LD}}(n) = \sum_{d \mid n} \ell_{\mathrm{LD}}(d) = \sum_{\substack{d_{\mathrm{LI}} \mid u \\ d_{\mathrm{LD}} \mid v}} \ell_{\mathrm{LD}}(d_{\mathrm{LI}} d_{\mathrm{LD}}) = \sum_{\substack{d_{\mathrm{LI}} \mid u \\ d_{\mathrm{LD}} \mid v}} d_{\mathrm{LD}}.$$

The inner sum does not depend on d_{LI}, hence

$$L_{\mathrm{LD}}(n) = \sum_{d_{\mathrm{LI}} \mid u} \sum_{d_{\mathrm{LD}} \mid v} d_{\mathrm{LD}} = \big(\#\{d_{\mathrm{LI}} \mid u\}\big) \Big(\sum_{d_{\mathrm{LD}} \mid v} d_{\mathrm{LD}} \Big) = \tau(u)\, \sigma(v)$$

and thus

$$L_{\mathrm{LD}}(n) = \tau\big(\ell_{\mathrm{LI}}(n)\big)\, \sigma\big(\ell_{\mathrm{LD}}(n)\big).$$

The computation for $L_{\mathrm{LI}}(n)$ is completely analogous:

$$L_{\mathrm{LI}}(n) = \sum_{d \mid n} \ell_{\mathrm{LI}}(d) = \sum_{\substack{d_{\mathrm{LI}} \mid u \\ d_{\mathrm{LD}} \mid v}} \ell_{\mathrm{LI}}(d_{\mathrm{LI}} d_{\mathrm{LD}}) = \sum_{\substack{d_{\mathrm{LI}} \mid u \\ d_{\mathrm{LD}} \mid v}} d_{\mathrm{LI}} = \sum_{d_{\mathrm{LD}} \mid v} \sum_{d_{\mathrm{LI}} \mid u} d_{\mathrm{LI}} = \tau(v)\, \sigma(u),$$

so

$$L_{\mathrm{LI}}(n) = \tau\big(\ell_{\mathrm{LD}}(n)\big)\, \sigma\big(\ell_{\mathrm{LI}}(n)\big).$$

For the inequalities we simply use that for each divisor $d \mid n$, $\ell_{\mathrm{LD}}(d) \mid d$ and $\ell_{\mathrm{LI}}(d) \mid d$, hence

$$\ell_{\mathrm{LD}}(d) \le d, \qquad \ell_{\mathrm{LI}}(d) \le d.$$

Summing over all divisors of n gives

$$L_{\mathrm{LD}}(n) = \sum_{d \mid n} \ell_{\mathrm{LD}}(d) \le \sum_{d \mid n} d = \sigma(n),$$

and likewise

$$L_{\mathrm{LI}}(n) \le \sigma(n).$$

□

Proposition 8.7 (7) Möbius inversion). *For all $n \ge 1$ we have*

$$L_{\mathrm{LD}}(n) = \sum_{d \mid n} \ell_{\mathrm{LD}}(d), \qquad L_{\mathrm{LI}}(n) = \sum_{d \mid n} \ell_{\mathrm{LI}}(d),$$

and conversely

$$\ell_{\mathrm{LD}}(n) = \sum_{d \mid n} \mu\Big(\frac{n}{d}\Big)\, L_{\mathrm{LD}}(d), \qquad \ell_{\mathrm{LI}}(n) = \sum_{d \mid n} \mu\Big(\frac{n}{d}\Big)\, L_{\mathrm{LI}}(d).$$

Proof. The identities

$$L_{\mathrm{LD}}(n) = \sum_{d|n} \ell_{\mathrm{LD}}(d), \qquad L_{\mathrm{LI}}(n) = \sum_{d|n} \ell_{\mathrm{LI}}(d)$$

are the definitions of L_{LD} and L_{LI}. In the language of Dirichlet convolution we can write these as

$$L_{\mathrm{LD}} = 1 * \ell_{\mathrm{LD}}, \qquad L_{\mathrm{LI}} = 1 * \ell_{\mathrm{LI}},$$

where $1(n) \equiv 1$ is the constant-one function and $*$ denotes Dirichlet convolution.

Since $\mu * 1 = \varepsilon$, the identity at 1 and zero elsewhere, we have

$$\ell_{\mathrm{LD}} = \mu * L_{\mathrm{LD}}, \qquad \ell_{\mathrm{LI}} = \mu * L_{\mathrm{LI}}.$$

In explicit divisor-sum form this reads

$$\ell_{\mathrm{LD}}(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, L_{\mathrm{LD}}(d), \qquad \ell_{\mathrm{LI}}(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, L_{\mathrm{LI}}(d),$$

as claimed. □

Thus ℓ_{LI} and ℓ_{LD} are completely determined by the global divisor sums L_{LI} and L_{LD}.

8.3 An injectivity criterion for Φ via L_{LD}

We now show that the injectivity of Φ can be characterized purely in terms of the function L_{LD} evaluated at the values $\Phi(n)$.

Recall from the first lemma that $\Phi(n)$ is always an LI-number, so

$$\ell_{\mathrm{LI}}(\Phi(n)) = \Phi(n), \qquad \ell_{\mathrm{LD}}(\Phi(n)) = 1.$$

Lemma 8.8. *For all $n \geq 1$ we have*

$$L_{\mathrm{LD}}(\Phi(n)) = \tau(\Phi(n)).$$

Proof. Insert $k = \Phi(n)$ into the product formula for L_{LD}:

$$L_{\mathrm{LD}}(k) = \tau\big(\ell_{\mathrm{LI}}(k)\big)\, \sigma\big(\ell_{\mathrm{LD}}(k)\big).$$

Since $k = \Phi(n)$ is LI, we have $\ell_{\mathrm{LI}}(k) = k$ and $\ell_{\mathrm{LD}}(k) = 1$. Thus

$$L_{\mathrm{LD}}(\Phi(n)) = \tau\big(\Phi(n)\big)\, \sigma(1) = \tau\big(\Phi(n)\big) \cdot 1 = \tau\big(\Phi(n)\big),$$

as claimed. □

In particular, any identity of the form $L_{\mathrm{LD}}(\Phi(n)) = \tau(\text{something})$ is equivalent to a statement about the divisor function $\tau(\Phi(n))$.

We now show that the injectivity of Φ is encoded by the requirement that the number of divisors is preserved.

Theorem 8.9 (Injectivity of Φ via L_{LD})**.** *The following statements are equivalent:*

1. $\Phi : \mathbb{N} \to \mathbb{N}$ *is injective.*
2. *For all* $n \geq 1$ *we have*

$$L_{\mathrm{LD}}(\Phi(n)) = \tau(n),$$

i.e.

$$\tau\big(\Phi(n)\big) = \tau(n).$$

Proof. (1) $\Rightarrow$ (2). Write n as a product of prime powers

$$n = \prod_{j=1}^{r} p_j^{e_j},$$

with distinct primes $p_1, \ldots, p_r$ and exponents $e_j \geq 1$. Because Φ is completely multiplicative and maps primes to LI-primes, we obtain

$$\Phi(n) = \prod_{j=1}^{r} \Phi(p_j)^{e_j}.$$

If Φ is injective, then the values $\Phi(p_j)$ are distinct primes, so the prime factorization of $\Phi(n)$ has exactly the same exponents $e_1, \ldots, e_r$ as that of n. The divisor function is given by

$$\tau(n) = \prod_{j=1}^{r} (e_j + 1), \qquad \tau(\Phi(n)) = \prod_{j=1}^{r} (e_j + 1),$$

hence $\tau(\Phi(n)) = \tau(n)$ for all $n \geq 1$. Using the lemma above this is equivalent to

$$L_{\mathrm{LD}}(\Phi(n)) = \tau(\Phi(n)) = \tau(n),$$

for all n.

(2) $\Rightarrow$ (1). Suppose (2) holds, but Φ is not injective. Then there exist distinct primes $p_1 \neq p_2$ such that $\Phi(p_1) = \Phi(p_2) =: q$. Consider

$$n := p_1 p_2.$$

Then $\tau(n) = 4$, while

$$\Phi(n) = \Phi(p_1)\Phi(p_2) = q \cdot q = q^2,$$

so

$$\tau(\Phi(n)) = \tau(q^2) = 3.$$

Hence

$$\tau(\Phi(n)) < \tau(n) \quad \Longrightarrow \quad L_{\mathrm{LD}}(\Phi(n)) = \tau(\Phi(n)) < \tau(n),$$

contradicting the assumed identity $L_{\mathrm{LD}}(\Phi(n)) = \tau(n)$ for all n. Therefore Φ must be injective.

This shows that Φ is injective if and only if $L_{\mathrm{LD}}(\Phi(n)) = \tau(n)$ holds for all $n \geq 1$. □

The argument above also shows that, in general, we always have

$$L_{\mathrm{LD}}(\Phi(n)) = \tau(\Phi(n)) \leq \tau(n)$$

for all $n \geq 1$, with strict inequality for some n if and only if Φ is not injective. Thus the family of values $\{L_{\mathrm{LD}}(\Phi(n))\}_{n\geq 1}$, which is defined purely in terms of the LI/LD-decomposition and divisor sums, encodes the injectivity of the dynamical map Φ.

9 Logarithmic representations for LD primes via the Φ-lattice

In this section we record an explicit representation of $p-1$ for linearly dependent primes p in terms of the values $r-1$ for linearly independent primes $r < p$. The key input is the unimodularity of the "Φ-lattice" constructed in [13], to which we refer for full details.

9.1 Exponent vectors and the Φ-lattice

Let $(p_k)_{k\geq 1}$ be the increasing sequence of all primes, $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$. For each integer $n \geq 2$ we consider its (infinite) exponent vector

$$\varphi(n) := \big(v_{p_1}(n-1), v_{p_2}(n-1), v_{p_3}(n-1), \ldots\big) \in \prod_{k\geq 1} \mathbb{Z},$$

where $v_{p_k}(\,\cdot\,)$ denotes the p_k-adic valuation. Only finitely many coordinates of $\varphi(n)$ are nonzero.

For a fixed cutoff $N \geq 2$ it is convenient to truncate to the first $\pi(N)$ primes:

$$\varphi_N(n) := \big(v_{p_1}(n-1), \ldots, v_{p_{\pi(N)}}(n-1)\big) \in \mathbb{Z}^{\pi(N)}.$$

For primes $q \leq N$ we view $\varphi_N(q)$ as vectors in $\mathbb{Q}^{\pi(N)}$.

Definition 9.1 (The Φ-lattice)**.** For each $N \geq 2$ we define the Φ-*lattice* by

$$\Lambda_N := \mathrm{Span}_{\mathbb{Z}}\big\{\varphi_N(q) : q \leq N,\ q \text{ prime}\big\} \subset \mathbb{Z}^{\pi(N)}.$$

We recall from [13] that Λ_N is an odd unimodular lattice, and that the truncated exponent vectors of the LI-primes $\leq N$ form a $\mathbb{Z}$–basis.

Proposition 9.2 (LI-primes form a unimodular basis)**.** *Let L_N be the set of LI-primes $\leq N$. Then*

1. *the family $\{\varphi_N(q) : q \in L_N\}$ is a $\mathbb{Z}$-basis of Λ_N;*
2. *the Gram matrix of this basis has determinant ± 1, i.e. Λ_N is unimodular.*

We shall use only the consequences that every vector in Λ_N admits a unique integral expansion in the basis $\{\varphi_N(q)\}_{q \in L_N}$, and that all coefficients are integers.

9.2 Logarithmic representation for LD primes

We now state and prove the logarithmic representation for LD primes.

Lemma 9.3 (Logarithmic representation for LD primes)**.** *Let p be a linearly dependent prime. Then there exist uniquely determined integers $c_r(p) \in \mathbb{Z}$, indexed by LI-primes $r < p$ and all but finitely many equal to 0, such that*

$$\log(p-1) = \sum_{\substack{r<p \\ r \text{ LI}}} c_r(p)\, \log(r-1). \tag{1}$$

Equivalently, we have the multiplicative representation

$$p - 1 = \prod_{\substack{r<p \\ r \text{ LI}}} (r-1)^{c_r(p)}. \tag{2}$$

Proof. Fix an LD prime p and choose $N := p$. Then $\varphi_N(p)$ belongs to Λ_N by definition. Let L_N denote the LI-primes $\leq N$.

Step 1: integral expansion in the LI-basis. By Proposition 9.2, the vectors $\{\varphi_N(r) : r \in L_N\}$ form a $\mathbb{Z}$-basis of Λ_N. Hence there exist unique integers $b_r(p) \in \mathbb{Z}$ (only finitely many non-zero) such that

$$\varphi_N(p) = \sum_{r \in L_N} b_r(p)\, \varphi_N(r). \tag{3}$$

Since p is LD, its valuation vector lies in the *span* of the earlier vectors but does not itself contribute a new basis element. In particular, the coefficient corresponding to $r = p$ in (3) vanishes, so we may rewrite this as

$$\varphi_N(p) = \sum_{\substack{r<p \\ r \text{ LI}}} c_r(p)\, \varphi_N(r), \tag{4}$$

for uniquely determined integers $c_r(p) \in \mathbb{Z}$.

Step 2: equality of p-adic valuations. Unwinding (4) coordinatewise, we obtain for each prime $\ell \leq p$:

$$v_\ell(p-1) = \sum_{\substack{r<p \\ r \text{ LI}}} c_r(p)\, v_\ell(r-1).$$

This holds for every prime $\ell \leq p$; for $\ell > p$ both sides are zero because neither $p-1$ nor any $r-1$ with $r \leq p$ contains primes larger than p in its factorisation. Thus in fact

$$v_\ell(p-1) = \sum_{\substack{r<p \\ r \text{ LI}}} c_r(p)\, v_\ell(r-1) \qquad \text{for all primes } \ell. \tag{5}$$

Step 3: multiplicative identity. The identity (5) shows that for every prime ℓ the ℓ-adic valuation of $p-1$ coincides with that of

$$\prod_{\substack{r<p \\ r \text{ LI}}} (r-1)^{c_r(p)}.$$

Since both $p-1$ and the product are positive integers, equality of all prime valuations forces equality of the integers themselves:

$$p-1 = \prod_{\substack{r<p \\ r \text{ LI}}} (r-1)^{c_r(p)}.$$

This is (2).

Step 4: taking logarithms. Because all factors are positive, we may apply the natural logarithm to (2) and obtain

$$\log(p-1) = \sum_{\substack{r<p \\ r \text{ LI}}} c_r(p)\, \log(r-1),$$

which is (1).

Step 5: uniqueness and non-triviality. Uniqueness of the integers $c_r(p)$ follows from the uniqueness of the integral expansion (4) in the unimodular basis $\{\varphi_N(r) : r \in L_N\}$. Indeed, if we had another family $d_r(p) \in \mathbb{Z}$ with

$$\sum_{\substack{r<p \\ r \text{ LI}}} c_r(p)\, \varphi_N(r) = \sum_{\substack{r<p \\ r \text{ LI}}} d_r(p)\, \varphi_N(r),$$

then subtracting gives a non-trivial integral relation among the basis vectors, contradicting their linear independence over $\mathbb{Z}$.

The representation is non-trivial: if $c_r(p) = 0$ for all $r < p$, then $\varphi_N(p) = 0$, i.e. $v_\ell(p-1) = 0$ for all primes ℓ, which is impossible because $p - 1 \geq 1$. Equivalently, if all $c_r(p)$ were zero, $\varphi(p)$ would not lie in the span of earlier vectors, contradicting the assumption that p is LD. $\square$

In summary, the unimodularity of the Φ-lattice and the choice of LI-primes as a $\mathbb{Z}$-basis yield an explicit and unique multiplicative and logarithmic representation of $p-1$ for every LD prime p in terms of $(r-1)$ for LI primes $r < p$.

10 The ψ–operator and infinite descent

We now introduce an auxiliary map ψ on the primes and analyse its iteration. The construction combines the successor map Φ from Section 3 and the LI/LD-decomposition from Section 2. Throughout, we continue to write $\mathbb{P}_{\mathrm{LI}}$ and $\mathbb{P}_{\mathrm{LD}}$ for the sets of LI and LD primes, respectively

Recall that $\Phi(p)$ is defined as the smallest prime q with $q \equiv 1 \pmod{p}$; it is always LI, and every LI prime occurs as $\Phi(r)$ for at least one smaller prime r, while no LD prime does (Proposition 4.8 and Corollary 4.9).

10.1 Definition of ψ and its iterates

Definition 10.1 (The ψ-operator on primes)**.** For a prime p we define

$$\psi(p) := \begin{cases} p, & \text{if } p \text{ is linearly dependent,} \\ \min\{\, r \in \mathbb{P} : \Phi(r) = p \,\}, & \text{if } p \text{ is linearly independent.} \end{cases}$$

By Corollary 4.9 every LI prime p has at least one predecessor under Φ, and by the defining property of Φ we have $\Phi(r) > r$ for every prime r, so $r < p$ whenever $\Phi(r) = p$. Hence the set $\{r \in \mathbb{P} : \Phi(r) = p\}$ is nonempty and finite, and $\psi(p)$ is well-defined.

Definition 10.2 (Iterates and terminal value of ψ)**.** For $k \geq 0$ we define the iterates of ψ on primes by

$$\psi^{(0)}(p) := p, \qquad \psi^{(k+1)}(p) := \psi\big(\psi^{(k)}(p)\big).$$

Since $(\psi^{(k)}(p))_{k\geq 0}$ will turn out to stabilise for every prime p, we define its terminal value by

$$\psi^{\infty}(p) := \lim_{k\to\infty} \psi^{(k)}(p),$$

i.e. the unique prime q such that $\psi^{(k)}(p) = q$ for all sufficiently large k.

10.2 Stabilisation and LD nature of the terminal value

We first show that the ψ-orbit of each prime stabilises after finitely many steps and its terminal value is always LD.

Lemma 10.3 (Stabilisation and LD fixed points)**.** *For every prime p the sequence $(\psi^{(k)}(p))_{k\geq 0}$ stabilises after finitely many steps, and its terminal value $\psi^{\infty}(p)$ is a linearly dependent prime.*

Proof. Fix a prime p and write

$$p_0 := p, \qquad p_{k+1} := \psi(p_k) \quad (k \geq 0),$$

so that $p_k = \psi^{(k)}(p)$ for all k.

If p_k is LD, then by definition $\psi(p_k) = p_k$, hence $p_{k+1} = p_k$ and the sequence is constant from that point on.

If p_k is LI, then by definition p_{k+1} is the smallest prime r with $\Phi(r) = p_k$. In particular, $r < p_k$, because $\Phi(r) > r$ for all primes r (the successor $\Phi(r)$ is congruent to 1 (mod r) and therefore strictly larger than r). Thus

$$p_{k+1} = \psi(p_k) < p_k \qquad \text{whenever } p_k \text{ is LI.}$$

The sequence (p_k) is therefore non-increasing in the usual order on primes, and strictly decreasing as long as p_k is LI. Since the primes are well-ordered, no infinite strictly decreasing chain exists, so there is some index $K \geq 0$ for which

$$p_{K+1} = p_K.$$

It follows that $p_k = p_K$ for all $k \geq K$, and by definition $\psi^\infty(p) = p_K$.

Finally, by construction the only fixed points of ψ are LD primes: if q is LD, then $\psi(q) = q$; if q is LI, then $\psi(q) < q$ and therefore $\psi(q) \neq q$. Hence $p_K = \psi^\infty(p)$ must be LD. □

Thus every prime p determines canonically a linearly dependent prime $\psi^\infty(p)$, obtained by iterating ψ until the process stabilises.

10.3 Linear relations and an infinite descent via α

We now combine Lemma 9.3 with Lemma 10.3 to obtain a simple "descent" mechanism inside the LI/LD-structure.

Definition 10.4 (The set A_p and the map α)**.** For a prime p let $q := \psi^\infty(p)$ be its terminal value. By Lemma 10.3, q is LD, so Lemma 9.3 gives a unique representation

$$\log(q-1) = \sum_{\substack{r<q \\ r \text{ LI}}} c_r(q)\, \log(r-1), \qquad c_r(q) \in \mathbb{Z}.$$

We define

$$A_p := \big\{\, r < q : r \text{ LI},\ c_r(q) \neq 0 \,\big\},$$

and set

$$\alpha(p) := \begin{cases} 0, & \text{if } A_p = \varnothing, \\ \max A_p, & \text{otherwise.} \end{cases}$$

By construction, whenever $\alpha(p) \neq 0$ it is a prime, it is LI, and it satisfies $\alpha(p) < \psi^\infty(p)$.

Lemma 10.5 (Descent step via α)**.** *Let p be a prime with $\alpha(p) \neq 0$. Then:*

1. *$\alpha(p)$ is LI and*
$$\psi^{\infty}(p) > \alpha(p).$$
2. *The terminal value $\psi^{\infty}(\alpha(p))$ is LD and satisfies*
$$\alpha(p) > \psi^{\infty}(\alpha(p)).$$
3. *Consequently, as long as the map α does not vanish, we obtain a strictly decreasing chain of primes*
$$\psi^{\infty}(p) > \alpha(p) > \psi^{\infty}(\alpha(p)) > \alpha\big(\psi^{\infty}(\alpha(p))\big) > \cdots .$$

Proof. (1) By definition, if $\alpha(p) \neq 0$ then $\alpha(p) \in A_p$, so $\alpha(p)$ is an LI prime with $\alpha(p) < \psi^{\infty}(p)$. This gives the first inequality.

(2) Since $\alpha(p)$ is LI, Lemma 10.3 shows that $\psi^{\infty}(\alpha(p))$ is a LD prime. Moreover, in the ψ-chain starting from $\alpha(p)$ the first step is
$$\psi(\alpha(p)) < \alpha(p),$$
and subsequent steps are non-increasing. Thus
$$\psi^{\infty}(\alpha(p)) \leq \psi(\alpha(p)) < \alpha(p),$$
which is the desired second inequality.

(3) Iterating (1) and (2) yields the strict inequalities in the chain; each arrow is either of the form $\psi^{\infty}(\cdot) > \alpha(\cdot)$ or $\alpha(\cdot) > \psi^{\infty}(\cdot)$, and both are strict whenever the corresponding α is non-zero. □

The lemma provides a simple mechanism for producing strictly decreasing chains of primes purely from the LI/LD-structure and the representation of LD primes in terms of LI primes.

10.4 Recovering a prime by iterating Φ

Finally we show that every prime can be recovered from its terminal value under ψ by iterating the successor map Φ.

Proposition 10.6 (Recovering p from $\psi^{\infty}(p)$)**.** *Let p be a prime. Then there exists an integer $k \geq 0$ such that*
$$\Phi^{(k)}\big(\psi^{\infty}(p)\big) = p,$$
where $\Phi^{(k)}$ denotes the k-fold iterate of Φ.

Proof. If p is LD, then by definition $\psi(p) = p$ and hence $\psi^{\infty}(p) = p$. Taking $k = 0$ gives

$$\Phi^{(0)}\big(\psi^{\infty}(p)\big) = \psi^{\infty}(p) = p.$$

Now suppose that p is LI. Consider again the ψ-sequence

$$p_0 := p, \qquad p_{i+1} := \psi(p_i) \quad (i \geq 0),$$

so that $p_i = \psi^{(i)}(p)$. By Lemma 10.3 there is a minimal index $m \geq 1$ with

$$p_m = \psi^{\infty}(p) \quad \text{and} \quad p_i \text{ LI for } 0 \leq i < m.$$

For each $0 \leq i < m$, the prime p_i is LI, hence lies in the image of Φ by Corollary 4.9. By the definition of ψ in the LI case,

$$p_{i+1} = \psi(p_i) = \min\{\, r \in \mathbb{P} : \Phi(r) = p_i \,\},$$

so in particular

$$\Phi(p_{i+1}) = p_i \qquad (0 \leq i < m).$$

Composing these identities, we obtain

$$\Phi(p_m) = p_{m-1}, \quad \Phi(p_{m-1}) = p_{m-2}, \ \ldots, \ \Phi(p_1) = p_0.$$

Thus

$$\Phi^{(m)}(p_m) = p_0 = p.$$

Since $p_m = \psi^{\infty}(p)$, this shows that

$$\Phi^{(m)}\big(\psi^{\infty}(p)\big) = p$$

with $m \geq 1$. Combining this with the LD case $k = 0$ proves the proposition. □

In particular, $\psi^{\infty}(p)$ may be viewed as a "base point" from which the original prime p is reached by a finite forward orbit of the successor map Φ. This ties together the backward dynamics encoded by ψ and the forward dynamics encoded by Φ in a closed finite-loop structure for every prime.

11 Lower bounds in the factorial decomposition

11.1 The successor map Φ

We work with the following successor map on the primes.

Definition 11.1 (Successor map on the primes)**.** For each prime p we define

$$\Phi(p) := \min\{q \in \mathbb{P} : q \equiv 1 \pmod{p}\},$$

the least prime q with $q \equiv 1 \pmod{p}$. Equivalently, there is a uniquely determined integer $k \geq 1$ such that

$$\Phi(p) = kp + 1, \qquad k \in \mathbb{N}. \tag{6}$$

We extend Φ multiplicatively to all positive integers as follows.

Definition 11.2 (Multiplicative extension of Φ)**.** For $n \in \mathbb{N}$ with prime factorisation

$$n = \prod_p p^{v_p(n)},$$

we define

$$\Phi(n) := \prod_p \Phi(p)^{v_p(n)}.$$

In particular, Φ is (completely) multiplicative: $\Phi(mn) = \Phi(m)\Phi(n)$ for all $m, n \in \mathbb{N}$, and $\Phi(1) = 1$.

By construction each factor $\Phi(p)$ is a prime, so $\Phi(n) \geq 1$ for all $n \in \mathbb{N}$, and $\Phi(n) > 1$ as soon as $n > 1$.

11.2 A basic inequality for Φ and its consequences

We now record the key inequality for Φ on primes that will be used to control $\Phi(n)$ and $\Phi(n!)$.

Lemma 11.3 (Prime inequality for Φ)**.** *For every prime p we have*

$$\Phi(p)\big(\Phi(p) - 1\big) \;\leq\; p\,\Phi\big(\Phi(p) - 1\big). \tag{7}$$

Proof. By definition of Φ there exists a unique integer $k \geq 1$ such that

$$\Phi(p) = kp + 1.$$

In particular,

$$\Phi(p) - 1 = kp,$$

so $\Phi(p) - 1$ is a multiple of p.

Now apply Φ to both sides and use multiplicativity:

$$\Phi\big(\Phi(p) - 1\big) = \Phi(kp) = \Phi(k)\,\Phi(p).$$

By construction, Φ sends every prime r to a prime $\Phi(r) \geq r + 1$, and extending multiplicatively gives $\Phi(n) \geq n$ for all $n \in \mathbb{N}$. In particular,

$$\Phi(k) \;\geq\; k,$$

hence

$$\Phi\big(\Phi(p) - 1\big) = \Phi(k)\,\Phi(p) \;\geq\; k\,\Phi(p).$$

Substitute $k = \dfrac{\Phi(p) - 1}{p}$ into this inequality:

$$\Phi\big(\Phi(p) - 1\big) \;\geq\; \frac{\Phi(p) - 1}{p}\,\Phi(p).$$

Multiplying both sides by p yields

$$p\,\Phi\big(\Phi(p)-1\big) \;\geq\; \Phi(p)\big(\Phi(p)-1\big),$$

which is exactly (7). □

Lemma 11.4. *For every prime q we have*

$$\psi(q) \;\geq\; \frac{q(q-1)}{\Phi(q-1)}.$$

Proof. Recall the prime inequality for Φ:

$$\Phi(p)\big(\Phi(p)-1\big) \;\leq\; p\,\Phi\big(\Phi(p)-1\big)$$

for every prime p.

Case 1: q is linearly independent.

Then q lies in the image of Φ, and by definition of ψ there exists at least one prime r with $\Phi(r)=q$, and among all such primes the smallest one is

$$\psi(q) = \min\{r \in \mathbb{P} : \Phi(r) = q\}.$$

Apply the prime inequality with $p = r$:

$$\Phi(r)\big(\Phi(r)-1\big) \;\leq\; r\,\Phi\big(\Phi(r)-1\big).$$

Since $\Phi(r) = q$ and $\Phi(r)-1 = q-1$, this becomes

$$q(q-1) \;\leq\; r\,\Phi(q-1).$$

Hence

$$r \;\geq\; \frac{q(q-1)}{\Phi(q-1)}.$$

This holds for every prime r with $\Phi(r)=q$, in particular for the minimal such prime $r = \psi(q)$, and therefore

$$\psi(q) \;\geq\; \frac{q(q-1)}{\Phi(q-1)}.$$

Case 2: q is linearly dependent.

By definition we then have $\psi(q) = q$. We need to check that

$$q \;\geq\; \frac{q(q-1)}{\Phi(q-1)}.$$

This is equivalent to

$$\Phi(q-1) \;\geq\; q-1.$$

But Φ is completely multiplicative and on primes satisfies $\Phi(p) \geq p+1$, hence $\Phi(p) \geq p$ for every prime p. For a general integer

$$n = \prod_p p^{v_p(n)}$$

we have

$$\Phi(n) = \prod_p \Phi(p)^{v_p(n)} \;\geq\; \prod_p p^{v_p(n)} = n.$$

Applying this with $n = q-1$ gives $\Phi(q-1) \geq q-1$, so the desired inequality holds.

In both cases we obtain

$$\psi(q) \;\geq\; \frac{q(q-1)}{\Phi(q-1)},$$

which completes the proof. □

Murthy's theorem in base 2 and exponential bounds for Φ

We now introduce Murthy's argument in base 2 and derive the bounds

$$\Phi(p) \leq 2^p \quad \text{for primes } p, \qquad \Phi(n) \leq 2^{\eta(n)} \quad \text{for all } n \geq 1,$$

where

$$\eta(n) := \sum_{p \mid n} v_p(n)\, p.$$

Murthy's theorem in base 2

For $m \geq 1$ let

$$R(m) := 2^m - 1$$

be the repunit in base 2 with m ones in binary. Let P_n denote the n-th prime, and for each n set

$$u(n) := R(P_n) = 2^{P_n} - 1.$$

Theorem 11.5 (Murthy, base 2 version)**.** *Let p be a prime and write $p = P_n$ for some n. If q is any prime divisor of*

$$u(n) = 2^{P_n} - 1,$$

then

$$q \equiv 1 \pmod{p}.$$

Proof. Let $p = P_n$ be prime and let q be a prime divisor of $2^p - 1$, so

$$2^p \equiv 1 \pmod{q}.$$

Let $\mathrm{ord}_q(2)$ denote the multiplicative order of 2 modulo q. Then

$$\mathrm{ord}_q(2) \mid p \quad \text{and} \quad \mathrm{ord}_q(2) \mid q - 1$$

(the first because $2^p \equiv 1 \pmod{q}$, the second by Fermat's little theorem).

Since p is prime, the only positive divisors of p are 1 and p itself. Thus

$$\mathrm{ord}_q(2) \in \{1, p\}.$$

We cannot have $\mathrm{ord}_q(2) = 1$, because this would imply $2 \equiv 1 \pmod{q}$ and hence $q \mid 1$, impossible. Therefore

$$\mathrm{ord}_q(2) = p.$$

But $\mathrm{ord}_q(2)$ divides $q - 1$, so $p \mid q - 1$, i.e.

$$q \equiv 1 \pmod{p}.$$

This is exactly the desired congruence. □

As a direct corollary we obtain a strong upper bound for the successor map on primes.

Corollary 11.6. *For every prime p we have*

$$\Phi(p) \leq 2^p.$$

Proof. Fix a prime p and write $p = P_n$ for some n. By Theorem 11.5 there exists a prime q dividing $2^p - 1$ with

$$q \equiv 1 \pmod{p}.$$

Thus q lies in the arithmetic progression $1 \pmod{p}$, and

$$q \mid 2^p - 1 < 2^p,$$

so $q \leq 2^p - 1 < 2^p$.

By definition, $\Phi(p)$ is the *smallest* prime congruent to 1 modulo p, hence

$$\Phi(p) \leq q \leq 2^p - 1 < 2^p.$$

In particular $\Phi(p) \leq 2^p$, as claimed. □

The bound $\Phi(n) \le 2^{\eta(n)}$

Recall the multiplicative extension of Φ: for

$$n = \prod_p p^{v_p(n)}$$

we set

$$\Phi(n) := \prod_p \Phi(p)^{v_p(n)}.$$

Proposition 11.7. *For every integer $n \ge 1$ we have*

$$\Phi(n) \;\le\; 2^{\eta(n)}, \qquad \eta(n) := \sum_{p \mid n} v_p(n)\, p.$$

Proof. First treat prime powers. Let p be prime and $e \ge 1$. Then, by multiplicativity,

$$\Phi(p^e) = \Phi(p)^e.$$

By Corollary 11.6,

$$\Phi(p) \le 2^p,$$

so

$$\Phi(p^e) = \Phi(p)^e \;\le\; (2^p)^e = 2^{ep}.$$

But $\eta(p^e) = ep$, hence

$$\Phi(p^e) \le 2^{\eta(p^e)}.$$

Now let n be arbitrary with prime factorisation $n = \prod_p p^{e_p}$. Then

$$\Phi(n) = \prod_p \Phi(p)^{e_p} \;\le\; \prod_p (2^p)^{e_p} = 2^{\sum_p e_p p} = 2^{\eta(n)}.$$

This proves the desired inequality for all $n \ge 1$. □

Remark 11.8. In many applications we actually have a strict inequality $<$ in (7), but the non-strict form suffices for our purposes here and leads to slightly cleaner algebraic manipulations.

We now propagate (7) from primes to general integers using the multiplicativity of Φ.

Proposition 11.9 (Extension to prime powers)**.** *Let p be a prime and $e \ge 1$. Then*

$$\Phi(p^e)\,\big(\Phi(p) - 1\big)^e \;\le\; p^e\,\Phi\big(\Phi(p) - 1\big)^e. \tag{8}$$

Proof. Raising (7) to the e-th power yields

$$\big[\Phi(p)\big(\Phi(p)-1\big)\big]^e \;\le\; \big[p\,\Phi\big(\Phi(p)-1\big)\big]^e,$$

that is

$$\Phi(p)^e\,\big(\Phi(p)-1\big)^e \;\le\; p^e\,\Phi\big(\Phi(p)-1\big)^e.$$

Using $\Phi(p^e)=\Phi(p)^e$ by multiplicativity gives (8). □

Proposition 11.10 (Extension to general integers)**.** *Let $n\in\mathbb{N}$ with prime factorisation $n=\prod_p p^{e_p}$. Then*

$$\Phi(n)\cdot\prod_{p\mid n}\big(\Phi(p)-1\big)^{e_p} \;\le\; n\cdot\prod_{p\mid n}\Phi\big(\Phi(p)-1\big)^{e_p}. \tag{9}$$

Equivalently,

$$\frac{\Phi(n)}{n} \;\le\; \prod_{p\mid n}\left(\frac{\Phi\big(\Phi(p)-1\big)}{\Phi(p)-1}\right)^{e_p}, \tag{10}$$

or, in inverted form,

$$\frac{n}{\Phi(n)} \;\ge\; \prod_{p\mid n}\left(\frac{\Phi(p)-1}{\Phi\big(\Phi(p)-1\big)}\right)^{e_p}. \tag{11}$$

Proof. Applying Proposition 11.9 to each prime power p^{e_p} dividing n we obtain

$$\Phi(p^{e_p})\,\big(\Phi(p)-1\big)^{e_p} \;\le\; p^{e_p}\,\Phi\big(\Phi(p)-1\big)^{e_p}$$

for every prime p with $e_p>0$. Multiplying these inequalities over all $p\mid n$ gives

$$\prod_{p\mid n}\Phi(p^{e_p})\prod_{p\mid n}\big(\Phi(p)-1\big)^{e_p} \;\le\; \prod_{p\mid n}p^{e_p}\prod_{p\mid n}\Phi\big(\Phi(p)-1\big)^{e_p}.$$

By multiplicativity, $\prod_{p\mid n}\Phi(p^{e_p})=\Phi(n)$ and $\prod_{p\mid n}p^{e_p}=n$, so we obtain (9). The forms (10) and (11) are obtained by simple rearrangement. □

11.3 Application to the factorial $n!$

We now apply Proposition 11.10 to the special case $n!=\prod_{p\le n}p^{v_p(n!)}$. Writing $e_p=v_p(n!)$ in (9), we obtain

$$\Phi(n!)\cdot\prod_{p\le n}\big(\Phi(p)-1\big)^{v_p(n!)} \;\le\; n!\cdot\prod_{p\le n}\Phi\big(\Phi(p)-1\big)^{v_p(n!)}. \tag{12}$$

Equivalently,

$$\frac{\Phi(n!)}{n!} \;\le\; \prod_{p\le n}\left(\frac{\Phi\big(\Phi(p)-1\big)}{\Phi(p)-1}\right)^{v_p(n!)}, \tag{13}$$

and hence

$$\frac{n!}{\Phi(n!)} \;\geq\; \prod_{p\leq n}\left(\frac{\Phi(p)-1}{\Phi\big(\Phi(p)-1\big)}\right)^{v_p(n!)}. \tag{14}$$

The inequality (14) expresses the "defect" $n!/\Phi(n!)$ as being bounded below by a product over primes $p \leq n$, with local factors determined by the ratio

$$\frac{\Phi(p)-1}{\Phi\big(\Phi(p)-1\big)}$$

and the exponents $v_p(n!)$ in the factorial. Combined with the lower bounds for $E_n(\Phi(p))$ from Proposition **??**, this provides a structural framework for estimating $n!/\Phi(n!)$ in terms of the successor dynamics of the primes.

12 H-numbers, growth bounds and injectivity on primes

In this section we introduce a class of integers defined by a comparison between $\Phi(n)$ and $\Phi(n!)$, and show that for such numbers $\Phi(n)$ is always strictly smaller than n^2. We then use this to establish a restricted injectivity statement for Φ on the set of H-primes.

12.1 Definition of H-numbers

Definition 12.1 (H-numbers)**.** For $n \geq 2$ we call n an *H-number* if

$$\Phi(n) \;\leq\; \log\big(\Phi(n!)\big),$$

where Φ is the successor map from Section 3, extended multiplicatively to all integers.

Thus being an H-number means that the value of Φ at n is at most the logarithm of the (usually much larger) value $\Phi(n!)$.

12.2 A quadratic upper bound for H-numbers

We first show that any H-number n satisfies a simple quadratic upper bound on $\Phi(n)$.

Lemma 12.2. *For every integer $n \geq 2$ we have*

$$\log\big(\Phi(n!)\big) \;<\; n^2.$$

Consequently, if n is an H-number, then

$$\Phi(n) \;<\; n^2.$$

Proof. We begin with the Dirichlet factorization of $n!$:

$$n! = \prod_{p \le n} p^{v_p(n!)}, \qquad \Phi(n!) = \prod_{p \le n} \Phi(p)^{v_p(n!)}.$$

Taking logarithms gives

$$\log \Phi(n!) = \sum_{p \le n} v_p(n!) \, \log \Phi(p).$$

We use two standard estimates:

1. For each prime $p \le n$,

$$v_p(n!) = \sum_{k \ge 1} \left\lfloor \frac{n}{p^k} \right\rfloor \; \le \; \sum_{k \ge 1} \frac{n}{p^k} = \frac{n}{p-1}.$$

2. By Murthy's theorem in base 2 (see Section **??**), we know that for every prime p,

$$\Phi(p) \le 2^p,$$

hence

$$\log \Phi(p) \le p \log 2.$$

Combining these inequalities, we obtain

$$\begin{aligned} \log \Phi(n!) &\le \sum_{p \le n} \frac{n}{p-1} \, \log \Phi(p) \; \le \; \sum_{p \le n} \frac{n}{p-1} \, p \log 2 \\ &= n \log 2 \sum_{p \le n} \frac{p}{p-1}. \end{aligned}$$

We now write

$$\frac{p}{p-1} = 1 + \frac{1}{p-1},$$

and sum over $p \le n$:

$$\sum_{p \le n} \frac{p}{p-1} = \sum_{p \le n} 1 + \sum_{p \le n} \frac{1}{p-1} = \pi(n) + \sum_{p \le n} \frac{1}{p-1},$$

where $\pi(n)$ denotes the prime-counting function.

Elementary estimates on primes (see e.g. standard analytic number theory texts) give that for all sufficiently large n,

$$\pi(n) \le \frac{2n}{\log n}, \qquad \sum_{p \le n} \frac{1}{p-1} \le C + \log \log n$$

for some absolute constant $C > 0$. Hence

$$\log \Phi(n!) \;\le\; n \log 2 \left(\frac{2n}{\log n} + C + \log\log n \right) = \frac{2\log 2}{\log n}\, n^2 + n \log 2\,(C + \log\log n).$$

For large n, the factor $\dfrac{2\log 2}{\log n}$ becomes arbitrarily small, and the linear term $n \log 2\,(C + \log\log n)$ is much smaller than n^2. In particular, there exists an integer n_0 (for example $n_0 = 20$ suffices) such that for all $n \ge n_0$ we have

$$\log \Phi(n!) < n^2.$$

For the finitely many integers $2 \le n < n_0$ the inequality $\log \Phi(n!) < n^2$ can be verified directly by computation. Thus the bound holds for all $n \ge 2$.

Now suppose n is an H-number. By definition,

$$\Phi(n) \le \log \Phi(n!).$$

Combining this with the established bound yields

$$\Phi(n) \le \log \Phi(n!) < n^2,$$

as claimed. □

12.3 Injectivity of Φ on H-primes

We now consider the behaviour of Φ on H-numbers that are prime.

Definition 12.3 (H-primes)**.** A prime p is called an *H-prime* if it is an H-number, i.e.

$$\Phi(p) \le \log \Phi(p!).$$

We show that Φ is injective on the set of H-primes.

Lemma 12.4 (No collisions among H-primes for large p)**.** *There exists a constant p_0 such that the following holds: if $p < q$ are primes with $p \ge p_0$, both H-primes, then*

$$\Phi(p) \ne \Phi(q).$$

Proof. Suppose, for contradiction, that there exist primes $p < q$ with

$$\Phi(p) = \Phi(q) =: M.$$

Since $\Phi(r)$ is the least prime congruent to $1 \bmod r$, we have

$$M \equiv 1 \pmod{p}, \qquad M \equiv 1 \pmod{q}.$$

Therefore pq divides $M - 1$, and hence

$$M \ge pq + 1 \ge p^2 + p + 1 > p^2.$$

On the other hand, p is an H-prime by assumption, so

$$M = \Phi(p) \leq \log \Phi(p!).$$

Using the estimate from the proof of Lemma 12.2, we obtain (for $n = p$)

$$\log \Phi(p!) \leq p \log 2 \left(\frac{2p}{\log p} + C + \log \log p \right).$$

For large p, the term $\dfrac{2 \log 2}{\log p} p^2$ dominates, so that there exists a constant $K > 0$ and a p_1 such that

$$\log \Phi(p!) \leq K \frac{p^2}{\log p}$$

for all $p \geq p_1$. Together with $M \geq pq$, this yields

$$pq < M \leq K \frac{p^2}{\log p} \quad \Rightarrow \quad q < K \frac{p}{\log p}.$$

Now choose $p_0 \geq p_1$ large enough such that

$$K \frac{p}{\log p} < p$$

for all $p \geq p_0$. This is possible since $\log p \to \infty$ and thus $\frac{p}{\log p}/p = 1/\log p \to 0$.

For every $p \geq p_0$, we then obtain from the inequality above

$$q < K \frac{p}{\log p} < p,$$

which contradicts $q > p$. Thus, for $p \geq p_0$, there can be no H-primes $p < q$ with $\Phi(p) = \Phi(q)$. □

For the finitely many H-primes $p < p_0$, the non-existence of such collisions can be verified directly (e.g. computationally). Combined with Lemma 12.4, this yields:

Proposition 12.5 (Injectivity of Φ on H-primes)**.** *If $p < q$ are primes and both are H-primes, then*

$$\Phi(p) \neq \Phi(q).$$

In other words, the map Φ is injective on the set of H-primes.

13 Numerical evidence for H-primes

In this section we present some computational evidence for the existence and distribution of H-primes, i.e. primes p with

$$\Phi(p) \ \leq \ \log\big(\Phi(p!)\big),$$

and we compare this with the theoretical results from the previous section.

13.1 Experimental setup

We implemented the successor map Φ and its multiplicative extension in SageMath as follows:

- For a prime p,

$$\Phi(p) := \min\{\, q \in \mathbb{P} : q \equiv 1 \pmod{p} \,\},$$

  found by scanning the arithmetic progression $q = kp + 1$ and testing each q for primality.

- For $n \geq 1$ with prime factorisation $n = \prod p^{v_p(n)}$,

$$\Phi(n) := \prod_{p} \Phi(p)^{v_p(n)}.$$

- To compute $\log \Phi(n!)$ we use the factorisation of $n!$:

$$n! = \prod_{p \leq n} p^{v_p(n!)}, \qquad \Phi(n!) = \prod_{p \leq n} \Phi(p)^{v_p(n!)},$$

  and thus

$$\log \Phi(n!) = \sum_{p \leq n} v_p(n!)\, \log \Phi(p),$$

  with $v_p(n!)$ computed via Legendre's formula

$$v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

A prime p is then declared an H-prime if the inequality

$$\Phi(p) \leq \log \Phi(p!)$$

holds in high-precision real arithmetic.

13.2 H-primes up to 500

Running this procedure on the interval $[2, 500]$ produces the following data.

- The primes p with $2 \leq p \leq 500$ that satisfy $\Phi(p) \leq \log \Phi(p!)$ are:

$$\begin{gathered} 11,\ 23,\ 29,\ 37,\ 41,\ 43,\ 53,\ 67,\ 73,\ 79,\ 83,\ 89, \\ 97,\ 113,\ 127,\ 131,\ 137,\ 139,\ 151,\ 163,\ 173,\ 179, \\ 181,\ 191,\ 193,\ 199,\ 233,\ 239,\ 241,\ 251,\ 257,\ 263, \\ 271,\ 277,\ 281,\ 283,\ 293,\ 307,\ 311,\ 313,\ 331,\ 347, \\ 359,\ 367,\ 373,\ 397,\ 409,\ 419,\ 431,\ 433,\ 443,\ 461, \\ 467,\ 487,\ 491,\ 499. \end{gathered}$$

- In total there are 56 H-primes in $[2, 500]$. Since $\pi(500) = 95$, this corresponds to a proportion of approximately $56/95 \approx 0.59$ of all primes in this interval.

- For each of these primes p we have numerically:

$$\Phi(p) \leq \log \Phi(p!) \quad \text{and} \quad \Phi(p) < p^2.$$

  For example:

p	$\Phi(p)$	$\log \Phi(p!)$
11	23	≈ 27.87
79	317	≈ 417.17
191	383	≈ 1231.00
499	1997	≈ 3852.40

  In all these cases $\Phi(p) < p^2$ holds, in agreement with Lemma 12.2.

- We also computed $\Phi(p)$ for all H-primes in this range and checked for collisions. There is *no* pair of distinct H-primes $p < q \leq 500$ with $\Phi(p) = \Phi(q)$:

$$\Phi(p) = \Phi(q),\ p < q,\ p, q \leq 500,\ p, q \text{ H-prime} \quad \text{never occurs.}$$

  This is consistent with Proposition 12.5, which shows that Φ is injective on the set of H-primes.

13.3 Discussion

The numerical data up to 500 shows that:

- H-primes are not rare: in the tested range they make up a positive proportion of the primes, and they appear to be reasonably regularly distributed.

- For every H-prime p we observe $\Phi(p) < p^2$, in perfect agreement with the general bound from Lemma 12.2.

- There are no observed collisions $\Phi(p) = \Phi(q)$ among H-primes in $[2, 500]$, again matching the theoretical injectivity result on H-primes.

These computations provide empirical support for the relevance of H-primes in understanding the finer arithmetic of the successor map Φ. In particular, the existence of infinitely many H-primes would immediately imply that Φ is injective on an infinite subset of the primes, thanks to Proposition 12.5. At present, however, the question of whether there are infinitely many H-primes remains open.

14 Heuristic why there should be infinitely many H-primes

In this section we give an informal heuristic why one should expect infinitely many H-primes. The argument is deliberately speculative: it combines the *structural* picture provided by the maps ψ, ψ^∞ and α with a *growth* picture for Φ and a putative density behaviour of LI-primes. None of the global density statements below are proved in this paper.

Recall that H-primes are those primes p for which $\Phi(p)$ grows "slowly" in the sense that

$$\Phi(p) \;\le\; \log \Phi(p!),$$

which, in particular, implies the quadratic bound $\Phi(p) < p^2$ from Lemma 12.2. By contrast, for general primes we only have very crude upper bounds such as Murthy's $\Phi(p) \le 2^p$. The heuristic below starts from the opposite extreme: it imagines a world in which, beyond some point, Φ always grows *fast*.

Step 1: A fast-growth world without H-primes

Assume, for contradiction, that there are only finitely many H-primes. Then there exists N_0 such that every prime $p > N_0$ is not an H-prime. For such primes the defining inequality for H-primes fails, so heuristically $\Phi(p)$ should very often be significantly larger than p.

For the sake of discussion we postulate a strong model assumption:

Hypothesis A (fast growth away from H-primes). There exist N_0 and $\varepsilon > 0$ such that

$$p > N_0,\ p \text{ not H-prime} \quad\Longrightarrow\quad \Phi(p) \;\ge\; p^{1+\varepsilon}$$

(in particular, one may keep in mind the exaggerated model $\Phi(p) \approx p^2$).

Under Hypothesis A, if $y = \Phi(x)$ with x a large non-H-prime, then $y \ge x^{1+\varepsilon}$, so

$$x \;\le\; y^{1/(1+\varepsilon)} \;\ll\; \sqrt{y}.$$

Thus, moving *backwards* along a Φ-orbit (or equivalently, applying the predecessor map ψ to a large LI-prime) shrinks numbers very quickly.

Step 2: Collapse of the predecessor trees

The maps ψ and ψ^∞ organise the prime numbers into rooted trees. For each LD-prime q we define its tree

$$\mathcal{T}(q) \;=\; \{\, p \text{ prime} : \psi^\infty(p) = q \,\},$$

so that every $p \in \mathcal{T}(q)$ is obtained from the root q by finitely many forward applications of Φ, and conversely one reaches the root by iterating ψ until stabilization: $\psi^{(k)}(p) \to \psi^{\infty}(p) = q$.

In the fast-growth world of Hypothesis A, each backward step $y \mapsto x$ with $\Phi(x) = y$ typically satisfies $x \ll y^{1/(1+\varepsilon)}$. This means that, starting from a very large prime p and repeatedly applying ψ, one falls below N_0 in at most $O(\log \log p)$ steps. In other words, all large nodes of the tree $\mathcal{T}(q)$ sit above a very shallow trunk built from primes $\leq N_0$, and the growth along each branch is roughly of the form

$$x,\ x^{1+\varepsilon},\ x^{(1+\varepsilon)^2},\ x^{(1+\varepsilon)^3}, \ldots$$

(up to branching and lower-order effects). Such trees produce a very sparse set of values overall.

Step 3: Surjectivity, LI-primes and a density tension

On the other side the structural part of the theory gives us two facts:

- The map Φ is surjective from the set of all primes onto the set $\mathbb{P}_{LI}$ of LI-primes. Thus every LI-prime occurs somewhere in one of the trees $\mathcal{T}(q)$ as a value of Φ.
- For each N the vectors $\phi_N(p)$ with $p \leq N$ and p LI form a $\mathbb{Z}$-basis of the unimodular lattice Λ_N. In particular, LD-primes $q \leq N$ admit unique integer relations of the form $\log(q-1) = \sum_{r<q,\ r\ LI} c_r(q) \log(r-1)$, and the map α selects the largest LI-prime appearing in such a relation.

It is natural (though unproved) to expect that the LI-primes are not too sparse among all primes; for instance one may posit:

Hypothesis B (mild density of LI-primes). The set $\mathbb{P}_{LI}$ has positive upper density among the primes, or at least grows comparably to the full set of primes in the sense that the n-th LI-prime q_n satisfies a bound of the form $q_n \ll n^C$ for some fixed C.

Combining Hypothesis A with the tree picture from Step 2, one is led to the following tension: starting from a finite set of primes $\leq N_0$ at the bottom and letting Φ grow at least like $p^{1+\varepsilon}$, the union of all values generated in the trees $\mathcal{T}(q)$ should have *asymptotic density zero* among the primes. In contrast, Hypothesis B suggests that $\mathbb{P}_{LI} = \mathrm{im}(\Phi)$ retains positive density or at least grows comparably fast to the full prime sequence. In a random map model, these two behaviours are incompatible.

Step 4: The rôle of α

The map α refines this heuristic by encoding "short dependencies" between an LD-root $q = \psi^{\infty}(p)$ and the LI-primes below it. The relation

$$\log(q-1) \;=\; \sum_{r<q,\ r\ LI} c_r(q)\,\log(r-1)$$

expresses $q-1$ multiplicatively in terms of smaller $r-1$, and $\alpha(q)$ picks the largest such r. Iterating α produces a descending chain of LI-primes. If all these LI-primes were forced, by Hypothesis A, to have very large Φ-values (and thus to be very far apart numerically), one expects a clash with the unimodular lattice structure: expressing the logarithm of a large composite $q-1$ using only very distant generators $\log(r-1)$ with integral coefficients becomes increasingly rigid. Informally, the α-chains insist that each LD-root q must be surrounded by "nearby" LI-primes, while the fast-growth model of Φ tends to push LI-preimages far away.

Step 5: Heuristic conclusion

Summarising, the heuristic can be phrased as follows: if there were only finitely many H-primes, then beyond some height Φ would grow so rapidly (Hypothesis A) that its image along Φ-orbits in the trees $\mathcal{T}(q)$ would form a set of primes of very small asymptotic density. This picture is hard to reconcile with the expectation that LI-primes occur with reasonable frequency (Hypothesis B) and with the combination of surjectivity of Φ onto $\mathbb{P}_{LI}$ and the unimodular lattice structure governed by ψ^{∞} and α. In order to avoid this "collapse of the predecessor trees", one is led to believe that there must be infinitely many primes at which Φ grows *slowly*, i.e. infinitely many H-primes.

Turning this heuristic into a theorem would require quantitative control on the distribution of LI-primes and on the typical size of $\Phi(p)$ outside the H-primes; the framework developed here suggests a concrete programme for such investigations.

15 The H-dominant regime of the dynamical zeta function

In this final synthesis, we connect the arithmetic functions L_{LD}, L_{LI}, the dynamical zeta function $\hat{\zeta}(s)$, and the class of H-numbers. Throughout we write

$$\hat{G}(s) := G_b(s), \qquad \hat{\zeta}(s) := \zeta_b(s) = \hat{G}(s)H(s),$$

and we use the notation L_{LD}, L_{LI} for the functions denoted LLD, LLI in Section 8. The growth bounds established for H-numbers suggest that they

constitute the analytically dominant part of the dynamical series, while the injectivity results suggest that they form an "arithmetically regular" core of the successor map.

15.1 Decomposition of $\hat{G}(s)$ by H-numbers

Recall the dynamical zeta function from Definition 5.4:

$$\hat{G}(s) = \sum_{n\geq 1} \frac{1}{\Phi(n)^s}.$$

Let $\mathcal{H}$ denote the set of H-numbers (Definition 12.1). We decompose the series into an *H-part* and a *complementary part*:

$$\hat{G}(s) = \hat{G}_{\mathcal{H}}(s) + \hat{G}_{\text{sing}}(s), \qquad \hat{G}_{\mathcal{H}}(s) := \sum_{n\in\mathcal{H}} \frac{1}{\Phi(n)^s}, \quad \hat{G}_{\text{sing}}(s) := \sum_{n\notin\mathcal{H}} \frac{1}{\Phi(n)^s}.$$

By Lemma 12.2, for every $n \in \mathcal{H}$ we have the quadratic bound $\Phi(n) < n^2$. Consequently, the terms in $\hat{G}_{\mathcal{H}}(s)$ satisfy

$$\frac{1}{\Phi(n)^s} > \frac{1}{n^{2s}},$$

so their decay is at best quadratic in n. In contrast, under the heuristic of "fast growth away from H-primes" (Hypothesis A in Section 14), terms with $n \notin \mathcal{H}$ would satisfy

$$\Phi(n) \gg n^{1+\varepsilon}$$

for some fixed $\varepsilon > 0$ (or even exhibit exponential growth), making $\hat{G}_{\text{sing}}(s)$ converge very rapidly for $\Re s > 1$.

Remark 15.1. Heuristically, this decomposition suggests that any slow divergence or possible singular behaviour of $\hat{G}(s)$ (and hence of $\hat{\zeta}(s) = \hat{G}(s)H(s)$) near its abscissa of convergence is driven primarily by the H-numbers. In particular, if $\hat{G}(s)$ were to develop a pole at some $\sigma_0 > 1$, then its main contribution would naturally be attributed to $\hat{G}_{\mathcal{H}}(s)$ rather than to the complementary part $\hat{G}_{\text{sing}}(s)$.

15.2 Arithmetical regularity on H-numbers

We recall the injectivity criterion from Theorem 8.9:

$$\Phi \text{ is injective} \iff L_{LD}(\Phi(n)) = \tau(n) \quad \text{for all } n \geq 1.$$

Moreover, for every n we always have

$$L_{LD}(\Phi(n)) = \tau(\Phi(n)) \leq \tau(n),$$

with strict inequality for some n if and only if Φ is not injective. On the other hand, Proposition 12.5 shows that Φ is injective on the set of H-primes.

It is therefore natural to view H-numbers as candidates for an "arithmetically regular" region of the dynamics where the LI/LD-decomposition behaves in a particularly tame way. Extrapolating from the prime case, one might conjecture that, for $n \in \mathcal{H}$, the image $\Phi(n)$ preserves much of the divisor structure of n in the sense that the defect

$$\tau(n) - L_{LD}(\Phi(n)) = \tau(n) - \tau(\Phi(n))$$

is typically small or even vanishes.

Using the identity

$$\hat{\zeta}(s) = \hat{G}(s)H(s) = \sum_{n \geq 1} \frac{c(n)}{n^s}, \qquad c(n) = a(\ell_{LI}(n)),$$

from Section 7.3, we make the following observations.

1. **On H-numbers.** If Φ is injective on $\mathcal{H}$, then for any $u \in \Phi(\mathcal{H})$ the multiplicity is $a(u) = 1$. Consequently, on the set $\Phi(\mathcal{H})$ the coefficients of $\hat{\zeta}(s)$ coincide with those of the Riemann zeta function (all equal to 1). Heuristically, if $\mathcal{H}$ has positive density in an appropriate sense, this suggests that H-numbers contribute the "least degenerate" part of the dynamical factor.

2. **The L_{LD}-witness.** The value $L_{LD}(\Phi(n)) = \tau(\Phi(n))$ serves as an arithmetic witness for how far $\Phi(n)$ is from preserving the divisor structure of n. For H-primes p we rigorously have $L_{LD}(\Phi(p)) = 2 = \tau(p)$, so the defect vanishes. It is natural to conjecture that this phenomenon extends, at least frequently, to composite H-numbers.

From this point of view, H-numbers form the region where the "exotic" arithmetic functions L_{LD} and L_{LI} synchronize best with the classical divisor function τ, and where the dynamical factorization underlying $\hat{\zeta}(s)$ exhibits minimal defect. This supports the heuristic picture of an H-dominant regime both analytically and arithmetically.

16 Conclusion and outlook

The central theme of this paper has been to combine a structural LI/LD–decomposition of the primes with the successor map

$$\Phi(p) = \min\{q \text{ prime} : q \equiv 1 \pmod{p}\},$$

and to use this interaction to obtain both dynamical Dirichlet series and arithmetic information about the values of Φ. We showed that the image of

Φ consists precisely of the linearly independent primes and that every LI-prime admits a unique predecessor under Φ, whereas LD-primes never occur as successors. Extending Φ multiplicatively to all positive integers leads to a natural notion of LI- and LD-numbers and to a factorisation $\zeta = G \cdot H$ of the Riemann zeta function into LI- and LD-zeta factors, together with a dynamical Dirichlet series G_b built from the successor values $\Phi(n)$.

On the level of integers, the maps ℓ_{LI}, ℓ_{LD} isolate the LI- and LD-components of n, and the divisor sums LLD, LLI encode global information about the LI/LD–structure. This allowed us to reinterpret the coefficients of the dynamically weighted zeta function $\zeta_b(s) = G_b(s)H(s)$ arithmetically as $c(n) = a(\ell_{LI}(n))$, where $a(u)$ counts the preimages of u under Φ, and to formulate a clean injectivity criterion:

$$\Phi \text{ is injective } \iff LLD(\Phi(n)) = \tau(n) \quad \text{for all } n \geq 1.$$

Thus the injectivity of the successor map is completely encoded by the behaviour of a divisor sum built from the LD-component.

The unimodular Φ-lattice provides a second structural pillar: choosing the exponent vectors of LI-primes as a $\mathbb{Z}$-basis, every LD-prime admits an explicit and unique representation of $p-1$ as a product of integer powers of $(r-1)$ for LI-primes $r < p$. This yields logarithmic relations of the form

$$\log(p-1) = \sum_{r<p,\ r\ \mathrm{LI}} c_r(p)\ \log(r-1),$$

and, together with the stabilising operator ψ and its terminal value $\psi_\infty(p)$, leads to an infinite descent mechanism via the map α. These constructions tie the successor dynamics to the LI/LD–basis in a rigid way and suggest that the local structure of Φ-orbits is strongly constrained by the lattice geometry.

In the second part of the paper we used the multiplicative extension of Φ to derive lower bounds in the factorial decomposition, culminating in a class of H-numbers defined by the growth condition $\Phi(n) \leq \log \Phi(n!)$. For H-numbers we showed a quadratic upper bound $\Phi(n) < n^2$, which contrasts sharply with the general exponential bounds known for $\Phi(p)$, and we proved that Φ is injective on H-primes. Numerical computations up to 500 indicate that H-primes occur with a positive proportion among the primes and exhibit no collisions under Φ, supporting the idea that H-primes form a large and arithmetically regular subset of the primes.

Finally, we proposed a heuristic that combines the surjectivity of Φ onto LI-primes, the unimodular lattice structure, and a fast-growth hypothesis away from H-primes to argue that there should be infinitely many H-primes. In this picture, H-numbers support an "H-dominant" regime for the dynamical zeta function $\hat{\zeta}(s) = \zeta_b(s)$: they are expected to govern any slow divergence or singularity of $\hat{G}(s) = G_b(s)$ near its abscissa of convergence, and,

arithmetically, they are the region where LLD and LLI synchronize best with the classical divisor function τ.

Several natural questions remain open. Chief among them are the global injectivity of Φ, the distribution of LI- and LD-primes, the analytic continuation and possible functional equations of G, H and G_b, and the existence and density of H-primes. The framework developed here reduces many of these problems to quantitative questions about the typical size of $\Phi(n)$ and the multiplicities $a(u)$, and suggests a concrete programme for further investigation at the interface of prime distribution, Dirichlet series, and arithmetic dynamics.

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory, Vol. 1: Efficient Algorithms*, MIT Press, Cambridge, MA, 1996.

[2] R. G. Wilson v, "Table of $n, a(n)$ for $n = 1 \ldots 10000$," electronic table, available at the On-Line Encyclopedia of Integer Sequences, e.g. entry A066674.

[3] E. Bach and L. Huelsbergen, "Statistical evidence for small generating sets," *Mathematics of Computation* **61** (1993), 69–82.

[4] E. Bach and J. Sorenson, "Explicit bounds for primes in residue classes," *Mathematics of Computation* **65** (1996), 1717–1735.

[5] D. R. Heath-Brown, "Almost-primes in arithmetic progressions and short intervals," *Mathematical Proceedings of the Cambridge Philosophical Society* **83** (1978), 357–375.

[6] D. R. Heath-Brown, "Siegel zeros and the least prime in an arithmetic progression," *Quarterly Journal of Mathematics (Oxford Ser. 2)* **41** (1990), 405–418.

[7] D. R. Heath-Brown, "Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression," *Proceedings of the London Mathematical Society* (3) **64** (1992), 265–338.

[8] S. S. Wagstaff, Jr., "Greatest of the least primes in arithmetic progressions having a given modulus," *Mathematics of Computation* **33** (1979), 1073–1080.

[9] T. Xylouris, "On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions," *Acta Arithmetica* **150** (2011), no. 1, 65–91.

[10] E. Labos, "A066674: Least number m such that $\varphi(m)$ is divisible by the n-th prime," *The On-Line Encyclopedia of Integer Sequences*, published electronically at `https://oeis.org/A066674`, 2001, accessed November 22, 2025.

[11] MATHOVERFLOWUSER, "Can every natural number be written as a product of integer powers of primes minus 1?" Question on *MathOverflow*, `https://mathoverflow.net/questions/503948`, asked November 16, 2025, accessed November 22, 2025.

[12] G. Martin, "Reference for a conjecture on the first primes congruent to 1 modulo other primes," Question on *MathOverflow*, `https://mathoverflow.net/questions/149670`, asked November 22, 2013, accessed November 22, 2025.

[13] O. Leka and ChatGPT 5.1, *Linear independent prime numbers*, preprint, 2025. Available at `https://www.orges-leka.de/linear_independent_prime_numbers.pdf`.