# Analytic Number Theory
# Lecture 2

Mariusz Mirek
Rutgers University

Padova, March 13, 2025.

Supported by the NSF grant DMS-2154712,
and the CAREER grant DMS-2236493.

# Arithmetic functions

## Definition

An arithmetic function is a map $f : \mathbb{Z}_+ \to \mathbb{C}$, i.e., a sequence of complex numbers, although this viewpoint is not very useful.

## Examples of arithmetic functions

- The constant $\mathbf{1}$ and the identity Id functions are defined respectively by

$$\mathbf{1}(n) := 1 \qquad \text{and} \qquad \mathrm{Id}(n) := n \quad \text{for all} \quad n \in \mathbb{Z}_+.$$

- The Dirac delta function $\delta_m$ is defined as follows

$$\delta_m(n) = \begin{cases} 1 & \text{if } n = m, \\ 0 & \text{otherwise.} \end{cases}$$

  We shall abbreviate $\delta_1$ to $\delta$.

- The divisor function $\tau(n)$ is the number of positive divisors of $n \in \mathbb{Z}_+$,

$$\tau(n) := \#\{d \in \mathbb{Z}_+ : d \mid n\} = \sum_{d|n} 1.$$

  Some authors also use the notation $d(n)$ for the divisor function.

# Examples of arithmetic functions

- More generally, the sum of powers of divisors is defined by

$$\sigma_k(n) := \sum_{d|n} d^k, \quad \text{where} \quad k \in \mathbb{N}.$$

  Observe that $\tau(n) = \sigma_0(n)$, and we abbreviate $\sigma_1$ to $\sigma$.
- The Euler totient function $\varphi$ is defined by

$$\varphi(n) := \#\{m \in [n] : (n,m) = 1\} = \sum_{m \in [n]} \delta((n,m)).$$

- The function $\omega$ is defined as follows: $\omega(1) = 0$ and $\omega(n)$ counts the number of distinct prime factors of $n$ for all $n \geq 2$.
- The function $\Omega$ is defined as follows: $\Omega(1) = 0$ and $\Omega(n)$ counts the number of prime factors of $n$ with multiplicities for all $n \geq 2$.
- The Liouville function $\lambda$ is defined as follows

$$\lambda(n) = (-1)^{\Omega(n)}.$$

# Examples of arithmetic functions

- The Möbius function $\mu(n)$ is defined as follows

$$\mu(n) := \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes}, \\ 0 & \text{if } n \text{ is divisible by the square of a prime.} \end{cases}$$

- The von Mangoldt function $\Lambda(n)$ is defined as follows

$$\Lambda(n) := \begin{cases} \log p & \text{if } n = p^k \text{ is a prime power}, \\ 0 & \text{otherwise.} \end{cases}$$

- Clearly, sums and products of arithmetic functions are still arithmetic functions.

$$(f+g)(n) := f(n) + g(n) \quad \text{and} \quad (f \cdot g)(n) := f(n) \cdot g(n).$$

- The other ways of multiplying arithmetic functions, such as Dirichlet convolution, will be discussed shortly.

# Rings

## Definition

A ring is defined as a set $\mathbb{K} := (\mathbb{K}, +, \cdot)$ equipped with two binary operations, commonly denoted as addition $+$, and multiplication $\cdot$, such that

(i) $(\mathbb{K}, +)$ is an abelian group, meaning that:
  - There exists an additive identity $0 \in \mathbb{K}$ such that $a + 0 = 0 + a = a$ for all $a \in \mathbb{K}$.
  - For every $a \in \mathbb{K}$, there exists an additive inverse $-a \in \mathbb{K}$ such that $a + (-a) = 0$.
  - Addition is commutative: $a + b = b + a$ for all $a, b \in \mathbb{K}$.
  - Addition is associative: $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{K}$.

(ii) $(\mathbb{K}, \cdot)$ is a monoid under multiplication, meaning that:
  - Multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbb{K}$.
  - There exists a multiplicative identity $1 \in \mathbb{K}$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in \mathbb{K}$.

(iii) Multiplication is distributive with respect to addition, meaning that:
  - For all $a, b, c \in \mathbb{K}$, the following hold:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

# Examples of rings

- We say that a ring $\mathbb{K}$ is commutative, if it satisfies conditions (i)–(iii) and additionally
$$xy = yx \quad \text{for all} \quad x, y \in \mathbb{K}.$$
- The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are examples of commutative rings. The set $M_2(\mathbb{C})$ of $2 \times 2$ matrices with complex coefficients and the usual matrix addition and multiplication is a noncommutative ring.
- Let $\mathbb{K}$ and $\mathbb{L}$ be rings with multiplicative identities $1_{\mathbb{K}}$ and $1_{\mathbb{L}}$, respectively. A map $f : \mathbb{K} \to \mathbb{L}$ is called a ring homomorphism if
$$f(x+y) = f(x)+f(y) \quad \text{and} \quad f(xy) = f(x)f(y) \text{ for all } x, y \in \mathbb{K}, \text{ and } f(1_R) = 1_S.$$
- An element $a$ in the ring $\mathbb{K}$ is called a unit or invertible element if there exists an element $x \in \mathbb{K}$, (which in fact is unique), such that
$$ax = xa = 1.$$
Then $x$ is called the inverse for $a$ and is denoted by $a^{-1}$.
- The set $\mathbb{K}^{\times}$ of all units in $\mathbb{K}$ forms a multiplicative group, called the group of units in the ring $\mathbb{K}$.
- A field is a commutative ring in which every nonzero element is a unit. For example, the rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$ are fields. The integers $\mathbb{Z}$ form a ring but not a field, and the only units in the ring of integers are $\pm 1$.

# Dirichlet convolutions

## Definition

The Dirichlet convolution $f \star g$ is defined by

$$(f \star g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right),$$

where the sum is over all positive divisors $d$ of $n$. Dirichlet convolution occurs frequently in multiplicative problems in elementary number theory.

## Theorem

*The set $\mathbb{A} := (\mathbb{A}, +, \star)$ of all complex-valued arithmetic functions, with addition $+$ defined by pointwise sum and multiplication $\star$ defined by Dirichlet convolution, is a commutative ring with additive identity $0$ and multiplicative identity $\delta$, which is the Dirac delta at $1$. Furthermore, if $f(1) \neq 0$, then $f$ is invertible.*

## Proof.

Let $\mathbb{D}(n) := \{d \in [n] : d \mid n\}$ be the set of all positive divisors of $n$.

$$(f \star g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d),$$

since the mapping $\mathbb{D}(n) \ni d \mapsto n/d \in \mathbb{D}(n)$ is one-to-one.

# Proof

- Now let $f$, $g$ and $h$ be three arithmetic functions and $n \in \mathbb{Z}_+$. Then

$$((f \star g) \star h)(n) = \sum_{d|n} (f \star g)(d) h\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{c|d} f(c) g\left(\frac{d}{c}\right) h\left(\frac{n}{d}\right),$$

  and

$$(f \star (g \star h))(n) = \sum_{d|n} f(d)(g \star h)\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \sum_{c|(n/d)} g(c) h\left(\frac{n}{cd}\right).$$

  Setting $e = cd$ in the last inner sum gives

$$(f \star (g \star h))(n) = \sum_{e|n} \sum_{d|e} f(d) g\left(\frac{e}{d}\right) h\left(\frac{n}{e}\right) = ((f \star g) \star h)(n)$$

  establishing the associativity.
- We also have

$$(\delta \star f)(n) = \sum_{d|n} \delta(d) f\left(\frac{n}{d}\right) = f(n).$$

# Proof

- Finally, we prove the invertibility by constructing inductively the inverse $g$ of an arithmetic function $f$ satisfying $f(1) \neq 0$. The function $g$ is the inverse of $f$ if and only if $(f \star g)(1) = 1$ and $(f \star g)(n) = 0$ for all $n > 1$. This is equivalent to

$$\begin{cases} f(1)g(1) = 1, \\ \sum_{d|n} g(d)f\left(\frac{n}{d}\right) = 0 \quad \text{for} \quad n \geqslant 2. \end{cases}$$

- Since $f(1) \neq 0$, we have $g(1) = f(1)^{-1}$ by the first equation. Now let $n > 1$ and assume that we have proved that there exist unique values $g(1), \ldots, g(n-1)$ satisfying the above equations. Since $f(1) \neq 0$, the second equation above is equivalent to

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d \neq n}} g(d)f\left(\frac{n}{d}\right),$$

which determines $g(n)$ in a unique way by the induction hypothesis, and this definition of $g(n)$ shows that the equations above are satisfied, which completes the proof. □

# Multiplicative functions

## Definition

Let $f : \mathbb{Z}_+ \to \mathbb{C}$ be an arithmetic function.

- The function $f$ is said to be multiplicative if $f(1) \neq 0$ and if, for all positive integers $m, n \in \mathbb{Z}_+$ such that $(m, n) = 1$, we have

$$f(mn) = f(m)f(n).$$

- The function $f$ is completely multiplicative if $f(1) \neq 0$ and if the condition

$$f(mn) = f(m)f(n)$$

holds for all positive integers $m$ and $n$.

- The function $f$ is strongly multiplicative if $f$ is multiplicative and if $f(p^\alpha) = f(p)$ for all prime powers $p^\alpha$.

## Remark

The condition $f(1) \neq 0$ is a convention to exclude the zero function from the set of multiplicative functions. Furthermore, it is easily seen that if $f$ and $g$ are multiplicative, then so are $fg$ and $f/g$ with $g \neq 0$ for the quotient.

# Additive functions

Let $f : \mathbb{Z}_+ \to \mathbb{C}$ be an arithmetic function.

- The function $f$ is said to be additive if for all positive integers $m, n \in \mathbb{Z}_+$ such that $(m, n) = 1$, we have

$$f(mn) = f(m) + f(n).$$

- The function $f$ is completely additive if the condition

$$f(mn) = f(m) + f(n)$$

holds for all positive integers $m$ and $n$.

- The function $f$ is strongly additive if $f$ is multiplicative and if $f(p^\alpha) = f(p)$ for all prime powers $p^\alpha$.

# Additive and multiplicative functions: simple criterium

## Lemma (Exercise, prove it!)

*Let $f : \mathbb{Z}_+ \to \mathbb{C}$ be an arithmetic function.*

(i) *$f$ is multiplicative if and only if $f(1) = 1$ and for all $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where the $p_i$ are distinct primes, we have*

$$f(n) = \prod_{j \in [r]} f\left(p_j^{\alpha_j}\right).$$

(ii) *$f$ is additive if and only if $f(1) = 0$ and for all $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where the $p_i$ are distinct primes, we have*

$$f(n) = \sum_{j \in [r]} f\left(p_j^{\alpha_j}\right).$$

## Theorem

*If $f, g : \mathbb{Z}_+ \to \mathbb{C}$ are multiplicative, then so is $f \star g$.*

# Proof

- Let $f$ and $g$ be two multiplicative functions and let $m, n \in \mathbb{Z}_+$ be such that $(m, n) = 1$.
- Note that each divisor $d$ of $mn$ can be written uniquely in the form $d = ab$ with $a \mid m$, and $b \mid n$ and $(a, b) = 1$.
- Hence,

$$(f \star g)(mn) = \sum_{d|mn} f(d) g\left(\frac{mn}{d}\right) = \sum_{a|m} \sum_{b|n} f(ab) g\left(\frac{mn}{ab}\right).$$

- Since $f$ and $g$ are multiplicative and $(a, b) = (m/a, n/b) = 1$, we infer that

$$(f \star g)(mn) = \sum_{a|m} \sum_{b|n} f(a) f(b) g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right) = (f \star g)(m)(f \star g)(n)$$

as required. $\square$

# Examples

- The functions $\mathbf{1}$, Id, $\delta$ are completely multiplicative, whereas log and $\Omega$ are strongly additive and consequently the function $\lambda$ is completely multiplicative.
- Since $\tau = \mathbf{1} \star \mathbf{1}$, $\sigma = \mathbf{1} \star \mathrm{Id}$ and $\sigma_k = \mathbf{1} \star \mathrm{Id}^k$ and both $\mathbf{1}$ and Id are completely multiplicative, so are $d, \sigma$ and $\sigma_k$.
- It is easily seen that, for all $m, n \in \mathbb{Z}_+$, we have

  $$\omega(mn) = \omega(m) + \omega(n) - \omega(m, n),$$

  since in the sum $\omega(m) + \omega(n)$, the prime factors of $(m, n)$ have been counted twice. This implies the additivity of $\omega$.
- The Möbius function $\mu(n)$ is multiplicative. Indeed, $\mu(1) = 1$ and for all prime powers $p^\alpha$, we also have

  $$\mu(p^\alpha) = \begin{cases} -1, & \text{if } \alpha = 1, \\ 0, & \text{otherwise.} \end{cases}$$

  So that, if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ where the $p_i$ are distinct primes, we have

  $$\mu(p_1^{\alpha_1}) \cdots \mu(p_r^{\alpha_r}) = \begin{cases} (-1)^r, & \text{if } \alpha_1 = \cdots = \alpha_r = 1, \\ 0, & \text{otherwise.} \end{cases}$$

  Hence $\mu(p_1^{\alpha_1}) \cdots \mu(p_r^{\alpha_r}) = \mu(n)$ as desired.

# Properties of Möbius function

- We intend to prove the following identity $\mu \star \mathbf{1} = \delta$, i.e.

$$(\mu \star \mathbf{1})(n) = \sum_{d|n} \mu(d) = \delta(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1. \end{cases}$$

- Now since $\mu$ and $\mathbf{1}$ are multiplicative, so is the function $\mu \star \mathbf{1}$ by the previous theorem and hence $(\mu \star \mathbf{1})(1) = 1 = \delta(1)$ is true for $n = 1$.
- Besides, it is sufficient to prove $\mu \star \mathbf{1} = \delta$ for prime powers by the previous lemma, which is easy to check. Indeed,

$$(\mu \star \mathbf{1})\left(p^\alpha\right) = \sum_{j=0}^{\alpha} \mu\left(p^j\right) = \mu(1) + \mu(p) = 1 - 1 = 0 = \delta(p^\alpha)$$

as asserted.

- Using the identity $\mu \star \mathbf{1} = \delta$, we deduce

$$g = f \star \mathbf{1} \quad \Longleftrightarrow \quad g \star \mu = f \star (\mathbf{1} \star \mu) = f.$$

This relation is called the Möbius inversion formula.

# Möbius inversion formula

The Möbius inversion formula is a key part of the estimates of average orders of certain multiplicative functions.

## Theorem (Möbius inversion formula)

*Let $f$ and $g$ be two arithmetic functions. Then we have*

$$g = f \star \mathbf{1} \quad \iff \quad f = g \star \mu$$

*Equivalently, by expanding Dirichlet's convolution, we have*

$$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) \quad \textit{for all} \quad \mathbb{Z}_+.$$

## Lemma

*For every $p \in \mathbb{P}$ and $\alpha \in \mathbb{N}$, one has*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

## Proof.

The desired conclusion follows from the observation that

$$[\,p^\alpha] \setminus \{m \in [\,p^\alpha] : (m, p^\alpha) = 1\} = \{p, 2p, \ldots, p^{\alpha-1}p\}. \qquad \square$$

# Euler's totient function

- Euler's totient function is multiplicative and $\varphi = \mu \star \mathrm{Id}$. Indeed, since $\mu \star \mathbf{1} = \delta$, then we have

$$\sum_{d|(m,n)} \mu(d) = \begin{cases} 1, & \text{if } (m,n) = 1 \\ 0, & \text{otherwise} \end{cases}$$

so that

$$\varphi(n) = \sum_{\substack{m \leqslant n \\ (m,n)=1}} 1 = \sum_{m \leqslant n} \sum_{d|(m,n)} \mu(d) = \sum_{d|n} \mu(d) \sum_{\substack{m \leqslant n \\ d|m}} 1$$
$$= \sum_{d|n} \mu(d) \left[\frac{n}{d}\right] = \sum_{d|n} \mu(d) \frac{n}{d} = (\mu \star \mathbf{1})(n),$$

which proves that $\varphi$ is multiplicative, as are both $\mu$ and $\mathbf{1}$.

- By the previous lemma, we have

$$\varphi\left(p^\alpha\right) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right),$$

and by the multiplicativity we obtain

$$\varphi\left(n\right) = n \prod_{\substack{p|n \\ p \in \mathbb{P}}} \left(1 - \frac{1}{p}\right).$$

# Further properties of multiplicative functions

## Theorem

*If both $g$ and $f \star g$ are multiplicative, then $f$ is also multiplicative.*

## Proof.

We shall assume that $f$ is not multiplicative and deduce that $h = f * g$ is also not multiplicative.

- Since $f$ is not multiplicative, there exist positive integers $m, n \in \mathbb{Z}_+$ with $(m, n) = 1$ such that

  $$f(mn) \neq f(m)f(n).$$

  We choose $m, n \in \mathbb{Z}_+$ for which the product $mn$ is as small as possible.
- If $mn = 1$, then $f(1) \neq f(1)f(1)$ so $f(1) \neq 1$. Since

  $$h(1) = f(1)g(1) \neq 1,$$

  this shows that $h$ is not multiplicative.
- If $mn > 1$, then we have

  $$f(ab) = f(a)f(b)$$

  for all $a, b \in \mathbb{Z}_+$ with $(a, b) = 1$ and $ab < mn$.

# Proof

- Except that in the sum defining $h(mn)$, we separate the term corresponding to $a = m$ and $b = n$. We then have

$$
\begin{aligned}
h(mn) &= \sum_{\substack{a|m,b|n \\ ab<mn}} f(ab)g\left(\frac{mn}{ab}\right) + f(mn)g(1) \\
&= \sum_{\substack{a|m,b|n \\ ab<mn}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) + f(mn) \\
&= \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right) - f(m)f(n) + f(mn) \\
&= h(m)h(n) - f(m)f(n) + f(mn).
\end{aligned}
$$

- Since $f(mn) \neq f(m)f(n)$, this shows that $h(mn) \neq h(m)h(n)$, so $h$ is not multiplicative. This contradiction completes the proof. □

# Further properties of multiplicative functions

## Theorem

*If $g$ is multiplicative, then so is $g^{-1}$, its Dirichlet inverse. In particular, the set of all multiplicative functions forms a multiplicative group with multiplication defined by the Dirichlet convolution.*

## Proof.

This follows from the previous theorem since both $g$ and $g \star g^{-1} = \delta$ are multiplicative. Hence $g^{-1}$ is also multiplicative. $\square$

## Theorem

*If $f$ is multiplicative, then we have*

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n}(1 - f(p)).$$

## Proof.

Let $g(n) := \sum_{d|n} \mu(d)f(d)$. This function is multiplicative, so to determine $g(n)$ it suffices to compute $g(p^\alpha)$. We have

$$g(p^\alpha) = \sum_{d|p^\alpha} \mu(d)f(d) = f(1) - \mu(p)f(p) = 1 - f(p). \qquad \square$$

# Multiplicative functions at infinity

## Theorem

*Let f be a multiplicative function. If*

$$\lim_{p^k \to \infty} f(p^k) = 0,$$

*as $p^k$ runs through the sequence of all prime powers, then*

$$\lim_{n \to \infty} f(n) = 0.$$

## Proof.

- Since
$$\lim_{p^k \to \infty} f(p^k) = 0,$$
it follows that there exist only finitely many prime powers $p^k$ such that $|f(p^k)| \geq 1$.
- We can define
$$A = \prod_{p^k : |f(p^k)| \geq 1} |f(p^k)|.$$
- Then $A \geq 1$.

## Proof

- Fix $\varepsilon \in (0,1)$ and choose a sufficiently large integer $N \in \mathbb{Z}_+$ such that for every $p^k > N$ we have
$$|f(p^k)| < \frac{\varepsilon}{A},$$
- If $n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$ then
$$f(n) = \prod_{p \in \mathbb{P}} f(p^{\nu_p(n)}) = \prod_{\substack{p \in \mathbb{P} \\ p^k \leq N}} f(p^{\nu_p(n)}) \prod_{\substack{p \in \mathbb{P} \\ p^k > N}} f(p^{\nu_p(n)}).$$
- If $n \in \mathbb{Z}_+$ is sufficiently large then there is at least one factor in the second product and consequently
$$\prod_{\substack{p \in \mathbb{P} \\ p^k > N}} |f(p^{\nu_p(n)})| < \frac{\varepsilon}{A}.$$
- On the other hand, the first factor is at most $A$ and we conclude that
$$|f(n)| \leq A \cdot \frac{\varepsilon}{A} = \varepsilon.$$

This completes the proof. □

# Estimates for the divisors function

## Theorem

*For every* $\varepsilon > 0$*, there exists a constant* $C_\varepsilon \in \mathbb{R}_+$ *such that*

$$\tau(n) \leq C_\varepsilon n^\varepsilon$$

## Proof.

- Let $\varepsilon > 0$. The function $f(n) = \frac{\tau(n)}{n^\varepsilon}$ is multiplicative.
- In view of the previous theorem, it suffices to prove that

$$\lim_{p^k \to \infty} f(p^k) = 0$$

  for every prime number $p \in \mathbb{P}$.
- Since $\tau(p^k) = k + 1$, we observe that

$$f(p^k) = \frac{\tau(p^k)}{p^{k\varepsilon}} = \frac{k+1}{p^{k\varepsilon/2}} \frac{1}{p^{k\varepsilon/2}}.$$

- Since $\frac{k+1}{p^{k\varepsilon/2}}$ is bounded, the desired conclusion follows. $\square$

# Estimates for the Euler totient function

## Theorem

*For every $\varepsilon > 0$, there exists a constant $C_\varepsilon \in \mathbb{R}_+$ such that*

$$C_\varepsilon n^{1-\varepsilon} \leq \varphi(n) < n.$$

## Proof.

The upper bound is clear. For the lower bound, we will proceed similarly to the previous theorem.

- Let $\varepsilon > 0$. The function $f(n) = \frac{n^{1-\varepsilon}}{\varphi(n)}$ is multiplicative.
- It suffices to prove that

  $$\lim_{p^k \to \infty} f(p^k) = 0$$

  for every prime number $p \in \mathbb{P}$.
- Since $\varphi(p^k) = p^k - p^{k-1}$ and $\frac{p}{p-1} \leq 2$ for every $p \in \mathbb{P}$, we obtain

  $$\frac{p^{k(1-\varepsilon)}}{\varphi(p^k)} = \frac{p^{k(1-\varepsilon)}}{p^k - p^{k-1}} = \frac{p}{p-1}\frac{p^{k(1-\varepsilon)}}{p^k} \leq \frac{2}{p^{\varepsilon k}}.$$

- The last term tends to 0 as $p^k \to \infty$, and the theorem follows. □

# von Mangoldt function

The von Mangoldt function is an example of a function that is neither multiplicative nor additive.

## Lemma

*For every $n \in \mathbb{Z}_+$ we have*

$$(\Lambda \star \mathbf{1})(n) = \sum_{d|n} \Lambda(d) = \log n.$$

## Proof.

- The theorem is true if $n = 1$ since both sides are 0. Therefore, assume that $n > 1$ and write $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. Then

$$\log n = \sum_{i=1}^{r} \alpha_i \log p_i.$$

- The only nonzero terms in the sum $\sum_{d|n} \Lambda(d)$ come from those divisors $d$ of the form $p_k^m$ for $m \in [a_k]$ and $k \in [r]$. Hence, we have

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{r} \sum_{m=1}^{a_i} \Lambda(p_i^m) = \sum_{i=1}^{r} \sum_{m=1}^{a_i} \log p_i = \sum_{i=1}^{r} a_i \log p_i = \log n. \qquad \square$$

# Properties of the von Mangoldt function

## Theorem

*If $n \geq 2$, we have*

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d.$$

## Proof.

- We know that $(\Lambda \star \mathbf{1})(n) = \sum_{d|n} \Lambda(d) = \log n$. So inverting this formula by using the Möbius inversion formula, we obtain

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d,$$

  which simplifies to

$$\Lambda(n) = \delta(n) \log n - \sum_{d|n} \mu(d) \log d.$$

- Since $\delta(n) \log n = 0$ for all $n \in \mathbb{Z}_+$, the proof is complete.

# Derivation

Recall that a derivation on a ring $\mathbb{K}$ is an additive homomorphism $D : \mathbb{K} \to \mathbb{K}$ such that

$$D(xy) = D(x)y + xD(y) \quad \text{for all} \quad x, y \in \mathbb{K}.$$

## Theorem

*Let $L(n) = \log n$ for all $n \in \mathbb{Z}_+$. Pointwise multiplication by $L(n)$ is a derivation on the ring of arithmetic functions $\mathbb{A}$.*

## Proof.

- If $d \mid n$, then $L(n) = L(d) + L\left(\frac{n}{d}\right)$. We must prove that

$$L \cdot (f \star g) = (L \cdot f) \star g + f \star (L \cdot g) \quad \text{for all} \quad f, g \in \mathbb{A}.$$

- We have

$$\begin{aligned} L \cdot (f \star g)(n) &= \sum_{d|n} L(n) f(d) g\left(\frac{n}{d}\right) \\ &= \sum_{d|n} (L \cdot f)(d) g\left(\frac{n}{d}\right) + \sum_{d|n} f(d)(L \cdot g)\left(\frac{n}{d}\right). \end{aligned}$$

This implies the desired result. □

# The Selberg identity

## Theorem

*For $n \in \mathbb{Z}_+$ we have*

$$\Lambda(n)\log n + \sum_{d|n} \Lambda(d)\Lambda\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)\log\left(\frac{n}{d}\right)^2.$$

*Equivalently, we have $L \cdot \Lambda + \Lambda \star \Lambda = \mu \star L^2$.*

## Proof.

- Observe that $\Lambda \star \mathbf{1} = L$.
- Thus by the previous theorem we have

$$L^2 = L \cdot (\Lambda \star \mathbf{1}) = (L \cdot \Lambda) \star \mathbf{1} + \Lambda \star (L \cdot \mathbf{1}).$$

- Since $\Lambda \star \mathbf{1} = L$, we obtain

$$L^2 = (L \cdot \Lambda) \star \mathbf{1} + \Lambda \star \Lambda \star \mathbf{1}.$$

- Multiplying the last identity by $\mathbf{1}^{-1} = \mu$, which follows from the Möbius inversion formula, we obtain the desired bound. □

# Dirichlet series

In view of the multiplicative properties of certain arithmetic functions, we use Dirichlet series rather than power series in analytic number theory.

## Definition

Let $f \in \mathbb{A}$ be an arithmetic function. The formal Dirichlet series of a variable $s \in \mathbb{C}$ associated to $f$ is defined by

$$D(s,f) := \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

Here, we ignore convergence problems, and $D(s,f)$ is the complex number equal to the sum when it converges.

## Examples

- $D(s,\delta) = 1$.
- Presumably, the most important example of a Dirichlet series is the Riemann zeta function
$$D(s,\mathbf{1}) = \zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

# Importance of the Dirichlet convolution

## Proposition

*Let $f, g$ and $h$ be three arithmetic functions. Then*

$$h = f \star g \quad \Longleftrightarrow \quad D(s,h) = D(s,f) \cdot D(s,g).$$

## Proof.

We have

$$D(s,f) \cdot D(s,g) = \sum_{k,m=1}^{\infty} \frac{f(k)g(m)}{(km)^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{n=1}^{\infty} \frac{(f \star g)(n)}{n^s},$$

which completes the proof. □

## Remark

The set $\mathbb{D} := (\mathbb{D}, +, \cdot)$ of formal Dirichlet series with addition $+$ and multiplication $\cdot$ defined respectively by

$$D(s,f) + D(s,g) = D(s,f+g), \quad \text{and} \quad D(s,f) \cdot D(s,g) = D(s,f \star g),$$

forms a commutative ring with additive identity 0 and multiplicative identity 1, which is isomorphic to the ring of arithmetic functions $\mathbb{A} = (\mathbb{A}, +, \star)$ via the mapping $\mathbb{A} \ni f \mapsto D(s,f) \in \mathbb{D}$.

# Dirichlet series for multiplicative functions

## Proposition

*Let $f$ be an arithmetic function. Then $f$ is multiplicative if and only if*

$$D(s,f) = \prod_{p \in \mathbb{P}} \left( 1 + \sum_{k=1}^{\infty} \frac{f\left(p^k\right)}{p^{sk}} \right).$$

*The above product is called the Euler product of $D(s,f)$.*

## Proof.

Expanding the product we obtain a formal sum of all products of the form

$$\frac{f(p_1^{a_1}) \cdots f(p_r^{a_r})}{(p_1^{a_1} \cdots p_r^{a_r})^s},$$

where $p_1, \ldots, p_r$ are distinct prime numbers, $a_1, \ldots, a_r \in \mathbb{Z}_+$, and $r \in \mathbb{N}$.

- By multiplicativity, the numerator can be written as $f(p_1^{a_1} \cdots p_r^{a_r})$.
- The Fundamental Theorem of Arithmetic implies that the products $p_1^{a_1} \cdots p_r^{a_r}$ are in one-to-one correspondence with all natural numbers.

This gives a formal proof of the desired identity. □

# Examples

- By the previous proposition $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}$, hence

$$\frac{1}{\zeta(s)} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

  which implies $\mu \star \mathbf{1} = \delta$.
- Taking logarithm we obtain

$$\log \zeta(s) = \sum_{p \in \mathbb{P}} \log \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{p \in \mathbb{P}} \sum_{k=1}^{\infty} \frac{1}{kp^{ks}}$$

- By formal differentiation, we have

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p \in \mathbb{P}} \sum_{k=1}^{\infty} \frac{\log p}{p^{ks}} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

- On the other hand, we have

$$-\zeta'(s) = \sum_{n=1}^{\infty} \frac{\log n}{n^s}.$$

- Thus $\Lambda = \mu \star \log$ and consequently $\Lambda \star \mathbf{1} = \log$.